



---

# SOC LEVEL 1 ESSENTIALS

## – PART D: THREAT INTELLIGENCE & INVESTIGATION (POSTS 29–37)

---

From Indicators to Investigation: Mastering Threat Intelligence in SOC Operations



AUGUST 8, 2025

INAAM KABBARA

SECURITY ANALYST | CYBERSECURITY CONTENT CREATOR | EPITA MSC GRADUATE

## Table of Contents

1- What Is Threat Intelligence? Use Cases for SOC Analysts.....	2
2- IoC vs IoA – Indicators Explained with Examples.....	4
3- VirusTotal, AbuseIPDB, Shodan – Analyst's Toolbox .....	6
4- What Is a CVE and How to Read It? .....	8
5- MITRE ATT&CK – Tactics and Techniques for SOC.....	10
6- Threat Hunting – Concepts and Starter Tactics.....	12
7- The Cyber Kill Chain – Phases of an Attack .....	14
8- Using MISP to Share Threat Intelligence.....	16
9- How to Investigate a Suspicious IP or Domain.....	18

# 1- What Is Threat Intelligence? Use Cases for SOC Analysts

## Understanding Threat Intelligence in a SOC Environment

In today's evolving cyber threat landscape, Threat Intelligence (TI) is a game-changer for SOC teams. It refers to evidence-based knowledge about existing or emerging threats, including indicators of compromise (IOCs), tactics, techniques, and procedures (TTPs), and threat actor profiles.

### Key Use Cases for SOC Analysts:

- 1- Enriching Alerts: TI helps analysts contextualize and validate alerts by matching IPs, domains, or hashes with known malicious indicators.
- 2- Threat Hunting: Proactively searching for hidden threats using intelligence from recent campaigns or actor behaviors.
- 3- Incident Response Acceleration: TI provides actionable data to assess impact more quickly and make informed decisions.
- 4- Detection Rule Enhancement: Creating more precise SIEM detection logic based on known TTPs from threat feeds.
- 5- Strategic Defense Planning: TI trends guide long-term security posture improvements and resource allocation.

 **Pro Tip:** Integrate multiple CTI sources (like OTX, AbuseIPDB, MISP) into your SOC workflows. The richer the data, the better your decision-making.

 **Question for you:** Do you use open-source or commercial threat intel feeds in your work or studies?

---

## Comprendre la Cyber Threat Intelligence (CTI) en Environnement SOC

Dans un contexte de menaces croissantes, la Threat Intelligence (TI) est essentielle pour les équipes SOC. Elle regroupe des connaissances fondées sur des preuves concernant les menaces existantes ou émergentes (IOC, TTP, profils d'acteurs malveillants).

### Cas d'usage clés pour les analystes SOC :

- 1- Enrichissement des alertes : Mise en contexte des alertes grâce à des correspondances avec des indicateurs malveillants connus.
- 2- Threat Hunting : Recherche proactive de menaces latentes à l'aide d'informations issues de campagnes récentes.
- 3- Accélération de la réponse aux incidents : Analyse plus efficace grâce à des données exploitables.
- 4- Amélioration des règles de détection : Utilisation des TTP pour affiner les règles SIEM.
- 5- Planification stratégique : Les tendances TI orientent les priorités de défense à long terme.

 Conseil : Intégrez plusieurs sources CTI (OTX, AbuseIPDB, MISP, etc.) dans vos outils SOC pour une meilleure visibilité et efficacité.

 Question : Utilisez-vous des flux d'intelligence open source ou commerciaux dans vos projets ou stages ?

## 2- IoC vs IoA – Indicators Explained with Examples

### Understanding Indicators of Compromise vs. Indicators of Attack

In threat detection, knowing the difference between an IoC and an IoA is essential for SOC analysts. Both are signals of malicious activity, but they serve different roles in the detection and response lifecycle.

#### IoC – Indicator of Compromise

A forensic artifact left behind after an attack.

Helps confirm that a system was compromised.

Examples:

- Malicious IP address
- Malware hash (e.g., MD5/SHA256)
- Suspicious domain
- Unusual registry key

#### IoA – Indicator of Attack

Focuses on attacker behaviors and intent, even before the compromise.

Helps detect ongoing or imminent threats.

