



---

# SOC LEVEL 1 ESSENTIALS

## – PART H: ADVENCED TOOLS & TECHNIQUES

### (Posts 57–61)

---

Mastering advanced SOC tools for deep visibility, scalable forensics, and effective threat detection.



OCTOBER 13, 2025

INAAM KABBARA

SECURITY ANALYST | CYBERSECURITY CONTENT CREATOR | EPITA MSC GRADUATE

## Table of Contents

1- Intro to OSQuery for Endpoint Visibility .....	2
2- Sysmon for Deep Windows Log Monitoring .....	4
3- Velociraptor – Endpoint Forensics at Scale .....	6
4-Zeek vs Suricata – Network Threat Detection.....	8
5-Sandbox Analysis for Suspicious Files (Intro) .....	10

# 1- Intro to OSQuery for Endpoint Visibility

## Topic Overview

OSQuery is an open-source framework developed by Facebook that turns your operating system into a high-performance relational database. It allows analysts to run SQL-like queries on endpoints (Windows, Linux, macOS) to retrieve real-time system information.

## Relevance to SOC

For SOC analysts, OSQuery provides lightweight yet powerful endpoint visibility. It is widely used in incident investigations, compliance monitoring, and threat hunting.

## Key Features

Query processes, users, network connections, and system state in real time

Cross-platform and resource-efficient

Integrates with SIEMs for centralized monitoring

Detects anomalies such as persistence mechanisms, privilege escalation, or unauthorized access

## Pro Tip

Begin with simple queries — for example, list logged-in users or recently created processes. Then, move toward automation by streaming OSQuery logs into your SIEM for continuous monitoring.

## Closing Question

Have you already used OSQuery in your environment? If yes, which query do you find most useful for endpoint visibility?

---

# Introduction à OSQuery pour la visibilité des endpoints

## Aperçu du sujet

OSQuery est un framework open source développé par Facebook qui transforme le système d'exploitation en base de données relationnelle performante. Il permet d'exécuter des requêtes SQL sur les endpoints (Windows, Linux, macOS) afin d'obtenir des informations système en temps réel.

## Pertinence pour le SOC

Pour les analystes SOC, OSQuery offre une visibilité légère mais puissante sur les endpoints. Il est largement utilisé dans les enquêtes d'incident, le suivi de conformité et le threat hunting.

## Fonctionnalités clés

Interroger les processus, utilisateurs, connexions réseau et état système en temps réel

Multi-plateforme et peu gourmand en ressources

S'intègre facilement à un SIEM pour une supervision centralisée

Déetecte des anomalies telles que les mécanismes de persistance, l'escalade de priviléges ou

