Gestion de la détection et de la réponse étendues

Limiter l'impact des cybermenaces en ajoutant des opérations de sécurité 24 heures sur 24 et 7 jours sur 7

Le défi

La cybermenace gagne en ampleur et en complexité chaque année, et de nombreuses entreprises estiment qu'il est trop difficile de se protéger contre l'attaque inévitable et ses conséquences. Pourquoi est-ce si difficile? Nous pensons que quatre facteurs entrent en ligne de compte:

1 Manque de visibilité

Les menaces potentielles peuvent passer inaperçues, ce qui permet à une attaque de faire surface.

2 Ressources limitées

Les services informatiques internes manquent de ressources ou d'expertise spécifique pour gérer leur propre cybersécurité.

3 La complexité

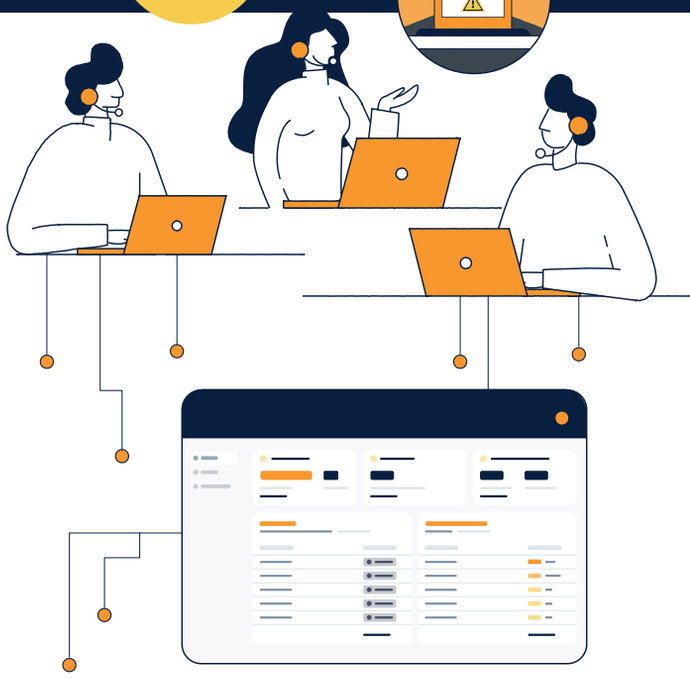
Les solutions de cybersécurité peuvent être complexes à mettre en œuvre et à maintenir, car elles nécessitent des connaissances et des ressources spécialisées.

4 Évolution rapide du paysage des menaces

Les entreprises ne peuvent pas suivre l'évolution constante des menaces.

La solution

Nous vous protégeons de l'intérieur vers l'extérieur et de l'extérieur vers l'intérieur, en fournissant une solution de Détection et Réponses Étendues Gérées 24/7, en utilisant nos connaissances et notre expertise pour identifier rapidement et contenir vos menaces cybernétiques. Mais il y a tellement plus:



Caractéristiques

- Détection et réponse étendues (Open XDR)
- Centre d'opérations de sécurité (SOC) 24 heures sur 24 et 7 jours sur 7
- Gestion de la surface d'attaque (ASM)
- Recherche de Menaces
- Réponse aux incidents
- Rapports de Gestion
- CISO en tant que Service (incl. Pentest Annuel et Conseils en Sécurité)

Fonctionnalités

Managed XDR

À la pointe de la technologie et conçus pour surveiller l'activité des terminaux et du cloud en temps réel, nous aidons à détecter, enquêter et réagir aux menaces de sécurité sur les terminaux tels que les ordinateurs, les ordinateurs portables, les serveurs et les environnements cloud, tels que Microsoft 365.

Le Portail Eye

Vous voulez des recommandations faciles à comprendre ? Heureusement, nous avons le portail Eye pour vous guider avec une interface descriptive et intuitive vous permettant d'agir rapidement, couvrant des domaines tels que la couverture des endpoints et la double authentification ainsi que des suggestions sur la manière d'améliorer la résilience cybernétique.

Centre des Opérations de Sécurité 24/7 (SOC)

Notre SOC est le centre névralgique où notre équipe de sécurité 24/7, composée d'experts chevronnés, surveille, répond à et atténue les menaces et incidents de sécurité. Considérez-nous comme la continuité de votre équipe.

Gestion de la surface d'attaque (ASM)

En utilisant l'expertise humaine et une configuration de sécurité de pointe, nous visons à rendre votre sécurité cybernétique aussi étanche que possible. Nous scannons continuellement votre surface d'attaque et intervenons lorsqu'une vulnérabilité critique est identifiée, vous mettant ainsi en position proactive.

Recherche de Menaces

Nos analystes en intelligence des menaces évaluent de nombreuses sources différentes, créent des recherches sur mesure, pour d'abord interpréter la vulnérabilité de votre système, puis fournir des conseils pour limiter la menace (y compris les menaces zero-day).

Réponse aux Incidents (IR)

Même en dehors des heures de bureau et lorsque vous êtes le plus vulnérable, vous avez des experts de niveau mondial qui veillent sur vous et assurent la continuité de votre activité. Managed XDR comprend 4 heures de support direct aux incidents par l'équipe IR de Eye Security, disponible 24/7 par téléphone, e-mail et sur site.

