QUODAGIS
Digital Security

LIVRE BLANC

Security Operation Center (SOC)

Sommaire

1. QU'EST CE QU'UN SOC ?

Un SOC (Security Operations Center) est un centre de commande pour les professionnels de la cybersécurité chargé de **surveiller, d'analyser et de protéger** une entreprise contre les cyberattaques. Ses activités doivent s'intégrer totalement dans la mise en œuvre de la politique de sécurité et de la gestion des risques de l'entreprise. Il est donc essentiel de définir au préalable, et de faire évoluer, une stratégie de cybersécurité en adéquation avec les objectifs, le contexte et les contraintes de l'entreprise. Celle-ci s'appuie notamment sur une évaluation et gestion des risques orientée sur les besoins métiers et réglementaires.

Dans le SOC, le trafic Internet, les réseaux d'entreprise, les ordinateurs de bureau, les serveurs, les terminaux, les bases de données, les applications et autres objets connectés sont continuellement examinés pour détecter les signes d'un incident de sécurité. Les SOC-Analystes s'appuient sur un ensemble de ressources, outils, et expertise en cybersécurité pour analyser et qualifier les alertes de sécurité, mettre en sécurité et lancer les actions de remédiation en cas d'incident avéré.

De plus, la plupart des SOC fonctionnent 24 heures sur 24, car les équipes sont organisées pour suivre en permanence l'activité et réagir aux menaces.

Le SOC a pour vocation de répondre aux préoccupations principales d'une entreprise quant à sa sécurité informatique. Celui-ci permet de tenir un maintien opérationnel et la continuité des activités métiers en s'adaptant aux menaces liées à la connectivités permanentes des infrastructures informatiques. Il permet à une organisation de bénéficier des avantages suivants:

> **Surveillance continue** de la sécurité des équipements, des flux et des données ;
> **Analyse, qualification et traitement** des alertes et incidents de sécurité ;
> **Optimisation des contrôles** et du **suivi** des opérations de sécurité ;
> **Actualisation et personnalisation** des menaces et risques sur actifs logiciels et matériels ;
> **Amélioration des délais** de détection et de réponse aux incidents de sécurité ;
> **Sécurisation et accompagnement** à la remédiation, du système d'information en cas de compromission ;
> **Réductions des coûts** liés aux impacts et au conséquences des incidents de sécurité ;
> **Mutualisation des compétences** et facilité d'accès aux experts cybersécurité ;
> **Une traçabilité fiable** concernant les données utilisées dans les activités de cybersécurité post-mortem ;
> **Conformité légale** aux règlementations (LPM, exigences OIV, SCEE GPG53, RGPD…) et standards définis (ISO27001, NIS, PCI DSS2 …) ;
> **Sécurisation des traces** permettant de poursuivre les auteurs de cybercriminalité

2. LES DIFFÉRENTS MODÈLES DE SOC

Plusieurs types de SOC existent sur le marché :

> **Internes :** L'ensemble des infrastructures et des personnels sont internes à l'entreprise
> **Hybrides :** L'entreprise exploite avec ses équipes des solutions/services d'un fournisseur externe
> **Externes (Managés) :** L'entreprise s'appuie sur les équipes et l'infrastructure d'un partenaire externe spécialisé pour l'ensemble de l'activité du SOC.

2.1 SOC Interne

La création d'un SOC interne dédié est recommandée pour les entreprises de cybersécurité matures. En effet, celles qui ont tendance à développer des SOC internes ont le budget pour assumer un investissement qui nécessite des efforts 24/24, 7j/7 et qui s'appuie sur de nombreux relais à l'intérieur et à l'extérieur de l'infrastructure. L'un des avantages essentiels de la création d'un SOC interne est une visibilité et une réactivité maximales au niveau de l'ensemble du réseau. Une équipe interne dédiée aura la capacité de surveiller l'environnement et ses applications, fournissant ainsi une image complète au niveau du paysage des menaces. Certains inconvénients sont une difficulté pour recruter et retenir les talents et des niveaux d'investissement initiaux élevés. Ce modèle prend généralement un temps considérable à mettre en place et à maintenir pour bénéficier d'un niveau de fonctionnement adapté et pleinement opérationnel.

