Les outils du SOC – Protection de l'Endpoint

Antoine Bénar

Objectifs du cours

- Comprendre les bases du fonctionnement des EDR
- Bases en troubleshooting EDR
- Comprendre les rôles et bases de fonctionnements de différents outils de sécurité
  - XDR : complémentarité avec les EDRs
  - SIEM : définition, use cases, mise en place et parsing de logs
  - SOAR : automatisation & orchestration
  - NDR : outils d'analyse réseau
- Présentation d'outils complémentaires : protection O365, sécurité des emails et mobiles
- Présentation de la matrice MITRE
- Démonstrations et manipulation de ces outils

Solutions de sécurité de l’Endpoint

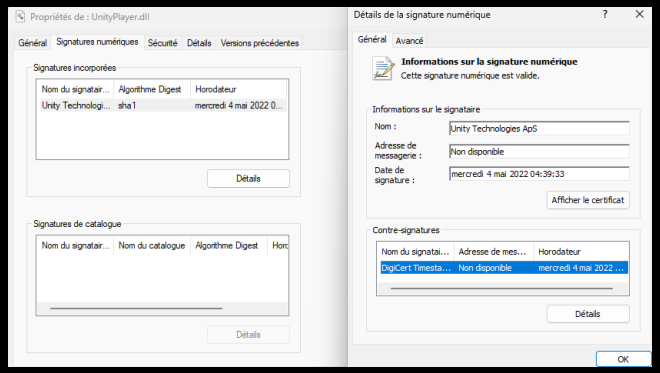
De l’antivirus à l’EDR, en passant par l’EPP et par l’XDR

Disclamer : certains raccourcis sont faits dans le but de rendre ce cours plus compréhensible sans perdre tout le monde!

Fonctionnement original :

L’antivirus

- Nom du fichier
- Métadonnées (strings en clair, commentaires, auteur…)
- Signatures numériques



- Base de données de hash (aka signature ou empreinte)

```
PS C:\> Get-FileHash .\mimikatz.exe -Algorithm SHA256

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          622D709D1CC428F28526904219E4A9764850F012E9F859C4356F16F5EF9B0265       C:\mimikatz.exe

PS C:\> [Text.Encoding]::UTF8.GetString([Convert]::FromBase64String("aidhZG9yZSBvdXRlciB3aWxkcw=="))
```

L’antivirus

Ecriture d’un nouveau fichier → Calcul du hash par l’antivirus → Comparaison avec sa base de données

Fichier non connu

Fichier connu

Mise en quarantaine du fichier

Des limitations !!

L’antivirus

Une histoire en 3 lignes :

```
PS C:\Users\antoi\Downloads> Get-FileHash '.\function Find-AVSignature.ps1'

Algorithm       Hash
---------       ----
SHA256          05997C0A23E36D1C22F5842BD4406B7822D43FAF8D744433D5327377A75AA456
```

```
    [Switch] $Force
)
$test = "pouet pouet je suis un potit blagueur"
#test variables
if (!(Test-Path $Path)) {Throw "File path not found"}
$Response = $True
```

```
PS C:\Users\antoi\Downloads> Get-FileHash '.\function Find-AVSignature.ps1'

Algorithm       Hash
---------       ----
SHA256          69AFF747760D573CFD24C44A6D2B1F7CD31F41FDF35934E061FB5E26ACC8FC66
```

Les noms des fichiers, contenus, signatures etc se modifient très facilement, il est rapidement devenu évident que l’analyse statique ne serait pas suffisante.

L’antivirus : non suffisant

- Monitoring des processus
- Chargement de librairies
- Lecture écriture et modification de fichiers & clés de registres
- Appels de fonctions

