exo data
CYBERDEFENSE

LE SOC*, NÉCESSAIRE, UTILE OU SANS INTÉRÊT ?

*Security Operation Center,
ou Centre d'Opérations Sécurité

LIVRE BLANC - EXODATA

Table des matières

1 Un contexte difficile sur le plan économique et sécuritaire

2 Le SOC, pour un contrôle optimal des processus de surveillance

3 Les fondamentaux du SOC

4 Pourquoi externaliser le SOC ?

5 L'évolution du SOC

1. Un contexte difficile sur le plan économique et sécuritaire

exo data CYBERDEFENSE

Les sociétés, privées ou publiques, quelle que soit leur taille, tentent de poursuivre leurs développements malgré un contexte économique mondial incertain et une généralisation des cyber-attaques.

Forcément impliquées dans la transition numérique, si la majorité des entreprises ont déjà initié des processus de cyber-protection, elles ne se sentent pas forcément équipées face aux menaces graves.

exo data CYBERDEFENSE

Stéphane Jaillet,
DG Stratégie et Developpement Cyberdéfense

Les défis auxquels les sociétés doivent faire face

Dans un contexte mondial économique morose, les entreprises cherchent à concilier plusieurs contraintes afin d'atteindre leurs objectifs de croissance

- Se distinguer face à la concurrence
- Continuer à se développer
- Réduire les coûts en conservant un bon niveau de qualité des produits et/ou services
- Attirer de nouveaux clients
- Faire preuve de réactivité pour intégrer les technologies issues d'internet dans leurs produits/services et leurs relations clients/fournisseurs

Pour réussir ces challenges, les sociétés doivent opérer des changements en profondeur et placer le numérique au centre de leur métier.

exo data CYBERDEFENSE

La transition numérique, inéluctable pour toutes les entreprises

La transformation digitale se généralise à tous les types de structures. Elle implique des modifications conséquentes dans les procédures de travail ainsi que dans les relations avec les clients et les fournisseurs. Ces changements organisationnels s'accompagnent de la nécessité de recourir à de nouveaux outils et de développer les systèmes d'information. Les possibilités de télétravail s'accroissent, amenant de nouveaux besoins en matière d'accès aux applications internes par des collaborateurs de plus en plus mobiles.

En outre, le développement des technologies issues de l'internet, telle que l'IdO (Internet des Objets) révolutionne les habitudes des consommateurs comme celles des entreprises. Le risque majeur inhérent à cette «explosion du numérique» est la multiplication des attaques informatiques à cause de l'accroissement exponentiel des points d'entrée reliés aux réseaux des sociétés.

exo data CYBERDEFENSE

DES SOCIÉTÉS QUI SE PROTÈGENT MAIS RESTENT PEU CONFIANTES

Selon le baromètre de la cyber-sécurité des entreprises (vague 5, janvier 2020), établi par le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique), en collaboration avec Opinionway, 39 % des entreprises déclarent être protégées en cas de cyber-attaque de grande ampleur.

Ces dernières considèrent qu'elles utilisent des solutions de protection adaptées, sont majoritairement engagées, ou en voie de le faire, dans des démarches de cyber-résilience et ont pour la plupart souscrit une cyber-assurance.

