Notions de base - Réponse à incident

Cours 1

Boussad AIT SALEM

March 18, 2025

Efrei Paris

Introduction

Introduction

- Les cyberattaques sont de plus en plus fréquentes et sophistiquées.
- Une réponse rapide et efficace est essentielle pour minimiser les dégâts.
- **Objectif** : Comprendre les principes fondamentaux de la réponse aux incidents ainsi que l'écosystème dont lequel elle opère.

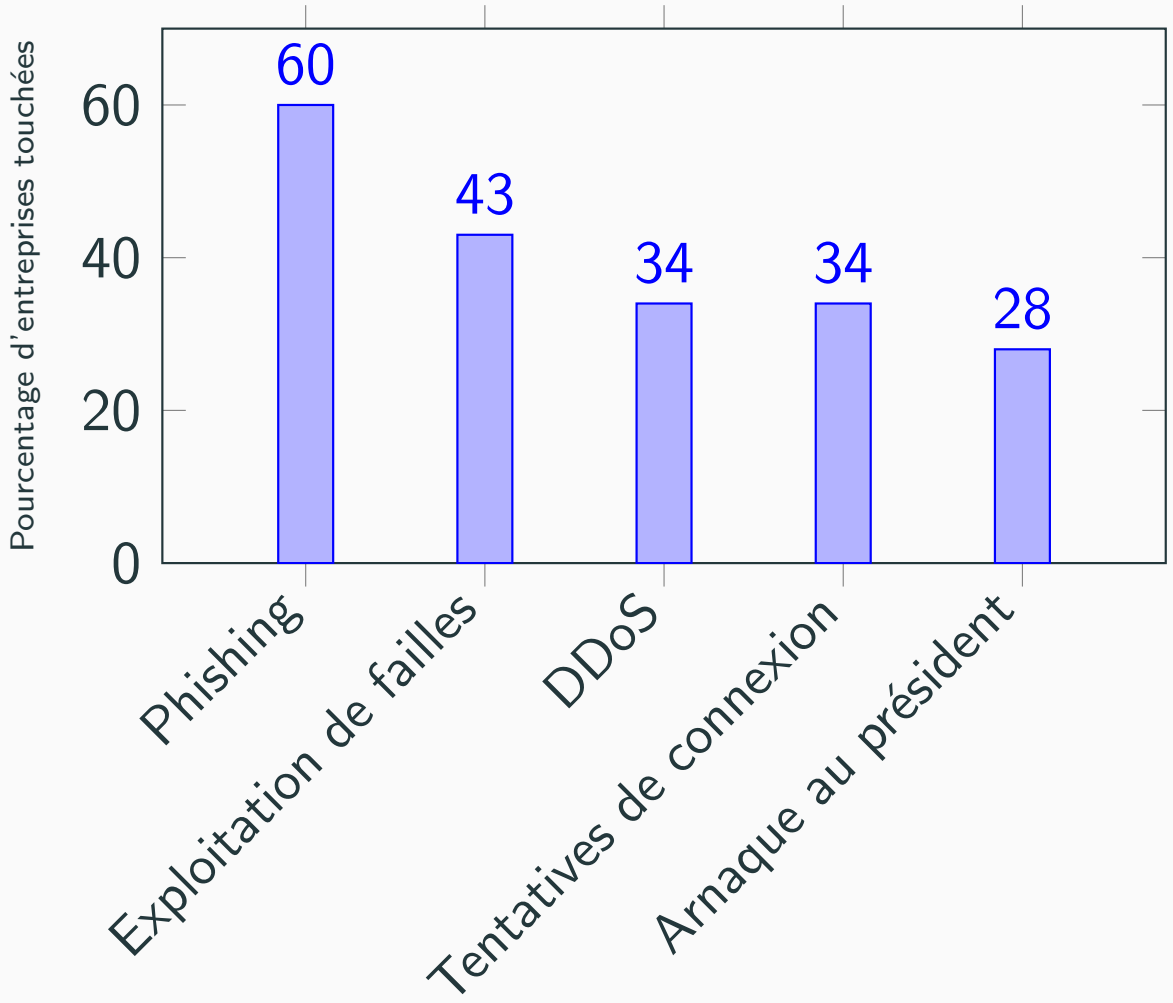
Etat des lieux et nouvelles tendances de la cybermenace en France (2024)

Menaces et Priorités

- **Les cyberattaques représentent une menace majeure** pour les entreprises françaises.
- En 2023, **49% des entreprises françaises ont subi au moins une cyberattaque** (Le 9e baromètre de la cybersécurité des entreprises, réalisé conjointement par le CESIN et OpinionWay en 2024).
- La cybermenace est la **première priorité pour 44% des décideurs en France**, dépassant la moyenne mondiale.
- Les entreprises craignent particulièrement les **ransomwares, les fuites de données et les sanctions liées au RGPD**.

Types d'Attaques

- **Top 5 des cyberattaques** ayant touché les entreprises françaises en 2023:



Notions de base

Security Operation Center (SOC)

Security Operations Center (SOC) - Définition et Rôle

Définition : Un SOC (Security Operations Center) est une unité de cybersécurité chargée de **surveiller, détecter, analyser et répondre** aux menaces de sécurité en temps réel.

Rôle du SOC :

- Surveillance continue des événements de sécurité.
- Analyse et tri des alertes (faux positifs, menaces avérées).
- Réponse aux incidents et escalade au CSIRT/DFIR.
- Gestion des menaces avancées (Threat Hunting, MITRE ATT&CK).

Qu'est-ce qu'un incident ?

- Un incident de cybersécurité est un événement compromettant la **confidentialité, l'intégrité ou la disponibilité** des données.
- Il peut s'agir d'une tentative d'accès non autorisée, d'une infection par un malware, ou d'une fuite de données.
- Importance de différencier :
  - Un simple **événement** d'un véritable **incident** nécessitant une réponse.
  - **Indicators of Compromise (IoC)** et **Indicators of Attack (IoA)** : outils clés pour identifier et analyser les menaces.

Différence entre Événements et Incidents en Cybersécurité

Événement (Event) : Toute activité observée dans un système informatique, pouvant être normale ou anormale.

- Un utilisateur se connecte à son compte avec succès
- Une tentative de connexion échouée
- Un fichier est téléchargé depuis Internet
- Une mise à jour de logiciel est installée
- Une augmentation soudaine du trafic réseau

Incident (Incident) : Un événement compromettant la sécurité du système, nécessitant une réponse.

- Une attaque par ransomware chiffre des fichiers sensibles
- Une exfiltration de données détectée sur un serveur
- Une compromission d'un compte administrateur après plusieurs tentatives
- Un malware détecté sur un poste de travail
- Une attaque DDoS rendant un service indisponible

Résumé : Un événement est une activité observée, tandis qu'un incident représente une menace nécessitant une action immédiate.

