Arctic Wolf Managed Detection and Response Lösung

Bedrohungserkennung und -abwehr durch das Concierge Security Team

Unternehmen weltweit haben Schwierigkeiten damit, moderne Cyberbedrohungen effizient zu erkennen und abzuwehren. Obwohl viele IT-Abteilungen Sicherheits-Tools einsetzen, um Abhilfe zu schaffen, führen der Mangel an Rund-um-die-Uhr-Abdeckung sowie an umfassendem Fachwissen im Bereich Security Operations und das Fehlen eines gut besetzten Sicherheitsteams dazu, dass viele Bedrohungen unbemerkt bleiben und monatelang in der Umgebung festsetzen können. Viele medienträchtige Datenschutzverletzungen treten nicht deshalb auf, weil das Sicherheits-Tool keine Warnung ausgelöst hat, sondern weil die Warnung nicht berücksichtigt oder übersehen wurde.

Das Arctic Wolf Concierge Security Team hat innerhalb der ersten 90 Tage des Auftrags in 73 % der Umgebungen unserer Kunden latente Bedrohungen festgestellt.

Die Arctic Wolf® Managed Detection and Response Lösung (MDR)-Lösung basiert auf der branchenweit einzigen Cloud-nativen Plattform, die Sicherheitsoperationen als Concierge-Service bereitstellt. Unsere Lösung reduziert die Überlastung mit Warnmeldungen und Fehlalarmen und ermöglicht eine schnellere Reaktion mit Erkennungs- und Reaktionsfunktionen, die auf die spezifischen Anforderungen Ihres Unternehmens zugeschnitten sind. Ihr Arctic Wolf Concierge Security® Team (CST) arbeitet für Bedrohungssuche, Incident Response und geführte Behebung direkt mit Ihnen zusammen, und stellt strategische Empfehlungen bereit, die speziell auf Ihre Umgebung zugeschnitten sind.

Erkennen

Mehr Erkennen mit kontinuierlicher Überwachung und Bedrohungssuche durch Security-Operations-Experten.

- Umfassende Transparenz
- Überwachung rund um die Uhr
- Bedrohungssuche

Reagieren

Gezielte Untersuchungen und kurze Reaktionzeiten zur schnellen Eindämmung von Bedrohungen.

- Gezielte Untersuchungen
- Incident Response
- Log Retention and Search

Wiederherstellen

Lernen aus Vorfällen und Implementieren benutzerdefinierter Regeln und Workflows für proaktiven Schutz.

- Begleitete Gefahrenbeseitigung
- Ursachenanalyse
- Personalisiertes Engagement

Concierge Security Team

Das Concierge Security Team (CST) ist Ihr zentraler Ansprechpartner für Ihre Arctic Wolf Managed Detection and Response Lösung. Das CST ist Ihr vertrauenswürdiger Security-Operations-Berater und eine Erweiterung Ihres internen Teams. Es übernimmt folgende Aufgaben:

- Überwachung rund um die Uhr
- Triage und Priorisierung von Warnmeldungen
- Benutzerdefinierte Schutzmaßnahmen
- Begleitete Gefahrenbeseitigung
- Detailliertes Reporting und Audit-Unterstützung
- Laufende strategische Sicherheitsüberprüfungen

Vorhandene Infrastruktur effektiv nutzen

Die Arctic Wolf MDR Lösung nutzt Sicherheitstechnologien in Ihrer aktuellen Umgebung, sodass Sie Bedrohungen schnell erkennen, abwehren und den Betrieb wiederherstellen können, ohne sich Gedanken über die Bindung an einen einzelnen Anbieter oder den Austausch Ihrer bestehenden Systeme machen zu müssen.

Erkennung komplexer Bedrohungen

Machine Learning mit adaptiver Optimierung bietet proaktive Bedrohungssuche und forensische Fernanalyse für mehr Effizienz und Skalierbarkeit.

Managed Containment

Schnelle Abwehr von Bedrohungen und Stoppen ihrer Verbreitung, indem die Kommunikation von Host-Geräten nach außen oder mit anderen Geräten im Netzwerk unterbunden wird.

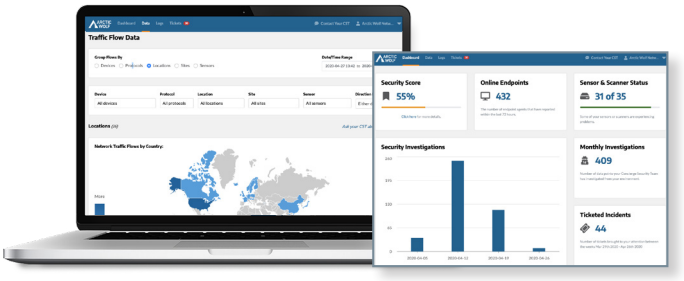
Das Besondere an Arctic Wolf

Umfassende Transparenz

Sicherheitstelemetrie von internen und externen Netzwerken, Endgeräten und Cloud-Umgebungen wird mit Bedrohungs-Feeds, OSINT-Daten, CVE-Informationen, ATO-Daten und mehr angereichert, um Granularität und Kontext für Vorfälle bereitzustellen, die vom Concierge Security Team untersucht und analysiert werden.

Arctic Wolf Kundenportal – Taktische und strategische Erkenntnisse

Eine speziell entwickelte Benutzeroberfläche (GUI) bietet einen Überblick über offene Tickets und ermöglicht es Ihnen, mit Ihrem CST zu interagieren, Ihre Sicherheitsbewertung einzusehen und Bereitstellungselemente wie die Anzahl der derzeit bereitgestellten Arctic Wolf® Agenten anzuzeigen.



Zusammenfassung und angepasste Berichte zum Sicherheitsniveau und zu den Compliance-Anforderungen

Bedrohungserkennung und -abwehr für Endgeräte

Der mitgelieferte Arctic Wolf Agent bietet Endgeräte-Intelligenz und erweiterte Funktionen zur Erkennung von Bedrohungen, die unseren Sicherheitsingenieuren einen tiefen und umfassenden Einblick in Ihre Sicherheitslage ermöglichen.

- Sysmon-Ereignisüberwachung für Ost/West-Sichtbarkeit von Lateral Movements von Bedrohungen
- Wöchentliches Endgeräte-Reporting
- Managed Containment

Unbefristete Log Retention and Search

Die Arctic Wolf® Platform sammelt, normalisiert, analysiert und speichert automatisch Protokolldaten aus bestehenden Netzwerken, Systemen und Anwendungen für mindestens 90 Tage und ist auf Abruf verfügbar, um Ihre Reporting- und Compliance-Anforderungen zu erfüllen.

> „Der Vorteil für mich ist, dass Arctic Wolf eine Erweiterung unseres Teams ist. Arctic Wolf hat dazu beigetragen, unsere Sicherheit zu verbessern und unser Compliance-Reporting zu verbessern. Das Team von Bay Federal konnte sich auf Projekte konzentrieren, die unserem Geschäft den größten Mehrwert bringen."
>
> **– Richard Roark,** Vice President und Chief Information Officer (CIO), Bay Federal Credit Union

Bay Federal CREDIT UNION

ARCTIC WOLF

SOC2-Type-II-zertifiziert

AICPA SOC

ISO 27001 CERTIFIED CYBERGUARD COMPLIANCE

Kontakt

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com