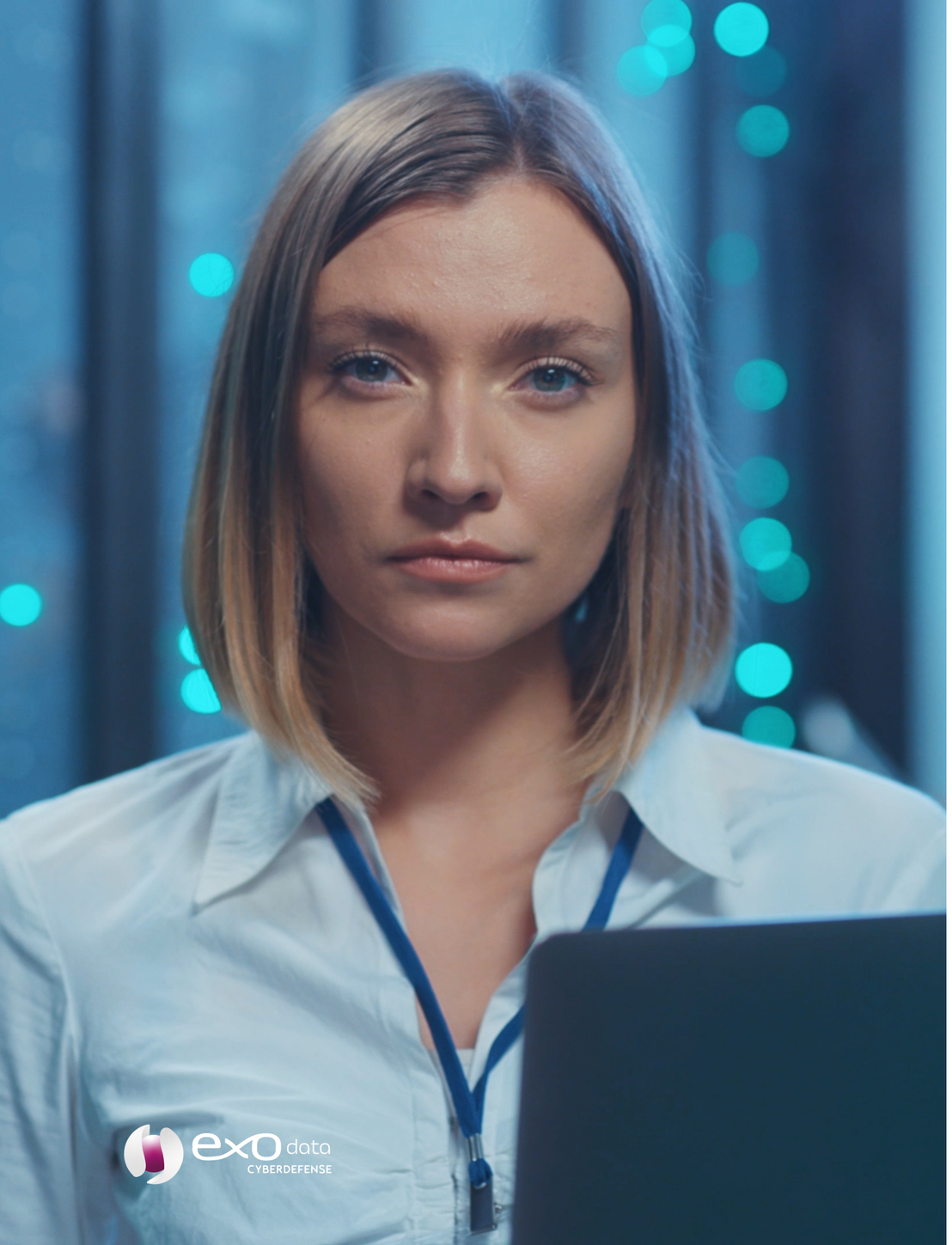
exo data CYBERDEFENSE

Cependant, malgré cette mobilisation autour de la cyber-sécurité, la moitié des sociétés interrogées doutent de pouvoir faire face efficacement aux cyber-attaques.

Selon elles, les principaux enjeux sont :

- La gouvernance
- La formation et la sensibilisation des utilisateurs
- La difficulté à recruter des profils spécialisés en sécurité des S.I
- Les contraintes budgétaires

exo data CYBERDEFENSE



Ces sociétés pensent que la pénurie de profils dans les métiers liés à la gestion des risques informatiques concerne principalement

les fonctions de pilotage, organisation et gestion des risques (Correspondant Sécurité, RSSI Responsable de la Sécurité des Systèmes d'Information,...) ainsi que le support et la gestion des incidents (analyste SOC...).

Une protection globale accrue mais encore des risques potentiels

Malgré un nombre croissant de sociétés engagées dans la cyber-sécurité, l'impact des cyber-attaques sur le business est toujours aussi important, entraînant notamment des perturbations des processus de production.

Selon ces sociétés, les principaux types d'attaques sont : le phishing, l'arnaque au Président, l'usurpation d'identité et l'infection par des malwares.

À l'origine de ces attaques, se trouve souvent une erreur humaine d'un collaborateur telle qu'une négligence, une manipulation incorrecte ou une configuration inadaptée. Ainsi, pourtant sensibilisés aux cyber-attaques, les salariés manquent d'implication et ne respectent pas les recommandations de leur société. Côté infrastructure, les entreprises pensent que les plus gros risques se situent au niveau du Cloud.

exo data CYBERDEFENSE

UN NOMBRE RECORD D'ATTAQUES

2020 pourrait encore être une année difficile pour les entreprises.

Si toutes les sociétés sont touchées, la plus forte augmentation concerne les ETI (Entreprises de Taille Intermédiaire). Publiques ou privées, les structures n'échappent pas aux cyber-attaques dont les conséquences sont parfois lourdes, pouvant aller jusqu'à la faillite.

C'est pourquoi il est crucial de placer la protection des données au cœur de la stratégie des entreprises et la mise en place d'un SOC est une réponse adéquate à ce type de problématique.

Avec 67 %

d'entreprises déclarant avoir été victimes de cyber-attaques en 2019

2. Le SOC, pour un contrôle optimal des processus de surveillance

exo data CYBERDEFENSE

Composé d'équipes d'experts en sécurité informatique et d'outils spécifiques, le SOC est chargé de prévenir, détecter et évaluer les menaces internes comme externes.

Lorsqu'un incident survient, il s'occupe de le régler et gère la récupération des données. Grâce à un SOC et à son principal outil technique, le SIEM, les sociétés ont la possibilité d'optimiser le contrôle de leurs processus de surveillance, de répondre plus rapidement et efficacement aux attaques et de satisfaire à leurs obligations réglementaires. Interne, externe, virtuel, hybride... le SOC peut prendre de nombreuses formes tout en gardant les mêmes objectifs.

exo data CYBERDEFENSE

COMMENT DÉFINIR UN SOC ?

Le SOC (Security Operation Center) ou COS (Centre des Opérations de Sécurité) d'une société se compose de l'équipe dédiée à la supervision de la sécurité informatique et des équipements qui sont utilisés pour cette tâche. Il se base sur des outils chargés de collecter des informations, de corréler des événements et d'intervenir à distance en cas d'attaques supposées ou avérées.