Outil Anti-Spoofing d'Eye (EAST)

EAST est notre solution de cybersécurité avancée pour lutter contre l'usurpation de page de connexion Microsoft. Il fonctionne lors de la connexion en utilisant un fichier CSS personnalisé pour distinguer les pages légitimes des pages malveillantes, ajoutant un indice visuel à l'utilisateur qui agit comme une alerte.

CISO en tant que Service

Nous soutenons les organisations avec des revues clients annuelles, des évaluations de risques cybernétiques/audits de pénétration approfondis et fournissons une assistance pour toutes les questions de sécurité et des conseils concernant les anomalies. Nos spécialistes sont là pour aider votre organisation à relever les défis liés à la gouvernance et à la conformité.

Commencez avec Managed XDR en 24 heures:

1.

Admission et Évaluation L'intégration est simplifiée grâce à une plateforme en ligne. Nous pouvons ensuite évaluer votre posture en matière de sécurité cybernétique et coordonner le plan de réponse aux incidents lors d'une réunion d'admission avec les parties prenantes internes et externes.

2.

Déploiement Notre service Managed XDR est déployé et vous êtes sous surveillance en quelques heures, avec une stratégie de déploiement prouvée et non intrusive.

3.

C'est tout ! Nos agents sont actifs. Nous vérifierons pendant l'intégration que tout se passe bien, et 2 mois après, nous tiendrons une revue de cybersécurité, où nous travaillerons à réduire encore davantage votre surface d'attaque.

Avantages de Managed XDR

Agnostique
Nous nous intégrons avec les meilleurs fournisseurs de sécurité des endpoints:

Microsoft Defender · SentinelOne · CROWDSTRIKE

Alignement sur les partenaires
Nous nous alignons avec les partenaires de services informatiques (MSP) pour garantir un déploiement adéquat.

Surveillance
Nous surveillons tous les systèmes, tels que Windows, Linux et Mac, ainsi que les environnements cloud (Microsoft et Google).

Réponse gérée active
Notre équipe de réponse aux incidents interne répond aux menaces actives et fournit un support complet jusqu'à la fermeture de l'incident.

Support
Nous vous aidons de manière proactive et sommes là pour répondre aux attaques 24/7.

Conseils d'experts
Nous proposons une réunion annuelle, analysant davantage les sources de données internes et externes pour améliorer la résilience cybernétique.

Pourquoi les entreprises choisissent Eye Security

1. Cybersécurité de pointe et abordable pour toutes les tailles d'entreprise.
2. Des experts chevronnés réagissant rapidement aux menaces numériques.
3. Équipes informatiques allégées, tirant parti de notre accès aux systèmes et aux données.
4. Possession complète des incidents et rapports transparents.
5. Des informations faciles à comprendre pour une sécurité améliorée.
6. Protection garantie par une assurance pour une couverture complète des attaques.

Suivez ces six étapes pour mieux gérer votre risque cybernétique

Le risque cybernétique est perçu comme l'une des plus grandes menaces pour les entreprises. Pour minimiser le risque de cyber-attaque, il est important de rendre votre entreprise plus résiliente. Voici six étapes pour commencer:

Authentification Multifacteur (MFA)

L'authentification multifacteur est indispensable pour toute personne accédant à votre réseau sur n'importe quel appareil.

Mises à Jour Régulières et Correctifs

Les correctifs de sécurité critiques protègent votre entreprise des attaques en corrigeant les vulnérabilités connues dans votre logiciel.

Sauvegardes et Récupération Sécurisées

Les solutions de sauvegarde sont essentielles pour votre entreprise. En cas d'attaque, votre entreprise pourra utiliser sa sauvegarde système au lieu de payer une rançon coûteuse.

Plan de Réponse aux Incidents Testé

Bien que l'objectif soit de ne jamais subir d'attaques cybernétiques, il est important de se préparer à un incident afin de réduire son impact.

Formation à la Sensibilisation des Employés

Une formation régulière à la sensibilisation des employés peut aider à éduquer les membres de l'équipe pour reconnaître les escroqueries telles que le phishing par e-mail, et agir de manière appropriée.

Durcissement de la Configuration de Sécurité des Systèmes et du Cloud

Vos postes de travail, serveurs et cloud doivent avoir des meilleures pratiques de sécurité et de configuration activées.

Plus d'informations?

Eye Security offre un package total abordable pour rendre votre risque cybernétique immédiatement gérable. Si vous souhaitez explorer votre résilience cybernétique dès aujourd'hui, veuillez scanner ici:

Eye Security est une entreprise de cybersécurité basée sur un abonnement qui propose une cybersécurité et une assurance réalisables pour les entreprises européennes. Avec une équipe croissante d'experts en sécurité et en assurance, Eye Security offre un service de sécurité tout-en-un de haute qualité et abordable en combinant Détection et Réponse Étendues Gérées (MDR) et assurance cyberné-tique. Fondée en 2020, Eye Security opère en Europe avec des bureaux aux Pays-Bas, en Belgique, en Allemagne et grâce à ses partenaires.

Rendez-vous sur eye security