Examples:

- PowerShell run from Word document
- Lateral movement between hosts
- Credential dumping
- Use of Living-off-the-Land binaries (LOLBins)

 Pro Tip: Use IoCs for alert correlation and triage, and IoAs for proactive threat detection and hunting.

 Question: Do you find it harder to detect IoAs than IoCs in your lab or real SOC work?

---

### Comprendre les IoC (Indicateurs de Compromission) vs IoA (Indicateurs d'Attaque)

Dans un SOC, il est crucial de différencier les IoC et les IoA. Ces deux types d'indicateurs signalent une activité malveillante, mais à des étapes différentes du cycle de détection.

#### IoC – Indicateur de Compromission

Preuve laissée après une attaque.

Sert à confirmer une compromission.

Exemples :

- Adresse IP malveillante
- Empreinte de malware (MD5/SHA256)
- Domaine suspect
- Clé de registre anormale

#### IoA – Indicateur d'Attaque

Met en évidence l'intention et le comportement de l'attaquant, même avant l'impact.

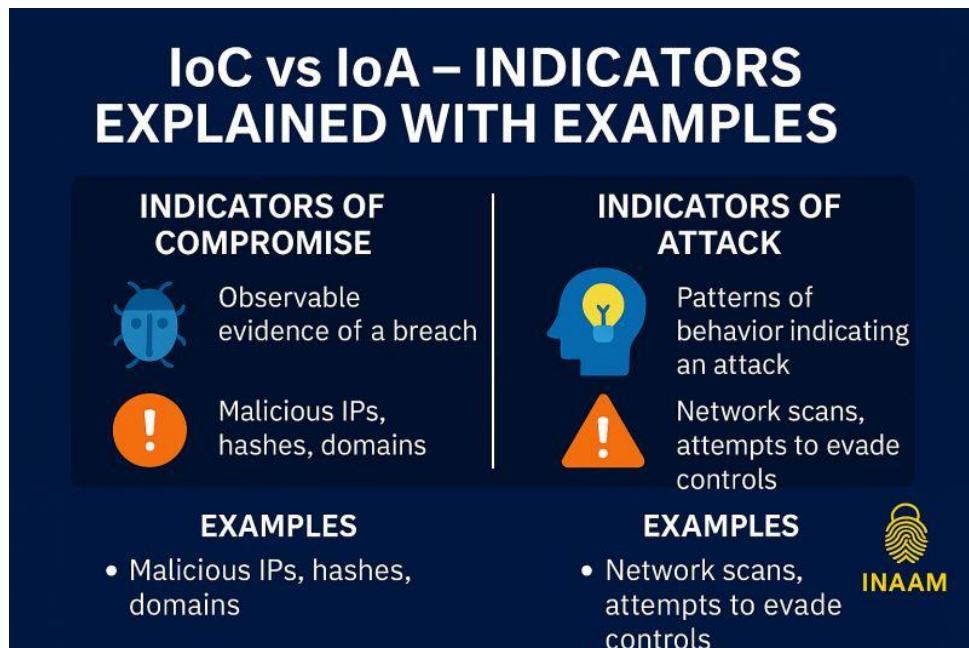
Sert à détecter une attaque en cours ou imminente.

Exemples :

- Exécution de PowerShell via un document Word
- Mouvement latéral entre machines
- Vol de mots de passe
- Utilisation de binaires système légitimes (LOLBins)

 Conseil: Les IoC sont utiles pour la corrélation et le triage, tandis que les IoA servent à la détection proactive et au threat hunting.

 Question : Trouvez-vous plus difficile de détecter les IoA que les IoC dans vos exercices ou expériences en SOC ?



## 3- VirusTotal, AbuseIPDB, Shodan – Analyst's Toolbox

### Free Intelligence Tools Every SOC Analyst Should Know

A well-equipped SOC analyst relies not only on logs and alerts but also on external tools to enrich investigations, validate alerts, and make informed decisions. Here are three essential platforms in the SOC analyst's toolbox:

#### VirusTotal

- Aggregates antivirus engines and URL scanners to analyze files, hashes, and domains.
- Use it to quickly check if a file or domain has been flagged as malicious.
- Great for verifying suspicious attachments or links.

#### AbuseIPDB

- A community-driven platform for checking if an IP has been reported for abuse (e.g., brute force, spam, scanning).
- Use it during triage to prioritize alerts or enrich incident reports.
- Includes confidence scores and categories.

