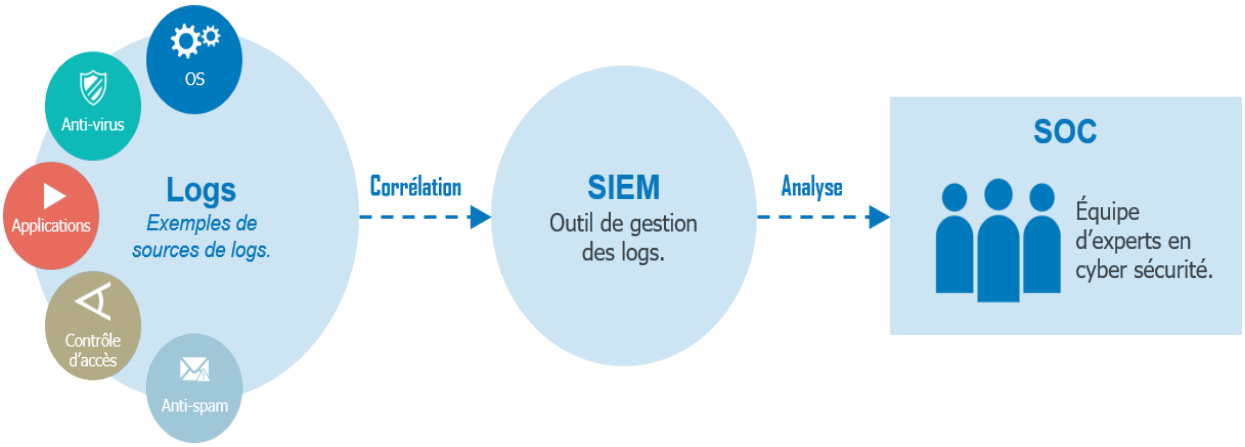
Evaluation : Supervision sécurité SIEM



Dhiya LAYADI | Lotfi DERRI

24/09/2020

Supervision SIEM – MSI P9

Encadré par : Tarek RADAH

Exercice 1 :

1. **Citez la source de logs qui permet d'identifier les accès aux partages de fichiers.**

Réponse :

La source de loge qui permet d’identifier l'accès au partage de fichier et WINDOWS SECURITY LOG avec le ID 5140: A network share object was accessed

Exemple de la 5140 :

```
A network share object was accessed.

Subject:

   Security ID:  ACME-FR\Administrator

   Account Name:  Administrator

   Account Domain:  ACME-FR

   Logon ID:  0x74a739

Network Information:

   Source Address:  10.42.42.221

   Source Port:  65097
```

On peut aussi les consulter à travers WINDOWS EVENT VIEWER.

Exercice 2 :

Event ID	Name
15	FileCreateHash

L’Event ID numéro 15 vise à capturer un événement lorsqu’un il y a un flux correspondant à un fichier, qui provient du navigateur, donc il permet d’identifier les fichiers téléchargés depuis internet via un browser.

Exercice 3 :

- Contournement de l’UAC avec l’Event Viewer

```
Title: UAC Bypass via Event Viewer
author: Lotfi Derri / Dhiya Layadi
logsource:
   Product: windows
   Service: sysmon
detection:
      methregistry:
          TargetObject: 'HKU\\*\mscfile\shell\open\command'
      methprocess:
          ParentImage: '*\eventvwr.exe'
      filterprocess:
          Image: '*\mmc.exe'
      condition: (methprocess and methregistry) and  not filterprocess
```

Description :

Cette règle permet de détecter la méthode de contournement de l'UAC à l'aide du visualiseur d'événements Windows. Elle va se baser sur l’utilisation de l'objet command via l'exécutable mmc.exe.

- Reverse Shell

```
title: Suspicious Reverse Shell Command Line
author: Lotfi Derri / Dhiya Layadi
Logsource:
   product: Windows
detection:
keywords:
   -  while read line 0<65; do'
   -  ‘; socket(S, PF_INET , SOCK_STREAM, getprotobyname(“ntcp”));if(connect(S,
      sockaddre_in($p, inet_aton($i))))’
   -  ; systemS_ whileo;
   -  $sendbyte ( [text. encoding] : :ASCII) .GetBytes ($sendback2); $stream.
      Write ($sendbyte , 0, $sendbyte. Length); $stream. Flush()}
```

```
    -   'while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;'
    -   '$data = (New-Object -TypeName
        System.Text.ASCIIEncoding).GetString($bytes,0, $i);'
    -   $sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);
    -   $stream.Write($sendbyte,0,$sendbyte.Length);
    -   'while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;'
    -   '$data = (New-Object -TypeName
        System.Text.ASCIIEncoding).GetString($bytes,0, $i);'
    -   '$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);'
    -   '$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};'
condition: keywords
Level: high
```

Description :

Cette règle permet de détecter les commandes shell suspectes ou le code de programme qui peut être exécuté ou utilisé en ligne de commande pour établir un reverse shell sous différente langage tel que python et surtout powershell.