2.2 Hybride : SOC Interne et Managé

Un modèle hybride donne accès au meilleur des deux mondes : du personnel interne complété par des experts externes, offrant ainsi une approche sécurisée en matière de détection et de réponse. La plupart des entreprises à ce niveau sont suffisamment grandes pour constituer leur propre petite équipe. Cependant, elles ne peuvent pas créer un SOC interne 24×7 pleinement fonctionnel. Cette solution est efficace en raison de la rapidité de la détection et du temps de réponse. De plus, le backlog est moins important en raison des analystes supplémentaires (internes et externes) qui travaillent sur les résultats hautement prioritaires. En outre, ce modèle offre la meilleure combinaison en termes d'apprentissage aussi bien pour l'entreprise que pour l'équipe de cybersécurité. Il peut également permettre le transfert de connaissances détenues jusque-là par les experts d'un MSSP.

Les inconvénients importants sont principalement le fait que certaines données seront traitées par un tiers et que ce modèle peut être coûteux à maintenir sur le long terme.

2.3 SOC, MSSP, et MDR Managés

La sélection d'un SOC géré est recommandée pour les entreprises qui recherchent l'assistance d'une entreprise externe pour effectuer des opérations de surveillance et de détection de haut niveau. Certaines d'entre elles peuvent être matures d'un point de vue IT et cybersécurité. Cependant, les contraintes budgétaires et l'expertise limitée peuvent entraver la capacité de créer un SOC interne 24×7 pleinement fonctionnel.

À l'inverse, certaines autres peuvent se trouver à des stades immatures au niveau de la protection de l'entreprises et ont besoin d'une meilleure expertise pour gérer rapidement les efforts de surveillance, de détection et de réponse (MDR : Monitoring, Detection, and Response).

Les avantages de ce modèle sont : une plus grande rapidité, simplicité, scalabilité ainsi qu'une mise en œuvre plus économique. Étant donné la grande variété de clients et d'industries que les MSSP (Managed Security Services Providers) prennent généralement en charge, l'expertise et la richesse des renseignements supplémentaires peuvent être véritablement d'une valeur inestimable.

La différence majeure entre un SOC traditionnel et un SOC intégrant des services MDR est que ces derniers non seulement détecteront et analyseront les menaces, mais y répondront également. Lorsqu'une menace est détectée, ils vérifieront la criticité tout en y répondant et en vous informant par la suite de l'incident.

Chaque modèle présente ses avantages et ses contraintes. Le contexte réglementaire ou la stratégie de l'entreprise, tant vis-à-vis du Cloud et de l'hébergement de leurs données chez des prestataires externes, ainsi que les ressources humaines disponibles orientent vers un choix adapté.

Ces dernières années, les sociétés ont été confrontées à une forte évolution des cyberattaques dans un contexte de transformation des infrastructures numériques pour s'adapter aux nouveaux usages et besoins d'agilité. Confrontées à des difficultés pour trouver les ressources humaines et expertises à un SOC et à la nécessaire maitrise budgétaire, elles s'orientent majoritairement vers le modèle externe.

3. LES EXPERTISES ET OUTILS D'UN SOC

3.1 Les équipes

Le SOC regroupe des compétences multiples en cybersécurité qui permettent d'appréhender l'ensemble des situations. Ils sont généralement répartis autour des 6 types de missions :

> **Gestion et coordination du service** (appels entrants ou sortants, coordination et suivi des actions de remédiation, gestion de crise) ;
> **Coordination et évolution du service** (reporting, mise en place et analyse des indicateurs, proposition d'améliorations et d'évolutions) ;
> **Mise en œuvre et maintien en condition opérationnelle** (installation, intégration et maintenance du SIEM1 et des outils de détection, personnalisation au contexte) ;
> **Analyses et réaction** (qualification et réaction aux alertes et incidents de sécurité)
> **Threat Intelligence** (amélioration continue des capacités de détection, enrichissement des scénarios de détection et indicateurs de compromission (IOC))
> **Investigations et R&D (**analyse de nouveaux malwares et vecteurs d'attaques, Forensics).

