Managed Threat Detection

Ein risikobasiertes Konzept für Ihr Sicherheitsmonitoring

DIE HERAUSFORDERUNG: IM SCHNITT DAUERT ES 146[1)] TAGE, BIS EIN UNTERNEHMEN EINE CYBER-ATTACKE ERKENNT

Aktuelle Angriffe auf namhafte Unternehmen zeigen, dass präventive Maßnahmen alleine nicht ausreichen, um sich vor den immer komplexer werdenden Cybersecurity-Bedrohungen zu schützen. Die durchschnittlichen Kosten von Sicherheitsvorfällen belaufen sich mittlerweile auf über $4 Mio. Das bedeutet einen Anstieg um mehr als 29 Prozent seit dem Jahr 2013.

Die Zeitspanne zwischen der Erkennung von Bedrohungen und der Einleitung von Gegenmaßnahmen kann drastische Auswirkungen auf die Kosten eines Sicherheitsvorfalls haben. Die effiziente und wirkungsvolle Erkennung von Bedrohungen stellt viele Unternehmen vor große Herausforderungen: Das betrifft beispielsweise das rasant ansteigende Volumen an sicherheitsrelevanten Informationen und Daten, technologische Einschränkungen, ineffiziente Nutzung von vorhandenen Bedrohungsinformationen, fehlende Überwachung von IoT-Geräten und den Mangel an qualifizierten Cybersecurity-Spezialisten.

[1] Ponemon Institute – 2016 Cost of Data Breach Study | The Impact of Data Breaches on Reputation & Share Value

DIE LÖSUNG: EINE RISIKOBASIERTE NEXT-GENERATION-LÖSUNG FÜR DIE SCHNELLE ERKENNUNG UND BEHANDLUNG VON SICHERHEITSVORFÄLLEN

Der Managed Threat Detection Service von TÜV Rheinland sorgt für die Ausrichtung und Integration der Erkennungsmechanismen und Gegenmaßnahmen in das Risikomanagement Ihres Unternehmens. So wird die Zeitspanne zwischen Erkennung der Bedrohung und Einleitung von Maßnahmen erheblich verkürzt.

Unsere Lösung besticht durch eine hohe Skalierbarkeit und eine kurze Implementierungszeit. Sie ist auf die Echt-Zeit-Analyse von sehr großen Mengen an Sicherheitsdaten ausgelegt und liefert schnelle, zielgruppenorientierte Ergebnisse, die in einfach zu verstehenden Dashboards zur Verfügung gestellt werden. Für die Identifizierung von bekannten und unbekannten Bedrohungen nutzen wir verschiedene Mechanismen zur Erkennung von Verhaltensabweichungen. Ergänzt durch maschinelles Lernen und die Integration von Bedrohungsinformationen, die wir tagtäglich sammeln, sowie der Bedrohungsdetails, die von unseren Kunden bereitgestellt werden, verbessern wir unsere Erkennungsfähigkeiten kontinuierlich und nachhaltig.

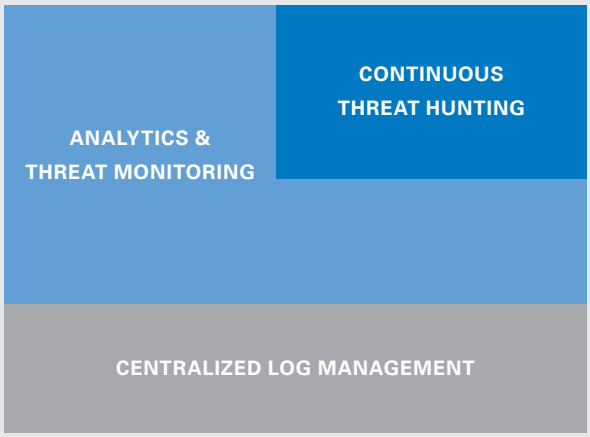
SICHERHEITSMONITORING: RISIKOBASIERTER ANSATZ

[2)] KRI = Key Risk Indicator, KPI = Key Performance Indicator

www.tuv.com/informationssicherheit

TÜVRheinland®
Genau. Richtig.

MANAGED THREAT DETECTION SERVICE



IHRE VORTEILE AUF EINEN BLICK

- Verbesserte Erkennung und Bekämpfung von bekannten und unbekannten Bedrohungen – zur Reduzierung der Häufigkeit und der geschäftskritischen Auswirkungen von Sicherheitsvorfällen.
- Unser Service basiert auf einem OPEX-Model. Damit entfallen die im klassischen Umfeld notwendigen initialen Investitionsausgaben (CAPEX) in Hardware und Software und die damit verbundenen Implementierungs- und Änderungsanforderungen.
- Schaffung von mehr Transparenz in Umgebungen, die keine traditionellen Log-Daten generieren. So werden Risiken in Technologiebereichen, die zunehmend zum Angriffsziel werden, reduziert.
- Senkung der Betriebskosten durch Integration und Automatisierung.

SERVICE HIGHLIGHTS

- Globaler 24x7-Service für Echtzeit-Monitoring und Threat-Hunting mit Big-Data-Analyse, maschinelles Lernen, Erkennung von Verhaltensabweichungen, sowie Threat Intelligence.
- Unterstützt durch eine skalierbare Plattform mit umfangreichen Datenschutzmechanismen.
- Zentrale Speicherung von Log-Daten und sicherheitsrelevanten Informationen.
- Überwachung von Unternehmens-, IoT- und OT-Umgebungen auf Cyber-Bedrohungen.
- Schnelle Ergebnisse durch kurze Implementierungszeit.

WARUM TÜV RHEINLAND?

- Beratungs- und Lösungskompetenz in den Bereichen Informationssicherheit und Cybersecurity seit nahezu 20 Jahren
- Ca. 20.000 Mitarbeiter in 70 Ländern in Europa, Amerika und Asien
- Weltweit führender unabhängiger Prüfdienstleister mit einem Jahresumsatz von über € 1,9 Milliarden
- Mitglied im Global Compact der Vereinten Nationen für mehr Nachhaltigkeit und gegen Korruption

LASSEN SIE SICH VON UNSEREN THREAT DETECTION EXPERTEN BERATEN.

TÜV Rheinland
ICT & Business Solutions
Am Grauen Stein
51105 Köln
Tel. +49 221 806-0
service@i-sec.tuv.com

www.tuv.com/de/managed-threat-detection

TÜVRheinland®
Genau. Richtig.