Fiche savoirs : Le centre opérationnel de sécurité

Une organisation doit se protéger des menaces de cybersécurité en adoptant :

- une approche structurée, formalisée,
- avec des professionnels de la cybesécurité,
- dans des centres opérationnels de sécurité (SOC).

> SOC : Security Operations center

Les services du SOC peuvent être installés en interne, ou être détenus et exploités par un prestataire de sécurité.

Les principaux éléments d'un centre opérationnel de sécurité sont :

- les personnes,
- les processus mis en oeuvre,
- et les technologies utilisées.

Les rôles des personnes d'un SOC

les SOC attribuent les rôles des postes par niveau, en fonction de l'expertise et des responsabilités requises pour chacun d'eux.

Analyste des alertes de niveau 1

- professionnels qui **surveillent les alertes entrantes**,
- **vérifient** s'il s'agit effectivement d'un véritable incident
- **transmettent** des tickets au niveau 2, si nécessaire.

Gestionnaires des incidents de niveau 2

- professionnels chargés d'examiner en détail les incidents
- recommandent des mesures ou des actions correctives à prendre.

Chasseurs de menace de niveau 3

- professionnels qui possèdent des compétences poussées dans le domaine des réseaux, des terminaux, des renseignements sur les menaces et de l'ingénierie inverse des malwares.
- savent très bien tracer les processus des programmes malveillants pour évaluer leur impact et déterminer comment les éradiquer.
- s'impliquent également dans la chasse aux menaces potentielles et dans l'implémentation d'outils de détection des menaces.
- recherchent les cybermenaces présentes dans le réseau mais qui n'ont pas encore été détectées.

Responsable du centre opérationnel de sécurité (SOC)

- professionnel qui gère toutes les ressources du centre
- joue le rôle d'interlocuteur principal de l'entreprise ou du client.

Processus dans un centre opérationnel de sécurité niveau 1

- analyse des files d'attente d'alertes de sécurité, en général en utilisant un système de création de tickets pour sélectionner des alertes dans une file d'attente afin de les examiner.

> Le logiciel qui génère les alertes peut parfois déclencher de fausses alarmes, c'est pourquoi l'analyste de Cybersécurité doit vérifier qu'une alerte correspond réellement à un incident.

- Après la vérification, l'incident peut être transmis aux enquêteurs ou à d'autres équipes de sécurité, ou désigné comme une fausse alerte. Sinon, l'alerte peut être rejetée en tant que fausse alarme.
- Si un ticket ne peut pas être résolu, l'analyste de cybersécurité de niveau 1 le transmettra à un analyste de gestionnaires des

incidents de niveau 2 qui l'examinera plus en détail.
- Si l'analyste de gestionnaires des incidents de niveau 2 ne peut pas résoudre le ticket, il le transmettra à un analyste de niveau 3 qui dispose de connaissances plus poussées et de compétences en matière de détection de menaces.

Niveau 3

- Connaissances approfondies
- Chasse aux menaces
- Mesures préventives

Niveau 2

- Analyse approfondies
- Recommande des mesures de résolution

Niveau 1

- Surveille les incidents
- Crée des tickets d'incidents
- Protection de base contre les menaces

Les technologies dans un centre opérationnel de sécurité : SIEM

Un centre opérationnel de sécurité a besoin d'un système :

- de gestion des événements
- et des informations liés à la sécurité (SIEM) ou d'un système équivalent.

> SIEM : Security Information and Event Management

SIEM prend en compte toutes les données générées par :

- les pare-feu,
- les appliances réseau,
- les systèmes de détection d'intrusion (IDS) et d'autres périphériques.

Les systèmes SIEM :

- collectent et filtrent les données,
- détectent et classent les menaces,
- analysent et examinent les menaces.

Les systèmes SIEM peuvent également gérer les ressources nécessaires pour mettre en œuvre des mesures préventives et faire face aux menaces futures.

Les technologies d'un centre opérationnel de sécurité sont les suivantes :

- **Collecte** d'événements, corrélation et analyse
- **Surveillance** de la sécurité
- **Contrôle** de la sécurité
- **Gestion** des événements
- **Évaluation** des vulnérabilités
- **Suivi** des vulnérabilités
- **Informations* sur les menaces Les CERT : https://www.cert.ssi.gouv.fr/ ===== Automatisation de la réponse avec un SOAR ===== Un SIEM gère l'orchestration de la cybersécurité. L'automatisation de la réponse aux incidents de cybersécurité est le SOAR. SIEM et SOAR se complètent mutuellement.**

  > SOAR : security orchestration, automation, and response.

  Plateformes de sécurité SOAR : * Recueillir les données d'alarme de chaque composant du système. * Fournir des outils qui permettent de faire des recherches, d'évaluer et d'enquêter sur les cas. * Mettre l'accent sur l'intégration comme moyen d'automatiser les workflows complexes de réponse aux incidents qui permettent une intervention plus rapide et des stratégies de défense adaptatives. * Inclure des playbooks prédéfinis qui permettent une réponse automatique à des menaces spécifiques. Les

playbooks peuvent être lancés automatiquement selon des règles prédéfinies ou peuvent être déclenchés par le personnel de sécurité. SOAR met l'accent sur les outils d'intégration et l'automatisation des workflows SOC. Il orchestre de nombreux processus manuels tels que l'investigation des alertes de sécurité ne nécessitant une intervention humaine que lorsque cela est nécessaire. Cela permet au personnel de sécurité de traiter des questions plus urgentes et de plus haut niveau afin de remédier aux menaces. Les systèmes SIEM produisent nécessairement plus d'alertes que la plupart des équipes SecOps ne peuvent étudier de manière réaliste afin de capturer de manière conservatrice autant d'exploits potentiels que possible. SOAR traitera un grand nombre de ces alertes automatiquement et permettra au personnel de sécurité de se concentrer sur des exploits plus complexes et potentiellement dommageables. ===== Métrique SOC ===== Cinq métrique sont couramment utilisées comme métrique SOC : * Temps d'immobilisation - durée pendant laquelle les acteurs de menace ont accès à un réseau avant qu'ils ne soient détectés et que l'accès des acteurs de menace soit arrêté * **MTTD (Mean Time to Detect)** - le temps moyen nécessaire au personnel du SOC pour identifier les incidents de sécurité valides s'est produit sur le réseau. * **MTTR (Mean Time to Respond)** - le temps moyen nécessaire pour arrêter et corriger un incident de sécurité. * **MTTC (Mean Time to Contain)** - le temps nécessaire pour empêcher l'incident de causer d'autres dommages aux systèmes ou aux données. * **Temps de contrôle** - le temps nécessaire pour arrêter la propagation des logiciels malveillants sur le réseau.