Sécurité - Le SOC et ses composantes

Difficulté : Novice

Notions : Cybersécurité, organisation, réponses aux incidents.

I. Introduction

Au fur et à mesure de l'avancée des technologies, les services informatiques sont devenus plus performants, rapide et automatisés. Aussi, cela a contribué à déplacer le terrain de la cyber-sécurité.

Le danger étant de moins en moins porté sur le vol ou l'accès direct au matériel ou au données, mais ciblant préférenciellement les échanges immatériels et les interconnexions.

De plus, le focus sur la productivité fait qu'il deviens ardu voire impossible sur les grands parcs de suivre l'intégralité des activités en lignes et ainsi de prévenir efficacement la menace. Là où à contrario, la découverte et l'exploitation de nouvelles vulnérabilités accélère drastiquement.

> **Info :** Avec l'arrivée de l'intelligence artificielle, cela change la donne pour les deux camps (attaquants et défenseurs).

Aussi, les approches traditionnelles de la cyber-sécurité sont aujourd'hui en grande partie dépassées et il deviens crucial pour les organisations de disposer d'équipes et de services dédiés à la cybersécurité.

C'est ici q'entre en jeu le ***SOC*** (**S**ecurity **O**perations **C**enter) ou en français : Centre des opérations de sécurité.

Le SOC est une équipe ou une entreprise dédiée gérant plusieurs clients. Son but est de se concentrer sur la surveillance et l'analyse des ressources et réseaux d'une entreprise afin de détecter les incidents et d'y apporter une réponse le plus rapidement possible.

Généralement, cette équipe est en service en 24/7.

II. Les missions du SOC

Les deux principales missions de la '***SOC team***' sont :

- La détection des incidents
- La réponse aux incidents

Cette équipe s'appuiera pour cela sur un ensemble de solutions logicielles, matérielles et de process qui l'aideront dans ses missions.

En effet, pour pouvoir répondre efficacement aux incidents, il faut déjà les voir.

2.1 Détection

Cette mission vise quatre axes principaux.

2.1.1 La détection des vulnérabilités

Une vulnérabilité ou une faille est une faiblesse qu'un attaquant peut exploiter pour effectuer des actions non autorisées au delà de ses privilèges normaux.

Elles permettent le plus généralement trois choses :

- Injection d'un code malveillant
- Escalade de privilège
- Accès non autorisé à une donnée ou un système

Ces vulnérabilités peuvent être introduite par un mauvais comportement utilisateur, un non respect des bonnes pratiques, ou simplement (car l'erreur est humaine) par le développeur du système ou logiciel lors de sa conception ou de son évolution.

> **Conseil** : C'est pour cela qu'il est important de s'assurer d'avoir toujours les derniers niveaux de correctifs pour ses systèmes et logiciels. En effet, la plupart du temps, ces failles sont assez vites découvertes et corrigées. Mais la non application de ces correctifs signifie que celle-ci est connue et exploitable en l'état.

2.1.2 La détection des activités non autorisées

Au delà de l'exploitation de failles logicielles, il peut s'agir d'une tentative d'exploitation de faille humaine.

Un utilisateur qui choisis un mot de passe faible ou présent dans un dictionnaire, un mot de passe compromis ou accessible d'une manière où d'une autre...

Mais pour autant, il n'est pas possible de surveiller humainement chaque collaborateur individuellement. Aussi il est important de disposer d'outils permettant de tracer ces activités et de différencier efficacement les activités potentiellement légitimes, des activités suspectes.

2.1.3 La détection des activités non autorisées

Par définition, une stratégie de sécurité et les bonnes pratiques associées sont un ensemble de règles permettant de minimiser les risques et de se protéger contres des menaces, mais aussi de veiller à la conformité des données.

Ce qui peut être considéré comme une violation varie d'une organisation à une autre et dépends des mesures mises en place.

Mais il peut s'agir par exemple de ne pas respecter une procédure sur la transmissions de données à l'extérieur de l'entreprise via un canal chiffré spécifique, ou un accès à un site web non autorisé qui contiendrai des éléments potentiellement dangereux.

2.1.4 La détection des intrusions

Et évidement, si toutes les mesures ci-dessus n'ont pas été suffisante et qu'une intrusion à quand même eu lieu. Il est crucial de la détecter le plus rapidement possible afin d'en limiter la portée et les dommages.

