Getting in the security flow with LogRhythm Axon

Improving security analyst and SOC team experience through event visibility and streamlined data workflows

An Intellyx Whitepaper for LogRhythm
by Jason English, Partner & Principal Analyst
December 2023

When we describe a developer who is moving quickly because they are in a creative moment of total understanding and control, we say they are 'in the flow.'

We seldom use the same concept of 'flow' to describe the work of security analysts and teams. We expect SecOps professionals to be thorough and efficient, of course, but maybe that's not helping us retain the creative talent that will produce long-term improvements in protecting our application estates.

Visibility and automation must go hand-in-hand to reduce the cognitive load and fruitless toil of sorting through event logs from hybrid cloud application environments, so security analysts can experience a 'state of flow' and discover new ways to eliminate risk.

Within cloud deployments, SaaS packages and API services, there are too many sources of logging and real-time event data coming in for mere mortals to make sense of it all.

Cybersecurity groups are eternally understaffed. Even with some recent tech layoffs, skilled security analysts are almost never considered redundant, and most companies still have 40 percent or more of their open positions in these groups unfilled.

That's why savvy companies are recruiting development and IT operations professionals as additional front line agents in a clandestine battle against determined attackers that get more sophisticated every day.

This paper will discuss how both scrappy startups and forward-thinking enterprises can leverage the scalability and reach of a cloud-based SIEM platform for better visibility and insight, while rule-based policies and automation can reduce analyst complexity so SecOps teams can stay 'in the flow' to reduce and remediate security flaws more quickly and effectively.

Challenges of securing cloud architecture

Companies started moving to cloud in earnest a decade ago, but now, it would be hard to find a company that hasn't invested most of its new infrastructure spend on cloud resources.

Cloud-hosted software and infrastructure comes with some built-in security advantages. For instance, all of the major public cloud hyperscalers (AWS, Azure, GCS) are backed up by top-notch security teams, with well-maintained perimeter fencing, network monitoring, and a wealth of available security and support services.

So why is ransomware still on the rise, in terms of reach, economic damage, and severity – with an average cost per breach of $4.24M and almost half of those breaches occurring in the cloud?

Highly distributed, ephemeral architecture

Kubernetes-orchestrated pods and container-based workloads can spin up in subseconds, and disappear just as quickly when released. Fast-changing microservices interact with third-party services and longer-running VMs and conventional servers.

Even with better release automation and orchestration, so many moving parts generate an explosion of metrics and logs—a mid-sized cloud application could generate hundreds of millions of logs a day, which presents a massive data load for SecOps teams to filter through.

Open source provides openings

We cannot underestimate the benefits of open source software (OSS). More than 30 million individuals have contributed time toward open source projects—from Java and Linux to Kubernetes and ChatGPT that are now in production around the world – a 2019 paper estimated the current value of OSS at more than $118 billion.

The risky side effect? No vendor can claim to be 100% responsible for security, even with their own packaged distributions and platforms. There's always a chance someone downloaded an unchecked package from npm, or failed to patch a vulnerability. Attackers take advantage of this openness to upload malware to well-trodden repos, and spike code libraries with rogue shell commands.

Insider threats are common

What do you do if a security problem is caused by someone within the organization? Bad results are often caused by employees with credentials—comprising as much as 60% of threats according to many reports. An employee may be compromised through dissatisfaction or financial motives of course, but even more often, malware package downloads and data exposures are caused by the inadvertent mistakes of employees who lack security awareness and education.

DevSecOps extends team awareness

Developers need to understand how their own code works in the cloud, but they are further incentivized to gain operator-level knowledge of clusters in deployment, network topology, API connections and even security, including secrets and permissions.

Conversely, IT Ops and security professionals are expected to sniff out the indicators of code-level problems and configuration issues, while watching the release and change pipeline. We're asking Dev, Sec and Ops teams to protect uncharted territory for putting attention and awareness at a premium.

Requirements for getting analysts in the flow

SIEM tools have been on the market for years, and proven very useful in the security operations center, but not every role in the org that has a hand in security can easily grasp them. Further, existing server-side tools tended to focus more on the analysis of collected historical data rather than current event-based logs.

Extended DevSecOps teams need help understanding where to focus their attention to address the most critical risks, with real-time visibility into the myriad of technologies developers and cloud operations teams are using. Therefore, the security workflow should reside in the cloud and be delivered through a SaaS form factor, since the secure edge of business interaction is no longer defined by the perimeter of a corporate data center. Requirements include:

A common event ontology that replaces the need to look up logIDs and unique event codes, enriching data with meaningful metadata identifiers for customer accounts, activity or alert types, services, regions and so on. Even if events come in from an as-yet-unattributed cloud source, business-aware queries and rules should be able to understand the data context.

