Managed Extended Detection und Response

Begrenzen Sie die Auswirkungen von Cyber-Bedrohungen durch zusätzliche 24/7-Sicherheitsmaßnahmen

Die Herausforderung

Das Ausmaß und die Komplexität von Cyber-Bedrohungen nehmen jedes Jahr zu, und viele Unternehmen finden es zu schwierig, sich gegen die unvermeidlichen Angriffe und deren Folgen zu schützen. Warum ist das so schwer? Wir sehen hier vier wesentliche Faktoren:

1 Mangelnde Sichtbarkeit

Potenzielle Bedrohungen können unentdeckt bleiben, so dass ein Angriff möglich wird.

2 Begrenzte Ressourcen

Den internen IT-Abteilungen fehlt es an Ressourcen oder spezifischem Fachwissen, um ihre eigene Cybersicherheit zu verwalten.

3 Komplexität

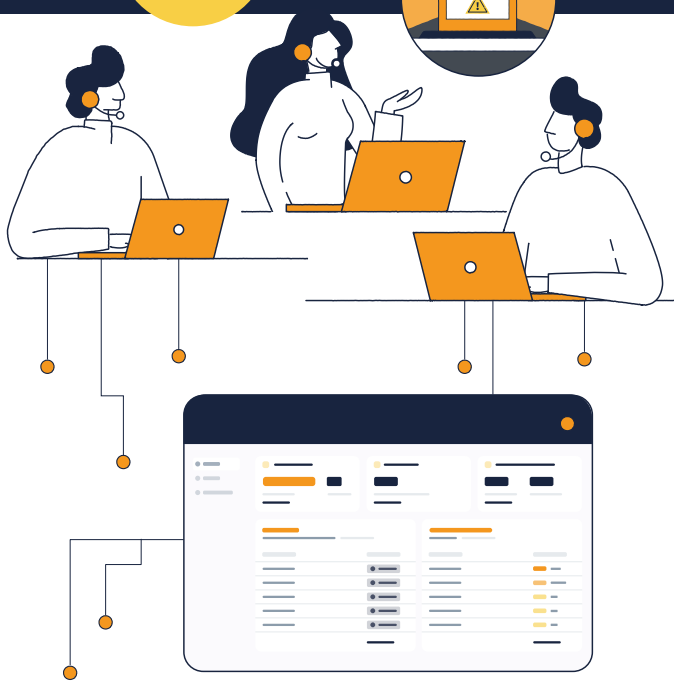
Die Implementierung und Wartung von Cybersicherheitslösungen kann komplex sein und erfordert spezielle Kenntnisse und Ressourcen.

4 Sich schnell verändernde Bedrohungslandschaft

Unternehmen können mit der sich ständig weiterentwickelnden Bedrohungslandschaft nicht Schritt halten.

Die Lösung

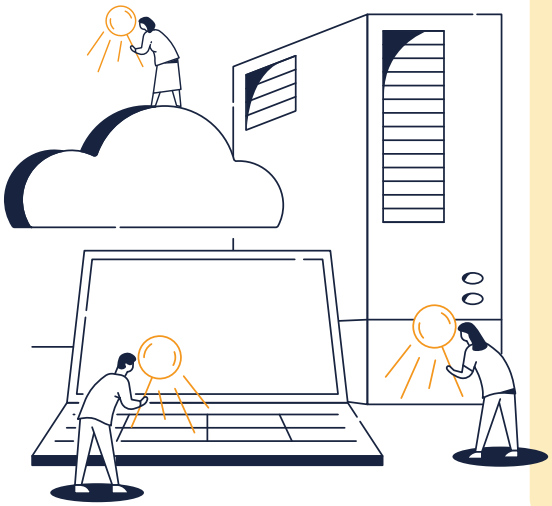
Wir schützen Sie umfassend, indem wir eine rund um die Uhr verfügbare Managed XDR-Lösung bereitstellen und unser Wissen und unsere Erfahrung nutzen, um Ihre Cyber-Bedrohungen schnell zu erkennen und einzudämmen. Und das ist noch nicht alles:



