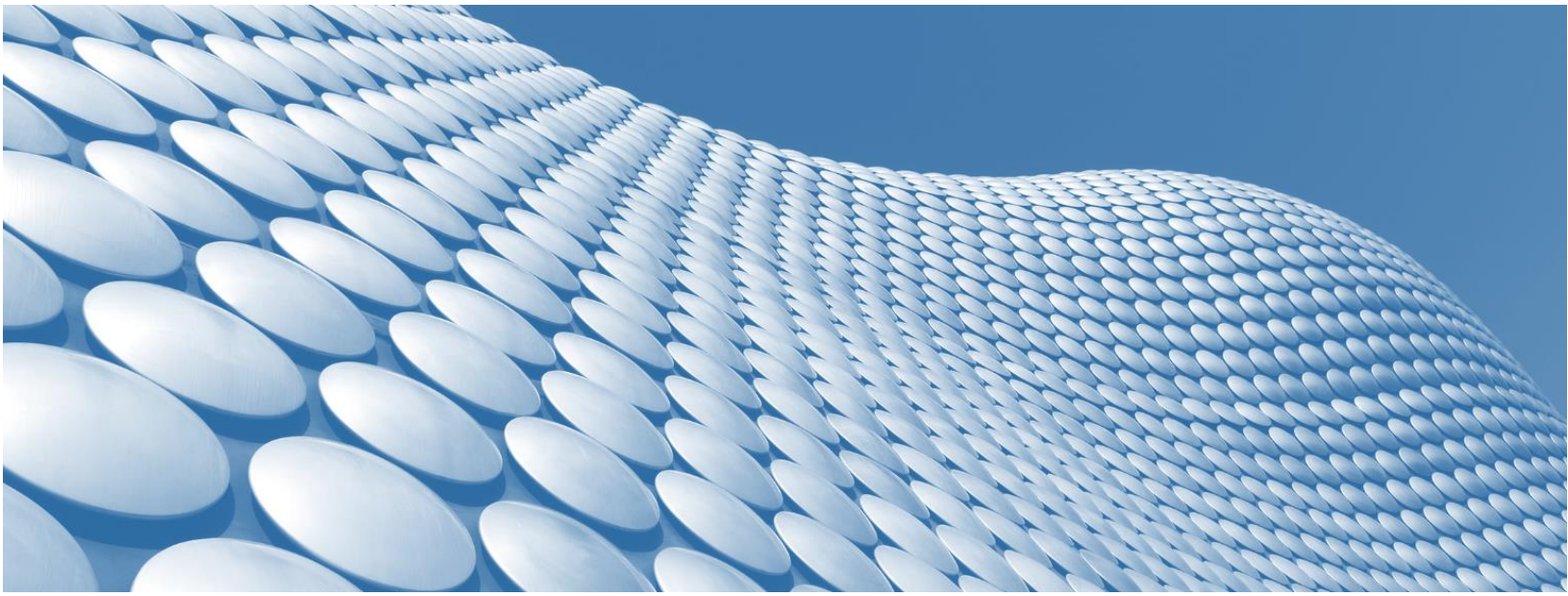

Warum Einblicke für die Sicherheit von Cloud-Anwendungen wichtig sind

Ein Intellyx-Whitepaper für LogRhythm

von Jason English Jason English, Partner & Principal Analyst

September 2023

Wenn es auf der geopolitischen Bühne nicht gelingt, einen zerstörerischen Terrorakt oder eine staatliche Aggression zu verhindern, heißt es seitens der Behörden: „Wir hatten zu dem Zeitpunkt einfach nicht genügend Informationen“.

Im Bereich der Cybersicherheit gilt dasselbe Alibi. Wenn Sicherheitsanalysten eine sich abzeichnende Cyberbedrohung nicht erkennen, wird dies häufig darauf zurückgeführt, dass nicht genügend Informationen über Ereignisse im Anwendungsbereich des Unternehmens zur Verfügung standen, um das Problem zu erfassen.

Beide Versagensszenarien haben gemeinsam, dass ein Mangel an Daten die Ursache des Problems zu sein scheint, auch wenn es viele Warnungen und Indikatoren gab, die vor der Bedrohung unbemerkt blieben.

