Arctic Wolf Managed Risk Lösung

Kontinuierliches Risiko-Management durch das Concierge Security Team

Überall kämpfen Unternehmen mit der Komplexität der Identifizierung und Verwaltung von Sicherheitsrisiken in ihrer Umgebung. Oftmals sind selbst grundlegende Informationen wie beispielsweise, welche Assets vorhanden sind, welche Systeme Schwachstellen aufweisen und welche Systeme nicht richtig konfiguriert sind, nur schwer zu beschaffen. Und wenn diese Informationen verfügbar sind, ist das Sicherheitsteam normalerweise von der Menge überfordert, da vorhandene Tools zu viele Warnungen generieren und keinen Kontext liefern. Während sie damit kämpfen, was als Nächstes zu tun ist und wie sie Prioritäten setzen sollen, häufen sich die Risiken und machen das Unternehmen anfällig für Bedrohungen und Datenschutzverletzungen.

> „Bis 2022 werden Unternehmen, die risikobasierte Vulnerability-Management-Prozesse einsetzen, 80 % weniger Sicherheitsverletzungen verzeichnen."
>
> **– Dale Gardner,** Forecast Analysis: Risk-Based Vulnerability Management, Worldwide | Veröffentlichungsdatum: 14. Juni 2019, ID: G00384640

Die Arctic Wolf® Managed Risk-Lösung basiert auf der branchenweit einzigen Cloud-nativen Plattform, die Security Operations als Concierge-Service bereitstellt. Die Lösung ermöglicht das kontinuierliche Scannen Ihrer Netzwerke, Endgeräte und Cloud-Umgebungen, um digitale Risiken zu quantifizieren. Ihr Security-Operations-Experte vom Concierge Security® Team arbeitet direkt mit Ihnen zusammen, um Risiken zu erkennen, die über einfache Schwachstellen hinausgehen, den aktuellen Zustand Ihrer Umgebung zu vergleichen und Risiko-Management-Prozesse zu implementieren, die Ihr Sicherheitsniveau im Laufe der Zeit stärken.

Entdecken

Identifizierung und Kategorisierung von riskanter Software, riskanten Assets und Konten.

- Risikotransparenz
- Dynamische Asset-Erkennung
- Risikoüberwachung rund um die Uhr

Benchmark

Quantifizierung des digitalen Risikos und Identifizierung von Lücken.

- Sicherheitskontroll-Benchmarks
- Risikobewertung
- Umsetzbares Reporting

Verstärken

Ermittlung von Schwachstellen und Priorisierung von Verbesserungen des Sicherheitsniveaus

- Geführte Abwehr
- On-Demand-Reporting
- Strategische Empfehlungen

ConciergeSecurityTeam

Das Concierge Security Team (CST) ist Ihr zentraler Ansprechpartner für Ihre Arctic Wolf Managed Risk Lösung. Das CST ist Ihr vertrauenswürdiger Sicherheitsberater und eine Erweiterung Ihres internen Teams. Es übernimmt folgende Aufgaben:

- Anpassung des Service an Ihre Bedürfnisse
- Kontinuierliches Scannen Ihrer Umgebung auf digitale Risiken
- Monatliche Überprüfungen der Risikolage
- Bereitstellung umsetzbarer Anleitungen zur Abwehr
- Erstellung von Risiko-Management-Plänen gemeinsam mit Ihnen
- Bereitstellung eines angepassten Risiko-Management-Plans zur Priorisierung der Abwehr und Messung des Fortschritts

Umfassender Überblick über Ihre Risikolage

Das Gesamtbild sehen

Bewerten Sie Risiken im Zusammenhang mit Ihren internen und externen Netzwerken, Geräten, Cloud-Umgebungen, Systemkonfigurationen und mehr, um zu verstehen, wie Ihre kritischen Ressourcen beeinträchtigt werden könnten.

