SOLUTION BRIEF

Optimierte Sicherheitsanalysen für mehr Resilienz

Bedrohungserkennung beschleunigen und Verfügbarkeit von Logdaten sicherstellen

SIEMs und Sicherheitsanalysen sind für die moderne Cybersicherheit von entscheidender Bedeutung, da sie eine Bedrohungserkennung in Echtzeit, eine Protokollkorrelation und eine effektivere Reaktion auf Vorfälle in der gesamten IT-Umgebung eines Unternehmens bieten. Sie erfassen enorme Datenmengen aus Netzwerk-, Benutzer-, System- und Anwendungsprotokollen, um anomale oder verdächtige Aktivitäten zu identifizieren.

Allerdings haben SIEMs und Sicherheitsanalysen aufgrund von Skalierbarkeitsbeschränkungen, hohen Storage-Kosten und Performance-Engpässen häufig Schwierigkeiten, mit den enormen Datenmengen Schritt zu halten. Der Zustrom von Protokollen aus verschiedenen Quellen überfordert herkömmliche Architekturen, was zu einer langsamen Abfrageperformance, einer verzögerten Erkennung von Bedrohungen und einer erhöhten Anzahl von Fehlalarmen führt. Darüber hinaus erfordert die Verwaltung und Korrelation großer Datenmengen in Echtzeit eine erhebliche Rechenleistung, was häufig die die Ressourcenauslastung und die betriebliche Komplexität erhöht.

Speicherherausforderungen für Cybersicherheits-Monitoring- und Analysesysteme

Im Bereich der Cybersicherheit wird Speicher häufig nur als Nebenaspekt betrachtet – dabei spielt er eine entscheidende Rolle für Transparenz, Leistung und Resilienz moderner Security-Monitoring- und Analysesysteme wie SIEM, UEBA und XDR. Unternehmen sollten Speicher als festen Bestandteil ihrer Strategien für Security Monitoring und Analysen berücksichtigen, da SIEM- und Sicherheitsanalysetools mit effizienter Datenspeicherung mehrere zentrale Herausforderungen adressieren:

1. **Transparenz**: Daten sind das primäre Ziel von Angreifern, insbesondere geschäftskritische Daten, die die Geschäftskontinuität gewährleisten. Speichersysteme für geschäftskritische Anwendungen müssen nahtlos in Sicherheits- und Analysetools integriert sein, um verdächtige Zugriffe zu erkennen, die auf Ransomware-Aktivitäten oder Datendiebstahl hindeuten könnten.
2. **Performance:** Die Erkennung von Bedrohungen in Echtzeit hängt von einem latenzarmen Zugriff auf große Datenmengen für schnelle Abfragen und Analysen ab. Diese Systeme verarbeiten große Mengen an Protokoll- und Ereignisdaten und erfordern daher **skalierbaren Storage mit hoher Perfomance,** um mit der Nachfrage Schritt zu halten. Die schnelle Identifizierung von IoCs (Indicators of Compromise) ist entscheidend, um Risiken zu minimieren und eine schnelle Wiederherstellung zu gewährleisten.

Transparenz Ihres Storage verbessern

Überwachen Sie die Analysen Ihrer kritischen Workloads zum Aufspüren von Daten- und Benutzungsanomalien.

Resilienz Ihrer Sicherheitsanalysen verbessern

Stellen Sie sicher, dass Ihre kritischen Protokolldaten bei Bedarf verfügbar sind.

Performance von Sicherheitsanalysen optimieren

Beschleunigen Sie die Erkennung von Bedrohungen und unterstützen Sie die Skalierungsanforderungen bei wachsenden Protokolldaten.

3. **Resilienz:** Die Verfügbarkeit hängt von einem wirksamen Schutz vor **zerstörerischen Cyberbedrohungen** ab – einschließlich Ransomware und Insiderangriffen. Bedrohungsakteure zielen gezielt auf Logdaten ab, um ihre Aktivitäten zu verschleiern und eine schnelle Wiederherstellung zu verhindern. **Und eine langfristige Datenaufbewahrung** ist entscheidend für Compliance, Forensik und Trendanalysen – sie erfordert kosteneffiziente, zugleich aber sichere Speicherlösungen.

Transparenz, Performance und Resilienz

Pure Storage® ermöglicht es Ihnen, Bedrohungen in kritischen Speicherumgebungen zu erkennen und diese an Ihr SIEM- sowie Ihre Sicherheitsanalysetools weiterzuleiten, Leistungsengpässe zu beseitigen und die Resilienz Ihres Logdaten-Repositorys sicherzustellen. Mit der Performance und Zuverlässigkeit von Pure Storage können Sie die Leistungsfähigkeit und Stabilität Ihrer On-Premises-Sicherheitsanalysen optimieren – für eine schnellere Erkennung von Anomalien und Bedrohungen. Sollte der Ernstfall eintreten, sind Logdaten von entscheidender Bedeutung. Die Pure Storage Plattform schützt Daten-Repositorys für Sicherheitsanalysen vor böswilligem Löschen durch Ransomware und andere Cyberbedrohungen – dank mehrschichtiger Resilienz, robuster Datensicherheit und Unveränderlichkeit der Daten.

