CQP ANALYSTE SOC

Vous avez une bonne compréhension des motivations des cybercriminels ? Etes entrainé à traquer les intrusions dans les systèmes d'information ? Vous êtes rigoureux et méthodique ? La veille et le reporting ne vous font pas peur ? Vous pouvez envisager une carrière d'opérateur analyste SOC.

MÉTIER

L'opérateur analyste SOC a pour mission la surveillance du système d'information d'une entreprise au sens large afin de détecter toutes les activités suspectes ou malveillantes. Il intervient aussi en amont pour faire de la prévention.

Qu'est-ce qu'un SOC ?

Le SOC, pour **Security Operation Center**, désigne dans une entreprise l'équipe chargée d'assurer la sécurité de l'information. Le SOC est une plateforme qui permet de superviser et d'administrer la sécurité du système d'information au travers d'outils de collecte, de corrélation d'événements et d'intervention à distance.

Le Security Operations center, SOC, désigne dans une entreprise l'équipe en charge d'assurer la sécurité de l'information. Le SOC est une plateforme permettant la supervision et l'administration de la sécurité du système d'information au travers d'outils de collecte, de corrélation d'événements et d'intervention à distance.

Le **SIEM** (Security Information Event Management) est l'outil principal du SOC.

L'**objectif d'un SOC** est de **détecter**, **analyser** et **remédier aux incidents de cybersécurité** à l'aide de solutions technologiques et d'un ensemble de procédés et de démarches de sécurisation du système informatique dans son ensemble.

Le SOC veille à ce que les failles et incidents de sécurité soient identifiés, analysés, compris et contrôlés.

Concrètement, les SOC **surveillent et analysent l'activité sur les réseaux**, les serveurs, les terminaux, les bases de données, les applications, les sites Web et autres systèmes, à la recherche de comportements anormaux qui pourraient être le signe précurseur d'un incident ou d'un compromis en matière de sécurité.

Le SOC pour Security Operation Center est la cellule de sécurité du système d'information de l'entreprise.

L'organisation du SOC

L'organisation du SOC doit permettre de répondre à différentes missions. Le SOC s'organise, de façon classique, en **3 couches distinctes** :

- **Le niveau 1 (opérateurs)** relève les alertes et fait un premier diagnostic. C'est ici que l'opérateur analyste SOC intervient.
- **Le niveau 2 (analyste sécurité)** réalise l'analyse détaillée des alertes, communique vers les équipes concernées, accompagne le traitement des incidents et, dans quelques cas, peut mettre en place des remédiations.
- **Le niveau 3 (experts sécurité)** prend la relève du niveau 2 pour les analyses approfondies ou nécessitant une compétence pointue. En s'appuyant sur l'analyse de risques, le responsable du SOC va proposer et implémenter des uses-cases en s'appuyant notamment sur un catalogue de use-cases couvrant de nombreuses menaces. Si l'use-case n'est pas déjà présent dans le catalogue, il est chargé de le développer pour répondre au besoin spécifique.

Constituer un SOC présente l'avantage pour l'entreprise d'**assurer la surveillance continue de ses systèmes et données** et ainsi de pouvoir rester au fait des menaces qui pèsent sur son environnement.

MISSIONS DE L'OPÉRATEUR ANALYSTE SOC

Les SOC sont composés **d'analystes**, **d'ingénieurs en sécurité**, ainsi que de **managers** supervisant les opérations de sécurité. Les équipes SOC travaillent étroitement avec les équipes d'intervention afin de s'assurer que le problème de sécurité soit bien réglé une fois qu'il a été découvert.

L'opérateur analyste SOC **identifie, catégorise, analyse et qualifie les événements de sécurité en temps réel ou de manière asynchrone** sur la base de rapports d'analyse sur les menaces. Il contribue au traitement des incidents de sécurité avérés en support des équipes de réponse aux incidents de sécurité.

Lorsque le système est compromis par une intrusion, l'analyste SOC évalue les dommages subis et apporte son aide pour concevoir une solution technique afin de rétablir le service en coordination avec d'autres acteurs de l'entreprise (administrateurs informatiques, computer emergency response team/CSIRT).

CQP ANALYSTE SOC

Il s'assure du maintien à jour des dispositifs de supervision de la sécurité comme le SIEM (Software Information Event Management), principal outil qui fait le lien en temps réel entre des événements et incidents pour en évaluer la dangerosité.

