riverbed

LÖSUNGSÜBERSICHT

Alluvio IQ automatisiert forensische Sicherheitsanalysen

Verbessert die Effektivität von herkömmlichen SIEM- und SOAR-Tools mit Zugriff auf detaillierte NPM-Daten.

Intelligente Sicherheit ist heute ein wichtiger Faktor für alle hybriden Netzwerke. Unternehmen wachsen über das Rechenzentrum hinaus, wodurch sie über das erweiterte Netzwerk angreifbar werden – durch Außenstellen-, Campus- und Cloud-Ressourcen. Um mit den allgegenwärtigen Bedrohungen Schritt zu halten, müssen SecOps-Teams intelligente Automatisierungen und eine effektive Netzwerkforensik für die aktive Bedrohungserkennung und -abwehr einsetzen. Herkömmliche Sicherheitstools reichen oft nicht mehr aus, weil sie eine unzuverlässige oder stichprobenartige Telemetrie verwenden und auf Vorfälle nicht automatisch reagieren können. Das Ergebnis sind zeitaufwendige, arbeitsintensive manuelle Untersuchungen, die häufig ungenauer sind. Das stellt Sicherheitsteams vor große Herausforderungen, denn es wird von ihnen erwartet, dass sie Sicherheitsrisiken reduzieren, aber auch das zuverlässige digitale Erlebnis für die Mitarbeiter und Kunden beibehalten.

Herkömmliche Sicherheitstools mit automatisierten Untersuchungen verbessern

Alluvio™ IQ, der Unified Observability-Service von Riverbed, verbessert die Zusammenarbeit zwischen NetOps- und SecOps-Teams, indem die Untersuchungen von allgegenwärtigen Bedrohungen mit intelligenter Automatisierung auf Grundlage von detaillierten Netzwerkdaten mit Flow-, Paket- und Infrastrukturkennzahlen unterstützt werden. Alluvio IQ untersucht die Bedrohungen, die in gängigen Sicherheitstools wie SIEM (Sicherheitsinformations- und Ereignismanagement) oder SOAR (Sicherheits-Orchestrierung, Automatisierung und Reaktion) gefunden werden, und verwendet effektive Low-Code-Runbooks, um die Erfassung von nützlichen forensischen Daten aus dem gesamten Alluvio™ NPM-Portfolio (Netzwerk-Performance-Management) zu automatisieren. Alluvio IQ ermittelt die forensischen Daten für verwertbare Erkenntnisse, damit sich SecOps auf echte Bedrohungen konzentrieren können und nicht manuell False-Positives hinterherjagen. Die automatisierte Sicherheitsforensik verwendet hochanpassbare, sicherheitsspezifische Runbooks, um die relevantesten Daten herauszufiltern, damit SecOps-Teams die erforderlichen Daten für intelligente Sicherheitsuntersuchungen und die Abwehr von Cyberbedrohungen erhalten.

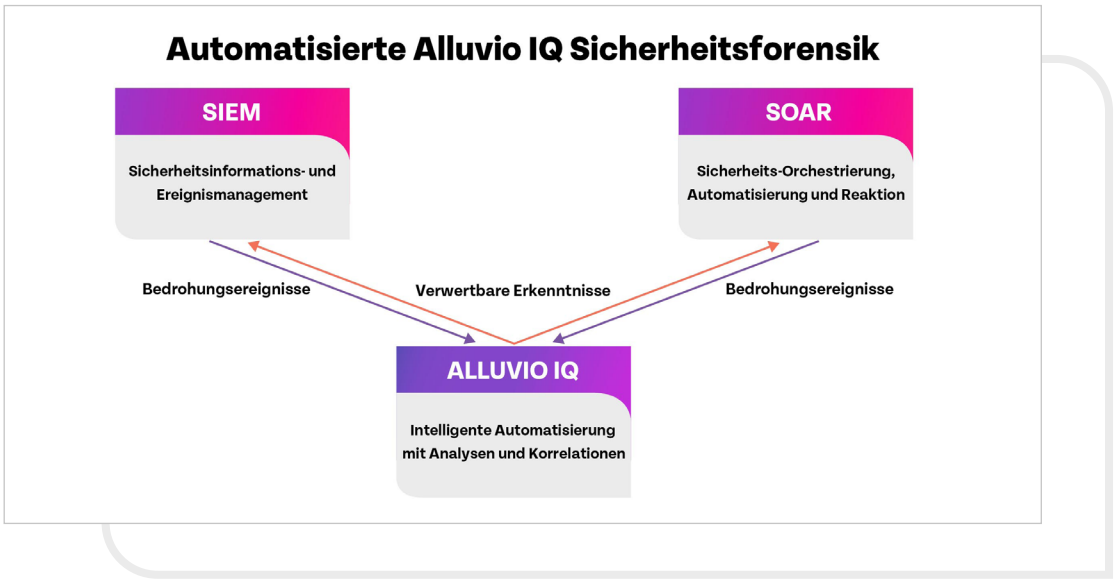


Abbildung 1: Alluvio IQ untersucht Bedrohungen in gängigen Sicherheitstools wie SIEM oder SOAR und bietet effektive Low-Code-Runbooks, um nützliche forensische Daten aus dem gesamten Alluvio NPM Portfolio zu sammeln.

