Threat Intelligence et IOCs

Antoine Bénar | ECE

Objectifs du cours

- Concepts clés de la Threat Intelligence : collecte et analyse
- Présentation des différents types d'IOC
- Utilisation de la Cyber Kill Chain
- Introduction aux CVE et patch management
- Enrichir un cas d'attaque avec des IOC réels

IoC & Threat Intelligence : c'est quoi ?

IoC : **Indicator of Compromission**

Artefacts observables indiquant une activité malveillante potentielle ou confirmée

Exemples: **adresse IP** publique, **hash**, **URL**, adresses mails, strings…

CTI : **Cyber Threat Intelligence**

Ensemble des données collectées analysées et structurées sur les menaces informatiques

Exemples : IoC, campagnes de phishings en cours, APT

IOC – en résumé

Il existe 3 catégories principales d'IOC :

IOC statiques

Pratiques
Facilement intégrables & utilisables

Facilement contournables
A courte durée dans le temps
Génère des faux positifs

Exemples : hashs, noms de domaines, URL..

IOC dynamiques

Durables
Bon ratio VP / FP
Détection d'APT / 0-days

Difficiles à collecter
Nécessites beaucoup de télémétrie
Analyse complexe

Exemples : chaîne de processus spécifique, commande Powershell particulière, créations de clés de registre dans des emplacements spécifiques…

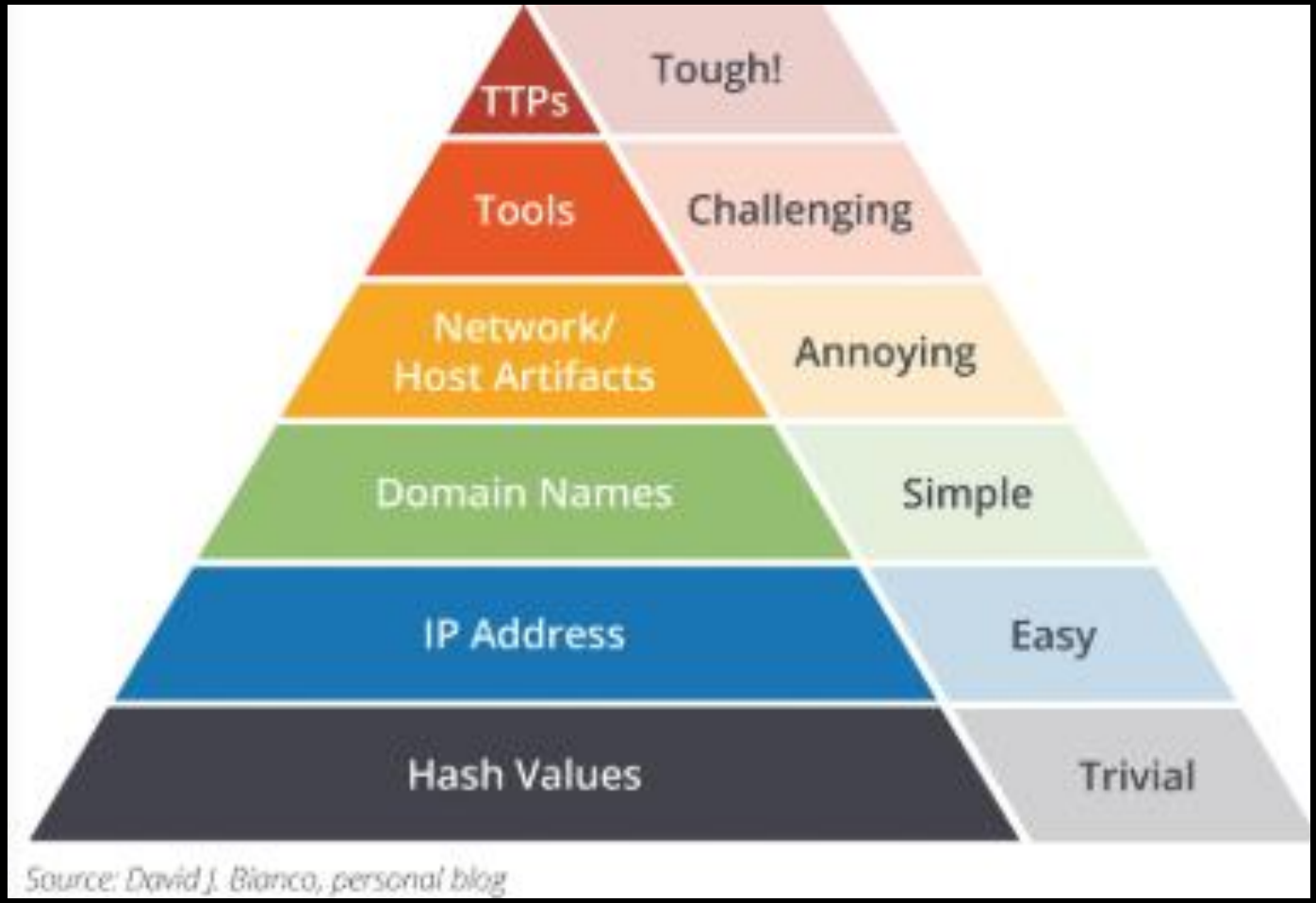
IOC contextuels

Implémentation pratique SOC
Moins manipulable par l'attaquant
Bonne reconstitution d'attaque