LES OBJECTIFS DU SOC

Le but du SOC est que les systèmes d'information d'une entreprise soient efficacement protégés des cyberattaques. Dans le cas où un incident aurait tout de même eu lieu, le SOC a pour mission de le gérer et de réduire au maximum son influence négative sur le fonctionnement de la société.

Les principales missions du SOC sont :

- La prévention, la détection, l'évaluation des menaces internes ou externes
- Si un incident survient : l'intervention, la récupération des données, l'analyse de l'incident et le plan de reprise
- L'évaluation de la conformité réglementaire
- La cyberveille

exo data CYBERDEFENSE

De plus, le SOC doit être capable d'évoluer pour tenir compte des modifications structurelles ou informatiques de la société.

L'ensemble de l'infrastructure informatique est concernée par la surveillance du SOC : terminaux, serveurs, réseaux, applications, bases de données quel que soit leur lieu d'hébergement, sites internet, intranet, etc.

L'objectif ultime du SOC est de garantir à l'entreprise la continuité de service. En effet, indépendamment de la taille et du secteur d'activité d'une société, elle dépend toujours fortement de son système informatique, qu'il s'agisse de communiquer, de faire fonctionner la production, de gérer les stocks, la finance, les RH, etc. Toute interruption, même courte, des systèmes d'information peut donc avoir des conséquences graves pour l'entreprise à court et long terme.

exo data CYBERDEFENSE

Le SOC doit inclure, en plus des spécificités liées aux métiers, l'émergence de nouveaux types d'attaques et de risques liés par exemple à l'hyper-connectivité.

Il doit arriver à combiner de manière optimale les dernières avancées technologiques en matière de gestion et d'analyse prédictive des données et l'expérience de spécialistes de la cybersécurité. En effet, même si les technologies évoluent sans cesse, il est impossible de faire l'impasse sur l'intervention humaine, notamment pour prévenir des attaques encore inconnues pour le moment.

exo data CYBERDEFENSE

LES ÉQUIPES DU SOC

Dans le SOC, les équipes se composent de plusieurs types de profils :

- Des spécialistes : ils installent et intègrent les outils, ils paramètrent les différents systèmes de supervision de la sécurité (SIEM, logiciels de détection, outils de protection, etc.).
- Des analystes : ils classifient, analysent et gèrent les alertes de sécurité. Lorsqu'un incident survient, ils se chargent de l'investigation et de la réponse à apporter. Ils prennent également en charge l'interprétation des alertes, la corrélation des événements et la recherche des vulnérabilités.
- Des membres du support : ils travaillent à l'amélioration continue du SOC.

exo data CYBERDEFENSE

Le SIEM,
crucial dans le SOC

Le Security Information Event Management (SIEM) est le centre névralgique de la partie technique du SOC. Il représente véritablement le cœur de l'architecture du SOC de par ses multiples fonctionnalités.

Avec l'ensemble des données collectées au niveau des systèmes d'information, le SIEM réalise des tâches d'archivage, de regroupement, de corrélation et de reporting.

LES AVANTAGES APPORTÉS PAR UN SOC

En mettant en place un système de surveillance tel que le SOC, les entreprises bénéficient ainsi :

- D'une force d'identification rapide des possibles attaques et d'une capacité à les faire échouer avant la survenue de dommages graves
- D'une rapidité accrue pour répondre aux attaques, ce qui est particulièrement utile dans le cas d'une infection par un malware
- D'une meilleure capacité à faire face aux attaques de type DDoS (Distributed Denial of Service) dont le but est de rendre indisponible une infrastructure, un serveur ou un service, que ce soit en amenant à un épuisement des ressources du système ou en saturant la bande passante du serveur par exemple.

Pourquoi mettre en place un SOC ?

Le SOC agit sur trois grands axes :
le contrôle, la détection et la mise en conformité.

exo data CYBERDEFENSE

Pourquoi mettre en place un SOC ?

Améliorer le contrôle des processus de surveillance

Avec un SOC, les sociétés ont une vue d'ensemble de leurs processus de surveillance et elles les contrôlent de manière plus efficace. Le suivi continu des données et de leurs évolutions permet une meilleure détection des comportements suspects et facilite aussi les investigations suite à un incident.

exo data CYBERDEFENSE

Pourquoi mettre en place un SOC ?

Savoir mieux détecter et répondre aux attaques

La conséquence directe d'un contrôle accru des processus de surveillance est la capacité de l'entreprise à être prête face à des attaques, qu'elles surviennent de l'intérieur ou de l'extérieur. Une fois qu'une attaque est avérée, le SOC permet une réponse rapide grâce aux procédures ciblées selon le type d'incident.

exo data CYBERDEFENSE

Pourquoi mettre en place un SOC ?

