

Intezer Unveils Integrations with Leading Cloud Companies to Deliver Cloud Security Alert Triage and Investigation

NEW YORK, NY, UNITED STATES, April 28, 2025 /EINPresswire.com/ -- Intezer, the leader in AI SOC solutions, today announced a major expansion of its [Autonomous SOC Platform](#), enabling security teams to triage and investigate alerts from leading cloud providers and security vendors, including AWS, Microsoft Azure, Google Cloud, Wiz, Lacework, FortiCNAPP, Upwind, and Sweet Security.



INTEZER

Intezer - Leave the SOC grunt work to technology. Keep noise, false positives, and alerts from overwhelming your security team.

SOC teams are overwhelmed by the increasing volume of cloud security alerts. A [recent study](#) found that cloud security alerts increased by 388% over the past year. Intezer's new integrations directly address this challenge by automating the investigation, triage, and response to an array of cloud alerts, including suspicious network connections, runtime threats, and risky administrative activities.

"Our customers tell us that cloud alerts dramatically increase the workload for their SOC teams. Given our mission to make life easier for security operations, this is a much needed addition to our Autonomous SOC Platform," said Itai Tevet, CEO and co-founder of Intezer.

"Malicious attackers are using AI tools to scale their attacks, making it harder for security teams to keep up with the sheer volume of incoming security alerts," Tevet added. "This noise is playing to the adversaries' advantage. They no longer need to worry about evading detection; they simply have to take actions that register as low-severity alerts, and then they'll likely be ignored until it's too late."

In addition to dealing with an ever-increasing volume of cloud security alerts, SOC teams often lack the same intimate expertise with the cloud as they do with firewalls and endpoint security solutions. This can make it challenging for them to understand and determine the severity of the cloud security alerts they receive. Intezer is able to ingest, autonomously triage, investigate, and deliver escalated alerts in a format that SOC teams can better understand.

"Right now, Intezer's SIEM API ingests our cloud alerts, which have been really helpful for us because cloud alerts make up over a quarter of our security alerts," said Zach Walker, director of security operations at Legato Security. "That being said, we look forward to these direct integrations with tools like Wiz and AWS because they will allow for faster remediation and further reduce our MTTR."

Additional key capabilities and benefits of Intezer's cloud alert triage and investigation include:

- Automated Alert Triage and Evidence Collection: Seamlessly gather logs, files, and forensic artifacts across diverse cloud workloads.
- Intelligent Alert Correlation and Prioritization: Intelligently correlates alerts from various cloud environments, reducing false positives so security teams can focus on critical threats.
- Autonomous Response and Containment: Auto-resolves false-positive alerts so the security team only receives critical alerts requiring their attention. Security policies are enforced with automated mitigation actions, and threats are responded to in near real-time.

"Upwind gives security teams the real-time context they need to act fast — across cloud workloads, applications, and identities," said Joshua Burgin, Chief Product Officer at Upwind. "This integration with Intezer's Autonomous SOC Platform helps customers cut through the noise, accelerate investigations, and respond to real threats before they escalate."

To learn more about how Intezer helps security teams manage the ever-growing number of security alerts, including those from cloud providers and vendors, visit [this page](#).

Intezer will exhibit at booth 2446 in Moscone South at the RSAC 2025 Conference in San Francisco from April 28 to May 1. [Visit their booth](#) to learn more about automated cloud alert triage and investigation with Intezer.

About Intezer

Intezer is a leading provider of AI-powered technology for autonomous security operations, with a vision to solve talent shortages and skill gaps in the cybersecurity industry. Intezer built the Autonomous SOC Platform to investigate alerts, make triage decisions, and escalate findings about serious threats like an expert SOC analyst (but without burnout, skill gaps, and alert fatigue). Learn more at www.intezer.com.

Mackenzie Kreitler

Intezer

[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/806730235>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2025 Newsmatics Inc. All Right Reserved.