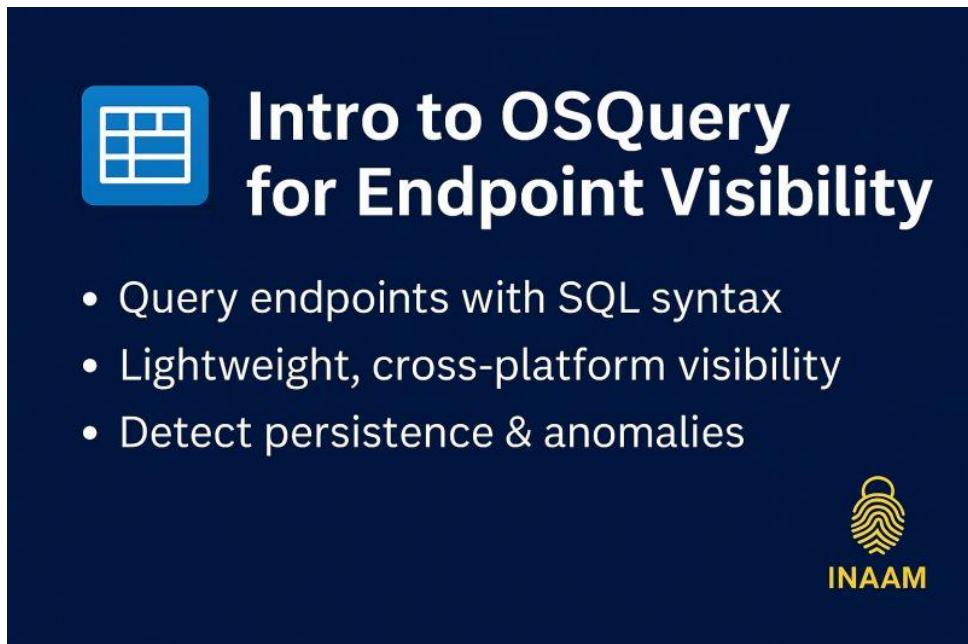
les accès non autorisés

 Astuce

Commencez par des requêtes simples — par exemple, la liste des utilisateurs connectés ou des processus récemment créés. Ensuite, automatisez l'analyse en envoyant les journaux OSQuery vers votre SIEM pour un suivi continu.

 Question de clôture

Avez-vous déjà utilisé OSQuery dans votre environnement ? Si oui, quelle requête trouvez-vous la plus utile pour la visibilité sur les endpoints ?



The slide has a dark blue background. On the left, there is a blue square icon containing a white grid of four squares. To its right, the title 'Intro to OSQuery for Endpoint Visibility' is displayed in large, bold, white font. Below the title is a bulleted list of three items in white font: '• Query endpoints with SQL syntax', '• Lightweight, cross-platform visibility', and '• Detect persistence & anomalies'. In the bottom right corner of the slide, there is a yellow circular logo with a fingerprint pattern and the word 'INAAM' in yellow capital letters.

- Query endpoints with SQL syntax
- Lightweight, cross-platform visibility
- Detect persistence & anomalies

## 2- Sysmon for Deep Windows Log Monitoring

### Topic Overview

Sysmon (System Monitor) is a Windows system service and driver from Microsoft Sysinternals that provides detailed monitoring of system activities. It logs critical events such as process creation, network connections, and file modifications to the Windows Event Log.

### Relevance to SOC

For SOC analysts, Sysmon is a cornerstone of Windows endpoint monitoring. It enriches visibility far beyond native Windows logs, enabling better detection of malicious behaviors like privilege escalation, persistence, and lateral movement.

### Key Features

Logs process creation, termination, and parent-child relationships

Captures network connections (IP, ports, protocols)

Detects file modifications and registry changes

Provides rich telemetry for threat hunting and forensic investigations

### Pro Tip

Use a well-maintained Sysmon configuration (e.g., from SwiftOnSecurity) to reduce noise and focus on high-value events. Fine-tuning ensures that your SIEM ingests actionable data instead of overwhelming analysts with irrelevant logs.

### Closing Question

Have you deployed Sysmon in your environment? If yes, what's your go-to event ID for detecting suspicious activity?

---

## Sysmon pour une surveillance approfondie des journaux Windows

### Aperçu du sujet

Sysmon (System Monitor) est un service système et un pilote Windows développé par Microsoft Sysinternals. Il enregistre des événements critiques comme la création de processus, les connexions réseau et les modifications de fichiers dans les journaux d'événements Windows.

### Pertinence pour le SOC

Pour les analystes SOC, Sysmon est un pilier de la surveillance des endpoints Windows. Il offre une visibilité bien plus riche que les journaux natifs de Windows, permettant de mieux détecter les comportements malveillants tels que l'escalade de priviléges, la persistance et les mouvements latéraux.

### Fonctionnalités clés

Journalise la création, l'arrêt et la hiérarchie des processus

Capture les connexions réseau (IP, ports, protocoles)

Déetecte les modifications de fichiers et de registre

Fournit une télémétrie détaillée pour le threat hunting et les enquêtes forensiques

 Astuce

Utilisez une configuration Sysmon bien maintenue (par exemple, celle de SwiftOnSecurity) pour réduire le bruit et cibler les événements les plus pertinents. Un bon réglage permet à votre SIEM d'ingérer des données exploitables plutôt que des journaux excessifs.

 Question de clôture

Avez-vous déployé Sysmon dans votre environnement ? Si oui, quel est votre ID d'événement préféré pour détecter une activité suspecte ?