Longue mise en place
Doit être combinée avec d'autres IOCs

Exemples : Horaires d'attaque, utilisateur compromis, patterns de mouvement latéraux…

La « pyramide de la douleur »



Ou « comment nuire à un attaquant »

Modèle proposé par D. Bianco

« Les types d'IoC les plus difficiles à changer pour un attaquant »

IOC – Les hashs

Hash : résultat d'un algorithme qui **transforme une donnée en une empreinte unique** de taille fixe. Propriétés :

≃ **Unicité** (résultat unique pour chaque entrée)

- **Non-réversibilité** (impossible de retrouver l'orignial)
- **Effet « avalanche »** (Une légère modification changement complètement l'apparence du hash)

En tant qu'IOC, les algorithmes fréquemment utilisés sont le md5, sha1 et **sha256**. L'objectif est d'avoir un calcul rapide et une utilisation répandue pour pouvoir comparer les hashs !

Usages : détecter un fichier malveillant, qu'un fichier n'ai pas été modifié (intégrité), comparer un fichier à une base de connaissance.

Limites : collisions, durée dans le temps, facilité de modification

Où comparer les hashs ? VirusTotal , any.run, JoeSandbox, Hybrid Analysis

IOC – Les IPs

IP : identifiant unique attribué à chaque appareil connecté à un réseau internet (lié à « l'adapteur »). Une IP privée permet de se reconnaître sur un réseau interne, une IP publique permet de se reconnaître sur internet.

Une IP privée peut être un IOC contextuel temporaire, alors qu'une IP publique est généralement un IOC statique.

En tant qu'IOC, une IP malveillante est souvent associée à :

- Un serveur C2 (command & control)
- Une infra d'attaque (ddos, phishing, botnet, hébergement malware)
- Une infra de scan de réseau ou de brute force

Les IP sont facilement collectables (par les CERT, bases CTI, feeds open sources), facilement détectables via les agents EDR, XDR, les firewall, proxy, WAF, NDR…) et peuvent être rapidement bloqués dans les équipements réseaux

Néanmoins, les IP changent rapidement (DHCP ou hébergeurs, VPN, proxies, cloud)

CTI IPs : AbuseIPDB, Shodan, VirusTotal

IOC – Les NDD

Nom De Domaine : Alias utilisé pour accéder à une ressource sur Internet (ex : exemple.com) — il est associé à une ou plusieurs adresses IP via le DNS.

IOC statique ou contextuel, souvent de courte durée car down par l'hébergeur après plaintes déposées par des SOC, CERT etc. Dépends de la durée de vie, propriétaire et usage.

Les NDD sont lisible, facilement partageable et détectable par DNS, EDR, proxy, FW, WAF, XDR...

Ils sont également facilement blocables niveau DNS ou Firewall, mais assez volatils.

CTI NDD : VirusTotal, AbuseIPDB (conversion IP auto), Shodan

IOC – Certificats & Signatures

- Une **Signature** numérique est un mécanisme cryptographique pour :
  - Vérifier **l'intégrité** d'une donnée (fichier…)
  - Garantir son **authenticité** (signé par entité connue)
  - Assurer la **non-répudiation** (impossible de nier)

Signature (HASH (fichier) + clé privée du signataire) = Signature

Vérification : clé publique → HASH conforme ?

- Un **Certificat** est un document numérique **émis par une autorité de certification** (CA) qui **atteste de l'identifié** d'une entité.
  - Il contient clé publique de l'entité, identité, signature, et date de validité.
  - Permet de signer des exécutables ou des certificats de sites WEB (TLS/SSL)

IOC : pour résumer

Il n'y a pas de « meilleur » type d'IOC

L'idéal est une combinaison de plusieurs IOC de chaque catégorie

Il est important de fréquemment actualiser les bases d'IOC statiques

Lorsque c'est possible, il peut être intéressant d'intégrer des bases d'IOC dans les équipements de sécurité du SI (FW, DNS, Proxy…)

Ou trouver des bonnes CTI

feedly.com/threat-intelligence 

Opencti 

MISP Feeds 

CERT-FR + 

VT, Abuse IP DB, checkurl, moteurs de recherche…

Les APTs

APT = Advanced Persistent Threat

Une APT est un groupe d'attaquants sophistiqués , souvent étatique, qui mène des attaques d'envergures

Utilisation de 0-day, malwares sur mesure, maintiennent une persistance pendant des mois.

