Arctic Wolf® Unternehmensprofil

Das Unternehmen auf einen Blick

Gründung:
2012

Hauptsitz:
Eden Prairie, MN (USA)

Mitarbeiter:
2000+

Lösungen:

- Arctic Wolf® Managed Detection and Response
- Arctic Wolf® Managed Risk
- Arctic Wolf Managed Security Awareness®
- Arctic Wolf® Incident Response

Die Bedeutung von Security-Operations-Lösungen

Unternehmen sind in der heutigen Zeit stärker denn je gefordert, sich umfassend vor zielgerichteten, hochgradig komplexen Angriffen zu schützen. Meist mangelt es jedoch an internen Ressourcen – der Aufbau eines schlagkräftigen Security Operations Centers scheitert an den Kosten, dem hohen Aufwand sowie dem hierfür notwendigen zusätzlichen Personal.

Unternehmen stehen vor grundlegenden Sicherheitsherausforderungen

Zu viele Informationen

Alarm-, Anbieter-, Konformitäts- und Regulierungsmüdigkeit – die Flut an Informationen und Neuerungen endet nie

Mangel an SecurityExperten

Cybersecurity-Experten zu rekrutieren und zu halten, ist schwierig bis unmöglich

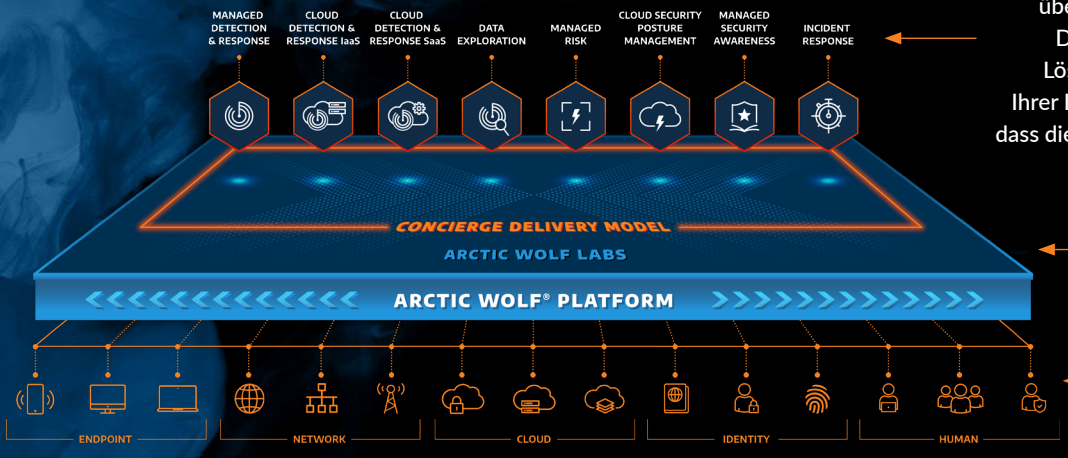
Kosten der Reaktionszeit

Je länger die Reaktion auf einen Vorfall dauert, desto teurer ist die Behebung

Die Bedeutung von Security-Operations-Lösungen

Wir helfen Unternehmen dabei, Cyberrisiken entgegenzuwirken. Hierfür setzen wir auf unsere herstellerunabhängige, Cloud-native Arctic Wolf® Plattform. Diese stellt die Basis für unsere als Concierge-Service angebotenen Security Operations. Hochqualifizierte Concierge Security®-Experten, die sich als verlängerter Arm ihres Teams verstehen, unterstützen Sie rund um die Uhr bei der unternehmensweiten Überwachung ihrer Infrastruktur sowie der Erkennung von und der Reaktion auf Bedrohungen. Des Weiteren schützen wir Ihre Systeme sowie Daten per RisikoManagement permanent und stärken damit ihre Sicherheitslage kontinuierlich. Ein weiterer Leistungsbaustein sind Security-Awareness-Schulungen, in denen wir Ihre Mitarbeiter für das Thema Sicherheit sensibilisieren. Neben bewährten Vorgehensweisen vermitteln wir, woran sich Social-Engineering-Angriffe erkennen lassen und wie man auf diese richtig reagiert.

Die Arctic Wolf Security Operations Cloud



Ihnen explizit zugewiesene und mit Ihrem Unternehmen vertraute Sicherheitsexperten überwachen Ihre Daten rund um die Uhr. Darauf basierend optimieren sie unsere Lösungen fortwährend für den Einsatz in Ihrer IT-Umgebung und stellen damit sicher, dass diese ein Höchstmaß an Effizienz bieten.

Führen sie alle Ihre Daten zur Speicherung, Anreicherung und Analyse in unserer Cloud-nativen Plattform zusammen.

Nutzen Sie Ihren vorhandenen Technologie-Stack, um Endgeräte, das Netzwerk und Cloud-Infrastrukturen im Blick zu behalten.

Lösungen von Arctic Wolf

Die Lösungen von Arctic Wolf sind im Handumdrehen einsatzbereit. Die Installation ist in kürzester Zeit erledigt, darauffolgend startet sofort die Überwachung Ihrer Umgebung. Bedrohungen, Eindringversuche und Angriffe lassen sich im Anschluss direkt erkennen. Dies wiederum ermöglicht proaktiv und dynamisch auf diese zu reagieren. Unternehmen erhalten aktuelle und verwertbare Informationen, anstatt einer endlosen Zahl an Fehlalarmen.

Arctic Wolf Managed Detection and Response

Angriffe erkennen und darauf reagieren

- Cloud Detection and Response für IaaS und SaaS
- Überwachung rund um die Uhr - 24x7x365
- Netzwerküberprüfung
- Zusammenführung von Protokollen, Korrelation und Analyse
- Bedrohungserkennung
- Compliance-Reporting
- Endgeräte-Transparenz
- Incident Response

Arctic Wolf Managed Risk

Angriffe im Keim ersticken

- Cloud Security Posture Management
- Dynamische Ermittlung vorhandener Assets
- Durchführung kontinuierlicher
- Bewertungen
  - Interne Schwachstelle
  - Externe Schwachstelle
  - Host-basierte Schwachstelle
- Erkennung des AccountÜbernahmerisikos
- Sicherheitskontrollen

Arctic Wolf Managed Security Awareness

Mitarbeitern das notwendige Wissen vermitteln, um Social-Engineering-Angriffe zu erkennen und abzuwehren

- Security-Awareness-Schulungen
- Nachverfolgung und Berichterstattung
- Phishing-Simulationen
- Darknet-Überwachung

Arctic Wolf Incident Response

Schnelle Behebung von Cyberangriffen, von der Eindämmung der Bedrohung bis zur Wiederherstellung des Geschäftsbetriebs

- Benannter Incident-Verantwortlicher
- Fortschrittsupdates und Meilensteinverfolgung
- Klare Erklärungen der Untersuchungsergebnisse der digitalen Forensik
- Response Service Level Agreement von 1 Stunde
- Unterstützung bei der IR-Planung, Überprüfung und sicheren Aufbewahrung