La détection et de la réponse aux incidents

Les systèmes de sécurité de l'information sont conçus pour protéger la confidentialité, l'intégrité et la disponibilité des informations au sein d'une organisation
Ces systèmes utilisent diverses technologies, pratiques et politiques pour protéger les données sensibles contre tout accès, modification ou destruction non autorisés. Voici un aperçu de certains composants et concepts clés des systèmes de sécurité de l'information :

1**.-Contrôle d'accès** : les mécanismes de contrôle d'accès garantissent que seuls les individus ou les systèmes autorisés peuvent accéder à certaines ressources ou effectuer des actions spécifiques. Cela inclut l'authentification de l'utilisateur (par exemple, mots de passe, données biométriques), l'autorisation (définition des privilèges d'accès) et la responsabilité (suivi des actions de l'utilisateur).

2.-Pare-feu : les pare-feu agissent comme une barrière entre les réseaux internes et les réseaux externes (comme Internet). Ils surveillent et contrôlent le trafic réseau entrant et sortant en fonction de règles de sécurité prédéfinies, aidant à prévenir les accès non autorisés et les attaques réseau.

3.-Systèmes de détection d'intrusion (IDS) et systèmes de prévention d'intrusion (IPS) : les IDS surveillent le trafic réseau ou les journaux système pour détecter les activités suspectes ou les schémas d'attaque connus, tandis que les IPS vont plus loin en bloquant ou en atténuant activement les menaces détectées.

4.-Cryptage : Le cryptage est le processus de codage des informations d'une manière qui les rend illisibles pour les personnes non autorisées. Il assure la confidentialité des données en convertissant le texte brut en texte chiffré à l'aide d'algorithmes cryptographiques. Le cryptage est couramment utilisé pour sécuriser les communications (par exemple, SSL/TLS) et protéger les données stockées.

5.-Évaluation des vulnérabilités et tests d'intrusion : ces techniques consistent à identifier systématiquement les vulnérabilités des systèmes, des réseaux ou des applications afin d'évaluer leur état de sécurité. Les évaluations de vulnérabilité recherchent les faiblesses connues, tandis que les tests d'intrusion simulent des attaques réelles pour découvrir les vulnérabilités et les exploits potentiels.

6.-Gestion des informations et des événements de sécurité (SIEM) : les systèmes SIEM collectent, corrèlent et analysent les journaux d'événements de sécurité provenant de diverses sources sur le réseau d'une organisation. Ils aident à détecter les incidents de sécurité, permettent une surveillance en temps réel et prennent en charge la réponse aux incidents et les rapports de conformité.

7.-Politiques et procédures de sécurité : des politiques et des procédures de sécurité bien définies établissent des lignes directrices et des meilleures pratiques pour la sécurité de l'information au sein d'une organisation. Ils couvrent des domaines tels que la classification des données, le contrôle d'accès, la réponse aux incidents et l'utilisation acceptable des ressources.

8.-Sauvegarde et reprise après sinistre : les mécanismes de sauvegarde et de reprise après sinistre garantissent que les données critiques peuvent être restaurées en cas de perte de données ou de défaillance du système. Des sauvegardes régulières, un stockage hors site et des plans de récupération testés sont essentiels pour minimiser les temps d'arrêt et atténuer l'impact des interruptions.

9.-Sensibilisation et formation des utilisateurs : les facteurs humains jouent un rôle important dans la sécurité de l'information. Les programmes de sensibilisation des utilisateurs et la formation informent les employés sur les risques de sécurité, les meilleures pratiques et les politiques, réduisant ainsi la probabilité d'erreur humaine ou d'attaques d'ingénierie sociale.

10.-Conformité et normes réglementaires : les systèmes de sécurité de l'information doivent souvent se conformer aux réglementations spécifiques à l'industrie (par exemple, GDPR, HIPAA, PCI DSS) et suivre des cadres de sécurité reconnus (par exemple, ISO 27001) pour garantir la protection des données, la confidentialité et la conformité légale.

Il est important de noter que la sécurité de l'information est un domaine en constante évolution et que les organisations doivent adapter leurs systèmes et pratiques pour faire face aux menaces et vulnérabilités émergentes.

1 - Principes généraux

1 – 1 – Standards

Assurer la sécurité des systèmes d'information implique la mise en œuvre d'une variété de normes et de bonnes pratiques. Voici quelques normes utiles couramment utilisées pour améliorer la sécurité des systèmes d'information :

1. **ISO/IEC 27001** : Il s'agit d'une norme internationale largement reconnue pour les systèmes de gestion de la sécurité de l'information **(ISMS).** Il fournit une approche systématique de la gestion des informations sensibles de l'entreprise, y compris leur disponibilité, leur intégrité et leur confidentialité.
2. **NIST SP 800-53** : publiée par le National Institute of Standards and Technology (**NIST)**, cette publication fournit un catalogue complet des contrôles de sécurité et de confidentialité pour les systèmes d'information et les organisations fédérales. Il est largement adopté à la fois dans le secteur public et dans de nombreuses industries privées.
3. **Norme de sécurité des données** de l'industrie des cartes de paiement **(PCI DSS)** : développée par le Conseil des normes de sécurité de l'industrie des cartes de paiement (PCI SSC), cette norme est spécialement conçue pour

les organisations qui gèrent les transactions par carte de crédit. Il décrit les exigences relatives au traitement, au stockage et à la transmission sécurisés des données des titulaires de carte.

4. **Health Insurance Portability** and **Accountability Act** (**HIPAA**) : HIPAA est une réglementation américaine qui établit des normes de sécurité et de confidentialité pour les informations de santé protégées (PHI). Elle s'applique aux prestataires de soins de santé, aux plans de santé et aux autres entités impliquées dans le traitement de données médicales sensibles.

5. **Règlement général sur la protection des données (RGPD)** : le RGPD est un règlement de l'Union européenne (UE) qui vise à protéger la vie privée et les données personnelles des citoyens de l'UE. Elle impose des exigences strictes sur la manière dont les organisations collectent, traitent, stockent et transfèrent les données personnelles.

6. **Contrôles du Center for Internet Security (CIS)** : les contrôles CIS sont un ensemble de bonnes pratiques en matière de cybersécurité, développé par le Center for Internet Security. Ils fournissent un cadre hiérarchisé de mesures de sécurité conçues pour protéger les systèmes et les données critiques.

7. **Critères communs (ISO/IEC 15408) :** Les Critères communs sont une norme internationale pour évaluer et certifier la sécurité des produits informatiques. Il définit un cadre pour spécifier les exigences de sécurité et mener des évaluations pour déterminer leur conformité.

8. **National Institute of Standards and Technology Cybersecurity** Framework (**NIST CSF**) : le NIST CSF est un cadre volontaire qui fournit aux organisations des conseils sur la gestion et la réduction des risques de cybersécurité. Il offre une approche structurée pour évaluer et améliorer la posture de cybersécurité d'une organisation.

9. **Commission électrotechnique internationale (CEI) 62443** : cette norme se concentre spécifiquement sur la sécurité des systèmes d'automatisation et de contrôle industriels. Il fournit des lignes directrices pour sécuriser les infrastructures critiques et minimiser les vulnérabilités dans les environnements industriels.

10.-**Bibliothèque d'infrastructure des technologies de l'information (ITIL)** : Bien qu'il ne soit pas uniquement axé sur la sécurité, ITIL est un cadre largement adopté pour la gestion des services informatiques. Il comprend des conseils sur la gestion des incidents de sécurité, des vulnérabilités et des risques au sein d'un environnement informatique.

11 -**Le Statement on Standards for Attestation Engagements No. 16 (SSAE 16)** est un ensemble de normes d'audit et de conseils sur l'utilisation des normes, publié par l'Auditing Standards Board (**ASB**) de l'American Institute of Certified Public Accountants (**AICPA**), pour redéfinir et mettre à jour la façon dont les entreprises de services rendent compte des contrôles de conformité. La norme SSAE 16 a été publiée en avril 2010 en tant que norme de rapport pour tous les rapports des auditeurs de service et a été publiée pour remplacer la déclaration sur les normes d'audit n ° 70 (SAS 70). SSAE 16

a été remplacée par un ensemble mis à jour de normes d'audit, SSAE 18, le 1er mai 2017.

Ces normes, entre autres, fournissent des conseils précieux et des meilleures pratiques pour améliorer la sécurité des systèmes d'information. Les organisations doivent évaluer leurs exigences spécifiques et leurs obligations réglementaires afin de déterminer les normes les plus pertinentes pour leurs opérations.

1 – 2 – Organisation

Organiser la sécurité d'un système d'information dans une entreprise nécessite une approche globale et systématique. Voici quelques étapes clés pour vous aider à démarrer :

1. **Identifier les actifs** : Commencez par identifier les actifs critiques au sein de votre système d'information. Cela inclut le matériel, les logiciels, les données, les réseaux et tout autre composant essentiel aux opérations de votre entreprise.
2. **Évaluation des risques** : Effectuez une évaluation approfondie des risques pour identifier les vulnérabilités, les menaces et les risques potentiels associés à votre système d'information. Évaluez la probabilité et l'impact de chaque risque pour hiérarchiser vos efforts de sécurité.
3. Développer des politiques de sécurité : Créez des politiques et des procédures de sécurité complètes qui décrivent les règles et les lignes directrices pour la protection de votre système d'information. Ces politiques doivent couvrir des domaines tels que la classification des données, le contrôle d'accès, la gestion des mots de passe, la réponse aux incidents et les responsabilités des employés.
4. **Contrôle d'accès** : mettez en place des contrôles d'accès rigoureux pour vous assurer que seules les personnes autorisées ont accès aux données et ressources sensibles. Cela inclut l'utilisation de mots de passe forts, d'une authentification multifacteur et d'un contrôle d'accès basé sur les rôles (RBAC) pour limiter l'accès en fonction des rôles et des responsabilités du poste.
5. **Protection des données** : implémentez le cryptage et d'autres mécanismes de protection des données pour sécuriser les informations sensibles, à la fois en transit et au repos. Sauvegardez régulièrement les données critiques et stockez les sauvegardes dans des emplacements hors site sécurisés.
6. **Sécurité du réseau** : implémentez des pare-feu, des systèmes de détection d'intrusion (IDS) et des systèmes de prévention d'intrusion (IPS) pour protéger votre réseau contre les accès non autorisés et les activités malveillantes. Mettez à jour et corrigez régulièrement votre infrastructure et vos systèmes réseau pour remédier à toute vulnérabilité connue.
7. **Sensibilisation et formation des employés** : formez vos employés aux meilleures pratiques de sécurité, y compris l'utilisation sécurisée d'Internet, la reconnaissance des tentatives d'hameçonnage et le signalement des activités suspectes. Organisez régulièrement des programmes de sensibilisation à la

sécurité pour tenir vos employés informés des menaces émergentes et des protocoles de sécurité.

8. **Réponse aux incidents** : établissez un plan de réponse aux incidents qui décrit les mesures à prendre en cas d'incident ou de violation de la sécurité. Cela devrait inclure des procédures de confinement, d'enquête, de communication et de récupération.

9. **Audits et tests réguliers** : effectuez des audits de sécurité et des tests d'intrusion réguliers pour identifier les vulnérabilités et les faiblesses de votre système d'information. Résolvez rapidement tout problème identifié pour maintenir une posture de sécurité solide.

10.-**Surveillance et mises à jour continues** : mettez en place un système de surveillance continue de votre système d'information, y compris la journalisation et l'examen des journaux système pour les activités suspectes. Restez à jour avec les derniers correctifs et mises à jour de sécurité pour vos composants logiciels et matériels.

11.-Gestion des risques liés aux tiers : si vous travaillez avec des fournisseurs ou des partenaires externes, assurez-vous qu'ils adhèrent aux pratiques de sécurité adéquates. Établissez des directives et des exigences claires pour l'accès des tiers à votre système d'information et évaluez régulièrement leur conformité.

12.-Conformité et réglementation : Familiarisez-vous avec les réglementations sectorielles et les lois sur la protection des données qui s'appliquent à votre entreprise. Assurez-vous que vos mesures de sécurité sont alignées sur ces exigences et évaluez et corrigez régulièrement tout écart de conformité.

N'oubliez pas que la cybersécurité est un processus continu et qu'il est essentiel de revoir et de mettre à jour régulièrement vos mesures de sécurité pour vous adapter à l'évolution des menaces. Envisagez d'engager un professionnel ou une équipe qualifié(e) en cybersécurité pour vous aider à mettre en œuvre et à gérer efficacement la sécurité de votre système d'information.

1 – 3 – Les cybermenaces

Le paysage de la cybersécurité évolue et se développe rapidement. Au cours de la dernière décennie, les outils de détection et de réponse aux menaces se sont multipliés, chacun essayant de garder une longueur d'avance sur les dernières cybermenaces. Avec l'essor du travail à distance et le transfert d'un nombre croissant de fonctions commerciales vers le cloud, la détection et la réponse ne sont pas toujours des tâches simples, notamment parce que les violations catastrophiques peuvent provenir de n'importe où et à tout moment.

Dans cet environnement numérique à haut risque, il est essentiel d'apprendre à gérer les cybermenaces de façon cohérente et holistique. Les équipes de sécurité doivent s'appuyer sur une intégration plus poussée et une automatisation accrue pour garder une longueur d'avance sur les cybercriminels.

Les caractéristiques du paysage moderne des menaces sont les suivantes :

- Les acteurs malveillants investissent désormais un temps considérable à la collecte de renseignements en amont pour déterminer leur cible, la manière dont ils comptent la cibler et le moment optimal de leur attaque. Ce niveau de pré-planification rend les attaques plus sophistiquées et donc plus difficiles à intercepter.
- De plus en plus, les pirates informatiques travaillent en collaboration les uns avec les autres pour exploiter différents ensembles de compétences. Par exemple, une équipe dont l'expertise réside dans la mise en place d'un accès initial peut travailler avec une équipe spécialisée dans les mouvements latéraux. Cette équipe peut ensuite vendre l'accès à une autre équipe spécialisée dans les ransomwares, qui volera des données à des fins d'extorsion. Ce niveau de collaboration crée une complexité supplémentaire.
- Les cyberattaques touchent désormais de nombreuses zones du réseau. Par exemple, elles peuvent commencer sur le poste de travail d'un employé par un email de phishing ou une IP ouverte qui peut être compromise, mais après avoir rapidement cartographié le réseau, les pirates informatiques peuvent accéder aux centres de données, aux infrastructures cloud et aux réseaux de technologie opérationnelle (TO). La transformation numérique de nombreuses organisations, associée à la progression du travail à distance, se traduit par un élargissement de la surface d'attaque pour la plupart des entreprises.
- Les pirates informatiques sont devenus de plus en plus habiles à dissimuler leurs activités. Pour ce faire, ils réagissent par des contre-incidents afin de dissimuler leurs actions aux défenseurs, c'est-à-dire qu'ils utilisent des outils légitimes de manière malveillante pour masquer leurs traces.
- Les méthodes d'extorsion sont devenues plus élaborées : vol de données, attaques DDoS, ransomware et, dans les cas extrêmes, contact de vos clients pour faire pression sur vous afin que vous payiez leurs frais d'extorsion.
- Dans certaines organisations, l'infrastructure de sécurité peut être cloisonnée sur le réseau. Si les solutions de sécurité indépendantes ne sont pas intégrées, elles peuvent provoquer un trop grand nombre d'alertes sans contexte, submergeant les équipes de sécurité et réduisant leur visibilité sur l'ensemble de la surface d'attaque.

Comme les criminels utilisent des techniques plus avancées pour exploiter les contrôles de sécurité traditionnels, les organisations peuvent avoir du mal à sécuriser les ressources numériques vulnérables à l'intérieur et à l'extérieur du périmètre traditionnel du réseau. Les équipes de sécurité étant sous pression en raison du passage au travail à distance, la pression sur les ressources a été amplifiée. Les entreprises ont besoin de mesures de sécurité proactives et unifiées pour défendre leurs ressources technologiques, y compris les terminaux existants ainsi que les charges de travail mobiles, réseau et cloud, sans surcharger le personnel ni les ressources internes

1 – 4 – Moyens de l’entreprise

Assurer la sécurité des systèmes d'information est crucial pour toute entreprise afin de protéger les données sensibles, de maintenir la continuité des activités et de se prémunir contre les cybermenaces. Voici plusieurs moyens clés pour une entreprise d'améliorer la sécurité du système d'information :

1. **Implémentez des contrôles d'accès solides** : utilisez des mécanismes d'authentification robustes tels que l'authentification multifacteur (MFA) pour empêcher l'accès non autorisé aux systèmes. Utilisez des contrôles d'accès basés sur les rôles (RBAC) pour restreindre les privilèges en fonction des responsabilités professionnelles et implémentez des politiques de mots de passe solides.
2. **Mettez régulièrement à jour et corrigez les systèmes** : gardez tous les logiciels, systèmes d'exploitation et applications à jour avec les derniers correctifs et mises à jour de sécurité. Examinez et appliquez régulièrement des correctifs pour corriger les vulnérabilités connues et minimiser le risque d'exploitation.
3. **Utilisez des pare-feu et des systèmes de détection/prévention des intrusions** : Déployez des pare-feu réseau pour surveiller et filtrer le trafic entrant et sortant. Les systèmes de détection/prévention des intrusions (IDS/IPS) peuvent détecter et répondre aux attaques potentielles ou aux activités suspectes.
4. **Organisez une formation de sensibilisation à la sécurité** : formez les employés aux meilleures pratiques de sécurité, telles que la reconnaissance des e-mails de phishing, l'utilisation de mots de passe sécurisés et le signalement des activités suspectes. Renforcez régulièrement ces pratiques pour maintenir une culture soucieuse de la sécurité.
5. **Mettre en œuvre le chiffrement des données** : utilisez des techniques de chiffrement pour protéger les données sensibles, à la fois en transit et au repos. Cela inclut l'utilisation de protocoles sécurisés (par exemple, HTTPS) pour la communication Web et le cryptage des bases de données, des fichiers et des périphériques de stockage.
6. **Sauvegardez régulièrement les données** : Maintenez des sauvegardes régulières des données critiques pour garantir leur disponibilité et leur intégrité. Stockez les sauvegardes en toute sécurité et testez le processus de restauration pour vous assurer de leur efficacité.
7. **Effectuer des évaluations de vulnérabilité et des tests d'intrusion** : effectuer des évaluations régulières pour identifier les vulnérabilités au sein des systèmes d'information. De plus, effectuez des tests de pénétration pour simuler des attaques réelles et identifier les faiblesses potentielles.
8. **Surveiller et analyser les journaux système** : implémentez un mécanisme de journalisation complet pour enregistrer les activités du système. Examinez et analysez régulièrement les journaux pour détecter les anomalies, identifier les incidents de sécurité potentiels et réagir rapidement.

9. **Établir des procédures de réponse aux incidents** : Élaborez un plan de réponse aux incidents qui décrit les étapes à suivre en cas de violation ou d'incident de sécurité. Définissez les rôles et les responsabilités et effectuez des exercices périodiques pour tester l'efficacité du plan.

10.-**Utilisez la segmentation du réseau** : segmentez les réseaux en sous-réseaux plus petits et isolés pour contenir l'impact d'une faille de sécurité. Cela aide à prévenir les mouvements latéraux des attaquants et minimise les dommages potentiels.

11.-**Engagez des services de sécurité tiers** : envisagez de tirer parti d'une expertise externe en matière de sécurité, comme l'embauche de testeurs d'intrusion ou l'engagement de fournisseurs de services de sécurité gérés (MSSP), pour compléter les efforts de sécurité internes et acquérir des connaissances spécialisées.

12.-**Auditez et surveillez régulièrement la conformité** : effectuez des audits internes pour garantir la conformité aux réglementations et aux normes de l'industrie en vigueur. Surveillez les modifications des lois et réglementations et adaptez les mesures de sécurité en conséquence.

N'oubliez pas que la sécurité est un processus continu et qu'elle nécessite une surveillance, une adaptation et une amélioration continues pour suivre les menaces émergentes et l'évolution des technologies.

1 – 5 – outils et technologies disponibles

Il existe plusieurs outils et technologies disponibles pour assurer la sécurité des systèmes d'information. Voici quelques-uns des plus courants :

1. **Pare-feu** : les pares-feux sont des dispositifs de sécurité réseau qui surveillent et contrôlent le trafic réseau entrant et sortant. Ils agissent comme une barrière entre les réseaux internes et externes, ne laissant passer que le trafic autorisé et bloquant les menaces potentielles.

2. **Systèmes de détection d'intrusion (IDS)** : les outils IDS surveillent le trafic réseau et identifient les activités suspectes ou non autorisées. Ils analysent les paquets réseau et les comparent aux signatures d'attaque connues ou aux modèles de comportement anormaux, alertant les administrateurs des failles de sécurité potentielles.

3. **Systèmes de prévention des intrusions (IPS)** : les outils IPS sont similaires à l'IDS, mais ont également la capacité de répondre activement aux menaces détectées. Ils peuvent automatiquement bloquer ou atténuer les attaques en reconfigurant les pare-feu ou en appliquant des règles de contrôle d'accès.

4. **Logiciel antivirus** : le logiciel antivirus est conçu pour détecter, prévenir et supprimer les logiciels malveillants, tels que les virus, les vers et les chevaux de Troie. Il analyse les fichiers et les activités du système à la recherche de modèles malveillants connus, et certaines solutions antivirus avancées utilisent la détection basée sur le comportement pour identifier les menaces jusque-là inconnues.

5. **Certificats SSL/TLS (Secure Sockets Layer/Transport Layer Security)** : les certificats SSL/TLS sont utilisés pour établir des connexions cryptées sécurisées entre les clients et les serveurs sur Internet. Ils garantissent que les données transmises entre les deux parties sont cryptées et protégées contre les écoutes clandestines ou la falsification.
6. **Réseaux privés virtuels (VPN)** : les VPN fournissent un accès à distance sécurisé aux réseaux privés sur l'Internet public. Ils créent un tunnel crypté entre l'appareil de l'utilisateur et le réseau, garantissant la confidentialité et l'intégrité des données transmises.
7. **Outils de chiffrement** : les outils de chiffrement sont utilisés pour coder les données d'une manière qui ne peut être décodée qu'avec une clé ou un mot de passe spécifique. Ils protègent les données au repos (données stockées) et les données en transit (données transmises entre systèmes ou sur des réseaux).
8. **Systèmes de gestion des informations et des événements de sécurité (SIEM) :** les systèmes SIEM collectent et analysent les données des journaux à partir de diverses sources au sein d'un système d'information. Ils aident à identifier les incidents de sécurité, à détecter les anomalies et fournissent des capacités de surveillance et de création de rapports en temps réel.
9. **Scanners de vulnérabilité** : les scanners de vulnérabilité analysent les réseaux, les systèmes ou les applications à la recherche de vulnérabilités de sécurité connues. Ils aident à identifier les faiblesses qui peuvent être exploitées par des attaquants, permettant aux organisations de remédier de manière proactive à ces vulnérabilités.
10. **Authentification à deux facteurs (2FA)** : 2FA ajoute une couche de sécurité supplémentaire au processus d'authentification en demandant aux utilisateurs de fournir deux types d'identification différents. Cela peut inclure une combinaison de quelque chose que l'utilisateur connaît (mot de passe), quelque chose que l'utilisateur possède (smartphone ou jeton) ou quelque chose que l'utilisateur est (données biométriques).

