PRÉSENTATION DE LA SOLUTION

Services managés EDR et XDR d'Insight

Les défis pour les entreprises

Dans le paysage digital en constante évolution d'aujourd'hui, les entreprises sont confrontées à une série de défis complexes en matière de cybersécurité. Le flot constant de cybermenaces représente un risque considérable pour les actifs de valeur et les données sensibles. Alors que les cybercriminels deviennent de plus en plus menaçants et créatifs, il devient de plus en plus difficile pour les organisations de détecter et de réagir efficacement à ces menaces.

Les entreprises ont du mal à renforcer les réglementations en matière de conformité, à compliquer les environnements informatiques et à faire face à la pénurie de cybercriminels qualifiés. Ces défis combinés créent le besoin de fournir des solutions de cybersécurité complètes et proactives pour protéger les entreprises des diverses menaces sophistiquées auxquelles elles sont confrontées au quotidien.

La préparation et la résilience en matière de cybersécurité sont essentielles pour protéger la pérennité et le succès de toute entreprise moderne.

En quoi Insight peut vous accompagner

Notre Centre des opérations de sécurité (SOC) fournit deux offres de services managés, offrant des capacités avancées de détection, d'investigation et de réponse aux menaces:

- **Détection et réponse des terminaux managés (MEDR)**
  Covering laptops, desktops and mobile devices.
- **Détection et réponse étendues managées (MXDR)**
  Réunissant des journaux et des flux provenant d'un large éventail de sources, il offre la capacité de détection la plus robuste pour votre environnement.

Combinant des technologies telles que l'IA, l'intelligence des menaces et l'analyse, notre équipe d'analystes experts en sécurité est capable de détecter et de réagir aux menaces pesant sur votre environnement en temps réel.

Nous mettons notre expertise à votre disposition concernant:

- Surveillance complète et détection et réponse aux menaces en temps réel.
- Réponse plus rapide aux incidents et temps d'arrêt réduits.
- Visibilité accrue sur l'activité des terminaux et les risques potentiels.
- La disponibilité du service
- Peut faciliter la conformité avec certaines exigences réglementaires et normes du secteur.
- Peut être combiné avec d'autres services Insight dans le cadre d'un service de sécurité de bout en bout.to-end security service.

PRÉSENTATION DE LA SOLUTION

Service managé de détection et de réponse des terminaux

AUn service managé conçu comme une capacité abordable et accessible de détection et de réponse pour les organismes ne disposant pas ou dont la structure de sécurité est limitée. Notre service est conçu autour de la technologie de pointe intégrée dans la solution de sécurité Microsoft et utilise Microsoft Defender for Endpoint comme cœur de ses capacités de détection.

Les éléments clés de notre service EDR managé incluent:

- **Monitoring des terminaux:** L'utilisation d'outils et de techniques de pointe pour surveiller les terminaux 24/7 afin de détecter tout signe d'activité suspecte, y compris les attaques sans fichier, les logiciels malveillants avancés, les rançongiciels et les menaces internes.
- **Détection des menaces:** Nous utilisons une combinaison d'intelligence sur les menaces, d'analyse comportementale et d'algorithmes d'apprentissage machine pour détecter les menaces avancées qui peuvent échapper aux contrôles de sécurité traditionnels.
- **Investigation et réponse:** Nos analystes de sécurité analysent et hiérarchisent les alertes et fournissent des rapports d'incidents détaillés à votre équipe. Nous travaillons également avec vous pour développer et mettre en œuvre un plan d'intervention afin d'atténuer l'impact de tout incident.
- **Protection des terminaux:** Notre solution EDR comprend des fonctionnalités avancées de protection des terminaux, notamment un antivirus, un antimalware et un système HIPS (Host-Based Intrusion Prevention System) pour aider à prévenir et à bloquer les attaques avant qu'elles ne puissent causer des dégâts.
- **Recherche de menaces:** Des fonctionnalités proactives de traque, où nos analystes recherchent et analysent les menaces potentielles qui peuvent être passées inaperçues par les systèmes automatiques.

Services managés étendus de détection et de réponse

Une capacité de détection plus robuste qui réunit tous vos journaux de sécurité et les transmet à une plateforme SIEM centrale basée sur la technologie Microsoft Sentinel.

Les éléments clés de notre service XDR managé incluent:

- **Surveillance:** Utilisation d'outils et de techniques de pointe pour surveiller 24/7 les signes d'activité suspecte, y compris les attaques sans fichier, les logiciels malveillants avancés et les menaces internes.
- **Collecte et analyse des logs:** Collecte et analyse centralisées des données des journaux à partir de diverses sources, y compris les terminaux, les appareils réseau, les applications et les services cloud.
- **Détection des menaces:** Nous utilisons une combinaison d'intelligence sur les menaces, d'analyse comportementale et d'algorithmes d'apprentissage machine pour détecter les menaces avancées qui peuvent échapper aux contrôles de sécurité traditionnels.
- **Investigation et réponse:** Nos analystes de sécurité analysent et hiérarchisent les alertes et fournissent des rapports d'incidents détaillés à votre équipe. Nous travaillons également avec vous pour développer et mettre en œuvre un plan d'intervention afin d'atténuer l'impact de tout incident.
- **Protection des terminaux:** Notre solution EDR comprend des fonctionnalités avancées de protection des terminaux, notamment un antivirus, un antimalware et un système HIPS (Host-Based Intrusion Prevention System) pour aider à prévenir et à bloquer les attaques avant qu'elles ne puissent causer des dégâts.
- **Recherche de menaces:** Des fonctionnalités proactives de traque, où nos analystes recherchent et analysent les menaces potentielles qui peuvent être passées inaperçues par les systèmes automatiques.

Résultats de nos services EDR/XDR managés Nous mettons notre expertise à votre disposition:

Détection et réponse proactives aux menaces

Aider à prévenir les violations de la sécurité et à minimiser les impacts des attaques potentielles

Surveillance et assistance

Protection continue et réponse rapide aux incidents

Rapport qualité-prix

Une alternative rentable à la constitution et à la maintenance d'une équipe interne

Conformité réglementaire

Aide à la conformité aux normes de sécurité et aux exigences de reporting