Risiken entdecken, die andere übersehen

Arctic Wolf® bietet eine kontinuierliche Erkennung digitaler Risiken, die über einfache Schwachstellen hinausgehen und von herkömmlichen Tools nicht identifiziert werden können.

Priorisieren, was wichtig ist

Quantifizieren Sie das digitale Risiko mithilfe von Daten, die von der Arctic Wolf® Platform angereichert wurden, sowie aussagekräftige numerische Risikobewertungen und Fall-Management-Workflows, damit Sie Fehlalarme herausfiltern und sich auf das Wesentliche konzentrieren können.

Arctic Wolf Managed Risk – Funktionen

Externe Schwachstellenanalyse

Kontinuierliche Scans von mit dem Internet verbundenen Assets, um den digitalen Fußabdruck des Unternehmens zu verstehen und das Risiko zu quantifizieren. Die wichtigsten Funktionen:

- Kontinuierliches Scannen von nach außen gerichteten Assets
- Cloud Security Posture Management (CSPM)
- Erkennung des Account-Übernahmerisikos
- OWASP-Top-10-Scannen
- Automatisierte Unterdomänen-Erkennung

Quantifizierung der Cyberrisiko-Lage

Ein Cloud-basiertes Dashboard bietet einen Überblick über die kontinuierliche Cyberrisiko-Bewertung mit allen aussagekräftigen Cyberrisiko-Indikatoren aus Ihrem Unternehmen. Probleme mit der höchsten Priorität werden identifiziert, und Sie werden vor aufkommenden Risiken gewarnt, bevor diese zu echten Problemen eskalieren. Mit folgenden Schlüsselfunktionen können Sie sinnvolle und effiziente Maßnahmen zur Risikominderung ergreifen:

- Umfassende Risikoprofilierung
- Informative Benutzeroberfläche
- Proaktive Benachrichtigungen und Warnungen
- Umsetzbares Reporting
- API-Integrationen

Abbildung 1: Umsetzbare Erkenntnisse aus dem Managed Risk Dashboard

Interne Schwachstellenanalyse

Kontinuierliches Scannen aller internen IP-verbundenen Geräte und Katalogisierung von Kerninfrastruktur, Geräten/Peripheriegeräten, Workstations, IoT-Geräten (Internet of Things) und persönlichen Geräten (z. B. Tablets). Die wichtigsten Funktionen:

- Kontinuierliches Scannen von internen Assets
- Proaktive Risikoüberwachung
- Dynamische Asset-Identifikation und -Klassifizierung
- Zustandsloses Scannen und sichere Übertragungen

Host-basierte Schwachstellenanalyse

Erweiterte Sichtbarkeit innerhalb von Geräten durch kontinuierliche Host-basierte Überwachung, um Assets zu identifizieren und zu kategorisieren und Systemfehlkonfigurationen, Benutzerverhalten und Schwachstellen aufzudecken, die das Unternehmen gefährden. Die wichtigsten Funktionen:

- Endgeräte-Agents für Windows Server/Workstation, MacOS und Linux-Distributionen
- Proaktive Risikoüberwachung für Endgeräte
- Audit-Reporting
- Sicherheitskontroll-Benchmarks

> „Ein Team, das Schwachstellen bewertet und managt und gleichzeitig unsere Umgebung überwacht, hilft uns wirklich, unsere Angriffsfläche zu verkleinern. Wir haben erhebliche Fortschritte bei der Wiederherstellung der Integrität und des Vertrauens in unsere IT-Systeme gemacht, aber das Risiko verschwindet nie. Wenn wir uns dessen nicht bewusst sind, können wir nicht daran arbeiten, es zu mindern."
>
> **– Dr. Jason A. Thomas,** Chief Operating Officer und Chief Information Officer, Jackson Parish Hospital

JACKSON PARISH HOSPITAL

ARCTIC WOLF

SOC2-Type-II-zertifiziert

AICPA SOC

ISO 27001 CERTIFIED CYBERGUARD COMPLIANCE

Kontakt

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com