The image shows the Sysmon Deep Windows Log Monitoring logo. It features a blue square icon containing a white Windows logo with a magnifying glass over it. To the right of the icon, the word "Sysmon" is written in a large, bold, white sans-serif font. Below "Sysmon", the words "Deep Windows Log Monitoring" are written in a slightly smaller, bold, white sans-serif font. Below this text, there is a bulleted list of features in white text: "• Process & parent logging", "• Network connection tracking", and "• File & registry change detection". In the bottom right corner of the dark blue background, there is a yellow fingerprint icon and the acronym "INAAM" in yellow capital letters.

- Process & parent logging
- Network connection tracking
- File & registry change detection

INAAM

## 3- Velociraptor – Endpoint Forensics at Scale

### Topic Overview

Velociraptor is an open-source endpoint visibility and digital forensics tool. It allows security teams to hunt, collect, and analyze forensic artifacts across thousands of endpoints in real time, using its query language VQL (Velociraptor Query Language).

### Relevance to SOC

For SOC analysts, Velociraptor provides deep insight into endpoint behavior during investigations and incident response. Its scalability makes it especially useful for organizations managing large fleets of endpoints.

### Key Features

Forensic artifact collection (processes, files, registry, memory)

Real-time endpoint hunting with VQL queries

Scales to thousands of endpoints for enterprise use

Supports incident response, threat hunting, and compliance monitoring

### Pro Tip

Leverage community-maintained Velociraptor artifacts to speed up investigations. Combine Velociraptor with a SIEM to enrich detection with forensic depth.

### Closing Question

Have you tried Velociraptor in your SOC environment? If yes, what kind of forensic data did you find most valuable?

---

## Velociraptor – Analyse forensique des endpoints à grande échelle

### Aperçu du sujet

Velociraptor est un outil open source de visibilité des endpoints et d'investigation forensique. Il permet aux équipes de sécurité de rechercher, collecter et analyser des artefacts forensiques sur des milliers d'endpoints en temps réel grâce à son langage de requêtes VQL (Velociraptor Query Language).

### Pertinence pour le SOC

Pour les analystes SOC, Velociraptor offre une visibilité approfondie sur le comportement des endpoints lors des enquêtes et des réponses aux incidents. Sa capacité d'évolutivité le rend particulièrement adapté aux grandes organisations.

### Fonctionnalités clés

Collecte d'artefacts forensiques (processus, fichiers, registre, mémoire)

Threat hunting en temps réel avec des requêtes VQL

S'adapte à des milliers d'endpoints à l'échelle entreprise

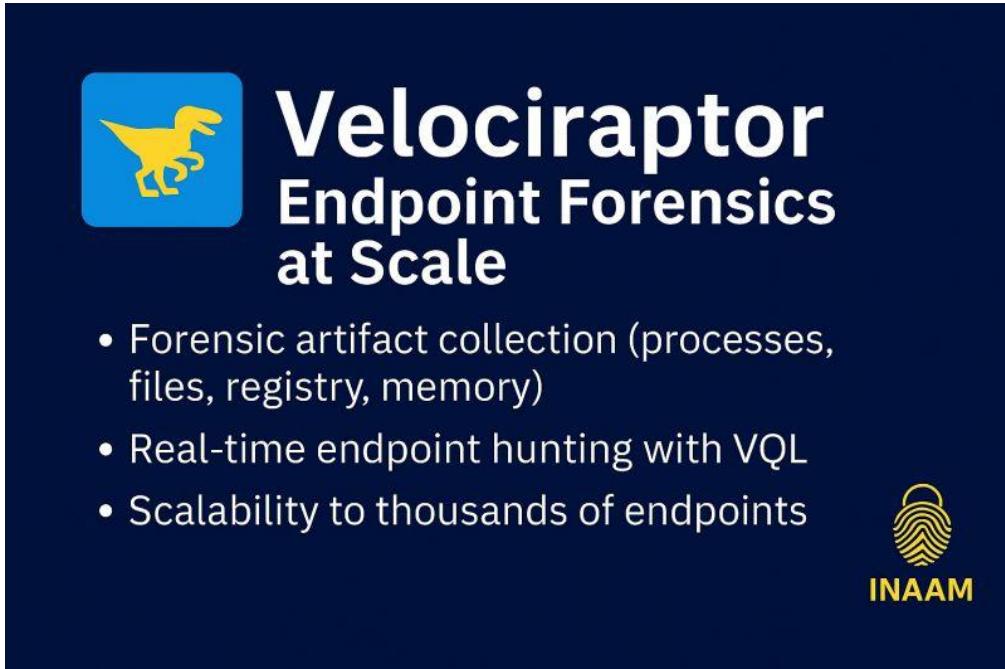
Utile pour la réponse aux incidents, le threat hunting et le suivi de conformité

