SOC NSI

Qu'est-ce qu'un SOC ?

Un SOC (Security Operations Center) est un centre opérationnel de sécurité managé 24/7 par une équipe d'expert en cybersécurité.

Les équipes d'expert utilisent une suite d'outils sophistiqués qui vont permettre de prévenir, détecter, analyser et répondre aux problèmes de sécurité des organisations.

Le SOC intervient non seulement en réponse aux incidents, mais aussi en prévention, en anticipant les menaces.

Technologies composantes d'un SOC

SIEM
Outil qui collecte et centralise les journaux (logs) de l'ensemble du réseau

SOAR
Outil communiquant avec d'autres solutions de sécurité qui permet d'automatiser des tâches telles que le tri des alertes et l'enquête sur les évènements

Gestion et réponse des incidents

Equipe présente 24/7 sur 3 niveaux pour une gestion rapide et efficace des incidents

NIVEAU 1

Surveillance des consoles de sécurité pour qualifier la menace

NIVEAU 2

Investigation approfondie des alertes du niveau 1 avec des outils avancés

NIVEAU 3

Chasse proactive des menaces non détectées et gestion des incidents les plus complexes et critiques par les cyber spécialistes

Face à la hausse exponentielle des attaques par ransomware et aux exigences réglementaires en matière de protection des données personnelles, le SOC s'impose aujourd'hui comme une nécessité.

Il constitue un investissement stratégique au service de la résilience de votre organisation.

C'est l'assurance d'évoluer dans l'environnement numérique en toute confiance, avec des experts mobilisés en permanence pour protéger vos actifs les plus précieux : vos données.

0561889955 contact@nsicorporation.com 2 rue du LAVET, 31210 AUSSON