Umfassende Cybersecurity mit Arctic Wolf

Arctic Wolf ®Managed Detection & Response

Umfassende Cybersicherheit dank 24/7-Überwachung

Angesichts der zunehmenden Cyberkriminalität ist es für Unternehmen unerlässlich geworden, eine kontinuierliche Überwachung und schnelle Reaktion auf Bedrohungen zu gewährleisten. Security-Lösungen im Bereich Managed Detection & Response setzen genau hier an und unterstützen Sie bei der Angriffserkennung sowie der Reaktion darauf.

Arctic Wolf® Managed Detection & Response ermöglicht eine Früherkennung von Angriffen und ein proaktives Handeln. Durch die 24/7-Überwachung und koordinierte Incident-Response-Prozesse minimiert die Lösung potentiellen Schaden. Die Sicherheitslage In Ihrem Unternehmen kann somit deutlich verbessert werden und Sie können kritische Daten und Systeme vor immer raffinierteren Cyberangriffen schützen.

Cybersecurity as a Service mit netgo und Arctic Wolf

Durch die zunehmende Anzahl von Cyberattacken und die steigende Komplexität der Angriffe ist es für Unternehmen unabdingbar geworden, ein entsprechendes höheres Sicherheitsniveau zu entwickeln. Doch oftmals ist dies eine große Herausforderung, da viele Unternehmen über limitierte Ressourcen in der IT verfügen.

Hinzu kommt: Den perfekten Schutzschild gegen Cyberangriffe gibt es nicht. Experten für Cybersecurity raten deshalb dazu, eine frühzeitige Bedrohungserkennung und eine effektive Abwehr von Angriffen sowie eine rasche Reaktion im Falle einer Attacke sicherzustellen.

Wie können Unternehmen also vorgehen? Managed Detection & Response (MDR) liefert die passende Antwort auf diese Frage und ist somit ein nicht mehr wegzudenkendes Element in der Cybersicherheit geworden. MDR-Anbieter stellen Security-Operations-Lösungen zur Verfügung, die insbesondere kleineren und mittleren Unternehmen mit begrenzten Ressourcen eine Möglichkeit bieten, um eine Überwachung rund um die Uhr zu ermöglichen und neben der Bedrohungserkennung eine entsprechende Incident Response zu gewährleisten.

Arctic Wolf® Managed Detection and Response (MDR) wird deshalb von vielen Unternehmen weltweit eingesetzt. Die Lösung ist im Handumdrehen einsatzbereit und bietet eine Rund-um-die-Uhr-Überwachung der Netzwerke, Endgeräte und Cloud-Umgebungen durch das Arctic Wolf Concierge Security Team. Bedrohungen, Eindringversuche und Angriffe werden direkt erkannt und eine proaktive sowie dynamische Reaktion darauf wird ermöglicht. Außerdem wird die Wiederherstellung durch Managed Triage- und Concierge-Services abgedeckt.

MDR adressiert somit die kritischsten Herausforderungen in der Cybersicherheit und bietet eine kostengünstige Möglichkeit für Unternehmen, die über keine oder nicht ausreichend In-House-Ressourcen im Bereich Security Operations verfügen.

Wie Arctic Wolf® Managed Detection and Response Unternehmen beim Thema Cybersecurity unterstützt

Über alle Branchen hinweg stehen Unternehmen vor großen Herausforderungen, wenn es um das Thema Cybersicherheit geht:

- Eine wachsende und sich ständig verändernde Bedrohungslandschaft
- Fachkräftemangel in der IT Security und insbesondere in der Cybersecurity
- Lange Reaktionszeiten auf Sicherheitsvorfälle und damit erhöhte Kosten

Hier kommen die Lösungen von Arctic Wolf ins Spiel, denn Managed Detection and Response geht die kritischsten Herausforderungen im Bereich der Cybersecurity an.

Die als Concierge-Service angebotenen Security-Operations-Lösungen von Arctic Wolf bieten die passende Unterstützung für die Cybersicherheit im Unternehmen. Die herstellerunabhängige, Cloud-native Arctic Wolf® Plattform als Basis hilft Ihrem Unternehmen dabei, Cyberrisiken entgegenzuwirken. Hochqualifizierte Concierge Security®-Experten unterstützen rund um die Uhr bei der Überwachung der Infrastruktur sowie der Erkennung von und der Reaktion auf Bedrohungen im Unternehmen.

