Services managés : EDR (Endpoint Detection and Response)

Faites mieux que les solutions traditionnelles. Libérez toute la puissance d'un service doté de fonctionnalités intégrées, pour une résilience inégalée.

Défis

Dans la mesure où plus de 60 % des compromissions ont recours à des techniques de piratage, les entreprises doivent se doter de contrôles de sécurité avancés pour lutter contre les cybermenaces sophistiquées actuelles.

Les cybercriminels sont motivés par l'appât du gain et l'accès à des données sensibles. Les secteurs hautement sensibles, comme la santé, les services financiers et les services publics, constituent donc des cibles de choix.

En revanche, compte tenu de la complexité et du coût des technologies EDR dont le retour sur investissement est long, même pour les grands centres SOC, la plupart des services avancés de sécurité des terminaux dont les PME et entreprises du marché intermédiaire peuvent se doter pour contrer ces menaces génèrent des problèmes majeurs :

- Coûts élevés, au-delà des budgets informatiques
- Analyse et réponse aux incidents de plusieurs heures, voire de plusieurs jours
- Neutralisation des menaces modernes impossible pour les solutions traditionnelles
- Correction limitée n'assurant pas la continuité des activités ni la protection des données
- Risque de retards du reporting de conformité ou absence de reprise d'activité après sinistre

Principaux avantages

Accès à une expertise en matière d'informatique et de sécurité

- Réduction des besoins en matière d'embauche et de formation
- Optimisation de vos fonctionnalités et alignement sur les dernières tendances

Rentabilité

- Coûts plus prévisibles basés sur les SLA
- Transformation des dépenses d'investissement (CAPEX) en dépenses d'exploitation (OPEX)

Assistance et support continus

- Surveillance continue de vos données et systèmes métier

Évolutivité rapide

- Adaptation des services à vos besoins et à votre budget

Solution : services EDR (Endpoint Detection and Response) managés

Que vous collaboriez avec un fournisseur pour les projets de sécurité très spécialisés ou que vous externalisiez l'ensemble de vos opérations informatiques, nous proposons des services EDR très efficaces et rentables.

Nous avons à cœur d'assurer la continuité d'exécution, la sécurité, la productivité et la fiabilité de votre entreprise tout en respectant votre budget informatique.

Pourquoi ?

Optimisation de l'analyse et de la priorisation des incidents	Sécurité, sauvegarde et restauration intégrées	Solution de cyberprotection complète
• Optimisez les investigations grâce à la priorisation des incidents potentiels et à la réduction de la désensibilisation aux alertes. • Réduisez le délai d'investigation de plusieurs heures à quelques minutes à grande échelle, avec une corrélation automatisée et des interprétations des attaques guidées par l'intelligence artificielle. • Une mise en correspondance plus claire avec le cadre MITRE ATT&CK® permet de comprendre facilement l'analyse et l'impact des attaques, y compris la méthode utilisée par le cybercriminel pour s'introduire dans l'environnement et propager l'attaque, de même que l'ampleur des dommages causés. • Signalez rapidement les incidents de sécurité.	• Des fonctionnalités de sauvegarde et de restauration intégrées assurent une véritable résilience que ne peuvent offrir les solutions de sécurité isolées — rétablissement spécifique aux attaques, restauration de fichiers ou d'images complètes, reprise d'activité après sinistre, etc. • Les fonctionnalités de correction et de restauration rapides en un clic vous permettent d'enquêter, d'appliquer des mesures correctives, de restaurer vos données et d'éliminer les failles de sécurité. • Profitez d'une protection complète intégrée conforme au cadre de sécurité NIST.	• Lancez rapidement et facilement de nouveaux services de cyberprotection à partir d'un unique agent et d'une seule console, ce qui accélère le déploiement et l'intégration des services. • Simplifiez la montée en charge des services pour plusieurs clients tout en conservant des marges confortables et en minimisant les dépenses d'exploitation (OPEX), en rendant superflu le recours à une grande équipe d'experts chevronnés.

Principales fonctionnalités

Détection des menaces avancées et des attaques en cours

Le service surveille et met en corrélation les événements suspects observés sur vos terminaux pour détecter et neutraliser les menaces complexes et furtives capables de contourner les autres défenses des terminaux, telles que les ransomwares, les menaces zero-day, les menaces persistantes avancées (APT) ou les attaques sans fichier.

Renforcement de la conformité réglementaire

Protégez les données sensibles soumises à des réglementations — comme le RGPD, la loi HIPAA et la norme PCI DSS — contre les menaces et gagnez en visibilité sur les données sensibles touchées par des incidents à des fins de reporting de conformité.

Réponse globale aux menaces afin d'assurer la continuité des activités

Nous assurons la continuité de vos activités et la restauration rapide de vos données, ainsi que l'annulation des modifications apportées au système en cas d'attaque. Contrairement aux autres services avancés de sécurité des terminaux exclusivement dédiés à la cybersécurité, nos services managés de sécurité des terminaux fournissent des fonctionnalités intégrées conformes au cadre de cybersécurité NIST pour assurer une véritable continuité des activités.

Optimisé par une technologie primée de protection des terminaux

Prix de la rédaction

Gagnant des tests AV-TEST

Certification de protection antimalware pour terminaux octroyée par ICSA Labs

Certification AV-Comparatives

Certification VB100

Administrer

Établissez rapidement des stratégies de cybersécurité et de gestion des risques, définissez des rôles et des stratégies, et assurez une surveillance continue via une plate-forme intégrée.

Identifier

Vous devez identifier les incidents nécessitant une investigation approfondie pour mieux vous en protéger. Notre service intègre des outils d'inventaire et de classification des données qui permettent de mieux déterminer vos surfaces d'attaque.

Protéger

Offrez une protection proactive à vos terminaux grâce à des flux d'informations sur les menaces très détaillés, à la correction des vulnérabilités existantes, au blocage des menaces connues et à la gestion des règles pour une sécurité renforcée.

Détecter

Bénéficiez d'une surveillance continue des menaces grâce à nos moteurs basés sur les comportements et les signatures, au filtrage des URL et à la mise en corrélation des événements.

Répondre

Réduisez le délai d'investigation des incidents au moyen d'une connexion à distance et de données d'investigation numérique. Procédez à une correction ultrarapide via l'isolement des terminaux, la neutralisation des processus, la mise en quarantaine et des rétablissements spécifiques aux attaques.

Restaurer

Vérifiez le bon fonctionnement des systèmes, des données et de votre activité grâce à nos solutions de sauvegarde et de restauration de pointe, entièrement intégrées pour une continuité des activités inégalée.

Pour plus d'informations, contactez-nous : Hermitage Solutions

frederic.cluzeau@hermitagesolutions.com - +33478287541
https://www.hermitagesolutions.com