ORGANISATION D'UN SERVICE SOC : PROXIMITÉ & SUIVI PERSONNALISÉ

3.2 Les outils

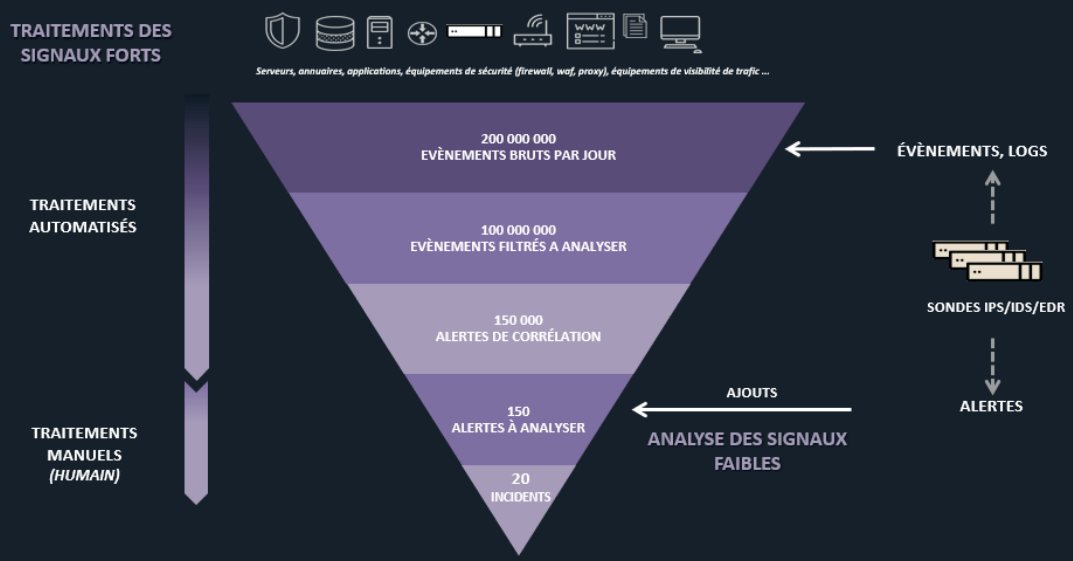
3.2.1 Les collecteurs de Logs

Ils collectent, normalisent et enrichissent les évènements de sécurité de tous les composants du système d'information et des extensions éventuelles (cloud, Datacenter externe ...), afin de permettre leur stockage sécurisé et leur exploitation en temps réel et en temps différé. Il est généralement intégré à la solution SIEM. Plusieurs collecteurs-relais peuvent également être mis en place pour répondre notamment à des contraintes de volume et de bande passante.

3.2.2 Le SIEM

Une solution SIEM assure la gestion, l'intégration, la corrélation et une première analyse des évènements de sécurité, ce qui facilite la surveillance et la résolution des problèmes de votre infrastructure informatique en temps réel. Le SIEM est un outil de collecte et de première analyse des alertes de sécurité sur un flux important de données, se basant sur des scénarios et des Indicateurs de Compromission (IOC) prédéfinis, permettant aux experts SOC de se concentrer sur éléments les plus critiques et pertinents.

TRAITEMENT DES ALERTES ET INCIDENTS DE SÉCURITÉ



3.2.3 Les solutions antivirales

Également appelée EPP (Endpoint Protection Platform), les solutions antivirus classiques sont composées d'un moteur d'analyse et de détection qui recherche des fichiers ou signatures connues comme malveillantes dans sa base de données. Celle-ci est enrichie et mise à jour régulièrement par les éditeurs, qui s'appuient sur des « honeypot » leur permettant de capter et d'analyser les nouveaux virus.

3.2.4 Les solutions EDR/XDR

Complément aux antivirus, les solutions de type Endpoint Detection and Response (EDR) ou Extended Detection and Response (XDR) désignent une technologie de recherche et d'analyse et de remédiation de menaces basée sur la détection d'activités suspectes, de comportements ou actions anormales de l'équipement. Un moteur d'intelligence artificielle/machine Learning lui permet d'être auto-apprenant et d'enrichir ses capacités de détection et de réaction.

3.2.5 Les plateformes d'analyses et de filtrage

Également appelées « Sandbox » ou « bac à sable », cette plateforme combine plusieurs outils de détection et d'analyse permettant de fichiers compromis ou de malwares. Elle utilise souvent des technologies de simulation d'environnement afin d'étudier le comportement d'un fichier ou logiciel, déterminer s'il présente un caractère malveillant et, le cas échéant, le bloquer avant qu'il n'atteigne le système d'information. Il participe également à l'enrichissement des bases de données de détection et à la mise à jour des Indicateurs de Compromission (IOC) et scénarios d'attaques.