Suivre les obligations réglementaires

Les entreprises ont l'obligation d'être en conformité avec différentes législations qui peuvent dépendre ou pas de leur secteur d'activité. Parmi les réglementations non sectorielles, il y a :

- Le RGPD : applicable au niveau européen, il encadre le traitement des données personnelles et demande aux entreprises de garantir un certain niveau de sécurité pour ces informations en tenant compte du potentiel risque numérique
- Le PCI DSS : cette norme internationale vise la protection des utilisateurs de carte bancaire en ligne contre la récupération de leurs données personnelles et leur utilisation frauduleuse.

exo data CYBERDEFENSE

Des organismes publics nationaux et internationaux comme l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) et le CIS (Center for Internet Security) encouragent les entreprises à créer un SOC pour améliorer leur sécurité informatique.

exo data CYBERDEFENSE

Les différents types de SOC

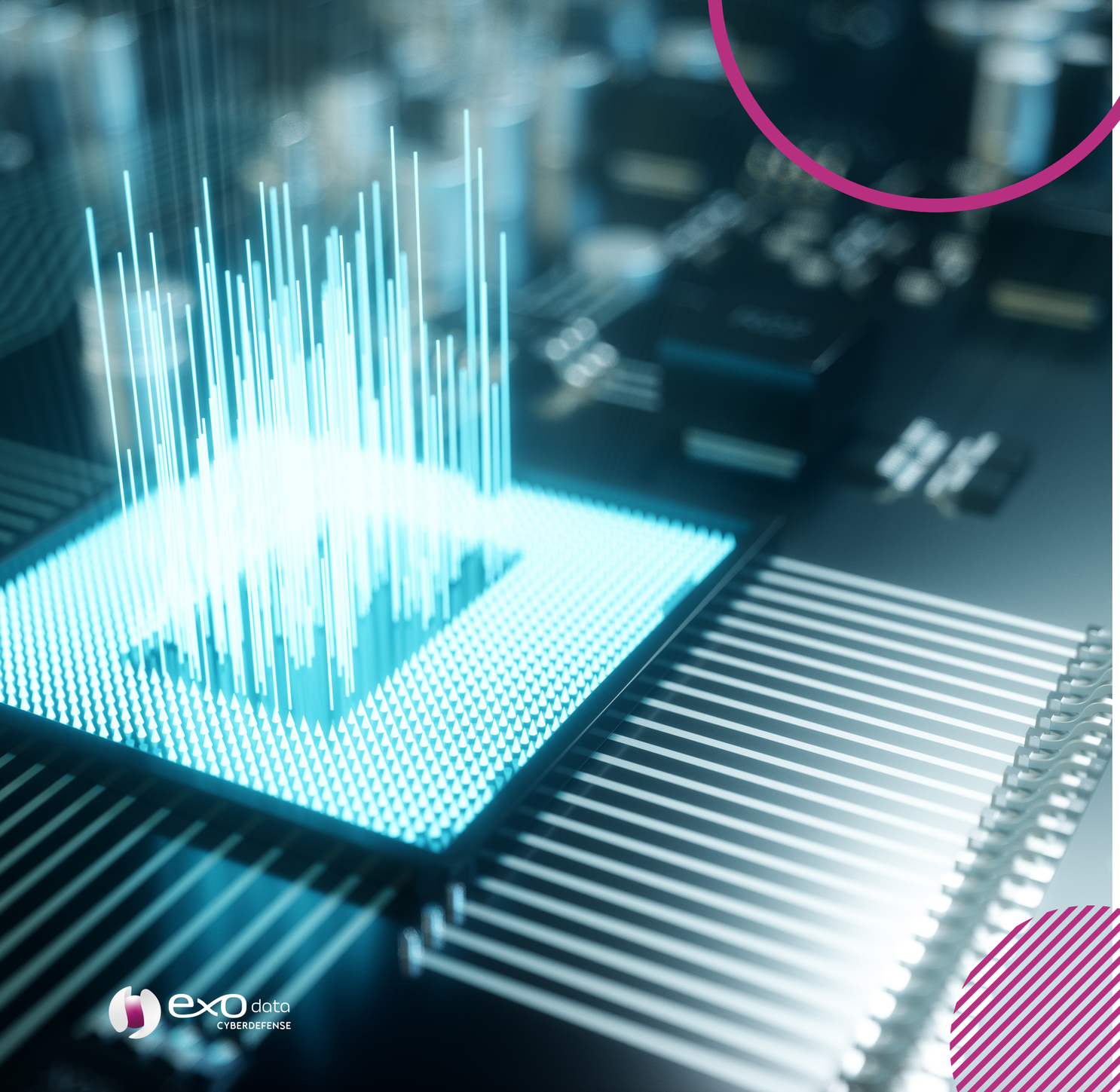
Il est possible de classifier les SOC en fonction de leur type d'implémentation technique et de leur localisation :

exo data CYBERDEFENSE

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 installation physique propre, 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 cyberveille (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	Aux fonctionnalités classiques du SOC s'ajoutent la Threat Intelligence (cyberveille). Son but est de compiler des informations sur les cyber-attaques 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.

3. Les fondamentaux du SOC

exo data CYBERDEFENSE



Afin que le SOC fonctionne de manière optimale, il est obligatoire de combiner plusieurs outils aux fonctions complémentaires, qui peuvent être intégrés pour certains dans le SIEM (Security Information Event and Management), brique centrale du système de surveillance de la sécurité.

Ainsi, les autres outils souvent utilisés sont : la technologie de Machine Learning, la Threat Intelligence, le scanner de vulnérabilité ainsi que les outils de visualisation et d'alerte.

Parfois, des logiciels de protection « Endpoint » et des logiciels d'intrusion sont également employés.

