# Intezer Expands AI SOC Offering to Support Identity-Based Alert Triage

*New Integrations with Microsoft Entra ID and Okta Enable Smarter Identity Threat Detection with Context-Aware Security*

Intezer - Extend Your Security Team with AI

NEW YORK, NY, UNITED STATES, March 4, 2025 /EINPresswire.com/ -- Intezer, the leader in AI-powered technology for autonomous security operations, today announced a major update to its AI SOC platform to autonomously triage and investigate identity-based threats with the precision and expertise of a seasoned SOC analyst.

Identity-related alerts, which include suspicious logins, impossible travel, and anomalous access attempts, require in-depth manual investigation, consuming valuable analyst time and slowing response rates. These delays increase mean time to respond (MTTR) and drain resources, leaving organizations vulnerable to threats. With IBM reporting a 71% year-over-year increase in cyberattacks leveraging stolen or compromised credentials, rapid and accurate identity threat response has become more important than ever.

Intezer's AI SOC platform now integrates with top identity providers like Microsoft Entra ID and Okta to autonomously triage identity alerts. By combining smart queries, contextual data enrichment, and AI-driven decisions, the platform replicates the investigative approach of a human analyst, dramatically improving accuracy and drastically cutting response times.

Key capabilities of Intezer's identity-based alert triage:
- Smart Queries Against IDP Data: Automatically enriches alerts with user activity logs, domain permissions, and suspicious patterns directly from identity providers.
- Autonomous Decision-Making: Analyzes the entire alert and its enriched data, correlates with similar activity, and leverages threat intelligence to distinguish legitimate access (i.e. enterprise VPNs) from malicious intent.
- Automated User Feedback Requests: Proactively contacts users, managers, or security teams via email, Slack, or other channels to validate activity; incorporates feedback directly into the decision-making process to ensure accurate and actionable outcomes.

"Identity alerts are one of the most common and time consuming alerts that security teams deal

with, so this is an important milestone for us as we help organizations further automate their SOCs, allowing security analysts to focus on strategic threats instead of getting buried in the noise," said Roy Halevi, co-founder and CTO at Intezer.

To learn more about how Intezer is transforming identity-based threat response, visit: https://intezer.com/blog/alert-triage/identity-based-alert-triage/.

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 Tier 1 SOC analyst (but without burnout, skill gaps, and alert fatigue). Learn more at www.intezer.com.

Mackenzie Kreitler
Intezer
press@intezer.com
Visit us on social media:
LinkedIn

---