Fiche-conseils

METTRE EN PLACE UN SOC ÉCONOMIQUE

Les systèmes informatiques sont aux premières loges des menaces, potentiels incidents et attaques de cybersécurité aux conséquences plus ou moins sévères et coûteuses (indisponibilité de système, perte de données sensibles, etc.) Aucune institution, aucune entreprise, ne peut se permettre de faire l'impasse sur la protection de son système d'information, même si elle ne dispose que de peu de ressources humaines et/ou financières.

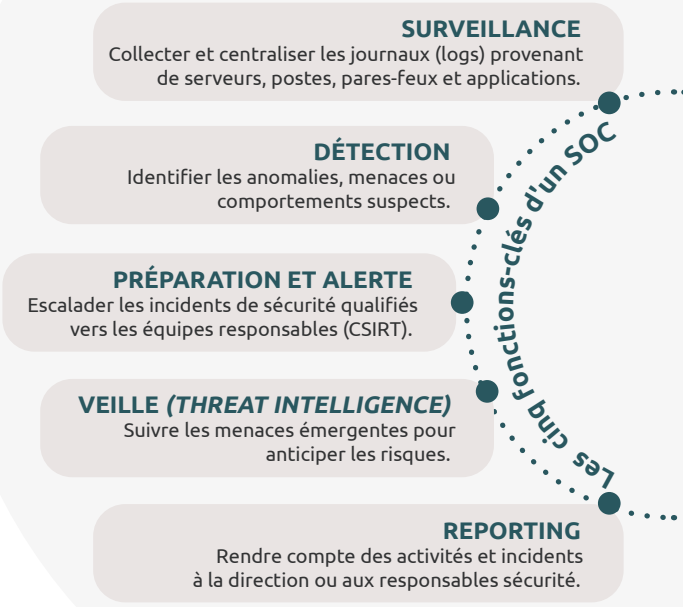
Surveiller son système d'information, détecter les menaces et réagir rapidement aux incidents est un enjeu vital.

Qu'est-ce qu'un SOC ?

Le Centre des Opérations de Sécurité ou *Security Operations Center* (SOC) assure la surveillance continue du système d'information.

Le SOC poursuit plusieurs missions.

- Il surveille en temps réel les événements de sécurité.
- Il détecte les comportements suspects, les anomalies ou actes malveillants.
- Il qualifie les alertes pour déterminer leur gravité et leur impact.
- Il informe et escalade vers les entités compétentes (telle qu'une équipe de sécurité informatique de réponse aux incidents ou *Computer Security Incident Response Team* - CSIRT) pour la prise en charge de la réponse.
- Il contribue à l'amélioration continue de la posture de sécurité (ajustement des règles de détection, rapports, indicateurs, etc.)



Au coeur du SOC : le SIEM

La gestion des événements et des informations de sécurité ou *Security Information and Event Management* (SIEM) est l'un des composants centraux d'un SOC.

1 Le SIEM collecte, centralise, corrèle et analyse les journaux (logs) provenant de toutes les composantes du système d'information. Il est alimenté par :

- des sondes réseau qui analysent le trafic et détectent les anomalies grâce à un système de détection d'intrusion (*Intrusion Detection System* - IDS),
- des agents sur les postes/serveurs qui collectent les logs systèmes et de sécurité,
- des équipements de sécurité de type pares-feux, proxies, antivirus, VPN, etc.
- des sources de *Threat Intelligence* qui enrichissent la détection avec des indicateurs externes (IoC).

2 Le SIEM traduit les données collectées en informations exploitables pour :

- **surveiller** en temps réel l'activité du système d'information,
- **détecter** les anomalies et incidents de sécurité,
- **alerter** automatiquement les analystes en cas de comportement suspect,
- **faciliter** l'investigation grâce à la recherche et à l'historisation des logs,
- **produire** des tableaux de bord et rapports pour le pilotage et la conformité,
- **visualiser** les logs de tout système informatique.