Pour s'assurer de la mise en place d'un SOC performant, plusieurs étapes sont requises

- Tenir compte des référentiels et de l'architecture informatique de la société
- S'assurer de l'implication de tous (collaborateurs, clients fournisseurs) dans le projet
- Vérifier la compatibilité entre la solution définie et les obligations réglementaires
- Choisir la stratégie de surveillance
- Définir les risques acceptables ou non
- Instaurer une politique de supervision
- Déployer la solution
- Prévoir le maintien en condition de sécurité

Les composantes essentielles du SOC

Quelles sont-elles ?

exo data
CYBERDEFENSE

Les composantes essentielles du SOC

Le SIEM (Security Information Event and Management)

Élément central du SOC, le SIEM se charge de collecter, surveiller, corréler et analyser les données générées par l'infrastructure informatique (les serveurs, les bases de données, les routeurs, les pare feux...). Il identifie les éventuels écarts par rapport à des normes ou des moyennes définies au préalable. Quand un problème est identifié, il crée une alerte qui va être analysée par des experts en sécurité. Ils vont s'assurer qu'il ne s'agisse pas d'un faux-positif ou d'une alerte redondante qui aurait pu passer au travers du paramétrage mis en place pour les éviter. Les vraies alertes sont ensuite transmises à d'autres outils de sécurité qui seront en charge d'arrêter la progression de ces menaces.

Le SIEM comprend parfois une fonctionnalité d'Analyse Comportementale des Utilisateurs et des Entités (UEBA, User and Entity Behaviour Analytics) qui surveille principalement les éventuelles actions suspectes des utilisateurs.

Si les analystes se basent forcément sur les informations fournies par le SIEM, il ne s'agit pas de leur unique source de données. D'autres outils sont nécessaires afin que la sécurité des systèmes d'information soit assurée le mieux possible.

exo data CYBERDEFENSE

Les composantes essentielles du SOC

L'apprentissage automatique ou machine learning

Cette technique, qui n'est pas forcément présente dans tous les SOC, est pourtant d'une importance cruciale. Elle permet en effet d'identifier des patterns (séquences ou événements répétitifs) et de réaliser des prédictions. Pour cela, elle se base sur le data mining, les statistiques, les analyses prédictives et les patterns.

exo data CYBERDEFENSE

Les composantes essentielles du SOC

La Threat Intelligence

Composante essentielle dans la cyberdéfense, elle permet de définir la nature des menaces les plus probables et dangereuses concernant une société donnée. Elle se base pour cela non seulement sur les données collectées mais aussi sur des informations externes provenant de sources aussi variées que des bases de connaissances internationales, le Darknet, les listes noires d'adresses IP...

exo data CYBERDEFENSE

Les composantes essentielles du SOC

Le scanner de vulnérabilité

Indispensable dans le SOC, il réalise des audits de manière automatisée et régulière. Les éventuelles vulnérabilités du réseau sont relevées et classées généralement en suivant le système de Notation Standard des Vulnérabilités (Common Vulnerability Standard Scoring, CVSS). Selon la criticité des failles découvertes, des mesures correctives sont alors prises.

exo data CYBERDEFENSE

Les composantes essentielles du SOC

Les outils d'alerte

Ils peuvent être inclus dans le SIEM ou déployés de manière indépendante. Leur objectif est la gestion des incidents et des alertes.

exo data CYBERDEFENSE

Les composantes essentielles du SOC

Les outils de visualisation

Le SIEM intègre souvent des logiciels de type « dashboard » (tableaux de bord) qui permettent de centraliser les données et d'agréger les résultats sous la forme de tableaux ou de graphes. Ces logiciels sont largement personnalisables afin de générer des états répondant exactement aux attentes de chaque entreprise.

Il est souvent possible d'envoyer des informations directement dans des tablettes ou des smartphones. Il peut s'agir aussi bien de messages d'alerte que de données concernant la sécurité du système informatique de la société.

exo data CYBERDEFENSE

Les composantes essentielles du SOC

Les logiciels de protection « Endpoint »

Optionnels, ces logiciels de sécurité gèrent la sécurité au niveau des terminaux tels que les ordinateurs et les appareils mobiles. Comme le nombre d'équipements connectés à un réseau, qu'ils soient dans ou hors des murs de la société, ne cesse d'augmenter, les portes d'entrées possibles pour les logiciels malveillants se multiplient également.

Les systèmes Endpoint permettent notamment d'authentifier les connexions et de prendre en charge le déploiement ainsi que la mise à jour à distance des logiciels. Ils peuvent aussi collecter des données utiles pour le SOC.

exo data CYBERDEFENSE

Les composantes essentielles du SOC

Les systèmes de détection d'intrusion

Également optionnels, les IDS (Intrusion Detection Systems) suivent l'évolution du trafic réseau au niveau du réseau lui-même (N-IDS : Network Based Intrusion Detection System) ou des hôtes (H-IDS : Host Based Intrusion Detection System). Ils repèrent les activités suspectes ou anormales et peuvent envoyer ces informations au SOC.

exo data CYBERDEFENSE

Les étapes nécessaires à la mise en place d'un SOC performant

exo data CYBERDEFENSE

1

Prendre en compte les référentiels et l'architecture de l'entreprise

Afin de définir les contours et la portée du SOC, il faut débuter par analyser le contexte de la société, aussi bien en matière d'activité que d'organisation informatique. La nature des risques, menaces et impacts doit être définie. Les architectures techniques et fonctionnelles sont également à prendre en compte. En fonction de l'entreprise, voici des questions auxquelles une réponse doit être apportée :

- Le SOC doit-il être créé au niveau local, régional ou groupe ?
- Quels paramètres fonctionnels doivent être couverts : liste des applications métiers concernées, sécurité des services data, inclusion de la mobilité... ?
- Quels outils de sécurité rentrent dans le paramètre de contrôle : anti-spams, pare-feu, anti-virus... ?
- Sur quelles données informatiques doivent porter la collecte et l'analyse ?

exo data CYBERDEFENSE

2

S’assurer de l’adhésion globale des collaborateurs au projet

Vu l’importance stratégique pour une société de la mise en place d’un SOC, ce projet doit réunir toutes les parties prenantes dans un même élan afin de réussir. L’implication de la direction générale est généralement acquise, vu que c’est souvent elle qui décide de lancer le projet.

