ANOMALI
MATCH

INTELLIGENCE-DRIVEN THREAT DETECTION THAT POWERS EXTENDED DETECTION AND RESPONSE (XDR)

PRECISION THREAT DETECTION

When a new threat emerges, security teams need answers fast: Have we been impacted? Are we protected? How are we responding? What are we doing to prevent this kind of breach in the future?

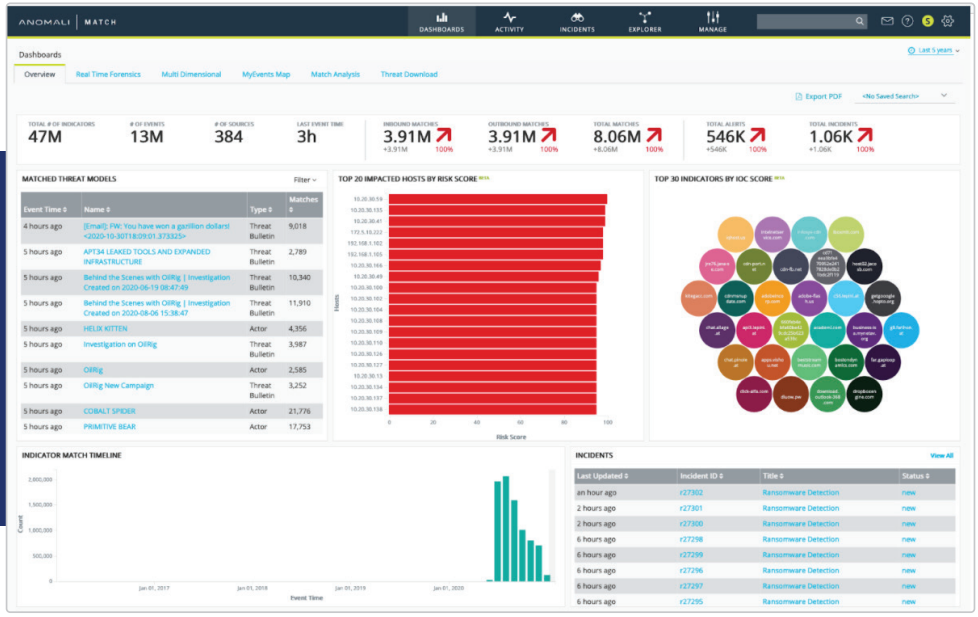
Match helps improve organizational efficiencies and productivity by automating detection activities to quickly profile a threat and its impact on the organization to enable an effective response.

Match collects security telemetry from across your organization – SIEM, EDR, Messaging and network – and integrates layered threat detection to pinpoint relevant threats and provide analysts with the actionable intelligence required to investigate the root cause or the precision confirmation of an attack to immediately respond.

KEY BENEFITS

- Quickly identify impact to understand criticality and prioritize response.
- Accelerate mean time to detection(MTTD) and mean time to respond (MTTR) to active threats.
- Leverage machine learning, automation, and available intelligence to automatically detect and respond to potential threats.
- Gain visibility into 5+ years of security telemetry, millions of IOCs, and asset and vulnerability scan data.
- Answer difficult questions quickly and with confidence for greater C-Level visibility.
- Reduce cost of security incidents and enable more efficient security operations.

Big data management with high performance indicator correlation at a rate of 190 trillion EPS to detect threats quickly.



KEY FEATURES

Anomali Match helps organizations achieve cyber resilience with key features that provide:

- Relevant Intelligence at Scale
- Precision Attack Detection
- Optimized Response across Security Ecosystems

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 your network using all 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 TTP-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 including tactics, techniques, and procedures (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 exploration of relationships and associations for holistic threat analysis

RESPOND

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

- Maintain a pulse on threats and indicators to uncover relationships during detection and response investigation
- Scan assets and vulnerabilities using consistent views that can be prioritized by severity and confidence
- Correlate internal environment with attack patterns to distill common tactics and sub-techniques to investigate and mitigate quickly

KEY USE CASES

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

ELEVATE STRATEGIC INTELLIGENCE
View alerts enriched with 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.

DEPLOYMENT OPTIONS

Match is available as an on prem or cloud native solution.

Additional Cloud Match Capabilities:

- High performance indicator correlation at a rate of 190 trillion EPS.
- Appliance and cloud to cloud-based ingestion of any security control telemetry.

info@anomali.com | www.anomali.com
808 Winslow St, Redwood City, CA 94063 USA 1-844-4-THREATS

ANOMALI