Funktionen

- Erweiterte Erkennung und Reaktion (Managed XDR)
- 24/7 Security Operations Center (SOC)
- Attack Surface Management (ASM)
- Bedrohungssuche
- Reaktion auf Vorfälle
- Berichterstattung
- CISO-as-a-Service (inkl. jährlichem Pentest und Sicherheitsberatung)

Funktionen



Managed XDR

Wir sind auf dem neuesten Stand der Technik und wurden entwickelt, um Endpunkt- und Cloud-Aktivitäten in Echtzeit zu überwachen. Wir helfen bei der Erkennung, Untersuchung und Reaktion auf Sicherheitsbedrohungen auf Endpunktgeräten wie Computern, Laptops, Servern und Cloud-Umgebungen wie Microsoft 365.

24/7 Security Operations Center (SOC)

Unser SOC ist das Zentrum, in dem unser Sicherheitsteam, das sich aus erfahrenen Experten zusammensetzt, rund um die Uhr Sicherheitsbedrohungen und -vorfälle überwacht, auf sie reagiert und sie entschärft. Betrachten Sie uns als einen erweiterten Teil Ihres Teams.

Attack Surface Management (ASM)

Mit menschlichem Fachwissen und einem hochmodernen Sicherheitssystem sorgen wir dafür, dass Ihre Cybersicherheit so undurchlässig wie nur möglich ist. Wir scannen kontinuierlich Ihre Angriffsfläche und melden uns, wenn eine kritische Schwachstelle entdeckt wird, damit Sie immer auf dem neuesten Stand sind.

Bedrohungssuche

Unsere Threat-Intelligence-Analysten überwachen Ihre Systeme ständig auf kritische Schwachstellen und bieten Ihnen umfassende Kenntnisse, Einblicke und Empfehlungen, bevor Hacker sie ausnutzen können.

Reaktion auf Vorfälle (IR)

Auch außerhalb der Geschäftszeiten und wenn Sie am verwundbarsten sind, haben Sie erstklassige Experten, die Ihnen den Rücken freihalten und die Geschäftskontinuität sicherstellen. Managed XDR umfasst 4 Stunden direkten Vorfallsupport durch das IR-Team von Eye Security, das rund um die Uhr per Telefon, E-Mail und vor Ort erreichbar ist.

Eye Anti-Spoofing Tool (EAST)

EAST ist unsere moderne Cybersicherheitslösung zur Bekämpfung des Spoofing (= Fälschens) von Microsoft-Anmeldeseiten. Es nutzt beim Anmeldevorgang eine benutzerdefinierte CSS-Datei, um zwischen legitimen und bösartigen Seiten zu unterscheiden, und gibt dem Benutzer einen visuellen Hinweis als Warnung vor gefälschten Seiten.

CISO-as-a-service

Wir unterstützen Organisationen mit jährlichen Kundenüberprüfungen, umfassenden Cyber-Risikobewertungen und bieten einen Helpdesk für alle sicherheitsrelevanten Fragen und Beratung bei Anomalien. Unsere Spezialisten helfen Ihrem Unternehmen auch bei Fragen im Zusammenhang mit Governance und Compliance.

Das Eye-Portal

Sie wünschen sich einfache, verständliche Empfehlungen – dafür haben wir das Eye-Portal, das Sie mit einer anschaulichen, intuitiven Benutzeroberfläche leitet, damit Sie sofort das Notwendige tun können. Es deckt Bereiche wie Endpunkt- und 2FA-Abdeckung sowie Vorschläge zur Verbesserung der Cyber-Resilienz ab.

Starten Sie mit Managed XDR innerhalb von 24 Stunden:

1.

Aufnahme und Bewertung Das Onboarding wird durch eine App vereinfacht. Anschließend können wir Ihre Cybersicherheitslage bewerten und den Plan für die Reaktion auf einen Vorfall während einer Aufnahmebesprechung mit internen und externen Beteiligten koordinieren.

2.

Bereitstellung Unser Managed XDR-Service wird innerhalb weniger Stunden bereitgestellt und überwacht, und zwar mit einer bewährten, nicht-intrusiven Bereitstellungsstrategie.

3.

