QUODAGIS
Managed Services

eBook

10 bonnes raisons de se doter d'un SOC

Security Operation Center - Centre des Opérations de Sécurité

Par Gérard GOMEZ

10 bonnes raisons de se doter d'un SOC

Security Operation Center - Centre des Opérations de Sécurité

Lorsqu'il est correctement mis en œuvre, un centre des opérations de sécurité peut offrir à une organisation les avantages suivants :

1. Surveillance et analyse ininterrompues des activités suspectes.
2. Amélioration des délais et des procédures de réponse aux incidents.
3. Réduction des écarts entre le moment du « compromis » (mise en situation critique) et le temps moyen de résolution.
4. La garantie des actifs logiciels et matériels sont centralisés pour une approche plus globale de la sécurité.
5. Une communication et une collaboration efficaces sont fortement privilégiées.
6. Les coûts associé à la gestion des incidents de sécurité sont maîtrisés
7. Tous les acteurs peuvent se sentir plus à l'aise de partager des informations sensibles.
8. Plus de transparence et de contrôle sur les opérations de sécurité.
9. Chaîne de contrôle pour récupérer les données qui sont nécessaires si une organisation est censée poursuivre les auteurs de cybercriminalité.
10. Réductions des coûts liés aux impacts et au conséquences des incidents de sécurité

Un centre des opérations de sécurité (SOC) est un centre de commandement (Command Center) avec une équipe de professionnels de l'informatique possédant une expertise en sécurité de l'information, chargée de surveiller, d'analyser et de protéger une organisation contre les cyberattaques.

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. Le personnel SOC peut travailler avec d'autres équipes ou départements, mais est généralement autonome avec des employés qui ont des compétences de haut niveau en technologie de l'information et en cybersécurité.
De plus, la plupart des SOC fonctionnent **24 heures sur 24**, car les équipes sont organisées pour enregistrer en permanence l'activité et souvent les menaces.

Avant de solliciter un MSP (Managed Services Provider) pour bénéficier des services du SOC, un client et sa DSI doivent définir leur stratégie de cybersécurité qui s'aligne sur les objectifs et problèmes actuels de l'entreprise. Les dirigeants et la DSI feront référence à une évaluation des risques qui se concentre sur ce qu'il faudra pour maintenir la mission de l'entreprise (orientation métier) et fourniront ensuite des informations sur les objectifs à atteindre. **Le MSP définit les infrastructures et les outils nécessaires pour atteindre ces objectifs ainsi que les types de compétences nécessaires.**

La mise en œuvre de la politique de sécurité avec un SOC est devenue plus importante pour toutes les organisations, quelle que soit leur taille, car les violations de sécurité sont en augmentation et le coût associé à la perte de données est souvent élevé. Un SOC efficace permet non seulement de minimiser le coût d'une violation de données en répondant rapidement aux intrusions, mais également en améliorant constamment les pratiques de détection et de prévention.

Que fait un centre des opérations de sécurité ?

La stratégie globale d'un centre des opérations de sécurité consiste à collecter des données et à analyser ces données pour détecter toute activité suspecte afin de sécuriser l'ensemble de l'organisation. Les données brutes surveillées par une équipe SOC sont importantes pour la sécurité et proviennent généralement de pare-feu, de renseignements sur les menaces, de systèmes de prévention et de détection des intrusions, de sondes et de systèmes SIEM (Security Information and Event Management).

Des alertes sont ensuite mises en place afin d'avertir immédiatement les membres de l'équipe SOC si l'une des données est anormale ou affiche des indicateurs inhabituels (système compromis).

En général, les responsabilités fondamentales d'un SOC sont :

- **Découverte et gestion des actifs** - Cela comprend l'acquisition d'une connaissance élevée de tous les outils, logiciels, matériels et technologies utilisés au sein du SOC. Il vise également à s'assurer que tous les actifs fonctionnent correctement et sont régulièrement mis à jour.

- **Surveillance comportementale continue** - Tous les systèmes sont examinés 24h/24 et 7j/7. Cela permet aux SOC d'accorder un poids égal aux mesures proactives et réactives car toute irrégularité d'activité est détectée instantanément. Les modèles comportementaux sont utilisés pour former les systèmes de collecte de données sur ce qui compte comme une activité suspecte et peuvent être utilisés pour ajuster les informations qui pourraient être enregistrées comme faux positifs.