Für Cyber-Teams in Unternehmen reicht es nicht mehr aus, einfach nur mehr Protokolldaten zu erhalten. Jetzt geht es bei der Cloud-Sicherheit darum, was man mit so vielen Daten macht.

Innerhalb von Cloud-Anwendungen, SaaS-Paketen und API-Diensten gibt es zu viele Quellen für Protokoll- und Echtzeit-Ereignisdaten, deren sinnvolle Nutzung schier unmöglich ist.

Cybersicherheitsabteilungen sind ständig unterbesetzt. Selbst bei den jüngsten Entlassungen im technischen Bereich werden qualifizierte Sicherheitsanalysten fast nie als überflüssig angesehen. Bei den meisten Unternehmen sind immer noch 40 Prozent oder mehr der offenen Stellen in diesen Gruppen unbesetzt.

Aus diesem Grund rekrutieren clevere Unternehmen Entwicklungs- und IT-Betriebsexperten als zusätzliche Akteure an vorderster Front in einem verborgenen Kampf gegen entschlossene Angreifer, die jeden Tag raffinierter werden.

In diesem Beitrag wird erörtert, wie sowohl findige Startups als auch vorausschauende Unternehmen die SecOps-Arbeit aus dem Rechenzentrum verlagern, um die Skalierbarkeit und Reichweite von cloudbasierten Plattformen für eine bessere Transparenz und einen besseren Einblick in aufkommende Bedrohungen zu nutzen.

Warum die Cloud schwer zu sichern ist

Die Umstellung auf die Cloud begann bereits vor einem Jahrzehnt, aber heute gibt es kaum noch ein Unternehmen, das nicht einen Großteil seiner Ausgaben für neue Infrastruktur in Cloud-Ressourcen investiert hat.

In der Cloud gehostete Software und Infrastruktur bietet einige integrierte Sicherheitsvorteile. So werden beispielsweise alle großen öffentlichen Cloud-Hyperscaler (AWS, Azure, GCS) von erstklassigen Sicherheitsteams unterstützt, die über gut gewartete Abgrenzungen, Netzwerküberwachung und eine Fülle von Sicherheits- und Supportservices verfügen.

Warum also ist Ransomware immer noch auf dem Vormarsch, was Reichweite, wirtschaftlichen Schaden und Schweregrad angeht – mit durchschnittlichen Kosten von 4,24 Millionen US-Dollar pro Vorfall und fast der Hälfte dieser Vorfälle in der Cloud?

Hochgradig verteilte, ephemere Architektur

Kubernetes-orchestrierte Pods und Container-basierte Workloads können in Sekundenschnelle hochgefahren werden und verschwinden ebenso schnell wieder, wenn sie freigegeben werden. Sich schnell ändernde Microservices interagieren mit Diensten von Drittanbietern und länger laufenden VMs und herkömmlichen Servern.

Selbst bei besserer Release-Automatisierung und -Orchestrierung erzeugen so viele bewegliche Teile eine Explosion von Metriken und Protokollen – eine mittelgroße Cloud-Anwendung kann täglich Hunderte von Millionen von Protokollen erzeugen.

Open Source bietet Möglichkeiten

Der Nutzen von Open-Source-Software (OSS) ist nicht zu unterschätzen. Mehr als 30 Millionen Menschen haben ihre Zeit in Open-Source-Projekte gesteckt, von Java und Linux bis hin zu Kubernetes und ChatGPT, die heute weltweit in Produktion sind. In einer Studie aus dem Jahr 2019 wird der aktuelle Wert von OSS auf mehr als 118 Milliarden US-Dollar geschätzt.

Der riskante Nebeneffekt? Kein Anbieter kann behaupten, zu 100 % für die Sicherheit verantwortlich zu sein, auch nicht bei seinen eigenen Paketdistributionen und Plattformen. Es besteht immer die Möglichkeit, dass jemand ein ungeprüftes Paket von npm heruntergeladen oder es versäumt hat, eine Sicherheitslücke zu schließen. Angreifer nutzen diese Offenheit aus, um Malware in bewährte Speicher hochzuladen und Code-Bibliotheken mit bösartigen Shell-Befehlen zu spicken.