Types d'Incidents

- **Intrusions réseau** : Tentatives d'accès non autorisées.
- **Malwares et ransomwares** : Programmes malveillants visant à compromettre le système.
- **Fuites de données** : Perte ou divulgation de données sensibles.
- **Attaques DDoS** : Surcharge d'un service pour le rendre indisponible.
- **Menaces internes** : Actes malveillants ou erreurs des employés.

Indicators of Compromise (IoC)

Définition : Indicator of Compromise est une preuve technique qu'un système a été compromis. Il s'agit d'un indicateur rétrospectif, utilisé après une attaque pour identifier des éléments liés à une compromission.

✓Exemples d'IoC :

- Adresses IP suspectes (ex: 192.168.1.50 utilisée pour une exfiltration de données).
- Hashes de fichiers malveillants (SHA256, MD5 d'un malware).
- Noms de domaine malveillants (ex: malicious-c2.com).
- Registres Windows modifiés (ex: HKLM\Software\Microsoft\Windows\CurrentVersion\Run\malware.exe).
- Signatures de malwares (YARA, ClamAV).

Utilisation : Les IoC permettent de rechercher des traces d'attaques passées, dans les logs **SIEM, EDR, IDS.**

Indicators of Attack (IoA)

Définition : Signaux avant ou pendant une attaque, visant à identifier les intentions des attaquants, indépendamment des outils utilisés.
Indique qu'une attaque est en cours ou sur le point de se produire (comportement anormal ou séquence d'actions correspondant à une technique d'attaque). Contrairement aux IoC, les IoA sont proactifs et se concentrent sur les **tactiques, techniques et procédures (TTP) adverses**.

✓Exemples d'IoA :

- Exécution de PowerShell avec -EncodedCommand (ex: `powershell.exe -EncodedCommand JABvAG...`).
- Création anormale d'un utilisateur avec privilèges admin.
- Exécution de scripts sur plusieurs machines simultanément (signe de mouvement latéral).
- Détection de commandes utilisées par les attaquants (`whoami`, `net user /domain`, `mimikatz`).
- Tunnels réseau chiffrés vers des destinations inconnues.

Utilisation : Les IoA sont utilisés pour **détecter une attaque en cours**, souvent en **Threat Hunting** et **SOC Tier 3**.

Artefacts Forensiques

Définition : Un artefact est une **trace laissée par une activité sur un système**.
C'est un élément neutre qui peut être interprété comme un **IoC** ou un **IoA** selon le contexte.

✓Exemples d'artefacts :

- Logs d'authentification Windows (`Security.evtx`).
- Mémoire RAM (dump mémoire avec Volatility).
- Journaux réseau capturés (PCAP, NetFlow).
- Modifications de fichiers système (`C:\Windows\Prefetch\malware.exe.pf`).

Utilisation : Les artefacts sont exploités par le **DFIR** pour analyser l'attaque après une compromission.

Différences entre IoC et IoA

IoC : Empreintes laissées après une attaque (traces de compromission), basées sur des artefacts numériques connus, permettent une réponse post-incident.

IoA : Activités suspectes avant ou pendant une attaque, basées sur des comportements suspects, permettent une détection proactive. Permet de détecter une menace en amont en analysant les intentions et les techniques utilisées par un attaquant. Exemples : Tactiques et Techniques observées (`MITRE ATT&CK`)

Artefact vs IoC : Quelle différence ?

Artefact

- Trace laissée sur un système (logs, fichiers, clés de registre).
- Peut être **légitime ou malveillant**.
- Utilisé en analyse forensique.
- Exemples :
  - Fichiers logs
  - Clés de registre modifiées
  - Processus en mémoire

IoC (Indicator of Compromise)

- Indicateur spécifique d'une **activité malveillante**.
- Permet de détecter des attaques.
- Utilisé pour la réponse aux incidents.
- Exemples :
  - Adresse IP suspecte
  - Hash de fichier malveillant
  - URL d'un serveur de C2

Analogie : Un artefact est comme une **empreinte dans le sable** (trace neutre), alors qu'un IoC est une **empreinte digitale d'un criminel recherché** (signe confirmé de compromission).

MITRE ATT&CK et son rôle

- Base de données de **Tactiques et Techniques** utilisées par les attaquants.
- Utilisée pour **mapper les IoA** et améliorer la **Threat Intelligence**.
- Permet aux SOC et IR de **détecter, analyser et répondre aux attaques**.
- Outil essentiel pour le **Threat Hunting et la détection proactive**.

Computer Security Incident Response Team (CSIRT)

Définition : Un CSIRT (Computer Security Incident Response Team) est une équipe spécialisée dans la gestion et la réponse aux incidents de cybersécurité. Son rôle est de **détecter, analyser, contenir, éradiquer et prévenir** les attaques informatiques affectant une organisation.

Objectifs :

- Assurer une réponse rapide et efficace aux incidents de sécurité.
- Minimiser les impacts d'une attaque sur l'organisation.
- Fournir une analyse détaillée des menaces et proposer des contre-mesures.
- Échanger des informations sur les menaces avec les **CERT** et les équipes internes.

Rôle et Responsabilités du CSIRT

Principales missions :

- Détection et analyse des incidents en collaboration avec le SOC.
- Coordination de la réponse aux incidents et communication avec les parties prenantes.
- Analyse forensic et investigation post-incident (DFIR).
- Développement et amélioration des processus de réponse aux attaques.
- Mise en place de mesures préventives (mise à jour des règles de détection, durcissement des systèmes).
- Rapport post-incident et recommandations pour éviter une réinfection.

Collaboration : Le CSIRT travaille en étroite collaboration avec le SOC, le DFIR et les équipes de Threat Intelligence pour **améliorer la cybersécurité globale de l'organisation**.

Processus de Réponse à Incident

- **Préparation** : Mise en place de stratégies, d'outils et de formations.
- **Détection et Analyse** : Identification et investigation des menaces (IoC et IoA).
- **Confinement, Éradication, Récupération** : Contenir l'incident, éliminer la menace et restaurer les services.
- **Retour d'expérience** : Analyse post-incident pour améliorer les processus futurs.

Techniques de Réponse à Incident

- **Analyse des journaux** : Identifier les anomalies dans les logs système.
- **Utilisation des IoC et IoA** : Détection proactive des menaces.
- **Isolation des systèmes compromis** : Limiter la propagation d'une attaque.
- **Forensic et investigation numérique** : Collecte et analyse des preuves numériques.
- **Remédiation et renforcement de la sécurité** : Patchs, corrections et formation des équipes.