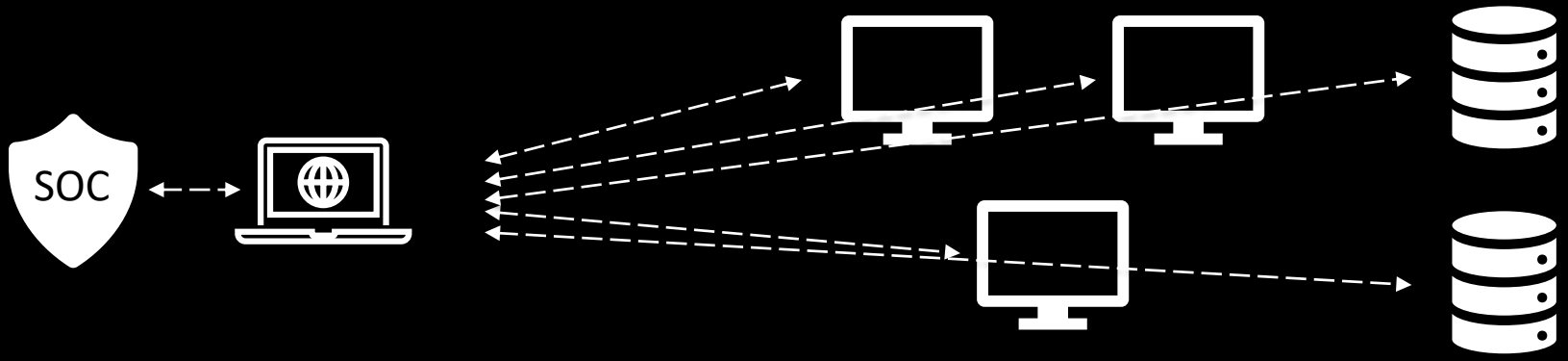
- Analyses de comportements suspects (sessions PS…)
- Tentatives d’évasion
- Journalisation
- Fileless
- IA

L’EDR

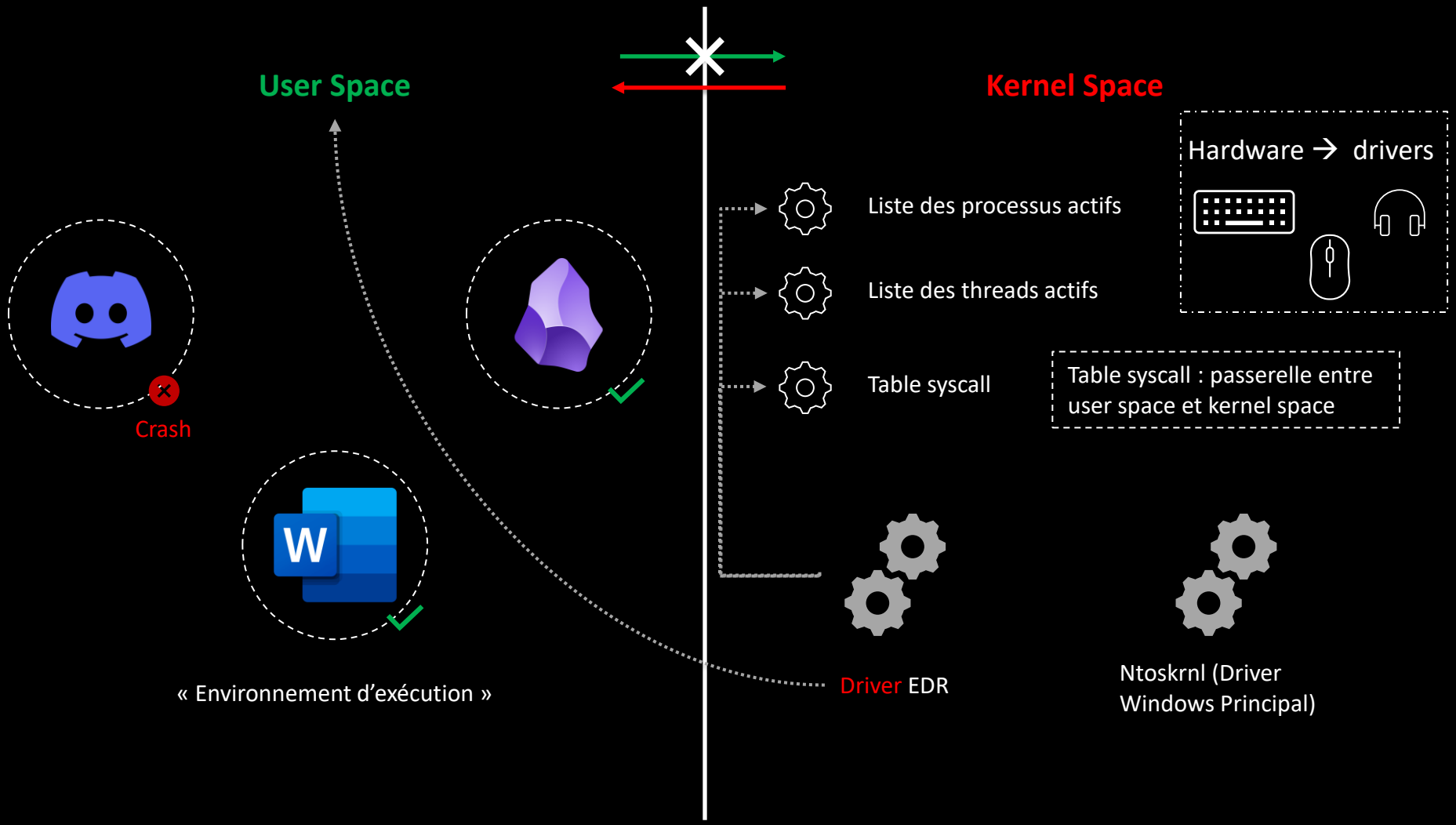
Bon, concrètement, un EDR, c’est quoi ?