Motivations souvent politiques, économiques ou militaires (ciblent gouvernements, infrastructures critiques etc)

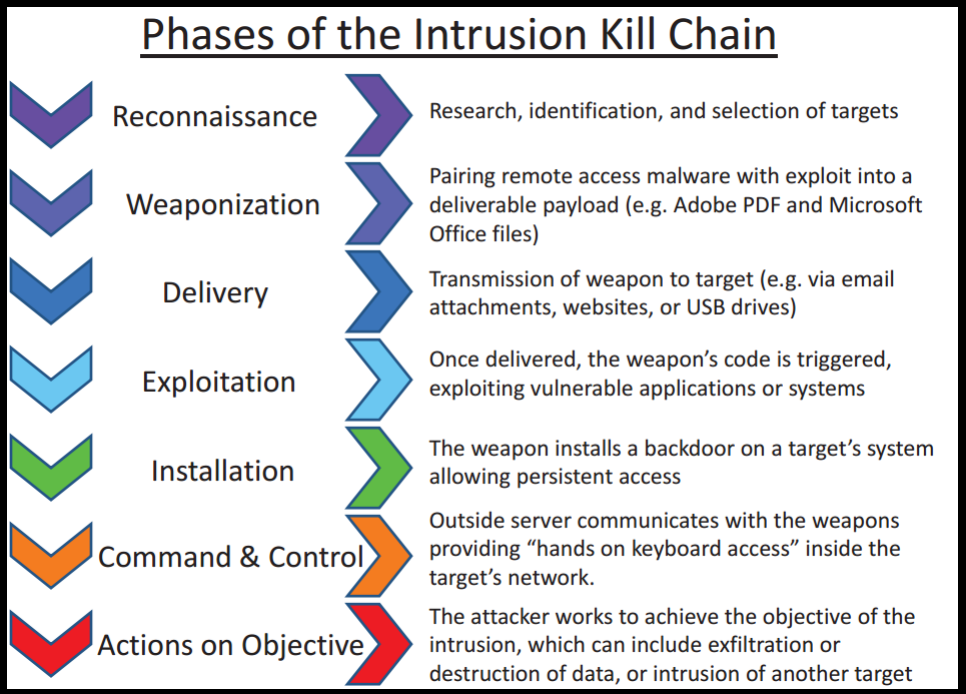
Les APTs, exemples

2006	**Premier usage public du terme “APT”**	**Par l’US Air Force**
2010	Stuxnet	Premier APT connu, attaque contre l’Iran (centrifugeuses nucléaires)
2011-2015	APT1, APT28, APT29 révélés	Groupes liés à la Chine et à la Russie identifiés par Mandiant
2016	Piratage du DNC (Clinton)	Campagne APT (Fancy Bear) durant les élections US : attaque Russe
2020+	SolarWinds, Hafnium, Volt Typhoon	Niveau mondial : attaques massives et furtives sur chaînes logistiques ou cloud

La Cyber Kill Chain

Développé par Lockheed Martin en 2011

Le modèle Cyber Kill Chain décrit les différentes phases d'une cyberattaque, de la reconnaissance à l'exfiltration.



Source : wikipedia.org

Moyens de défense associés :

- Détecter (la découverte)
- Refuser (accès, RBAC…)
- Interrompre (le trafic réseau)
- Dégrader (contre attaque)
- Tromper (casser C2)
- Contenir (hardening réseau)

Intégré dans certains frameworks comme la matrice MITR

Introduction aux CVE et Patch management

Une CVE (Common Vulnerabilities and Exposures) est une base de données publique qui répertorie les **failles de sécurité connues**, avec un identifiant unique (ex : CVE-2024-12345). (Année - Identifiant)

Le Score CVSS - Gravité (0–10), évalue l'urgence du correctif
Les CVE sont gérées par le MITRE et les CVSS par le NIST, et sont utilisées par tous les éditeurs.

Exemple : PrintNightmare (CVE-2021-34527) – 8.8/10 – RCE (faille dans le service d'impression Windows permettant d'exécuter du code arbitraire à distance, et escalade de privilèges SYSTEM. Patch déployé en urgence par Microsoft, mettre à jour pour corriger la vulnérabilité.

Le patch management, c'est donc un processus d'identification, de test et de déploiement de mises à jour (patchs) pour :

- Corriger les CVE
- Stabiliser les systèmes
- Maintenir des niveaux pour audits de conformité (27001…)

Questions