RSECURE

Antivirus, MDR ou SOC ?

Comment choisir la solution la mieux adaptée à votre stratégie de sécurité ?

Face à la multiplication et à la sophistication des cybermenaces, toutes les solutions de sécurité ne répondent pas au même besoin. Antivirus, service MDR et Security Operations Center (SOC) jouent chacun un rôle distinct dans la protection d'un système d'information. Comprendre ces niveaux de protection permet de choisir la solution la plus adaptée à vos enjeux, à vos ressources et à votre niveau de maturité en cybersécurité.

Critères	Antivirus	Service MDR	Security Operations Center (Rsecure)
Objectif	Bloquer les menaces simples et connues	Bloquer et répondre aux menaces avancées	Surveiller, détecter, analyser, bloquer et répondre aux menaces sophistiquées
Type de protection	Préventive	Préventive + détective + réactive	Préventive + détective + réactive
Couverture	PC + serveurs	*Selon la licence* : PC, serveurs, réseaux, Cloud, M365, applications, identités	*Tout compris, sans coût supplémentaire* : PC, serveurs, réseaux, Cloud, M365, applications, identités
Méthodes de détection	Règles prédéfinies	Règles prédéfinies, corrélation d'événements, indicateurs de compromission	Règles prédéfinies et règles personnalisées, corrélation d'événements, anomalies, indicateurs de compromission
Menaces détectées	Malwares connus et comportements suspects	Attaques avancées et complexes	Attaques complexes et interconnectées, internes ou externes, risques globaux du SI
Interopérabilité	Aucune	Moyenne	Totale
Supervision humaine	Aucune	Oui, équipe mutualisée	Oui, analystes spécialisés de niveau 1 à 3
Surveillance 24/7	Oui	Oui	Oui
Localisation des équipes	Aucune	Bureaux et call-centers dans plusieurs pays	Luxembourg
Temps de réaction	Dépend de l'utilisateur	Rapide	Immédiate
Réponse aux incidents	Actions automatiques très limitées	Blocage & recommandations	Blocage de l'attaque & isolation de la machine, notification au client, investigation et recommandations
Visibilité et reporting	Résumé basique	Rapports réguliers sur les incidents	Accès read-only au SIEM, rapports mensuels, rapports d'incidents
Facturation	Abonnement	Abonnement	Abonnement
Cas d'usage	Particuliers ou TPE qui veulent se protéger facilement	TPE et PME qui veulent une sécurité proactive avec un niveau de protection intermédiaire	TPE, PME et grandes entreprises qui souhaitent une sécurité de haut niveau, sur mesure, avec une équipe dédiée et locale

Rsecure SARL / www.rsecure.lu
38-40, Parc d'Activités L-8308 Capellen