#### Shodan

- A search engine for Internet-connected devices and services.
- Use it to see what ports or services are exposed on a given IP or host.
- Helpful for identifying vulnerable assets or confirming exposure during investigations.

 **Pro Tip:** Bookmark these tools and use them in parallel for context-rich triage. External validation strengthens your SOC decisions.

 **Question:** Have you integrated any of these tools into automated enrichment or daily workflows?

---

## Outils gratuits incontournables pour les analystes SOC

Un bon analyste SOC ne se limite pas à analyser des journaux — il utilise aussi des outils externes pour enrichir ses enquêtes, valider les alertes et gagner en réactivité. Voici trois plateformes essentielles :

#### VirusTotal

- Agrège plusieurs moteurs antivirus et analyseurs d'URL.
- Permet de vérifier rapidement si un fichier, un hash ou un domaine est malveillant.
- Idéal pour analyser des pièces jointes ou des liens suspects.

#### AbuseIPDB

- Plateforme collaborative pour vérifier si une IP a été signalée pour abus (brute force, scan, spam...).
- Utile pour prioriser une alerte ou enrichir un rapport d'incident.
- Fournit des scores de confiance et des catégories d'abus.

 Shodan

- Moteur de recherche des appareils connectés à Internet.
- Permet d'identifier les services exposés sur une IP donnée.
- Très utile pour détecter les actifs vulnérables ou mal configurés.

 Conseil: Enregistrez ces outils dans vos favoris et utilisez-les ensemble pour enrichir le contexte de vos analyses.

 Question : Avez-vous déjà intégré ces outils dans vos workflows ou vos scripts d'enrichissement automatisé ?



## 4- What Is a CVE and How to Read It?

Understanding CVEs – A Must for SOC Analysts

A CVE (Common Vulnerabilities and Exposures) is a standardized identifier for a known cybersecurity vulnerability. Managed by MITRE and used globally, CVEs help SOC teams, red teams, and vendors communicate clearly about specific flaws.

🔍 Example:

CVE-2023-23397

- CVE: Common Vulnerabilities and Exposures
- 2023: The year the CVE was assigned
- 23397: A unique ID number

🧠 How to Read It in Practice:

1- Search the CVE on <https://nvd.nist.gov> or vendor bulletins.

2- Check:

- Severity (CVSS Score – calculate it here: <https://lnkd.in/eVb8svpg>)
- Attack Vector (Remote, Local, etc.)
- Impact (Privilege escalation, code execution, etc.)
- Patch availability

💡 Pro Tip: Use CVEs to assess the risk level of alerts or asset exposure in vulnerability scans. Most SIEMs and threat intel tools link directly to CVE data.

❓ Question: Do you check the CVE description when analyzing alerts linked to vulnerability exploits?

---

## Comprendre les CVE – Une compétence clé pour les analystes SOC

Un CVE (Common Vulnerabilities and Exposures) est un identifiant normalisé pour une vulnérabilité connue. Il est géré par MITRE et utilisé dans le monde entier pour désigner les failles de sécurité de manière claire et unique.

🔍 Exemple:

CVE-2023-23397

- CVE : Common Vulnerabilities and Exposures
- 2023 : Année d'enregistrement
- 23397 : Numéro unique

🧠 Comment lire un CVE ?

1- Recherchez le CVE sur <https://nvd.nist.gov> ou dans les bulletins des éditeurs.

2- Analysez :

- Gravité (score CVSS – calculez-le ici : <https://lnkd.in/eVb8svpg>)
- Vecteur d'attaque (à distance, local, etc.)
- Impact (élévation de priviléges, exécution de code...)
- Disponibilité du correctif

 Conseil: Les CVE permettent d'évaluer la gravité d'une vulnérabilité détectée dans une alerte ou un scan. La plupart des SIEM et outils de Threat Intel intègrent déjà ces données.

 Question: Est-ce que vous consultez les détails des CVE lorsque vous traitez des alertes liées aux vulnérabilités ?

# WHAT IS A CVE AND HOW TO READ IT?



**IDENTIFIER**  
CVE-2021-44228  
format



**DESCRIPTION**  
Summary of the  
vulnerability



**SCORE**  
Severity from  
0 to 10



**CALCULATOR**  
[nvd.nist.gov/vuln-metrics/cvss/v3-calc](http://nvd.nist.gov/vuln-metrics/cvss/v3-calc)



## 5- MITRE ATT&CK – Tactics and Techniques for SOC

What is MITRE ATT&CK?