2.2 Réponse

Cette mission vise à répondre à un incident détecté et classé comme avéré. Elle va se traduire dans les faits par des actions pour endiguer l'intrusion, en minimiser les impact.

Réaliser une ***RCA*** (**R**oot **C**ause **A**nalysis) ou en français, Analyse de la cause racine. Soit l'analyse de l'élément ayant originellement permis l'incident.

La '***SOC team***' apportera également un soutien aux équipes opérationnelles en charges de la résolution de l'incident et de la procédure d'amélioration qui en suivra.

III. Les moyens du SOC

Afin de pouvoir mener à bien sa mission de réponse, la '***SOC team***' va s'appuyer sur 3 leviers d'actions

Ces Trois leviers sont :

- Les personnes
- Les process
- La technologie

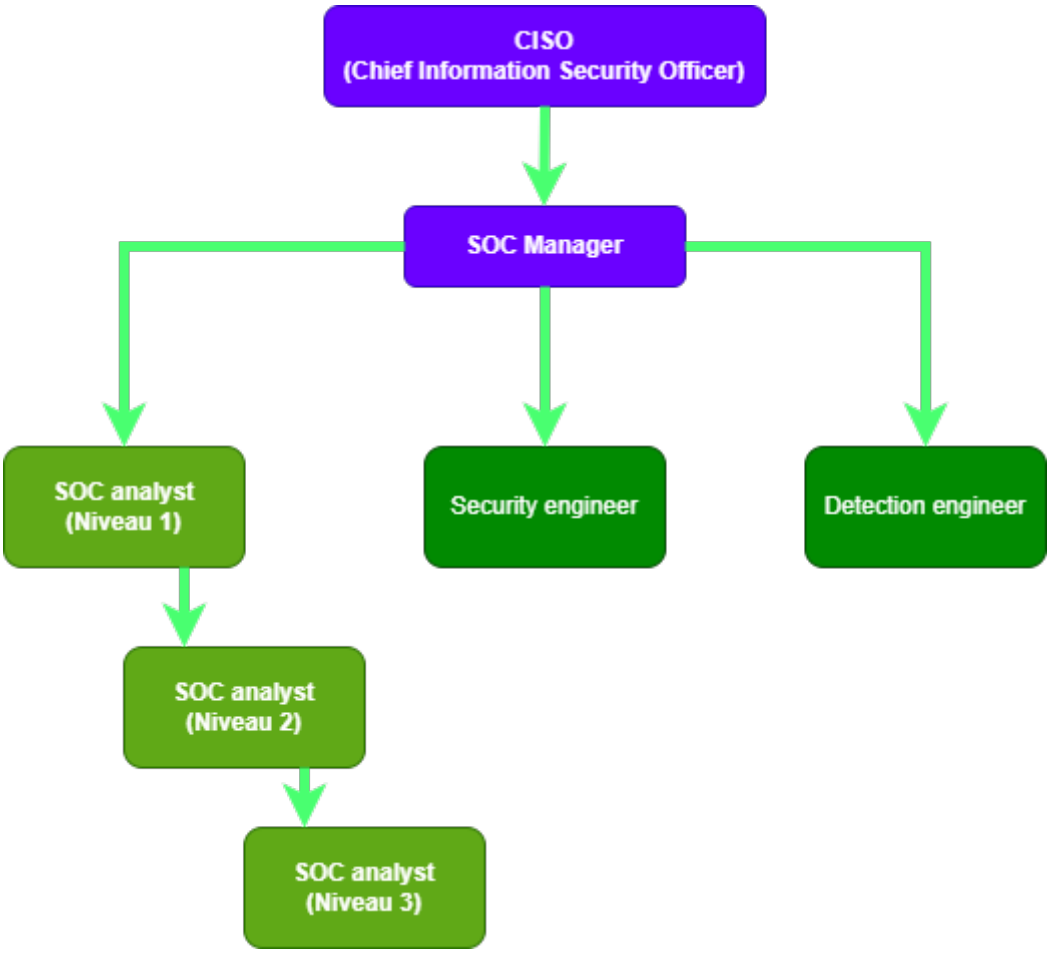
Utilisés ensembles, ils vont être les piliers de la maturité et de l'efficacité des activités de détection et de réponse.

Dans un environnement SOC, ces trois éléments co-existent.

Les personnes sont une équipe de professionnels travaillant ensemble à l'élaboration de processus aidés par des outils technologiques.