Ce ne sont là que quelques-uns des outils disponibles pour renforcer la sécurité des systèmes d'information. Les outils et technologies spécifiques utilisés peuvent varier en fonction des exigences de l'organisation, de l'industrie et du niveau de sécurité requis. Il est important de mettre à jour et de maintenir régulièrement ces outils pour assurer des mesures de sécurité efficaces.

2 – Composants clés de l’infrastructure de sécurité

2 – 1 – SOC et SIEM : Quelles différences ?

Le **SOC** (Security Operations Center) et le **SIEM** (Security Information and Event Management) sont tous deux des composants clés de l'infrastructure de cybersécurité d'une organisation, mais ils ont des objectifs différents et ont des fonctionnalités distinctes. Voici un aperçu des différences entre SOC et SIEM :

1. **Fonction et objectif** :

• SOC : un centre d'opérations de sécurité est une équipe ou un service responsable de la surveillance, de la détection et de la réponse aux incidents de sécurité en temps réel. La fonction principale du SOC est de défendre activement les systèmes, les réseaux et les données de l'organisation contre les cybermenaces. Cela implique une combinaison de personnes, de processus et de technologies pour assurer la sécurité de l'organisation.
• SIEM : Security Information and Event Management est une solution ou une plate-forme technologique qui collecte et analyse des données d'événements de sécurité provenant de diverses sources au sein de l'infrastructure informatique d'une organisation. SIEM agrège et corrèle les données pour fournir une visibilité complète sur les événements de sécurité, aidant à identifier les modèles, détecter les anomalies et générer des alertes.

2. **Composants**:
   • SOC : un SOC se compose généralement d'une équipe d'analystes de la sécurité, d'intervenants en cas d'incident et d'autres professionnels de la cybersécurité qui travaillent ensemble pour surveiller les alertes de sécurité, enquêter sur les incidents potentiels, répondre aux menaces et assurer la sécurité globale de l'organisation. Ils utilisent divers outils, technologies et processus pour effectuer ces tâches efficacement.
   • SIEM : SIEM est une solution logicielle qui combine deux fonctionnalités principales : la gestion des informations de sécurité (**SIM**) et la gestion des événements de sécurité (**SEM**). SIM se concentre sur la collecte, le stockage et l'analyse des données des journaux de sécurité provenant de différentes sources, telles que les pare-feu, les systèmes de détection d'intrusion, les logiciels antivirus et les serveurs. SEM se concentre sur la corrélation d'événements en temps réel, les alertes et la génération de rapports basés sur les données de journal agrégées.
3. **Portée**:
   • SOC : un SOC est un concept plus large qui englobe les personnes, les processus et la technologie. Cela implique l'établissement de politiques de sécurité, de procédures de réponse aux incidents, d'une formation de sensibilisation à la sécurité et d'une surveillance et d'une analyse continues des événements de sécurité. L'équipe SOC est responsable de la gestion active et de l'atténuation des risques de sécurité.
   • SIEM : SIEM est une solution technologique qui prend en charge les opérations SOC. Il fournit les outils et les capacités nécessaires pour collecter, stocker, analyser et corréler les données d'événements de sécurité. SIEM aide les analystes SOC à surveiller et à enquêter sur les événements de sécurité, à identifier les menaces potentielles et à répondre efficacement aux incidents.
4. **L'intégration**:

• SOC : le SOC intègre diverses technologies de sécurité, telles que des systèmes de détection et de prévention des intrusions, des pares-feux, la protection des terminaux, des outils de gestion des vulnérabilités, etc. Il exploite ces technologies pour surveiller et défendre l'infrastructure informatique de l'organisation.

• SIEM : SIEM s'intègre à plusieurs outils et systèmes de sécurité au sein de l'organisation, y compris les périphériques réseau, les serveurs, les bases de données, les Appliance de sécurité, etc. Il collecte et regroupe les journaux d'événements de ces sources pour fournir une vue centralisée du paysage de la sécurité.

En résumé, SOC fait référence à une équipe ou à un département responsable de la gestion active des incidents de sécurité, tandis que SIEM est une plate-forme technologique qui aide à collecter, analyser et corréler les données des événements de sécurité. Le SOC et le SIEM travaillent ensemble, le SOC utilisant le SIEM comme un outil essentiel pour la surveillance, la détection et la réponse aux incidents

2 – 2 – Description du SOC

2 – 2 – 1 – le SOC de base

SOC signifie Security Operations Center. Il s'agit d'une unité centralisée au sein d'une organisation qui est responsable de la surveillance, de la détection et de la réponse aux incidents et menaces de cybersécurité. L'objectif principal d'un SOC est d'assurer la sécurité des systèmes d'information d'une organisation et de les protéger contre les accès non autorisés, les violations de données et autres activités malveillantes.

Le SOC fonctionne comme une installation 24 heures sur 24, 7 jours sur 7 et emploie une combinaison de technologies, de processus et de professionnels qualifiés en cybersécurité pour s'acquitter efficacement de ses fonctions. La structure et la configuration spécifiques d'un SOC peuvent varier en fonction de la taille et de la complexité de l'organisation, mais elles comprennent généralement les composants suivants :

1. **Surveillance** : le SOC surveille en permanence les réseaux, les systèmes, les applications et les autres actifs numériques de l'organisation à la recherche de signes d'incidents ou d'anomalies de sécurité potentiels. Cela implique la collecte et l'analyse des journaux de sécurité, des données d'événements, du trafic réseau et d'autres informations pertinentes.
2. **Détection et réponse aux incidents** : lorsqu'un incident de sécurité potentiel est détecté, le SOC lance une enquête pour déterminer la nature et l'étendue de l'incident. Les analystes de la sécurité utilisent divers outils et techniques pour analyser les données disponibles et identifier toute activité malveillante ou violation. Une fois qu'un incident est confirmé, le SOC répond en contenant et en atténuant l'impact de l'incident, en prenant les mesures appropriées pour minimiser les dommages ou les pertes supplémentaires.

3. **Threat Intelligence** (renseignement sur les menaces): Le SOC tient à jour ses connaissances sur les dernières menaces, vulnérabilités et techniques d'attaque en matière de cybersécurité. Cela implique la collecte d'informations auprès de sources externes, telles que les fournisseurs de sécurité, les flux de renseignements sur les menaces et les forums de l'industrie, ainsi que l'analyse des données internes sur les incidents. Les renseignements recueillis aident à identifier de manière proactive les menaces potentielles et à améliorer la sécurité globale de l'organisation.
4. **Signalement et documentation des incidents** : le SOC génère des rapports et conserve une documentation sur les incidents de sécurité, y compris les détails de l'incident, les mesures prises et les leçons apprises. Ces rapports sont essentiels pour les exigences de conformité, l'analyse post-incident et la prise de décision de la direction.
5. **Collaboration et communication** : le SOC collabore avec diverses équipes internes, telles que les informaticiens, les administrateurs réseau et les propriétaires d'applications, pour garantir la résolution rapide des incidents de sécurité. Il maintient également des canaux de communication avec des entités externes, telles que les forces de l'ordre et les organisations de cybersécurité, pour le signalement des incidents et le partage d'informations sur les menaces.
6. **Amélioration continue** : Le SOC s'efforce constamment d'améliorer son efficacité en procédant à des examens réguliers, en mettant à jour les processus et les procédures et en tirant parti des technologies émergentes. Cela comprend l'évaluation de nouveaux outils de sécurité, la mise en œuvre de capacités d'automatisation et d'orchestration, et l'amélioration des compétences et des connaissances du personnel du SOC grâce à des programmes de formation et de développement.

Dans l'ensemble, le SOC joue un rôle essentiel dans la protection des actifs numériques d'une organisation et dans le maintien d'une défense proactive contre les menaces de cybersécurité. En fournissant des capacités de surveillance, de détection des incidents et de réponse en temps réel, le SOC aide les organisations à identifier et à traiter rapidement les incidents de sécurité, en minimisant les dommages potentiels et les perturbations des opérations commerciales.

2 - 2 – 2 – Différents types de SOC

Il existe plusieurs types de SOC que l’on peut classifier en fonction de leur type d’implémentation technique et leur localisation

- ### SOC interne ou dédié

  Installé dans les locaux de l'entreprise, il fonctionne grâce à des équipes d'exploitation et des ressources IT internes ;

- **SOC externe**
  Localisé chez un prestataire de sécurité informatique (MSSP, Managed Security Service Provider), il est opéré grâce aux équipes informatiques de ce prestataire ;
- **SOC virtuel**
  Sans installations physiques propres, il est constitué par une équipe dont les membres agissent dès lors qu'un incident survient ou qu'une alerte est déclenchée ;
- **SOC hybride**
  Certaines tâches sont prises en charge par l'entreprise comme le support de niveau 3, c'est-à-dire la gestion des incidents bloquants, voire critiques qui pourraient éventuellement impacter la production.
  Les autres tâches sont gérées par des équipes externes notamment les analyses forensiques, réalisées après des incidents, et les opérations liées à la cyberguerre (ou Threat Intelligence) ;
- **SOC dans le Network Operation Center (NOC)**
  Le NOC inclut les tâches du SOC tout en **se chargeant aussi de maintenir le réseau**, de stocker, virtualiser et sauvegarder les données, etc.

- **SOC orienté cyberveille et IA (Intelligence Artificielle)**
  Aux fonctionnalités classiques du SOC, s'ajoute la Threat Intelligence (cyberveille). Son but est de compiler des informations sur les cyberattaques pour définir des tendances et créer des profils d'attaquants potentiels. Plusieurs outils interviennent dans la cyberveille parmi lesquels l'IA et l'apprentissage automatique (machine learning).

- **Le SOC-as-a-Service**

(SOCaaS)est un modèle de sécurité dans le cadre duquel un fournisseur tiers exploite et gère un SOC entièrement managé via le cloud, sur la base d'un abonnement.Le SOCaaS met à disposition toutes les fonctions de sécurité d'un SOC interne traditionnel : surveillance du réseau ; gestion des journaux ; détection des menaces et renseignements sur les cybermenaces ; investigations et réponse à incident ; création de rapports ; et risques et conformité. Le fournisseur endosse également la responsabilité de l'ensemble des personnes, des processus et des technologies requis pour activer ces services et assurer un support 24 h sur 24, 7 j sur 7.

2 – 2 – 3 – meilleurs acteurs de SOCaaS

- **PeerSpot** - https://www.peerspot.com/ Arctic Wolf Managed Detection and Response est la solution classée #1 dans les meilleurs **fournisseurs SOC as a Service** et #2 dans les **meilleurs outils de détection et de réponse gérés (MDR).**
- **NetSurion** _ https://www.netsurion.com

Netsurion® fournit une solution de sécurité gérée adaptative qui intègre notre plate-forme XDR à vos investissements de sécurité et à votre pile technologique existants, s'adaptant facilement aux besoins de votre entreprise. L'offre gérée de Netsurion comprend notre SOC 24h/24 et 7j/7 qui fonctionne comme votre partenaire de confiance en matière de cybersécurité, travaillant en étroite collaboration avec votre équipe informatique pour renforcer votre position en matière de cybersécurité

- **AlertLogic** – https://www.alertlogic.com
  L'aspect le plus précieux d'Alert Logic est sa plate-forme technologique. Ils ont des SOC aux États-Unis et en Europe, ce qui leur donne une visibilité mondiale du paysage des menaces. Ils détectent et répondent aux menaces en quelques minutes. Leur plus grande valeur est l'expertise humaine. Vous êtes attaqué par un humain, et vous ne pouvez pas y répondre à moins d'avoir un humain de l'autre côté. Ils ont les ressources humaines et technologiques pour réagir
- **Expel Workbench –** https://expel.com
  Expel Workbench élimine les silos sur une variété de surfaces technologiques et d'attaque pour obtenir des résultats mesurables, améliorer la sécurité globale et minimiser les risques commerciaux.
  À l'aide des données d'événement, des alertes et du contexte métier de votre environnement, Expel Workbench automatise la détection, la réponse et la correction sur toutes les surfaces d'attaque : cloud, sur site, SaaS, SIEM, Kubernetes, etc. Nous utilisons une combinaison de technologie et d'analystes de sécurité Expel hautement qualifiés pour l'aide à la décision afin de nous aider à donner un sens à la sécurité.Expel Workbench était auparavant connu sous le nom d'Expel SOC-as-a-Servi
- **CyberHat CYREBRO** – https://www.cyrebro.io
  CYREBRO a été fondée en 2012 sous le nom de CyberHat pour aider les entreprises à porter la cyberprotection à de nouveaux sommets sans précédent. Aujourd'hui, nous sommes devenus CYREBRO et avons pour mission de révolutionner complètement les opérations de cybersécurité en mettant la puissance d'un centre d'opérations de sécurité (SOC) à part entière entre les mains de n'importe quel utilisateur de n'importe quelle organisation. Notre équipe d'experts en cybersécurité de premier plan a développé la première plate-forme SOC-as-a-Service basée sur le cloud et indépendante de la technologie.
- **Cygilant SOC -** https://blog.cygilant.com/
  Cygilant est l'un des principaux fournisseurs de solutions de sécurité. Le solide portefeuille de sécurité de la société comprend diverses solutions, notamment MDR, la sécurité proactive et réactive et le SOC en tant que service. L'offre Cygilant SOC as a Service permet de faire face aux menaces grâce à un personnel de sécurité dédié 24 heures sur 24. L'offre réduit non seulement les risques liés aux informations sensibles, mais garantit également que les fournisseurs se conforment à diverses réglementations, notamment PCI DSS, GLBA, NIST, FFIEC SOX et

HIPAA. La société dispose d'une large base de partenaires qui comprend des acteurs majeurs de l'industrie, tels que Qualys, Rapid7 et Tenable. I

- **Delta Risk** - https://deltarisk.com/
  Delta Risk peut combler les lacunes de sécurité de votre organisation grâce à une Surveillance de votre réseau. Notre solution ActiveEye empêche les petites menaces de évoluant vers des incidents plus importants, et réduisant le temps nécessaire pour détecter, contenir, et éliminer les problèmes au fur et à mesure qu'ils se développent. Avec des années d'expérience dans la détection et la réponse aux incidents dans le monde
  réel, nous nous concentrons sur votre surveillance de la sécurité afin que vous peut se concentrer sur votre entreprise.
- **Profilio** - https://www.proficio.com/
  Proficio est un fournisseur de services de sécurité gérés (MSSP) de classe mondiale qui fournit des solutions de détection et de réponse gérées, une surveillance de la sécurité 24 heures sur 24, 7 jours sur 7 et des services avancés de prévention des violations de données aux organisations du monde entier. Notre croissance rapide est alimentée par l'essor des services basés sur le cloud, l'acceptation du modèle Software-as-a-Service (SaaS) et le nombre croissant d'attaques de cybersécurité contre les entreprises, les hôpitaux et le gouvernement. Nous avons développé des outils propriétaires de contenu de sécurité et de renseignement sur les menaces pour identifier et se défendre de manière proactive contre les attaques avancées et les menaces internes. Les fondateurs de Proficio sont des vétérans de l'industrie de la sécurité et des réseaux qui ont aidé à guider plusieurs entreprises vers des sorties réussies. Les clients de Proficio bénéficient de la surveillance de la sécurité la plus avancée et des services de sécurité gérés 24h/24 et 7j/7 qui, jusqu'à récemment, n'étaient pas dans le budget de toutes les entreprises, sauf les plus grandes.
- **Menlo security** – https://www.menlosecurity.com/
  La plate-forme d'isolation en nuage de Menlo Security empêche les logiciels malveillants d'atteindre les utilisateurs finaux. La plate-forme d'isolement de sécurité Menlo basée sur le cloud (MSIP) élimine la possibilité que des logiciels malveillants atteignent les machines des utilisateurs via des sites Web, des courriers électroniques ou des documents compromis ou malveillants. Ce n'est pas une détection ou une classification, mais plutôt la session Web de l'utilisateur et tout le contenu actif (par exemple, Flash), qu'il soit bon ou mauvais, est entièrement exécuté et contenu dans la plate-forme d'isolation de sécurité Menlo. Seules les informations de rendu sécurisées et exemptes de logiciels malveillants sont transmises au point de terminaison de l'utilisateur avec une expérience utilisateur totalement native.
- **blackStratus** - https://www.vertica.com/partner/blackstratus/
  Depuis 1999, BlackStratus fournit des produits et services fiables et innovants de gestion des événements d'information de sécurité (SIEM). Basés en partie sur nos nombreuses années d'expérience avec les principaux fournisseurs de services gérés (MSP) et entreprises du monde, nous sommes en mesure d'offrir les logiciels de gestion de la sécurité et de la conformité les plus évolués. Nous offrons également un support inégalé pour aider les MSP à développer de nouvelles activités de

sécurité en tant que service ou à améliorer leur activité actuelle de sécurité en tant que service.

- **AT&T SOC** - https://www.business.att.com/products/security-operations-center.html
- **MobileSOC -** application sur Google Play
- **Digital Hands SOC -** https://www.digitalhands.com/
- **Ebryx -** https://www.ebryx.com /
- **Ascend Technology -** https://teamascend.com/managed-security/soc-as-a-service/

2 – 3 – Rapports SOC

2 – 3 - 1 - Définition et importance des rapports SOC

Les rapports SOC (Service Organisation Controls), déclinés en SOC 1, SOC 2 et SOC 3, sont des cadres de référence établis par l'American Institute of Certified Public Accountants (AICPA) pour rendre compte des dispositifs de contrôle internes mis en place dans une entrepriseCes rapports sont essentiels pour contrôler les mesures de protection des données en place et s'assurer qu'elles remplissent leur rôle.

2 – 3 – 2 -Bonnes pratiques de sécurité avec les rapports SOC

Les rapports SOC sont plus importants que jamais en raison du cloud computing et de la nécessité pour un fournisseur de services de maintenir une relation de confiance avec ses clients. Dropbox communique constamment avec ses clients pour s'assurer que les meilleures mesures de sécurité ont été mises en place et qu'elles sont régulièrement et scrupuleusement vérifiées par un organisme tiers indépendant.

2 – 3 – 3 - Rapports SOC 1, SOC 2 et SOC 3

Évaluation par un organisme tiers indépendant
Dropbox fait valider ses systèmes, ses applications, son personnel et ses processus par Ernst & Young LLP, un cabinet d'audit indépendant qui vérifie que l'entreprise répond à des critères de sécurité, de confidentialité et de conformité très stricts.

Bonnes pratiques et normes objectives
Ce processus de certification confirme que Dropbox suit les bonnes pratiques et est conforme à des normes objectives concernant les rapports financiers, la sécurité, la confidentialité, la disponibilité et l'intégrité des traitements.

2 – 3 – 4 - SOC 3 pour la sécurité, la confidentialité, l'intégrité et la disponibilité

SOC 3 pour la sécurité, la confidentialité, l'intégrité et la disponibilité
Le rapport d'attestation SOC 3 couvre les grands principes des services de confiance : sécurité, disponibilité du système, intégrité des traitements et confidentialité (TSP, section 100). Ce rapport Dropbox généraliste est un résumé analytique du rapport SOC 2 qui inclut l'opinion de l'auditeur tiers indépendant concernant l'efficacité de nos dispositifs de contrôle, tant en termes de conception que de fonctionnement.

2 – 3 – 5 - SOC 2 pour la sécurité, la confidentialité, l'intégrité et la disponibilité

Le rapport SOC 2 atteste de l'efficacité de nos dispositifs de contrôle et couvre les grands principes des services de confiance portant sur la sécurité, la disponibilité du système, l'intégrité des traitements et la confidentialité (TSP section 100).

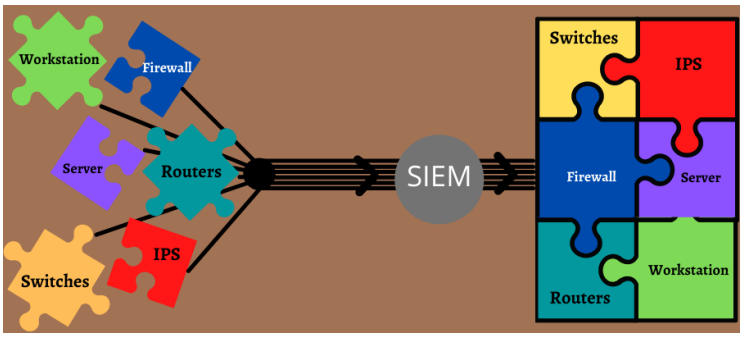
Il offre également une description détaillée des processus de Dropbox et des dispositifs de contrôle (plus d'une centaine) que nous avons mis en place pour protéger vos données. Outre l'avis de notre auditeur tiers indépendant sur l'efficacité de nos dispositifs de contrôle, tant du point de vue de la conception que du fonctionnement, ce rapport intègre également les procédures de test de cet auditeur et les résultats pour chaque contrôle.

2 – 3 – 6 - SOC 1/SSAE 18/ISAE 3402 (anciennement SSAE 16 ou SAS 70)

Le rapport SOC 1 offre des garanties spécifiques aux clients qui considèrent les produits comme indispensables à leurs contrôles internes sur l'établissement de rapports financiers (ICFR). Ces garanties sont principalement utilisées par nos clients pour se mettre en conformité avec la loi Sarbanes-Oxley (SOX).

L'audit réalisé par l'organisme tiers indépendant est mené en accord avec les normes SSAE 18 (Statement on Standards for Attestation Engagements n° 18) et ISAE 3402 (International Standard on Assurance Engagements n° 3402). Ces normes ont remplacé les normes SAS 70 (Statement on Auditing Standards n° 70) et SSAE 16 (Standards for Attestation Engagement n° 16) devenues obsolètes.

2 – 4 – description du SIEM
2 - 4 -1 - fonctionnalités



Une solution de gestion des informations et des événements de sécurité (SIEM) est un système complet qui permet aux organisations de collecter, d'analyser et de gérer les événements de sécurité et les journaux provenant de diverses sources au sein de leur infrastructure réseau. Les solutions SIEM sont conçues pour aider les organisations à identifier et à répondre aux incidents de sécurité, à surveiller et à gérer les événements liés à la sécurité et à se conformer aux exigences réglementaires

Voici un aperçu des composants et fonctionnalités clés d'une solution **SIEM typique :**

1. **Collecte de données** : les solutions SIEM collectent des données sur les événements de sécurité à partir d'un large éventail de sources, telles que des périphériques réseau, des serveurs, des pare-feu, des systèmes de détection d'intrusion (IDS), des logiciels antivirus, etc. Ces données sont collectées en temps réel ou quasi réel pour assurer une détection et une réponse rapides aux incidents de sécurité.
2. **Gestion des journaux** : les solutions SIEM stockent et gèrent les journaux de sécurité générés par les différentes sources mentionnées ci-dessus. Ces journaux contiennent des informations précieuses sur les activités du réseau, le comportement des utilisateurs, les événements système et les incidents de sécurité. Les fonctionnalités de gestion des journaux incluent des capacités d'agrégation, de stockage, d'indexation et de recherche de journaux pour faciliter une analyse efficace des données.
3. **Corrélation des événements** : les solutions SIEM analysent et corrèlent les événements de sécurité et les journaux provenant de plusieurs sources pour identifier les modèles, les anomalies et les menaces potentielles. En corrélant les événements sur différents systèmes et appareils, les outils SIEM peuvent aider à détecter les attaques sophistiquées et fournir une vue plus complète de la posture de sécurité globale.
4. **Détection des menaces** : les solutions SIEM utilisent une gamme **de** techniques, telles que la détection basée sur les signatures, la détection des anomalies et l'analyse comportementale, pour identifier les menaces de sécurité potentielles et les activités malveillantes. Ils s'appuient sur des règles et des algorithmes prédéfinis pour détecter les schémas d'attaque connus et peuvent également utiliser l'apprentissage automatique et des analyses avancées pour détecter les menaces émergentes et les attaques zero-day.