4. LES CRITÈRES DE RÉUSSITE D'UN PROJET SOC

La réussite d'un projet SOC ne peut pas simplement s'exprimer. Nous pouvons cependant envisager quelques axes de réflexions :

« On n'achète pas un SOC efficace, on le construit »

Un SOC est un projet complet qui nécessite une interactivité et une synergie forte entre les équipes sécurité, infrastructures & réseaux, métiers, et même utilisateurs. Sa mise en œuvre doit s'effectuer progressivement et s'adapter au contexte, contraintes et besoins métiers. Un projet mené dans l'urgence est rendu plus difficile ; un projet trop ambitieux est, quant à lui, voué à l'échec

« Le SOC est prescripteur pour le SI (et inversement) »

Le SOC n'est pas une fonction support du SI, mais son client. Des interfaces doivent être définies avec les acteurs du SI, et permettre de suivre et analyser de façon macroscopique les différents alertes et incidents détectés afin de déterminer des axes d'amélioration ou d'évolution pertinents.

« Le SOC n'a pas vocation à résoudre seul les incidents de sécurité »

mais il doit en avoir les compétences pour accompagner la remédiation des incidents de cybersécurité et peut mettre en œuvre des actions de protection et de réaction prédéfinies pour limiter la propagation d'un incident de sécurité.

« Le SOC ne peut pas construire tous les scénarios, ou détecter instantanément toutes les attaques »

Il est important qu'il mette en œuvre des analyses complémentaires sur une échelle de temps plus longue pour rechercher et traiter les signaux faibles et attaques dites silencieuses. Il se nourrit également des incidents pouvant lui être remontés par les utilisateurs ou les équipes de la DSI

« Il faut remettre de l'humain dans l'IT pour qu'il fonctionne »

Le SOC s'appuie sur un ensemble d'outils existants ou développés par ses équipes afin de pouvoir traiter, corréler et pré-qualifier un volume important d'alertes. Cela permet d'extraire les éléments pertinentes indicateurs de potentiels incidents que l'expertise des analystes permettra de traiter.

« Un SOC qui remonte seulement les alertes n'est pas efficace »

Un SOC doit prendre en compte les alertes pour déterminer si elles sont relatives, ou non, à des incidents de sécurité. Il doit également relever les éventuelles anomalies, parfois significative dans la recherche d'attaques silencieuses ou dans l'amélioration/évolution de sa capacité de détection.

« Les bases de données publiques, des CERT3 ou éditeurs sont des sources essentielles pour l'efficacité du SOC »

Elles contribuent à l'enrichissement des modules de détections du SOC, et permettent de bâtir ou faire évoluer les scénarios d'attaques existants.

« La pertinence d'un SOC est liée à la vitalité de sa R&D »