Transparenz, Performance und Resilienz bilden die Grundlage für eine effektive Sicherheitsanalyse. Transparenz gewährleistet, dass Sie die Angriffsfläche Ihres Daten-Storage verstehen, die Kontrolle über Ihre Datensicherheitsvorkehrungen erlangen und Ihr Repository für Protokolldaten auf Bedrohungen überwachen können. Hohe Performance bedeutet, dass Sie mit den enormen Mengen an Logdaten Schritt halten können, die Ihre SIEM-, UEBA-, XDR- und andere Lösungen korrelieren und analysieren müssen, um Bedrohungen schnell zu erkennen. Mehrschichtige Resilienz gewährleistet Datenverfügbarkeit, wenn Angreifer Ihr Repository für Sicherheitsanalysedaten ins Visier nehmen.

Für maximale Transparenz ist Pure Storage in gängige SIEM- und Analysetools integriert – darunter CrowdStrike, Varonis, Cisco, Splunk, Microsoft Sentinel, Cisco XDR, Exabeam, LogRhythm, Palo Alto Networks, QRadar und Elastic. Logdaten von Pure Storage liefern Einblicke in ungewöhnliche Datenänderungen, die auf ein Ransomware-Verschlüsselungsereignis hinweisen könnten, oder in Benutzeraktivitäten, die auf Datenexfiltration oder Datendiebstahl hindeuten. Die Überwachung Ihrer wichtigen Daten verbessert Ihre Cyberresilienz und verringert das Risiko von Schäden durch Ransomware oder andere böswillige Angriffe.

Pure Storage bietet durch lokale SIEM- und Sicherheitsanalysetools eine optimale Performance bei der Erkennung von Bedrohungen. Die Pure Storage-Plattform mit FlashArray™ und FlashBlade® erfüllt vielfältige Anforderungen mit leistungsstarken, einheitlichen Block- und Dateiservices, die auf einem einzigen Storage-Pool ausgeführt werden. Sie konsolidiert unterschiedliche Workloads, skaliert auf Petabyte-Ebene bei extrem geringem Footprint und bietet fortschrittliche Datenreduktion mit intelligenter Deduplizierung und Kompression, wodurch sie herkömmlichen festplattenbasierten Storage effektiv ersetzt.

Für die Resilienz Ihrer lokalen Sicherheitsanalysetools bieten die umfassenden Resilienzfunktionen von Pure Storage eine Datenverfügbarkeit von 99,9999 %. Sicherheits- und Wiederherstellungsinnovationen wie SafeMode™-Snapshots, Zero-Trust-Sicherheitsfunktionen, Anomalieerkennung sowie schnelle Problemlösung und Wiederherstellung sind in unsere Plattform integriert. In Verbindung mit strengen Service Level Agreements (SLAs) gewährleisten diese Funktionen, dass Pure Storage nicht nur Daten schützt und die Erkennung von Bedrohungen unterstützt, sondern auch eine schnelle und nahtlose Wiederherstellung von Sicherheitsanalysedaten ermöglicht. Pure1®-Tools stärken Unternehmen durch proaktive Bewertungen zusätzlich und bieten eine Datenschutz- und Sicherheitsbewertung zur Optimierung und Verfeinerung von Sicherheitsstrategien.

Pure Storage erweitert die Transparenz, Performance und Resilienz von Sicherheitsanalysen durch die Integration mit führenden Sicherheitstools, die Optimierung der Protokolldatenanalyse und den Schutz von Repositorys vor Cyberbedrohungen. Mit branchenführenden Performance-, Sicherheits- und Wiederherstellungsfunktionen stellt Pure Storage sicher, dass Unternehmen Angriffe schnell und effektiv erkennen, darauf reagieren und sich davon erholen können.