5. **Réponse aux incidents** : les solutions SIEM permettent aux équipes de sécurité de réagir rapidement aux incidents de sécurité en fournissant des alertes, des notifications et des workflows en temps réel. Lorsqu'une menace potentielle est détectée, les outils SIEM peuvent déclencher des actions automatisées ou générer des alertes pour une enquête et une réponse manuelles.
6. **Rapports et conformité** : les solutions SIEM génèrent des rapports et des tableaux de bord complets pour fournir une visibilité sur les événements de sécurité, les incidents et l'état de conformité. Ils peuvent aider les organisations à respecter les exigences réglementaires en collectant et en analysant les données nécessaires aux audits de conformité.
7. **Capacités d'intégration** : les solutions SIEM s'intègrent souvent à d'autres outils de sécurité, tels que des scanners de vulnérabilité, des plates-formes de protection des terminaux et des flux de renseignements sur les menaces, pour améliorer leurs capacités. L'intégration permet une meilleure analyse contextuelle, une détection plus précise des menaces et des workflows de réponse aux incidents rationalisés.

Dans l'ensemble, les solutions SIEM jouent un rôle crucial dans l'amélioration de la posture de sécurité d'une organisation en fournissant une surveillance en temps réel, une détection des menaces, des capacités de réponse aux incidents et une prise en charge de la conformité. Ils permettent aux équipes de sécurité d'identifier et de répondre de manière proactive aux incidents de sécurité, minimisant ainsi l'impact des violations potentielles et améliorant la résilience globale de la sécurité. Une solution de gestion des informations et des événements de sécurité (SIEM) est un système complet qui permet aux organisations de collecter, d'analyser et de gérer les événements de sécurité et les journaux provenant de diverses sources au sein de leur infrastructure réseau. Les solutions SIEM sont conçues pour aider les organisations à identifier et à répondre aux incidents de sécurité, à surveiller et à gérer les événements liés à la sécurité et à se conformer aux exigences réglementaires

2 – 4 – 2 – principaux fournisseurs

Consulter dans l’annexe 1 , l’étude du Gardner qui communique dans un majic quadrant : Gestion des informations et des événements de sécurité (onglet technologie de www. asprom.com - 2022)

1 – Fusion SIEM - https://www.exabeam.com/product/

Exabeam offre une combinaison unique de SIEM et de détection et de réponse étendues **2**) dans une solution moderne pour SecOps. Il s'agit d'une solution cloud qui vous permet de tirer parti de l'investigation, de la détection et de la réponse aux menaces de classe mondiale.
L'utilisation d'analyses comportementales de pointe a fait progresser sa détection des menaces. Vous pouvez également obtenir des résultats productifs avec des plans de cas d'utilisation normatifs et centrés sur les menaces. En conséquence, votre efficacité au travail augmente et les temps de réponse sont réduits grâce à l'automatisation.

Fusion SIEM offre un stockage de journaux basé sur le cloud, des rapports de conformité détaillés et une recherche guidée et rapide afin que vous puissiez facilement répondre aux exigences d'audit et à la conformité réglementaire, notamment GDPR, HIPAA, PCI, NERC, NYDFS ou NIST.

- **2 – graylog -**
  https://www.graylog.org/?utm_campaign=GeekFlare%20Campaign&utm_source=Geekflare-SIEM
  Graylog est un des outils de collecte et d'analyse de journaux centralisés les plus rapides pour votre pile d'applications, vos opérations informatiques et vos opérations de sécurité. Conçue pour surmonter les défis hérités de la gestion des informations et des événements de sécurité (SIEM), la plate-forme de cybersécurité flexible et évolutive de Graylog facilite et accélère le travail des analystes de sécurité.
  Avec les capacités SIEM, **Anomaly Detection** et **User Entity Behavior Analytics** (UEBA), Graylog offre aux équipes de sécurité une confiance, une productivité et une expertise encore plus grandes pour atténuer les risques causés par les menaces internes, les attaques basées sur les informations d'identification et d'autres cybermenaces.
- **3 – IBM QRADAR** - IBM Security QRadar SIEM - France | IBM
  Effectuez des analyses de sécurité intelligentes pour obtenir des informations exploitables sur les menaces critiques à l'aide de IBM QRadar SIEM. Il aide vos équipes de sécurité à détecter les menaces avec précision et à les hiérarchiser dans toute votre entreprise.
  Réduisez l'impact des incidents en répondant rapidement aux menaces grâce à des informations sur les journaux, les événements et les flux de données. Vous pouvez également consolider les données de flux réseau et consigner les événements de nombreux appareils, applications et points de terminaison sur votre réseau. QRadar peut corréler différentes données et agréger les événements associés en une seule alerte pour des analyse et prévention des incidents. Il peut également générer des alertes prioritaires ainsi que la progression de l'attaque dans la kill chain. Cette solution est disponible sur le cloud (environnements IaaS et SaaS) et sur site.

- 4 – **LogRythm -** https://logrhythm.com/products/logrhythm-siem/ Créez votre sécurité organisationnelle avec une base solide en utilisant Plateforme NextGen SIEM par LogRhythm. Racontez votre histoire autour des données de l'hôte et de l'utilisateur de manière cohérente pour obtenir facilement des informations appropriées sur la sécurité et prévenir les incidents plus rapidement.Découvrez la véritable puissance du SOC en utilisant cette solution optimisée pour la vitesse afin que vous puissiez identifier les menaces plus rapidement, collaborer sur les tâches d'enquête, automatiser les processus et prévenir les menaces immédiatement. De plus, bénéficiez d'une visibilité plus large sur l'ensemble de l'environnement, du cloud aux terminaux, pour supprimer les angles morts.
- **5 - SolarWinds -** https://www.solarwinds.com/security-event-manager

Améliorez la sécurité et démontrez la conformité à l'aide d'une solution de gestion de la sécurité prête à l'emploi, abordable et légère - Gestionnaire d'événements de sécurité par SolarWinds. Il offre une excellente surveillance en travaillant 24h/7 et XNUMXj/XNUMX pour détecter les activités suspectes et y répondre en temps réel

Il est livré avec une interface utilisateur intuitive, un contenu prêt à l'emploi et un déploiement virtuel pour vous aider à obtenir des informations précieuses à partir de vos journaux en un minimum de temps et d'expertise.

- **6 – SPLUNK -** https://www.splunk.com/

  L'outil SIEM basé sur le cloud et basé sur l'analyse - Splunk vous permet de détecter, d'enquêter, de surveiller et de répondre aux cybermenaces. Il vous permet d'injecter des données à partir de déploiements sur site et multi-cloud pour obtenir une visibilité complète sur vos environnements pour une détection rapide des menaces.

  Corrélez les activités de différents environnements dans sa vue claire et unifiée pour découvrir des menaces et des anomalies inconnues que vous n'obtiendrez peut-être pas dans les outils traditionnels. Le cloud SIEM offre également des résultats immédiats pour vous concentrer sur les tâches prioritaires sans perdre de temps à gérer du matériel compliqué.

- **7 - Elastic Security -** https://www.elastic.co/fr/security

  Obtenez un système de protection unifié – Sécurité élastique – construire sur Elastic Stack. Cet outil open source et GRATUIT permet aux analystes de détecter, d'atténuer et de répondre immédiatement aux menaces. En plus de fournir SIEM, il offre également la sécurité des terminaux, la surveillance du cloud, la chasse aux menaces, etc.

  Elastic Security automatise la détection des menaces tout en minimisant le MTTD grâce à son puissant moteur de détection SIEM. Découvrez comment détecter les menaces de sécurité dans votre environnement, réaliser des économies et bénéficier d'un retour sur investissement accru.

- **8 – InsightsIDR** - https://www.rapid7.com/products/insightidr/

  Offres **Rapid7** InsightsIDR, une solution de sécurité pour détecter les incidents, y répondre, la visibilité des terminaux et la surveillance de l'authentification. Il peut identifier les accès non autorisés à partir de menaces internes et externes et affiche les activités suspectes pour simplifier le processus à partir d'un plus grand nombre de flux de données. Leur SIEM adaptable, agile et sur mesure est créé dans le cloud pour offrir un déploiement et une évolutivité rapides à mesure que votre organisation se développe. Vous pouvez également découvrir les menaces immédiatement et résoudre les problèmes à l'aide d'une analyse avancée, de détections uniques et de l'apprentissage automatique, le tout dans une **in**terface unique.

- **9 – Sumo Logic -** https://www.sumologic.com/solutions/cloud-siem/

  Cloud SIEM Entreprise by Sumo Logic fournit une analyse de sécurité approfondie avec une visibilité améliorée pour surveiller vos

infrastructures sur site, multi-cloud ou hybrides de manière transparente afin de comprendre le contexte et l'impact d'une cyberattaque.
L'outil est utile pour un large éventail de cas d'utilisation, tels que la conformité. Il combine l'automatisation et l'analyse pour effectuer automatiquement une analyse de sécurité précise et des alertes de tri. En conséquence, votre efficacité augmente et les analystes peuvent également se concentrer sur des fonctions de sécurité à haute valeur ajoutée.
Cloud SIEM Enterprise fournit aux organisations un SIEM moderne basé sur SaaS pour protéger leurs systèmes cloud, apporter des innovations au SOC et répondre à l'évolution rapide de la surface des cyberattaques. De plus, il est déployé via la plate-forme cloud native, sécurisée et multi-locataire de Sumo Logic

- 10 **GURUCUL-** de classe mondiale de NetWitness - Analyse de la cybersécurité | Solutions SIEM & UEBA avancées | Gurucul
  GURUCUL offre une gestion, une analyse et une conservation des journaux hautes performances sous une forme cloud simple. Il élimine les exigences traditionnelles d'administration et de déploiement à l'aide d'un modèle de licence simple.En conséquence, vous pouvez acquérir un SIEM de haute qualité facilement et rapidement sans sacrifier la puissance ou la capacité. Démarrez plus rapidement avec une configuration minimale et tirez parti des derniers logiciels et systèmes d'application. L'outil prend en charge des centaines de sources d'événements avec des rapports rapides, une fonction de recherche et une détection des menaces robuste. Cela vous évite d'investir de l'argent dans des activités administratives au lieu de la sécurité et de la conformité pour protéger davantage votre organisation.
- **11 – AlienVault OSSIM** - https://cybersecurity.att.com/products/ossim
  L'un des outils SIEM open source les plus utilisés - AlienVault OSSIM, est excellent pour que les utilisateurs installent l'outil par eux-mêmes. Ce logiciel de gestion des événements et d'informations sur la sécurité fournit un SIEM riche en fonctionnalités avec corrélation, normalisation et collecte d'événements.
  AlienVault OSSIM peut résoudre de nombreuses difficultés rencontrées par les professionnels de la sécurité, telles que la détection des intrusions, l'évaluation des vulnérabilités, la découverte d'actifs, la corrélation des évents et la surveillance comportementale. Il utilise AlienVault Open Threat Exchange et vous permet de recevoir des données en temps réel sur des hôtes malveillants.
- **12 – Microsoft Sentinel -** Microsoft Sentinel – Solution SIEM cloud native | Microsoft Azure
  Microsoft est un Leader de ce Magic Quadrant. Son produit SIEM, Microsoft Sentinel, est fourni uniquement en tant que SaaS via les centres de données Azure de Microsoft. Microsoft dispose d'une base de clients importante et diversifiée, qui s'adresse aussi bien aux grands qu'aux petits clients, et qui propose le produit SIEM dans plusieurs contextes à l'échelle internationale.

La licence est basée sur le volume de données ingérées, via une capacité réservée ou le paiement à l'utilisation. Cependant, de nombreux niveaux d'entreprise Microsoft pour Microsoft 365 incluent des crédits pour l'utilisation de Sentinel et Defender. Un stockage de données amélioré, des capacités complémentaires de l'écosystème Microsoft (telles que Defender for Endpoint et Defender for IoT) sont disponibles à un coût supplémentaire.

- **13 – MicroFocus –** https://www.microfocus.com/fr-fr/cyberres
  Son produit **ArcSight** est principalement axé sur les fonctionnalités SIEM, UEBA, SOAR et TIP. Les opérations d'ArcSight sont géographiquement diversifiées (à l'exception de l'Amérique latine) et son profil client est principalement de taille moyenne. Les déploiements sur site l'emportent de loin sur les déploiements cloud-natifs, largement attribués à la disponibilité récente de son option cloud. Micro Focus a investi massivement dans son portefeuille de produits de sécurité CyberRes qui comprend la sécurité des données, la gestion de l'accès aux identités (identity access management, IAM), la sécurité des applications et les opérations de sécurité. Le premier produit phare du portefeuille d'opérations de sécurité CyberRes est Galaxy, une solution cloud-native de threat intelligence qui s'intègre au workflow ArcSight. La licence est basée sur l'EPS pour SIEM et par entité pour UEBA.
- **14 – Securonix –** Securonix : Analyse de la sécurité à l'échelle du cloud
  Sa solution SIEM est **Next-Gen SIEM** et comprend Next-Gen SIEM, Security Data Lake, UEBA, SOAR, NDR, la threat intelligence, l'analyse du comportement des adversaires et plusieurs applications spécifiques à un scénario d'utilisation (comme pour les soins de santé et SAP). La plupart des clients de Securonix se trouvent en Amérique du Nord, puis en Europe, en Asie/Pacifique, au Moyen-Orient et en Afrique, et en Amérique latine. Les clients sont principalement de grandes entreprises, mais ses produits attirent également certains clients de taille moyenne. Les clients de plus petite taille sont principalement servis par des partenaires de services gérés. La licence est basée sur les identités et l'EPS. La plupart des acheteurs optent pour des licences à durée déterminée, mais des licences perpétuelles sont disponibles.

2 – 5 – NIST et SOC quelles différences ?

NIST et SOC sont deux concepts différents liés à la sécurité de l'information. Laissez-moi vous expliquer chacun d'eux :

1. **NIST (National Institute of Standards and Technology)** : le NIST est une agence fédérale non réglementaire relevant du Département du commerce des États-Unis. Il fournit des lignes directrices, des normes et des meilleures pratiques pour améliorer la sécurité et la confidentialité des systèmes d'information. Le NIST développe et publie diverses publications, y compris la série Special Publications (SP), qui couvre un large éventail de sujets tels que la gestion des risques, les cadres de cybersécurité, les guides de configuration sécurisée, les normes cryptographiques, etc. Ces publications servent de référence aux organisations pour établir leurs politiques,

procédures et contrôles techniques de sécurité. Le cadre de cybersécurité du NIST, en particulier, est largement utilisé pour évaluer et améliorer la posture de cybersécurité d'une organisation.

2. **SOC (Security Operations Center)** : SOC fait référence à une installation ou à une équipe centralisée au sein d'une organisation responsable de la surveillance, de la détection et de la réponse aux incidents de sécurité. Un SOC se compose généralement d'analystes de la sécurité, d'intervenants en cas d'incident et d'autres professionnels de la sécurité qui travaillent ensemble pour se défendre contre les cybermenaces. L'objectif principal d'un SOC est d'identifier et de répondre aux incidents de sécurité en temps opportun afin de minimiser les dommages et de protéger les actifs de l'organisation. Les équipes SOC utilisent une combinaison d'outils, de technologies et de processus pour collecter et analyser les données de sécurité, enquêter sur les alertes et coordonner les efforts de réponse aux incidents. Ils exploitent souvent des systèmes de gestion des informations et des événements de sécurité (SIEM), des systèmes de détection d'intrusion (IDS) et d'autres technologies de sécurité pour surveiller les activités du réseau et du système.

En résumé, le NIST fournit des directives et des normes pour améliorer la sécurité des informations, tandis que SOC fait référence à une équipe ou à une installation chargée de surveiller activement et de répondre aux incidents de sécurité. Les publications du NIST peuvent être utilisées comme référence par les organisations lors de la conception et de la mise en œuvre de leurs opérations SOC, car elles fournissent des informations précieuses sur les meilleures pratiques de sécurité et les cadres de gestion des risques.

3 – Autres solutions

3 – 1 – EDR : Endpoint Detection Response

Détection et réponse des terminaux (EDR) est une solution de sécurité des terminaux qui inclut la surveillance en temps réel et la collecte des données de sécurité des terminaux avec un mécanisme de réponse automatisée aux menaces.

Gartner utilise le terme EDR pour décrire une catégorie de systèmes de sécurité émergents qui détectent et analysent les activités suspectes sur les hôtes et les terminaux pour informer les équipes responsables de la sécurité et permettre une réponse rapide, ce que rend possible leur degré élevé d'automatisation.

3 – 1 -1 Les systèmes EDR assurent cinq fonctions principales :

1. **Surveille**r activement les terminaux et collecter des données sur les activités susceptibles de représenter une menace

2. **Analyser** les données collectées pour identifier les modèles de menace connus
3. **Générer** une réponse automatique à toutes les menaces identifiées pour les supprimer ou les contenir
4. **Notifier** automatiquement le personnel de sécurité en cas de détection d'une menace
5. **Utiliser** des outils d'analyse et d'étude pour effectuer des recherches sur les menaces identifiées susceptibles de mener à d'autres activités suspectes

3 – 1- 2 Quels sont les avantages d'une solution EDR ?

Les systèmes EDR se sont imposés dans les listes de contrôle des équipes de sécurité modernes. Ils protègent le périmètre numérique contre les menaces (connues et changeantes) et les incidents de sécurité de différentes manières.

En premier lieu, la collecte complète de données de surveillance permet aux systèmes EDR de compiler une vue exhaustive des attaques potentielles. La surveillance continue de tous les terminaux, en ligne et hors ligne, facilite l'analyse et la réponse aux incidents. Elle offre une analyse et une visibilité approfondies afin que les professionnels puissent se familiariser avec les anomalies et les vulnérabilités du réseau de l'entreprise et mieux se préparer à contrer les futures attaques. La détection de chaque menace sur les terminaux va au-delà des possibilités d'un antivirus traditionnel, et la capacité de la solution EDR à traiter en temps réel un large éventail de menaces permet aux équipes en charge de la sécurité de visualiser les attaques et menaces potentielles à mesure qu'elles évoluent.

Vous évitez ainsi les pertes en sabotant les attaques dès leurs phases initiales, avant que des pertes ou des compromissions critiques ne se produisent. La réponse en temps réel permet également à une entreprise de détecter un comportement suspect ou non autorisé sur le réseau, et d'identifier la cause profonde d'une menace avant qu'elle n'affecte les opérations. Enfin, les systèmes EDR peuvent s'intégrer à d'autres outils de sécurité, ce qui permet de mettre en corrélation les données des terminaux, du réseau et des systèmes SIEM, et de développer ainsi une expertise dans les pratiques et techniques appliquées par les personnes malveillantes qui tentent d'accéder sans autorisation aux ressources numériques.

3 – 1 – 3 -Comment fonctionne une solution EDR ?

Une solution EDR surveille le trafic du réseau et des terminaux, collecte les informations potentiellement liées à des problèmes de sécurité dans une base de données centrale pour analyse ultérieure, et facilite la génération de rapports et les recherches sur les menaces.

Toutes les solutions EDR ne se valent pas : l'étendue de leurs activités peut varier d'un fournisseur à l'autre. Les principaux composants d'une solution EDR standard sont les suivants :

- **Agents de collecte de données**. Installés sur les terminaux, ces agents surveillent et collectent des données sur les processus en cours d'exécution, les connexions aux réseaux et aux terminaux, le volume d'activité et les transferts de données.
- **Hub central.** Ce hub intégré recueille, met en corrélation et analyse les données collectées sur les terminaux. Le hub central coordonne également les alertes et les réponses aux menaces immédiates.
- **Automatisation de la réponse.** Un système EDR utilise des règles, généralement préconfigurées, qui identifient les menaces connues dans les données collectées et déclenchent une réponse automatique, par exemple pour alerter le personnel de sécurité ou déconnecter un utilisateur du système.
- **Observabilité et analyse.** Les solutions EDR peuvent inclure des outils d'analyse permettant d'éliminer les menaces, ou d'effectuer des analyses après coup et des analyses en temps réel qui accélèrent la détection de menaces n'entrant pas dans le champ des règles préconfigurées existantes7

3 -1- 4 -Quelle est la différence entre une solution EDR et un antivirus ?

Les solutions EDR peuvent être considérées comme un super-ensemble de programmes antivirus traditionnels, dont la portée est limitée par rapport aux nouvelles solutions EDR. Sous cet angle, un antivirus fait partie intégrante d'une solution EDR.

Un antivirus exécute des fonctions de base comme l'analyse, la détection et la suppression des virus, alors qu'une solution EDR met en œuvre de nombreuses autres fonctions. Au-delà du rôle d'antivirus, la solution EDR peut proposer des fonctions supplémentaires comme, entre autres, la surveillance et la création de listes autorisées/bloquées, conçues pour renforcer la protection contre les menaces connues et émergentes.

Étant donné que le périmètre de réseau numérique a été étendu partout, un antivirus traditionnel ne peut plus protéger tous les terminaux utilisés pour accéder aux ressources de l'entreprise. Les systèmes EDR sont mieux adaptés pour se protéger contre les cyberattaques avancées, et leur mécanisme de réponse automatisée allège la charge des équipes informatiques responsables de la protection contre les attaques.

Cette fonctionnalité gagne en importance en raison de l'évolution rapide du paysage des menaces. Dans la mesure où les cybercriminels perfectionnent leurs attaques et utilisent des menaces avancées pour accéder aux réseaux, un simple antivirus basé sur des signatures ne détecte pas les menaces zero-day ou multicouche en temps opportun alors qu'à l'inverse, les systèmes EDR détectent tous les types de menaces et combattent en temps réel celles qui sont identifiées.

3 – 1 – 5 – Acteurs du domaine EDR

- **Cynet -** https://www.cynet.com
  Cynet fournit la détection et la réponse des points de terminaison dans le cadre de la plate-forme holistique qui protège l'ensemble de l'environnement interne, y compris les hôtes, le réseau, les fichiers et les utilisateurs. C'est la raison pour laquelle Cynet est en mesure de fournir une visibilité totale de l'environnement plutôt que la seule visibilité des points de terminaison et de prévenir et de détecter les menaces que les autres solutions EDR ne peuvent pas.
  Il dispose également de l'ensemble le plus large d'outils de correction non seulement pour les points de terminaison, mais également pour les utilisateurs et le trafic réseau. La plateforme se déploie en quelques heures et dispose d'une console de gestion très simple d'utilisation.
- **CrowdStrike -** https://www.crowdstrike.fr/ CrowdStrike propose une plateforme Falcon flexible et extensible. Il fournit une variété de modules basés sur cette plate-forme Falcon comme Falcon Prevent, Falcon Insight, Falcon Discover, etc. CrowdStrike propose des produits comme Falcon Pro, Falcon Enterprise, Falcon Premium et Falcon Complete.
  - Falcon Enterprise aura géré la chasse aux menaces et intégré les renseignements sur les menaces.
  - Avec Falcon Complete, vous obtiendrez une protection des points de terminaison en tant que service.
  - Falcon Premium vous offrira une protection complète des terminaux et une visibilité étendue.
  - Falcon Pro est destiné à l'intelligence des menaces intégrée et à la réponse immédiate.