DevSecOps erweitert das Wahrnehmungsbewusstsein des Teams.

Entwickler müssen verstehen, wie ihr eigener Code in der Cloud funktioniert. Sie haben jedoch auch einen Anreiz, sich Kenntnisse auf Betreiberebene über Cluster in der Bereitstellung, Netzwerktopologie, API-Verbindungen und sogar Sicherheit, einschließlich Geheimnisse und Berechtigungen, anzueignen.

Umgekehrt wird von IT-Ops- und Sicherheitsexperten erwartet, dass sie die Indikatoren für Probleme auf Code-Ebene und Konfigurationsprobleme aufspüren, während sie die Release- und Change-Pipeline überwachen. Für Entwicklungs-, Sicherheits- und Ops-Teams ist das Neuland, das Aufmerksamkeit und Wahrnehmungsbewusstsein erfordert.

Anforderungen an das Cloud-Wahrnehmungsbewusstsein in Echtzeit

SIEM-Tools sind seit Jahren auf dem Markt und haben sich im Security Operations Center als sehr nützlich erwiesen, aber nicht jede Rolle in der Organisation, die mit Sicherheit zu tun hat, kann sie leicht erfassen. Außerdem konzentrierten sich die vorhandenen serverseitigen Tools eher auf die Analyse der gesammelten historischen Daten als auf aktuelle ereignisbasierte Protokolle.

Größere DevSecOps-Teams benötigen Echtzeiteinsicht in die unzähligen Technologien, die Entwickler und Cloud-Betriebsteams verwenden. Daher müssen die Sicherheitsfunktionen in der Cloud angesiedelt sein und über einen SaaS-Formfaktor bereitgestellt werden, da die sichere Grenze der geschäftlichen Interaktion nicht mehr durch den Bereich eines Unternehmensrechenzentrums definiert ist. Die Anforderungen beinhalten:

Search-based threat hunting oder Scans auf der Grundlage von CVEs und dem MITRE ATT&CK®-Framework werden auch in Zukunft unverzichtbar sein, um bekannte Angriffe in Cloud- und servicebasierten Anwendungen sowie in herkömmlichen On-Premise-Anwendungen aufzuspüren.

Zero-day behavioral modeling sucht nach einzigartigen Angriffen auf Code- und Komponentenebene, die nicht den bekannten Bedrohungsketten oder Signaturen folgen. Da jederzeit neue Exploits auftauchen können, haben die Benutzer die Möglichkeit, die Absichten der Angreifer in Echtzeit zu verstehen und gleichzeitig die Live-Systemaktivität mit historischen Mustern zu vergleichen, wodurch die Erkennungszeit verkürzt wird und die Lösung schneller eingesetzt werden kann.

Event-based data collection und enrichment bedeutet, dass das Sicherheits-Dashboard so aufgebaut ist, dass es die auf der „ersten Meile" gesammelten Daten filtert, um eine direktere Sicht auf den Datenverkehr und die ereignisbasierten Daten zu erhalten, die näher an dem bereitgestellten Cloud-Service liegen, der die Anwendungssitzung des Endnutzers betreibt. Zudem werden diese Daten weiter angereichert, um sie für die Suche nützlicher und relevanter zu machen.

Multi-dimensional correlation ist unerlässlich, um Einblicke in die Ursachen von Schwachstellen und Exploits in der erweiterten Anwendungslandschaft von Cloud-Infrastrukturen und Drittanbieterdiensten zu erhalten. Analysten sollten in der Lage sein,

Suchen durchzuführen und benutzerdefinierte Alarme und Metriken zu speichern, um Daten nach Anwendung, Netzwerk, Infrastrukturkomponente, Kundentyp, geografischer Region und anderen relevanten Dimensionen zu vergleichen.

Visualisieren, um das Endspiel der Analystenerfahrung zu gewinnen

Sicherheitsteams verwenden seit langem Dashboards im Stil von „Mission Control", um das Rechenzentrum auf Systemereignisse, Metriken und Datenverkehr auf potenzielle Anomalien zu überwachen. Die Daten, mit denen wir es bei den heutigen cloudnativen Anwendungen zu tun haben, sind jedoch beispiellos – nicht nur in Bezug auf den Datenfluss und die Datenmenge, sondern auch in menschlicher Hinsicht.