L'EDR : Protection des machines

- 1 agent EDR par endpoint protégé
- Une console de management
- « Antivirus boosté »
- Détections comportementales
- Ex : SentinelOne, Cortex, Crowdstrike, HarfangLab



L'EDR - Prérequis



Les moteurs de détections

C’est quoi un moteur de détection ?

Les moteurs sont tous les composants de l’EDR qui génèrent les alertes de sécurités selon différents mécanismes

Moteurs statiques

- Analyse de hashs ~AV
- Règles YARA
- Calcul d’entropie
- Analyse des signatures | certificats
- Analyse des « headers »

Moteurs comportementaux

- Recherche d’anomalies & comportements suspects
- Règles SIGMA
- Heuristiques | IA
- Decoys à ransomwares

Varie beaucoup d’un EDR à l’autre

Règles YARA et SIGMA

Règles YARA

Recherche statique de patterns dans un binaire

```
rule Mimikatz_Detection
{
    meta:
        author = "Antoine"
        description = "Detects binary with a suspicious function name"
        threat_level = 3

    strings:
        $func = "mimikatz"
        $hex_pattern = { E8 ?? ?? ?? ?? 83 C4 04 }  // shellcode, injection

    condition:
        $func or $hex_pattern
}
```

Utilisé avec EDR, AV, Forensic…

Règles SIGMA

Détection d'obfuscation dans Powershell

```
title: Encoded PowerShell Command
id: a1b2c3d4-5678-90ab-cdef-1234567890ab
status: test
description: Detects PowerShell launched with encoded command
author: Antoine
logsource:
  product: windows
  service: security
detection:
  selection:
    EventID: 4688
    NewProcessName|endswith: '\powershell.exe'
    CommandLine|contains: '-EncodedCommand'
  condition: selection
level: medium
tags:
  - Powershell
  - T1027.010
```

Utilisé avec EDR, XDR, SIEM…

https://github.com/Yara-Rules/rules

Focus – les règles YARA

Règles YARA : identification des fichiers, processus, binaires à travers des **patterns** (strings, hexa, regex)

```
rule Mimikatz_Detection
{
    meta:
        author = "Antoine"
        description = "Detects binary with a suspicious function name"
        threat_level = 3

    strings:
        $func = "mimikatz"
        $hex_pattern = { E8 ?? ?? ?? ?? 83 C4 04 }  // shellcode, injection

    condition:
        $func or $hex_pattern
}
```

meta : métadonnées (auteur, version, description)

strings : motifs à rechercher (texte, hex, regex)

condition : logique booléenne (and, or, of, any, for all of them, etc.)

Patterns : **Textuels** ("MZ", "cmd.exe") ; **Hexadécimaux** ({4D 5A} = entête PE)

Regex (/[A-Z0-9._%+-]+@[A-Z0-9.-]+\.[A-Z]{2,}/i)

YARA = *Yet Another Recursive Acronym*

https://github.com/SigmaHQ/sigma

Focus – les règles SIGMA

Règles SIGMA : règles YARA adaptées aux logs
Objectif de standardiser les détections pour les convertir vers la syntaxe du SIEM

```yaml
title: Encoded PowerShell Command
id: a1b2c3d4-5678-90ab-cdef-1234567890ab
status: test
description: Detects PowerShell launched with encoded command
author: Antoine
logsource:
  product: windows
  service: security
detection:
  selection:
    EventID: 4688
    NewProcessName|endswith: '\powershell.exe'
    CommandLine|contains: '-EncodedCommand'
  condition: selection
level: medium
tags:
  - Powershell
  - T1027.010
```

title, description, author : métadonnées

logsource : type de log (process_creation, proxy)…

detection : conditions (sélections, and/or/not)

condition : lien logique entre blocs

level : sévérité (low, medium, high, critical)

Opérateurs :

|contains, |endswith, |startswith, |re, |all, |cidr

Support multi-plateforme :
Windows, Linux, Proxy, Firewall, DNS, Cloud (Azure, AWS…)

