

## SOC (Security Operations Center)

Un SOC (Security Operations Center) en français (Centre d'Opérations de Sécurité) est une cellule dédiée à la surveillance, la détection, l'analyse et la réponse aux incidents de sécurité d'un système d'information, en continu (24/7 ou horaires étendus).

Ses objectifs sont de détecter les attaques et comportements suspects, réagir rapidement aux incidents de sécurité, réduire le temps de détection et de réponse d'une attaque, améliorer la posture de sécurité globale et d'assurer la traçabilité et la conformité.

Un SOC est toujours dédié à un périmètre précis, qui peut être :

- Une entreprise
- Un groupe d'entreprises ou plusieurs clients (dans le cas d'un SOC externalisé).

Prenons l'exemple d'un SOC interne (par entreprise ou groupe)

L'entreprise A a son propre SOC

L'entreprise B a aussi son propre SOC

Chaque SOC surveille ses propres systèmes, applique ses propres règles de sécurité et connaît son environnement métier, c'est l'ensemble de ce qui entoure l'entreprise dans son activité professionnelle et qui influence la façon dont elle fonctionne, prend des décisions et atteint ses objectifs.

Dans un groupe (maison mère + filiales) un SOC central peut surveiller toutes les entités du groupe ou chaque entité peut avoir son SOC local.

Prenons l'exemple d'un SOC mutualisé / externalisé (MSSP)

Un prestataire de cybersécurité (MSSP) peut avoir un SOC unique qui surveille plusieurs entreprises clientes.

Le SOC du prestataire surveille :

- L'entreprise A
- L'entreprise B
- L'entreprise C

Les données sont strictement séparées et chaque client a ses propres règles, ses propres alertes ainsi que son propre périmètre. On parle de SOC multi-tenant.

Il existe aussi des SOC par service dédié à des services comme :

SOC IT (bureautique, serveurs)

SOC OT (industriel)

SOC Cloud

SOC pour un service critique (finance, R&D...)

Les analystes SOC sont répartis en différents niveaux de compétence et de responsabilité. En fonction de la complexité des incidents à traiter, chaque niveau intervient de manière différente.

Niveau 1 : Analyste L1 (ou Analyste de surveillance)

Sa mission consiste à la surveillance et au tirage d'alertes, à l'aide d'outils comme :

- Les SIEM (Splunk, IBM QRadar, Microsoft Sentinel, Elastic SIEM, ArcSight) collectent et analyse de grands volumes de données provenant d'applications, de dispositifs, et d'utilisateurs à l'échelle de l'organisation en temps réel combinant les fonctions SIM (gestion des informations de sécurité) et SEM (gestion des événements de sécurité) en un seul système de gestion de la sécurité "SIEM".

- IDS "Intrusion Detection System est un outil de sécurité des réseaux qui surveille le trafic réseau et les appareils pour détecter les activités malveillantes connues, les activités suspectes ou les violations des politiques de sécurité.

- EDR (Endpoint Detection and Response), une solution de cybersécurité conçue pour surveiller en continu les terminaux d'un réseau, détecter des comportements anormaux et intervenir automatiquement en cas de menace. Elle collecte des données telles que les fichiers créés ou modifiés, les processus en cours d'exécution et les connexions réseau. L'EDR utilise l'analyse pour détecter et répondre rapidement aux cyber menaces, ce qui en fait un outil essentiel pour la sécurité des endpoints.

L'analyste L1 filtre les alertes non pertinentes, si elles sont sérieuses il l'escalade vers les analystes de niveau 2, il gère également les incidents basiques telle que les tentatives d'intrusion simples.

Il doit avoir des connaissances de base des systèmes d'exploitation (Windows, Linux), être familiarisé avec les outils de surveillance et de gestion des alertes et en toute logique savoir interpréter des logs de sécurité simples.

#### Niveau 2 : Analyste L2 (ou Analyste en investigation)

Alertes escaladé depuis le niveau 1, l'analyste L2 analyse en profondeur celle-ci, l'identifie et mesure sa gravité. Il est autorisé à prendre des décisions sur les actions immédiates à entreprendre comme l'isolation d'un poste infecté, mise en quarantaine d'un fichier...

Il sera également chargé de la documentation des incidents et à la préparation des rapports pour les équipes de gestion d'incidents.

Il doit être capable de comprendre les différentes techniques d'attaques existantes et savoir les documenter. La maîtrise des SandBoxes et outils pour analyser les activités des endpoints "EDR/XDR" sont nécessaires.

#### Exemple de situation :

Un malware a été détecté sur un poste de travail. L'analyste L2 va :

Analyser le fichier suspect dans une sandbox

Identifier le type de malware (ex : ransomware)

Isoler le poste pour éviter la propagation

Mettre en place un plan de remédiation (réinitialisation du mot de passe, rapports, analyse complète du réseau, restauration à partir de sauvegardes)

### Niveau 3 : Analyste L3 (ou Expert/Specialist)

Spécialiste expert l'analyste L3 effectue des analyses avancées, gère des incidents complexes et donne des réponses tactiques.

#### Activités principales :

Gestion des incidents complexes ou sophistiqués (ex : attaques persistantes avancées, APT).

Investigations forensiques détaillées (analyse de mémoire et périphériques, récupération de données).

Hunting des menaces : chasse proactive des attaques cachées dans le réseau (Threat Hunting).

Développement des règles de détection pour améliorer le SOC (ex : création de règles SIEM personnalisées).

Analyse des malwares et développement de techniques de détection avancées

Conseils stratégiques aux autres niveaux, ainsi qu'à la direction de la sécurité

#### Compétences :

Expertise en sécurité avancée (malware analysis, reverse engineering, hacking)

Très bonne compréhension des systèmes d'exploitation et des réseaux

Expérience avec des outils de forensic (Wireshark, Volatility, IDA Pro)

Connaissances approfondies des techniques d'attaque (MITRE ATT&CK, TTPs)

Capacité à identifier des menaces avancées et des techniques d'évasion

#### Outils utilisés :

Forensics (Volatility, EnCase)

Malware analysis (IDA Pro, Ghidra, OllyDbg)

Threat Intelligence (MISP, OpenDXL, IBM X-Force)