Fiche produit

ThreatDown EDR managé (Managed Detection & Response, ou MDR)

Protégez votre organisation grâce à une surveillance des menaces, des enquêtes et des mesures correctives gérées par nos analystes MDR experts.

VUE D'ENSEMBLE

Pour les équipes de sécurité des petites et moyennes entreprises, la fourniture de **services de cybersécurité de haute qualité** et le maintien des environnements **professionnels à l'abri des menaces** nécessitent une équipe qualifiée capable **d'analyser et d'interpréter les signaux recueillis par l'EDR** pour trier et prioriser les alertes les plus sérieuses. Or, de nombreuses organisations sont confrontées à **des ressources humaines limitées** et manquent de compétences approfondies en matière de cybersécurité. En outre, elles sont constamment surchargées de responsabilités en matière de triage des alertes. À cela s'ajoutent **la montée en flèche des coûts** et la complexité de la gestion de solutions multiples pour découvrir les menaces cachées, ce qui conduit à **l'inefficacité et à de longs délais de réponse aux incidents.**

Les équipes de sécurité, soumises à des contraintes, ont besoin **d'un moyen simple, efficace et rentable de détecter les cyber-menaces et d'y répondre.**

IPgarde relève ces défis **grâce à une offre de détection et de réponse gérée** (MDR) spécialement conçue à cet effet : ThreatDown, développé par Malwarebytes. Notre solution de MDR propose **une offre puissante et abordable** de détection des menaces et de remédiation **avec un suivi par nos analystes de sécurité de haut niveau.** Votre entreprise gagnera en cyber-résilience grâce à des services d'experts qui **accélèrent la détection des menaces** et **répondent aux incidents** avec précision. ThreatDown MDR offre des options de réponse aux menaces flexibles qui répondent aux besoins de votre entreprise et de votre environnement de sécurité, vous garantissant ainsi **une visibilité et un contrôle complets sur les éléments de votre SI.**

AVANTAGES DE THREATDOWN MDR

- **Surveillance 24 heures sur 24, 7 jours sur 7 et 365 jours par an** : Nous surveillons les points finaux et effectuons des enquêtes spécialisées jour et nuit, en semaine, le week-end et les jours fériés.
- **Des analystes MDR compétents** : Notre équipe d'experts en sécurité est composée de chasseurs de menaces accomplis, dotés **d'une solide expérience en matière de réponse aux incidents** et de dizaines d'années d'expérience dans le triage et l'atténuation des menaces complexes liées aux logiciels malveillants.

DÉFIS

- **Ressources limitées pour répondre aux besoins en matière de sécurité :** 67 % des personnes interrogées font état d'une pénurie de personnel dans le domaine de la cybersécurité[1] .
- **Le trop grand nombre d'alertes entraîne une lassitude** : 80 % des alertes EDR sont ignorées par les services informatique car n'arrivent pas à prioriser les plus sérieuses des alertes bénignes. [2]
- **La lenteur de la réaction permet aux attaquants de disposer de plus de temps sur vos points d'accès :** 277 jours - nombre moyen de jours pour identifier et contenir une violation.

AVANTAGES

Protégez les postes de travail, les serveurs et bien plus encore avec ThreatDown MDR.

- **Une meilleure sécurité :** Atténuer les risques de manière proactive avant qu'une violation ne se produise.
- **Moins d'efforts** : Économisez les ressources de votre équipe en vous appuyant sur les analystes de sécurité experts de ThreatDown pour surveiller les activités suspectes sur vos réseaux.
- **Meilleurs résultats** : Obtenez des temps de réponse et de remédiation plus rapides, à un coût nettement inférieur à celui de l'internalisation d'un service cyber-sécurité.

1 Rapport Malwarebytes sur l'état des logiciels malveillants.
2 Anomali's Cybersecurity Insights Report

- **EDR primé et reconnu** : Alimenté par la plateforme ThreatDown Endpoint Detection and Response (EDR) et enrichi par de multiples sources de renseignements sur les menaces, dont MITRE et d'autres.

- **Options de remédiation flexibles** : Notre équipe MDR peut fournir un soutien actif à la remédiation aux menaces au fur et à mesure qu'elles sont découvertes ou fournir des conseils très utiles aux équipes informatiques dans le cadre de leurs propres efforts de remédiation.

- **Chasse active aux menaces** : Notre équipe MDR traque les menaces invisibles en se basant sur les indicateurs de compromission (IOC) antérieurs et les activités suspectes observées sur les terminaux.

- **Roll back de 72 heures** (restauration jusqu'à 72 h en arrière) en cas de ransomware pour vos machines Windows

- Déploiement rapide : ThreatDown EDR est réputé pour sa facilité d'installation, ce qui permet à votre équipe de **sécurité d'intégrer rapidement de nouveaux points d'extrémité à notre service MDR** 24x7 en quelques minutes.

COMMENT CELA FONCTIONNE-T-IL ?

Une fois les agents déployés, le service MDR est activé en quelques minutes et les analystes d'IPgarde peuvent **surveiller l'environnement du client.** Les données de détection sont intégrées dans la plateforme MDR Security Orchestration, Automation, and Response (SOAR), où elles sont **enrichies par des flux de renseignements internes et externes** sur les menaces. Ce processus **accélère** l'identification, l'analyse et le triage (**hiérarchisation** des réponses et enquêtes) des événements de sécurité. À ce stade, la plateforme MDR SOAR vérifie que les alertes d'activité suspecte **sont des menaces réelles ou des détections bénignes** et peut augmenter le niveau de gravité de certaines détections EDR sur la base de renseignements sur les menaces. Les cas qui nécessitent une remédiation sont soit complétés par l'analyste, soit guidés par le client ou le MSP s'ils ont choisi d'effectuer leurs propres actions de remédiation.

IPgarde
01 77 49 24 50
contact@ipgarde.com
www.ipgarde.com