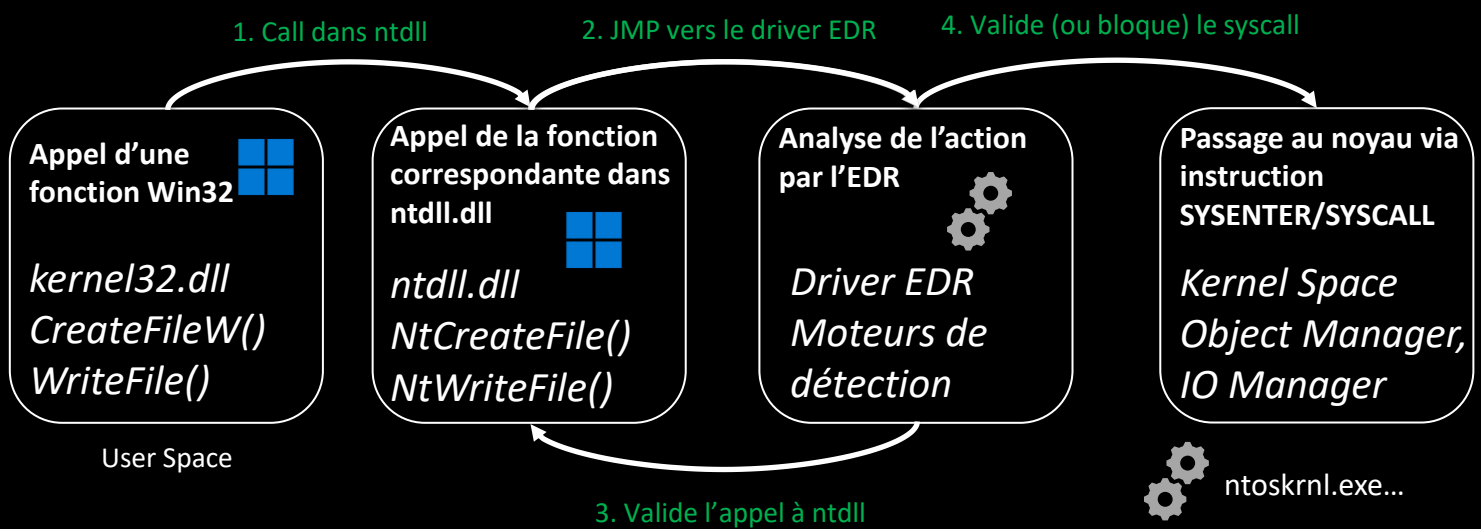
Hooking - Windows

Hooker = intercepter un appel à une fonction

Comment : modifie le pointeur vers la fonction dans son propre espace mémoire, puis le renvoie vers le point de la fonction initialement souhaitée (ou pas !)

Exemple :

```
PS C:\Users\antoi> echo "1234" > .\nouveau_fichier.txt
```



Troubleshooting & Cohabitation

Les règles d'or :

1. Un antivirus et un EDR peuvent coexister, mais pas 2 EDRs
2. Un EDR est complexe, il peut engendrer des problèmes
3. Toujours désactiver l'EDR pour valider son implication avant tout
4. Favoriser les exclusions sur hash que sur dossiers
5. Être le plus granulaire et précis possible sur les exclusions de paths
6. Maintenez à jour vos EDR !

Méthodologie de déploiement

Un token de déploiement est un **identifiant unique** qui permet d'installer / **connecter** un agent à une **console saas** de manière **sécurisée**

- Souvent, un token de déploiement doit être fourni au programme pour s'activer, récupérer sa politique et se connecter à sa console
- Il est souvent communicable dans par **ligne de commande** avec l'installeur, et / ou dans un GUI
- Le plus courant est un déploiement par GPO, SCCM, Intune etc

Parfois, certaines solutions embarquent même des modules d'installation depuis d'autres agents!

Et les autres OS ?

Windows

EDR dans le Kenel Space

Hooking des processus & fonctions

Bonne gestion des logs, troubleshooting et interopérabilité

Monitoring le plus fort, mais malwares les plus évolués

Linux

Pas nativement conçu pour l'EDR

Les EDRs s'appuient sur des outils spécifiques pour le monitoring :

eBPF | auditd | AppArmor | SELinux

Requière une installation en root, mais très compliqué d'empêcher un autre utilisateur root de désinstaller l'agent

MacOS

Système fermé : L'EDR doit passer par l'API Apple (Endpoint Security Framework)