Peux importe l'état d'avancement de l'automatisation de la majorité des tâches cyber et des progrès effectués en matière d'intelligence artificielle, les personnes seront toujours indispensables au bon fonctionnement du SOC au vu des nombreux faux positifs engendrés par les outils. Il faudra toujours en effet trier de manière éclairée les vrais alertes des faux positifs et avoir un regard critique sur les différentes situation.

Une équipe SOC se constitue généralement de la façon suivante. Chacun ayant ses missions et responsabilités.



Le **SOC Analyst (N1)** : Ils sont les premiers maillons de la chaîne de détection et de réponse. Leur mission est de réceptionner les alertes sortant des solutions de sécurité et d'effectuer un premier tri afin d'éliminer tous les faux positifs. Leur devoir est également de faire remonter les informations concernant les vrais incidents et les faux positifs aux autres membres de l'équipe.

Le **SOC Analyst (N2)** : Malgré le dispatch effectué par le niveau 1, il se peut que certains incidents soient particulièrement difficiles à analyser ou répertorier correctement. Le niveau 2 va alors procéder à des investigations plus poussées, mettant entre autre ces éléments en relation avec d'autres afin d'affiner le diagnostic.

Le **SOC Analyst (N3)** : Il s'agit généralement d'analystes expérimentés qui ont un regard proactif sur les indicateurs et qui vont supporter la mission de réponse aux incidents. Leurs activités incluent donc la réponse détaillée aux incidents avec la mise en place d'actions comme :

- La quarantaine
- L'éradication de la menace
- Le rétablissement des données / du service

Le **Security Engineer** : Les 3 niveaux d'analystes ont besoin d'outils et de solutions permettant le bon déroulement et l'efficacité de leur missions. Le rôle de l'ingénieur en cyber-sécurité est donc de déployer et maintenir ces solutions afin de garantir la bonne exécution des missions.

Le **Detection Engineer** : Son rôle est de construire et d'affiner les règles de détections afin d'éliminer au maximum les faux positifs, de s'adapter aux nouvelles menaces et de permettre ainsi des temps de réactions plus rapides.

Le **SOC Manager** : Il est en charge des processus que la SOC team va suivre et en fournit un support. Il assure également le contact avec le CISO afin de lui transmettre les informations importantes comme les incidents repérés, évités, contenu ou résolus. Mais également le moral de l'équipe, etc...

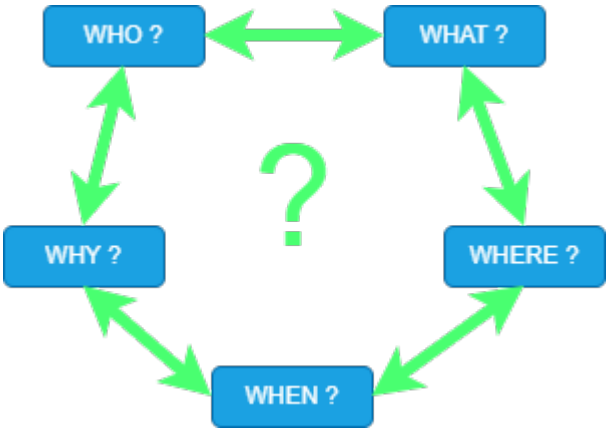
Le **CISO** : Il est le décisionnaire sur les processus à adopter, les politiques de sécurité et la garantie de la conformité du SI avec celles-ci.

IV. Le processus de gestion d'un incident

4.1 Le tri

Le tri des alertes est à la base du travail de la '***SOC team***'. Comme évoqué plus haut, ce tri se concentre sur le repérage des incidents réels et des faux positifs. Il s'agira également, dans le cas des incidents avérés, de déterminer la sévérité des alertes afin d'aider à leur priorisation.

Pour ce faire, il faut répondre à 5 questions. Appelées les '***5W***'.