- Technique T1170

```
title: MSHTA Spawning Windows Shell
author: Lotfi Derri / Dhiya Layadi
Logsource:
   product: Windows
   service: sysmon
detection:
keywords:
   selection:
      EventID: 1
      ParentImage:
          -   '*\mshta.exe'
      Image:
          -   '*\cmd.exe'
          -   '*\powershell.exe'
          -   '*\wscript.exe'
          -   '*\sh.exe'
          -   '*\bash.exe'
   condition: selection
Level: high
```

Description :

Cette règle permet de détecter un exécutable en ligne de commande Windows lancé depuis la MSHTA (**M**icro**S**oft **HT**ml **A**pplication)

- Technique T1060

```
title: Persistence via Windows Registry Run Keys with Visual Basic Scripting
author: Lotfi Derri / Dhiya Layadi
Logsource:
   product: Windows
   service: security
detection:
keywords:
   selection:
      EventID: 4688
      NewProcessName:
          -  ‘add’
          -  ‘.vbs’
   selection1:
      ProcessCommandLine:
          -  '\Software\Microsoft\Windows\CurrentVersion\Run'
          -  '\Software\Microsoft\Windows\CurrentVersion\RunOnce'
          -  '\Software\Microsoft\Windows\CurrentVersion\RunOnceEx'
          -  '\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce'
          -  '\Software\Microsoft\Windows\CurrentVersion\RunServices'
          -  '\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run'
   condition: selection and selection1
Level: high
```

Description :

Cette règle va permettre de détecter l'ajout d'un script de base visuel à la clé d'exécution du registre Windows. Les adversaires peuvent obtenir la persistance en ajoutant un programme à une clé d'exécution du registre. L'ajout d'une entrée aux "clés d'exécution" dans le registre entraînera l'exécution du programme référencé lorsqu'un utilisateur se connecte.

- Exécution de macro suspicieux

```
title: VBA DLL Loaded Via Microsoft Word
status: experimental
author: Lotfi Derri / Dhiya Layadi
logsource:
      category: image_load
      product: windows
detection:
      selection:
      Image:
```

```
            - '*\winword.exe'
            - '*\powerpnt.exe'
            - '*\excel.exe'
            - '*\outlook.exe'
      ImageLoaded:
            - '*\VBE7.DLL'
            - '*\VBEUI.DLL'
            - '*\VBE7INTL.DLL'
            - '*\dsparse.dll*'
      condition: selection
```

Description :

Cette règle permet de détecter les DLL chargées via un mot contenant des macros VBA. En utilisant les DLL permettant le lancement de VBA, en empêchant celle ci d'être utilisée, on va suspendre l'exécution des macros VBA.

- Dump de la NTDS

```
title: Activity Related to NTDS.dit Domain Hash Retrieval
author: Lotfi Derri / Dhiya Layadi
Logsource:
   product: Windows
   service: sysmon
detection:
keywords:
   selection:
      EventID: 1
      CommandLine:
          #Ransomware
          -  'vssadmin.exe Delete Shadows'
          #Hacking
          -  'vssadmin create shadow /for=C:'
          -  'copy \\?\GLOBALROOT\Device\*\windows\ntds\ntds.dit'
          -  'copy \\?\GLOBALROOT\Device\*\config\SAM'
          -  'vssadmin delete shadows /for=C:'
          -  'reg SAVE HKLM\SYSTEM'
   condition: selection
```

Description :

Cette règle permet de détecter les commandes suspectes qui pourraient être liées à une activité qui utilise la copie de volume pour voler et récupérer à distance les hachs du fichier NTDS.dit

- Injection de DLL par MSBUILD

```
title: Ainject dll msbuild
author: Lotfi Derri / Dhiya Layadi
Logsource:
   product: Windows
   category:image_load
detection:
   selection:
     ImageLoaded:
    -'\*.dll'
     Image:
     - '\msbuild.exe'
 filter:
       Image|contains: 'Visual Studio'

condition: (ImageLoaded AND Image) and not filter
```

Description :

Cette règle permet de détecter les téléchargements de DLL par l'exécutable "*msbuild.exe*".

