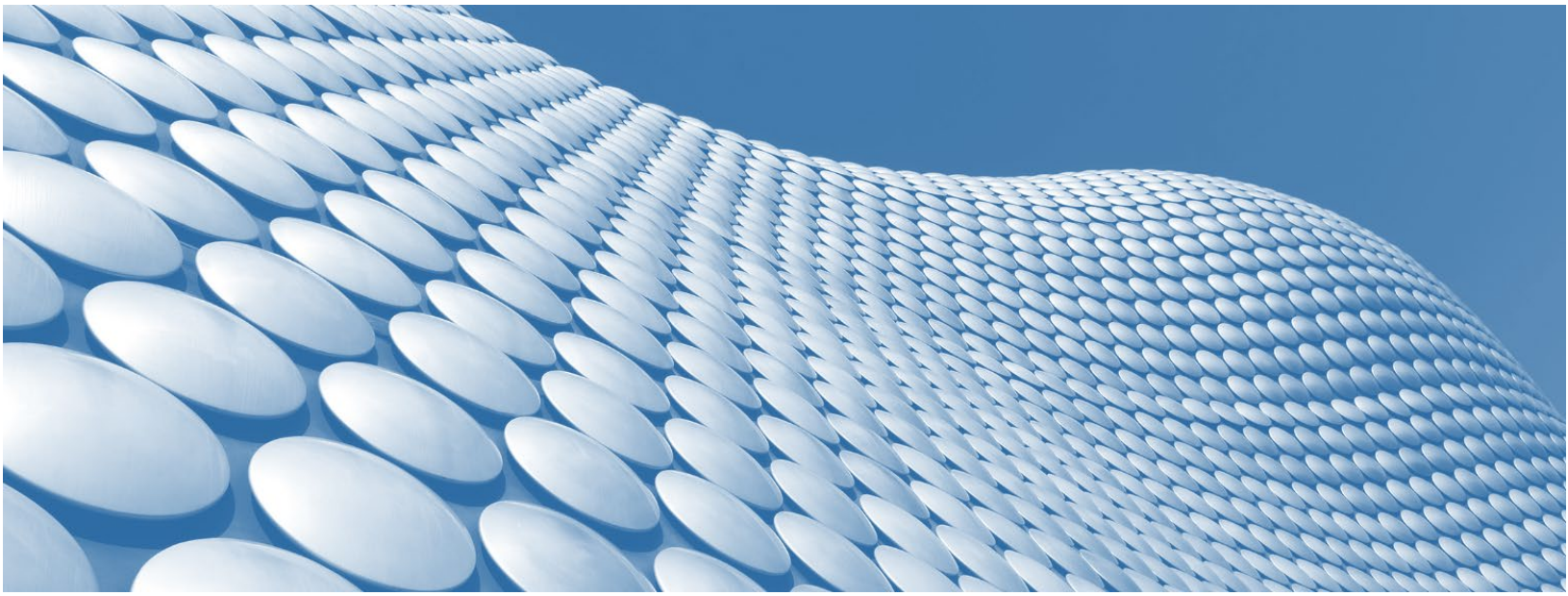

Why Insight Matters for Cloud Application Security

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

On the geopolitical stage, whenever there's a major failure to prevent a destructive act of terrorism or state aggression, government agencies and officials will say 'we just didn't have good enough intelligence at the time.'

In cybersecurity arenas, that same alibi is applied. When security analysts fail to spot an emerging cyber threat, it is often chalked up to not having enough intelligence about what is going on inside the company's application estate to gain awareness of the problem.

Both failure scenarios have a common thread, in that a lack of data is seemingly the source of the problem, even when there were plenty of warnings and indicators that went unnoticed ahead of the threat.

For enterprise cyber teams, just getting more log data is no longer enough. Now the cloud security frontier is about what you do with so much data.

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 are moving SecOps work out of the datacenter to leverage the scalability and reach of cloud-based platforms for better visibility and insight into emerging threats.

Why the cloud frontier is hard to secure

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.

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.

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 in uncharted territory for Dev, Sec and Ops teams, putting attention and awareness at a premium.

Requirements for real-time cloud awareness

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 than current event-based logs.

Extended DevSecOps teams need real-time visibility into the myriad of technologies developers and cloud operations teams are using. Therefore, security capabilities must 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:

Search-based threat hunting or scans based on CVEs and the MITRE ATT&CK® framework will remain essential for spotting 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. Since 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 means the security dashboard is built for 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, and this data is further enriched to make it more useful and relevant for searches.

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.

Visualize to win the analyst experience endgame

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

How can we help security stakeholders make sense of so much cloud data, beyond simply designing nicer-looking reports and graphs in dashboards?

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.

