ANOMALI

THE ANOMALI PLATFORM

CLOUD NATIVE, INTELLIGENCE-DRIVEN EXTENDED DETECTION AND RESPONSE (XDR)

BIG DATA SECURITY. ACTIONABLE INTELLIGENCE. RELEVANT INSIGHTS.

The cybersecurity threat landscape continues to evolve and expand. The acceleration of digital transformation has not only expanded an organization's attack surface but it's also increased the challenges security teams deal with on a daily basis.

Organizations continue to make investments but are still working in silos, collecting and analyzing data without any context or correlation. As a result, security teams are being hindered by the fact that those technologies are not customizable to each organization, leaving them with a lack of visibility or threat intelligence needed to help them quickly identify threats and respond to threats.

The Anomali Platform is a cloud native extended detection and response (XDR) solution that automates the collection of threat data and drives detection, prioritization, and analysis, taking security from intelligence to detection in seconds.

The Anomali Platform is fueled by big data management, machine learning, and the world's largest intelligence repository, to automatically correlates ALL installed security telemetry against active threat intelligence to stop breaches and attackers in real-time.

By cutting through the noise to surface relevant threats, the Anomali Platform improves organizational efficiencies, providing security teams with the tools and insights needed to detect threats, make informed decisions and defend against today's sophisticated threats.

The Anomali Platform includes:

- ***Anomali ThreatStream:*** Threat Intelligence Management that automates the collection and processing of raw data and transforms it into actionable threat intelligence for security teams.
- ***Anomali Match:*** Intelligence-driven 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 reporting on them cross functionally.

KEY USE CASES

PINPOINT RELEVANT THREATS
Learn in seconds if a threat indicator is present inyour historical event logs,asset data, vulnerability scan data,and threat intelligence goingback at least five years.

ELEVATE STRATEGIC INTELLIGENCE
View alerts enrichedwith comprehensive threat intelligence context,MITRE ATT&CK framework IDs, asset criticality, and risk scores.

ACCELERATE THREAT HUNTING
Proactively identify threats in your environment based on MITRE ATT&CK TTPs, actors, campaigns,threat bulletins, and vulnerabilities.

PREDICT THE NEXT ATTACK
Gain relevant visibility through continuous intelligence monitoring to uncover threats and prioritize response.

TUNE SECURITY POSTURES
Manually or automatically push identified IoCs to security controls.

AGGREGATE

Automate the collection of all security telemetry and threat intelligence.

- Automated collection of current and historical event logs, asset data and active threat intelligence
- Comprehensive visibility into historic security telemetry logs, millions 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 yournetwork usingall of your security telemetry and intelligence to identify "known bads."

- 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 C2 domains created by attacker domain generation algorithms

HUNT

Scale threat hunting with real-time search and HTTP-based hunting.

- 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 a selected actor
- Predictive DGA analysis to identify bots in your network making connections to C&C servers

INVESTIGATE

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

- Alert enrichment with comprehensive threat intelligence context includingtactics, techniques, andprocedures(TTPs), actor,and available MITRE ATT&CK techniques, as well as event, asset, indicator, and links to raw system logs
- Perform real-time and retrospective search on an indicator, TTP, actor, or vulnerability across the past five years of event data to uncover previously hidden incursions
- Interactive visual explorationof relationships and associationsfor holistic threat analysis

RESPOND

MITRE ATT&CK mapping w/ immediate view of globally matched threat impact on organizations security posture.

- Continuous monitoringof detected indicators and associated threat models for response and ROI assessment
- Organizationcritical asset I.D. and alignmentwith 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) for secure rapid response and ongoing intelligence collaboration with industry peers
- **STIX/TAXII compliant** 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 your desired level of detail

KEY CAPABILITIES

High performance indicator correlation at a rate of 190 trillion EPS.

Appliance and cloud to cloudbased ingestion of any security control telemetry.

Global intel management across open, commercial, and proprietary sources.

STIX/TAXII for bi-directional intelligence exchange between TAXII source and clients Interactive, simplified dashboards for visualization of IOCs.

Global Intelligence feed optimizer and scoring. OOTB appliance/API integration for response orchestration with security tools.

Vulnerability enrichment aligning global threats with potential org impact.

- **Turnkey integrations** with leading enterprise SIEMs, firewalls, EDRs, and SOARs
- **Extensible platform** with restful API and SDKs for feeds, enrichments, and security system integrations
- **Security tool integration** for inbound data ingestion and outbound response orchestration via API/appliance

info@anomali.com | www.anomali.com

808 Winslow St, Redwood City, CA 94063 USA 1-844-4-THREATS

ANOMALI