La solution Group SOC tient l'objectif de renforcer la sécurité de votre SI et détecter ses vulnérabilités et ses tailles de sécurité afin de les corriger / protéger.

Description du service

En s'appuyant sur l'expertise de la DSIT éprouvée à l'échelle du Groupe EDF, Group Support Services propose un service de surveillance 24/7 des évènements de sécurité de votre SI pour mieux prévenir et répondre efficacement aux cyberattaques.

Cette prestation comprend les éléments suivants :

- Surveillance et alerte en temps réel basée sur une plate-forme SIEM (Security Information and Event Management) sécurisée et protégée par des pare-feu,
- Service basé sur deux SIEM de production, répliqués pour assurer la continuité du service,
- Plateforme SIEM située dans un Datacenter de niveau 4,
- Plateforme SIEM située dans une zone spécifique entièrement sécurisée sur le plan technique et géographique au sein du Datacenter,
- Les collecteurs cryptent puis compressent les logs avant de les envoyer à la plate-forme SIEM via la Group WAN,
- L'accès au SIEM est protégé par un compte individuel avec un mot de passe et des logs d'accès stockés et surveillés,
- Les licences SIEM et Collectors incluses dans les coûts du service,
- Intégrité des données : l'accès aux logs de données brutes est entièrement protégé (serveurs sur le datacenter dans une zone sécurisée par des pare-feu, calcul du hachage SHA-256 de chaque journal reçu).

Notre équipe SOC bilingue (français et anglais) vous accompagne et vous conseille sur la prévention et les actions post mortem, en plus d'assurer la surveillance des applications et infrastructures.

Prérequis

Pour l'infrastructure du client :

- Action du Client pour fournir et maintenir l'infrastructure requise pour le SOC Collector (environnements de pré-production (quand ils sont disponibles) et de production) : Allocation des ressources de la VM, configuration et installation, configuration du réseau.
- Configuration du réseau pour l'envoi du journal de bord du client au Group SOC (ouverture des règles de pare-feu).
- Configuration des dispositifs de sécurité pour rediriger les logs de sécurité vers le collecteur Group SOC.
- Fournir des droits d'accès pour l'équipe du Group SOC sur le(s) collecteur(s) : environnements de pré-production (lorsqu'ils sont disponibles) et de production.

Pour la configuration de la plateforme SOC :

- Informations sur les infrastructures (cartographie des actifs, cartographie IP, hiérarchie des réseaux…).
- Lors de l'analyse des performances, des informations supplémentaires sont nécessaires (pcap, fichiers infectés…).
- Les scénarios d'attaque déjà existants du Client doivent être intégrés dans le SIEM et les alertes existantes doivent être mises en œuvre dans le SIEM. Ils sont validés par le client.
- Les dispositifs collectés enregistrent les connaissances et les spécifications (types requis, format).
- Comptes de service avec les droits nécessaires pour extraire les logs des appareils si la méthode de collecte des logs l'exige.
- Exigences légales et réglementaires concernant la surveillance et le logging.
- Liste des technologies et de leurs caractéristiques (logiciel, version…) utilisées dans l'infrastructure surveillée par le client.
- Liste des parties prenantes contactant le service de gestion des vulnérabilités.
- Les scénarios de corrélation du client sont à intégrer dans le Group SOC, à condition qu'ils soient suffisamment détaillés.
- Le client notifiera le Group SOC une semaine avant les tests de pénétration prévus car cette activité génère des alertes de sécurité et un volume important de logs.
- Le client fournira et tiendra à jour au moins une fois par an une liste de mots-clés afin d'améliorer la surveillance effectuée sur Internet et le dark web.

Pour l'intégration de nouvelles sources de logs :

- Réalisation d'une analyse de risque ARISOC pour les nouvelles demandes/projets ou si ce n'est pas possible, le client doit fournir d'autres analyses de risque réalisées précédemment qui seront validées par le Groupe SOC.
- Le client doit fournir l'expertise et les informations nécessaires pour aider le groupe SOC à élaborer des règles de corrélation pour les infrastructures/applications spécifiques.
- QRadar supporte nativement la collecte de logs pour des centaines de produits et d'appareils différents. La liste comprenant les appareils/produits, les

protocoles et les formats d'événements est accessible à partir du lien ci-dessous :
https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/com.ibm.dsm.doc/r_supported_dsm_list.html).
Pour tout autre type de log, des développements spécifiques devront être effectués par le groupe SOC afin d'extraire et de corréler les informations nécessaires à la filiale.