MITRE ATT&CK is a globally accessible knowledge base that maps real-world adversary behaviors. It structures cyberattacks into Tactics (the “why”) and Techniques (the “how”), helping SOC analysts understand and detect threats more effectively.

### Why It Matters for SOC Analysts

In a SOC environment, ATT&CK provides:

- A shared language between blue and red teams
- Contextual insights during alert investigation
- A framework to build detection rules and enrich alerts

### Key Components

- Tactics – The attacker’s objectives (e.g., Initial Access, Persistence, Exfiltration)
- Techniques – How they achieve that objective (e.g., Phishing, Registry Run Keys, Exfil via Web)
- Sub-techniques – More granular actions (e.g., Spearphishing via Service)
- Mitigations – Defensive strategies to stop or detect them
- Detection – How to spot the behavior in your logs

**?** Pro Tip: Use ATT&CK Navigator (<https://lnkd.in/em8Ui-Yw>) to map detections, simulate attack paths, or prioritize coverage based on threat intel.

---

## MITRE ATT&CK – Tactiques et Techniques pour le SOC

Qu'est-ce que MITRE ATT&CK ?

MITRE ATT&CK est une base de connaissances mondiale qui cartographie les comportements des attaquants. Elle structure les attaques en Tactiques (le « pourquoi ») et Techniques (le « comment »), ce qui aide les analystes SOC à mieux détecter et comprendre les menaces.

### Pourquoi c'est important pour un analyste SOC

Dans un SOC, ATT&CK permet de :

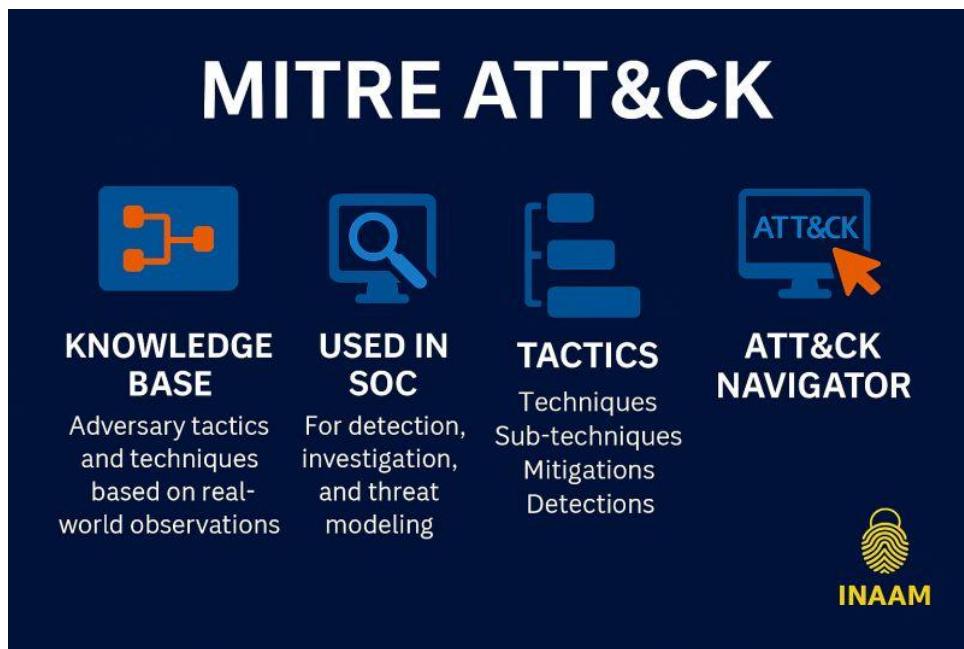
- Créer un langage commun avec l’équipe offensive
- Mieux analyser les alertes de sécurité
- Renforcer la détection avec des règles alignées sur des scénarios réels

### Éléments clés

- Tactiques – Objectif de l’attaquant (ex : accès initial, persistance, exfiltration)
- Techniques – Moyens utilisés (ex : hameçonnage, clés de registre, exfiltration via le web)
- Sous-techniques – Détails plus précis (ex : spearphishing via un service)

- Contremesures – Moyens de se défendre
- Détection – Comment repérer le comportement dans les journaux

❓ Astuce SOC: Utilisez ATT&CK Navigator (<https://lnkd.in/em8Ui-Yw>) pour cartographier vos règles, simuler des scénarios, ou combler les lacunes de visibilité.