 Astuce

Profitez des artefacts Velociraptor maintenus par la communauté pour accélérer vos enquêtes. Combinez Velociraptor avec un SIEM afin d'enrichir vos détections par une profondeur forensique.

 Question de clôture

Avez-vous déjà utilisé Velociraptor dans votre environnement SOC ? Si oui, quels types de données forensiques vous ont paru les plus utiles ?



The slide features a blue background with a white border. In the top left corner is a blue square icon containing a yellow velociraptor silhouette. To its right, the text "Velociraptor" is written in large, bold, white sans-serif font, with "Endpoint Forensics" and "at Scale" stacked below it in a slightly smaller font. Below this title is a bulleted list of features in white text:

- Forensic artifact collection (processes, files, registry, memory)
- Real-time endpoint hunting with VQL
- Scalability to thousands of endpoints

In the bottom right corner, there is a yellow fingerprint icon above the word "INAAM" in a bold, yellow sans-serif font.

## 4-Zeek vs Suricata – Network Threat Detection

### Topic Overview

Zeek and Suricata are two powerful open-source network monitoring tools widely used in SOCs. While both improve network visibility, they serve different purposes:

Zeek focuses on rich protocol analysis, metadata extraction, and behavioral monitoring.

Suricata is a high-performance intrusion detection/prevention system (IDS/IPS) with signature-based detection and packet capture.

### Relevance to SOC

Together, Zeek and Suricata complement each other:

Zeek gives analysts deep insights into network behaviors (e.g., DNS tunneling, unusual HTTP requests).

Suricata alerts on known attack patterns using rule sets (like Emerging Threats).

### Key Features

#### Zeek

Protocol parsing and metadata logging

Behavioral analysis (DNS, HTTP, SSL/TLS, etc.)

Extensible scripting for custom detections

#### Suricata

IDS/IPS with signature-based rules

Real-time traffic inspection and alerting

High-performance packet capture and logging

### Pro Tip

Use Zeek for context and visibility, and Suricata for real-time detection. Many SOCs deploy both in parallel to maximize coverage.

### Closing Question

If you had to choose, would you prioritize behavioral visibility (Zeek) or signature-based alerts (Suricata) in your SOC?

---

## Zeek vs Suricata – Détection des menaces réseau

### Aperçu du sujet

Zeek et Suricata sont deux outils open source puissants de surveillance réseau, largement utilisés dans les SOC. Bien qu'ils améliorent tous deux la visibilité réseau, leurs objectifs diffèrent :

Zeek se concentre sur l'analyse approfondie des protocoles, l'extraction de métadonnées et la surveillance comportementale.

Suricata est un système IDS/IPS performant basé sur des signatures, capable de détecter et bloquer des attaques connues.

 Pertinence pour le SOC

Ensemble, Zeek et Suricata se complètent :

Zeek fournit aux analystes une visibilité détaillée des comportements réseau (ex. tunneling DNS, requêtes HTTP inhabituelles).

Suricata alerte sur des schémas d'attaque connus via des règles (comme Emerging Threats).

 Fonctionnalités clés

**Zeek**

Analyse des protocoles et journalisation des métadonnées

Analyse comportementale (DNS, HTTP, SSL/TLS, etc.)