Wie können wir den Sicherheitsverantwortlichen dabei helfen, die vielen Cloud-Daten sinnvoll zu nutzen und nicht nur schönere Berichte und Diagramme in Dashboards zu erstellen?

Bei der ***Datenvisualisierung*** geht es um den Entwurf und die Entwicklung einer Mensch-Computer-Schnittstelle (oder eines Sicherheits-Dashboards), die eine bessere menschliche Wahrnehmung und Analyse von Daten in Live-Datenströmen und archivierten Daten ermöglicht.

Hier erfahren Sie, wie die Datenvisualisierung dazu beiträgt, erfolgreiche Ergebnisse für Cloud-Sicherheitsteams zu erzielen

Verringerung der kognitiven Belastung, wenn Analysten Überwachungs-, Bedrohungserkennungs- und Abhilfemaßnahmen durchführen. Sicherheitsexperten sollten auf einen Blick in der Lage sein, Entwarnung zu geben oder Hotspots zu erkennen. Ein effektives Dashboard kombiniert mehrere Datendimensionen in gemeinsamen Grafiken und folgt einer konsistenten Kennzeichnungssemantik von Metadaten sowie nonverbalen Design- und Farbhinweisen.

Beseitigung von Ablenkungen bei der Suche nach Bedrohungen und bei Abhilfemaßnahmen durch richtlinienbasiertes Filtern eingehender Daten und Metadaten sowie durch AIOps-ähnliche Reduzierung der potenziellen Warnmeldungen auf dem Bildschirm. Analysten sollten in der Lage sein, die wichtigsten Indikatoren zu finden, ohne Code oder komplizierte SQL-Abfragen schreiben zu müssen.

Kontextabhängige benutzerdefinierte Ansichten ermöglichen Teams und Einzelpersonen den Zugriff auf Echtzeit- und historische Daten für die richtigen Bereiche und auf der richtigen Lösungsebene für ihre Bedürfnisse. Auf Richtlinien basierende Zugriffsberechtigungen erleichtern die Zusammenarbeit von Teams bei der Lösung gemeinsamer Probleme, während sensible Bereiche speziellen Gruppen oder Einzelpersonen vorbehalten werden.

Das angestrebte Endergebnis ist eine **verbesserte Analystenerfahrung**. Durch die Verringerung unnötiger Arbeit und die Erhöhung der Erfolgsquote bei jeder Bedrohungslösung bleiben Mitarbeiter motoviert und dem Team erhalten. Vorgesetzte wandern seltener aus Burnout-bedingten Gründen ab.

Lösen mit Einsicht mit LogRhythm Axon

Vor kurzem haben wir die neue Plattform für Sicherheitsoperationen von **LogRhythm Axon** getestet, eine vollständig für die Cloud konzipierte SaaS-Lösung, die die weit verbreitete SIEM-Plattform des Unternehmens, die in SoC-Centern läuft, sowie die neueren UEBA- und NDR-Dienste ergänzt. Alle sind in der Lage, zusätzliche Datenquellen darzustellen.

Die Lösung ist auf einer Microservices-Architektur aufgebaut und nutzt native Cloud-to-Cloud-Kollektoren, um Daten von SaaS-Anwendungen und öffentlichen Cloud-Hyperscalern (AWS, Azure, GCP usw.) zu sammeln sowie Protokolle und Warnmeldungen von einer Vielzahl von On-Premise- oder Remote-Agenten zu empfangen.