Le département informatique est forcément en première ligne mais les équipes opérationnelles, les clients voire les fournisseurs peuvent également être associés à la mise en place du SOC. Pour cela, il est possible de communiquer avec eux via des tableaux de bord, des lettres d’information et en utilisant la méthode REX (Retour d’Expérience).

exo data CYBERDEFENSE

3

Vérifier l'adéquation de la réponse aux obligations légales

Le SOC est tenu de répondre aux réglementations correspondant au secteur d'activité de l'entreprise concernée, qu'il s'agisse de structures commerciales et industrielles classiques ou d'opérateurs d'importance vitale (OIV), qui sont des organisations dont les activités ont été reconnues comme dangereuses ou indispensables par le gouvernement.

Parmi les réglementations figurent le RGPD (Règlement Général de Protection des Données) et la LPM (Loi de Programmation Militaire). Ils imposent notamment de mettre en place des systèmes permettant une corrélation et une analyse des journaux informatiques. Le cadre réglementaire détaillé se trouve dans le référentiel d'exigences destiné aux PDIS (Prestataires de Détection des Incidents de Sécurité) défini par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). Ce cadre légal demande aussi d'informer les autorités très rapidement en cas d'incidents.

D'autres réglementations s'appliquent selon l'activité de la société : HDS (Hébergement des Données Sensibles), SOX (Sarbanes Oaxley) qui concerne les entreprises - américaines ou non - cotées sur un marché des États-Unis, norme PCI DSS (Payment Card Industry Data Security Standard) relative aux paiements par carte bancaire sur internet, accords de Bâle III concernant le secteur bancaire...

exo data CYBERDEFENSE

4

Définir la meilleure stratégie de surveillance

Il s'agit de créer un document dans lequel sont définis le périmètre couvert, l'architecte choisi, les règles de détection, les processus de maintien... Grâce à ce document, il est possible de vérifier l'efficacité du SOC, de surveiller la conformité de son fonctionnement et d'anticiper sa montée en puissance.

exo data CYBERDEFENSE

5

Choisir le niveau de sécurité acceptable

En dépit de tous les efforts mis en place, il est évidemment impossible de garantir 100 % de la sécurité informatique. Il faut donc définir les risques majeurs et les distinguer de ceux qui restent acceptables c'est-à-dire ne créant pas de gêne critique pour le fonctionnement de l'entreprise. Répondre aux questions suivantes permet d'effectuer des choix :

- Quels incidents mettent en péril l'activité ?
- Quels sont les 10 scénarios de menace à impérativement contrecarrer ?
- Quels risques la société peut-elle accepter ?

exo data CYBERDEFENSE

6

Instaurer une politique de supervision

Grâce à l'établissement de scénarios de menace détaillés et au choix des risques majeurs à éviter, il est possible de définir les procédures de détection des incidents préjudiciables, l'architecture adaptée, les outils de reporting adéquats...

Afin de donner une visibilité maximale à la Direction de la société, un état des lieux journalier, bref mais précis, peut être mis en place.

exo data CYBERDEFENSE

7

Déployer la solution

La phase d'implémentation du SOC consiste à traduire la PSSI (Politique de Sécurité des Systèmes d'Information) et les orientations définies dans la politique de supervision en termes techniques. Il s'agit également de mettre en place l'ensemble des modèles organisationnels et des procédures pour mener à bien l'exploitation du SOC.

Afin d'assurer une mise à jour efficace des systèmes d'information, il est conseillé de prévoir une politique de gestion des correctifs (ou patch management) qui permet d'industrialiser les processus visant à détecter, analyser et déployer les mises à jour de sécurité logicielles.

exo data CYBERDEFENSE

8

Organiser le MCS (Maintien en Condition de Sécurité)

Complémentaire du MCO (Maintien en Condition Opérationnelle), le MCS a pour but d'assurer un fonctionnement optimal du SOC, notamment par des actions de maintenance préventive et corrective ainsi que par l'analyse des impacts des attaques s'étant réellement produites.

Afin de vérifier la bonne configuration globale du système et de prouver la fiabilité du SOC, des scripts de hard.

exo data CYBERDEFENSE

4. Pourquoi externaliser le SOC ?

exo data CYBERDEFENSE

Avec un coût important dû non seulement au fonctionnement en continu mais aussi à la rareté des profils pointus dans le domaine de la cybersécurité,

le SOC en interne est souvent délaissé au profit d'une solution en externe. Un SOC externe est à la fois plus performant et moins onéreux, et permet à la société de bénéficier d'une mutualisation des savoirs et des ressources humaines. Avant de choisir un SOC externe, une évaluation est recommandée concernant les profils des experts ainsi que les méthodes employées. De plus, collaborer avec un prestataire proposant un SOC en mode « Follow the sun » avec des équipes françaises disséminées dans le globe peut être une solution des plus avantageuses.

exo data CYBERDEFENSE

Les difficultés inhérentes à un SOC en interne

Un des principaux points noirs de la mise en place d'un SOC en interne est évidemment son coût. Le budget est conséquent pour deux raisons.