Exercice 4 :

1. **Donnez les règles de détection qui correspondent aux outils (SIGMA Rules)**

- Mimikatz

```
title: Mimikatz détection
author: Lotfi Derri / Dhiya Layadi
logsource:
       category: process_creation
       product: windows
detection:
       selection_1:
       CommandLine|contains:
              - DumpCreds
              - invoke-mimikatz
       selection_2:
```

```
      CommandLine|contains:
            - rpc
            - token
            - crypto
            - dpapi
            - sekurlsa
            - kerberos
            - lsadump
            - privilege
            - process
      selection_3:
      CommandLine|contains:
            - '::'
      condition: selection_1 or selection_2 and selection_3
```

Description :

Cette règle va permettre de détecter les commandes réalisées par Mimikatz en filtrant sur celles-ci.

- PowerShell Dnscat2

```
title: Dnscat powershell Execution
status: experimental
author: Lotfi Derri / Dhiya Layadi
logsource:
      product: windows
      service: powershell
detection:
      selection:
      EventID: 4104
      ScriptBlockText|contains: "Start-Dnscat2"
      condition: selection
```

Description :

Cette règle permet de détecter l'envoi d'informations via des trames DNS, on va donc empêcher le lancement de "*start_Dnscat2*" pour éviter ce genre d'incident.

Exercice 5 :

Cette méthode permet de détecter les services malveillants mentionnés dans le rapport sur les pipettes PNG de Turla, publié par le groupe NCC en novembre 2018. La famille de pipettes, appelée en interne PNG_dropper, a été observée comme outil de deuxième étape dans différentes attaques ciblées. L'une des dernières charges utiles créées par ce dropper est une variante d'Uroburos utilisée par le groupe Turla, qui opère traditionnellement depuis la Russie. Cette technique est utilisée pour permettre aux attaquants de dissimuler leurs charges utiles secondaires, en contournant les différents produits audiovisuels. Les attaquants, quelles que soient leurs compétences et leurs motivations, tentent souvent d'envelopper le code malveillant d'une manière qui semblera inoffensive aux praticiens et aux produits de sécurité.

```
title: Turla Droper Detection.

author: Lotfi Derri / Dhiya Layadi
logsource:
      product: Windows
      service: system
detection:
     selection_1:
        EventID: 7045
        ServiceName: WerFaultSvc
logsource:
      product: Windows
      service: sysmon
detection:
     selection_2:
        EventID: 1
        file-hash:
            - 6ed939f59476fd31dc4d99e96136e928fbd88aec0d9c59846092c0e93a3c0e27
            - fea27eb2e939e930c8617dcf64366d1649988f30555f6ee9cd09fe54e4bc22b3
            - eca66eed6966ed237252630bf353336bbb6789daa5764afba45e43108c7cd536
      CommandLine:
            - "*kernel32.dll"
      condition: selection_1 or selection_2
```

Description :

Pour la règle sigma on va utiliser les hash connu de sysmon pour empêcher l'exécution d'un exécutable avec ses hash comme valeur

Du côté système nous allons alerter dès l'apparition d'un evente ID avec la valeur 7045.

Exercice 6 :

1. **Donnez les règles de détections pour la suite des techniques suivante (SIGMA Rules) :**

    1. Initial foothold (Using MSHTA Stag) – T1170

```yaml
title: MSHTA Stage
status: experimental
author: Lotfi Derri / Dhiya Layadi
Logsource:
   product: Windows
   service: sysmon
detection:
    selection:
        ParentImage: '*\mshta.exe'
        Image:
            - '*\cmd.exe'
            - '*\powershell.exe'
            - '*\wscript.exe'
            - '*\cscript.exe'
            - '*\sh.exe'
            - '*\bash.exe'
            - '*\reg.exe'
            - '*\regsvr32.exe'
            - '*\BITSADMIN*'
    condition: selection and not filter
```

Description :

Cette règle permet de détecter un exécutable en ligne de commande Windows lancé depuis la MSHTA (**M**icro**S**oft **HT**ml **A**pplication).