L'analyste SOC joue également un rôle en termes de prévention auprès des utilisateurs. Il veille au respect des bonnes pratiques et apporte ses conseils sur toutes les questions relatives à la sécurité.

Les missions quotidiennes de l'opérateur analyste SOC sont les suivantes.

Détection des menaces :

- Identifier les événements de sécurité en temps réel, les analyser et les qualifier
- Évaluer la gravité des incidents de sécurité
- Notifier les incidents de sécurité, escalader le cas échéant

Réaction face aux menaces :

- Transmettre les plans d'action aux entités en charge du traitement et apporter un support concernant les correctifs ou palliatifs à mettre en œuvre
- Faire des recommandations sur les mesures immédiates
- Accompagner le traitement des incidents par les équipes d'investigation

Mise en place des d'usages et des outils :

- Contribuer à la mise en place du service de détection (SIEM, etc.)
- Contribuer à la définition de la stratégie de collecte des journaux d'évènements
- Participer au développement et au maintien des règles de corrélation d'événements

Veille et amélioration :

- Collaborer à l'amélioration continue des procédures ; construire les procédures pour les nouveaux types d'incidents
- Contribuer à la veille permanente sur les menaces, les vulnérabilités et les méthodes d'attaques afin d'enrichir les règles de corrélation d'événements

Reporting et documentation :

- Renseigner les tableaux de bord rendant compte de l'activité opérationnelle
- Maintenir à jour la documentation
- Activités de recherche de compromissions (threat hunting)

En interne, l'opérateur analyste SOC travaille de concert avec l'analyste de.la menace de cybersécurité et le pentester. A l'externe, il sera très souvent en interaction directe avec les clients, prestataires, fournisseurs et la DSI client.

LES OUTILS DE L'OPÉRATEUR ANALYSTE SOC : LE SIEM

L'Agence Nationale de la Sécurité des Systèmes d'Information ou ANSSI recommande le recours à un SOC (Security Operating Center) dans le cadre d'une politique de sécurité renforcée. Un SOC s'appuie sur les technologies SIEM (Security Information and Event Management) afin de gérer les évènements du système d'information.

Le SIEM est une technologie spécifique qui permet d'analyser les menaces. Concrètement, le SIEM permet à une entreprise de centraliser toutes les informations de sécurité en un seul outil. Les données collectées auprès des logiciels antivirus, des pares-feux, des serveurs, des protections anti-theft ou encore des systèmes d'exploitation en tout genre seront analysées dans un même outil, ne laissant place au hasard. Une telle technologie permet aux équipes de cybersécurité de surveiller et de traiter plus facilement en temps réel les problèmes concernant l'infrastructure IT.

Les produits SIEM améliorent l'efficacité et la précision lors de la détection et de la réponse aux menaces. Sans solution SIEM, l'opérateur analyste SOC aura la tâche impossible de parcourir des millions de données cloisonnées et impossible à comparer.

Le choix de la solution SIEM au sein d'une organisation sera fonction des besoins de l'entreprise. Plusieurs aspects doivent être pris en compte au moment du choix de la technologie SIEM afin de se doter de l'outil le plus adapté pour sa propre structure.

L'opérateur analyste SOC et les équipes cybersécurité devront notamment hiérarchiser les sources de données et choisir un éditeur SIEM prenant en charge toutes les applications utilisées par l'entreprise.

COMPÉTENCES

Pour exercer en qualité d'opérateur analyste SOC, il est indispensable de posséder un socle de compétences informatiques solides orientées cybersécurité. Il est également nécessaire de connaître le cadre réglementaire relatif à la sécurité informatique :

- Sécurité des systèmes d'exploitation
- Sécurité des réseaux et protocoles
- Cyberdéfense : pratique de l'analyse de journaux (systèmes ou applicatifs)
- Cyberdéfense : pratique de l'analyse de flux réseaux
- Cyberdéfense : connaissance d'outils et de méthodes de corrélation de journaux d'événements (SIEM)
- Cyberdéfense : connaissances des solutions de supervision sécurité
- Cyberdéfense : connaissance des techniques d'attaques et d'intrusions
- Cyberdéfense : connaissances des vulnérabilités des environnements
- Scripting

QUALITÉS

- Capacité à travailler en équipe
- Capacité à définir des procédures
- Autonomie et organisation
- Capacité d'analyse et de synthèse
- Rigueur, sens de la méthode
- Qualité rédactionnelle
- Communication et expression orale