  Le graphique des menaces est basé sur le big data et l'intelligence artificielle.
- **Carbon Black -** https://www.vmware.com/products/carbon-black-endpoint.html
  Carbon Black fournit des solutions pour sécuriser les centres de données virtualisés, la protection contre les logiciels malveillants et autres que les logiciels malveillants, les risques et la conformité, la protection contre les ransomwares et les antivirus. Il peut être déployé sur site ou en tant que SaaS. Il peut analyser le modèle de comportement de l'attaquant. Il fournira l'enregistrement d'activité complet pour chaque point de terminaison, même s'il est hors ligne.
  Sa réponse isole les systèmes infectés et supprime les fichiers malveillants.
  Interrogation et correction des points de terminaison en temps réel.
  Cette plate-forme vous fournira l'antivirus de nouvelle génération avec des capacités EDR.
- **sentinelOne -** https://www.sentinelone.com **-**
  SentinelOne offre une protection contre les divers modes d'attaques. Cela fonctionnera en utilisant le moteur Static AI qui vous fournira la protection de pré-exécution.
  Le moteur d'IA comportementale de SentinelOne peut suivre tous les processus et leurs interrelations même s'ils sont actifs pendant une longue période. Il protégera les terminaux contre de larges modes d'attaques.

Caractéristiques:

- lpeut détecter les menaces à toutes les étapes.
- Ieffectuera une inspection approfondie des fichiers.
- protégera des attaques de ransomware.
- a un agent léger et holistique.
- dispose d'un EDR automatisé,

ce qui signifie une atténuation automatique des menaces, une isolation du réseau et une immunisation automatique des terminaux contre les nouvelles menaces.

- Les attaques avancées sont détectées à partir des politiques comportementales. Les chercheurs de Symantec mettent continuellement à jour ces politiques.
- Il fournit des défenses imbriquées au niveau de l'appareil, de l'application et du réseau.
- Il n'y aura pas de complexité car il utilise un seul agent et une seule console.

➢ **Symantec EDR -** Endpoint Security (broadcom.com)

Le fabricant américain de semi-conducteurs **Broadcom** a annoncé jeudi l'acquisition de la division « sécurité des entreprises » du gro : upe de sécurité informatique Symantec. Avec ce rachat à 10,7 milliards de dollars (9,6 milliards d'euros), Broadcom poursuit sa série d'acquisitions dans le domaine des logiciels. Symantec EDR peut détecter, isoler et éliminer les intrusions pour tous les terminaux. Il utilise l'IA pour effectuer cela. Il effectue une chasse aux menaces 24 * 7. Il vous permettra de créer des flux d'enquête personnalisés. Vous serez en mesure d'automatiser des tâches manuelles répétitives, sans script complexe. Less attaques avancées sont détectées à partir des politiques comportementales. Les chercheurs de Symantec mettent continuellement à jour ces politiques.
Il fournit des défenses imbriquées au niveau de l'appareil, de l'application et du réseau.
Il n'y aura pas de complexité car il utilise un seul agent et une seule consoleLes Les attaques avancées sont détectées à partir des politiques comportementales. Les chercheurs de Symantec mettent continuellement à jour ces politiques.

➢ **CyberReason –** https://www.;cyberreason.com/fr/

De nombreux flux de menaces différents ne sont souvent pas d'accord les uns avec les autres sur les IOC malveillants ou inconnus. Ces informations contradictoires rendent difficile la détermination rapide du caractère malveillant d'une menace et la prise de mesures.
Cybereason Threat Intelligence regroupe plusieurs flux de menaces et les contre-examine par rapport à l'analyse de l'apprentissage automatique afin de classer les différents flux de menaces en fonction de leur précision historique pour des types particuliers de menaces provenant de divers groupes d'adversaires. Cela permet à Cybereason de déterminer la bonne source de renseignements sur les menaces pour répondre rapidement et avec précision, ce qui simplifie le processus d'enquête et de réponse. -

➢ **CISCO Secure Endpoint (AMP for EndPoint) -**
https://www.cisco.com/site/fr/fr/products/security/endpoint-security/

Cisco Secure Endpoint (anciennement AMP for Endpoints) est une solution complète de sécurité des terminaux conçue pour fonctionner à la fois comme un produit autonome de détection et de réponse aux points de terminaison (EDR) et comme une partie importante de l'architecture® Cisco SecureX EDR/XDR. Les clients et les partenaires doivent prendre en compte de nombreuses considérations avant de déployer et de configurer Secure Endpoint dans leur environnement. L'objectif de ce document est de fournir des conseils sur les meilleures pratiques pour la méthodologie, l'installation et la configuration de déploiement.
Remarque : le Guide des meilleures pratiques est conçu comme un document supplémentaire à la documentation produit existante et ne contient pas une liste complète de toutes les options de configuration Secure Endpoint. Pour des paramètres de produit détaillés plus détaillés, consultez d'autres documents officiels Secure Endpoint disponibles à l'adresse suivante : https://docs.amp.cisco.com/.
Ce document décrit les étapes recommandées pour un déploiement réussi de Cisco Secure Endpoint. L'organigramme sert ici de cadre généralisé que les clients peuvent utiliser dans leur environnement.

- FireEyes HX - https://www.fireeye.com/
  FireEye Endpoint Security s'appuie sur le meilleur des produits de sécurité traditionnels pour y ajouter la technologie, l'expertise et la Cyber Threat Intelligence (CTI) signées FireEye. Objectif : vous protéger efficacement face aux cyberattaques actuelles. Conçu sur un modèle de défense en profondeur (Defense-in-Depth), Endpoint Security s'appuie sur une architecture modulaire dotée de moteurs préconfigurés et de modules téléchargeables pour protéger, détecter et gérer les agents. Pour bloquer les malwares courants, Endpoint Security utilise un moteur EPP (Endpoint Protection Platform) basé sur les signatures. Pour les menaces émergentes qui n'ont pas encore été caractérisées par une signature, MalwareGuard fait appel à des technologies de machine learning nourries par une CTI de terrain. Face aux menaces APT, les fonctionnalités EDR (Endpoint Detection and Response) déploient un moteur d'analyse des comportements capable de détecter toute activité suspecte
- **McAfee EDR – Trellix -** https://www.trellix.com/fr-fr/
  Trellix : tel est le nom du nouveau géant mondial de la cybersécurité issu de la fusion entre McAfee Enterprise et FireEye.
  Trellix offre une sécurité de pointe entre les appareils et le cloud dans les environnements multicloud et sur site. Nos solutions protègent les données, se défendent contre les menaces et fournissent des informations exploitables via une plate-forme ouverte et le plus grand réseau de télémétrie des menaces

  - **Ne laissez aucune attaque invisible avec Network Detection and Response (NDR)**
    Bénéficiez d'une visibilité inégalée et appliquez une détection et une protection de pointe sans signature contre les menaces les plus avancées et les plus évasives, y compris les attaques zero-day.

- **Répondez aux alertes importantes**
  Améliorez l'efficacité des analystes avec des alertes haute fidélité qui se déclenchent au moment le plus important, économisant du temps et des ressources et réduisant le volume d'alertes et la fatigue.
- **Automatisez et simplifiez les flux de travail de sécurité**
  Générez des preuves concrètes en temps réel et des métadonnées de couche 7 pour fournir un contexte de sécurité supplémentaire pour pivoter vers la validation des enquêtes et des alertes, le confinement des terminaux et la réponse aux incidents.

3 – 1 – 6 – Micro Focus : Micro-SOC-EDR

Le Micro-SOC est une nouvelle génération de service de protection, remédiation et de détection proactive sur vos postes de travail et serveurs. Il combine l'Intelligence Artificielle et l'expertise des analystes Orange Cyberdefense. La détection proactive du Micro-SOC EDR permet de détecter les actions malveillantes sur votre système d'information avant que l'attaque soit réellement déclenchée. Cela permet de confiner l'appareil infecté et de remédier à l'attaque avant qu'elle n'envahisse les autres postes.

Exemple : **Orange-Cyberdefense**- https://www.orangecyberdefense.com/ar-ma/solutions/micro-soc

Avec Micro-SOC, Orange Cyberdefense définit avec vous les alertes et les mesures de confinement activables à tout moment (même dès la phase de mise en service). En cas d'attaque, vous avez ainsi la capacité d'isoler ou confiner les postes compromis via un portail personnalisé.

3 - 2 - NDR : Network Detection and Response

Le NDR apporte une visibilité étendue aux équipes du SOC, à l'échelle du réseau, pour détecter le comportement d'attaquants possiblement cachés, ciblant les infrastructures physiques, virtuelles et dans le Cloud. Il apporte de la complémentarité aux outils EDR et SIEM.
L'approche du NDR offre une vue d'ensemble et se concentre sur les interactions entre les différents nœuds du réseau. Le fait d'obtenir un contexte de détection plus large, peut révéler toute l'étendue d'une attaque et permettre des actions de réponse plus rapides et mieux ciblées.
À noter qu'il est indispensable d'avoir un outil d'EDR et/ou de SIEM avant d'acquérir un NDR, pour pouvoir investiguer correctement sur les alertes remontées par le NDR. Le NDR seul n'apporte pas assez de contexte pour pouvoir traiter l'alerte qu'il remonte.

3 – 2 – 1 -Avantages de Network Detection & Response

Les solutions NDR les plus avancées offrent une multitude d'avantages :

- **Visibilité sur les menaces omniprésentes :** Les équipes de sécurité peuvent visualiser les menaces, des intrusions aux mouvements latéraux, sur l'ensemble du réseau, aussi bien on premise que dans le Cloud.
- **Réduction du nombre de faux positifs** Les organisations peuvent réduire le nombre de faux positifs et libérer les équipes de sécurité pour qu'elles se concentrent sur l'arrêt des intrusions.
- **Prévenir ou arrêter plus rapidement les intrusions :** La NDR utilise l'IA et l'autoapprentissage pour opérer en temps réel et détecter et arrêter rapidement les menaces.
- **Visualisation complète des attaques :** Avec un modèle complet des intrusions et une chronologie détaillée des menaces sur le réseau, les équipes de sécurité peuvent rapidement comprendre la portée d'une attaque et hiérarchiser les ressources.

Parmi les leaders en matière de détection et réponse réseau, VMware NSX Network Detection and Response fournit un ensemble intégré de fonctionnalités de détection et de réponse réseau pour assurer la sécurité est-ouest au sein du Data Center et des environnements multicloud. La solution Network Detection and Response de VMware fournit le plus large éventail de fonctionnalités de détection, qui couvrent des IDS/IPS, une analyse comportementale du trafic réseau et un **sandbox réseau** basé sur l'émulation du système complet.

3 – 2 – 2 -Comment fonctionne Network Detection & Response ?

Network Detection and Response ingère et met constamment en corrélation d'importants volumes de trafic réseau et d'événements de sécurité couvrant plusieurs ressources et tronçons. En collectant des données issues du périmètre du réseau (pour couvrir le trafic nord-sud) et de capteurs intégrés au réseau (pour couvrir le trafic est-ouest), les solutions Network Detection and Response exploitent l'IA et l'autoapprentissage pour développer une compréhension de base des flux de trafic réseau normaux, et par conséquent une capacité à détecter les activités malveillantes qui ne suivent pas de modèles normaux.

Les outils NDR reposant sur l'IA apprennent et s'adaptent continuellement pour fournir une détection automatique des menaces sophistiquées en constante évolution.

Si une attaque est détectée, les solutions NDR peuvent fournir une analyse de bout en bout de la chronologie de l'attaque, de l'infiltration initiale aux mouvements latéraux au sein du réseau, et peuvent déclencher automatiquement des workflows de prévention et d'atténuation.

3 – 2 – 3 -Comment l'intégration de N D R fonctionne-t-elle ?

Généralement, les entreprises décident globalement si elles préfèrent :

- Une solution NDR **gérée**, avec laquelle un fournisseur tiers assure la protection sous forme de service et offre un certain niveau d'intégration avec les produits d'autres fournisseurs éventuellement déployés.
    - Une solution NDR **en interne**, avec laquelle vous détenez et gérez le système et l'intégrez à vos autres technologies de sécurité. Cette situation était courante dans le passé, mais devient de plus en plus contraignante à mesure que le paysage des menaces s'étend.
    - Une solution NDR **automatisée**, telle qu'une offre SOAR, est un système plus élaboré qui va au-delà de la NDR pour fournir des fonctionnalités complètes de collecte de données fournies par plusieurs technologies de sécurité et de réponse automatisée aux incidents.

3 – 2 – 4 – Fournisseurs représentatifs

- **Arisrta Networks**- https://www.arista.com/
  Arista Networks est un fournisseur mondial de réseaux et d'infrastructures, qui vend principalement des rapports de non-remise aux États-Unis et dont le siège social est situé à Santa Clara, en Californie. Le produit NDR d'Arista Networks (Arista NDR) est basé sur l'acquisition d'Awake Security en 2020. Arista propose également des services gérés (Arista managed NDR service).
  Arista collecte principalement des données à partir de capteurs, qui peuvent être autonomes ou intégrés dans des commutateurs Arista. Arista NDR inclut un moteur de recherche de chasse aux menaces, basé sur un langage propriétaire (Adversarial Modeling Language [AML]). Arista cible les réseaux à grande échelle et propose des intégrations avec les principaux fournisseurs et hyperviseurs IaaS pour mieux servir les équipes réseau et sécurité avec une visibilité accrue pour les cas d'utilisation des centres de données.
- **Cisco -** https://blogs.cisco.com/tag/network-detection-and-response-ndr
  Cisco est un fournisseur mondial basé à San Jose, en Californie. Le portefeuille de Cisco comprend deux produits en compétition dans les listes restreintes de rapports de non-remise : Secure Network Analytics (SNA), un outil principalement sur site, et Secure Cloud Analytics (SCA), un rapport de non-remise fourni dans le cloud. Les produits Cisco NDR peuvent collecter NetFlow/IPFIX à partir de capteurs tiers ou du fournisseur. L'architecture SNA est une architecture à trois niveaux, avec Flow Collector agrégeant les flux de plusieurs capteurs avant d'envoyer des événements à la console de gestion centralisée avec un moteur d'analyse hébergé dans le cloud en option. Cisco SCA utilise des API natives pour collecter des événements IaaS et peut être déployé en tant qu'agent sur un pod Kubernetes. Les produits Cisco NDR privilégient l'heuristique, l'analyse statistique et les renseignements sur les menaces, combinés à des règles prédéfinies de violation de politique et de seuil pour détecter les anomalies de réseau et de sécurité.
- **Corelight** - https://corelight.com/
  Corelight est un fournisseur mondial, basé à San Francisco, en Californie. Corelight est le résultat de l'effort de construire un produit commercial

sur le dessus des moteurs Zeek et Suricata. Le produit NDR du fournisseur, Corelight Open NDR, fournit une capture sélective complète des paquets (Smart PCAP) et a récemment publié une console d'analyse et de gestion SaaS (Investigator).
Corelight NDR (**Open NDR**) s'appuie sur son propre matériel et ses capteurs virtuels (y compris VM sur les plates-formes IaaS) pour collecter des données. Il propose une VM de gestion de capteurs (Fleet Manager). Les détections de rapports de non-remise ouvertes sont principalement basées sur des règles, exploitant leurs propres règles et moteurs de détection pour l'heuristique, et utilisant des ensembles de règles complémentaires de partenaires tels que **CrowdStrike** et **Proofpoint.**

- **Darktrace -** https://fr.darktrace.com/
  Darktrace est un fournisseur mondial de rapports de non-remise dont le siège social est situé à Cambridge, au Royaume-Uni. Le rapport de non-remise de Darktrace, maintenant connu sous le nom de Darktrace DETECT, s'appelait auparavant Enterprise Immune System (EIS). Il reste leur produit phare, avec un abonnement séparé pour la réponse automatisée (Darktrace RESPOND, anciennement Antigena). Le fournisseur a récemment lancé Darktrace PREVENT, qui comprend la gestion de la surface d'attaque externe et l'analyse des chemins d'attaque.
  Darktrace NDR collecte principalement des données à partir de son propre matériel, de capteurs virtuels et de capteurs de terminaux, mais peut également collecter des données à partir de produits de sécurité des terminaux et de l'infrastructure. Darktrace DETECT peut tirer parti d'API tierces pour enrichir ses propres analyses. Le fournisseur inclut plusieurs moteurs de détection, avec un fort accent sur l'apprentissage non supervisé pour la détection des anomalies. Darktrace s'est également diversifiée en surveillant le cloud (IaaS), les applications (SaaS), le courrier électronique et les réseaux OT et en appliquant ses techniques ML pour automatiser le processus d'enquête sur les incidents (appelé Cyber AI Analyst).
- **ExtraHop-** https://www.extrahop.com/fr/
  ExtraHop est un fournisseur mondial de réseau et de sécurité avec des racines dans la surveillance des performances réseau, avec une majorité de ses ventes de NDR provenant des États-Unis aujourd'hui. Le siège social d'ExtraHop est situé à Seattle, dans l'État de Washington. ExtraHop Reveal(x) est la plate-forme de notification d'échec de remise du fournisseur , disponible en mode SaaS ou reposant sur des appliances physiques ou virtuelles pour l'analyse et la gestion. Le fournisseur propose désormais principalement son architecture d'analyse SaaS, appelée Reveal(x) 360.
  ExtraHop Reveal(x) collecte des données à partir de ses capteurs appliances, d'infrastructures tierces et d'API de visibilité des paquets de plate-forme IaaS. Reveal(x) combine plusieurs techniques de détection, y compris les signatures et l'heuristique. Le fournisseur a récemment ajouté des articles interactifs sur les renseignements sur les menaces (Threat Briefing). Reveal(x) et Reveal(x) 360 fournissent des analyses statistiques et d'apprentissage automatique supplémentaires, effectuées dans le cloud et basées sur des événements anonymisés agrégés. ExtraHop fournit en option des capacités de

déchiffrement du trafic et de capture complète des paquets (ce qui nécessite des périphériques de stockage de paquets supplémentaires pour les organisations souhaitant conserver les données locales), qui peuvent ensuite être consultées directement à partir du moteur de recherche de métadonnées (« vue Enregistrements »). Pour une réponse automatisée, ExtraHop s'intègre à divers fournisseurs, notamment Endpoint, SIEM et SOAR.

- **Fidelis Cybersecurity-** https://fidelissecurity.com/

  Fidelis Cybersecurity est un fournisseur mondial, qui vend principalement des rapports de non-remise aux États-Unis, dont le siège social est situé à Bethesda, dans le Maryland.

  Le produit NDR du fournisseur s'appelle Fidelis Network et obtient la plupart de ses ventes auprès de clients basés aux États-Unis, suivis par EMEA. Fidelis Cybersecurity est disponible en tant que plate-forme de gestion et de capteurs entièrement sur site, mais une option SaaS pour la gestion est également disponible.

  Fidelis Network peut ingérer des données provenant de capteurs dédiés et de diverses sources tierces, y compris des enregistrements de flux, des événements EDR et des journaux Active Directory, pour aider à détecter les menaces. Le système peut analyser via une gestion sur site ou basée sur le cloud. Fidelis Network comprend un moteur de recherche de métadonnées de chasse aux menaces. Le trafic crypté peut être analysé via JA3 ou déchiffré dans un processus de l'homme du milieu. Suricata est intégré dans le produit avec ses signatures pour la détection. Les moteurs d'analyse de Fidelis Network sont fortement axés sur l'analyse de contenu, le sandboxing et la prévention des fuites de données.

- **Gatewatcher -** https://www.gatewatcher.com/

  Gatewatcher est un fournisseur régional de NDR, basé à Paris, en France. La notification d'échec de remise de Gatewatcher, appelée AionIQ, peut être déployée sur un serveur ou en tant que machine virtuelle. Il combine des capteurs matériels pour les cas d'utilisation sur site et des capteurs virtualisés avec la prise en charge de l'IaaS d'Amazon Web Services. Le portefeuille du fournisseur comprend également un IDS appelé Trackwatch, destiné à la surveillance des infrastructures critiques locales. Gatewatcher a commencé à se développer à l'international.

  Le moteur d'analyse AionIQ comprend un moteur d'analyse de fichiers qui repose sur un antivirus tiers, un bac à sable, des signatures IDS, des renseignements sur les menaces et un ML supervisé pour détecter les activités malveillantes. AionIQ permet une réponse automatisée en tirant parti des intégrations d'API.

- **Gigamon -** https://www.gigamon.com/fr/

  Gigamon est un fournisseur mondial, vendant principalement NDR aux États-Unis, dont le siège social est situé à Santa Clara, en Californie. Le produit NDR de Gigamon, ThreatINSIGHT est principalement vendu aux États-Unis et en Australie. Gigamon inclut un service appelé DiN Guided-SaaS, qui fournit une approche dirigée de la notification d'échec de remise et tire parti de l'expérience du personnel de Gigamon en matière de réponse aux incidents.

  Gigamon collecte principalement des données à partir de capteurs dédiés, physiques et virtuels. Ila également des intégrations avec certains fournisseurs EDR et peut ingérer des journaux tiers. Toutes les analyses sont effectuées dans le cloud. La chasse aux menaces fait partie de l'offre, en mettant l'accent sur la

chasse guidée. Le trafic crypté est analysé via des signatures JA3, des techniques propriétaires et un décryptage de l'homme du milieu. Le fournisseur privilégie l'heuristique pour la détection des menaces suivie d'un ML supervisé. Gigamon utilise par défaut une période de rétention de 365 jours pour toutes les métadonnées. Suricata a été intégré pour aider à la détection des attaques basée sur les signatures.

- **IronNet-** https://www.ironnet.com/

  IronNet est un fournisseur mondial de NDR coté à la Bourse de New York (IRNT) et dont le siège social est situé à McLean, en Virginie. La solution NDR d'IronNet est fournie via la plate-forme de défense collective d'IronNet. Il comprend deux composants principaux, IronDefense, qui inclut toutes les capacités de détection et d'analyse, et IronDome, qui est une communauté collaborative de clients IronNet NDR. IronDome facilite le partage sécurisé de la détection et de l'analyse avec les pairs afin d'améliorer la compréhension d'une équipe SOC dans le paysage actuel des menaces.

