ANOMALI

Amplify Visibility and Unlock Your SOC

Automating and providing visibility into a Security Operations Center is mission-critical for effective cyber security. Here are nine useful ways to drive Actioned Visibility into your SOC.

Uplevel Log Management

Leverage log data going back years (not months) and correlate to new threats, increasing the efficiency and value of your existing SIEM investments.

Real-Time Monitoring

Drive visibility across all security telemetry and potential risk exposure, including cloud environments and your supply chain for immediate visibility and response.

Threat Intelligence Correlation

Enrich and prioritize threat intelligence and attacker insights with data from SIEMs, augment with curated and peer intel, decrease MTTD/R, and relieve pressure on security analysts.

Network Security Event Telemetry

Collect IoCs across a broad range of indicator types, integrated with threat intelligence and correlated to your potential attack surface.

Security Analytics

Run data queries against a significantly larger (historical) data set to build more sophisticated and actionable threat models.

Threat Hunting

Automatically prioritize intelligence and historical telemetry to optimize the threat hunting process.

Workflow Automation

Automate intelligence workflows to ingest, enrich, score, share and distribute intel, automating routine analyst tasks and reducing human errors.

Incident Response Automation

Automate precision threat detection, investigation, and response workflows with attacker context.

Collaboration and Knowledge Sharing

Fully integrate threat intelligence data into the analysis of operational and supply chain systems.

Anomali's Security Analytics Platform can directly address your requirements across a broad and deep range of use cases, including everything listed in this infographic.

For more detail, or to schedule a demo, please click here.

ANOMALI