Structuration d'un SOC économique

Le SOC est souvent décrit comme le centre nerveux de la cybersécurité. Contrairement à l'image d'une salle remplie d'écrans et d'analystes 24/7, un SOC peut être léger, distribué et économique. Pour cela, une méthode rigoureuse, une priorisation claire et un outillage *open-source* adapté sont indispensables. Un SOC économique est la solution pour accéder à un niveau de sécurité opérationnelle jusque-là réservé aux grandes structures.

Info !

Qu'il soit économique ou non, la réussite d'un SOC repose sur l'engagement humain, la rigueur des processus et un investissement proportionné aux risques. Une équipe réduite, des processus clairs et des outils *open-source* suffisent à démarrer.

Une équipe d'opérateurs et d'opératrices motivée

Une équipe réduite

Une à plusieurs personnes compétentes (ingénieur-e informatique, responsable de la sécurité des systèmes d'information (RSSI), etc.)

Une dynamique d'amélioration continue

Des processus clairs

- **Définir des rôles** (qui surveille, qui analyse, qui décide et qui agit ?)
- **Documenter les procédures** (*playbooks*) pour les incidents types (hameçonnage *(phishing)*, logiciels de rançon *(ransomware)*, compromission de compte, etc.)
- **Tester la réactivité** (à travers des exercices réguliers)
- **Monter en puissance progressivement** (selon la taille et la maturité de l'organisation)

Des outils adaptés

Des outils *open-source* gratuits

SURVEILLANCE

OpenSearch, pour centraliser les logs et détecter des anomalies.
Open Search collecte, corrèle et visualise les logs de tous les systèmes. C'est la colonne vertébrale du SOC pour la surveillance et la détection.

DÉTECTION

Suricata et **Zeek**, pour identifier les menaces sur le réseau et les postes de travail.
Suricata détecte et prévient les intrusions (IDS/IPS) réseau ; Zeek identifie des comportements inhabituels ou malveillants.

PRÉPARATION ET ALERTE

Flowintel ou **DFIR-RIS**, pour gérer les cas et répondre aux incidents.
Flowintel ou DFIR-RIS permettent aux analystes de suivre les investigations et de collaborer entre elles et eux.

VEILLE *(THREAT INTELLIGENCE)*

MISP, pour enrichir la détection avec des informations sur les menaces.
MISP donne des indicateurs de compromissions (IoC) et d'informations sur les menaces.

REPORTING

OpenSearch Dashboards, pour visualiser les données enregistrées.
OpenSearch Dashboards permet de construire des tableaux de bord clairs et dynamiques.

Le saviez-vous ?

L'outil *open-source* OpenSearch peut être utilisé en tant que SIEM.

Conditions préalables et points de vigilance

Bien que les outils *open-source* permettent de réduire les coûts, la mise en place d'un SOC ne s'improvise pas. Certaines conditions doivent être réunies pour garantir son efficacité.

- **Un minimum de ressources humaines** : des personnes formées à l'analyse de logs et à la gestion d'incidents sont indispensables.
- **Du temps** : la surveillance, la maintenance et la réponse nécessitent une présence régulière.
- **Un budget initial** : la mise en place d'une infrastructure (serveurs, stockage, réseau) et la montée en compétence nécessitent un investissement financier.
- **Une gouvernance claire** : les responsabilités et les processus décisionnels en cas d'incident doivent être définis.
- **Une stratégie de déploiement réaliste** : commencer petit, prioriser les systèmes critiques, et élargir progressivement en suivant un plan structuré.