Tout d'abord, le SOC doit être opérationnel 24 h/24 et 7j/7.

D'autre part, il faut constituer une équipe dédiée qui se compose de profils informatiques spécifiques. Comme ces experts sont très recherchés et peu nombreux, les recruter est à la fois difficile et coûteux. De plus, une fois embauchés, ces collaborateurs doivent être formés régulièrement afin de se tenir informés des dernières évolutions technologiques et il faut éviter à tout prix leur départ de l'entreprise.

4-1. Les bénéfices apportés par un SOC externalisé

exo data CYBERDEFENSE

- Une transparence facilitant la promotion du projet en interne : afin de sélectionner le prestataire, un appel d'offres est réalisé et la direction doit valider le budget alloué au SOC

- Une mutualisation des ressources humaines et des solutions techniques permettant un coût inférieur à celui d'un SOC interne

- Des experts en cybersécurité à disposition : un long processus de recrutement est évité et les analystes font bénéficier la société de l'expérience accumulée durant la surveillance d'autres environnements

- Un niveau de service sur-mesure : le Service Level Agreement (SLA) garantit à la société un niveau de service précis, notamment grâce à des indicateurs chiffrés et des éléments factuels

- Une cyberveille facilitée : les prestataires ont la capacité à consolider diverses sources d'information pour fournir un service de Threat Intelligence performant.

exo data CYBERDEFENSE

Comment évaluer un SOC externe ?

Avant de choisir quel SOC externe est le mieux adapté à ses besoins, toute société se doit de l'évaluer non seulement en termes techniques et méthodologiques mais aussi par rapport à la composition de ses équipes.

exo data CYBERDEFENSE

Côté RH, il est important de connaître les profils précis des différents membres des équipes, le nombre de personnes travaillant en fonction du moment de la journée ou de la nuit ainsi que le nombre d'experts pouvant être mobilisés dans le cas d'une attaque.

Pour la partie méthodologie, il est recommandé de s'informer sur les façons d'analyser les différents événements, sur les procédures applicables lors de la survenue d'un incident ou d'une attaque, sur le nombre et la qualité des rapports fournis en temps réel aux analystes, sur les modalités de communications entre les équipes du SOC etcelles de l'entreprise, etc.

Quant à l'avancement technologique du SOC, la répartition entre processus manuels et automatisés est importante. D'une part, une grande partie d'opérations manuelles implique une quantité importante d'Équivalent Temps Partiel (ETP). D'autre part, un grand nombre de tâches automatisées peut amener une réduction trop grande des interventions manuelles, ce qui pourrait engendrer des défaillances de sécurité. Le juste milieu est à trouver pour optimiser la sécurité informatique.

Serge Payet,
SOC Manager du groupe exodata

Cette évaluation du SOC est une manière de choisir la proposition la plus adaptée à une entreprise donnée.

Elle peut être appliquée de manière régulière, notamment pour s'assurer que le SOC remplit toujours ses fonctions même quand la structure de la société évolue.

Le SOC doit intégrer les éventuelles transformations de l'entreprise, qu'elles soient structurelles, relatives à une modification du portefeuille d'activités ou à un changement important dans le domaine de production. En effet, pendant les périodes de changements dans une société, le risque d'attaques informatiques est plus important.

exo data CYBERDEFENSE

Les challenges d'un SOC en externe.

Pour que le SOC externe fonctionne le mieux possible, il faut s'assurer d'une bonne communication entre les prestataires et les équipes informatiques internes.

Un temps suffisant doit être consacré à la compréhension des problématiques métiers de la société et de son organisation. Des procédures doivent être rédigées pour les différents cas de figure relatifs à la sécurité en impliquant des interlocuteurs internes et externes. Il s'agit de combiner au mieux l'expertise des prestataires en sécurité et les connaissances des services informatiques internes.

Le SOC externe implique une analyse des données et parfois un stockage à l'extérieur des locaux de la société. Cela demande de bien réfléchir aux mesures de sécurité requises afin que cette externalisation ne pose pas de problème en matière d'accroissement des risques. Une procédure de conduite du changement peut éventuellement être nécessaire afin que les collaborateurs comprennent et ne freinent ce processus de délégation de la gestion de la sécurité.

4-2. Les avantages du mode « Follow the sun »

La stratégie de surveillance internationale, également nommée « Follow the sun » (Suivre le soleil) s'appuie sur des équipes situées dans des zones géographiquement éloignées les unes des autres et qui gèrent la surveillance de la sécurité chacune à tour de rôle. Ce mode de gestion du SOC apporte plusieurs avantages par rapport à un SOC classique, installé dans une zone couverte par un seul fuseau horaire :

- Une grande réactivité : ce SOC assure une surveillance de l'informatique tous les jours et à toute heure

- Des conditions optimales de travail : chaque équipe travaillant pendant des horaires classiques, elle bénéficie de meilleures conditions de travail que celles des équipes devant opérer de nuit ou en horaires décalés

- Un coût réduit : le travail en heures ouvrées est forcément moins onéreux que celui de nuit

- Une gestion facilitée des tâches et une réduction des incidents grâce à une surveillance réellement ininterrompue toute l'année.