Frameworks et Standards

- **NIST 800-61** : Guide de gestion des incidents informatiques.
- **SANS Incident Response** : Modèle en 6 étapes pour la gestion des incidents.
- **ISO/IEC 27035** : Norme internationale pour la gestion des incidents de sécurité.

Computer Emergency Response Team (CERT)

Définition : Un CERT (Computer Emergency Response Team) est une entité spécialisée dans la gestion des incidents de cybersécurité à un **niveau national, sectoriel ou organisationnel**. Son rôle est de **prévenir, détecter et coordonner la réponse aux incidents de cybersécurité** en collaboration avec d'autres acteurs de la cybersécurité.

Objectifs :

- Assurer la coordination des réponses aux incidents à grande échelle.
- Diffuser des alertes et recommandations de sécurité aux entités concernées.
- Collaborer avec les CERT nationaux et internationaux pour partager des menaces.
- Analyser les tendances des cyberattaques et publier des rapports.

Différence entre CERT et CSIRT

Périmètre et Responsabilités :

- **CERT** : Coordonne la réponse aux incidents **à un niveau global** (national, sectoriel ou organisationnel). Il joue un rôle **stratégique** en partageant les alertes et en assurant la coordination des interventions.
- **CSIRT** : Répond aux incidents **au sein d'une organisation spécifique**. Il est plus **opérationnel**, menant des investigations approfondies et assurant l'atténuation des menaces.

Principales Différences :

- **CERT** : Prévention, coordination, diffusion d'alertes et assistance aux entités affectées.
- **CSIRT** : Investigation des incidents, réponse technique, forensic et mitigation des menaces.

Exemples d'Intervention d'un CSIRT

Cas 1 : Détection d'un Ransomware

1. Un **SOC Analyst (Tier 1)** reçoit une alerte d'un **EDR** sur une activité suspecte.
2. L'**Incident Responder (Tier 2)** identifie le malware et **met en quarantaine les postes infectés**.
3. Un **Threat Hunter (Tier 3)** analyse le ransomware et crée une **règle YARA** pour éviter une récidive.
4. Le **CSIRT Manager** coordonne la communication et les actions à prendre avec la direction.

Exemples d'Intervention d'un CSIRT

Cas 2 : Exfiltration de Données

1. Une anomalie dans les **logs SIEM** révèle **une connexion suspecte vers un serveur externe**.
2. Le **CSIRT enquête** et découvre un **compte compromis** utilisé pour voler des fichiers sensibles.
3. Le **compte est désactivé**, les accès sont revus, et une **analyse forensic** est menée.
4. Un **rapport est transmis aux autorités et aux régulateurs** si nécessaire.

Analyste SOC (Niveau 1 - Tier 1)

Rôle : Premier tri et escalade des alertes.

Responsabilités :

- Surveille les alertes générées par le SIEM ou l'EDR.
- Analyse en premier lieu les fichiers suspects et les logs associés.
- Vérifie les IoC basiques (hashes, IP, domaines, fichiers suspects).
- Confirme si l'alerte est un faux positif ou une activité malveillante.
- Escalade au SOC Tier 2 si une investigation approfondie est nécessaire.

Analyste SOC (Niveau 2 - Tier 2)

Rôle : Investigation approfondie.

Responsabilités :

- Recherche et collecte les IoC et IoA dans les logs et outils forensic.
- Analyse les artefacts réseau et hôte (fichiers, clés de registre, processus).
- Fait du Threat Intelligence Enrichment en vérifiant VirusTotal, MISP, OTX.
- Utilise YARA Sigma pour identifier des modèles de comportement.
- Mappe les IoA avec MITRE ATT&CK pour identifier les techniques adverses.
- Produit un rapport d'incident et escalade au SOC Tier 3 si nécessaire.

Analyste SOC Senior (Niveau 3 - Tier 3)

Rôle : Analyse avancée et réponse active.

Responsabilités :

- Analyse avancée de la chaîne d'attaque et des TTP adverses.
- Threat Hunting pour rechercher d'autres traces du malware dans les SIEM/EDR.
- Collaboration avec Threat Intelligence pour identifier l'attaque.
- Mise en place de contre-mesures (règles YARA, Sigma, SIEM tuning).
- Isolation des machines compromises et quarantaine des fichiers.
- Alerte au CSIRT si l'incident est critique.

Threat Intelligence (TI)

Définition : Le Threat Intelligence (TI) est l'ensemble des processus permettant de **collecter, analyser et partager des informations sur les menaces** afin d'anticiper et de répondre aux cyberattaques.

Objectifs :

- Identifier les nouvelles menaces et les TTP (Tactiques, Techniques et Procédures) des attaquants.
- Enrichir les indicateurs de compromission (IoC) et les indicateurs d'attaque (IoA).
- Partager les renseignements sur les cybermenaces avec les équipes SOC et CSIRT.
- Renforcer la détection et la prévention des incidents en anticipant les nouvelles campagnes d'attaques.

Implication du Threat Intelligence dans la Réponse à Incident

Rôle du TI dans la gestion des incidents :

- Collecte et analyse des IoC et IoA pour aider les analystes SOC et CSIRT à identifier les menaces.
- Cartographie des attaques avec MITRE ATT&CK pour comprendre les techniques utilisées.
- Corrélation des menaces avec des bases de données comme MISP, VirusTotal, AlienVault OTX.
- Partage des renseignements avec les équipes internes et partenaires pour renforcer la défense collective.

Impact : Permet une réponse plus rapide et efficace en fournissant **un contexte sur les attaques et en aidant à attribuer une menace à un acteur malveillant**.

Intégration du Threat Intelligence dans le SOC

Rôle du TI au sein du SOC :

- Fournit des indicateurs de compromission (IPs, Hashes, Domaines) pour enrichir le SIEM.
- Aide à créer des règles de détection avancées (Sigma, YARA, Suricata).
- Informe les équipes SOC Tier 1, 2 et 3 sur les campagnes d'attaques en cours.
- Permet aux analystes SOC de détecter des attaques avant leur exécution en surveillant les nouvelles techniques adverses.

Collaboration : Le Threat Intelligence travaille en synergie avec **le SOC, le CSIRT et le DFIR** pour améliorer la détection et la réponse aux incidents.

Threat Hunting

Définition : Le Threat Hunting est une approche proactive de la cybersécurité qui consiste à **rechercher des menaces inconnues ou non détectées par les outils automatisés** comme le SIEM et l'EDR.

Objectifs :

- Identifier les attaques avancées et persistantes (APT).
- Détecter les comportements anormaux en l'absence d'alertes SIEM.
- Compléter les investigations SOC et CSIRT avec une analyse proactive.
- Réduire le dwell time (temps de présence des attaquants).