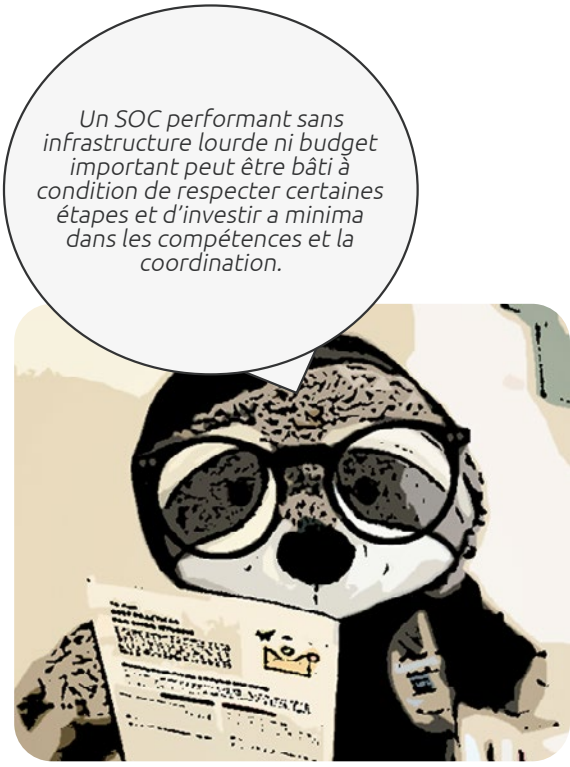
Attention aux pièges classiques !

- Vouloir tout surveiller dès le départ.
- Sous-estimer la charge d'analyse quotidienne.
- Négliger la formation des analystes et l'entretien des règles de détection.

Un SOC, même "à moindre coût", reste un projet structurant qui doit s'inscrire dans la durée et s'appuyer sur un minimum de moyens humains et financiers.

Bonnes pratiques à petit budget

1. **Automatisez** les tâches répétitives (alertes, corrélation, reporting).
2. **Concentrez-vous** sur vos actifs critiques avant d'élargir le périmètre.
3. **Capitalisez** sur la communauté *open-source* pour les modèles de détection et la veille.
4. **Documentez** chaque incident pour améliorer les processus.
5. **Formez et sensibilisez** les utilisateurs et utilisatrices de votre réseau, la sécurité commence par elles et eux.



Conseil !

Une architecture *open-source* cohérente constitue une chaîne complète de détection et de corrélation, performante et à faible coût. Ces défis nécessitent d'être relevés grâce à des solutions adaptées incluant des mécanismes de supervision robustes, des formations sur les meilleures pratiques, un investissement dans des outils d'analyse conviviaux, des méthodes de sécurisation des données et un plan de continuité d'activité complet.

À (RE)DÉCOUVRIR DANS LA MÊME SÉRIE...

- 'Choisir son mot de passe avec soin'
- 'Les messages spam & phishing'
- 'D'une cyberattaque à la saisie des données'
- 'Les attaques d'ingénierie sociale'
- 'Sauvegarder ses données sans risque'
- 'Les bonnes pratiques d'hygiène e-mail'

LU ET APPROUVÉ PAR HEX

Offre de services

Restena a conçu et mis en place un SOC complet basé sur des outils *open-source* et animé par une équipe d'expert-e-s en cybersécurité dans le cadre du projet européen 'Enhancing Cybersecurity Services for the Luxembourgish Research and Education community' - LuCySe4RE destiné à améliorer la protection face aux risques de cybersécurité rencontrés par la communauté luxembourgeoise de la recherche et de l'éducation. Ajouté au portefeuille de services de Restena dans le courant de l'année 2026, le SOC sera mis à disposition de la communauté de l'éducation et de la recherche au Luxembourg. Cette dernière pourra alors bénéficier d'une surveillance continue de son système d'information, d'une détection et d'une réponse aux incidents centralisées, et d'un accompagnement par des spécialistes à coût maîtrisé.

Pour plus d'informations sur ce service, rendez-vous sur www.restena.lu

Co-funded by the European Union

Cette fiche-conseils est l'une des activités de sensibilisation mises en place dans le cadre du projet européen LuCySe4RE, financé par le programme Digital Europe de l'Union européenne (DIGITAL) dans le cadre de la convention de subvention n° 101127864.

restena
réseau · sécurité · .lu