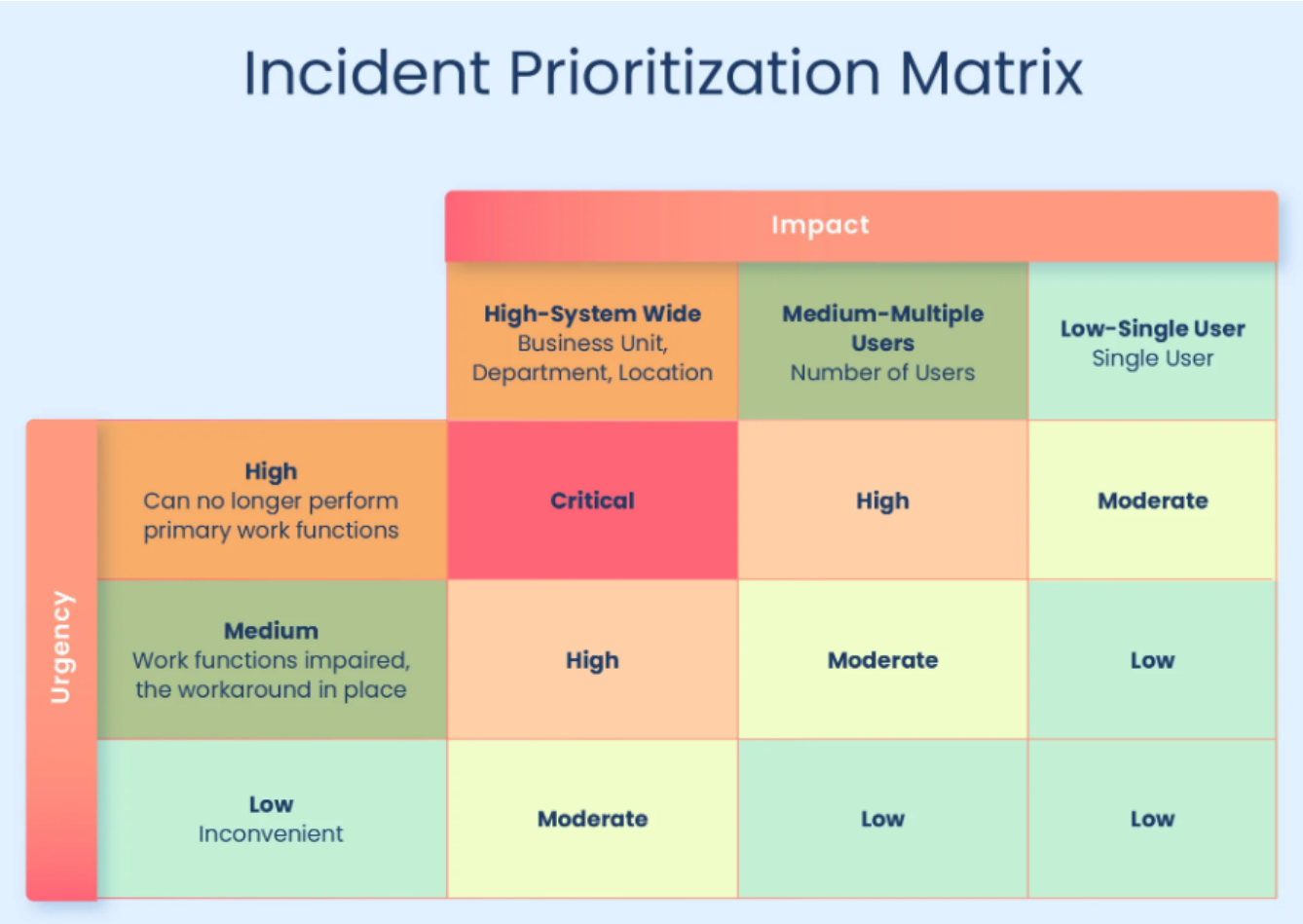
Par exemple :

Question	Réponse
What? (quoi?)	Un fichier malicieux à été détecté sur l'un des postes dans le réseau de l'entreprise.
When? (quand ?)	Le fichier a été détecté le 6 Juillet 2026 à 22h08.
Where? (où ?)	Le fichier a été détecté sur le PC "Cedric-PC".
Who? (qui ?)	Le fichier a été détecté pour l'utilisateur "Cedric".
Why? (Pourquoi ?)	Après analyse, il a été déterminé que le fichier malicieux avait été téléchargé depuis un site proposant au téléchargement du contenu piraté. Puis, suite à la concertation avec l'utilisateur, il s'est avéré que celui-ci voulait installé un logiciel de CAO en version piratée pour ne pas payer la licence.

4.2 Le reporting

Après la phase de tri et d'analyse, Il s'agit d'escalader l'incident au niveau d'analyste au dessus afin d’apporter une réponse appropriée.

Ces alertes sont remontées sous la forme de ticket classifiés en '***Incidents de sécurité***' puis qualifiés selon une matrice de priorisation.



Source : invgate

Avec la création du ticket, un rapport doit être fourni répondant aux '***5W***', avec si possible des screenshots, des extracts de fichiers de log. Tout ce qui pourra aider l'équipe d'investigation à remonter à la source de l'incident.