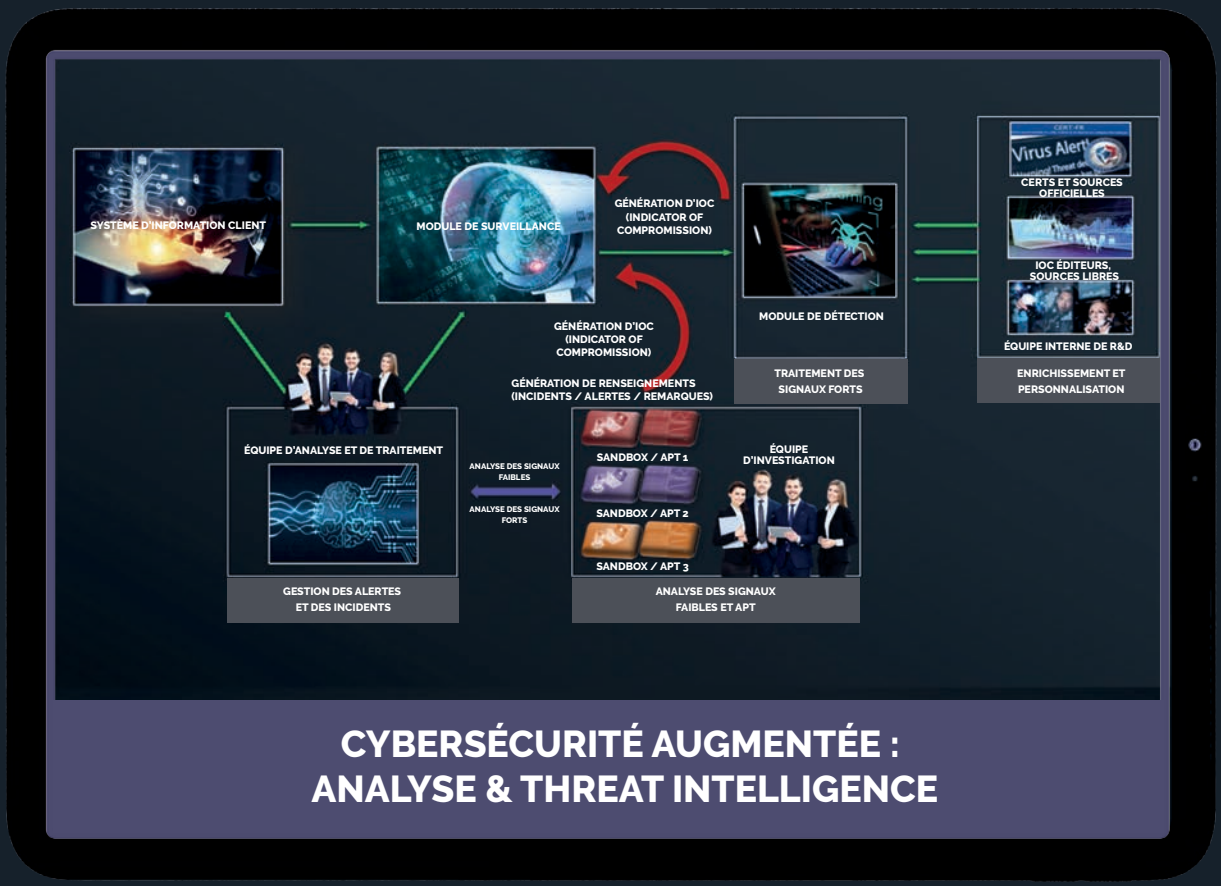
La recherche et développement (R&D) est essentielle pour établir de nouveaux patterns et outils de détection. La structure de R&D doit exister et proposer des plans de progrès. Le SOC n'est pas un système statique, et son apprentissage et son évolution sont permanents.

5. FONCTIONNEMENT D'UN SOC

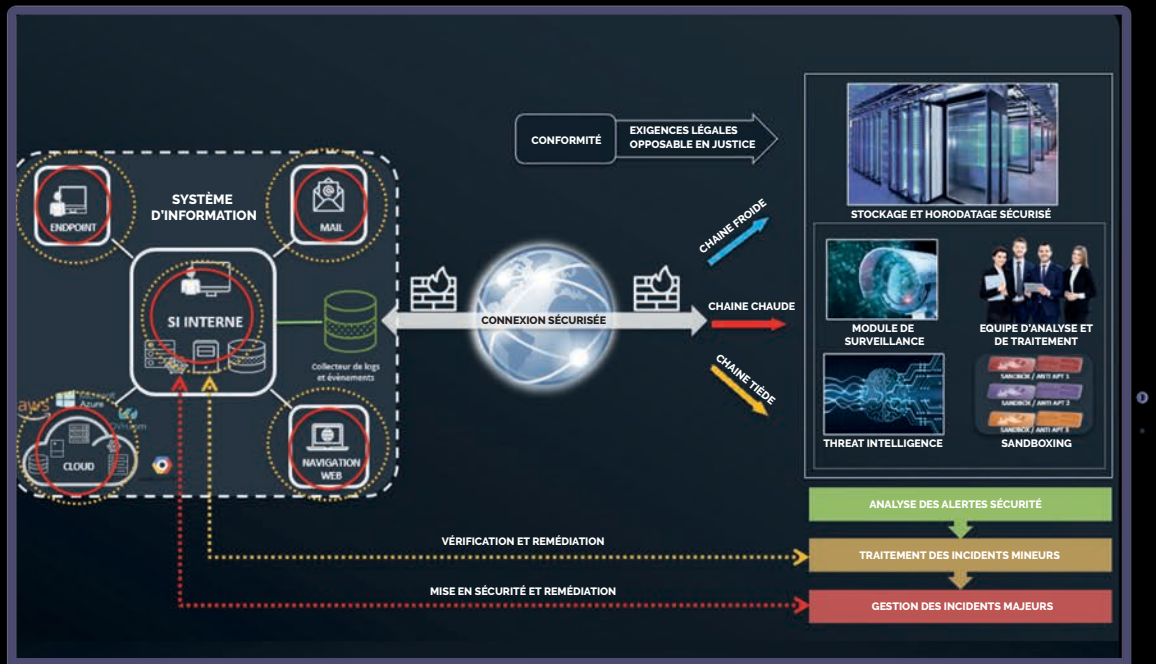
Le SOC surveille les données de sécurité générées au niveau de l'ensemble de l'infrastructure IT de l'entreprise, en allant des systèmes hôtes et des applications jusqu'aux périphériques réseau et de sécurité, tels que les pares-feux et les solutions antivirus.

