Analyst1 Releases Version 2.13.0 Featuring Custom Indicators, New Microsoft Defender, and CrowdStrike SIEM Integrations

Analyst1 2.13.0 introduces custom indicators plus new EDR and SIEM integrations, giving security teams greater speed, flexibility, and operational insight.

ANALYST1®

Analyst1 - Threat Intelligence Platform

RESTON, VA, UNITED STATES, November 24, 2025 /EINPresswire.com/ -- Analyst1 announces the release of Analyst1 v2.13.0, delivering major advancements in intelligence flexibility, endpoint and SIEM correlation, and enterprise-grade API management.

The release introduces Custom Indicators, giving security teams the ability to design, validate, and operationalize their own indicator types to capture proprietary, emerging, or mission-specific threat patterns. This unlocks new levels of precision and customization previously unavailable in traditional TIPs.

Analyst1 v2.13.0 also expands real-time operational visibility with two new integrations:
- Microsoft Defender for Endpoint, enabling automated indicator exports and correlation of real-world observation data across intelligence.
- CrowdStrike Next-Gen SIEM, providing streamlined and powerful lookup file generation, and automated matching for faster triage and detection.

Additional enhancements include the first phase of API modernization including expanded request limits, and improved key management—as well as UI/UX updates, and multiple security, stability, and enrichment improvements.

"This release is all about delivering on our promise to give teams greater flexibility while continuing to deliver an approachable experience," said Michael Wenger, Director of Product at Analyst1. "From custom indicators to deeper EDR and SIEM integrations, we're removing the rigid limitations that have historically slowed down threat intelligence operations. Version 2.13.0 empowers analysts to shape their data, automate their workflows, and respond with greater speed and confidence."

Analyst1 v2.13.0 is available now. Customers may contact their CSM for upgrade support.

About Analyst1:

Threat intelligence teams often struggle to bridge the gap from insight to action. Analyst1 is the Orchestrated Threat Intelligence Platform designed to resolve this issue. It automatically organizes threat data, links it to your assets and vulnerabilities, and customizes views for different roles. Analyst1's orchestration layer streamlines workflows and automates reliable actions by integrating with SIEM, ticketing, and vulnerability management systems. From Fortune 500 financial institutions to national security agencies, enterprises trust Analyst1 to unify their defenses, significantly reducing their response time from days to minutes.

Julia Linn
Analyst1
+1 720-854-8738
email us here
Visit us on social media:
LinkedIn
Facebook
YouTube
X

This press release can be viewed online at: https://www.einpresswire.com/article/869016298