Search-based threat hunting and scans based on threat behavior profiles and targeted security policies. Of course, CVEs and the MITRE ATT&CK® framework will define key starting points for classifying known attacks in cloud and service-based applications, as well as within the conventional on-prem application estate.

Zero-day behavioral modeling looks for unique code and component level attacks that don't follow known threat chains or signatures. New exploits can appear at any time. Giving users the ability to understand attacker intent in real-time, while comparing live system activity to historical patterns, reduces recognition time so resolution can start faster.

Event-based data collection and enrichment, filtering data collected at the 'first mile' for a more direct view of traffic and event-based data closer to the deployed cloud service that powers the end user's application session. This data is further enriched with a common ontology to make it more useful and relevant for searches and workflow.

Multi-dimensional correlation is essential for gaining insight into the root cause of vulnerabilities and exploits across the extended application estate of cloud infrastructure and third-party services. Analysts should be able to conduct searches and save custom-defined alerts and metrics to compare data by application, network, infrastructure component, customer type, geographic region, and any other relevant dimensions.

Staying in the flow with visualization and automation

As security is a continuous process, teams have long used 'mission control' style dashboards to monitor system events, metrics and traffic for potential anomalies. However, we're grappling with an unprecedented amount of data in today's cloud-native applications, not just in terms of flow and quantity—but from a human factors perspective.

How can we help security stakeholders maintain flow, and make sense of so much cloud data?

- **Data visualization** involves designing and engineering a human-computer interface (or security dashboard) to allow better human cognition and analysis of data atop live data streams and archived data. At a glance, security professionals should be able to get an all-clear signal or notice hotspots. An effective dashboard combines multiple data dimensions into common graphics, and follows consistent metadata labeling semantics and non-verbal design and color cues.
- **Rules-based behavioral mapping** of data to common events so analysts can see when particular threat chains are in play. For instance, mapping can be used to identify if the same credentials are used from two different cities in a short time interval that would be improbable for humans to travel, or if a particular MITRE ATT&CK scenario variation is being played out.
- **Remove distractions** from threat hunting and remediation workflows through policy-based filtering of incoming data, metadata, and AIOps-style reduction of the storm of potential alerts presented on screen. Analysts should be able to get to the most relevant indicators without having to write code or complicated queries.
- **Contextualized custom views** allow teams and individuals to access real-time and historical data for the right domains, and at the right level of resolution for their needs.

Improved analyst experience is the end result we're looking for—reducing useless toil and increasing success ratios on each threat resolution exercise. Valuable team members are retained with higher morale, and managers suffer less burnout-related attrition.

Solving with insight using LogRhythm Axon

We recently reviewed **LogRhythm Axon**, a built-for-cloud SaaS SIEM platform running in SOC centers alongside UEBA and NDR services—all of which can be additional sources of data.

The solution was built on a microservices architecture and leverages native cloud-to-cloud collectors to collect from SaaS applications and public cloud hyperscalers (AWS, Azure, GCP, etc.), as well as receiving logs and alerts from a host of on-prem or remote agents.

Figure 1. The LogRhythm Axon cloud SIEM platform dashboard.

Upon first seeing a LogRhythm Axon dashboard, an analyst might think it looks like any number of graphical system and network monitoring tools that have been running on SecOps screens for years, albeit designed to more modern aesthetics.

Users are largely watching the passage of continuous events within the customizable widgets of the dashboard, which is summarizing millions or even billions of logs flowing through the system over the past hours, days, or months so they can drill into anomalies for any time frame. However, a closer look behind the ongoing graphs and indicators makes it clear the analyst isn't simply monitoring metrics or historical trends here.

Through an **Analytics Rule Builder** feature, they can build their own declarative rules in a point-and-click fashion from common events or leverage a library of dozens of relevant scenarios to match known CVEs and suspicious attack patterns such as a DDoS, or an attack spray.

Rather than writing queries in regex statements, the analyst can enter plain text queries or point and click on the common event parameters to refine analytics rules as they work to hunt threats or resolve active cases.