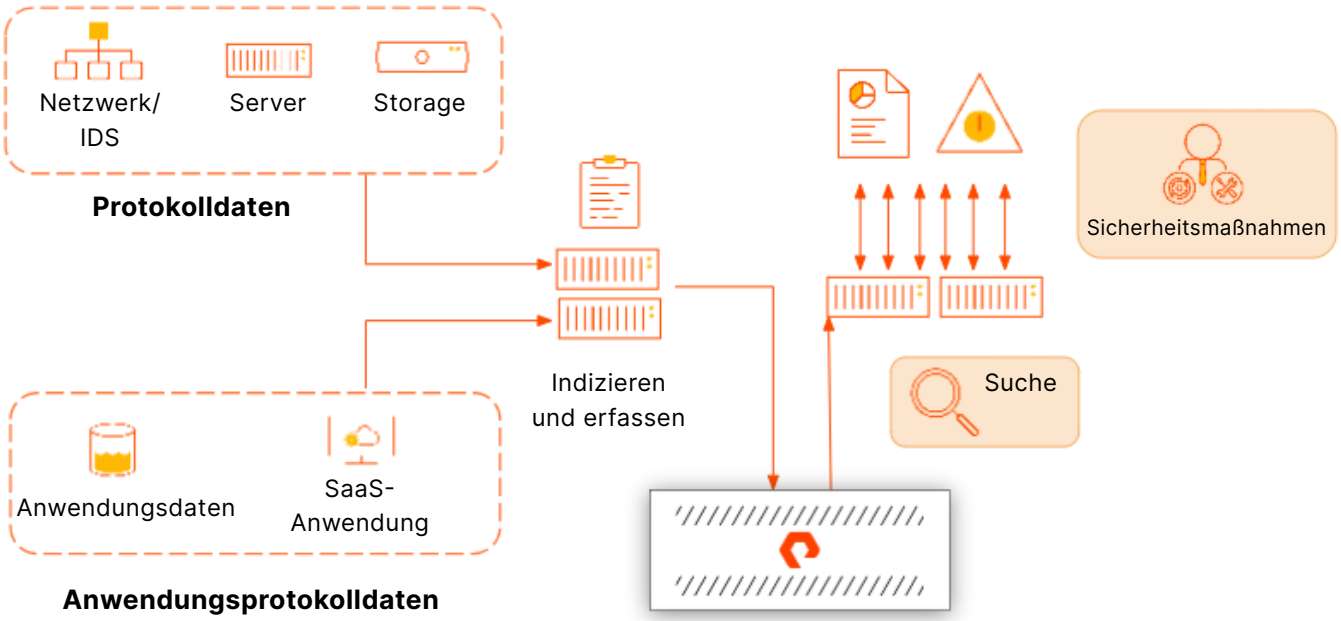

FIGURE 1 Architektur zur Erhöhung der SIEM-Performance

Kritische Funktionen

Die marktführenden Funktionen und Integrationen von Pure Storage unterstützen Unternehmen dabei, sich schnell von Cyberangriffen und Katastrophen zu erholen. Die Pure Storage-Plattform unterstützt die Erkennung und Reaktion auf Bedrohungen, die auf die Plattform abzielen, mit folgenden Funktionen:

Integrationen für Cybersicherheit:

- Integration mit SIEM-, UEBA- und XDR-Lösungen, um Transparenz in Echtzeit für Storage-Bedrohungen zu bieten
- Verbesserung der Bedrohungserkennung, Performance und Skalierbarkeit bei Verwendung als lokale SIEM-, UEBA- und XDR-Storage-Tier
- Gewährleistung maximaler Resilienz des lokalen Storage für SIEM-, UEBA- und XDR-Lösungen

Sichere, skalierbare und leistungsstarke Plattformgrundlage für Cyberresilienz:

- Unterstützung bei der Vereitelung von Ransomware-Angriffen mit unveränderlichen und unlöschbaren SafeMode-Snapshots, Zero-Trust-Sicherheitsprinzipien und Anomalieerkennung
- Konsolidierung von Block- und Datei-Workloads sowie Beseitigung von Datensilos durch dynamische Bereitstellung von Wiederherstellungs-Workloads
- Erzielung einer extrem niedrigen Latenzperformance (150 µs bis 1 ms) für schnellen Datenzugriff mit hoher Verfügbarkeit (99,9999 %)

Cyberresilienz mit Pure1:

- Nutzung von Datenschutz- und Sicherheitsbewertungen zur Beurteilung des Systemzustands, des Sicherheitsstatus und der Performance
- Dashboards und vorausschauende Analysen zur Echtzeitüberwachung und Optimierung der Kapazitätsperfomance
- Praxisrelevante Erkenntnisse und nahtlose Integration mit Wiederherstellungs- und Sicherheitsservices

Weitere Informationen finden Sie auf unserer Seite zu Cyberresilienz-Lösungen.

Weitere Ressourcen

- Mehr über Pure Storage und Varonis erfahren
- Mehr über Pure Storage und Cisco Splunk erfahren
- Mehr über Pure Storage und Cisco XDR erfahren
- Mehr über Pure Storage und LogRhythm erfahren
- Mehr über Pure Storage und QRadar erfahren
- Mehr über Pure Storage und Microsoft Sentinel erfahren
- Mehr über Technology Alliance Partners von Pure Storage erfahren

purestorage.com/de

+49 89 26200662

PS2754-01-de 11/25