Contact@cyber-expert.fr
06 04 50 71 06

S.O.C ON PREMISE

Le S.O.C Sur Site de votre Entreprise

Déployer un SOC sur site vous permet d'être autonome sur vos enjeux de cybersécurité mais aussi la supervision de votre infrastructure. Cette configuration permet un contrôle total de la plateforme de sécurité et la possibilité de la personnaliser en fonction du contexte spécifique de l'entreprise.

FONCTIONNALITÉS & AVANTAGES

- Grâce à une stack ELK (Elasticsearch, Logstash, Kibana) optimisée, nous collectons, normalisons et corrélons les événements pour **identifier immédiatement les menaces** et réduire le temps de **détection des incidents.**
- Notre SOC **analyse en continu les logs de votre infrastructure** (serveurs, endpoints, réseaux, applications) pour **détecter les anomalies et comportements suspects**, tout en **minimisant les faux positifs** grâce à des règles de corrélation avancées
- **Intégration de pipelines Logstash** personnalisés et d'outils de threat intelligence pour **enrichir automatiquement les logs** avec des sources externes (IOC, bases de menaces, etc.), réduisant ainsi la charge opérationnelle et le bruit des alertes inutiles.
- Un SOC On-Premise avec ELK permet de **conserver le contrôle total sur les données sensibles** et d'assurer la **conformité avec les réglementations en vigueur** (ISO 27001, RGPD, NIS2). Toutes les actions et incidents sont journalisés et traçables pour **faciliter les audits de sécurité**.
- Nos ingénieurs optimisent ELK pour une **scalabilité horizontale**, garantissant ainsi une **montée en charge fluide** et une **gestion efficace des logs même sur des infrastructures complexes**.
- Déploiement de **tableaux de bord personnalisés et dynamiques**, offrant une vue d'ensemble sur les incidents de sécurité et permettant **d'accélérer les processus d'investigation.**

LES BÉNÉFICES CONCRETS POUR VOUS

Un SOC sur votre site avec Cyber Expert est construit pour aller au-delà de la sécurité. Nous offrons des retours mesurables à court et long terme.

Réduction des coûts liés aux incidents

Grâce à une surveillance en temps réel et à des équipes dédiées, vous minimisez les interruptions de service et les pertes financières liées aux compromissions de données.

Impacts positifs sur la conformité et la réputation

Un SOC sur site est un atout essentiel pour la conformité aux réglementations comme le RGPD, ISO 27001 ou NIS2 et positionne votre entreprise comme un acteur de confiance sur son marché.

Optimisation des coûts de collecte et de stockage de données

Grâce à des technologies comme ELK (Elasticsearch, Logstash, Kibana), vous pouvez réduire les coûts liés aux infrastructures de stockage et garder un contrôle total sur vos données.

Amélioration de l'efficacité des équipes internes

Un SOC sur site outille et renforce vos équipes internes grâce à des workflows automatisés et une meilleure visibilité sur les incidents il vous permet de réduire le temps consacré aux tâches répétitives et améliore la réactivité de vos analystes face aux cyberattaques.