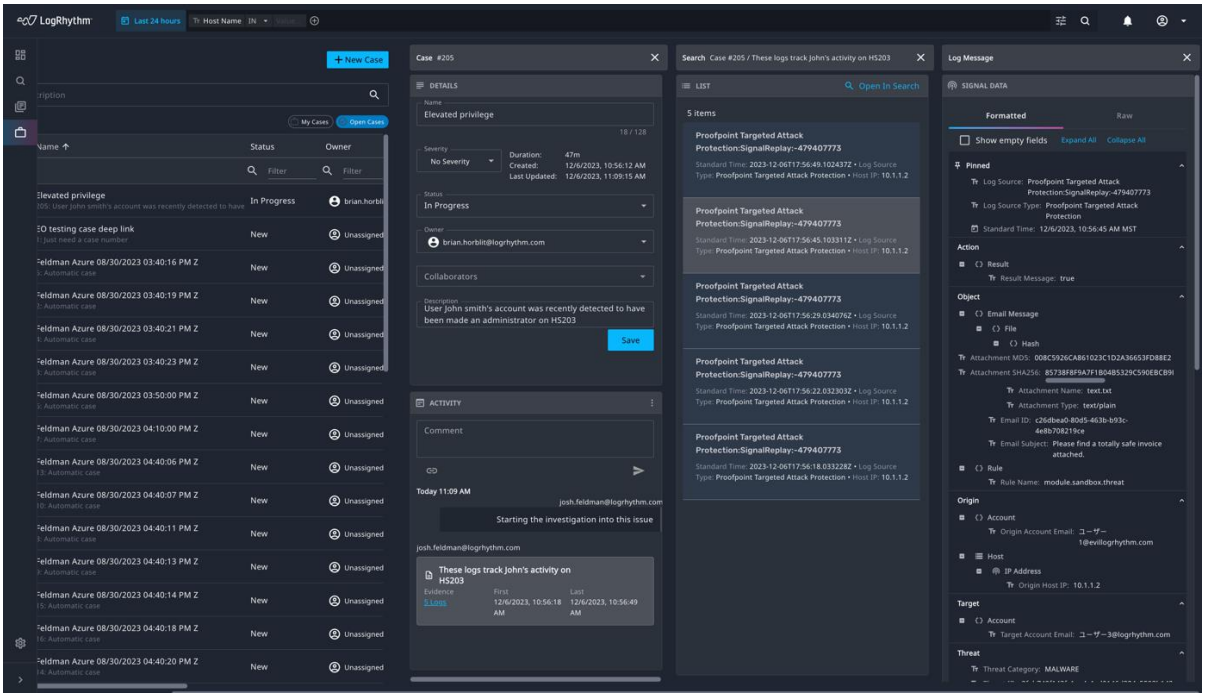

Figure 2.. Case Management view in LogRhythm Axon.

The **Case Management** feature allows analysts to act on a work queue that prioritizes the most critical and recently discovered threats. When analysts are in the flow, they can contribute new activities, rules, and remediation actions to the case, so future analysts can avoid duplicate work.

Behind the scenes, analysts can still drill down into relevant logs underneath each case.

The Intellyx Take

Cloud-native application security data comes at us fast—just like life.

Dealing with the velocity of so much change by dumping billions of logs into an ever-expanding cloud data warehouse, then manually searching historical data without rule-based context and visualization won't get the job done for today's modern applications. It will only force security analysts to seek more needles in more haystacks, and likely seek employment elsewhere out of frustration.

The ideal analyst experience makes the hard problems of cloud-native security look easy for the security analyst—as well as for other stakeholders like developers, operators, connected partners and even customers who are being asked to participate in security exercises for their own compliance and risk reasons.

About the Author

Jason "JE" English (@bluefug) is a Partner & Principal Analyst at Intellyx, a boutique analyst firm covering digital transformation. His writing is focused on how agile collaboration between customers, partners and employees can accelerate innovation.

In addition to several leadership roles in supply chain, interactive, gaming and cloud computing companies, Jason led marketing efforts for the development, testing and virtualization software company ITKO, from its bootstrap startup days, through a successful acquisition by CA in 2011. JE co-authored the book Service Virtualization: Reality is Overrated to capture the then-novel practice of test environment simulation for Agile development.

About LogRhythm

LogRhythm helps security teams stop breaches by turning disconnected data and signals into trustworthy insights. From connecting the dots across diverse log and threat intelligence sources to using sophisticated machine learning that spots suspicious anomalies in network traffic and user behavior, LogRhythm accurately pinpoints cyberthreats and empowers professionals to respond with speed and efficiency.

With cloud-native and self-hosted deployment flexibility, out-of-the-box integrations, and advisory services, LogRhythm makes it easy to realize value quickly and adapt to an ever-evolving threat landscape. Together, LogRhythm and our customers confidently monitor, detect, investigate, and respond to cyberattacks.

To learn more about LogRhythm's offerings, please visit: https://logrhythm.com.