Scripting extensible pour des détections personnalisées

**Suricata**

IDS/IPS basé sur des signatures

Inspection et alertes en temps réel du trafic

Capture et journalisation haute performance des paquets

 Astuce

Utilisez Zeek pour la visibilité et le contexte, et Suricata pour la détection en temps réel. De nombreux SOC les déplient ensemble pour une couverture maximale.

 Question de clôture

Si vous deviez choisir, privilégieriez-vous la visibilité comportementale (Zeek) ou les alertes basées sur des signatures (Suricata) dans votre SOC ?

# Zeek vs Suricata Network Threat Detection



**Zeek**

- Protocol analysis & behavioral visibility
- Combined → Stronger SOC coverage



**Suricata**

IDS/IPS with signature detection

 INAAM

## 5-Sandbox Analysis for Suspicious Files (Intro)

### Topic Overview

Sandbox analysis is the process of executing suspicious files in an isolated, controlled environment to observe their behavior safely. This helps SOC analysts determine if a file is malicious without risking production systems.

### Relevance to SOC

For SOC teams, sandboxes provide critical insights beyond static analysis. They reveal real execution behaviors such as process creation, network communication, registry modifications, and persistence techniques.

### Key Features

Executes files in a virtualized or emulated environment

Monitors file, process, registry, and network activity

Detects malware techniques like persistence, C2 connections, or privilege escalation

Integrates with SIEM/EDR for automated enrichment of alerts

### Pro Tip

Start with free or open-source sandboxes (e.g., Cuckoo Sandbox, Joe Sandbox Community, [ANY.RUN](#) free mode) to build familiarity. Then, consider enterprise integrations for automated SOC workflows.

### Closing Question

Do you currently use sandboxing in your SOC? If yes, which tool (Cuckoo, [ANY.RUN](#), Hybrid Analysis, etc.) has been the most effective for your investigations?

---

## Analyse en sandbox des fichiers suspects (Introduction)

### Aperçu du sujet

L'analyse en sandbox consiste à exécuter des fichiers suspects dans un environnement isolé et contrôlé afin d'observer leur comportement en toute sécurité. Cela permet aux analystes SOC de déterminer si un fichier est malveillant sans mettre en danger les systèmes de production.

### Pertinence pour le SOC

Pour les équipes SOC, les sandboxes offrent une visibilité précieuse au-delà de l'analyse statique. Elles révèlent les comportements réels à l'exécution, tels que la création de processus, les communications réseau, les modifications de registre et les mécanismes de persistance.

### Fonctionnalités clés

Exécution des fichiers dans un environnement virtualisé ou émulé

Surveillance des activités (fichiers, processus, registre, réseau)

Détection de techniques malveillantes : persistance, connexions C2, escalade de priviléges

Intégration possible avec un SIEM/EDR pour enrichir automatiquement les alertes

### Astuce

Commencez par des sandboxes gratuites ou open source (ex. Cuckoo Sandbox, Joe Sandbox Community, [ANY.RUN](#) en mode gratuit) pour vous familiariser. Ensuite, envisagez des solutions d'entreprise pour une intégration automatisée dans les workflows SOC.

### Question de clôture

Utilisez-vous déjà une sandbox dans votre SOC ? Si oui, quel outil (Cuckoo, [ANY.RUN](#), Hybrid Analysis, etc.) vous semble le plus efficace pour vos enquêtes ?



The image is a promotional graphic for 'Sandbox Analysis for Suspicious Files'. It features a dark blue background with white text and icons. At the top, the title 'Sandbox Analysis for Suspicious Files' is displayed in large, bold, white font. Below the title is a blue square icon containing a white document with a magnifying glass over it, symbolizing analysis. To the right of the icon, the text 'Isolated & safe environment' is written in white. Below this section, there is a bulleted list of features in white text: '• Monitors file, process & network activity' and '• Detects persistence & malicious techniques'. In the bottom right corner, there is a yellow fingerprint icon above the acronym 'INAAM' in white capital letters.

# Sandbox Analysis for Suspicious Files



Isolated & safe  
environment

- Monitors file, process & network activity
- Detects persistence & malicious techniques



INAAM