  Laplate-forme de défense collective ronNet utilise à la fois des paquets réseau et des enregistrements de flux réseau, ainsi que des journaux provenant de services d'annuaire, de DNS et d'une large gamme d'autres produits de sécurité (par exemple, pare-feu, NAC, SIEM, EPP et autres). IronNet peut également fonctionner avec des journaux provenant de plates-formes IaaS. IronNet Collective Defense Platform utilise le ML ainsi qu'une analyse statistique importante pour la détection, mais une grande contribution à ses détections provient des communautés de défense collective, où les clients peuvent échanger des renseignements sur les attaques en temps quasi réel, identifiant les attaques avancées ou uniques au fur et à mesure qu'elles se déroulent, telles que les infrastructures C2 nouvelles ou auparavant inconnues

- **Plixer -** https://www.plixer.com/

  Plixer est un fournisseur mondial de NDR, dont le siège social est situé à Kennebunk, dans le Maine. Plixer est en train de redéfinir son portefeuille de produits. Le fournisseur a commencé comme un fournisseur de performances réseau, avec un produit appelé Plixer Network Intelligence (PNI, anciennement connu sous le nom de Plixer Scrutinizer). Plixer NDR est appelé Plixer Security Intelligence (PSI) Platform. Les deux produits peuvent utiliser les mêmes capteurs pour la collecte de données.

  Plixer NDR surveille principalement le trafic via les enregistrements de flux réseau (NetFlow ou IPFIX) collectés sur site auprès des collecteurs de données, mais peut également ingérer des sources IaaS. Une partie de l'analyse s'exécute directement sur le collecteur de données et l'analyse basée sur le ML est effectuée sur une appliance dédiée (matérielle ou virtuelle) qui peut être déployée sur site ou dans le cloud. Plixer peut ingérer n'importe quel flux de renseignements sur les menaces à l'aide de STIX/TAXII et apporte également du contexte provenant de sources multiples, y compris les terminaux, les serveurs DNS, les pare-feu et les journaux des systèmes de prévention des intrusions (IPS

- **Progress** (Flowmon Networks)- https://www.whatsupgold.com/fr/flowmon
  Progress, un fournisseur mondial de développement d'applications et d'expérience numérique, est coté au Nasdaq (PRGS) et son siège social est situé à Burlington, dans le Massachusetts. Le fournisseur a acquis Flowmon Networks, un fournisseur mondial de rapports de non-réponse, grâce à l'acquisition de sa société mère Kemp Technologies en 2021. La solution NDR de Progress est le système de détection des anomalies Flowmon (ADS). La solution Flowmon ADS se compose de deux composants principaux. Le premier est un collecteur requis qui stocke, traite, analyse et visualise les données réseau. La seconde est une sonde facultative utilisée pour exporter des données de flux réseau et des métadonnées étendues. Cette architecture est également utilisée pour la gamme de produits de surveillance et de diagnostic des performances réseau Flowmon de Progress.
  Flowmon ADS utilise principalement les enregistrements de flux réseau pour la détection et l'analyse, mais peut également utiliser les journaux des services d'annuaire. Flowmon Collector est le référentiel pour les enregistrements de données de flux et prend en charge plusieurs formats de flux, y compris IPFIX. Les enregistrements de flux peuvent être générés en mode natif à partir de périphériques d'infrastructure réseau conformes, ou les sondes de
  Flowmon peuvent être utilisées sur un port SPAN ou un TAP réseau pour générer des enregistrements IPFIX enrichis , y compris des informations IDS écrites sur l'extension IPFIX de Flowmon. Flowmon utilise une variété de méthodes, y compris l'analyse statistique, l'heuristique et le ML, les flux de renseignements sur les menaces et les signatures IDS.
- **QI-ANXINE -** https://en.qianxin.com/
  QI-ANXIN est un fournisseur régional, basé à Pékin, en Chine. QI-ANXIN propose une **suite de produits de sécurité, y compris SkyEye, son produit de détection des menaces,** qui est en concurrence sur le marché des rapports de non-remise. QI-ANXIN concentre actuellement ses efforts sur son marché domestique et a commencé à se développer à l'international.
  SkyEye s'appuie fortement sur un large ensemble de règles, qui comprend une combinaison de signatures traditionnelles et de détection plus générique, basée sur l'apprentissage automatique supervisé. SkyEye comprend des capteurs d'appareils physiques et un bac à sable (qui fait partie de sa gamme de produits TSS). Le déchiffrement TLS (Transport Layer Security) est disponible pour le trafic vers les serveurs internes. Le fournisseur exploite également plusieurs sources de renseignements sur les menaces.
- **Sangfor** - https://www.sangfor.com/
  Sangfor est un fournisseur mondial d'informatique et de sécurité, axé sur la notification d'échec de remise régionale, basé à Shenzhen, en Chine. Sangfor Cyber Command est la plate-forme analytique centralisée du fournisseur, collectant les événements des capteurs et autres produits Sangfor. Sangfor Cyber Command combine plusieurs techniques de détection, y compris le ML supervisé et non supervisé, les signatures plus traditionnelles et les

renseignements sur les menaces. Sangfor Cyber Command ne fournit pas de décryptage TLS natif, mais peut repérer les anomalies en analysant les métadonnées TLS. La réponse est disponible via l'intégration avec le pare-feu ou la passerelle Web sécurisée du fournisseur, mais aussi avec des pare-feu tiers et des produits de sécurité des terminaux.

- **stamus Network -** https://www.stamus-networks.com/
  Stamus Networks est un fournisseur mondial de rapports de non-remise dont le siège social est situé à Indianapolis, dans l'Indiana et à Paris, en France. La solution de notification d'échec de remise de Stamus est Stamus Security Platform et est disponible en deux niveaux : Stamus Network Detection and Response (NDR) et Stamus Network Detection (ND). Stamus ND comprend la détection de base de Suricata, le triage et la chasse aux menaces. Stamus NDR ajoute des renseignements personnalisables sur les menaces, une hiérarchisation automatisée des alertes et des analyses basées sur le ML.
  Stamus Networks est fortement investi dans l'évolution de Suricata et, en tant que tel, utilise des paquets réseau complets comme source de données principale. Les capteurs Stamus (logiciels et matériels) peuvent prendre en charge les déploiements sur site et IaaS et alimenter le serveur central Stamus (logiciel). L'analyse commence avec le moteur Suricata dans les capteurs Stamus. Stamus peut déployer ses propres capteurs Suricata ou, dans de nombreux cas, peut utiliser vos capteurs Suricata existants . L'analyse comprend également le ML, l'analyse statistique, les renseignements sur les menaces et l'heuristique.
- **Tencent** - https://www.tencent.com/
  Tencent est une grande société mondiale de technologie Internet, basée à Shenzhen, en Chine. Tencent propose un portefeuille complet de produits et services de sécurité (**T-Sec**), avec une gamme de produits NDR petite mais en croissance (T-Sec NDR), principalement proposée aux grandes entreprises en Chine. T-Sec NDR est principalement déployé en tant qu'appliances physiques, mais prend également en charge les environnements IaaS avec VM et les options de déploiement logiciel.
  T-Sec NDR collecte des paquets complets et inclut la possibilité de stocker des PCAP pour l'analyse médico-légale, en plus de la détection en temps quasi réel. Il peut déchiffrer le trafic TLS et combine plusieurs moteurs de détection, y compris un bac à sable malveillant. Certaines détections ML sont disponibles et le fournisseur continue d'étendre son utilisation, mais T-Sec NDR combine principalement des renseignements sur les menaces, des signatures et des politiques basées sur des seuils pour détecter les anomalies. Son module de réponse s'appelle Tianmu. T-SEC NDR tire également parti de l'intégration avec Tencent et les produits de sécurité tiers.

- **Trellix-** https://www.trellix.com/fr-fr/products/endpoints.html

Trellix est un fournisseur mondial de sécurité d'infrastructure dont le siège social est situé à Plano, au Texas, issu de la fusion en 2022 des fournisseurs de sécurité établis **McAfee Enterprise** et **FireEye**.
La solution de notification d'échec de remise Trellix se compose de la console de gestion et de surveillance (Trellix Network Investigator) qui peut être déployée en tant que produit autonome avec ses propres capteurs, ou en plus des déploiements existants des produits de l'entreprise : Trellix NX (anciennement FireEye), Trellix IPS (anciennement McAfee NSP) et Trellix Network Forensics. Trellix NDR utilise principalement des paquets réseau pour la détection, mais peut également exploiter les enregistrements de flux réseau, ainsi que les journaux du DNS. Trellix utilise à la fois l'apprentissage automatique supervisé et non supervisé pour compléter l'analyse statistique, l'heuristique, les signatures IDS et les renseignements sur les menaces. Trellix NDR utilise l'analyse de session multiflux héritée de son moteur FireEye MVX via des environnements de système d'exploitation émulés pour recomposer le trafic réseau et obtenir la perspective de l'hôte cible. La technologie de sandboxing Trellix est également disponible pour fournir une analyse des logiciels malveillants.

- **Trend Micro** – https://www.trendmicro.com/fr _

  Trend Micro est un fournisseur mondial dont le siège social est situé à Tokyo, au Japon. Le produit NDR de Trend Micro est basé sur sa plate-forme **Vision One**, qui utilise Deep Discovery et TippingPoint comme capteurs réseau. L'APAC et la région EMEA sont des marchés clés pour Trend Micro.
  Trend Micro collecte principalement des données à partir de capteurs matériels et logiciels, mais peut également ingérer les journaux des pare-feu et les alertes de son produit EDR. Le produit NDR de Trend Micro inclut la chasse aux menaces par le biais de son moteur de recherche, basé sur un langage propriétaire et une approche clé en main pour trouver les menaces. Le fournisseur privilégie les renseignements sur les menaces et les signatures IPS pour la détection des menaces. Un grand nombre de signatures est disponible car le système utilise le moteur TippingPoint pour IPS. Trend Micro cible l'intégration avec son portefeuille de produits de sécurité existant, et les clients utilisant Vision One obtiennent une corrélation entre plusieurs produits.

- **Vectra**

  Vectra est un fournisseur mondial de NDR, dont le siège social est situé à San Jose, en Californie. Le NDR de Vectra, maintenant connu sous le nom de Vectra Threat Detection and Response Platform, (anciennement appelé Vectra Cognito) est leur produit phare. Le fournisseur propose également une offre complémentaire de détection et de réponse gérées (MDR), appelée Vectra MDR. Vectra a récemment enrichi son portefeuille avec un produit d'évaluation de la posture de sécurité pour M365, suite à l'acquisition de Siriux Security Technologies au début de 2022.

Vectra Threat Detection and Response Platform analyse principalement les paquets réseau avec des capteurs d'appliances matérielles et des capteurs logiciels virtuels. Vectra travaille également directement avec certaines API SaaS et les journaux des services d'annuaire IaaS cloud pour fournir une détection et une réponse aux menaces pour ces cas d'utilisation. Vectra NDR s'appuie sur plusieurs moteurs de détection mettant fortement l'accent sur le ML et les méthodes d'apprentissage profond pour les détections basées sur le comportement. Un flux propriétaire de renseignements sur les menaces est intégré à l'analyse, et les clients peuvent également importer leurs propres flux de menaces.

- **VMware**

VMware est un fournisseur mondial qui vend principalement des rapports de non-remise aux clients de son hyperviseur ESX lorsqu'ils utilisent également NSX comme commutateur virtuel. Le siège social de VMware est situé à Palo Alto, en Californie. Le produit NDR de VMware, NSX Network Detection and Response, est une acquisition de Lastline.

VMware collecte les données de la carte d'interface réseau virtuelle (vNIC) dans l'hyperviseur, si elle est concédée sous licence pour NSX, ainsi qu'à partir de la passerelle NSX pour irewall et des capteurs NSX. Pour les clients fortement investis dans l'exécution de leurs charges de travail sur les hyperviseurs VMware, il s'agit d'un moyen efficace d'ingérer des données réseau, car NSX ne nécessite pas de capteurs matériels. Le trafic ingéré peut être analysé sur site ou dans le cloud. Le trafic chiffré est analysé de plusieurs façons, y compris l'analyse propriétaire, les signatures JA3 et le déchiffrement TLS.

Pour détecter les menaces, NSX NDR utilise une combinaison de techniques, notamment le ML supervisé et non supervisé, les signatures IPS et un moteur de détection des logiciels malveillants. Le moteur IPS de NSX NDR est basé sur Suricata et inclut un grand nombre de signatures.

- **Autres fournisseurs**
  - Adhérent
  - Allentis
  - aizoOn (Aramis)
  - Blue Hexagon (acquis par Qualys))
  - BluVector
  - CloudCover
  - Réseaux cPacket
  - Cryptoimage
  - GARDE
  - CyGlass
  - Cynamics
  - Instinct profond
  - Exeon
  - Fortinet
  - GREYCORTEX
  - Réseaux Hillstone

- Huawei (en anglais)
- Prises de vues réelles
- Lumu Technologies
- Mode Mixage
- Muninn
- NANO Corp
- Netographie
- NetWitness
- SuivantRayon
- Nominet
- OpenText (Bricata)
- Ordr
- Quad Miners
- Qihoo 360
- Sésame IT
- Cyber stellaire
- TEHTRIS
- ThreatBook
- ThreatWarrior
- Tophant
- Vehere
- Venustech
- Verizon

3 – 3 - XDR : Extended Detection and Response

Face à l'évolution constante du paysage des cybermenaces, la XDR promet de réduire considérablement les temps d'enquête et de réponse des équipes de sécurité. Mais comme pour toute approche innovante, une certaine confusion peut entourer le concept de la XDR, sa différence avec les solutions de sécurité traditionnelles et les résultats de sécurité que les utilisateurs peuvent en attendre. Lisez la suite pour en savoir plus

3 – 3 – 1 – Définitions

La **XDR** ou la détection et la réponse étendues, est une technologie de sécurité à plusieurs niveaux qui protège l'infrastructure informatique. Pour ce faire, elle collecte et met en corrélation des données provenant de plusieurs couches de sécurité, notamment les terminaux, les applications, les emails, les clouds et les réseaux, offrant ainsi une meilleure visibilité de l'environnement technologique d'une entreprise. Les équipes de sécurité peuvent ainsi détecter les cybermenaces, enquêter sur celles-ci, et y répondre rapidement et de façon efficace.

La XDR est considérée comme une version plus avancée de la détection et de la réponse au niveau des terminaux (EDR). Alors que l'EDR se concentre sur les terminaux, la XDR se concentre plus largement sur de multiples points de contrôle de sécurité pour détecter les menaces plus rapidement, en utilisant des analyses approfondies et l'automatisation.

La XDR se distingue des autres outils de sécurité par la centralisation, la normalisation et la mise en corrélation de données provenant de sources multiples – afin de fournir une visibilité complète et de mettre en évidence les menaces avancées.

En collectant et en analysant les données provenant de sources multiples, la technologie XDR permet de mieux valider les alertes, ce qui réduit le nombre de faux positifs et augmente la fiabilité. Cette méthode fait gagner du temps aux équipes de sécurité, et permet des réponses plus rapides et plus automatisées.

La XDR diffère de l'EDR. Les systèmes EDR aident les entreprises à gérer les menaces en se concentrant sur l'activité en cours sur tous leurs terminaux, en utilisant l'apprentissage machine avancé pour comprendre cette activité et définir des réponses, et en utilisant l'automatisation pour prendre des mesures rapides en cas de besoin.

Les systèmes XDR reposent sur ce principe en intégrant des flux de données hors terminaux, comme les réseaux, les emails, les charges de travail dans le cloud, les applications, les appareils, l'identité, les données, l'Internet des objets et bien plus encore. Ces éléments supplémentaires permettent de découvrir un plus grand nombre de menaces, de violations et d'attaques, et de réagir plus efficacement, car vous pouvez piloter des actions sur l'ensemble de votre infrastructure, et pas seulement sur les terminaux. La XDR permet également de mieux comprendre ce qui se passe exactement.

Certaines organisations tentent de gérer les cybermenaces en utilisant une combinaison de solutions EDR et de gestion de l'information et des événements de sécurité (SIEM). Cependant, alors que les solutions SIEM collectent des données superficielles provenant de nombreuses sources, la XDR collecte des données plus profondes provenant de sources ciblées. Ainsi, la XDR fournit un meilleur contexte pour les événements et élimine le besoin de réglage manuel ou d'intégration de données. Les sources d'alertes sont natives de la solution XDR, ce qui signifie que les efforts d'intégration et de maintenance nécessaires à la surveillance des alertes dans un SIEM sont éliminés.

Finalement, plus une menace reste longtemps dans le réseau d'une organisation, plus le pirate informatique a de chances d'endommager les systèmes et de voler des données précieuses. Il est donc crucial d'agir aussi rapidement que possible face à toute menace présumée. Les équipes de sécurité ont besoin de meilleurs outils pour détecter la présence de menaces, ainsi que de moyens plus rapides pour les mettre en évidence et les neutraliser lorsqu'elles se manifestent, afin de réduire les pertes potentielles. En fin de compte, c'est le défi que la XDR est censée relever.

3 – 3 – 2 -Comment la XDR fonctionne-t-elle ?

La XDR renforce l'efficacité de la sécurité en améliorant les capacités de détection et de réponse grâce à l'unification de la visibilité et du contrôle sur les terminaux, le réseau et le cloud.

En connectant les données des solutions de sécurité cloisonnées, la visibilité des menaces est améliorée, et le temps nécessaire pour identifier une attaque et y répondre est réduit. La XDR facilite les enquêtes avancées et la recherche des menaces dans plusieurs domaines à partir d'une seule console.

De manière générale, le fonctionnement de la sécurité de la XDR comporte trois aspects

1. **Collecte de données :** La première étape consiste à rassembler et à normaliser des volumes importants de données provenant des terminaux, des charges de travail du cloud, des emails, du trafic réseau, des conteneurs virtuels et bien plus. Toutes les données sont rendues anonymes et ne comprennent que les éléments indispensables à l'identification des anomalies et des menaces.
2. **Détection :** Ensuite, l'accent est mis sur l'analyse et la corrélation des données pour détecter automatiquement les menaces secrètes à l'aide d'une intelligence artificielle (IA) et d'un apprentissage machine (ML) avancés.
3. **Réponse :** Il s'agit ensuite de hiérarchiser les données relatives aux menaces en fonction de leur gravité, afin que les équipes de sécurité puissent analyser et trier les nouveaux événements en temps utile, et automatiser les activités d'enquête et de réponse. Le processus de réponse devrait se dérouler à partir d'un centre unique, comprenant les données, le contexte et les outils pertinents.

La technologie XDR est utile pour indiquer aux analystes les étapes traversées par un pirate informatique en révélant la séquence des processus avant l'attaque finale. La chaîne d'attaque est complétée par des informations provenant de l'inventaire des ressources, comme les vulnérabilités liées à la ressource en question, le ou les propriétaires de celle-ci, son rôle dans l'entreprise et sa réputation observable grâce à la Threat Intelligence.

3 - 3 – 3 - Pourquoi les entreprises ont besoin de la XDR

La XDR coordonne les outils de sécurité cloisonnés, en unifiant et en simplifiant l'analyse, l'enquête et la réponse. Cette démarche offre des avantages considérables aux organisations, notamment :

- **Visibilité consolidée des menaces :**

La sécurité XDR fournit des données rendues anonymes au niveau d'un terminal en combinaison avec les communications du réseau et des applications. Ces informations portent sur les autorisations d'accès, les fichiers consultés et les applications utilisées. La visibilité totale de votre système vous permet de détecter et de bloquer les attaques plus rapidement.

- **Amélioration des capacités de prévention :**

La Threat Intelligence et l'apprentissage machine adaptatif fournissent une capacité de configuration et de renforcement centralisée avec des conseils permettant de prévenir d'éventuelles attaques.

- **Réponse efficace :**

  La collecte et l'analyse approfondies des données permettent aux équipes de sécurité de tracer le chemin d'accès et de reconstituer les actions du pirate informatique, ce qui augmente les chances d'identifier les auteurs. Ces données fournissent également des informations précieuses que vous pouvez utiliser pour renforcer vos défenses.

- **Meilleur contrôle :**

  La possibilité de bloquer et d'autoriser le trafic et les processus de la liste de blocage garantit que seuls les utilisateurs approuvés effectuant les actions autorisées peuvent accéder à votre système.

- **Amélioration de la productivité :**

  La centralisation réduit le volume des alertes et améliore leur précision, ce qui permet de réduire le nombre de faux positifs à passer au crible. Comme la XDR est une plateforme unifiée et non une combinaison de plusieurs solutions ponctuelles, elle est plus facile à gérer et réduit le nombre d'interfaces auxquelles la sécurité doit accéder pendant une réponse.

- **Restauration des hôtes après une compromission :**

  La XDR peut aider les équipes de sécurité à se remettre rapidement d'une attaque en supprimant les fichiers et les clés de registre malveillants, ainsi qu'en restaurant les fichiers et les clés de registre endommagés à l'aide de suggestions de remédiation.

3- 3 – 4 - Quels sont les avantages de la XDR ?

La technologie de détection et de réponse étendues apporte une valeur ajoutée en regroupant plusieurs outils de sécurité en une plateforme cohérente et unifiée de détection et de réponse aux incidents de sécurité. Voici les principaux avantages de la XDR :

- Consolidation d'un volume important d'alertes en un nombre beaucoup plus restreint d'incidents qui peuvent être classés par ordre de priorité en vue d'une enquête manuelle
- Options intégrées de réponse aux incidents qui fournissent un contexte suffisant pour que les alertes puissent être résolues rapidement
- Options de réponse qui s'étendent au-delà des points de contrôle de l'infrastructure, y compris le réseau, le cloud et les terminaux, afin de fournir une protection complète
- Automatisation des tâches répétitives dans le but d'améliorer la productivité

- Gestion et flux de travail communs à tous les modules de sécurité pour une plus grande efficacité

En résumé, les principaux avantages sont l'amélioration des capacités de protection, de détection et de réponse, l'amélioration de la productivité du personnel de sécurité opérationnel, ainsi que la réduction du coût total de possession pour une détection et une réponse efficaces aux menaces de sécurité.

3 - 3 – 5 – Principales plateformes XDR

➢ Cortex XDR – Palo Alto Networks - Cortex - Palo Alto Networks

Pour une protection étendue de l'infrastructure, Palo Alto propose la première solution étendue Cortex XDR. Cortex XDR combine des informations sur les données des terminaux, du réseau et du cloud pour réduire le travail manuel des administrateurs. Parmi les autres fonctionnalités clés, citons la chasse aux menaces et le renseignement via l'unité 42 du PAN, l'analyse comportementale basée sur le ML et le déploiement rationalisé

Caractéristiques Principales

Détection de problèmes tels que les menaces internes et les attaques d'informations d'identificationÉvaluation des incidents et catégorisation des alertes pour aider les équipes à choisir les problèmes à traiter en premier

Capacités automatisées d'analyse des causes premièresModule de détection et de réponse aux menaces d'identité pour la détection des problèmes des utilisateurs malveillants

Avantages

Fournit des services de recherche et de renseignement sur les menaces par l'entremise de l'Unité 42, une équipe de chercheurs et de consultantsDestiné à simplifier et à unifier les opérations de sécurité d'entreprise pour les réseaux, le cloud, les terminaux et les données tierces

➢ Trend Micro Vision One - https://www.trendmicro.com/fr_fr/what-is/xdr.html

Entrée précoce dans l'espace XDR, Trend Micro propose des services XDR gérés et SaaS depuis 2019. Sa couverture comprend les serveurs, les plates-formes de messagerie, les environnements cloud et les identités des utilisateurs. Vision One produit un lac de données XDR qui collecte des données d'activité telles que les métadonnées, les journaux et la télémétrie, contribuant ainsi à réduire les silos d'informations de sécurité.