Das war's! Unsere Agenten sind aktiv. Während des Onboardings schauen wir nach, ob alles reibungslos läuft, und 2 Monate später führen wir eine Überprüfung der Cybersicherheit durch, bei der wir Ihre Angriffsfläche weiter reduzieren können.

Vorteile von Managed XDR

Agnostisch
Wir arbeiten mit den besten Anbietern von Endpunktsicherheitslösungen zusammen:

Microsoft Defender · SentinelOne · CROWDSTRIKE

Partner-Ausrichtung
Wir arbeiten mit IT-Servicepartnern (MSPs) zusammen, um sicherzustellen, dass die Bereitstellung ordnungsgemäß erfolgt.

Überwachung
Wir überwachen alle Systeme, wie Windows, Linux und Mac sowie Cloud-Umgebungen (Microsoft und Google).

Aktive Managed Response
Unser internes Incident-Response-Team reagiert auf aktive Bedrohungen und bietet umfassenden Support, bis der Vorfall abgeschlossen ist.

Unterstützung
Wir unterstützen Sie proaktiv und sind rund um die Uhr für Sie da, um auf Angriffe zu reagieren.

Fachkundige Beratung
Wir bieten ein jährliches Treffen an, bei dem wir interne und externe Datenquellen weiter analysieren, um die Cyber-Resilienz zu verbessern.

Warum sich Unternehmen für Eye Security entscheiden

1. Erschwingliche Cybersicherheit auf dem neuesten Stand der Technik für alle Unternehmensgrößen.
2. Erfahrene Experten, die schnell auf digitale Bedrohungen reagieren.
3. Unsere Systeme und Daten entlasten IT-Teams signifikant.
4. Vollständige Übernahme der Zuständigkeit bei Vorfällen und transparente Berichterstattung.
5. Leicht verständliche Erkenntnisse zur Verbesserung der Sicherheit.
6. Versicherungsschutz für eine umfassende Abdeckung von Angriffen.

Mit diesen sechs Schritten managen Sie Ihr Cyber-Risiko besser

Cyberrisiken werden als eine der größten Bedrohungen für Unternehmen angesehen. Um das Risiko eines Cyberangriffs zu minimieren, ist es wichtig, Ihr Unternehmen widerstandsfähiger zu machen. Hier sind sechs Schritte, mit denen Sie einfach beginnen können:

Multi-Faktor-Authentifizierung (MFA)

Die Multi-Faktor-Authentifizierung ist ein Muss für jeden, der mit einem beliebigen Gerät auf Ihr Netzwerk zugreift.

Regelmäßige Updates und Patches

Kritische Sicherheits-Patches schützen Ihr Unternehmen vor Angriffen, indem sie bekannte Schwachstellen in Ihrer Software beheben.

Gesicherte Backups und Wiederherstellung

Backup-Lösungen sind für Ihr Unternehmen von entscheidender Bedeutung. Im Falle eines Angriffs kann Ihr Unternehmen sein System-Backup nutzen, anstatt ein teures Lösegeld zu zahlen.

Geprüfter Plan zur Reaktion auf Vorfälle

Auch wenn das Ziel darin besteht, nie von Cyberangriffen betroffen zu sein, ist es wichtig, sich auf einen Vorfall vorzubereiten, um die Auswirkungen zu verringern.

Sensibilisierung der Mitarbeiter

Regelmäßige Schulungen zur Sensibilisierung der Mitarbeiter können dazu beitragen, dass Teammitglieder Betrugsversuche wie E-Mail-Phishing erkennen und entsprechend handeln.

Härtung der System- und Cloud-Sicherheitskonfiguration

Auf Ihren Workstations, Servern und in der Cloud müssen bestimmte Best Practices für Sicherheit und Konfiguration aktiviert sein.

Möchten Sie weitere Informationen?

Eye Security bietet ein erschwingliches Gesamtpaket, mit dem Sie Ihr Cyber-Risiko sofort in den Griff bekommen. Wenn Sie herausfinden möchten, wie widerstandsfähig Sie heute sind, scannen Sie bitte hier:

Besuchen Sie eyesecurity.de