Implication du Threat Hunting dans la Réponse à Incident

Rôle du Threat Hunting :

- Recherche proactive d'indicateurs d'attaque (IoA) et de tactiques adverses.
- Corrélation des données avec MITRE ATT&CK pour cartographier les menaces.
- Utilisation des logs réseau, endpoint et SIEM pour détecter des signaux faibles.
- Escalade des découvertes vers le CSIRT et DFIR pour investigation approfondie.

Impact : Le Threat Hunting améliore la détection et permet d'anticiper les attaques **avant qu'elles ne génèrent des alertes automatiques**.

Intégration du Threat Hunting dans le SOC

Rôle du Threat Hunting au sein du SOC :

- SOC Tier 3 utilise le Threat Hunting pour enrichir la détection.
- Exploitation des données SIEM et EDR pour rechercher des comportements suspects.
- Amélioration des règles de détection (YARA, Sigma) pour le SOC Tier 1 et 2.
- Collaboration avec les équipes de Threat Intelligence pour affiner les indicateurs de menace.

Résultat : Réduction du nombre d'incidents non détectés et amélioration de la réponse aux menaces avancées.

Apport de la Pyramid of Pain en Threat Hunting

Concept de la Pyramid of Pain :

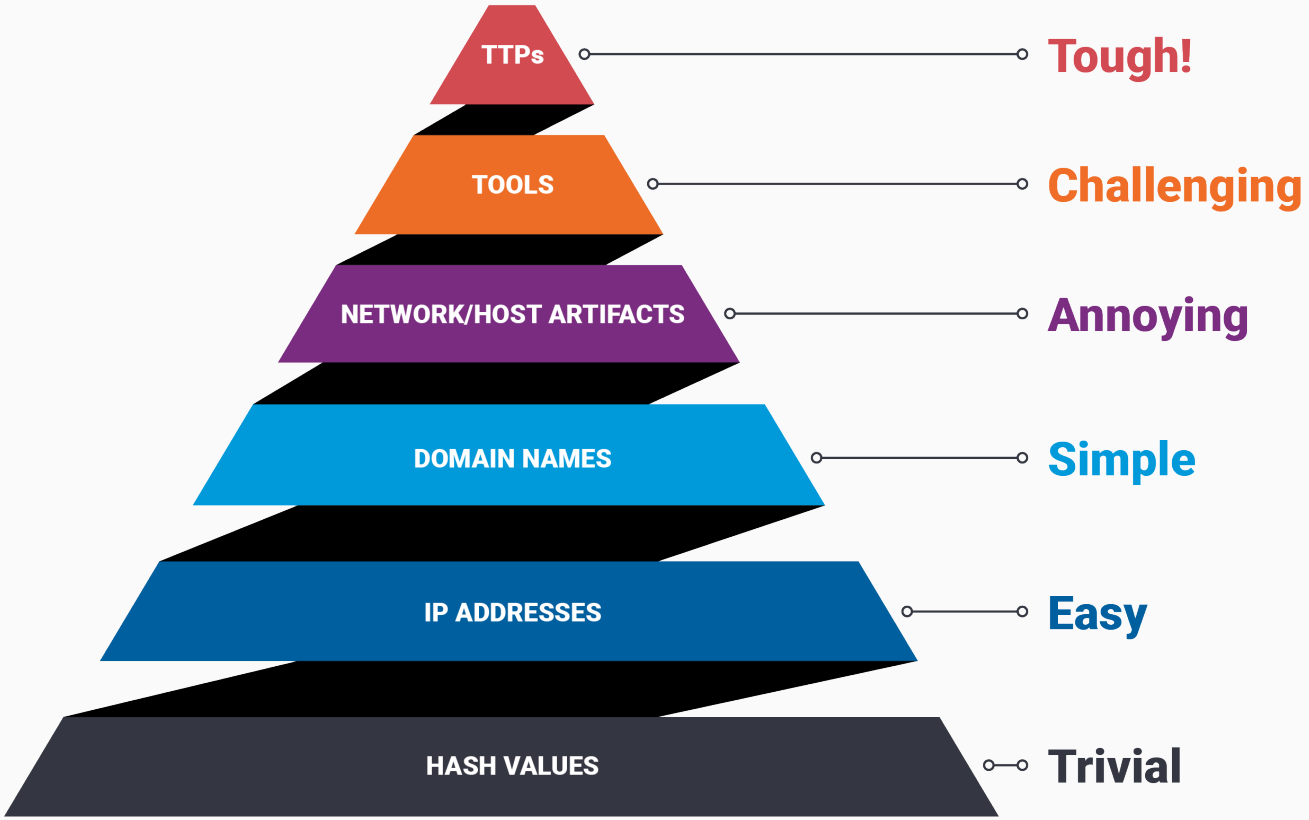
- La Pyramid of Pain classe les indicateurs de menace en fonction de la difficulté pour l'adversaire de les modifier.
- Plus un indicateur est haut dans la pyramide, plus il est difficile pour l'attaquant de s'adapter.

Application en Threat Hunting :

- Éviter de se baser uniquement sur des IoC (hash, IP) facilement changeables.
- Focaliser la détection sur les artefacts réseau et les TTP adverses (MITRE ATT&CK).
- Créer des règles de détection sur des comportements et techniques difficiles à modifier.

Bénéfice : Un Threat Hunting efficace se concentre sur **les comportements et TTP des attaquants plutôt que sur des indicateurs statiques**.

Apport de la Pyramid of Pain en Threat Hunting



Exemple d'Application : Hunting basé sur la TI et la Pyramid of Pain

Cas : Campagne d'un APT utilisant Cobalt Strike

- La Threat Intelligence fournit des informations sur une attaque en cours.
- Le Threat Hunting utilise la Pyramid of Pain pour déterminer quels indicateurs sont les plus efficaces.
- Objectif : Trouver et bloquer l'attaque en fonction de ses **TTP adverses**.

Indicateurs de menace et leur efficacité selon la Pyramid of Pain

1. **Hash** $\rightarrow$ La TI fournit un hash de la charge utile.
   - Peu utile, les attaquants changent facilement les hashes.

2. **IP** $\rightarrow$ On récupère les IP des serveurs C2 de l'APT.
   - Contournable, les attaquants utilisent des serveurs temporaires.

3. **Domaine** $\rightarrow$ La TI signale un domaine utilisé par le C2 (maliciousC2.com).
   - Plus utile, mais contournable via des services dynamiques.

Artefacts et Techniques de Chasse Avancée

4. Network Artifacts → La TI indique que le C2 utilise des **paquets HTTPS avec une entropie élevée** (obfuscation).

- Hunting possible sur les logs réseau pour détecter ces patterns.

5. Host Artifacts → L'attaque laisse des traces **dans le registre Windows** (clé de persistance).

- Hunting efficace via SIEM et EDR.