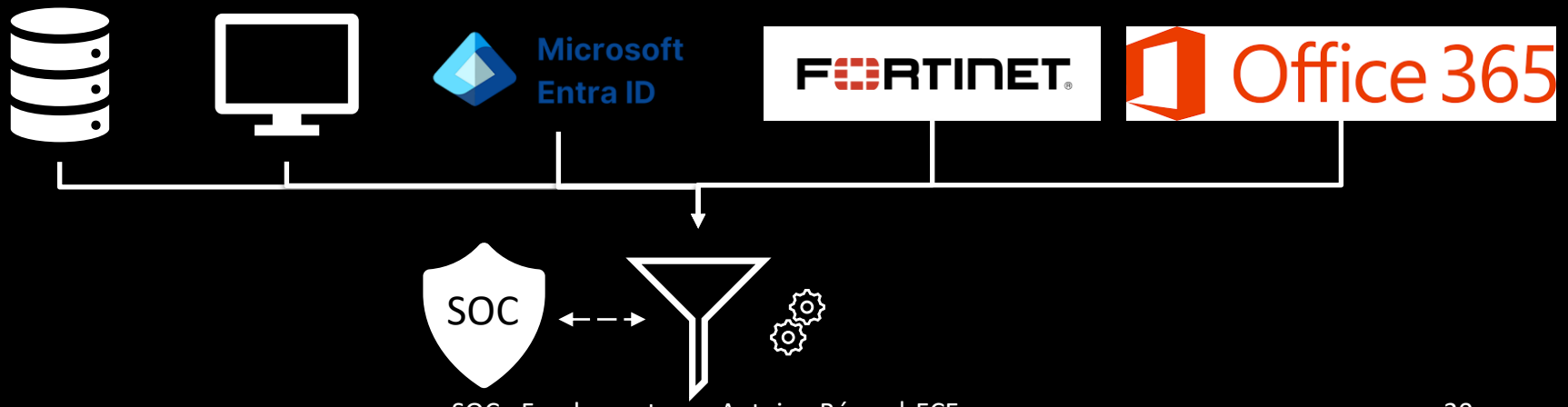
Complexité et efficacité souvent moindre

Déploiement complexe (autorisations, MDM)

Rarement implémenté

Le SIEM

- Un SIEM collecte et corrèle les journaux pour détecter des comportements anormaux.
- « **Puits** » **de logs** permettant les **détections** et **l'investigation**
- Possibilité de mettre des règles de détections