4.3 La réponse à l'incident et l'analyse forensic

Si la gravité ou l'impact de l'incident l'exige, il est primordial d'initier une action de réponse immédiate. Comme, par exemple, dans le cas de la détection d'une menace particulièrement grave ('trojan', 'backdoor potentiellement active', accès non autorisé en cours').

Soit celle-ci a déjà été définie dans le cadre de la méthode Ebios, soit il faut procéder à une réunion d'urgence afin de déterminer de la réponse à apporter.

Il peut également être nécessaire d'effectuer des analyses forensiques plus poussées. Notamment si la menace était présente mais en dormance. Auquel cas, il faudra examiner les traces de

l'attaque afin d'en déterminer le scénario et le point d'origine. Cela se fera en examinant les traces et les 'artefacts' laissés par la menace ou par le hacker.

V. Les outils

Un réseau d'entreprise est un enchevêtrement de devices interconnectés et d'applications plus ou moins exposées.

En tant qu'équipe de sécurité, il est essentiel d'avoir une visibilité sur l'ensemble des activités au sein de l'organisation.

Il est en effet impossible de répondre à une menace qui n'a pas été vue.

Le rôle des outils de sécurité est de centraliser cette information afin d'en rendre la gestion plus simple, d'automatiser les détections et éventuellement les réponses les plus simples. De plus, cela permettra également de pouvoir croiser plus facilement les informations, rendant ainsi les analyses plus pertinentes.

5.1 Le SIEM

Le premier outil indispensable est le ***SIEM*** (**S**ecurity **I**nformation and **E**vent **M**anagement) ou, en français 'Informations de sécurités et gestion d'événements'.

Il s'agit de l'outil indispensable de tout service SOC.

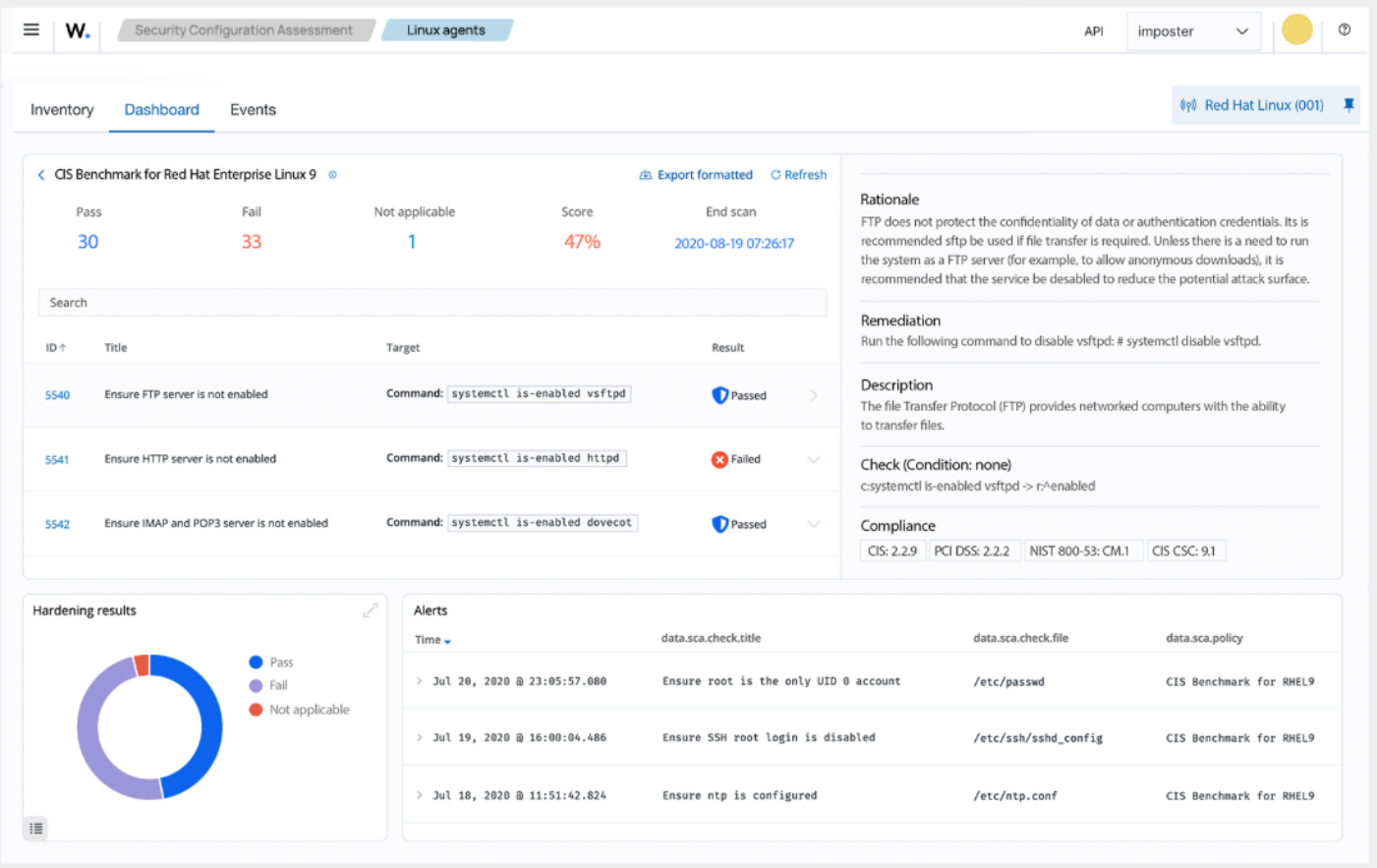
Il est en effet devenu impossible de suivre manuellement l'activité et les événements de l'ensemble des équipements du parc informatique individuellement. Il faut donc rassembler et centraliser ces informations afin d'en avoir une vision d'ensemble.