2. Local Recon – T1087

```
title: Suspicious Reconnaissance Activity

status: experimental

author: Lotfi Derri / Dhiya Layadi

logsource:
      category: process_creation
      product: windows
detection:
      selection:
      CommandLine:
            - net group "domain admins" /domain
            - net localgroup administrators
      condition: selection
```

3. SAM Database dump – T1003

On va empêcher l'extraction de la base de données SMA contenant les mot de passe et leurs utilisateurs en empêchant la création de n'importe quel fichier commençant par SAM et ce finissant par .dmp dans le repertoire \AppData ce que font la plupart des outils d'extraction , aussi on va empêcher l'exécution de la commande "*reg save*" pour une extraction manuelle de celui-ci.

```
title: SAM Dump to AppData
status: experimental
author: Lotfi Derri / Dhiya Layadi
logsource:
      product: windows
      service: system
detection:
      selection:
      EventID: 16
      Message:
            - '*\AppData\Local\Temp\SAM-*.dmp *'
      selection2:
      CommandeLine:
      -'reg save hklm\sam'

      condition: selection or selection2
```

4. Pass-The-Hash - T1075

On va détecter la technique d'attaque "*pass the hash*" qui est utilisée pour se déplacer latéralement à l'intérieur du réseau.

L'utilisation réussie du PtH pour les mouvements latéraux entre les postes de travail déclencherait l'événement ID 4624, une tentative de connexion échouée déclencherait l'événement ID 4625.

```
title: Pass the Hash
status: experimental
author: Lotfi Derri / Dhiya Layadi

logsource:
      product: windows
      service: security
detection:
      selection:
      - EventID: 4624
      LogonType: '3'
      LogonProcessName: 'NtLmSsp'
      WorkstationName: '%Workstations%'
      ComputerName: '%Workstations%'
      - EventID: 4625
      LogonType: '3'
      LogonProcessName: 'NtLmSsp'
      WorkstationName: '%Workstations%'
      ComputerName: '%Workstations%'
      filter:
      AccountName: 'ANONYMOUS LOGON'
      condition: selection and not filter
```

5. LSASS memory dump – T1003

On va détecter le processus de vidage de la mémoire ("DUMP") LSASS en utilisant procdump ou taskmgr basé sur le CallTrace généralement cette méthode utilise dbghelp.dll ou dbgcore.dll pour win10

```
title: LSASS Memory Dump
status: experimental
author: Lotfi Derri / Dhiya Layadi
```

```
logsource:
       category: process_access
       product: windows
detection:
       selection:
       TargetImage: 'C:\windows\system32\lsass.exe'
       GrantedAccess: '0x1fffff'
       CallTrace:
       - '*dbghelp.dll*'
       - '*dbgcore.dll
```

6. Getting a domain admin account and attacking DC with PTH attack– T1075

On va détecter une connexion réussie avec le type de connexion 9 (NewCredentials) qui correspond au comportement "*Overpass the Hash*" du module *sekurlsa::pth* de Mimikatz, par exemple.

```
title: Successful Overpass the Hash Attempt

logsource:
       product: windows
       service: security
detection:
       selection:
       EventID: 4624
       LogonType: 9
       LogonProcessName: seclogo
       AuthenticationPackageName: Negotiate
       condition: selection
```

7. NTDS Database dump – T1003

```
title: Activity Related to NTDS.dit Domain Hash Retrieval
status: experimental
author: Lotfi Derri / Dhiya Layadi
logsource:
       category: process_creation
       product: windows
detection:
       selection:
       CommandLine:
              - vssadmin.exe Delete Shadows
              - 'vssadmin create shadow /for=C:'
              - copy \\?\GLOBALROOT\Device\\*\windows\ntds\ntds.dit
       - copy \\?\GLOBALROOT\Device\\*\config\SAM
```

```
        - 'vssadmin delete shadows /for=C:'
              - 'reg SAVE HKLM\SYSTEM '
              - esentutl.exe /y /vss *\ntds.dit*
              - esentutl.exe /y /vss *\SAM
              - esentutl.exe /y /vss *\SYSTEM
        condition: selection
```

Description :

Cette règle permet de détecter les commandes suspectes qui pourraient être liées à une activité qui utilise la copie de volume pour voler et récupérer à distance les hash du fichier NTDS.dit

8. Adding a user to domain admin group to achieve domain persistence

On va détecter une tentative de création de compte admine evc Event ID 4732 puis on va notifier les tentatives de connexion avec des comptes “*admin*”

```
title: User Added to Local Administrators
status: stable
logsource:
        product: windows
        service: security
detection:
        selection:
        EventID: 4732
        selection_group1:
        GroupName: '"domain admins" /domain'
        selection_group2:
        GroupSid: 'S-1-5-32-544'
        selection_connection_AD:
        EventID: 4624
        LogonType: 10
        AuthenticationPackageName: Negotiate
        AccountName: 'Admin-*'
        filter:
        SubjectUserName: '*$'
        condition: (selection and (1 of selection_group*) and not filter )or
selection_connection_AD
```