- **Conservation des journaux d'activité** - Toutes les communications et activités de l'organisation doivent être enregistrées par le SOC. Cela permet aux membres de l'équipe de revenir en arrière ou d'identifier les actions précédentes qui peuvent avoir entraîné une violation.

- **Classement de la gravité des alertes** - Un élément de la gestion des vulnérabilités consiste à s'assurer que les alertes les plus graves ou les plus urgentes sont traitées en premier. Cela fait partie du travail d'une équipe SOC pour classer les menaces de cybersécurité en termes de dommages potentiels.

- **Développement et évolution de la défense** - Une équipe SOC doit utiliser un plan de réponse aux incidents et agressions pour aider à défendre les systèmes contre les attaques. De plus, il leur appartient d'ajuster le plan si nécessaire lorsque de nouvelles informations sont connues.

- **Récupération après incident** - En plus d'empêcher et d'arrêter les violations de données, un SOC est également chargé de récupérer les données qui ont été compromises. Cela peut inclure la reconfiguration, la mise à jour ou la sauvegarde des systèmes.

- **Maintien de la conformité** - Tous les membres d'une équipe dans un SOC doivent suivre les normes de conformité réglementaires lors de la réalisation des business plans. En règle générale, un membre de l'équipe est chargé de former (voire « évangéliser ») et d'appliquer les règles de conformité.

Les capacités supplémentaires d'un SOC et de son personnel pourraient inclure le reverse engineering, l'analyse judiciaire, la télémétrie de réseau et la cryptanalyse en fonction des besoins spécifiques de l'organisation.

Toutes les responsabilités d'un SOC peuvent être divisées en trois catégories :

Prévention

Détection

Protection.

Organisation d'une équipe du centre des opérations de sécurité

Un centre des opérations de sécurité peut prendre diverses formes en fonction des besoins, des compétences techniques des employés, des ressources physiques et des modèles organisationnels.
Construire un SOC et son équipe est donc une approche personnalisée.
Les SOC sont dotés d'une variété de personnels qui jouent un rôle particulier dans les opérations de sécurité globales.

Les rôles et les responsabilités qui peuvent être trouvés dans un SOC comprennent :

- **Gestionnaire SOC** - Cet employé est responsable de la gestion des opérations quotidiennes du SOC et de son équipe. Cela fait également partie de son rôle de partager les informations avec sa direction et le client.

- **Technicien Répondant aux incidents** - Cet employé gère les attaques ou les violations qui se sont produites avec succès, respectant les processus et appliquant les modes opératoires nécessaires pour réduire et éliminer la menace.

- **Enquêteur judiciaire** - Cet employé est chargé d'identifier la cause profonde et de localiser la source de toutes les attaques, en collectant toutes les preuves disponibles.

- **Auditeur de conformité** - Cet employé s'assure que tous les processus du SOC et les actions des employés répondent aux exigences de conformité.

- **Analyste de sécurité** - Cet employé examine les alertes de sécurité pour les organiser par urgence ou par gravité et effectue régulièrement des évaluations de vulnérabilité. Les compétences de cet employé pourraient inclure la connaissance des langages de programmation, des capacités d'administrateur système et des meilleures pratiques de sécurité.

- **Chasseur de menaces** - Cet employé examine les données collectées par les outils du SOC pour identifier les menaces les plus difficiles à détecter. Les tests de résilience et de pénétration peuvent également faire partie de ses missions récurrentes.

- **Ingénieur sécurité** - Cet employé développe et conçoit des systèmes ou des outils nécessaires à la mise en œuvre de capacités efficaces de détection d'intrusions et de gestion des vulnérabilités.

En plus de décider quels rôles et missions de l'équipe, les différents types de modèles organisationnels qu'un SOC peut avoir sont :

- ***Dédié*** - Ce modèle dispose d'une installation dédiée chez le client ou en centre de services avec du personnel exclusivement dédié à un client et un périmètre de service.

- ***Mutualisé / Partagé*** - Ce modèle utilise du personnel mutualisé/partagé à temps partiel et qui répondent aux alertes de sécurité de plusieurs Clients ou interviennent sur différents périmètres de service en centre de service.

- ***Distribué / cogéré*** - Ce modèle a des membres d'équipe semi-dédiés qui sont employés en interne ou en centre de services pour travailler aux côtés des équipes de la DSI.