Here's how data visualization helps drive successful outcomes for cloud security teams:

Reducing cognitive load when analysts conduct monitoring, threat detection and remediation activities. 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.

Removing 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 SQL 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. Policy-based access permissions make it easier for teams to collaborate on resolving shared problems, while cordoning off sensitive issues to specialized groups or individuals.

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

Solving with insight using LogRhythm Axon

We recently reviewed the new **LogRhythm Axon** security operations platform, a completely built-for-cloud SaaS solution that complements the firm's widely adopted SIEM platform running in SoC centers and their more recent UEBA and NDR services—all of which could 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.

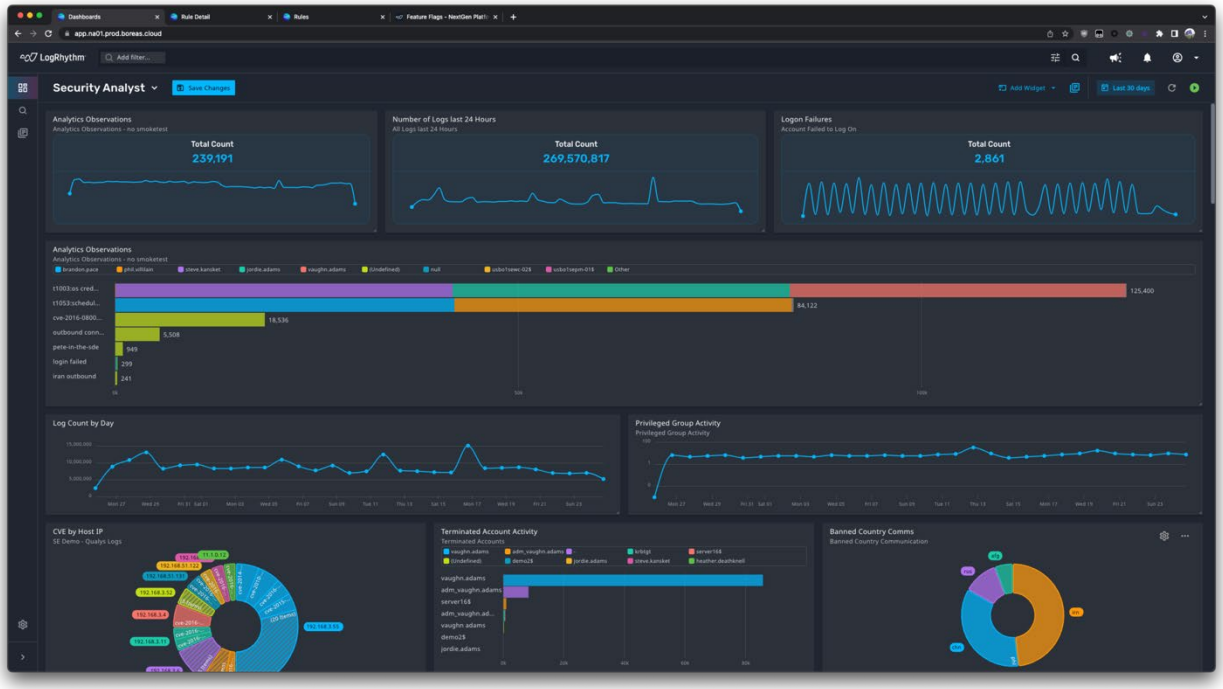

Figure 1. The LogRhythm Axon security operations platform dashboard.

In some ways, upon first seeing an 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.

However, a closer look at the ongoing graphs and indicators makes it clearer the analyst isn't simply doing historical trending here. Users are largely playing with continuous events, or 'hot' data, as they design their own search queries in a point-and-click fashion,

which are then pulling and filtering active logs from all kinds of distributed systems and services, including other security tools, streaming data, API messages, emails, and more.

Axon treats these active threat searches as component 'widgets' that can be customized and placed on the dashboard interface. Analysts can modify the widgets by changing any dimension of data or metadata represented within them, rather than writing or changing query code (though an expert can still access that). Behind the scenes of the interface, analysts can still drill down into relevant logs through a graph or alert.

For instance, a widget may contain a treemap view of likely ransomware attack attempts, for a particular business unit's cloud applications and all of its connected resources and services. A global version of this widget could be shared with other teams across the organization, while a regional version could be kept private for the use of the analyst to spot such attacks in their own geography.

Widgets can be combined into a dashboard view, which can also be remixed or shared with peers.

Behind the scenes, Axon includes AI Ops-style features to further accelerate threat recognition and resolution time. Policy Builder parses and tags incoming data with metadata across hundreds of dimensions according to the organization's preferred ontology. Observation clustering further automates the correlation of log analytics data so analysts can more quickly group and surface threats from several different logs and log data streams.

The Intellyx Take

Cloud-native application security data comes at you 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 clear 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.