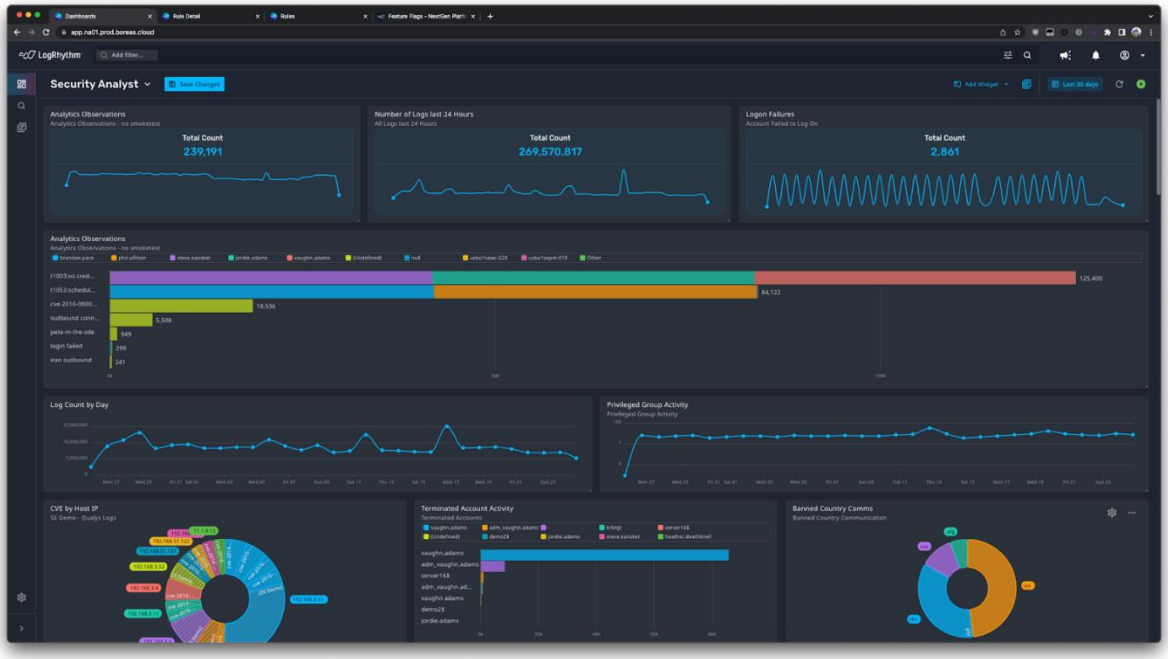

Abbildung 1: Das Dashboard der Sicherheitsbetriebsplattform von LogRhythm

In gewisser Weise könnte ein Analyst beim ersten Anblick eines Axon-Dashboards denken, dass es wie eine beliebige Anzahl von grafischen System- und Netzwerküberwachungs-Tools aussieht, die schon seit Jahren auf SecOps-Bildschirmen laufen, wenn auch in modernerer Aufmachung.

Ein genauerer Blick auf die fortlaufenden Diagramme und Indikatoren macht jedoch deutlich, dass der Analyst hier nicht einfach nur eine historische Trendanalyse durchführt. Die Benutzer verwenden größtenteils kontinuierliche Ereignisse oder „heiße" Daten, da sie ihre eigenen Suchabfragen per Mausklick erstellen, die dann aktive Protokolle von allen möglichen verteilten Systemen und Diensten abrufen und filtern, einschließlich anderer Sicherheitstools, Streaming-Daten, API-Nachrichten, E-Mails und mehr.

Axon behandelt diese aktiven Bedrohungssuchen als Komponenten-Widgets, die angepasst und auf der Dashboard-Oberfläche platziert werden können. Analysten können die Widgets modifizieren, indem sie eine beliebige Dimension der darin dargestellten Daten oder Metadaten ändern, anstatt den Abfragecode zu schreiben oder zu ändern (obwohl ein Experte auch darauf zugreifen kann). Im Hintergrund der Schnittstelle können Analysten über ein Diagramm oder eine Warnung weiterhin relevante Protokolle einsehen.

Ein Widget könnte beispielsweise eine Baumansicht der wahrscheinlichen Ransomware-Angriffsversuche für die Cloud-Anwendungen einer bestimmten Geschäftseinheit und alle damit verbundenen Ressourcen und Dienste enthalten. Eine globale Version dieses Widgets könnte an andere Teams im Unternehmen weitergegeben werden, während eine regionale Version für den Analysten privat gehalten werden könnte, um solche Angriffe in der eigenen Region zu erkennen.

Widgets können zu einer Dashboard-Ansicht kombiniert werden, die auch neu gemischt oder mit anderen Nutzern geteilt werden kann.