## 6- Threat Hunting – Concepts and Starter Tactics

- 🧠 Explore how proactive hunting boosts detection capabilities
- 💡 Learn simple tactics you can apply even as a junior
- ❓ Have you tried hunting before an alert fires?

### What is Threat Hunting?

It's the proactive search for threats that evade detection tools.

Rather than waiting for alerts, analysts examine logs and behavior to find stealthy attackers: fileless malware, LOLBins, and persistence tricks.

### 🔒 SOC Relevance

You may not lead hunts yet, but knowing how threat hunting works helps you:

- ✓ Understand attack patterns
- ✓ Support senior investigations
- ✓ Ask better questions

### 🔧 Starter Tactics

Baseline "normal" activity (logins, processes, network flows)

Use a hypothesis (e.g., "What if a user runs malicious PowerShell?")

Leverage CTI tools: Sigma, MITRE ATT&CK, VirusTotal, AbuseIPDB

Hunt for rare or risky behaviors: unusual parent-child processes, odd ports, privilege escalations

### 💡 Pro Tip

Even if you're not officially assigned to a hunt, you can still contribute:

Ask "What's strange here?" — and document it.

### ❓ Ever uncovered a hidden threat?

Share your experience or favorite tactic below 

---

## Qu'est-ce que le Threat Hunting ?

C'est une recherche proactive des menaces qui échappent aux outils.

Au lieu d'attendre les alertes, on analyse les logs pour détecter des attaques furtives (malware sans fichier, LOLBins, persistance discrète).

### 🔒 Utilité en SOC

Même en tant que junior :

- ✓ Vous comprenez mieux les attaques

- ✓ Vous soutenez les analyses seniors
- ✓ Vous développez votre instinct d'analyste

 Tactiques pour débuter

Connaître l'activité "normale" (connexions, processus)

Utiliser une hypothèse ("Et si un script PowerShell était malveillant ?")

Utiliser des outils : Sigma, MITRE ATT&CK, VirusTotal, AbuseIPDB

Chercher l'anormal ou rare : processus étranges, ports inhabituels, élévarions de priviléges

 Astuce

Même sans être en mission "threat hunt" officielle :

Soyez curieux, posez des questions, notez l'anormal.

 Et vous, avez-vous déjà détecté une activité cachée ? Partagez vos idées !

## 7- The Cyber Kill Chain – Phases of an Attack

- 🧠 Understand how attackers move step by step
- 💡 Learn to detect and break the chain early
- ❓ Which phase do you think SOC teams can disrupt most effectively?

What Is the Cyber Kill Chain?

Developed by Lockheed Martin, the Cyber Kill Chain describes the stages of a cyberattack, from reconnaissance to data theft.

It helps SOC teams understand attacker behavior, align detections, and intervene earlier.

### The 7 Kill Chain Phases

- 1- Reconnaissance – Gathering intel (emails, IPs, targets)
- 2- Weaponization – Crafting malware (exploit + payload)
- 3- Delivery – Sending it (phishing, USB, watering hole)
- 4- Exploitation – Triggering the malware
- 5- Installation – Gaining persistence
- 6- Command & Control (C2) – Remote control established
- 7- Actions on Objectives – Data theft, lateral movement, destruction

### SOC Relevance

- ✓ Helps map detections to attack phases
- ✓ Supports MITRE ATT&CK correlation
- ✓ Improves threat hunting and response
- ✓ Enables defense-in-depth: stop attacks earlier

 Pro Tip: SOC teams often catch attacks at delivery or C2, but the real win is detecting earlier — during recon or weaponization.

❓ Which phase do you focus on most in your current environment?

Let's share experiences 

---

## Qu'est-ce que le Cyber Kill Chain ?

Créé par Lockheed Martin, le Cyber Kill Chain décrit les phases d'une cyberattaque, de la reconnaissance à l'exfiltration.

Il aide les SOC à comprendre l'adversaire et à agir plus tôt dans la chaîne.

### Les 7 phases du Kill Chain

- 1- Reconnaissance – Collecte d'informations (emails, IPs...)