6. TTPs → L'APT utilise **T1059.001 - PowerShell Execution** pour injecter son malware.

- **Chasse comportementale très efficace** → force l'attaquant à modifier sa méthode d'attaque.

Digital Forensics and Incident Response (DFIR)

Définition : Le DFIR (Digital Forensics and Incident Response) est un domaine spécialisé de la cybersécurité qui regroupe les techniques d'**investigation numérique et de réponse aux incidents** afin de comprendre, contenir et éradiquer une attaque.

Objectifs :

- Analyser les preuves numériques pour comprendre l'attaque et ses impacts.
- Effectuer une réponse aux incidents pour limiter les dégâts et restaurer les systèmes.
- Identifier les tactiques adverses et créer des contre-mesures adaptées.
- Produire un rapport forensic pour documenter l'attaque et améliorer la sécurité future.

Implication du DFIR dans la Réponse à Incident

Rôle du DFIR dans la gestion des incidents :

- Collecte et préservation des preuves numériques (disque, mémoire, logs réseau).
- Analyse forensic des systèmes compromis (extraction des IoC et IoA).
- Identification des artefacts laissés par l'attaquant (clés de registre, fichiers suspects, processus anormaux).
- Utilisation des frameworks MITRE ATT&CK et Diamond Model pour reconstituer l'attaque.
- Collaboration avec les équipes SOC et CSIRT pour contenir et éradiquer l'incident.

Impact : Le DFIR permet une analyse approfondie des incidents et joue un rôle clé dans l'éradication des menaces avancées.

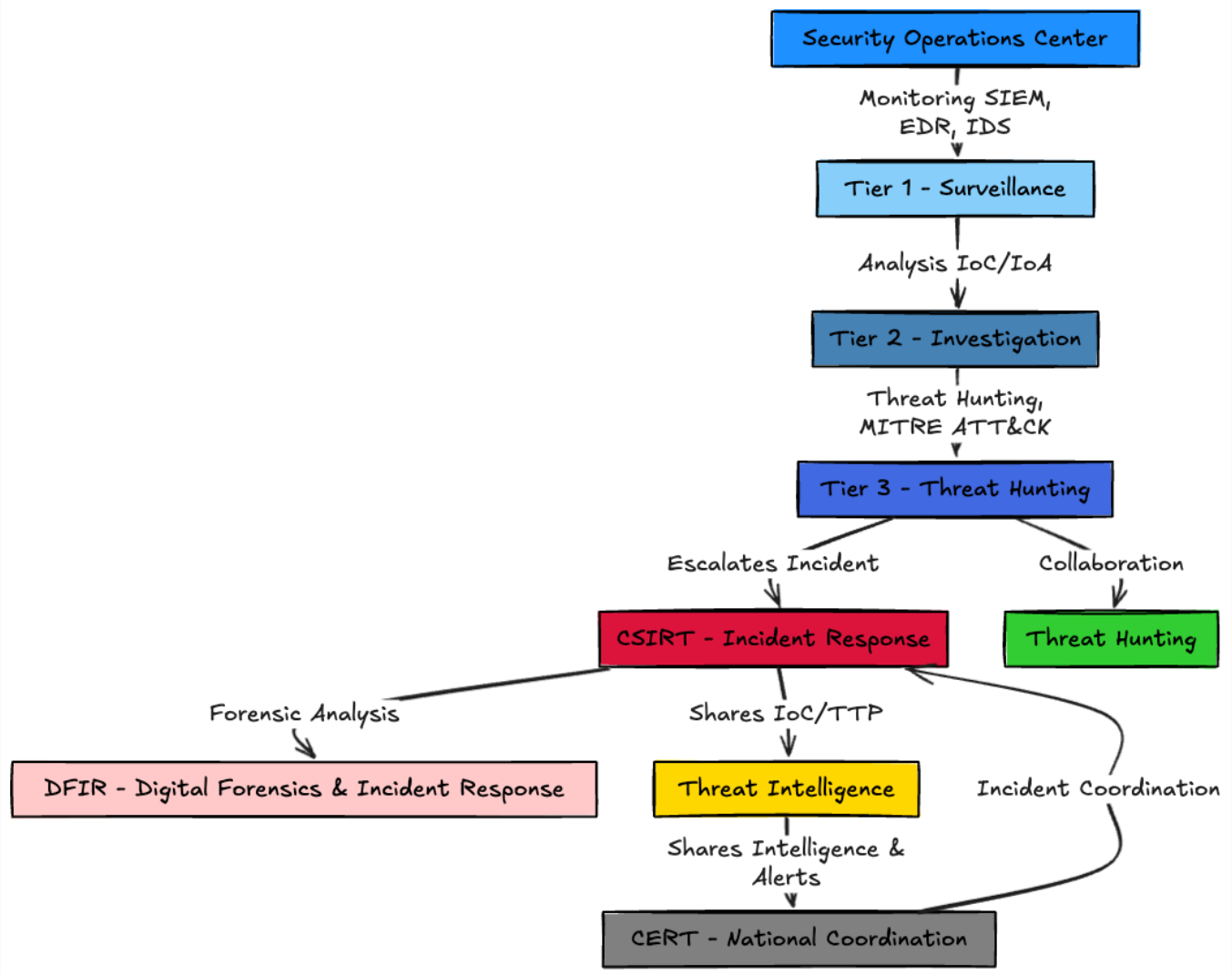
Intégration du DFIR dans le SOC

Rôle du DFIR au sein du SOC :

- Assiste le SOC Tier 2 et Tier 3 en cas d'incident critique nécessitant une analyse approfondie.
- Fournit des preuves numériques pour valider ou invalider une attaque suspectée.
- Identifie des traces avancées qui ne sont pas détectées par les outils SIEM et EDR.
- Met en place des recommandations post-incident pour éviter une nouvelle compromission.

Collaboration : Le DFIR travaille en synergie avec **le SOC, le CSIRT et le Threat Intelligence** pour améliorer la réponse aux incidents et la résilience de l'organisation.

Synthèse


Security Operations Center
Monitoring SIEM, EDR, IDS
Tier 1 - Surveillance
Analysis IoC/IoA
Tier 2 - Investigation
Threat Hunting, MITRE ATT&CK
Tier 3 - Threat Hunting
Escalates Incident
Collaboration
CSIRT - Incident Response
Threat Hunting
Forensic Analysis
Shares IoC/TTP
DFIR - Digital Forensics & Incident Response
Threat Intelligence
Incident Coordination
Shares Intelligence & Alerts
CERT - National Coordination

Étude de Cas : Exécution de Code via PowerShell

Contexte : Une alerte EDR détecte une exécution PowerShell suspecte.

- **IoA détecté :**
  - Utilisation de `-EncodedCommand` pour exécuter un script caché.
  - Connexion suspecte vers `127.26.152.13`.
  - Injection dans `rundll32.exe`.