En combinant une gamme d'outils avancés et les compétences de professionnels expérimentés en matière de cybersécurité, le SOC remplit les fonctions vitales suivantes :

- Surveillance, détection, investigation et triage des alertes des événements de sécurité.
- Gestion des réponses aux incidents de sécurité, notamment l'analyse des malwar es et les investigations forensiques.
- Gestion des renseignements sur les menaces (ingestion, production, curation et diffusion).
- Gestion des vulnérabilités basée sur les risques (notamment, la priorisation des c orrectifs).
- Traque des menaces.
- Gestion et maintenance des dispositifs de sécurité.
- Développement de données et d'indicateurs pour le reporting/la gestion de la conformité.

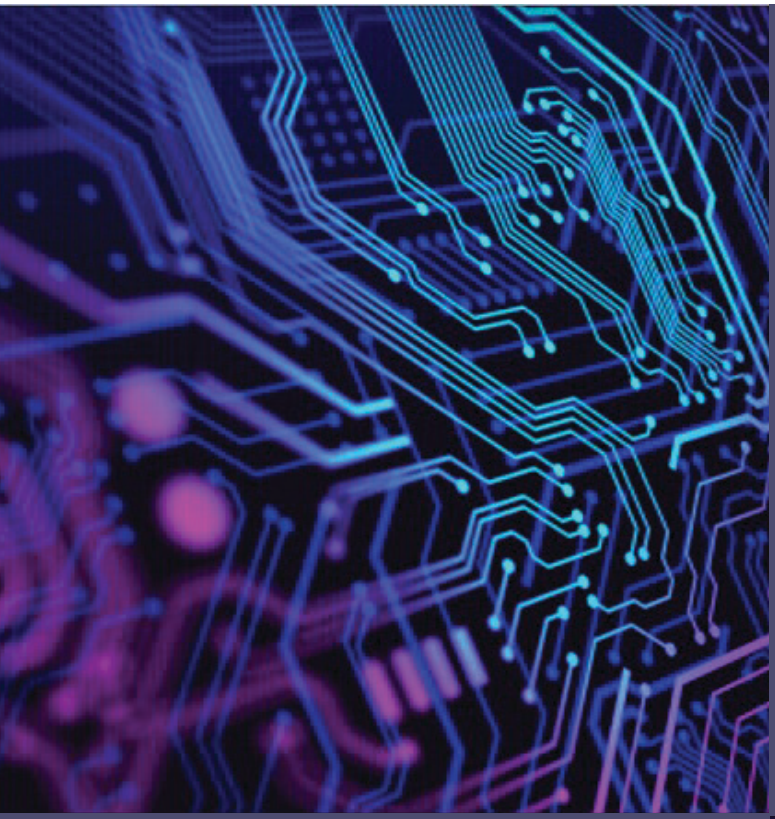


CYBERSÉCURITÉ AUGMENTÉE : ANALYSE & THREAT INTELLIGENCE



MAITRISE & RÉACTIVITÉ

6. LES DÉFIS D'UN SOC



CYBERSÉCURITÉ, UN DÉFI PERMANENT

> **Enjeux stratégiques vitaux** pour l'entreprise et nécessité de se conformer aux obligations légales

> **Coûts** de maintien en condition opérationnelle et d'évolution des infrastructures et des ressources humaines

> **Organisation** complexe et charge de travail importante pour les équipes

> **Multiples expertises complémentaires et une proactivité** nécessaires face aux évolutions rapides des menaces

VOS ENJEUX CYBERSÉCURITÉ

> Trouver le **bon compromis entre Production et Sécurité** «Sécuriser en maintenant les performances et l'expérience utilisateur»