Darüber hinaus werden Security-Awareness-Schulungen für die Mitarbeitenden in Ihrem Unternehmen angeboten, um Best Practices vorzustellen und Vorgehensweisen von kriminellen Hackern zu veranschaulichen, z. B. bei Social-Engineering-Angriffen.

Die Lösung Arctic Wolf® Managed Detection and Response (MDR) basiert auf den folgenden Säulen:

- **Erkennen**
  Umfassende Transparenz und Überwachung rund um die Uhr durch die Arctic Wolf Security-Operations-Experten – sodass auch komplexe Bedrohungen erkannt werden können

- **Reagieren**
  Gezielte Untersuchungen auf verdächtige Aktivitäten, Log Retention and Search für die vereinfachte Verwaltung von Protokollen und eine umfassende Incident Response für eine rasche Erkennung von und Reaktion auf Sicherheitsvorfälle

- **Wiederherstellen**
  Angeleitete Wiederherstellung und Learnings aus Vorfällen, Ursachenanalyse und regelmäßige Besprechungen zum Überprüfen sowie Verbessern des Sicherheitsniveaus im Unternehmen

Gut zu wissen: Von NIS-2 betroffenen Unternehmen wird Arctic Wolf als MDR-Dienstleister auf der APT-Response-Dienstleister-Liste vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen.

Die wichtigsten Funktionen von Arctic Wolf® Managed Detection and Response

Arctic Wolf® Managed Detection and Response unterstützt Sie mit den folgenden Funktionen, um Angriffe im Unternehmen zu erkennen und darauf zu reagieren:

- **Cloud Detection and Response für IaaS und SaaS:** Zuverlässige Bedrohungs-Identifizierung in Ihrer Cloud-Umgebung
- **Überwachung rund um die Uhr:** Eine 24x7x365-Überwachung stellt sicher, dass Sicherheitsvorfälle und verdächtige Aktivitäten jederzeit erkannt und sofort adressiert werden können
- **Netzwerküberprüfung:** Erkennung von Schwachstellen und Anomalien im Netzwerkverkehr, um proaktiv gegen potentielle Bedrohungen vorgehen zu können
- **Zusammenführung von Protokollen, Korrelation und Analyse:** Umfassende Einblicke in das Sicherheitsgeschehen, um gezielte Maßnahmen gegen Bedrohungen zu ergreifen
- **Bedrohungserkennung:** Frühzeitige Identifizierung potentieller Sicherheitsrisiken, damit Schaden vermieden oder verringert werden kann
- **Compliance-Reporting:** Compliance-Anforderungen wird mit den passenden Berichten entgegengekommen
- **Transparenz:** Die Lösung funktioniert mit Ihrem bestehenden Technologie-Stack, um Assets zu erkennen und zu profilieren sowie Daten und Beobachtungen zu Sicherheitsereignissen aus mehreren Quellen zu sammeln.
- **Incident Response:** Schnelle Reaktion und umfassende Maßnahmen nach einem Sicherheitsvorfall, um die Ursache zu identifizieren, den Schaden zu begrenzen und die Systeme schnellstmöglich wiederherzustellen.

Tipp: Falls Sie mit dem Gedanken spielen eine **Cyberversicherung** abzuschließen oder dies bereits getan haben, kann Sie eine MDR-Lösung dabei unterstützen, die Kosten zu senken: Die Analytics- & Reporting-Möglichkeiten können wichtige Voraussetzungen bei Cyberversicherungen erfüllen. Auch die von Arctic Wolf angebotene **"Security Operations Warranty"** kann eine zusätzliche Sicherheit bieten – oder durch Anrechnung als Eigenanteil die Kosten der Cyberversicherung reduzieren.

Cybersecurity? Kein Problem mit Arctic Wolf!
Insbesondere kleine und mittlere Unternehmen, die nicht über die notwendigen Ressourcen für den Aufbau eines unternehmensinternen Security Operation Centers verfügen, bekommen mit den Lösungen und Services von Arctic Wolf die passende Unterstützung, um die zunehmenden Herausforderungen in der Cybersecurity zu meistern. Für eine zuverlässige, effektive und schnelle Bedrohungserkennung und -abwehr in Ihrem Unternehmen.