Dans le cas d'un SOC en mode « Follow the sun », le plus avantageux pour une entreprise française est de trouver un prestataire qui propose une surveillance internationale en se basant sur des équipes installées uniquement en France métropolotaine ainsi que dans les départements et territoires d'Outre-Mer comme par exemple la Martinique, la Guadeloupe, l'Île de La Réunion, la Nouvelle-Calédonie, etc.

5. L'évolution du SOC

exo data CYBERDEFENSE

Dans l'optique de mettre en place des SOC toujours plus efficaces, de nouvelles orientations se dessinent.

Ainsi, la rapidité de résolution des incidents est accrue par une utilisation des sandbox à des fins d'analyses détaillées des menaces. La cyberveille joue aussi un rôle important, en incluant aussi bien les données internes que des informations payantes externes.

Enfin, le Machine Learning enrichit le SOC de ses fonctionnalités prédictives.

5-1. Une efficacité améliorée grâce aux sandbox

exo data CYBERDEFENSE

LE CLASSEMENT DES SOC SELON LEUR MATURITÉ

Pour différencier l'état de maturité d'un SOC, il est possible de comparer le pourcentage réel d'automatisation des processus par rapport au pourcentage idéal à atteindre.

Plus cette différence est faible, plus le SOC est mature.
C'est ainsi que les SOC sont classés en niveaux : 0/1, 2, 3 et 4 avec comme différences respectives entre les pourcentages d'automatisation réels et idéaux d'environ 10 %, 7 %, 5 % et 3%.

Une utilisation différente des sandbox

Dans les entreprises ayant des SOC avancés, les investigations sur les incidents sont clôturées plus rapidement qu'avec des SOC moins évolués.

De même, la cause d'une attaque est plus souvent identifiée et la performance globale est accrue par l'utilisation de sandbox. Plus le SOC a un niveau de maturité élevé, plus il se sert des sandbox afin de mener des investigations. Il utilise les sandbox d'une manière différente d'un SOC moins évolué : il s'agit de passer au-delà de la simple identification de la menace pour vérifier la réalité de celle-ci en s'intéressant au contenu des fichiers suspectés.

En plus d'une action d'automatisation et de consolidation des outils, la sandbox intervient pour permettre une analyse poussée de menaces complexes.

5-2. L'utilité de la cyberveille

exo data CYBERDEFENSE

La cyberveille, également appelée Threat Intelligence, correspond à un ensemble de connaissances relatives à des menaces d'attaques informatiques qui sont étayées par des preuves telles que des indicateurs, des informations contextuelles, des mécanismes ...

Il existe 4 types de cyberveille :

Opérationnelle : Elle donne des informations sur les attaques en cours et les cyberpirates

Technique : Elle sert principalement à classifier les malwares selon leurs caractéristiques

Tactique : Elle se concentre sur les modes opératoires (techniques, tactiques) des cyberpirates

Stratégique : Elle analyse les tendances du moment.

exo data CYBERDEFENSE

Dans les entreprises qui utilisent des SOC, la cyberveille a bien sûr une place importante mais la source des données varie selon le type de SOC.

Dans les SOC de type 0/1, les flux de cyberveille prédominants sont eux publics. Par contre, dans ceux de type 4, ce sont des flux payants qui sont majoritairement utilisés.

exo data CYBERDEFENSE

5-3. Les apports du Machine Learning

exo data CYBERDEFENSE

Dans le cadre du SOC, le but du machine learning, ou apprentissage automatique, est de détecter les comportements qui s'écartent du modèle de normalité défini au préalable.

En se basant sur un grand nombre de données, le Machine Learning sert à découvrir des séquences répétitives (patterns) et à réaliser des prédictions.

Cette méthodologie intervient pour faire des cartographies préalables à des intrusions. Elle permet aussi de détecter des comportements suspects : exfiltration de données, propagation d'un malware, communications entre un malware et son centre de commande et de contrôle (C&C). Enfin, elle est également employée afin de détecter des actions suspectes réalisées par des utilisateurs : consultation inhabituelle de données (nature, volume, etc.), accès à des logiciels normalement non utilisés, usage de droits incompatibles avec les fonctions d'un collaborateur, etc.

exo data CYBERDEFENSE

Par exemple, pour détecter une évasion de données, il faut au préalable analyser les flux habituels d'informations de l'entreprise.

Après une phase de compréhension et de modélisation du trafic, des analyses encore plus poussées peuvent être réalisées : numéros de séquence, taille des paquets, nombre de paquets par secondes et par adresses IP, etc. Ensuite, tout flux sortant de la norme définie pourra être détecté. Il en va de même concernant la problématique des logiciels malveillants de type rogue, qui sont de faux antivirus affichant des détections fictives. Grâce à une cartographie du réseau, le Machine Learning est capable de les détecter.

exo data CYBERDEFENSE

exo data

reunion@exodata.fr | france@exodata.fr

caraibes@exodata.fr | pacifique@exodata.fr