Mapping MITRE ATT&CK

- **T1059.001** - PowerShell Execution
- **T1105** - Remote File Copy
- **T1027** - Obfuscated Files or Information
- **T1547.001** - Registry Run Keys / Startup Folder

Détection avec YARA

Règle YARA pour détecter l'attaque :

```
rule Suspicious_PowerShell_EncodedCommand {
    meta:
        description = "Détection d'exécution PowerShell encodée en Base64"
        author = "SecurityLab SOC"
        reference = "MITRE ATT&CK T1059.001"
    strings:
        $encoded_ps = /powershell.*-EncodedCommand\s+[A-Za-z0-9+/=]{20,}/ nocase
    condition:
        $encoded_ps
}
```

Détection avec Sigma

Règle Sigma pour détection SIEM :

```yaml
title: Suspicious PowerShell Encoded Command Execution
id: e8b7dc6f-9b1c-4e5d-91b5-d3dba9b12345
status: experimental
description: Detects encoded PowerShell commands used for potential obfuscation
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    Image|endswith: '\powershell.exe'
    CommandLine|contains: '-EncodedCommand'
  condition: selection
level: high
```

Le Paysage des Menaces et des Attaques en cybersécurité

Introduction au Paysage des Menaces

- Le paysage des menaces couvre l'ensemble des risques informatiques.
- Il inclut les malwares, les attaques DoS, l'exploitation des vulnérabilités (Zero-day, Buffer-over-flow, SQL Injection, XSS, ...), etc.

Motivations des attaquants

- **Gains financiers** : Cybercriminalité organisée visant un bénéfice monétaire.
- **Espionnage** : Vol de données stratégiques pour un État ou une entreprise.
- **Déstabilisation** : Manipulation de l'opinion, attaques sur l'image d'une entité.
- **Pré-positionnement stratégique** : Infiltration longue durée pour sabotage ou espionnage.

Définition d'un malware

Malware (logiciel malveillant) : Tout code, charge utile ou fichier conçu pour infiltrer et endommager un endpoint.

- Les dommages incluent :
  - Accès complet à l'appareil
  - Vol d'informations sensibles
  - Chiffrement de fichiers (ransomware)
  - Détérioration de l'expérience utilisateur
  - Affichage de publicités indésirables
  - Attaque d'autres endpoints (botnet)

Types de Malwares (1/2)

- **Virus** : Se réplique lui-même dans le système.
- **Worm (ver)** : Se propage à travers un réseau pour infecter les endpoints.
- **Rootkit** : Masque d'autres fichiers malveillants dans les niveaux inférieurs du système d'exploitation.
- **Downloader (téléchargeur)** : Télécharge et exécute d'autres fichiers malveillants depuis Internet.
- **Ransomware (rançongiciel)** : Chiffre l'endpoint et exige une rançon financière. Exemple : Locky.
- **Botnet** : Intègre l'appareil dans un réseau d'ordinateurs infectés.

Types de Malwares (2/2)

- **Backdoor (porte dérobée)** : Fournit un accès continu à l'appareil.
- **PUP (Programme potentiellement indésirable)** : Affiche du contenu indésirable.
- **Dropper** : Dépose un composant de lui-même sur le disque dur.
- **Scareware** : Affiche de fausses alertes pour inciter l'utilisateur à des actions potentiellement malveillantes.
- **Trojan (cheval de Troie)** : Se présente comme une application légitime mais contient des fonctionnalités malveillantes. Exemple : TrickBot.
- **Spyware (logiciel espion)** : Vole des informations à des fins financières.

Étude de Cas : WannaCry (2017)

- **Attaque mondiale de ransomware** exploitant la vulnérabilité SMB (EternalBlue).
- Plus de **300 000 ordinateurs infectés** dans 150 pays.
- Impact sur des hôpitaux, entreprises et infrastructures critiques.

Analyse forensique :

- Recherche des artefacts dans les journaux d'événements Windows.
- Extraction des adresses IP de Command & Control (C2).
- Détection du **kill switch** stoppant la propagation.

Étude de Cas : WannaCry (2017)

Kill Switch Découverte

Le kill switch était une découverte accidentelle par le chercheur en cybersécurité Marcus Hutchins (MalwareTech). Il a remarqué que le ransomware tentait de contacter un nom de domaine non enregistré (ex: iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com). Lorsqu'il a acheté ce domaine pour l'analyser, le ransomware a cessé de se propager.

Points Importants

- Les classifications peuvent se chevaucher.
- Exemple : WannaCry est à la fois un ransomware, un cheval de Troie et un worm.
- La détection de ces malwares peut être réalisée par des outils comme YARA.

Techniques utilisées par les malwares

Comprendre les différentes techniques utilisées par les malwares est crucial pour une défense efficace. Cette présentation se concentre sur l'offuscation, le métamorphisme et le polymorphisme.

Qu'est-ce qu'un fichier packé ?

- Un fichier packé est un exécutable compressé ou chiffré pour masquer son contenu.
- Utilisé pour réduire la taille du fichier et échapper à la détection des antivirus.
- Le fichier est décompressé dynamiquement en mémoire lors de l'exécution.