Caractéristiques Principales

Recherche automatisée d'indicateurs de compromission

Évaluations dynamiques des risques liés aux menaces et outils de correction automatisésDécouverte de la surface d'attaque qui inclut les domaines Internet, les conteneurs et les réseaux d'entreprise privésCorrélation des menaces provenant de plusieurs sources de sécurit

Avantages

Intégration avec la solution Workload Security de Trend MicroPrise en charge des capteurs de l'Internet des objets (IoT) et de la technologie opérationnelle (OT)

Capacités de gestion des risques liés à la surface d'attaque

- Cynet 360 - https://www.cynet.com/platform/

L'une des plus petites entreprises de notre liste et la plus jeune, Cynet a construit un ensemble impressionnant de solutions comprenant un antivirus (AV), un EDR, un UEBA, une réponse à l'incidence et une analyse de réseau. Ensemble, ces technologies créent la plateforme Cynet 360. Les solutions de Cynet 360 incluent XDR, l'automatisation des réponses et MDR. Les autres fonctionnalités incluent une correction prédéfinie et personnalisée, une console centrale pour une visibilité holistique et une analyse du trafic réseau.

Caractéristiques Principales

Mots de passe leurres, connexions réseau et fichiers de données pour attirer et identifier le comportement des auteurs de menaces
Technologie avancée de chasse aux menaces
Fonctionnalités d'investigation telles que les graphiques et les tableaux de bord pour afficher les données de journal
Corrélation d'événements à partir de plusieurs emplacements, y compris des réseaux, des points de terminaison et des leurres prédéfinis

Avantages

Éloges de la part des clients pour l'équipe de support Cynet
Destiné aux petites équipes de sécurité, avec l'option de détection et de réponse gérées 24h/7 et <>j/<>

- **Faucon Crowdstrike** - https://go.crowdstrike.com/try-falcon-prevent-fr.html?

En moins d'une décennie, CrowdStrike et sa gamme de produits phares Falcon ont changé l'industrie de la cybersécurité. Les analystes estiment que le fournisseur de protection des terminaux et de renseignements sur les menaces est l'un des principaux candidats pour prendre d'assaut le marché XDR. Les plans et fonctionnalités du logiciel Falcon incluent un antivirus avancé, des renseignements sur les menaces et la chasse aux menaces, la gestion des pare-feu, l'EDR et la réponse aux incidents.

Pour les entreprises de toutes tailles, CrowdStrike propose plusieurs plans à plusieurs niveaux et des licences autonomes pour des solutions spécifiques.

Caractéristiques Principales

Intégrations tierces avec les partenaires Technology Alliance de CrowdStrike
Explorateur de graphes qui affiche les modèles d'attaque inter-domaines
Analyse comportementale
Intégrations avec les pipelines CI/CD

Avantages

La solution MDR est bonne pour les petites équipes qui ne disposent pas d'une équipe de sécurité dédiée forte
Solides performances globales de la plate-forme

- Microsoft 365 Defender - https://www.microsoft.com/fr-fr/security/business/siem-and-xdr/microsoft-365-defender

Microsoft 365 Defender offre une solution XDR native du cloud pour les entreprises. Les fonctionnalités XDR de Microsoft incluent la couverture de tous les composants et environnements réseau, les alertes prioritaires et la coordination de la réponse aux menaces. Il y a toujours une incitation financière à se regrouper avec un fournisseur de sécurité, de sorte que la capacité de Microsoft à étendre rapidement ces capacités aux clients existants est un avantage inhérent. Pour les combinaisons SIEM et XDR, 365 Defender s'intègre à Microsoft Sentinel et Defender for Cloud.

Caractéristiques Principales

- Informations sur la sécurité des e-mails
- Tableau de bord unique pour la gestion des incidents et les catégories d'alertes
- Capacités d'auto-réparation automatique
- Fonctionnalités de chasse aux menaces avec requêtes personnalisables

Avantages

- Intégrations avec d'autres solutions Microsoft
- Les clients ont trouvé l'interface utilisateur conviviale

- **SentinelOne Singularity XDR-** https://fr.sentinelone.com/

En 2013, **SentinelOne** a été lancé dans le domaine de la protection des terminaux ; Le mois dernier, le fournisseur a levé 1,2 milliard de dollars lors de son introduction en bourse. Il y a un an, les évaluations MITRE ATT&CK ont montré que SentinelOne détectait 100% des techniques d'attaque, battant Palo Alto et Trend Micro. Pour améliorer les opérations au niveau SOC avec une visibilité de bout en bout de l'infrastructure, SentinelOne propose Singularity XDR. Les fonctionnalités incluent un écosystème d'automatisation facile à utiliser, une fonctionnalité SOAR améliorée et un confinement de la vitesse de la machine.

Caractéristiques Principales

- Options personnalisables de contrôle d'accès basé sur les rôles
- Intégration avec les solutions MFA
- Intégration de l'analyse de données Skylight pour une visibilité accrue des données XDR
- Intégration MITRE ATT&CK

Avantages

- Prise en charge des charges de travail de conteneur natives du cloud
- Facile à déployer
- Bon support client

- **Plateforme de cyberdéfense Cybereason -** https://www.cybereason.com/fr/

Les racines de **Cybereason** sont dans la communauté du renseignement israélien et, bien qu'il s'agisse encore d'une équipe relativement petite, son ascension dans l'industrie de la cybersécurité a été impressionnante. Offrant des services de sécurité gérés EDR tels que la détection et la réponse gérées (MDR) et les évaluations de réseau, Cybereason dispose d'une gamme de solutions de sécurité qui forment la plate-forme de défense Cybereason. En unissant tous les terminaux et en étendant la visibilité sur l'infrastructure réseau, Cybereason offre des contrôles automatisés, des mesures correctives et des renseignements exploitables sur les menaces.

Caractéristiques Principales

Intégrations avec de nombreuses solutions de sécurité, notamment Okta, Fortinet, Palo Alto et Check Point

- Graphiques classant les opérations malveillantes (MalOps) par gravité et état actuel

Histoire complète de l'attaque pour chaque MalOp

Avantages

Interface facile à utiliser

Enquête intensive sur le cycle de vie des menaces

Capacités MDR

- **Cisco SecureX et Secure Endpoint -** https://www.cisco.com/c/fr_fr/products/collateral/security/securex/cisco-xdr-aag.html

Pour les solutions axées sur XDR, Cisco propose SecureX. SecureX s'intègre à Secure Endpoint, ainsi qu'à d'autres solutions Cisco Secure telles que Network Analytics. En plus des fonctionnalités EDR traditionnelles, les fonctionnalités de XDR incluent la gestion avancée des incidents, la veille sur les menaces, l'automatisation et la création de flux de travail low-code. Les avantages de la solution Secure Endpoint incluent la criminalistique des terminaux, l'analyse de l'apprentissage automatique.

Caractéristiques Principales

Création de flux de travail personnalisé low-code avec fonctionnalité glisser-déposer

Playbooks partageables pour les scénarios ITOps, NetOps et SecOps

Graphiques des relations entre les éléments observables dans une enquête sur la menace

Instantanés d'un point dans le temps au cours d'une enquête

Avantages

Visibilité centralisée pour toutes les autres solutions de sécurité Cisco

Gratuit si vous êtes déjà client Cisco Security

- **Mandiant Advantage -** https://www.mandiant.fr/advantage/threat-intelligence

Mandiant – qui fait maintenant partie de **Google** – propose la plate-forme Advantage pour l'espace XDR. L'entreprise est très appréciée pour sa gestion des incidents et ses contributions à la recherche sur les indicateurs de compromission (IOC). Advantage est une plate-forme d'automatisation des équipes de réponse à la sécurité. À l'aide de la science des données et du ML, le logiciel de défense automatisée trie les alertes, met à l'échelle les capacités SOC et effectue des enquêtes précises 24 heures sur 7, <> jours sur <>.

Caractéristiques Principales

Surveillance du dark web

Vues dynamiques de l'hôte et des programmes malveillants

Données sur les acteurs de la menace

Indicateurs OSINT pour identifier les menaces potentielles médiatisées

Avantages

Offre un module complémentaire pour la surveillance des menaces numériques, qui signale les problèmes tels que les informations d'identification divulguées ou les données personnellement identifiables

Plan gratuit

- **Sophos Intercept X -** https://www.sophos.com/fr-fr/products/endpoint-antivirus/xdr

Sophos a progressivement construit un portefeuille diversifié qui comprend l'EDR, les pare-feu, la sécurité du cloud et les services gérés. Sophos Intercept X combine Intercept X Endpoint avec une sélection d'autres produits dans sa solution XDR. Les options de regroupement de solutions incluent des solutions de serveur, de pare-feu, de gestion de la posture de sécurité du cloud et de sécurité des données de messagerie.

Caractéristiques Principales

Fonctionnalités de protection contre les ransomwares très appréciées
Chasse aux menaces 24h/7 et <>j/<> effectuée par les analystes Sophos
Option de ligne de commande pour l'exécution de scripts et la modification des fichiers de configuration
Interface utilisateur facile à comprendre

Avantages

Les utilisateurs trouvent Intercept X facile à utiliser et à gérer
Les produits de sécurité Sophos sont centralisés dans une seule console

3 – 4 - MDR : Managed Detection and Responsa

L'acronyme MDR regroupe les solutions managées (**gérées** par un fournisseur de cybersécurité) et le service de détection et de réponse aux incidents. Les solutions sont opérées par un SOC, interne **ou** externalisé, et permettent d'adresser de bout en bout les menaces cyber.

Grâce à l'automatisation, notamment via l'usage d'un outil d'orchestration (**SOAR** pour Security Orchestration Automation and Response), un analyste peut procéder à une remédiation lorsqu'une menace est détectée et confirmée. Il est également parfaitement possible, selon le niveau de maturité en cybersécurité d'une entité, d'appliquer automatiquement la remédiation.

Ces solutions permettent une accélération du traitement des alertes.

3 – 4 - 1 – Objectifs

Alors que le volume, la variété et la sophistication des menaces de cybersécurité augmentent de manière exponentielle, les organisations ont du mal à maintenir des centres d'opérations de sécurité dotés de personnel et de ressources hautement qualifiés. En conséquence, les fournisseurs de détection et de réponse gérées offrent un menu de services rentables conçus pour améliorer les défenses de cybersécurité d'une entreprise et minimiser les risques sans investissement initial dans la cybersécurité.

Les services MDR fournissent des analystes de niveau de compétence supérieur utilisant des outils de sécurité de pointe et des bases de données mondiales à la minute au-delà de la portée et de la rentabilité de la plupart des budgets, niveaux de compétence et ressources de l'entreprise. Ainsi, aider à suivre le rythme des tactiques et techniques de confrontation en constante évolution.
Les services MDR offrent une alternative aux entreprises à la recherche des derniers produits de sécurité avancés en intégrant des outils de détection et de réponse aux points finaux (EDR) qui deviennent un défi pour les équipes des opérations de sécurité à apprendre et à entretenir.
En conséquence, le niveau de surveillance, de détection et d'analyse des menaces d'une entreprise est amélioré sans le défi et les dépenses nécessaires pour maintenir une équipe de sécurité interne entièrement équipée et à jour avec les dernières données sur les menaces.
Les services MDR ne se limitent pas à de plus grandes capacités de détection et de réponse. Ils fournissent également des renseignements de défense proactifs et un aperçu des menaces avancées aux équipes de sécurité potentiellement débordées. Les niveaux de détection sont améliorés tandis que le temps d'attente des brèches est réduit. Les défis de conformité peuvent également être relevés en utilisant les services MDR fournissant des rapports complets aux parties prenantes et la conservation des journaux sur un large éventail de réglementations et de normes.

3 – 4 – 2 - Avantages des plateformes MDR

Face à des menaces et des campagnes de sécurité apparemment écrasantes, les organisations doivent également faire face à des budgets de sécurité croissants et à un marché du travail difficile qui s'appuie sur des analystes de sécurité qualifiés. Obtenir plus de protection, d'informations et de conformité sans ajouter plus d'outils et de personnes est un objectif recherché par les entreprises de toutes tailles. MDR peut fournir des services de sécurité bénéfiques capables d'atteindre et de maintenir les objectifs d'une organisation :

- **Surveillance** 24h/24 et 7j/7 et mécanismes de communication améliorés avec des analystes SOC expérimentés
- **Des analystes** de sécurité expérimentés supervisent les défenses de votre organisation sans ajouter de personnel et de ressources à temps plein
- **Service complet** de détection et de réponse aux menaces pour les terminaux gérés
- **Détection** des menaces améliorée et couverture de détection étendue
- **Enquête** d'experts sur les alertes et les incidents, et les actions ultérieures
- **Chasse** proactive aux menaces
- **Amélioration** des informations sur les menaces basées sur des indicateurs et des comportements capturés à partir d'informations globales
- **Amélioration** de la réponse aux menaces
- **Diminution** de la réponse aux violations
- **Amélioration** de la criminalistique et des enquêtes de haut niveau

- Gestion des vulnérabilités
- Réponse aux incidents majeurs et gestion des journaux
- Supprimez le fardeau de la gestion quotidienne de la sécurité de votre personnel et de votre budget
- Maintenez l'accès et la personnalisation des défenses de sécurité de votre organisation
- Amélioration de la conformité et des rapports

- Réduction des investissements en sécurité, augmentation du retour sur investissement 3

3 – 4 – 3 – SOAR

➢ définition

Le sigle anglais **SOAR** (Security Orchestration, Automation and Response, que l'on pourrait traduire par Orchestration, automatisation et réponse aux incidents de sécurité informatique) décrit les technologies qui permettent de protéger les systèmes informatiques contre les menaces.

Le SOAR fait référence à trois capacités logicielles clés qu'utilisent les équipes de sécurité :

- la gestion des cas et des workflows,
- l'automatisation des tâches
- la centralisation de l'accès, de l'interrogation et du partage des renseignements sur les menaces.

C'est le cabinet d'études Gartner qui a employé ce sigle pour la première fois. Les analystes de la sécurité désignent le même concept avec des signes différents : **AIRO** (Security Analytics, Intelligence, Response, and Orchestration) pour IDC et **SAO** (Security Automation and Orchestration) pour Forrester.

Le SOAR est généralement mis en œuvre en coordination avec le centre opérationnel de sécurité d'une entreprise. Les plateformes SOAR surveillent les flux de renseignement sur les menaces et déclenchent des réponses automatisées aux problèmes de sécurité, ce qui peut aider les équipes informatiques à maîtriser rapidement et efficacement les menaces sur de nombreux systèmes complexes.

➢ Gestion des cas et des workflows dans le SOAR

Que vous disposiez d'un centre opérationnel de sécurité mature et solidement établi ou que vous commenciez tout juste la transformation de la sécurité dans votre entreprise, les meilleures pratiques en matière de gestion des vulnérabilités imposent que chaque incident de sécurité soit documenté et géré comme un cas. Les pratiques de gestion des cas désignent les méthodes utilisées pour documenter

les incidents et produire les renseignements concernant les menaces. Elles assurent que les menaces sont identifiées, classées par ordre de priorité en fonction du risque et examinées. Elles permettent également de documenter les informations recueillies suite à un incident, et de les partager au sein des entreprises et des communautés.

Les technologies SOAR s'accompagnent souvent de workflows préconfigurés pour les cas d'utilisation courants. Si ces cas d'utilisation par défaut ne répondent pas aux besoins spécifiques de votre entreprise, ils peuvent être personnalisés conformément à vos exigences.

➢ Pourquoi automatiser ?

L'un des principaux avantages de l'automatisation des tâches est qu'elle permet aux équipes de sécurité d'être plus efficaces et d'avoir plus de temps à consacrer à d'autres tâches. Comme il n'y a tout simplement pas assez de professionnels de la sécurité pour répondre aux besoins de toutes les entreprises, l'automatisation peut contribuer à combler cette pénurie de talents en aidant les équipes de sécurité à en faire plus, plus vite.

Les équipes chargées de la sécurité doivent jongler entre plusieurs outils et produits différents, tels que les logiciels de détection et de réponse au niveau des points d'accès (EDR), les pare-feu et les solutions de gestion des informations et des événements de sécurité (SIEM), qui ne sont souvent pas intégrés les uns avec les autres. La gestion manuelle de ces outils peut retarder la détection et la résolution des problèmes, générer des erreurs au niveau de la configuration des ressources et empêcher l'application cohérente des politiques. Les systèmes sont ainsi vulnérables face aux attaques graves et aux problèmes de conformité. L'automatisation permet de rationaliser les tâches quotidiennes et d'intégrer d'emblée la sécurité aux processus, aux applications et à l'infrastructure, comme dans le cadre d'une approche DevOps.

D'après le **Ponemon Institute**, la détection et le contrôle des failles de sécurité en 200 jours ou moins réduisent le coût moyen d'une faille de 1,22 million de dollars en moyenne. La détection rapide des menaces peut réduire la probabilité d'une violation de la sécurité et vous épargner les coûts qui y sont associés, mais l'application de mesures de correction sur plusieurs plateformes et outils peut s'avérer compliquée, longue et source d'erreurs.

Si les processus manuels peuvent retarder l'identification des menaces dans les écosystèmes informatiques complexes, l'automatisation des processus de sécurité aide les entreprises à identifier, valider et faire remonter les menaces plus rapidement, sans intervention manuelle. Les équipes de sécurité peuvent utiliser l'automatisation pour améliorer les temps de réponse et appliquer simultanément des correctifs aux systèmes affectés dans leurs environnements.

3 – 4 – 4 – quelques fournisseurs de plateformes

➢ Comparaison des fournisseurs

Les fournisseurs de services MDR ont tendance à se répartir en trois catégories : Ì

- Surveillance uniquement : Les services se concentrent sur la priorisation et la notification des clients lorsqu'une alerte automatique est générée par le produit. Ils ne proposent pas d'options de remédiation autres que des conseils sur ce que le client doit faire. En outre, ils ne font que tirer parti de la traque des menaces « automatisée » et ne procèdent pas à des investigations ou à une traque proactive au nom du client. Ì
- Réponse limitée ('r' minuscule) : Les services comprennent des actions de réponse plus légères, mais se limitent à des actions automatisées. La traque des menaces est menée, mais uniquement lorsqu'une alerte déclenche l'investigation. Ì
- Réponse complète ('R' majuscule) : Les services comprennent des capacités de réponse complètes. L'équipe MDR agit de manière proactive au nom du client grâce à une réponse manuelle et humaine. La traque des menaces n'est pas seulement menée à partir d'indices, mais l'équipe MDR traque systématiquement les menaces même lorsqu'un indicateur d'attaque n'est pas visible.
- Critères de comparaison (Sophos)

Capacités clés	Surveiller uniquement	Réponse limitée ('r' minuscule)	Réponse complète ('R' majuscule)
Surveillance 24/7	✓	✓	✓
Notification et priorisation	✓	✓	✓
Conseils de remédiation	✓	✓	✓
Rapport d'activité	✓	✓	✓
Traque des menaces 'automatisée'	✓	✓	✓
Réponse automatisée		✓	✓
Traque des menaces à partir d'indices		✓	✓
Traque des menaces sans indices de départ			✓
Réponse managée par des experts			✓

➢ Principaux acteurs

Éditeurs représentatifs[4]		
Surveiller uniquement	Réponse limitée ('r' minuscule)	Réponse complète ('R' majuscule)
Carbon Black Managed Detection	Arctic Wolf	Sophos MTR Standard
CrowdStrike Falcon OverWatch	eSentire	Sophos MTR Advanced
Huntress	Expel	CrowdStrike Falcon Complete
Perch	Rapid7	
	Red Canary	
	SentinelOne Vigilance Respond	

Beaucoups de ces acteurs sont decrits dans des paragraphes précédents car ils offrent souvent des solutions diversifiées adaptées aux clients

- **Sophos** - [Services de sécurité MDR | Solution Sophos MDR]

Sophos MDR est personnalisable avec plusieurs niveaux de service et options de réponse aux menaces. L'équipe Sophos MDR peut au choix réaliser un service complet de réponse aux incidents, travailler avec vous pour gérer les cyber menaces ou avertir votre équipe de sécurité interne dès que des menaces sont détectées. Notre équipe détermine rapidement les qui, quoi et comment d'une attaque. Nous pouvons répondre aux menaces en quelques minutes, avec un temps de résolution des incidents moyen de 38 minutes*.Grâce aux capacités de Sophos XDR (Extended Detection and Response) qui couvrent tous vos besoins de sécurité partout où se trouvent vos données, Sophos MDR peut :

- **Détecter plus de menaces que les outils de sécurité ne peuvent en identifier à eux seuls**

  Nos outils bloquent automatiquement 99,98 % des menaces, ce qui permet à nos analystes de se concentrer sur la chasse aux attaquants les plus sophistiqués, ceux qui ne peuvent être détectés et arrêtés que par un expert hautement qualifié.

- **Identifier la cause profonde des menaces afin de prévenir de futurs incidents**

  Nous prenons des mesures proactives et fournissons des recommandations qui réduisent les risques pour votre entreprise. Moins d'incidents signifient moins de perturbations pour vos équipes informatiques et de sécurité, vos employés et vos clients.

- **Nous prenons des mesures en votre nom pour empêcher les menaces de perturber vos activités**

  Notre équipe spécialisée, composée d'ingénieurs, de chasseurs de menaces, d'ethical hackers et de spécialistes SOC détectent, investiguent et répondent aux menaces en quelques minutes – que vous ayez besoin d'un service

complet de réponse aux incidents ou d'une simple aide pour prendre des décisions précises.

- **Outcome-Focused Security ™**
  Chaque chasse aux menaces, chaque investigation et chaque réponse enrichit le service MDR de données décisionnelles qui permettront d'optimiser automatiquement les configurations et les fonctionnalités de détection. Sophos MDR aide à minimiser les risques pour l'entreprise afin de satisfaire aux exigences des cyberassurances et d'améliorer le retour sur investissement en exploitant les investissements technologiques de cybersécurité existants.

- **Services continus de prévention des ransomwares et des violations**
  Les services Sophos de prévention des ransomwares et des violations peuvent rassurer les entreprises sur le fait que leurs employés, leurs réseaux et leurs données sont protégés 24h/24, 7j/7 et 365j/an contre les violations de données et les attaques de ransomwares coûteuses.

➢ Kudelsky group- https://kudelskisecurity.com/fr/

Kudelski Group est une multinationale basée à Cheseaux-sur-Lausanne[3] en Suisse. Elle est spécialisée dans la sécurité digitale ainsi que les solutions numériques pour la télévision payante et les systèmes d'accès sécurisé. Sa filiale Nagravision a une importante part du marché des décodeurs pour la télévision.
Kudelski Security s'est fixé pour objectif de remettre en question le statu quo en matière de cybersécurité. Il adopte une approche de partenariat pour travailler avec les clients, explorer le défi en profondeur avant de proposer des solutions. De la même manière que chaque client est différent, les solutions fournies par Kudelski Security sont uniques et adaptées aux besoins de chaque organisation, à son profil de menace et à ses objectifs commerciaux. Le portefeuille de solutions de Kudelski Security couvre les principales composantes de la cybersécurité complète, en mettant l'accent sur les catégories de services très demandées et permettant un enrichissement grâce à une innovation propriétaire.

