Stream.Security

Enhancing SIEM with Real-Time Cloud Context

Security Information and Event Management (SIEM) platforms are essential for aggregating and analyzing logs from diverse environments, including on-premises infrastructure, cloud platforms, and SaaS applications. However, SIEMs often struggle to interpret the complexity of cloud-native attacks due to the intricate nature of cloud identities, configurations, and networks.

Stream Security dynamically models the cloud environment in real time, creating a comprehensive map of all cloud activities, configurations, and dependencies. This enables Stream to trace the impact of all activity whether it's a configuration change, identity shift, or network event — and understand how it affects the broader cloud environment. By analyzing these real-time insights, Stream reveals the true context behind each activity, helping security teams detect threats more accurately and respond faster.

Stream Security enhances SIEM capabilities by providing real-time cloud insights, enriching raw logs with actionable context, and correlating events across cloud layers to reveal the full attack storyline — transforming fragmented data into a clear, actionable picture.

With Stream, security teams no longer need to maintain detection rules manually in the SIEM. Stream continuously adapts to cloud changes and applies real-time detection rules, ensuring that threat detection remains accurate and up to date without requiring constant rule updates.

Stream allows security teams to send all their cloud logs directly to Stream instead of forwarding them to the SIEM. This reduces log ingestion volume and associated costs, allowing SIEM to focus on enriched, high-value alerts rather than processing raw cloud data.

Gartner COOL VENDOR



How Stream.Security Improves SIEM Alerts

Suspicious Login from a New Location

- Without Stream: SIEM logs an alert for a login from an unusual IP address. The alert has no information on user permissions and access to critical resources in the cloud.
- With Stream: Using cloud context, Stream identifies that the user in question assumed an overprivileged role and accessed a sensitive S3 bucket post-login from the unusual IP address, providing full context on potential privilege escalation.

Failed API Calls

- Without Stream: SIEM logs an alert for a login from an unusual IP address. The alert has no information on user permissions and access to critical resources in the cloud.
- With Stream: Using cloud context, Stream identifies that the user in question assumed an overprivileged role and accessed a sensitive S3 bucket post-login from the unusual IP address, providing full context on potential privilege escalation.

Excessive Data Transfe

- Without Stream: SIEM logs high data transfer rates but cannot determine if the transfer is malicious or routine.
- With Stream: Stream correlates the transfer with an IAM role change and recent misconfiguration, identifying it as an exfiltration attempt.

Configuration Change in Cloud Firewall

- Without Stream: SIEM detects a change to cloud firewall rules but cannot assess the security impact – i.e., which assets are now exposed and what the risk of having them exposed is.
- With Stream: Stream shows that the new configuration exposes a sensitive workload with PII to the internet, identifying the risk of lateral movement.



How Stream Security and SIEM Work Together



Real-Time Event Enrichment

Stream enriches SIEM events with cloud-layer insights, including identity misuse, misconfigurations, and network anomalies, transforming raw data into actionable intelligence.



Full Attack Storyline

By correlating cloud activity, Stream enables the SIEM to present a unified attack view, helping security teams understand the full scope and impact.

Reduced Noise, Increased Clarity

Stream filters out false positives and low-priority events, ensuring that SIEM alerts are accurate and high-fidelity.



8

Accelerated Response

With enriched context and clear attack progression, SOC teams can triage and respond to threats faster and more effectively.



Lower SIEM Costs

By sending cloud logs directly to Stream instead of the SIEM, organizations reduce log ingestion volume and associated costs while improving detection quality.

Better Together: Real-Time Cloud Context for Your SIEM

Organizations gain a powerful, unified defense system by combining Stream Security's real-time cloud modeling with SIEM's centralized log management. This ensures that:

- SIEM alerts are enriched with cloud-specific context to reduce investigation time.
- Security teams can detect and respond to threats faster with a clear understanding of attack progression.
- Noise is reduced, and high-fidelity alerts allow SOC teams to focus on real threats.
- SIEM costs are lowered by reducing log ingestion volume and focusing on high-quality, enriched data.



CSA

Interested in learning more about how Stream can complement your SIEM with cloud context? Meet with one of our cloud experts today.

Stream.Security