Le rôle principal du SIEM est donc de collecter ses journaux auprès des équipements (aussi appelé '***log sources***') à travers des agents par exemple.

La plupart des SIEM possèdent également des outils d'analyse automatique et d'alertes permettant de mettre rapidement en évidence des événements suspects. Cette mécanique s'appuie sur des jeux de règles qui seront mise en oeuvre et améliorées par les 'Detection Engineer'. Elles iront

croiser les sources, filtrer les entrées pertinentes et émettre une alerte si l'une des règle est vérifiée.

Les outils les plus avancés utilisent également de l'IA ou des algorithmes d'apprentissages afin d'apprendre et d'affiner cette capacité de détection et d'alerte.



Wazuh est un SIEM opensource

> **Info** : Le SIEM n'apporte en soi qu'une capacité de détection et d'alerte, mais ne gère pas lui-même la réponse à l'incident.

5.2 L'EDR/XDR

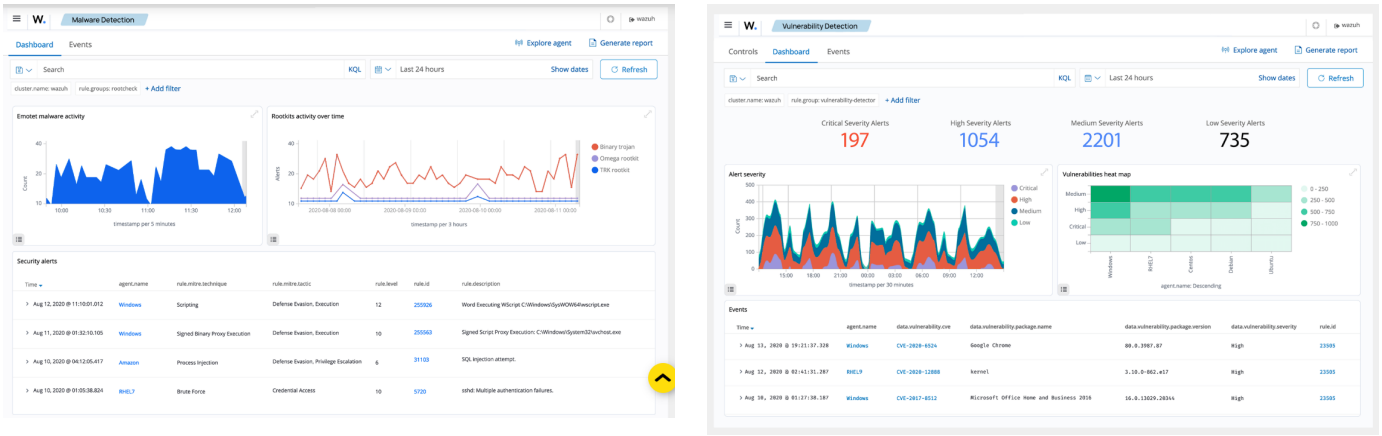
Le second outil utilisé par le SOC est l'***EDR*** ou ***XDR***.

l'EDR (**E**ndpoint **D**etection and **R**esponse) ou XDR (e**X**tended **D**etection and **R**esponse) sont des agents installés sur les équipements. Principalement les '***Endpoints***'.