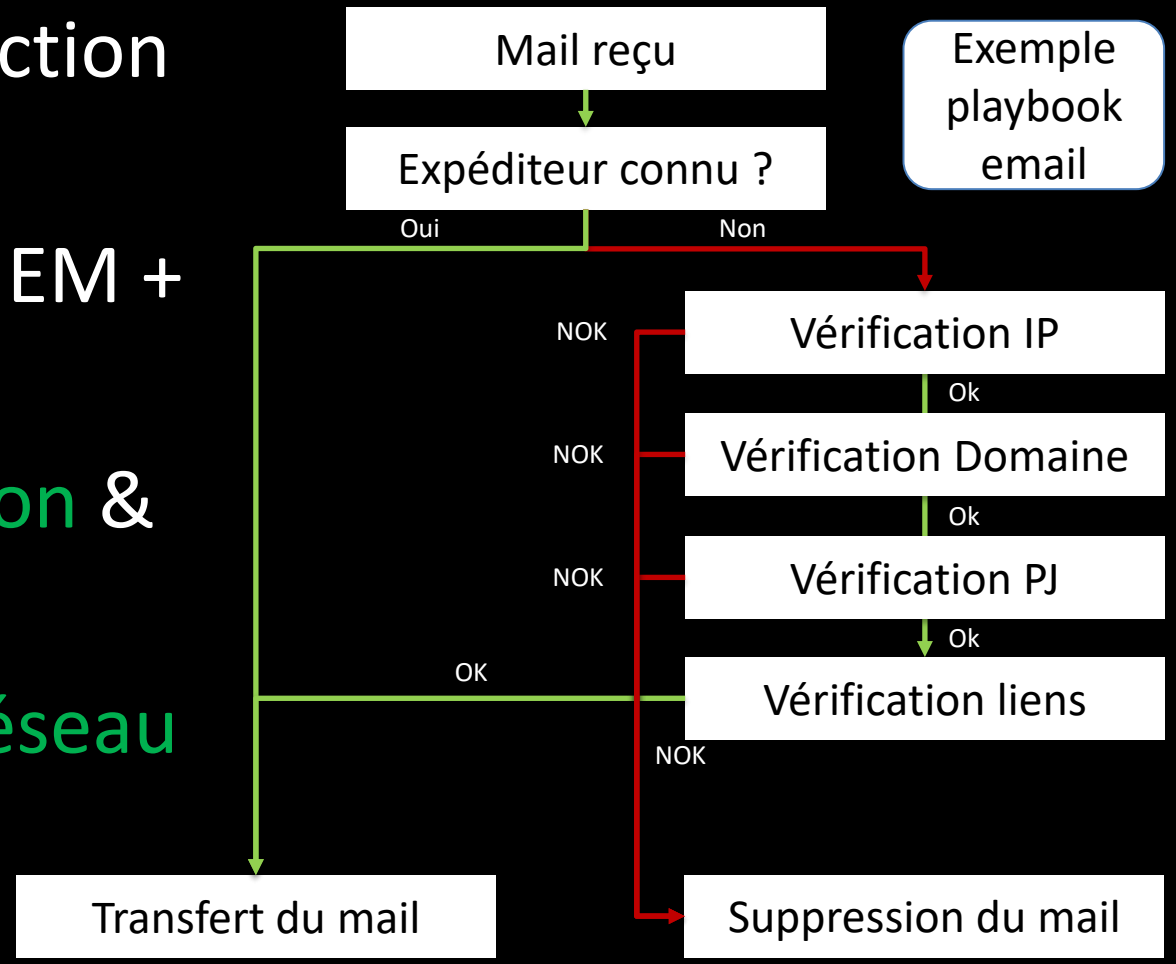
XDR : Protection périmétrique

«Extended» Detection &Response

Souvent, XDR ~ SIEM + EDR + Playbook

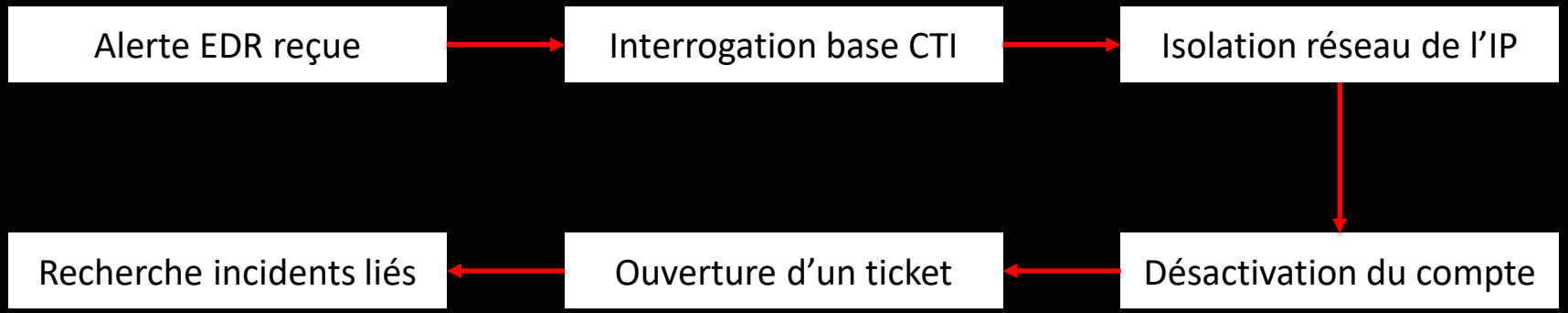
Règles de détection & Playbooks

Surveillance du réseau



Et le SOAR ?

- Le SOAR (Security Orchestration, Automation and Response) automatise les réponses aux alertes et orchestre plusieurs outils
- Exemples : Cortex XSOAR, IBM Resilient



Pour aller plus loin : Réseau & NDR

Les **NDR** | **Network Detection and Response-** sont des solutions de sécurité qui **surveillent le trafic réseau**

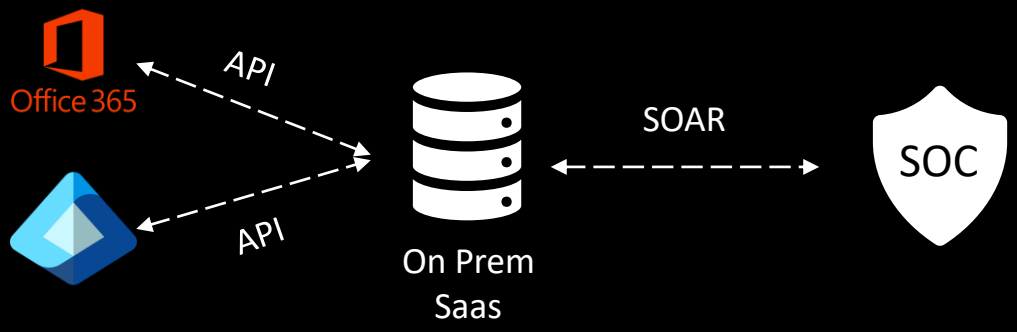
- Similaire à l'XDR mais spécialisé réseau
- Couverture du réseau sans agent (imprimantes, IoT…)
- Installé sur les switchs, TAP, probes, cloud