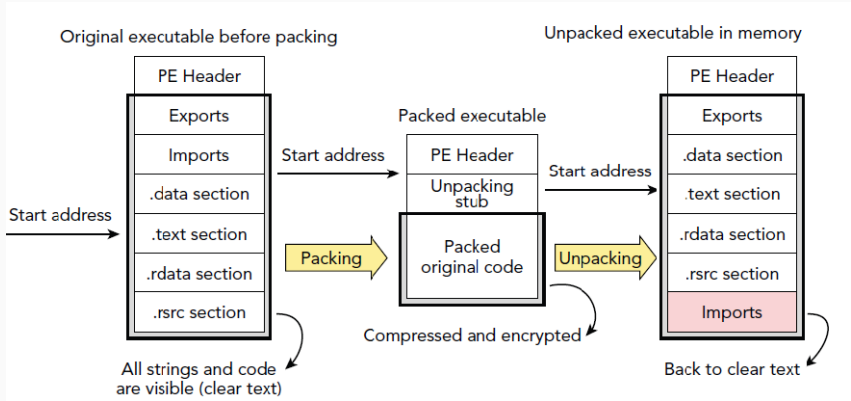
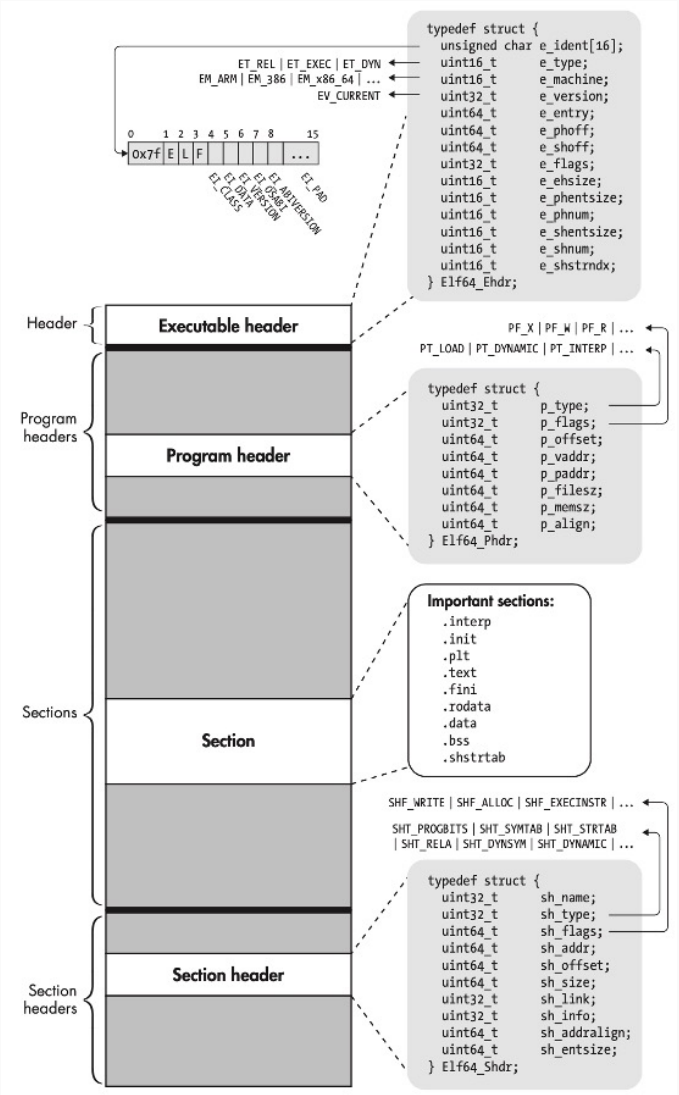


Figure 8-5: The life cycle of a program being packed and loaded into memory

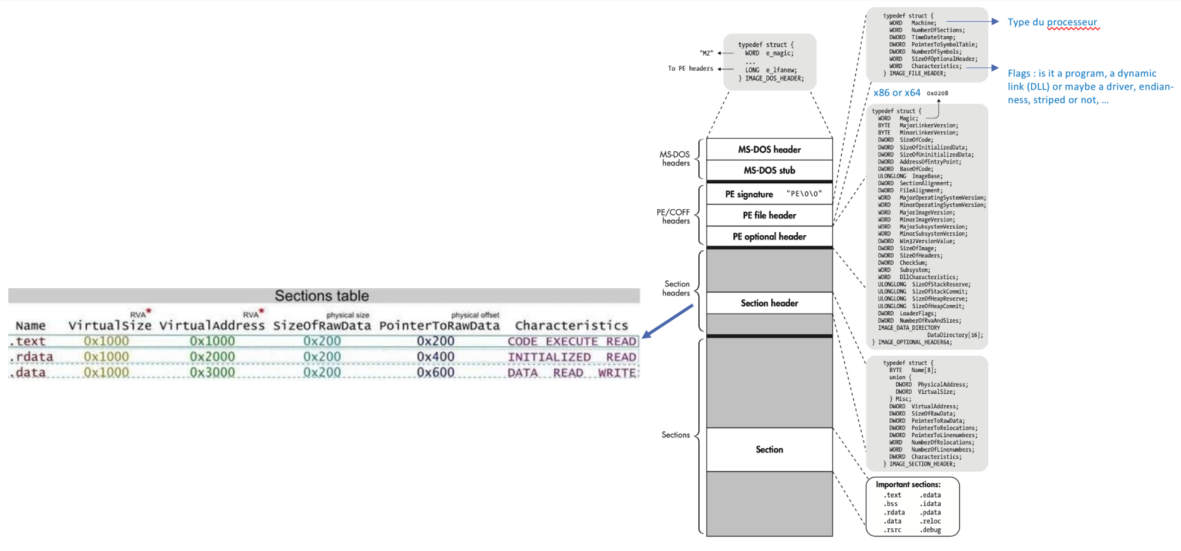
Lien avec le format Portable Executable (PE)

- Un fichier packé reste un fichier PE valide.
- Les sections importantes du PE sont souvent modifiées :
  - **.text** (code) est souvent très petite.
  - **.rsrc** (ressources) et **.data** peuvent être anormalement grandes.
- L'Entry Point du programme pointe généralement vers une section inhabituelle.



Détection des fichiers packés

- Vérification des tailles des sections avec un outil comme **PE-Bear**, **PEview** ou **CFF Explorer**.
- Indices d'un fichier packé :
  - Section **.text** inhabituellement petite (taille en memoire virtuelle vs taille sur disk).
  - Une seule grande section anormale (ex: **.data**, **.UPX**).
  - Point d'entrée (**EP**) situé dans une section non standard.



Les Virus Chiffrés

- **Principe** : Le code du virus est chiffré pour masquer son fonctionnement.
- **Méthode** : Un décodeur constant est placé en début de code pour déchiffrer le corps du virus.
- **Exemples** :
  - **Cascade** (virus DOS)
  - **Win95/Mad** et **Win95/Zombie** (versions 32 bits)
- **Détection** : Possible en identifiant le motif du décodeur, bien que cette méthode ne soit pas parfaite.
- **Contre-mesure** : Le code de réparation peut déchiffrer le virus et traiter ses variantes.

Virus Oligomorphes : La Génération Initiale de l'Obfuscation

- **Réaction aux techniques de signature**: Apparition en réponse aux méthodes de détection par signature.
- **Début de l'obfuscation de la routine de décryptage**: Le code du virus est chiffré, nécessitant une routine de déchiffrement. Cette routine est ensuite légèrement modifiée pour éviter la détection.
- **Limitation majeure**: Nombre limité de routines de déchiffrement possibles. Une fois toutes les variations utilisées, le virus devient détectable.
- **Exemple**: Le virus Whale DOS (1990).
- **Fonctionnement**: Utilisation d'une routine de déchiffrement obfusquée et chiffrée pour déchiffrer le corps du virus.

Virus Polymorphes : Mutation du Code et du Décrypteur

- **Extension de l'oligomorphisme**: Introduction de l'obfuscation dans la routine de déchiffrement elle-même, menant à un nombre potentiellement infini de routines.
- **Génération dynamique du décrypteur**: Le virus non chiffré crée un nouveau décrypteur muté en utilisant un algorithme de chiffrement aléatoire.
- **Le décrypteur chiffre le corps du virus**: Après la création du décrypteur, celui-ci chiffre le corps principal du virus avant de relier les deux parties.
- **Contournement des limitations de l'oligomorphisme**:
  - Taille constante du code viral.
  - Ajout au début ou à la fin du fichier infecté.
  - Segments de code similaires entre les générations.
- **Exemples de générateurs**: Phalcon/Skism mass-produced code generator (PS-MPC) et virus creation lab (VCL).