Ces agents offrent au SOC la capacité de disposer des informations de chaque équipement connecté, d'un historique de celles-ci, mais également d'automatiser de manière proactive la réponse aux éventuels incidents qui se présenteraient sur le poste.

Notamment par le biais de surveillance heuristique en arrière plan.

Le XDR quand à lui dispose également de capacité de détections étendues.



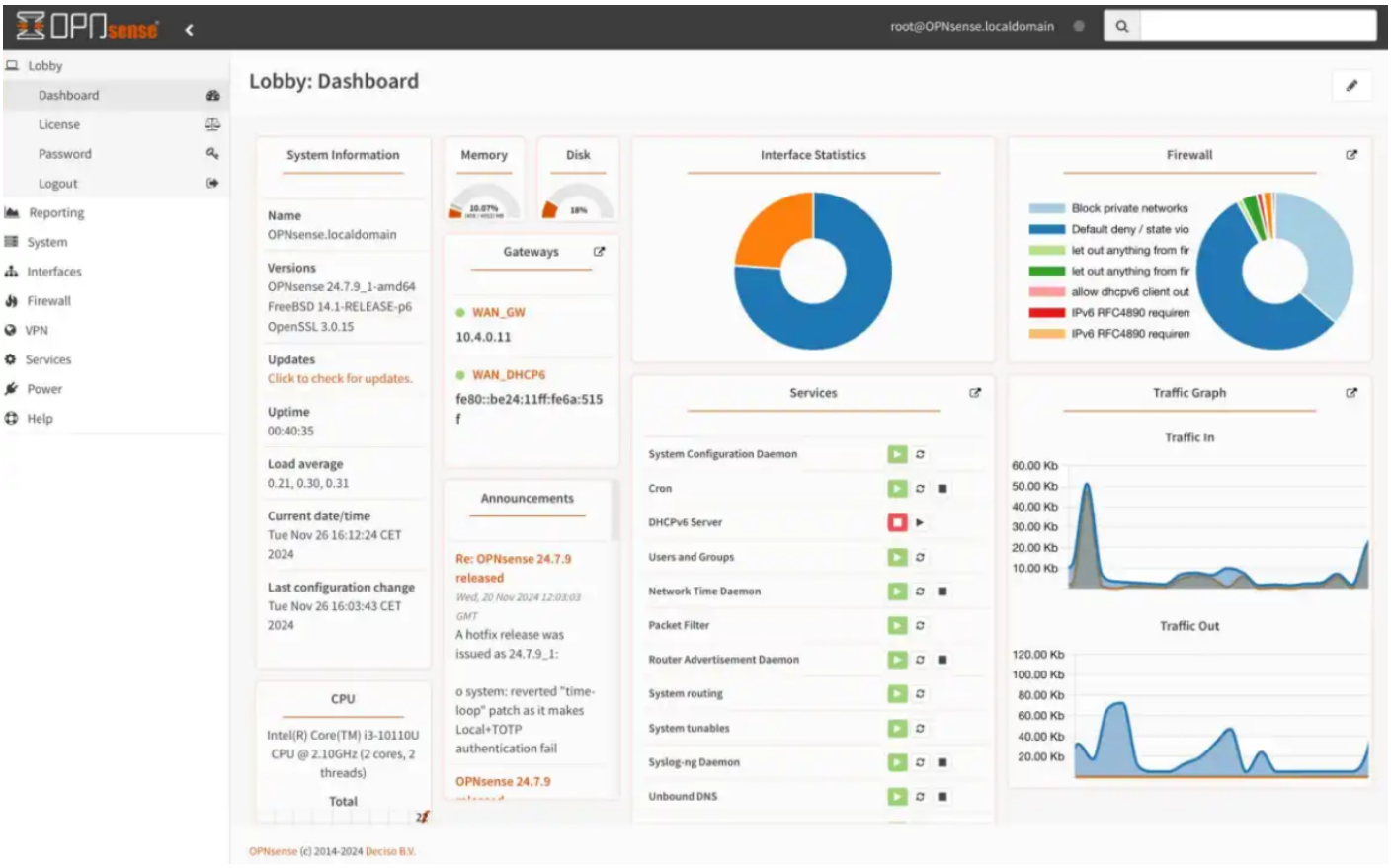
Wazuh comprends également des agents XDR pour les endpoints.

