Anomali Platform Meshes World-Class Intelligence With Instantaneous Threat Detection

EMA IMPACT BRIEF

ANOMALI

Anomali recently announced The Anomali Platform, a cloud-native extended detection and response (XDR) solution that couples the world's largest repository of security intelligence with best-in-class threat detection and prevention capabilities. Using big data analytics and machine learning, The Anomali Platform automatically discovers threats, giving security teams the information needed to make rapid and informed decisions to protect the enterprise.

Background

Founded in 2013 as ThreatStream and rebranded in 2016, Anomali is consistently recognized as a leader in the security space. Their most recent release, The Anomali Platform, is the integrated effort of their three primary security offerings:

- 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 extension 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.

Combining these three products into a single unified platform, The Anomali Platform creates a cloud-native XDR solution that can continuously detect threats and prevent attacks before they happen.

Key Ramifications

The Anomali Platform solution is a major step forward for Anomali and delivers the following key capabilities:

- Aggregated Threat Intelligence – The Anomali Platform will automate the collection of past and present event logs, as well as all active threat intelligence. The Platform also provides greater visibility into historic security scans, event correlation, and analytics.
- Continuous Threat Detection – The Anomali Platform constantly scans networks and devices, identifying known threats and potential attacks. It also reconciles past security vulnerabilities with current threat intelligence.
- Reduced Threat Hunting – The Anomali Platform simplifies and streamlines HTTP-based hunting. It also provides context-based threat intelligence based on the MITRE ATT&CK framework for specific threat actors.
- Prioritized Research and Investigations – The Anomali Platform provides contextual intelligence with relevant and specific remediation procedures (based on MITRE ATT&CK framework). It also provides a visual, relational representation of the attack surface for better threat analysis.
- Coordinated Response – The Anomali Platform provides specific recommendations for breaches while offering continuous monitoring. Ranked responses allow practitioners and decision makers to prioritize risk/response actions.

All in all, The Anomali Platform delivers a best-in-breed cloud XDR solution that continuously detects threats and prevents attacks before they happen.

EMA Perspective

Seemingly, every security company is coming out with their flavor of detection and response, all of which are the "best" or "leading" at stopping the bad guys from doing damage to enterprise networks and systems (one may wonder how the bad guys could even stand a chance). Anomali make those claims as well, but the real difference here is that they have the experience and credentials to back up those claims, while many of the others are still improving on their products.

Anomali has taken three of the better security solutions on the market and bundled them together into a comprehensive security tool, one that uses the world's largest (this is not hyperbole) threat/security intelligence repository to detect and identify suspicious activity and put a stop to it. Really, at the end of the day, The Anomali Platform actually does what it says that it does—it continuously detects security threats and prevents attacks before they happen.

Time will tell how well The Anomali Platform does in the crowded XDR market. They have to overcome lots of competitors that are already promising their customers that they can deliver the bad guys on a platter. For those companies that are interested in a complete security solution without the noise and nonsense that sometimes comes with technology marketing, The Anomali Platform is very much worth a deeper look and evaluation.