- ***Centre de Commandement*** - Ce modèle fournit des informations sur les menaces et une expertise en matière de sécurité à d'autres centres d'opérations de sécurité, généralement dédiés. Il n'est pas impliqué dans les opérations ou processus de sécurité proprement dits, mais uniquement dans le domaine du renseignement (intelligence), du suivi (reporting et analyse) et de la veille (évolution).

- ***Conseil / AMOA*** - Ce modèle supervise tout type d'installation ou d'initiative axée sur la sécurité, y compris d'autres types de SOC ou d'équipes du service informatique.

- ***Externalisé / Étendu*** - Ce modèle dispose d'une installation dédiée et d'un personnel dédié, mais les rôles et responsabilités s'étendent à d'autres domaines critiques de la gestion des technologies de l'information, tels que les opérations de réseau (NOC).

Toutes les possibilités ci-dessus doivent disposer d'un plan de continuité des opérations (PCA) solide et régulièrement testé qui peut nécessiter la combinaison ou le remplacement des modèles organisationnels choisis. On peut retrouver chez certains MSP la capacité de SOC multi-sites (différentes implantations).

Bonnes pratiques du centre des opérations de sécurité

Alors que la technologie et les initiatives de cybersécurité ont continué de croître et de progresser, il existe plusieurs « meilleures pratiques » convenues pour gérer un SOC. La suggestion la plus courante consiste à mettre en œuvre des processus d'orchestration, d'automatisation et de réponse de sécurité dans la mesure du possible. La combinaison de la productivité d'un outil d'automatisation avec les compétences techniques d'un analyste permet d'améliorer l'efficacité et les temps de réponse aux incidents. Il permet également au centre de fonctionner plus efficacement sans interruption.

De plus, **les SOC s'appuient fortement sur les connaissances des membres individuels de l'équipe**. Par conséquent, les gestionnaires doivent veiller à ce qu'une formation continue soit dispensée pour rester au fait des menaces émergentes en matière de cybersécurité, des rapports d'incidents et des vulnérabilités. Tous les outils de surveillance SOC doivent ensuite être mis à jour pour refléter tout nouveau changement.

De même, un SOC n'est jamais aussi efficace que les stratégies qu'il a mises en place. Par conséquent, les gestionnaires devraient mettre en œuvre des protocoles opérationnels solides qui sont suffisamment robustes lorsqu'une réponse cohérente, rapide et efficace est attendue.

Quelques autres bonnes pratiques SOC incluent la collecte d'autant de données que possible aussi souvent que possible, en tirant parti de l'analyse des données et en développant des processus plus faciles à mettre à l'échelle pour la croissance.

Il est indispensable que le SOC dispose aussi de certifications ISO :

- Système de gestion de la sécurité de l'information ISO 27001
- Contrôles de sécurité ISO 27002
- Système de gestion des risques ISO 31000
- Système de gestion de la continuité des activités ISO 22301 (Business Continuity Management)

NOC ou SOC ?

Bien qu'ils puissent sembler ou être similaires, il existe des différences majeures dans les objectifs d'un centre d'exploitation de réseau et d'infrastructure (NOC) et ceux d'un centre des opérations de sécurité.

Un NOC et un SOC ont en commun des critères clé : ils doivent travailler avec la DSI pour résoudre les incidents informatiques, et jamais avec l'utilisateur final (end-user). Cependant, lorsqu'un NOC se concentrera sur la surveillance et la maintenance à distance de l'environnement informatique d'un client pour respecter les SLA et garantir la disponibilité du client sans dysfonctionnement technique, un SOC sera beaucoup plus axé sur la sécurité : Il surveille les vulnérabilités, les vecteurs et angles d'attaque et les menaces émergentes sur un réseau client. Les équipes du SOC sont prêtes à détecter les anomalies et à atténuer les cyberattaques à mesure qu'elles surviennent.

Un centre d'exploitation de réseau (NOC) est similaire à un SOC dans la mesure où ses responsabilités de base consistent à identifier, enquêter, classer et résoudre les problèmes. Les NOC fonctionnent également avec un gestionnaire de NOC, qui supervise tous les employés et processus au sein du centre. La plupart des employés d'un NOC sont des ingénieurs réseau ou de la circulation qui peuvent avoir des antécédents plus spécialisés ou techniques pour couvrir un large éventail d'incidents.