➢ **EXEO** - https://exeo.net/fr/fournisseur-de-services-de-la-detection-et-lintervention-managees-mdr/

Le service MDR (Managed Detection and Response) est un type de service de cybersécurité qui fournit aux organisations des capacités complètes de détection des menaces et de réponse aux incidents. Le service MDR associe des **technologies de sécurité avancées** à **une expertise humaine** pour détecter, enquêter et remédier aux cybermenaces.
Nous proposons un service holistique basé sur la combinaison d'une solution EDR/XDR de pointe et des services d'experts en cybersécurité qui surveillent les menaces en temps réel 24×7 et supervisent les équipements, les applications et les utilisateurs managés depuis notre centre d'opérations de sécurité (SOC). Le service

MDR (EDR managé) offre un ensemble complet de fonctionnalités qui permettent de protéger votre entreprise contre les cyberattaques, de détecter toute menace potentielle et de répondre aux incidents de manière rapide et efficace. En confiant votre cybersécurité à un fournisseur de service MDR comme Exeo, vous pouvez vous concentrer sur vos activités principales et laisser la sécurité aux experts.

- **Countercept** - www.withsecure.com/fr/expertise/campaigns/countercept-mdr . Lorsqu'une cybermenace cible votre entreprise, il ne faut que quelques minutes à l'équipe *Detection and Response* de Countercept pour réagir. Countercept se comporte comme le prolongement de votre personnel de cybersécurité : nous partageons avec vous notre expertise en Threat Hunting et accompagnons votre équipe, pour renforcer en continu votre sécurité.
  - Les Threat Hunters de **WithSecure**™ consacrent jusqu'à 50 % de leur temps à la recherche pour mettre en évidence les nouveaux outils et stratagèmes utilisés par les pirates informatiques. Chaque alerte d'intrusion réseau est examinée par notre équipe de *Detection and Response* (DRT) qui s'appuie sur son expertise pour décider des mesures à prendre.
  - L'agent Endpoint Detection & Response (EDR) et les collecteurs de logs exclusifs de Countercept MDR viennent alimenter notre plateforme de détection xDR. Les données collectées offrent une excellente visibilité sur l'activité des utilisateurs, sur le comportement des endpoints, sur le cloud et le réseau.
  - Le service *First Response* de Countercept MDR, disponible 24h/24, 7j/7, permet de contenir les cyberincidents et d'intervenir avant que des dommages ne soient causés. Notre méthodologie éprouvée *First Response* permet aux Threat Hunters de répondre aux incidents efficacement et au bon moment : à ce jour, moins de 1% des incidents nécessitent une remontée hiérarchique du problème (escalation) à WithSecure™ Incident Response.Nous offrons aux clients une efficacité opérationnelle et une résilience qui leur permet d'atteindre leurs objectifs.

  Nous offrons à nos clients les performances de sécurité et la résilience dont ils ont besoin pour atteindre leurs objectifs commerciaux
- **Countercraft** - https://www.countercraftsec.com/
  CounterCraft permet aux organisations de renforcer leur posture de sécurité plus efficacement que jamais. Conçue et développée par des experts, la plate-forme **CounterCraft Cyber Deception** s'intègre parfaitement dans les stratégies de sécurité existantes et offre une tromperie haut de gamme pour la chasse aux menaces et la détection des menaces à l'aide d'environnements synthétiques contrôlés et hautement crédibles. CounterCraft accélère la détection des menaces plus tôt dans le cycle de vie de l'attaque, fournit des preuves d'activités malveillantes et de modus operandis et protège déjà les principales organisations des secteurs financier, commercial et gouvernemental, ainsi que les organismes d'application de la loi. La plate-forme de cyber-tromperie CounterCraft, riche en fonctionnalités, délivre des alertes de haute qualité sans faux positifs et automatise

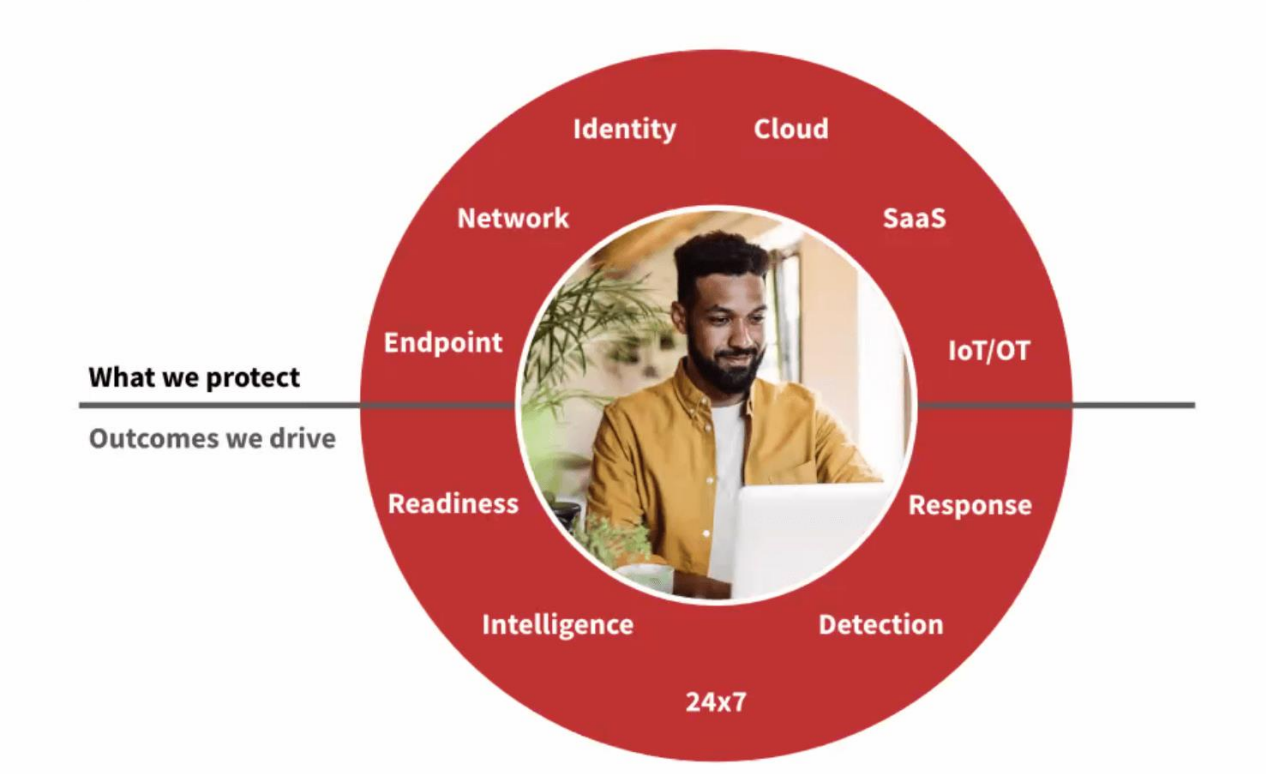
les campagnes de cyber-tromperie sur une gamme complète d'actifs numériques afin de renforcer la posture de sécurité globale.
La solution CounterCraft offre :

- Tromperie haut de gamme (high-end deception)
- Plus que de la détection
- Large portée du contre-espionnage

CounterCraft est reconnu dans le monde entier pour sa contribution radicale au marché des technologies de tromperie et opère dans plus de 20 sociétés de l'indice Fortune500 dans le monde, y compris des institutions financières, des gouvernements et des organismes d'application de la loi.

- **Red Canary -** https://www.redcanary.com/

Red Canary bloque les cybermenaces que personne d'autre ne fait, afin que les organisations puissent poursuivre leurs missions sans crainte. Pour ce faire, nous fournissons une détection et une réponse gérées (MDR) sur les terminaux d'entreprise, les charges de travail cloud, le réseau, les identités et les applications SaaS. En tant qu'allié de la sécurité, nous définissons le MDR selon nos propres termes avec une assistance illimitée 24 heures sur 7, <> ×jours sur <>, une expertise approfondie en matière de menaces, une correction pratique et en faisant ce qui est bon pour nos clients et partenaires.



- **CyberProof -** Services gérés de détection et de réponse – CyberProof

Les équipes de sécurité d'aujourd'hui ont du mal à rester au fait du nombre croissant d'alertes et d'incidents provenant d'attaques de plus en plus sophistiquées et agressives contre leurs organisations.

Grâce aux services MDR avancés de CyberProof, nous pouvons soutenir vos équipes de sécurité en vous aidant à détecter et à répondre plus rapidement aux menaces validées, sans ajouter de complexité à votre infrastructure de sécurité existante. Notre plateforme CyberProof Defense Center (CDC) comprend SeeMo – notre analyste virtuel – qui peut automatiser jusqu'à 85 % de vos activités L1+L2. De la surveillance et de l'enrichissement des alertes au triage, à l'enquête et au confinement des problèmes. Cette combinaison unique d'un analyste virtuel permanent et d'analystes humains experts garantit que les faux positifs et les alertes en double sont éliminés plus rapidement, et que vous êtes en mesure de réagir plus rapidement pour réduire l'impact commercial des attaques réelles. Grâce à notre plate-forme CyberProof Defense Center (CDC) très avancée, votre équipe de sécurité et vos parties prenantes internes peuvent voir exactement ce qui se passe, en toute transparence, dans l'ensemble de votre parc informatique à tout moment. La plate-forme CDC s'intègre parfaitement à vos investissements de sécurité existants et agrège et met en corrélation des volumes illimités de données, quel que soit leur emplacement, en vous les présentant sous la forme d'une vue unique mais complète de toutes les alertes et activités de gestion des incidents

- **Bitdefender -** https://www.bitdefender.com/

BitdefenderManaged Detection and Response **(Bitdefender MDR**) est un service offrant un ensemble d'avantages en matière de sécurité aux organisations, 24 heures sur <>, tous les jours de l'année.
Le service est fourni en combinant les technologies de sécurité de pointe de Bitdefender avec l'analyse humaine. Il s'agit notamment de technologies avancées de prévention des attaques, d'une analyse humaine des détections de sécurité, ainsi que d'actions et de recommandations de réponse personnalisées. Les services MDR de Bitdefender combinent la cybersécurité pour les terminaux, ainsi que l'analyse des réseaux et de la sécurité, avec l'expertise en matière de chasse aux menaces d'un SOC entièrement composé d'analystes de sécurité issus d'agences de renseignement sur plusieurs continents.
Avantages
Bitdefender BitdefenderMDR offre les avantages suivants :

- **Intégration gérée**. Vous bénéficiez d'une gestion de projet et de services professionnels pour être opérationnel et protégé le plus rapidement possible.

- **Gestionnaire de compte de sécurité désigné**. Votre interlocuteur unique pour notre Bitdefender MDR, le Security Account Manager, vous assure de tirer le meilleur parti du service grâce à une approche personnalisée.

- **GravityZone Business Security Enterprise**. Avec Bitdefender BitdefenderMDR, vous obtiendrez un meilleur retour sur investissement et bénéficierez de la prévention et de la détection avancées

de notre solution de sécurité complète, conçue pour vous aider à relever les défis de sécurité au sein de votre organisation.

- **Opérations de sécurité 24h/7 et <>j/<>**. Nous éliminons les frais généraux opérationnels liés à la gestion des alertes et des événements de sécurité. Nos analystes de sécurité proactifs, hautement qualifiés et certifiés, avec une expérience de l'US Air Force, de la US Navy, du British Intelligence et de la NSA, travaillent en partenariat avec vous sur les lignes de front de vos cyberdéfenses.

- **Services de chasse aux menaces**. La chasse aux menaces est essentielle pour réduire le risque de compromission et réduire au minimum le temps d'arrêt. Bitdefender Les laboratoires, les équipes de renseignement sur les menaces et les chercheurs en sécurité surveillent en permanence tous les aspects du paysage mondial des menaces, en utilisant les connaissances acquises pour mener des chasses aux menaces sur vos systèmes.

➢ **PaloAlto – unité 42-** https://www.paloaltonetworks.fr/unit42/respond/managed-detection-response

L'Unité 42 dispose d'une équipe expérimentée d'analystes et de consultants en sécurité qui ont géré certaines des plus grandes cyberattaques de l'histoire. Notre équipe de chasseurs de théats chevronnés, d'experts Cortex XDR et d'experts en renseignement sur les menaces s'associera à votre équipe pour identifier et arrêter rapidement les activités malveillantes les plus susceptibles d'avoir un impact sur votre organisation.

Des couches d'expertise et de protection qui vous donnent confiance, 24 heures sur 7, <> jours sur <>

- Des experts en sécurité de classe mondiale surveilleront en permanence votre environnement Cortex XDR à la recherche de menaces 24 heures sur 7, 365 jours sur <>, <> jours par an, et rechercheront de manière proactive les menaces émergentes dans votre infrastructure.
- Intervention et mesures correctives accélérées
- Les automatisations et les processus propriétaires permettront une réponse plus précise et une correction plus rapide.
- Réduction de la fatigue liée aux alertes

  L'Unité 42 peut gérer les alertes critiques, y compris les alertes de terminaux, de réseau et de cloud, à partir d'un seul écran. Nous pouvons gérer le triage des alertes et l'enquête afin que votre équipe puisse se concentrer sur d'autres initiatives plus stratégiques.
- Amélioration de la posture de sécurité

Voyez la valeur immédiate avec les rapports de cyberhygiène avec des conseils personnalisés sur la façon de renforcer votre posture de sécurité.

➢ **Crowdstrike** – https://www.crowdstrike.fr/

CrowdStrike Falcon® Complete pour la détection et l'intervention managées (MDR) combine la puissance de la plateforme de sécurité Falcon, cloud native et à la pointe du secteur, avec l'efficacité, l'expertise et la protection 24 h/24 et 7 j/7 de l'équipe internationale d'experts en sécurité de CrowdStrike, qui surveille, trie et neutralise en continu les menaces ciblant les entreprises de nos clients.
Fonctionnalités

Service MDR Falcon Complete Gestion,

Adaptation et optimisation 24 h/24 et 7 j/7

- Gestion par des experts
- Gestion proactive de la plateforme
- Conseiller en sécurité attitré
- Priorisation des groupes de ressources
- Expertise pluridisciplinaire

Détection et prévention

- Surveillance continue avec visibilité en temps réel
- Investigation de toutes les détections (gravité faible/moyenne/élevée/critique)
- Données, outils et processus spécialisés
- Protection managée des workloads cloud
- Prévention managée des menaces liées à l'identité

Threat Hunting et recherche de menaces

- Recherche de menaces native et indicateurs de compromission intégrés
- Rapports de Threat Hunting trimestriels
- Visibilité totale sur l'arborescence de tous les endpoints
- Threat Hunting proactif par une équipe d'experts, 24 h/24 et 7 j/7

Threat Hunting proactif par une équipe d'experts, 24 h/24 et 7 j/7

- Isolation et confinement de toutes les menaces
- Correction ultraprécise, interactive et proactive

- **NOMIOS** – https://www.nomios.com/managed-service/mdr

Nomios fournit une détection et une réponse gérées (MDR) pour minimiser les cyber-risques auxquels votre organisation est exposée. Nos centres d'opérations de sécurité en Europe surveillent votre infrastructure numérique jour et nuit pour détecter d'éventuelles tentatives d'intrusion. Nos experts en sécurité et nos spécialistes réseau utilisent les dernières technologies pour protéger votre organisation contre les cybermenaces.
Nomios propose des solutions de détection et de réponse gérées pour protéger les entreprises contre les attaques numériques. Nos centres d'opérations de sécurité (SOC) enquêtent sur les activités anormales sur les réseaux afin de reconnaître les attaques à un stade précoce et d'aider les entreprises à se conformer aux lois et réglementations.
Combinant seize ans d'expérience en matière de réseau et de sécurité, notre équipe possède une connaissance approfondie du paysage actuel des menaces. Les experts en sécurité de nos SOC surveillent de près votre réseau en observant en permanence les événements, les fichiers journaux et le trafic réseau. Forts d'années d'expérience dans la détection d'attaques avancées et de menaces internes, les experts en sécurité ont développé des centaines de règles de détection capables de détecter les activités suspectes en une fraction de seconde.

Grâce aux technologies avancées SIEM et SOAR renforcées par la Threat Intelligence et le Machine Learning, les experts en sécurité sont en mesure de prendre des mesures rapidement et efficacement. De cette façon, votre organisation n'a plus à s'inquiéter des faux positifs. Si des anomalies et des modèles à risque sont découverts qui pourraient être le signe d'une cyberattaque, une enquête approfondie sera menée pour identifier les systèmes ou les employés à risque. En agissant rapidement et de manière adéquate et en informant les bonnes personnes au sein de votre organisation, nous sommes en mesure de minimiser les risques associés aux cybermenaces.

- **Fortinet -** Services gérés de détection et de réponse (MDR) FortiGuard | Fortinet
  Le service **FortiGuard** Managed Detection and Response (MDR) est conçu pour les clients des plates-formes avancées de sécurité des terminaux **FortiEDR** et **FortiXDR**. Les services MDR fournissent aux organisations une surveillance continue 24h/7 et <>j/<> des alertes et des menaces détectées par FortiEDR. Les experts Fortinet examinent et analysent chaque alerte, traquent les menaces de manière proactive et prennent des mesures pour s'assurer que les clients sont protégés en fonction de leur profil de risque. L'équipe fournit également des conseils et les étapes suivantes aux intervenants en cas d'incident et aux administrateurs informatiques, au besoin.
  FortiGuard Labs compte plus de 500 chercheurs et analystes experts, qui étudient tous les domaines critiques du paysage des menaces, y compris les logiciels malveillants, les botnets, les mobiles et les vulnérabilités zero-day. Les services MDR FortiGuard tirent parti de cette vaste expérience et expertise, en complétant votre équipe SOC et en agissant en tant qu'analystes SOC seniors pour garantir la sécurité de vos terminaux.

- Une liste des fournisseurs représentatifs est fournie dans le tableau ci-dessous. Il ne s'agit pas d'une liste de tous les fournisseurs du marché des services MDR. Il ne s'agit pas, ni n'est destiné à être, d'une analyse concurrentielle des fournisseurs.

Tableau 1 : Fournisseurs représentatifs

Ackcent	https://ackcent.com/
Aiuken	https://www.aiuken.com/
ArcticWolf	https://arcticwolf.com/
Atos	https://atos.net/en/solutions/cyber-security
Binary Defense	https://www.binarydefense.com/
Bitdefender	https://www.bitdefender.com/
BlueVoyant	https://www.bluevoyant.com/
Critical insight	https://www.criticalinsight.com/
CriticalStart	https://www.criticalstart.com/
Crowdstrike	https://www.crowdstrike.com/
Cybereason	https://www.cybereason.com/
Cyberoo	https://cyberoo.com/
Cyderes	https://www.cyderes.com/

Cysiv	https://www.forescout.com/cysiv/
DeepSeas	https://www.deepseas.com/
DeepWatch	https://www.deepwatch.com/
Esentire	https://www.esentire.com/
Expel	https://expel.com/
Fortra	https://www.fortra.com/
Integrity360	https://www.integrity360.com/
IBM	https://www.ibm.com/fr-fr/
Kroll	https://www.kroll.com/en
Kudelski Security	https://kudelskisecurity.com/
Mandiant	https://www.mandiant.com/
Microsoft defender	https://www.microsoft.com
Mnemonic	https://www.mnemonic.io/
Nccgroup	https://www.nccgroup.com/
Obrela	https://www.obrela.com/
OpenSystems	https://www.open-systems.com/ - division (Ontinue)
Optiv	https://www.optiv.com/
Orange	https://www.orangecyberdefense.com/
Pondurance	https://www.pondurance.com/
Proficio	https://www.proficio.com/
Quorum Cyber	https://www.quorumcyber.com/
Rapid7	https://www.rapid7.com/
Red Canary	https://redcanary.com/
Secureworks	https://www.secureworks.com/ - plateforme Taegis
Sophos	https://www.sophos.com
Trustwave	https://www.trustwave.com/en-us/services/managed-detection-and-response/
Verizon	https://www.verizon.com/
WithSecure	https://www.withsecure.com/en/home

4 – CSIRT / CERT

4 – 1 – Définition du CSIRT

CSIRT signifie Computer Security Incident Response Team. Il s'agit d'un groupe spécialisé au sein d'une organisation chargée de coordonner et de répondre aux incidents de sécurité informatique. L'objectif principal d'un CSIRT est de protéger les actifs informationnels de l'organisation, y compris ses systèmes informatiques, ses réseaux et ses données, contre les menaces et les failles de sécurité

Un CSIRT est généralement composé d'une équipe de professionnels qualifiés ayant une expertise dans divers domaines de la cybersécurité. Leurs principales responsabilités comprennent :

- **Détection et surveillance des incidents** : les CSIRT surveillent activement le réseau et les systèmes de l'organisation à la recherche de signes d'incidents de sécurité, tels que des tentatives d'accès non autorisées, des infections par des

logiciels malveillants ou un trafic réseau inhabituel. Ils utilisent divers outils et techniques pour détecter et analyser les menaces potentielles.

- **Réponse aux incidents** : Lorsqu'un incident de sécurité est identifié, le CSIRT est chargé de lancer un processus de réponse aux incidents bien défini. Cela implique de contenir rapidement l'incident, d'enquêter sur son ampleur et son impact, d'atténuer toute menace en cours et de rétablir les opérations normales le plus rapidement possible.

- **Threat Intelligence** : les CSIRT recueillent en permanence des informations sur les dernières menaces, vulnérabilités et techniques d'attaque en matière de cybersécurité. Ils analysent ces renseignements sur les menaces pour comprendre l'évolution du paysage des cybermenaces et adapter leurs stratégies de défense en conséquence.

- **Gestion des vulnérabilités** : les CSIRT travaillent en étroite collaboration avec d'autres équipes de l'organisation, telles que les équipes d'exploitation et de développement informatiques, pour identifier et résoudre les vulnérabilités des logiciels, des systèmes et de l'infrastructure. Ils coordonnent les évaluations de vulnérabilité, effectuent des tests de pénétration et s'assurent que les correctifs et mises à jour appropriés sont appliqués pour atténuer les risques potentiels.

- **Signalement et documentation des incidents** : les CSIRT conservent des enregistrements détaillés des incidents de sécurité, y compris les mesures prises, les leçons apprises et les recommandations pour améliorer la posture de sécurité de l'organisation. Ces rapports aident à évaluer l'efficacité des efforts de réponse aux incidents et à identifier les domaines à améliorer.

- **Coordination des incidents** : dans le cas de grandes organisations ou en cas d'incidents de sécurité importants, les CSIRT collaborent avec des parties prenantes externes, telles que des organismes chargés de l'application de la loi, des pairs de l'industrie ou des fournisseurs de cybersécurité. Ils facilitent le partage d'informations, coordonnent les efforts de réponse et s'assurent que les exigences légales et réglementaires appropriées sont respectées.

