ANOMALI

The Anomali Security Operations Platform: Cloud-Native, AI-Driven Cybersecurity

Big Data Security. Actionable Intelligence. Immediate, Relevant Insights.

The cybersecurity threat landscape is continuously growing, evolving, and adapting. At the same time, the acceleration of digital transformation initiatives is not only expanding organizational attack surfaces, it increases the challenges and stresses security teams deal with on a daily basis.

Organizations continue to make investments in cybersecurity but still work in silos, collecting and analyzing vast amounts of data without any context or correlation. As a result, security teams are being hindered by the fact that those technologies are not serving enterprise-wide needs, leaving them with a lack of visibility to immediately identify threats and respond quickly and effectively.

The Anomali Security Operations Platform is a cloud-native cybersecurity solution that automates the collection of threat data and drives detection, prioritization, and analysis, taking security from detection to remediation in literally seconds.

The Anomali Security Operations Platform is fueled by security analytics, curated GPT, and the world's largest intelligence repository to automatically correlate all security telemetry against active threats intelligence to stop attacks and attackers in real-time.

By cutting through the noise to surface relevant threats, the Anomali Security Operations Platform improves organizational efficiencies, providing security teams with the tools and insights needed to detect threats, make informed decisions, and act immediately against sophisticated attacks.

KEY USE CASES

- **Accelerate Threat Hunting**
  Proactively identify threats in your environment based on MITRE ATT@CK, TTPs, actors, campaigns, threat bulletins, and vulnerabilities.
- **Pinpoint Relevant Threats**
  Learn in seconds if a threat indicator is present in your historical event logs, asset data, vulnerability scan data, and/or threat intelligence going back years.
- **Elevate Strategic Intelligence**
  View alerts enriched with comprehensive threat intelligence context, MITRE ATT@ACK framework IDs, asset criticality, and risk scores.
- **Predict the Next Attack**
  Gain actionable visibility through continuous intelligence monitoring to uncover threats and prioritize responses.
- **Tune Security Postures**
  Automatically push identified IoCs to security controls, accelerating security workflows across your organization.

The Anomali Platform includes:

Anomali Threat Stream:

Threat Intelligence Management that automates the collection and processing of raw data and transforms it into actionable threat intelligence for security teams.

Anomali Match:

Security analytics-based threat detection that helps organizations quickly identify threats in real-time by automatically correlating all security telemetry against active threat intelligence to stop breaches and attackers,

Anomali Lens:

A powerful Natural Language Processing engine that helps operationalize threat intelligence by automatically scanning web-based content to identify relevant threats and streamline the lifecycle of researching and cross-functional reporting.

Aggregate

Automate the collection and correlation of security telemetry and threat intelligence

- Automate collection of current and historical event logs, asset data, and active threat intelligence
- Comprehensive visibility into historic security telemetry logs, billions of IOCs, and asset and vulnerability scan data
- Big data security management supporting event/alert correlation and machine learning analytics

Detect

Continuously identify known threats in your network using all available security telemetry and intelligence

- Continuous, real-time correlation of millions of indicators of compromise (IOCs) with all relevant security telemetry and log data
- Automated retrospective search and correlation of historical event logs with newly identified threat intelligence
- Predictive detection of malicious Command and Control domains created by attacker DGAs (domain generation algorithms)

Hunt

Scale threat hunting with real-time search and TTP-based execution

- TTP-based hunting by actor, threat bulletin, or vulnerability using advanced detection analytics
- Contextual threat intelligence in the form of actors, TTPs, campaigns, threat bulletins, and vulnerabilities, including MITRE ATT@CK details on the TTPs for any selected actor
- Predictive DGA analysis to identify bots in your network making connections to Command and Control servers

Investigate

Quickly research and prioritize alerts with advanced threat analytics and a powerful investigation workbench

- Alert enrichment with comprehensive threat intelligence context including tactics, techniques, and procedures, (TTPs), actors, correlated to MITRE ATT@CK techniques, as well as events, asset indicators, and links to raw system logs
- Perform real-time and retrospective search on an indicator, TTP, actor, or vulnerability across years of event data to uncover previously hidden incursions

Respond

MITRE ATT@CK mapping with an immediate view of globally matched threat impacts on your organization's security posture

- Continuous monitoring of detected indicators and associated threat models for response and ROI assessment
- Organization critical asset ID and alignment with known vulnerabilities and observed IOCs for response prioritization

Collaborate

Distribute and collaborate on threat intelligence with your peers and partners

- Collaborative threat visibility and identification in ThreatStream Trusted Circles (used by over 2,000 organizations and ISACs) for secure rapid response and ongoing intelligence collaboration with industry peers
- STIX/TAXII compliance for bi-directional intelligence exchange between TAXII servers and clients
- High-quality publishing to distribute threat bulletins and other finished intelligence products to stakeholders at customized levels of detail

KEY CAPABILITIES

- High-performance correlation of indicators at a rate of 190 trillion EPS
- Appliance and cloud-to-cloud based ingestion of any security control telemetry
- Global intel management across open, commercial, and proprietary resources
- STIX/TAXII for bidirectional intelligence exchange between TAXII sources and clients
- Interactive simplified dashboard and visualization of all IOCs
- Global intelligence feed optimization and scoring OOTB appliance/API integration for response orchestration with security tools
- Vulnerability enrichment aligning global threats with potential organizational impact
- Turnkey integration with leading enterprise SIEMS, firewalls, EDRs, and SOARs
- Extensible platform with restful APIs and SDKs for feeds, enrichments, and security system integrations
- Security tool integration for inbound data ingestion and outbound response orchestration via API/ appliance

ANOMALI