

Antivirus nouvelle génération (EDR)

Une solution de protection de tous vos devices permettant de détecter et bloquer les cyberattaques en temps réel, opérée et supervisée par notre service SOC by Qyyp.



Une offre de sécurité managée et centrée sur la supervision SOC By Qyyp, s'appuyant sur une solution EDR WatchGuard pour une protection proactive, continue et contextualisée de l'ensemble des terminaux de votre SI.

Pourquoi mettre en place un EDR (Endpoint Detection and Response) ?

Les cyberattaques ciblant les entreprises sont aujourd'hui de plus en plus sophistiquées et difficiles à détecter : ransomwares, attaques sans fichier, compromission de postes utilisateurs ou vol de données.

Les antivirus traditionnels reposent sur des bases de signatures connues.

Ils sont efficaces contre les menaces identifiées, mais restent limités face aux attaques modernes.

L'EDR permet d'aller plus loin et devient une brique essentielle de la stratégie cyber Zero Trust.



Détecter

les comportements suspects sur les devices



Analyser

les activités anormales grâce à l'IA



Bloquer

les attaques connues et inconnues



Réagir

rapidement en cas de compromission

Une solution complète et clé en main !

- › Licence EDR Watchguard
- › Installation et déploiement des agents sur les postes
- › Paramétrage et configuration par des ingénieurs certifiés
- › Supervision et exploitation par nos experts
- › **Surveillance et réponse aux incidents via SOC by Qyyp**

Tous vos devices
(Postes de travail, serveurs, terminaux...)

Plusieurs systèmes d'exploitation
(Windows, macOS...)

NOC
by Qyyp

Notre centre de support assure la supervision opérationnelle de l'EDR :

- › Surveillance de l'état du service
- › Traitement des incidents de sécurité
- › Gestion des demandes de support
- › Coordination avec les équipes techniques
- › Suivi des tickets et communication

SOC
by Qyyp

Les événements remontés par les agents EDR sont centralisés dans notre SIEM :

- › Détection proactive des menaces
- › Analyse des comportements suspects
- › Qualification des incidents par matrice de criticité
- › Remédiation automatique lorsque possible
- › Alerte et préconisation en temps réel
- › Morning check cyber quotidien - météo hebdomadaire

4

Différences majeures

ANTIVIRUS	EDR	XDR*
Réactif	Proactif	Proactif
Détecte les menaces déjà connues dans la base de données	Détecte tous les types de menaces, connues ou non	Détecte tous les types de menaces et partout
Cherche des marqueurs connus pour identifier la menace	Cherche des comportements inhabituels	Cherche des comportements inhabituels sur toutes les couches
Utilise une base de données	Utilise l'IA	Utilise la corrélation et l'IA

*XDR - en option avec une licence Total Security sur le pare-feu

Une stratégie Zéro Trust

CLASSIFICATION NON FIGÉE PAR L'IA
Analyse des flux et classification en Malware et Goodware



THREAT HUNTING
Analyse des flux suspects (0,02% du flux) par nos experts

Prérequis techniques

Pour garantir le bon fonctionnement du Pack EDR, les éléments suivants doivent être disponibles :

- postes de travail, serveurs ou terminaux compatibles
- connexion Internet active pour la communication avec la console EDR
- accès administrateur pour le déploiement des agents
- environnement informatique maintenu à jour

Pour une sécurité complète, découvrez aussi :