Netzwerkinformationen und Sicherheitsforensik von einem zentralen Anbieter nutzen

Unternehmen müssen oft mehrere Produkte von verschiedenen Anbietern einsetzen, um eine durchgängige Transparenz für ihre hybriden Netzwerke zu erhalten. Alluvio IQ und Alluvio NPM-Lösungen (Netzwerk-Performance-Management) gehören zum Alluvio Unified Observability Portfolio von Riverbed und bieten eine detaillierte Telemetrie und einheitliche Transparenz, um allen Abteilungen wertvolle Daten zu liefern. Riverbed vereint Daten, Erkenntnisse und Aktionen für die gesamte IT, einschließlich NetOps und SecOps. Mit Alluvio IQ Unified Observability gehören isolierte Daten, Krisensitzungen und ständige Warnungen der Vergangenheit an. Die IT kann bessere Entscheidungen in allen Bereichen ermöglichen, Fachwissen umfassender anwenden und das digitale Erlebnis und die Unternehmensleistung kontinuierlich verbessern.

Effektivität der Sicherheitstools verbessern

Herkömmliche Sicherheitstools wie SIEM und SOAR sind nur so gut wie die Informationen, die sie verarbeiten. Die Netzwerkdaten, die diese Tools verwenden, werden oft nur stichprobenartig erfasst oder die SecOps-Teams können nur schwer darauf zugreifen. Verwenden Sie stattdessen eine Datenquelle, die detaillierte Netzwerktelemetrie mit der Erfassung aller Paket-, Flow- und Gerätekennzahlen und verwertbare Erkenntnisse von intelligenten, automatisierten Runbooks bietet, um die Effektivität der Sicherheitsuntersuchungen zu steigern.

Intelligente Automatisierung nutzen und manuelle Untersuchungen von False-Positives reduzieren

Alluvio IQ kann Daten von Alluvio Telemetrie sowie Drittanbieterlösungen erfassen und anpassbare Automatisierungsskripts anwenden, um wichtige Sicherheitsvorfälle zu identifizieren. Die optimierten verwertbaren Erkenntnisse beinhalten nur die relevantesten Vorfälle, während False-Positives aussortiert werden. SecOps-Teams können sich auf echte Gefahren konzentrieren, um Sicherheitsbedrohungen im gesamten modernen hybriden Netzwerk zu identifizieren und abzuwehren.

Zusammenarbeit zwischen NetOps und SecOps verbessern

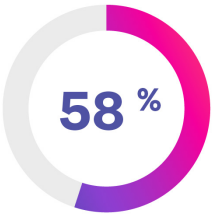
Diese beiden Abteilungen konkurrieren oft um operative Prioritäten, die sich letztendlich auf die Netzwerk-Performance und -Sicherheit auswirken. Beide Teams brauchen Netzwerkdaten, um ihre Arbeit effektiv zu erledigen. NetOps-Teams müssen eine hohe Performance im Netzwerk und in den Anwendungen sicherstellen, während Sicherheitsteams auf Netzwerkdaten angewiesen sind, um Risiken für das Netzwerk und die Infrastruktur zu vermeiden.

Die automatisierten Untersuchungen von Alluvio IQ erleichtern die Zusammenarbeit, indem die Verantwortungsbereiche klar getrennt werden. NetOps ist für die Netzwerktelemetrie verantwortlich, während SecOps für die herkömmlichen Sicherheitstools verantwortlich ist, welche die detaillierten Netzwerk-Performance-Daten von Alluvio nutzen, um das Unternehmen vor Cyberbedrohungen zu schützen.

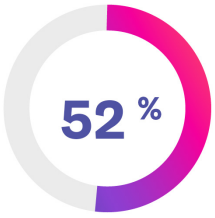
Vorteile der automatisierten Sicherheitsforensik von Alluvio

Neben der besseren Zusammenarbeit zwischen NetOps- und SecOps-Teams bietet die automatisierte Sicherheitsforensik den SecOps-Teams die folgenden Vorteile:

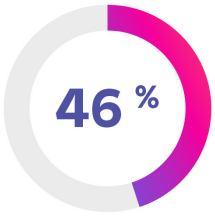
Die 3 wichtigsten Vorteile der erfolgreichen NetSecOps-Zusammenarbeit:



Schnellere Behebung von Sicherheitsproblemen



Reduzierte Sicherheitsrisiken



Betriebseffizienz

Enterprise Management Associates

- **Geschwindigkeit und Effizienz:** Mit Automatisierung können große Datenmengen schnell verarbeitet, Muster erkannt und detaillierte Diagnosedaten erfasst werden, damit Sicherheitsvorfälle deutlich schneller identifiziert, analysiert und gelöst werden.
- **Genauigkeit:** Automatisierte Tools sind weniger anfällig für menschliche Fehler und können größere Datenmengen konsistenter und zuverlässiger analysieren. Dadurch wird das Risiko, dass äußerst wichtige Anzeichen einer Sicherheitsverletzung übersehen oder unwichtige Ereignisse als Bedrohungen missverstanden werden, deutlich reduziert.
- **Konsistenz:** Alluvio IQ verwendet eine Kombination aus KI, Korrelation und Automatisierung, um Sicherheitsvorfälle konsistent zu analysieren und zu priorisieren, während auch nützliche und verwandte Diagnosedaten erfasst werden, um alle verwandten Bedrohungen zuverlässig zu identifizieren.
- **Skalierbarkeit**: Die automatisierte Sicherheitsforensik kann einfach skaliert werden, um große Datenmengen von verschiedenen Systemen und Geräten zu analysieren. Dadurch können Sicherheitsvorfälle schnell und effizient identifiziert und bearbeitet werden.
- **Wirtschaftlichkeit:** Automatisierte Tools können die Workload von Sicherheitsanalysten reduzieren, damit diese sich auf komplexere Sicherheitsprobleme konzentrieren können. Das kann dazu beitragen, die Gesamtkosten für die Verwaltung von Sicherheitsvorfällen zu reduzieren.

Wenn die Sicherheitsforensik automatisiert wird, können SecOps-Teams insgesamt schneller und effektiver auf Sicherheitsvorfälle reagieren, während der Workload und die Kosten im Vergleich zu manuellen Methoden sinken.

Über Alluvio IQ

Alluvio IQ, die cloudnative, freie und programmierbare Riverbed SaaS-Lösung für Unified Observability, ermöglicht es dem gesamten IT- und Sicherheitspersonal, Probleme auf schnelle Weise zu identifizieren und zu beheben. Sie verwendet maschinelles Lernen (ML), um detaillierte Nutzererlebnis- und Netzwerk-Performance-Daten bei jeder Transaktion zu erfassen und ungewöhnliche Ereignisse zu erkennen. Dann korreliert sie die Datenströme im Kontext, um die Ereignisse mit den größten geschäftlichen Auswirkungen zu identifizieren. Diese Informationen fließen in die automatisierten Runbooks für Untersuchungen ein, welche die Fehlerbehebungs-Workflows von IT- und Sicherheitsexperten replizieren, um nützlichen Kontext zu erfassen, False-Positives auszusortieren und Prioritäten zu setzen, damit die Warnungen mit den größten geschäftlichen Auswirkungen herausgefiltert werden.

Alluvio IQ fördert die Zusammenarbeit zwischen NetOps- und SecOps-Teams, indem die aktive Suche nach gefährlichen Bedrohungen im gesamten Netzwerk mit automatisierten Sicherheitsuntersuchungen unterstützt wird. Die automatisierte Sicherheitsforensik erkennt die relevantesten Ereignisse und wendet hochanpassbare, sicherheitsspezifische Runbooks auf die Ereignisse an, die in SIEM- oder SOAR-Lösungen identifiziert wurden. SecOps-Teams erhalten die erforderlichen Netzwerkdaten für intelligente Sicherheitsuntersuchungen.

Für weitere Informationen zur automatisierten Alluvio IQ Sicherheitsforensik, klicken Sie hier.

riverbed

Riverbed – Empower the Experience

Riverbed ist das einzige Unternehmen, das über die kollektive Fülle an Telemetriedaten vom Netzwerk über die App bis hin zum Benutzer verfügt, die jede Interaktion beleuchten und dann beschleunigen, damit die Benutzer das einwandfreie digitale Erlebnis erhalten, das sie über das gesamte digitale Ökosystem hinweg erwarten. Riverbed bietet zwei branchenführende Lösungsbereiche: Alluvio by Riverbed, ein innovatives und differenziertes Unified Observability-Portfolio, das Daten, Einblicke und Aktionen in der IT vereinheitlicht, damit Kunden nahtlose digitale Erlebnisse bereitstellen können. Riverbed Acceleration hingegen bietet eine schnelle, agile und sichere Beschleunigung von Anwendungen über jedes beliebige Netzwerk (mobil, remote oder vor Ort) für alle Benutzer. Gemeinsam mit Tausenden von Partnern und marktführenden Kunden weltweit holen wir aus jedem Klick und jedem digitalen Erlebnis das Maximum heraus. Weitere Informationen auf riverbed.com/de/.