Virus Métamorphiques : La Mutation Complète du Code

- **Absence de corps constant**: Aucune similarité de signature entre les générations.
- **Obfuscation complète du code**: L'ensemble du code du virus est obfusqué.
- **Moteur de métamorphisme**: Utilisation d'un moteur sophistiqué pour l'obfuscation et la reconstruction du code.
- **Plus besoin de chiffrement**: La séparation entre le décrypteur et le corps du virus n'est plus possible, et le niveau d'obfuscation rend le chiffrement inutile.
- **Exemples**: W95/Regswap (1998) et W32/Ghost (2000).
- **Moteur de mutation sophistiqué**: Contient de nombreux sous-processus.
- **Outils**: W32/ NGVCK.

Code Polymorphe

- Modifie son code de chiffrement ou son emballage (cryptage, obfuscation) à chaque infection ou exécution, tout en conservant le même code de base.
- Utilise souvent des techniques comme la substitution de clés ou la modification des signatures pour échapper aux antivirus.

Code Métamorphe

- **Mutation du Code** : Modifie son contenu à chaque exécution.
- **Techniques de Mutation** :
  - Ajout de conditions et variables inutiles.
  - Modification des instructions machine.
  - Insertion d'instructions NOP (No Operation).

Offuscation

- **Complexification du Code** : Rend le code source illisible et difficile à comprendre.
- **Techniques d'Offuscation** :
  - Renommage (variables, fonctions).
  - Offuscation du flux de contrôle.
  - Concaténation de chaînes.
  - Encodage de chaînes.
  - Remplacement de chaînes.
- **Objectif** : Ralentir l'analyse et la rétro-ingénierie du malware.

Les Vecteurs d'Attaque

- **Phishing** : Tromperie pour voler des informations.
- **Exploitation des Vulnérabilités** : Failles logicielles exploitées.
- **Attaques DoS/DDoS** : Saturation des ressources d'un système.
- **Injections SQL** : Manipulation de bases de données.
- **Attaques Wi-Fi** : Piratage de réseaux sans fil.
- **USB Malveillants** : Clés USB infectées.
- **Attaques API** : Exploitation de vulnérabilités des API.

Attaques de la Chaîne d'Approvisionnement (Part 1)

- **Définition** : Attaques visant un fournisseur ou un partenaire pour compromettre un produit ou service en amont.
- **Méthodes** :
  - **Manipulation des mises à jour logicielles** : Introduction de malwares dans des mises à jour légitimes.
  - **Compromission des fournisseurs tiers** : Cyberattaques ciblant des prestataires ayant accès aux systèmes des victimes.

Attaques de la Chaîne d'Approvisionnement (Part 2)

- **Méthodes** (suite) :
  - **Injection de malwares dans le code source** : Modification du code avant son intégration dans des produits utilisés en production.
  - **Attaques sur la chaîne logistique matérielle** : Introduction de composants physiques compromis dans des équipements informatiques.
- **Conséquences** :
  - Diffusion massive de malwares via des produits de confiance.
  - Accès non autorisé à des systèmes critiques.
  - Vol et exfiltration de données sensibles.
  - Déstabilisation de la sécurité de grandes infrastructures.

Attaques de la Chaîne d'Approvisionnement (Part 3) - L'attaque SolarWinds

Une attaque sur la chaîne d'approvisionnement logicielle

- Exploitation d'une faille dans **Orion** de SolarWinds.
- Affecte des milliers d'organisations, y compris **des agences gouvernementales américaines et des entreprises du Fortune 500**.
- Introduction de la **porte dérobée (backdoor) Sunburst** dans une mise à jour logicielle légitime.
- **Accès discret** aux réseaux infectés.

Conséquences :

- Intrusion restée **inaperçue pendant plusieurs mois**.
- Exfiltration de **données sensibles**.
- Mise en lumière de la vulnérabilité des **chaînes d'approvisionnement logicielles**.
- Stratégie prisée par les **cybercriminels et les États-nations**.

Attaques sur les Infrastructures Critiques

- **Exemple** : Stuxnet ciblant des systèmes industriels.
- Objectif : Perturber des secteurs clés (énergie, eau, communications).
- Méthodes : Exploitation de SCADA, protocoles non sécurisés.

Attaques Persistantes Avancées (APT)

- **Définition** : Attaques sophistiquées menées par des groupes organisés (États, cybercriminels).
- **Objectif** : Obtenir un accès prolongé et furtif aux systèmes cibles.
- **Méthodes** :
  - Utilisation de malwares sur mesure pour éviter la détection.
  - Phishing ciblé (spear phishing) pour obtenir des accès initiaux.
  - Exploitation des failles zero-day.
  - Mouvements latéraux pour se propager sur le réseau interne.
  - Exfiltration discrète de données sensibles.

Attaques Persistantes Avancées (APT)

Exemples :

- *APT28* (Fancy Bear) : Groupe lié à des cyberattaques étatiques.
- *APT29* (Cozy Bear) : Associé à des campagnes d'espionnage.

Anayse d'un malware

Qu'est-ce que l'analyse de malware ?

- Examen d'un programme malveillant pour comprendre son fonctionnement.
- Identification des indicateurs de compromission (IOC), IoA et mapping avec MITRE&ATTCK.
- Objectif : amélioration de la détection et mise en place de contre-mesures.

Collecte et Acquisition des échantillons

- Objectif : Obtenir un fichier suspect sans l'altérer (lors d'un incident remonté par le SOC).
- Méthodes : Sources d'incidents, bases de partages de malwares.
- Outils : VirusTotal, Any.Run, Hybrid Analysis.

Analyse Statique

- Objectif : Extraire des informations sans exécuter le fichier.
- Techniques : Métadonnées, chaînes de caractères, signatures.
- Outils : Strings, Radare2, PE Studio, ExifTool, IDA Pro.

Analyse Dynamique

- Objectif : Observer le comportement du malware en exécution.
- Techniques : Suivi des modifications système et réseau.
- Outils : Sandbox (Any.run), Process Monitor, Wireshark.

Analyse du Code

- Objectif : Désassembler ou décompiler le malware.
- Techniques : Étude du code et rétro-ingénierie.
- Outils : Ghidra, IDA Pro, Radare2.

Rétroconception et Remédiation

- Objectif : Développer des signatures et des contre-mesures.
- Techniques : Règles YARA, détection réseau.
- Outils : YARA, Snort, Suricata.