> Maintenir l'**efficacité permanente de la Protection** «Les menaces évoluent, la protection doit s'anticiper et s'adapter»

> S'adapter aux nouveaux **Usages et Besoins** « La sécurité au service des Usages et des Métiers»

> **Surveiller, Protéger et Réagir** face à la menace «Assurer continuité et agilité dans la protection et les actions»

6.2 Répondre aux contraintes techniques

6.2.1 Le volume

Le défi le plus courant auquel sont confrontées les entreprises est le volume d'alertes de sécurité, dont beaucoup nécessitent à la fois des systèmes avancés et des ressources humaines pour catégoriser, prioriser et répondre correctement aux menaces. Avec un grand nombre d'alertes, certaines menaces peuvent être mal classées ou passées complètement inaperçues. Ce risque souligne le besoin d'outils de surveillance avancés et de capacités d'automatisation ainsi que la nécessité de disposer d'une équipe de professionnels qualifiés en matière de cybersécurité.

6.2.2 La complexité

La nature de l'entreprise, la flexibilité du lieu de travail, une utilisation accrue de la technologie Cloud et d'autres problèmes ont augmenté la complexité de la défense d'une entreprise et de la réponse aux menaces. Aujourd'hui, des solutions relativement simples, comme les pares-feux, sont insuffisantes en tant que mesure isolée pour protéger l'entreprise contre ses adversaires numériques. Une sécurité plus efficace nécessite une solution qui combine la technologie, l'humain et les processus, ce qui peut être difficile à organiser, à mettre en place et à faire fonctionner.

Dans le cas d'un SOC externe ou hybride, la relation et l'organisation mise en œuvre entre la société et son prestataire doit être simple et stable dans le temps. Cela permet d'augmenter de façon significative la réactivité des équipes et la pertinence des évolutions et réactions par l'amélioration des synergies et de la connaissance du contexte propre à l'entreprise.

6.2.3 Le coût

La maitrise des coûts de mise en œuvre et de fonctionnement d'un SOC est primordiale :

> **Des coûts financiers mal anticipés** peuvent se confronter à des arbitrages budgétaires conduisant limitant le périmètre de surveillance et augmentant l'exposition de l'entreprise aux cyberattaques
> **Une charge de travail sous-évaluée** peut contraindre les équipes à survoler certaines alertes et à se reposer entièrement sur les outils mis en place, entrainant une perte d'efficacité et de compétences importante.
> **L'absence de prise en considération du maintien en condition opérationnel** (MCO) des équipements, tout comme la veille sur les nouvelles techniques et technologies de détection conduirait à l'érosion des capacités et de la pertinence SOC.

6.2.4 La pénurie des compétences

La création d'une solution de sécurité interne est à l'heure actuelle encore plus compliquée étant donné la disponibilité limitée des professionnels qualifiés en cybersécurité. Ces derniers sont très demandés dans le monde entier, rendant ainsi difficile le recrutement et la rétention des talents. Cette situation signifie que le turnover au sein d'une organisation de cybersécurité peut potentiellement affecter les opérations de sécurité.

7. DÉPLOIEMENT D'UN SOC

La mise en œuvre d'un projet SOC passe généralement par 4 étapes :

1. Une préparation amont, organisationnelle et technique
2. Une phase de tests sur un périmètre réduit
3. Le déploiement à l'ensemble du système d'information
4. La mise en production opérationnelle sur l'ensemble du périmètre

La phase préparatoire est primordiale dans le projet SOC. Elle permet de connaitre l'existant, de corriger en amont les vulnérabilités, de déterminer l'architecture optimale et de prendre en compte les contraintes éventuelles :

COMPRÉHENSION DE LA GOUVERNANCE CYBERSÉCURITÉ

> Intégrer vos enjeux et besoins métiers
> Adapter l'approche à votre organisation et contexte métier
> Déterminer les meilleurs circuits de communication

ÉTUDE DE L'INFRASTRUCTURE

> Définir le périmètre cible
> Analyser l'infrastructure, les équipements existants et les points d'interconnexion
> Définir les meilleurs axes de surveillance et de remontée d'informations et de logs

AUDIT DE VULNÉRABILITÉS

> Réaliser un audit de vulnérabilité initial sur le périmètre, afin de réduire les risques et alertes
> Mettre en oeuvre le plan d'amélioration proposé
> Organiser une récurrence des contrôles

FINALISATION

> Adapter le paramétrage aux points spécifiques de surveillance
> Déployer les compléments sécurité nécessaire si souhaité par le client
> Préparer la conservation sécurisée et les flux d'exploitation des informations collectées

8. CONCLUSION

Un SOC est un projet cybersécurité majeur qui s'inscrit dans la stratégie globale de maitrise et gestion des risques d'une entreprise. La réussite du projet doit s'appuyer sur une préparation initiale définissant l'organisation, les ressources matérielles, les expertises nécessaires à son fonctionnement.

