SERVICE DE SURVEILLANCE DE LA CYBERSÉCURITÉ 24/7 (SOC / SIEM) EXEMPLE DE RÉUSSITE

Entreprise transport privée

SURVOL

Notre client était à la recherche d'une approche proactive pour protéger ses données et ses systèmes contre les cyberattaques. Il se méfiait particulièrement des attaques Apache Tomcat sur des serveurs vulnérables. Afin de prévenir de telles attaques, le client souhaitait aussi obtenir plus de visibilité sur les activités qui se déroulaient au sein de ses systèmes et de ses réseaux. Pour mettre en œuvre cette stratégie, le client a décidé de souscrire à notre service de surveillance de la cybersécurité 24/7.

Visibilité accrue

Surveillance de l'activité 24/7

DÉFIS

En travaillant dans l'environnement du client, nous voulions construire une base pour la mise en œuvre d'un SIEM sécurisé qui répondra aux besoins de couverture de l'infrastructure croissante du client.

NOTRE CONTRIBUTION

Gardien Virtuel a dès lors commencé la surveillance de l'infrastructure du client avec une plateforme SIEM de pointe : QRadar d'IBM. Ce client souhaitait également réduire davantage sa surface d'attaque en engageant notre service de gestion des vulnérabilités, service également fourni par nos analystes SOC en utilisant Qualys.

SERVICES

- Collecte, corrélation et stockage des journaux
- Surveillance comportementale des usagers
- Surveillance du trafic réseau et Gestion de la vulnérabilité
- Gestion de la protection des points de terminaison (EDR)

RESULTS

Le client a continué à développer cette approche SIEM efficace avec notre équipe et continue à améliorer l'étendue de ses besoins SOC croissants. Aujourd'hui, le client se retrouve avec une surface d'attaque réduite et une visibilité complète sur les activités suspectes sur ses systèmes.