Exemples : Vectra, Darktrace, Corelight

Solutions spécialisées : O365 & EntraID

- Certaines solutions existent également pour analyser spécifiquement les logs Office 365 et EntraID, et sont souvent utilisées par des SOC plus matures
- Objectifs : détecter les connexions suspectes, sparephishing, exfiltration…

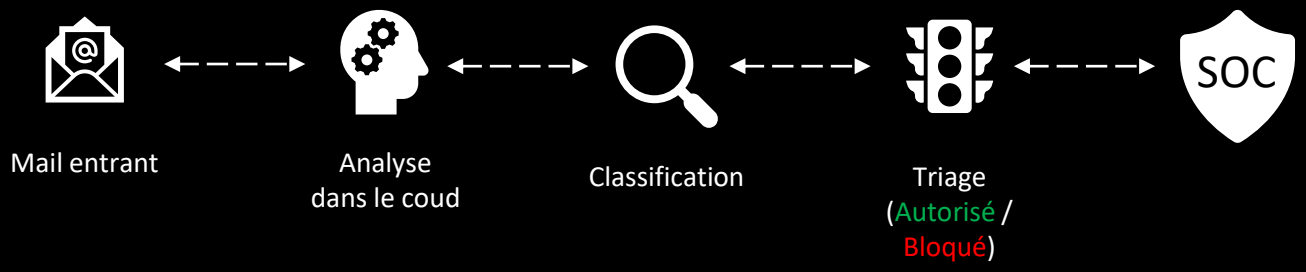
Entra ID est le **service d'identité cloud de Microsoft** pour **gérer et authentifier** les utilisateurs (AD CS).



Exemples : VectraAI, MDO…

Protection des mails

- Chaque mail entrant et sortant est analysé
- L'analyse & gestion se fait dans le cloud
- Classification des mails (ex : bénin, spam, scam, phishing)
- Règles de suppression / déplacement en fonction de la classification



Exemples : VadeSecure, MailinBlack…

Et les mobiles ? – Intro aux MTD

- Le MTD est l'équivalent de l'EDR sur le mobile
- Du fait du support, il va nativement moins loin qu'un EDR en investigation, mais permet tout de même de :
  - Analyser & bloquer les applications non autorisées
  - Analyser le trafic réseau (Mitm, evil twins…)
  - Monitorer tous les paramètres du mobile (VPN, chiffrement, localisation etc etc)
- Pour être plus efficace, il doit être couplé à un MDM (Mobile Device Management)