La mise en perspective des besoins et des moyens internes à l'entreprise permet d'orienter le choix du modèle de SOC (interne, hybride ou externalisé). Dans tous les cas, la maitrise et la responsabilité des aspects cybersécurité du système d'information doivent rester

Les aspects budgétaires doivent être maitrisés, en prenant en considération les coûts de fonctionnement, le maintien en condition opérationnel des équipements et les aspects de développement et d'évolution.

9. ANNEXES

I. **MSSP (Managed Security Service Provider),** il facilite la gestion des services de sécurité pour l'utilisateur final. Il assure la surveillance des évènements et la gestion externalisées des dispositifs et des systèmes de sécurité de l'environnement client. Il assure également la surveillance et la gestion des contrôles de sécurité informatiques et des fonctions fournies à distance via des services partagés hors des centres d'opérations de sécurité (SOC).

II. **SIEM** signifie Security Information and Event Management ou gestion des informations et des événements de sécurité. On peut définir le SIEM comme la collecte d'événements en temps réel, la surveillance, la corrélation et l'analyse des événements à travers des sources disparates.

III. **PCI DSS L'acronyme PCI DSS (Payment Card Industry Data Security Standard)** désigne les normes de sécurité des données applicables à l'industrie des cartes de paiement. Élaborée par le conseil des normes de sécurité PCI, la norme PCI DSS vise à réduire la fraude en ligne. Toute organisation qui traite les données de titulaires de cartes de paiement est tenue de s'y conformer.

IV. **CERT (ou CSIRT, Computer Security Incident Response Team),** est une division qui a pour mission de gérer et traiter les alertes à la suite d'incidents, et de prévenir des incidents de sécurité. Il réagit et pro-agit en collectant des données de sources externes à l'organisation, dont les alertes seront traitées avec des analystes.

V. **SLA "Service Level Agreement"**. En français, cette expression peut être traduite par « accord de niveau de service », « convention de services », ou encore « engagements de service ».
Le SLA peut définir le contrat en lui-même, ou la partie du contrat qui concerne plus précisément le niveau de service que le prestataire s'engage à délivrer à l'utilisateur

QUODAGIS
Digital Security

A propos de QUODAGIS Digital Security

QUODAGIS Digital Security est une société de conseil et d'expertises spécialisée en cybersécurité. Nous avons pour vocation d'aider les entreprises à améliorer la sécurisation de leur système d'information et son adaptation aux nouveaux besoins et usages. Nos clients peuvent ainsi s'appuyer sur nos équipes expérimentées en Pentest, Audits, Gouvernance de la sécurité, Gestion des risques, Conformité, Gestion des identités & des accès (IAM), Sensibilisation et Formations. Ils bénéficient également de nos services de surveillance et la protection des actifs et équipements au travers de notre Security Operation Center (SOC).

A propos du Groupe QUODAGIS

QUODAGIS est un groupe IT qui délivre des services permettant un fonctionnement optimal des infrastructures informatiques. Le groupe QUODAGIS propose des offres complémentaires et accompagne plusieurs centaines de clients mid-market et grands comptes dans leurs projets de transformation IT et de déploiement de technologies. La synergie entre les entités du groupe QUODAGIS (Intégration, Services Managés, Accompagnement et Transformation vers les services Cloud, Assistance Technique) permet à nos clients d'intégrer leur démarche cybersécurité dans leur stratégie IT globale.

Le groupe QUODAGIS accompagne depuis plus de dix ans des centaines de clients dans leurs projets de transformation de leur système d'information, de déploiement de technologies et de sécurisation des services.

Plus d'informations sur :

digital-security.quodagis.fr
www.quodagis.fr

Pour nous contacter :

digital-security@quodagis.fr
+33 (0)1 55 06 11 91