Im Hintergrund bietet Axon Funktionen im Stil von AI Ops, um die Erkennung von Bedrohungen und die Lösungszeit weiter zu beschleunigen. Der Policy Builder analysiert und kennzeichnet eingehende Daten mit Metadaten über Hunderte von Dimensionen gemäß der bevorzugten Ontologie des Unternehmens. Observation Clustering automatisiert die Korrelation von Protokollanalysedaten weiter, sodass Analysten Bedrohungen aus verschiedenen Protokollen und Protokolldatenströmen schneller gruppieren und aufdecken können

Die Intellyx-Einschätzung

Daten zur Sicherheit von cloudnativen Anwendungen kommen schnell auf Sie zu.

Die Geschwindigkeit so vieler Veränderungen zu bewältigen, indem man Milliarden von Protokollen in ein ständig wachsendes Cloud-Data-Warehouse einspeist und dann historische Daten ohne klaren Kontext und Visualisierung manuell durchsucht, ist für die modernen Anwendungen von heute nicht zielführend. Es wird Sicherheitsanalysten nur dazu zwingen, noch mehr Nadeln in noch mehr Heuhaufen zu suchen und wahrscheinlich aus Frustration einen anderen Arbeitsplatz zu suchen.

Die ideale Analystenerfahrung lässt die schwierigen Probleme der cloudnativen Sicherheit für den Sicherheitsanalysten einfach aussehen – und auch für andere Beteiligte wie Entwickler, Betreiber, verbundene Partner und sogar Kunden, die aus Gründen der Compliance und des Risikos zur Teilnahme an Sicherheitsübungen aufgefordert werden.

Über den Autor

Jason "JE" English (@bluefug) ist Partner & Principal Analyst bei Intellyx,, einem Analyseunternehmen, das sich mit der digitalen Transformation befasst. Er schreibt darüber, wie die agile Zusammenarbeit zwischen Kunden, Partnern und Mitarbeitern Innovationen beschleunigen kann.

Neben verschiedenen Führungspositionen in Unternehmen in den Bereichen Lieferkette, Interaktivität, Spiele und Cloud Computing leitete Jason das Marketing für das Entwicklungs-, Test- und Virtualisierungssoftwareunternehmen ITKO, von den Anfängen bis zur erfolgreichen Übernahme durch CA im Jahr 2011. JE ist Co-Autor des Buches Service Virtualization: Reality is Overrated (Service-Virtualisierung: Die Realität wird überbewertet), um die damals neuartige Praxis der Simulation von Testumgebungen für die agile Entwicklung zu beschreiben.

Über LogRhythm

LogRhythm hilft Sicherheitsteams, Sicherheitsverletzungen zu stoppen, indem es unzusammenhängende Daten und Signale in vertrauenswürdige Erkenntnisse umwandelt. Von der Verknüpfung verschiedener Protokoll- und Bedrohungsdatenquellen bis hin zu hochentwickeltem maschinellem Lernen, das verdächtige Anomalien im Netzwerkverkehr und im Benutzerverhalten erkennt, macht LogRhythm Cyberbedrohungen genau ausfindig und versetzt Fachleute in die Lage, schnell und effizient zu reagieren.

Mit der Flexibilität von cloudnativen und selbst gehosteten Implementierungen, sofort einsetzbaren Integrationen und Beratungsdiensten ist es mit LogRhythm einfach, schnell Werte zu realisieren und sich an eine sich ständig verändernde Bedrohungslandschaft anzupassen. Gemeinsam können LogRhythm und unsere Kunden Cyberangriffe zuverlässig überwachen, erkennen, untersuchen und darauf reagieren.

Weitere Informationen zu den Angeboten von LogRhythm finden Sie unter: https://logrhythm.com.

©2023 Intellyx LLC. Die redaktionelle Verantwortung für dieses Dokument liegt bei Intellyx. Es wurden keine KI-Bots verwendet, um diesen Inhalt zu schreiben. Zum Zeitpunkt der Erstellung dieses Artikels ist LogRhythm ein Kunde von Intellyx. Bildquellen: iStock, Adobe Stock (lizenziert durch LogRhythm); Screenshot: LogRhythm Axon-Dashboard