- 2- Armes (Weaponization) – Création du malware
- 3- Livraison – Phishing, clé USB, site piégé...
- 4- Exploitation – Déclenchement via une vulnérabilité
- 5- Installation – Accès et persistance
- 6- Commande & Contrôle (C2) – Connexion avec l'attaquant
- 7- Actions finales – Exfiltration, déplacement latéral, sabotage

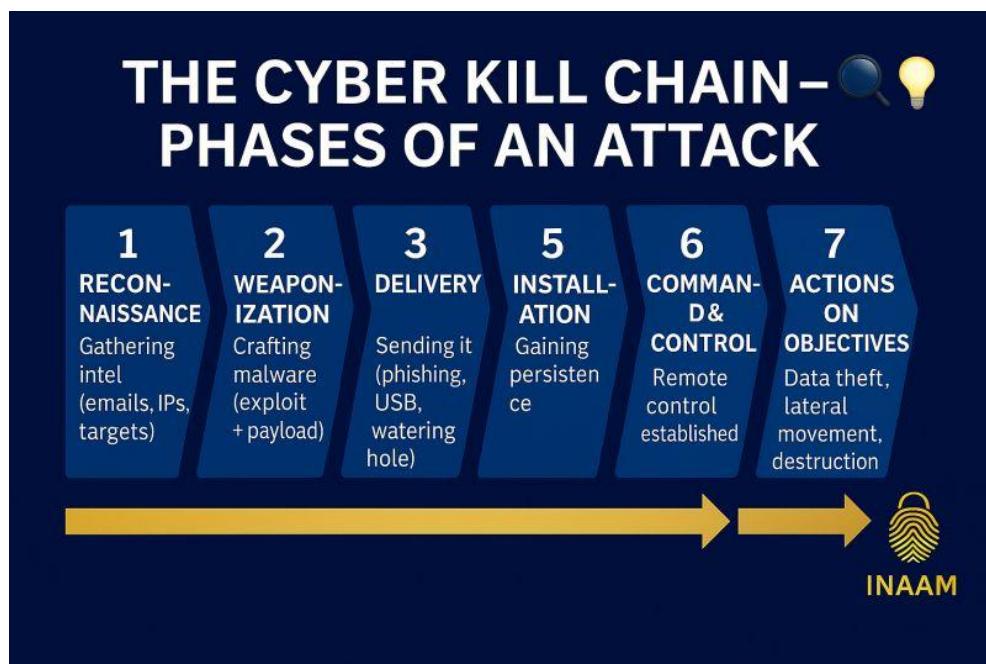
 Utilité en SOC

- ✓ Relier les alertes aux phases de l'attaque
- ✓ Soutenir les analyses avec MITRE ATT&CK
- ✓ Renforcer la chasse et la réponse
- ✓ Stopper l'attaque dès les premières étapes

 Astuce: La plupart des SOC détectent à l'étape livraison ou C2, mais l'objectif est de réagir plus tôt — dès la reconnaissance si possible.

 Quelle étape vous semble la plus critique à surveiller dans un SOC ?

Partagez en commentaires 



## 8- Using MISP to Share Threat Intelligence

🧠 Discover how MISP supports collaboration between analysts

💡 Learn what indicators you can share — and why it matters

❓ Have you used MISP or another threat sharing platform?

What is MISP?

MISP (Malware Information Sharing Platform) is an open-source platform that enables structured sharing of threat intelligence (TI) between organizations, SOC teams, and CERTs. It helps analysts collect, enrich, store, and distribute IOCs (Indicators of Compromise), TTPs, and threat event data securely and efficiently.

🔒 How MISP Supports the SOC

- ✓ Centralized repository for internal and external threat data
- ✓ Easy correlation of IOCs (e.g., IPs, hashes, domains)
- ✓ Visualize threat events and related indicators
- ✓ Export to SIEMs, EDRs, and CTI feeds
- ✓ Supports taxonomies (e.g., MITRE ATT&CK, TLP levels)

💡 Use Cases

- ◆ A phishing email's indicators (URLs, senders, attachments)
- ◆ A malware hash detected by EDR
- ◆ IPs flagged by AbuseIPDB or OTX
- ◆ Correlating shared threat events across different SOCs

💡 Pro Tip

MISP is most powerful when used collaboratively. Sharing anonymously with trusted communities boosts collective defense.