Ex : Zimperium, Pradeo MTD

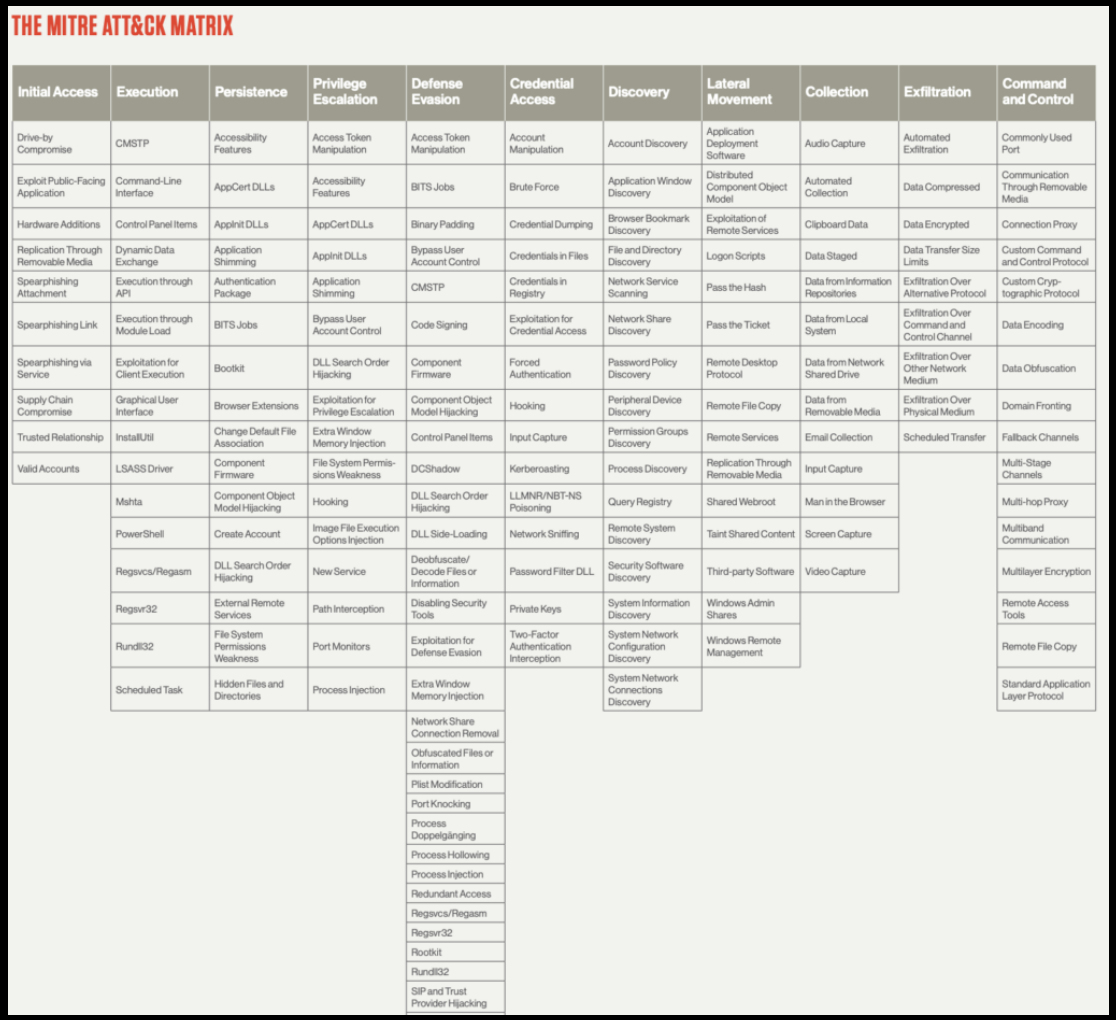
Matrice Mitre

La matrice MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) est une **base de connaissances** publique et gratuite qui **recense les techniques utilisées** par les **cyberattaquants** à chaque étape d'une attaque.

Elle est organisée comme une matrice avec :

- Des tactiques (colonnes) = objectifs de l'attaquant (ex : persistance, exfiltration)
- Des techniques (lignes) = comment l'attaquant atteint ces objectifs (ex : credential dumping, DLL injection)

Matrice Mitre



THE MITRE ATT&CK MATRIX

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	AppCert DLLs	Accessibility Features	BITS Jobs	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Control Panel Items	AppInit DLLs	AppCert DLLs	Binary Padding	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	AppInit DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Logon Scripts	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Execution through API	Authentication Package	Application Shimming	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryp-tographic Protocol
Spearphishing Link	Execution through Module Load	BITS Jobs	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Exploitation for Client Execution	Bootkit	DLL Search Order Hijacking	Component Firmware	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote File Copy	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Permission Groups Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	LSASS Driver	Component Firmware	File System Permis-sions Weakness	DCShadow	Kerberoasting	Process Discovery	Replication Through Removable Media	Input Capture		Multi-Stage Channels
	Mshta	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	Query Registry	Shared Webroot	Man in the Browser		Multi-hop Proxy
	PowerShell	Create Account	Image File Execution Options Injection	DLL Side-Loading	Network Sniffing	Remote System Discovery	Taint Shared Content	Screen Capture		Multiband Communication
	Regsvcs/Regasm	DLL Search Order Hijacking	New Service	Deobfuscate/ Decode Files or Information	Password Filter DLL	Security Software Discovery	Third-party Software	Video Capture		Multilayer Encryption
	Regsvr32	External Remote Services	Path Interception	Disabling Security Tools	Private Keys	System Information Discovery	Windows Admin Shares			Remote Access Tools
	Rundll32	File System Permissions Weakness	Port Monitors	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Network Configuration Discovery	Windows Remote Management			Remote File Copy
	Scheduled Task	Hidden Files and Directories	Process Injection	Extra Window Memory Injection		System Network Connections Discovery				Standard Application Layer Protocol
				Network Share Connection Removal						
				Obfuscated Files or Information						
				Plist Modification						
				Port Knocking						
				Process Doppelgänging						
				Process Hollowing						
				Process Injection						
				Redundant Access						
				Regsvcs/Regasm						
				Regsvr32						
				Rootkit						
				Rundll32						
				SIP and Trust Provider Hijacking						

Matrice souvent implémentée dans les SOCs

Très utile pour la classification, documentation, établissement des criticités

Également pratique pour standardiser (ex règles SIGMA & YARA), constituer la kill chain

https://attack.mitre.org/matrices/enterprise/ - image provenant de CrowdStrike

Lab 1 : consignes

- Groupes de 3 à 4
- Rendu d’un livrable par groupe
- Conseil : un livrable par personne, puis mutualisation

Questions