5.3 Le pare-feu

Il s'agit de la première ligne de défense. Qu'elle soit périphérique ou en profondeur.

Celui-ci génère effectivement les journaux qui permettrons d'anticiper le mieux, car ils voient les activités de scan et le trafic réseau potentiellement suspect. Mais cela reste une défense passive sur le principe.

C'est pour cela qu'il va être couplé avec le prochain outil.



OPNsense est un firewall opensource, fork de PFsense, en plus modernisé.

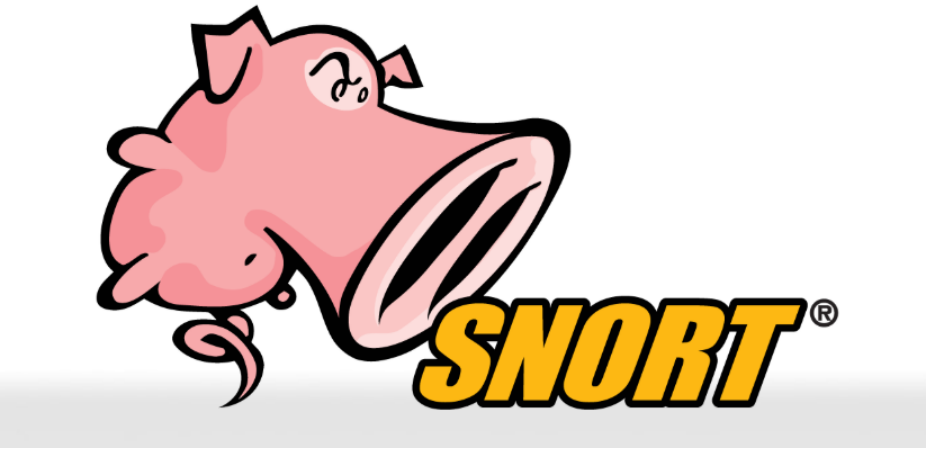
5.4 l'IDS / IPS

L'IDS / IPS (**I**ntrusion **D**etection **S**ystem / **I**ntrusion **P**revention **S**ystem) est un système de détection qui se base sur les règles de pare-feu pour repérer des pattern d'attaques ou de scan et lever des alertes. En mode IPS, en plus de lever l'alerte, il bloquera le trafic et blacklistera les IP qui en sont à l'origine.

Il faut toutefois faire attention aux réseaux sur lesquels l'IPS sera activé, car certain trafics sont, par nature, très proche d'un comportement d'attaque.

(*exemple : le trafic VoIP emet des trames en continu lors des communications. Ce qui peut laisser à penser à l'IPS qu'il s'agit d'une attaque DDoS. Alors qu'il s'agit en réalité de trafic légitime*)

Il peut être intéressant dans ces cas là, d'ajuster le comportement de l'IDS / IPS sur les flux continu.



Snort est un IDS/IPD avec un modèle community et une version payante. Il est nativement présent dans OPNSense

5.5 le WAF

Le WAF (**W**eb **A**pplication **F**irewall) ou pare-feu applicatif web est un système qui se place sur une reverse proxy afin d'intercepter les requêtes sur les flux http(s) et s'assure qu'elles ne contiennent pas d'éléments dangereux (payloads, requêtes forgées, etc...)

Exemple : Open Source Web Application Firewall | OWASP Coraza

---

VI. Conclusion

En conclusion, le SOC constitue aujourd'hui un élément essentiel de la cyber-sécurité moderne. Face à l'augmentation du volume d'alertes, à la complexité des menaces et à l'automatisation croissante des attaques, les organisations doivent s'appuyer sur des équipes capables de détecter, analyser et répondre efficacement aux incidents.

En combinant les compétences humaines, les processus structurés et les outils spécialisés vu ci-dessus, le SOC permet de réduire l'impact des attaques, d'améliorer la résilience du système

d’information et de renforcer la posture de sécurité globale de l’entreprise.
Comprendre son fonctionnement, ses missions et ses outils est donc une étape fondamentale pour tout professionnel souhaitant évoluer dans le domaine de la cyber-sécurité.

Revision #20
Created 2026-07-20 13:35:14 UTC by Olivier
Updated 2026-09-16 07:03:08 UTC by Olivier