kaspersky

EDR vs MDR vs XDR

EDR
Endpoint Detection and Response

Identifie les menaces nouvelles, inconnues et furtives qui contournent la protection des terminaux et automatise les tâches de sécurité de routine

MDR
Managed Detection and Response

Fournit une protection managée en continu, même contre les menaces d'origine non malveillante les plus complexes et les plus innovantes

XDR
Extended Detection and Response

Détecte de manière proactive les menaces complexes dans plusieurs niveaux de l'infrastructure et y répond automatiquement pour les contrer

Comment ça fonctionne ?

- Active la détection avancée et la recherche des menaces qui contournent les mécanismes de prévention
- Améliore la visibilité et la visualisation des menaces
- Simplifie l'analyse des causes profondes
- Délivre une réponse automatisée et centralisée

- Regroupe les données de télémétrie des produits de sécurité, analyse de manière proactive les métadonnées de l'activité du système pour rechercher des signes d'une attaque active ou imminente, et fournit une réponse gérée ou guidée

- Intègre plusieurs outils et applications de sécurité
- Surveille les données sur les terminaux, les réseaux, les clouds, les serveurs Web, les serveurs de messagerie, etc. pour détecter et éliminer les menaces complexes
- Simplifie la gestion des informations de sécurité grâce à l'automatisation de l'interaction entre les produits

Pour qui est-ce le mieux adapté ?

- Entreprises disposant d'une équipe de sécurité informatique en interne ayant besoin d'une visibilité granulaire des points de terminaux et d'une réponse centralisée afin de réduire les tâches de traitement manuelles

- Sociétés cherchant à développer leur capacité de sécurité informatique interne en se déchargeant des tâches principales de détection et de réponse
- Organisations qui ne disposent peut-être pas du budget ou de l'équipe de spécialistes pour élaborer leur propre centre d'opérations de sécurité (SOC)

Organisation mature sur le plan de la sécurité souhaitant une plate-forme délivrant les éléments suivants :

- Une image cohérente de ce qui se passe d'un bout à l'autre de leur infrastructure
- Recherche des menaces et Threat Intelligence intégrées
- Hiérarchisation des incidents supérieure et moins d'alertes de faux positifs

Valeur commerciale

- Donne au personnel de sécurité la visibilité et le contrôle unifiés dont il a besoin pour rechercher les menaces de manière active, plutôt que d'attendre les alertes
- Exploite au maximum les capacités de l'équipe sécurité informatique en automatisant tout un éventail de processus d'analyses, d'examens et de réponses
- Assure une meilleure rentabilité en permettant aux équipes de sécurité informatique de travailler de manière plus efficace, sans avoir à jongler entre plusieurs outils et consoles

- Résout la crise des talents en matière de cybersécurité en garantissant une protection instantanée contre les menaces complexes
- Permet l'externalisation des processus de gestion des incidents, afin de mieux concentrer les ressources internes limitées et coûteuses sur les résultats critiques obtenus
- Réduit le coût global de la sécurité, sans avoir à déployer des solutions de sécurité complexes et à recourir à un large éventail de spécialistes dédiés en interne

- Fournit une protection globale contre le paysage des menaces en évolution
- L'approche par écosystème optimise l'efficacité des outils de cybersécurité mis en œuvre, économise des ressources et réduit le risque
- Simplifie le travail des spécialistes de la sécurité informatique et leur procure le contexte supplémentaire nécessaire pour enquêter sur les attaques perpétrées avec plusieurs vecteurs
- Minimise les temps moyens de détection et de réponse (MTTD et MTTR), ce qui est essentiel pour combattre les menaces complexes et les attaques ciblées
- Permet une réponse centralisée et automatisée sur la totalité de la pile de technologies de sécurité

Si votre organisation est mature en ce qui concerne la sécurité et cherche à bénéficier des capacités XDR, jetez un œil à

Kaspersky Expert Security

En savoir plus