Les CSIRT jouent un rôle crucial dans l'amélioration de la résilience de la cybersécurité d'une organisation en fournissant une approche centralisée et coordonnée de la réponse aux incidents. Ils aident à minimiser l'impact des incidents de sécurité, à protéger les actifs critiques et à améliorer les capacités globales de réponse aux incidents.

4 – 2 - Structure d’un CSIRT

Un CSIRT est une équipe chargée de la gestion des incidents de sécurité informatique au sein d'une organisation. Voici un aperçu de la structure typique d'un CSIRT :

Responsable du CSIRT : Il s'agit de la personne responsable de la gestion globale de l'équipe CSIRT. Le responsable définit les objectifs stratégiques, coordonne les activités de l'équipe et assure la liaison avec la direction de l'organisation.

- **Analystes de sécurité** : Ce sont les membres principaux de l'équipe CSIRT. Les analystes de sécurité sont chargés de surveiller les systèmes et les réseaux de l'organisation, de détecter les incidents de sécurité, d'analyser leur impact et de prendre des mesures pour les contenir et les résoudre. Ils utilisent des outils de détection d'intrusion, des systèmes de gestion des journaux, des sondes de sécurité, etc.

- **Coordinateurs d'incident** : Ces membres sont responsables de la gestion opérationnelle des incidents de sécurité. Ils coordonnent les activités de l'équipe CSIRT lorsqu'un incident est détecté, y compris la communication avec les parties prenantes internes et externes, l'escalade des problèmes et la planification des réponses.

- **Experts techniques** : Les experts techniques sont des spécialistes dans différents domaines de la sécurité informatique, tels que la cryptographie, les réseaux, la gestion des vulnérabilités, les logiciels malveillants, etc. Ils apportent une expertise spécifique pour aider à résoudre les incidents complexes et à renforcer la sécurité globale de l'organisation.

- **Chercheurs en sécurité** : Certains CSIRT disposent également de chercheurs en sécurité qui sont responsables de la veille sur les nouvelles menaces, les vulnérabilités et les techniques d'attaque émergentes. Ils analysent les tendances de la sécurité, évaluent les outils et les méthodes de défense, et contribuent à l'amélioration continue des capacités du CSIRT.

- **Personnel de soutien** : En plus des membres principaux, un CSIRT peut également compter sur du personnel de soutien administratif et technique. Ils assurent la logistique, la documentation, la gestion des outils, la planification des ressources et d'autres tâches nécessaires au bon fonctionnement de l'équipe.

Il est important de noter que la structure et les rôles spécifiques peuvent varier d'une organisation à l'autre, en fonction de la taille, des objectifs et des besoins en matière de sécurité. Certaines organisations peuvent avoir un CSIRT interne, tandis que d'autres peuvent externaliser certains aspects de leur gestion des incidents à des fournisseurs de services de sécurité**.**

4 - 3 – qu’est - ce qu’un CERT

CERT signifie Computer Emergency Response Team. Il s'agit d'un groupe ou d'une organisation chargée de répondre et de coordonner le traitement des incidents de sécurité

informatique. Les CERT sont généralement créés pour aider à prévenir, détecter et répondre aux menaces et incidents de cybersécurité au niveau national ou organisationnel. À la suite de la création de la première équipe CERT par l'autorité responsable du réseau Arpanet (DARPA – Defense Advanced Research Projects Agency), une structure permanente a été fondée, le CERT Coordination Center (Computer Emergency Response Team). L'appellation **CERT devient alors une marque déposée** aux États-Unis par l'Université Carnegie-Mellon.
Ainsi, l'appellation CSIRT est alors privilégiée dans beaucoup de pays étant libres de droits. Cependant, les CSIRT qui en font la demande et qui obtiennent l'autorisation peuvent utiliser le terme CERT au sein de leur nom, par exemple le CERT-FR.
La fonction principale d'un CERT est de fournir des services de réponse aux incidents, y compris l'analyse et l'atténuation de l'impact des incidents de sécurité tels que les intrusions sur le réseau, les infections par des logiciels malveillants, les violations de données et autres cyberattaques. Les CERT agissent souvent comme un point de contact central pour signaler les incidents et offrent une assistance et des conseils aux parties concernées.

Les CERT jouent également un rôle essentiel dans la promotion de la sensibilisation, de l'éducation et des meilleures pratiques en matière de cybersécurité au sein de leurs communautés respectives. Ils peuvent proposer des programmes de formation, des ateliers et des ressources pour aider les individus et les organisations à améliorer leur posture de sécurité et à se défendre contre les cybermenaces.

Divers pays et organisations ont leurs propres CERT. Parmi les exemples les plus marquants, citons l'équipe de préparation aux urgences informatiques des États-Unis (US-CERT), le centre de coordination de l'équipe d'intervention en cas d'urgence informatique (CERT/CC) de l'Université Carnegie Mellon et le CERT de l'Agence de l'Union européenne pour la cybersécurité (ENISA).

4 – 4 - différences entre CSIRT et CERT

L'équipe de réponse aux incidents de sécurité informatique (CSIRT) et l'équipe d'intervention d'urgence informatique (CERT) sont toutes deux responsables de la gestion et de la réponse aux incidents de sécurité, mais elles diffèrent dans leur objectif et leur portée. Voici une ventilation des différences entre les deux:

- **Focus** : le CSIRT se concentre principalement sur les incidents liés à la sécurité informatique, tandis que le CERT traite un plus large éventail d'urgences, notamment les catastrophes naturelles, les atteintes à la sécurité physique et les cybermenaces.

- **Portée** : CSIRT opère généralement au sein d'une organisation ou d'une entreprise spécifique, en se concentrant sur les incidents qui se produisent au sein de son réseau ou de son infrastructure. En revanche, les CERT sont souvent établis au

niveau national ou international et desservent plusieurs organisations, secteurs ou même des pays entiers.

- **Expertise** : les membres du CSIRT possèdent des connaissances et des compétences spécialisées en sécurité informatique, y compris la surveillance du réseau, l'évaluation des vulnérabilités, l'analyse médico-légale et la réponse aux incidents. Les équipes CERT ont une expertise plus large qui englobe diverses disciplines de gestion des urgences, telles que la réponse aux incidents, la communication de crise, la reprise après sinistre et la planification de la résilience.

- **Coordination** : les CSIRT coordonnent principalement les réponses aux incidents de sécurité au sein de leur organisation. Ils travaillent en étroite collaboration avec les parties prenantes internes, telles que les services informatiques, les équipes juridiques et la direction, pour gérer et atténuer efficacement les incidents. Les CERT, d'autre part, jouent souvent un rôle de coordination entre plusieurs organisations, facilitant le partage d'informations, les meilleures pratiques et les efforts collaboratifs de réponse aux incidents.

- **Rapports** : les CSIRT se concentrent généralement sur la documentation et le signalement des incidents de sécurité au sein de leur organisation. Ils fournissent des résumés d'incidents, des analyses et des recommandations pour améliorer les mesures de sécurité. Les CERT peuvent également s'engager dans le signalement d'incidents, mais ils ont souvent un mandat plus large pour analyser les tendances, développer des systèmes d'alerte précoce et diffuser des informations sur les menaces dans plusieurs secteurs ou régions.

- **Engagement** : les CSIRT interagissent généralement avec les parties prenantes internes, telles que les employés, les équipes informatiques et la direction, pour dispenser une formation de sensibilisation à la sécurité, effectuer des exercices et garantir le respect des politiques de sécurité. Les CERT collaborent avec diverses parties prenantes externes, notamment des agences gouvernementales, des forces de l'ordre, des organisations du secteur privé et des partenaires internationaux, pour promouvoir la collaboration en matière de réponse aux incidents, partager des renseignements et améliorer les capacités de cybersécurité.

Il convient de noter que les termes CSIRT et CERT sont parfois utilisés de manière interchangeable et que les rôles et responsabilités spécifiques peuvent varier en fonction de l'organisation et du contexte dans lequel ils opèrent.

4 - 5 – Plates formes

4 – 5 - 1 – CSIRT Régionaux

Issus d’un projet du plan France Relance en 2021, les CSIRT sont des centres de réponse aux incidents cyber au profit des entités implantées sur le territoire régional. Ils traitent les demandes d’assistance des acteurs de taille intermédiaire (ex : PME, ETI, collectivités territoriales et associations) et les mettent en relation

avec des partenaires de proximité : prestataires de réponse à incident et partenaires étatiques.
L'émergence de ces CSIRT doit permettre de fournir localement un service de réponse à incident de premier niveau gratuit, complémentaire de celui proposé par les prestataires, la plateforme Cybermalveillance.gouv.fr et les services du CERT-FR.
Ces équipes portent également des missions de prévention, sensibilisation et d'accompagnement dans la montée en maturité des acteurs de leurs territoires.
Les CSIRT régionaux ont pu bénéficier d'un financement France Relance ainsi que d'un accompagnement méthodologique sous la forme d'un parcours d'incubation.
Le dispositif est constitué de 12 CSIRT régionaux, avec la liste des centres désormais ouverts ci-dessous :

Bourgogne-Franche-Comté	CSIRT Bourgogne-Franche-Comté
Centre-Val de Loire	CybeRéponse
Grand Est	Grand Est Cybersécurité
Hauts-de-France	CSIRT Hauts-de-France
Normandie	Cybersécurité - AD Normandie
Nouvelle-Aquitaine	https://www.campuscyber-na.fr
Occitanie	https://www.cyberocc.com/en-cas-durgence

4 - 5 – 2- Différents types de CERT

- **CERT gouvernementaux ou publics :**

  - CERT-FR (anciennement CERTA appartenant à l'ANSSI / SGDSN) est le CERT affecté au secteur de l'administration française[6] ;
  - CERT Santé [archive] est le CERT du secteur de la santé en France, il est opéré par l'ANS
  - CERT-PJ : CERT de la Police Judiciaire
  - CERT-RENATER : CERT de la communauté des membres du GIP RENATER (Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche) ;

- **CERT privés**
  - Airbus – AXA – crédit agricole – Société Générale – Areva- Banque de France
  - Paribas – Bouygues – Caisse des depots et consignation – BPCE – la Poste –
  - Michelin- groupe Orange – SNCF – Thalès - Cyberdian
- **CERT public (commercial)**
  - **CERT-Axians** - https://cert.axians.com
  - **CERT-Akaoma** - https://www.akaoma.com/cert-akaoma
  - **CERT-AlgoSecure** - https://www.algosecure.com/cert

- **CERT-AMOSSYS - https://www.amossys.fr/fr**
- **CERT- ATOS – ex UBIK-** https://atos.net/f/solutions/cybersecurite/
- **CERT- SOPRASTERIA (EVA Group) - https://www.soprasteria.com/fr/**
- **CERT-CS -** https://www.csgroup.eu/fr/offres-solutions/cybersecurite
- **CERT- CWATCH** – group Almond -https://almond.eu
- **CERT- CYBERPROTECT**- https://www.cyberprotect.one
- **CERT-DEVOTEAM** - https://france.devoteam.com
- **CERT-Intrinsec** - https://www.intrinsec.com
- **CERT-IST** : (Alcatel , CNES , ELF,France Telecom) opéré par Thalès - https://www.cert-ist.com
- **CERT-LEXSI** - https://www.orangecyberdefense.com/fr/
- **CERT-OPMD** – (rachat par Accenture**) -** https://www.accenture.com/fr/
- **CERT-Sogeti** - https://www.sogeti.com/services/cybersecurity
- **CERT-W** - https://www.wavestone.com/fr/
- **CERT-XMCO** - https://www.xmco.fr/

5 – MSSP – Manager Security service Provider

5 – 1- definition MSSP

Au cours des années 90, l'utilisation d'Internet dans les entreprises s'est intensifiée, et le nombre de cyberattaques contre leurs systèmes informatiques aussi. Les fournisseurs d'accès à Internet commencèrent à proposer certains services de sécurité à leurs clients sous forme de solutions dites de pare-feu gérés. L'objectif était alors de permettre aux utilisateurs de surfer en toute sécurité sans devoir eux-mêmes se méfier en permanence des cyberattaques. Les premiers services de sécurité gérés (MSS) étaient nés, faisant des fournisseurs d'accès à Internet les premiers fournisseurs de services de sécurité gérés (**MSSP**).. Pour ce faire, l'entreprise a le plus souvent recours à tout un lot de services **MSS** qui sont mis en œuvre à distance, gérés et régulièrement mis à jour par le prestataire de services de sécurité concerné. Cela va du scanner antivirus à la gestion des logiciels, en passant par la protection contre les logiciels malveillants. Pour ce faire, le MSSP dispose d'un vaste accès aux interfaces importantes au sein de l'infrastructure informatique, généralement via un client VPN ou directement via Internet. Dans le même temps, les spécialistes de la cybersécurité d'une entreprise peuvent également contrôler eux-mêmes les différents services de sécurité gérés (MSS) via une plateforme en ligne correspondante et intervenir activement si besoin est.

5 – 2 – différence entre MSP et MSSP

MSP (Managed Service Provider) et MSSP (Managed Security Service Provider) sont deux types de fournisseurs de services qui offrent des services gérés aux entreprises. Cependant, ils diffèrent par leur objectif principal et l'étendue des services qu'ils fournissent. Voici un aperçu des différences entre MSP et MSSP :

Fournisseur de services gérés (MSP) :

- **Présentation** : Un MSP est une entreprise ou une organisation qui fournit une large gamme de services proactifs de gestion et de support informatique aux entreprises. Ils assument la responsabilité de la gestion et de la surveillance de l'infrastructure informatique du client, y compris le matériel, les logiciels, les réseaux et les systèmes.
- **Focus** : les MSP se concentrent sur la fourniture de services informatiques complets, tels que la surveillance du réseau, la maintenance du système, la sauvegarde et la récupération des données, les mises à jour logicielles, le support technique et le conseil informatique général. Leur principal objectif est d'assurer le bon fonctionnement et l'efficacité de l'environnement informatique du client.
- **Services** : les MSP proposent généralement une large gamme de services couvrant divers aspects de la gestion informatique, notamment la gestion de l'infrastructure, l'informatique en nuage, le stockage des données, l'administration du réseau et l'assistance aux utilisateurs finaux. Ils peuvent également fournir des services tels que l'achat de matériel et de logiciels, l'octroi de licences et la gestion des fournisseurs.

Fournisseur de services de sécurité gérés (MSSP) :

- **Présentation** : un MSSP est un type spécialisé de fournisseur de services qui se concentre sur la fourniture de services de sécurité gérés aux entreprises. Leur objectif principal est de protéger les systèmes informatiques et les données du client contre les menaces de cybersécurité.
- Focus : les MSSP se spécialisent dans l'offre de services liés à la sécurité, tels que la surveillance des menaces, les évaluations de vulnérabilité, la détection et la prévention des intrusions, la réponse aux incidents, la gestion des informations et des événements de sécurité (SIEM) et le conseil en sécurité. Ils accordent la priorité à la protection de l'infrastructure, du réseau et des données du client contre les failles de sécurité et les attaques.
- Services : les MSSP fournissent une gamme de services axés sur la sécurité conçus pour atténuer les risques et améliorer la posture de sécurité du client. Ces services peuvent inclure la gestion du pare-feu, des solutions antivirus et anti-malware, le cryptage des données, le contrôle d'accès, les audits de sécurité et la gestion de la conformité. Les MSSP exploitent souvent des technologies et des outils de sécurité avancés pour détecter, prévenir et répondre aux incidents de sécurité.

En résumé, les MSP offrent des services complets de gestion et de support informatique, tandis que les MSSP se spécialisent dans la fourniture de services de sécurité gérés pour protéger les entreprises contre les menaces de cybersécurité. Alors que les MSP se concentrent sur l'infrastructure informatique globale, les MSSP se concentrent spécifiquement sur la sécurisation des systèmes et des données du client contre les risques potentiels.

5 – 3 – Différence entre MDR et MSSP

Les petites entreprises, en particulier, n’ont souvent pas les moyens de mettre en place leur propre centre opérationnel de sécurité (SOC) avec le personnel informatique et les outils de sécurité informatique correspondants.

.

Les services sous-traités de supervision et de résolution des incidents de sécurité peuvent également être mis en œuvre au moyen d'un service de Managed Detection and Response (**MDR**). Il s'agit d'une forme relativement récente de services de sécurité gérés en externe et surtout utilisés pour la protection des terminaux. Les MDR réagissent principalement aux cyberattaques des logiciels d'achat standard. Les entreprises qui doivent faire le choix entre ces deux prestataires de services se basent au final toujours sur les problèmes qui doivent être résolus par l'assistance externe. Si un SOC ou une équipe de sécurité est déjà en place et qu'une assistance externe est nécessaire, la meilleure solution est probablement de faire appel à un MSSP. Les petites entreprises qui ne disposent pas du budget ou de la main-d'œuvre requise préféreront plutôt se tourner vers un fournisseur MDR pour répondre à leurs propres besoins de base en matière de sécurité.

5 – 4 – Fonctions principales

Aperçu des fonctions principales du MSSP :

- supervision et gestion sous-traitées des réseaux d'entreprise, des systèmes informatiques et de leurs points de terminaison ;
- supervision, gestion et contrôle des services de sécurité informatique sur la base d'une gestion des informations et des événements de sécurité (SIEM) ;
- gestion des réponses aux incidents 24 heures sur 24, par exemple en cas de cyberattaques, de phishing, d'attaques par e-mail, de rançongiciels ou de logiciels malveillants ;
- intégration et sécurisation des infrastructures basées sur le cloud ;
- détection proactive des failles de sécurité ;
- identification des cyberattaques et défense contre celles-ci ;
- mise à disposition d'outils de sécurité, tels qu'un scanner antivirus, un pare-feu, etc. ;
- exécution autonome de mises à jour de logiciels, de modifications de systèmes ou de réseaux ;
- développement et mise à disposition de politiques de sécurité informatique, de catalogues de mesures et de processus de sécurité ;
- allègement de la charge de travail du personnel informatique et réduction des coûts en cas de sinistre ;
- service complet sous forme d'un centre des opérations de sécurité (SOC) sous-traité.

5 – 5 – Exigences en termes de Cybersécurité d'un MSSP

- **Une efficacité opérationnelle maximale :** grâce à des processus de sécurité automatisés et à une infrastructure de sécurité informatique mise en œuvre de façon optimale
- **Des tableaux de bord MSSP clairs :** une interface utilisateur personnalisable pour garantir une expérience client optimale et une charge administrative minimale
- **Une assistance 24 h/24 et 7 j/7 :** un centre des opérations de sécurité (SOC) disponible 24 h/24 et 7 j/7 et un accès direct aux connaissances spécifiques au secteur des experts en sécurité informatique pour aider rapidement l'équipe de sécurité informatique en cas de cyberattaque critique

- **Des temps de réaction courts :** des processus de travail et de sécurité informatique les plus efficaces possibles pour corriger les failles de sécurité
- **Une flexibilité et une évolutivité maximales :** des services de sécurité standardisés et modifiables ou des solutions de sécurité MSS gérées qui peuvent être facilement adaptées aux besoins individuels de l'entreprise
- **Accès en ligne permanent :** threat intelligence et recherche efficace de menaces pour combattre les menaces en temps réel
- **Solution de sécurité informatique complexe :** association intelligente d'experts en sécurité informatique, de technologies de sécurité informatique basées sur l'IA et de services de Managed Detection and Response (MDR) ou de services de gestion des réponses aux incidents
- **Automatisation complète ou semi-automatisation :** pour une détection, une supervision et une lutte efficaces contre les menaces de sécurité, ainsi que pour la gestion et la mise à jour optimales de toutes les solutions de sécurité informatique
- **Gestion de cas performante :** des processus de travail et de sécurité automatisés pour une collaboration efficace entre le SOC du MSSP et l'entreprise

5 – 6 -Principaux fournisseurs de services de sécurité gérés MSSP

- **Cypher -** https://cipher.com/blog/cipher-security-name
- **SecureWorks -** https://www.secureworks.com/
- **IBM -** https://www.ibm.com/in-en
- **Verizon -** https://www.verizon.com/business/en-au/?cpur=1
- **Accenture (ex-Symantec) –** https://www.accenture.com/dk-en/services/security/cyber-strategy
- **Alert Logic –** https://www.alertlogic.com/managed-security-services/
- **AT&T –** https://cybersecurity.att.com/sentinel-one
- **Capgemini –** https://www.capgemini.com/services/cybersecurity/
- **Deloitte** – https://www2.deloitte.com/fr/fr/services/risk-advisory/cyber-risk.html
- **Fujitsu –** https://fujitsu.com/global/services.security/offering/managed
- **Lumen –** https://www.lumen.com/en-us/managed-it-services/managed-security.html
- **NTT-** https://services.global.ntt/fr-fr/services-and-products/security/managed-security-services
- **Optiv -** https://www.optiv.com/insights/discover/videos/optivs-managed-security-services
- **Trustwave –** https://www.trustwave.com/en-us/services/managed-security-services/
- **Wipro -** https://www.wipro.com/cybersecurity/managed-security-services/

Annexe 1 : Theart-intelligence :

1 documents Asprom (onglet application)

- Threat-Intelligence – 2023 –: Quand, Quoi,Comment . https://www.asprom.com/application/Thread.pdf
- **WatchGuard** – **2023** – Accéder à l'univers du **XDR –** https://www.asprom.com/application/XDR.pdf
- **Sophos – guide d'achat des services MDR** https://www.asprom.com/application/sophos2.pdf
- **Gartner** – 2023- Guide du marché des services de détection et de réponse gérés – https://www.asprom.com/application/gartner.pdf
- **Gartner – 2022 –** Guide du marché pour la détection et réponse réseau- NDR – https://www.asprom.com/application/GartnerA1.pdf
- **Exodata** – 2022 : Le **SOC** (livre blanc)- (application)
- **Kaspersk**y - 2020 : Faire vivre un **SOC** (livre blanc)
- **Cyberark** – 2020 – Etude de la combinaison EDR-EPM
- **ITtrust** – 2018 – tout savoir sur le **SOC** (livre blanc)

2- documents Asprom onglet technologie

- Gartner 2023 - Guide du modèle SOC (Rapport)

3 – Bibliographie

- https://www.orangecyberdefense.com/fr/insights/blog/detection/soc-siem-xdr-mdr-edr-quelles-differences
- Rapports de conformité SOC 1, 2 et 3 (dropbox.com)
- https://geekflare.com/fr/best-siem-solutions/
- https://www.crowdstrike.fr/cybersecurity-101/soc-as-a-service/
- Meilleures solutions SOC as a Service pour 2023 | PeerSpot
- Services de détection et d'intervention (MDR) les mieux gérés pour 2023 | PeerSpot
- https://www.vmware.com/fr/topics/glossary/content/endpoint-detection-and-response-edr.html
- https://www.kaspersky.fr/resource-center/definitions/what-is-xdr
- https://www.esecurityplanet.com/products/xdr-security-solutions/#Trend-Micro-Vision-One
- https://www.splunk.com/fr_fr/data-insider/what-is-an-mssp.html
- https://fre.myservername.com/top-15-best-managed-security-service-providers-2021

4 - Majic Quadrant – Gardner

- SIEM : Gestion des informations et des événements de sécurité (onglet technologie- 2022)
- MDR – Guide du marché des solutions de détection et de réponse gérées : https://www.asprom.com/application/gartner.pdf