SERVICES DE SOC

Détection & Réponse à incident, Surveillance 24/7/365

Dans un environnement technique complexe & hybride, la réglementation intégrant le risque cyber est de plus en plus exigeante.

La mise en place d'un dispositif de détection et de traitement des incidents de violation de données est devenue stratégique pour limiter les impacts financiers et de réputation qui pèsent sur les organisations.

Nos offres SOC

SOC
CLÉ EN MAIN

Notre offre clé en main vous permet de déployer la solution Azure Sentinel pour un SIEM prêt à l'emploi. Vous pourrez ainsi rapidement construire un centre de sécurité des opérations (SOC) moderne et bénéficier des avantages et automatismes proposés par Koasec.

SOC
HYBRIDE

Nous supportons Sentinel et surveillons votre environnement 24/7. Nous vous assurons une gestion efficace de votre SIEM grâce à notre équipe experte et à l'aide d'outils de surveillance avancés. Cette offre vous permet de bénéficier de la flexibilité et de la sécurité d'une solution hybride, adaptée à vos besoins spécifiques.

SOC
GÉRÉ

Notre offre de SOC géré vous permet de bénéficier d'une surveillance de sécurité informatique complète. Nous déployons Sentinel, supportons le SIEM, surveillons les alertes 24/7, et vous alertons en cas d'attaque avérée. Vous pouvez ainsi vous concentrer sur votre entreprise en toute tranquillité.

Nos engagements

SURVEILLANCE **24/7/365**

PRISE EN CHARGE DES INCIDENTS EN **15 MINUTES**

RÉPONSE AUX INCIDENTS INCLUANT **ISOLATION DE LA MENACE**

GESTION ET MISE À JOUR DES **RÈGLES SOAR**

SERVICE EN **FRANÇAIS** ET AU **QUÉBEC**

GESTION DES **TABLEAUX DE BORD**

Nos services SOC

- **Surveillance du Dark Web**
- **Architecture de solution de surveillance**
- **Intégration de journaux "custom"**
- **Développement de connecteurs**
- **Développement de règles SIEM**
- **Développement de règles d'orchestration SOAR**
- **Optimisation des coûts**
- **Support aux besoins de conformité.**

Certifié

Microsoft Solutions Partner

Forts d'un savoir-faire reconnu dans l'implémentation de plusieurs technologies SIEM, Koasec a su démontrer son expertise dans l'intégration de la technologie SIEM Microsoft Sentinel.

Cette expertise lui a valu le titre de **partenaire désigné Microsoft dans les catégories de sécurité et d'infrastructure depuis 2023**, ainsi que **le titre de spécialiste dans la catégorie 'Threat Protection' en 2024.**

Cela fait de nous un partenaire de choix pour le déploiement et la gestion de Sentinel au Québec.

Microsoft Solutions Partner
Infrastructure
Azure

Microsoft Solutions Partner
Sécurité
Spécialiste
Protection contre les menaces

www.koasec.com
450-499-6050
contact@koasec.com

SERVICES DE CENTRE D'OPÉRATIONS DE SÉCURITÉ (SOC) 24/7/365

KOASEC

SOC Géré

Un service complet de détection et de réponse aux incidents de sécurité

Le SOC Géré de KOASEC offre une expertise en cybersécurité pour surveiller votre infrastructure informatique et la protéger contre toutes sortes de menaces et de cyberattaques, 24 heures sur 24 et 7 jours sur 7. **Ce service couvre les environnements cloud, postes de travails, serveurs, appareil mobiles, utilisateurs, logs, réseaux, etc.**

- Public Cloud
- Productivité
- Identité
- Réseau
- Endpoint

Solution centralisée de surveillance

SOC et COCD

- **Examinez et répondez aux menaces plus rapidement.**
- **Priorisez les alertes à haut risque.**
- **Gagnez du temps grâce à une intégration transparente.**
- **Hiérarchisation des incidents en fonction du risque.**
- **Réduire le temps médian de réponse (MTTR).**
- **Atténuez la fatigue liée aux alertes.**
- **Maximisez la collaboration entre les équipes.**
- **Assurez un enregistrement complet des activités.**

Koasec améliore les capacités de votre SOC/COCD en fournissant **une solution centralisée et complète conçue pour offrir des informations approfondies à vos analystes. Notre solution, spécifiquement adaptée aux environnements multi-SIEM**, permet de centraliser la collecte des incidents issues de plusieurs systèmes de gestion des événements et des informations de sécurité (SIEM).

Cette centralisation permet d'optimiser la visibilité globale et d'unifier les réponses aux cybermenaces en consolidant les informations provenant de différentes sources. Ainsi, votre SOC est équipé pour identifier et atténuer efficacement les cybermenaces, quelle que soit leur origine. Grâce à cette approche centralisée, votre entreprise peut maintenir une posture de sécurité solide et prendre des actions en temps réel face aux incidents.

Des analystes SOC toujours prêts à détecter et à répondre aux menaces

SKARLET

AICPA SOC

PRESCIENT SECURITY

www.koasec.com

450-499-6050

contact@koasec.com