La plupart des SOC utilisent un processus de gestion des informations et des événements de sécurité (SIEM) qui regroupe les informations de divers flux de données des systèmes axés sur la sécurité. Tout, depuis les systèmes de découverte de réseau et d'évaluation de la vulnérabilité, les systèmes de gouvernance, de risque et de conformité, les outils de test d'intrusion, les systèmes de détection et de prévention des intrusions, les systèmes de gestion des journaux ; L'analyse du comportement du réseau et bien plus, est collectée et analysée par les techniciens SOC, qui sont eux-mêmes des experts en sécurité, formés et expérimentés.

Une différence majeure dans le type d'incidents auxquels les SOC et les NOC répondent est leur nature. Les incidents systèmes, réseaux, applications ou poste de travail sont généralement des événements naturels et presque habituels, tels qu'un dysfonctionnement ou une surcharge de trafic. Les problèmes de sécurité sont plus « intelligents » et peuvent provenir de sources « indépendantes de la volonté de l'organisation ». Pour cette raison, un NOC doit couvrir plus régulièrement les réparations ou configuration de systèmes, logiciels et d'équipements, alors qu'un SOC doit faire face pour la plupart des incidents à des événements « logiques ».

Faire ou faire-faire ?

Les coûts fixes de main-d'œuvre et d'infrastructure liées à la constitution d'une équipe interne sont généralement trop élevés à couvrir, tout en maintenant une entreprise rentable et en croissance. Même avec un personnel complet, il ne serait pas en mesure de s'organiser pour prendre en charge les pics et creux de la demande tout en se préparant simultanément à la maintenance des tâches informatiques quotidiennes qui doivent être effectuées.

Au lieu de cela, le fournisseur de services managés (MSP) qui dispose d'un SOC peut assumer la plupart des travaux techniques qui doivent être effectués quelque soient la variabilité de la charge**. Au lieu d'une opération interne lourde, un SOC agit comme une extension de la main-d'œuvre existante du service informatique interne, laissant le personnel technique de la DSI se concentrer sur des projets à forte valeur ajoutée et à fort retour sur investissement pour le Client.**

Les Services Desk (SD), les Centres de Opérations Réseau (NOC) et les centres des opérations sécurité (SOC) fournissent de nombreux services - tous ont une valeur critique pour une DSI et les utilisateurs finaux - mais il y a peu de chevauchement dans leurs missions ou objectifs. **Au contraire, en sollicitant les services complémentaires chez un MSP, en s'appuyant sur ses équipes, ses compétences et ses offres pour profiter d'une gamme plus large de solutions et services, les DSI bénéficient d'un plus grand avantage opérationnel et économique qu'en tentant de fusionner les tâches associées à ces missions en une seule équipe hybride au sein de sa propre organisation.**

A propos de QUODAGIS Managed Services

Vos équipes informatiques sont écartelées entre différentes missions et des attentes contradictoires. Il leur est difficile de se consacrer aux nouveaux projets et, en même temps, répondre aux demandes des utilisateurs au quotidien ou se concentrer sur les projets métier à forte valeur ajoutée pour votre entreprise.

QUODAGIS Managed Services est ce qu'on appelle un MSP : Managed Services Provider. Pour vous aider, QUODAGIS Managed Services propose des solutions de services managés et vous garantit les résultats concrétisés par des SLA, c'est-à-dire des engagements de niveaux de service.

Quels sont ces services ? La mise à disposition de personnel, sur site ou dans nos locaux, 2 centres de services, situés à Aurillac, et à Barcelone en Espagne, appuyés par nos bureaux de Paris et de Toulouse, pour des projets ponctuels ou un service récurrent, avec des équipes dédiées ou mutualisées, en plusieurs langues, pendant les heures ouvrées mais aussi sur des plages étendue, jours fériés, nuits et week-ends.

QUODAGIS s'appuie sur des méthodes et des pratiques reconnues du marché, des outils performants, et des équipes compétentes. Elles sont certifiées ITIL et QUODAGIS Managed Services est certifié ISO9001 et ISO27001.

Paris, Aurillac, Toulouse, Barcelone
+33 4 71 43 49 96 | managed-services.quodagis.fr | quodagis.fr