Nos engagements

Indicateur	Engagement	Fréquence de mesures	Rapport d'indicateur
Détection des incidents par gravité Basé sur un service 24/7 de surveillance et d'alerte	• 20 minutes dans 90% des cas de chaque niveau de gravité • 2 heures pour les 10% restants de chaque niveau de gravité	Mensuellement	Mensuellement
Prise en charge, communication au client et proposition d'intervention pour un incident de gravité =1 Basé sur un service 24/7 de surveillance et d'alerte	A partir de la détection des incidents : • 2 heures dans 90% des cas • 8 heures pour les 10% restants		
Prise en charge et proposition de réponse aux incidents et communication au client pour les incidents de gravité 2 et 3 Basé sur un service 24/7 de surveillance et d'alerte	A partir de la détection des incidents, Dans 90% des cas : • Gravité 2 : 8 heures • Gravité 3 : 11 heures Pour les 10% restants : • Gravité 2 : 24 heures • Gravité 3 : 48 heures		
Disponibilité des plateformes QRadar et Secops (sans compter la période d'indisponibilité prévue)	• QRadar : 99% • SECOPS : 95 %		

Pour toute question non liée à la détection et à la communication des incidents, les heures d'ouverture du groupe SOC sont comprises entre 8h00 et 18h00 (heure française) – les jours ouvrables uniquement.

Le service de surveillance et d'alerte 24 heures sur 24 et 7 jours sur 7 ne sera pas entièrement disponible pendant les périodes d'arrêt prévues (communiquées au préalable) pour les opérations de mise à niveau du SIEM.

Les degrés de gravité des incidents sont les degrés de gravité définis selon le modèle de soutien des services du GIO.

Offres & services à la carte

Services additionnels disponibles lors de la signature du cahier des charges :

- Intégration de nouveaux périmètres de surveillance (applications ou infrastructures) :

    - Si l'intégration d'un seul élément d'un type d'infrastructure connu avec des règles déjà présentes sur le catalogue de règles du Group SOC nécessite plus de 3 jours de travail, alors elle fera l'objet d'un devis fourni par G2S et validé par le client avant toute action.
    - Si l'intégration d'un seul élément concerne une nouvelle application/infrastructure spécifique au client, elle fera l'objet d'un devis fourni par G2S et validé par le client avant toute action.
    - Si pour un projet ou une extension d'un périmètre existant qui peut être réalisé dans un délai bien défini, l'intégration concerne de multiples éléments d'un type d'infrastructure connu avec des règles déjà présentes dans le catalogue de règles du Group SOC et/ou une nouvelle application/ infrastructure spécifique au client, alors elle fera l'objet d'un devis fourni par G2S et validé par le client avant toute action.
    - Le processus d'intégration comporte les étapes suivantes :
        1. Un premier atelier pour discuter des scénarios de risque identifiés par le client et définir avec le Group SOC les règles de corrélation qui peuvent en être déduites.
        2. La collecte de logs dans l'environnement de pré-production (lorsqu'il est disponible).
        3. La mise en œuvre des règles définies sur QRadar pré-production (lorsque le collecteur de pré-production est disponible).
        4. La phase de test d'acceptation pour déclencher les règles définies.
        5. La mise en œuvre des règles définies sur le QRadar de production.
        6. La collecte des logs dans l'environnement de production.

- Surveillance et démantèlement des domaines web de phising ayant fait leurs preuves :

    - Suivi de l'évolution d'un domaine web de phishing (après détection).
    - En cas de phising avéré utilisant des éléments de la marque client pour semer la confusion chez les utilisateurs et nuire à son image publique, les actions en justice nécessaires seront engagées pour supprimer ou désactiver l'accès à un site internet.
    - Plan contenant un montant fixe de démantèlement par mois par filiale.
    - Aucun engagement sur le délai de démantèlement car il dépend des lois de chaque pays hébergeur de site internet.

- Analyse avancée approfondie et analyse médico-légale :
    - Cela comprend les analyses qui prennent plus d'une demi-journée : enquête sur l'activité de l'utilisateur, analyse PCAP, rétro-ingénierie des logiciels malveillants, enquêtes médico-légales…
- Reports mensuels additionnels :
    - Se concentrer sur des applications ou des projets spécifiques.
    - Le contenu et les chiffres du rapport global ne seront pas modifiés si d'autres sont créés.

- Formation avancée sur les outils SOC :
    - Une demi-journée de formation en ligne via Skype pour QRadar et SECOPS (outil de ticketing).
    - Des bases de QRadar (architecture, interface console) aux recherches avancées et aux conseils.
    - L'interface SECOPS, la gestion des incidents, les recherches et les rapports.

- Sensibilisation des utilisateurs :
    - Organiser avec le client des campagnes de faux phishing.
    - Fournir au client du matériel de sensibilisation des utilisateurs.

- Autres :
    - Toute autre demande concernant le service Group SOC prenant plus d'une demi-journée de travail qui n'est pas liée à un changement de périmètre et non couverte par les services additionnels fera l'objet d'un devis.

Services additionnels disponibles à l'avenir et déjà prévus lors de la signature du cahier des charges :

- Boîte aux lettres dédiée à l'analyse de la cyber-sécurité du courrier électronique interne
    - Vérification des URL et des fichiers joints pour détecter les contenus malveillants.
    - Détection du phishing, du spam et des tentatives de fraude.
    - Le client doit fournir un contact pour une analyse de 2nd niveau si une intensification est nécessaire.
    - La réponse sera fournie en français ou en anglais.

Domaine d’application

Ouvert à toutes les filiales d’EDF.

Durée de l’engagement

La durée minimum d’engagement est de 1 an.

Modalités de souscription

Contactez votre responsable commercial G2S.

Références clients