❓ Have you contributed or consumed data from a threat-sharing platform?

Let's exchange experiences 👋

---

### Qu'est-ce que MISP ?

MISP (Malware Information Sharing Platform) est une plateforme open-source conçue pour le partage structuré d'informations de cybermenaces entre organisations, équipes SOC, et CERTs.

Elle permet de collecter, enrichir, stocker et partager des IOCs, TTPs et données d'événements de manière sécurisée.

 Utilité de MISP pour le SOC

- ✓ Base centralisée des menaces internes et externes
- ✓ Corrélation facile des IOCs (IPs, hash, domaines...)
- ✓ Visualisation des événements liés
- ✓ Export vers SIEM, EDR ou outils CTI
- ✓ Support des taxonomies (MITRE ATT&CK, TLP...)

 Cas d'usage

- ◆ Indicators d'un email de phishing (URL, pièces jointes...)
- ◆ Hash de malware repéré par un EDR
- ◆ IPs suspectes via AbuseIPDB ou OTX
- ◆ Corrélation entre plusieurs événements partagés

 Astuce

MISP devient réellement puissant quand il est utilisé en collaboration. Partager (même anonymement) renforce la défense collective.

 Avez-vous déjà partagé ou utilisé des données via une plateforme de Threat Intelligence ?  
Faites-nous part de votre expérience 

# USING MISP TO SHARE THREAT INTELLIGENCE



-  **COLLECT**  
IOCs, TTPs, threat events
-  **ENRICH**  
Correlate data, add context
-  **STORE**  
Centralized repository
-  **SHARE**  
Within trusted communities



## 9- How to Investigate a Suspicious IP or Domain

- 🧠 Learn how to pivot and enrich threat data like a SOC analyst
- 💡 Discover free tools to analyze reputation, behavior, and context
- ❓ What's your go-to platform for IP/domain investigation?

### Why Investigate IPs and Domains?

In the SOC, alerts often involve network indicators like suspicious IPs or domains. Quickly understanding their reputation, activity, and context is critical to validating threats and reducing false positives.

#### 🔍 Investigation Workflow (Basic Steps)

##### Check Reputation

- Tools: VirusTotal, AbuseIPDB, Cisco Talos, Pulsedive
- Look for malware flags, abuse reports, classifications

##### Enrich with Context

- WHOIS info: Owner, registration date, ASN
- GeolP: Location and hosting provider
- Passive DNS: Related domains and history

##### Correlate with Threat Intelligence

- Cross-check with CTI platforms (e.g., OTX, MISP, ThreatFox)
- Link indicators to malware campaigns or threat actors

##### Pivoting & Graph Analysis

- Use tools like VirusTotal Graph, Maltego, or Spiderfoot
- Explore connected domains, IP clusters, shared certs

💡 Pro Tip: Document everything. Tag IOCs in your SIEM and CTI platform for faster detection and response next time.

#### ❓ Which tools do you rely on most when checking IOCs?

Let's compare techniques in the comments 👇

---

## Pourquoi enquêter sur des IPs ou domaines ?

Dans un SOC, les alertes impliquent souvent des indicateurs réseau. Enquêter rapidement sur leur réputation, activité et contexte est essentiel pour valider une menace ou éliminer un faux positif.

#### 🔍 Étapes d'analyse (workflow de base)

Vérifier la réputation

- Outils : VirusTotal, AbuseIPDB, Cisco Talos, Pulsedive
  - Signaux : rapports d'abus, détection malware, réputation
- Enrichir le contexte
- WHOIS : propriétaire, date d'enregistrement, ASN
  - GeoIP : localisation, hébergeur
  - DNS passif : domaines liés, historique
- Corréler avec du Threat Intel
- Plateformes CTI (OTX, MISP, ThreatFox...)
  - Identifier des campagnes ou groupes d'attaquants
- Pivot et analyse de graphe
- Outils : VirusTotal Graph, Maltego, Spiderfoot
  - Explorer les connexions : IPs, domaines, certificats SSL...

💡 Astuce: Documentez vos recherches et taguez les IOCs dans vos outils (SIEM/CTI) pour une détection plus rapide à l'avenir.

? Quels outils utilisez-vous le plus pour analyser un IOC ?

Partagez vos bonnes pratiques en commentaire 👉

