DETAILS

Vendor Anomali

Price $50,000

Contact anomali.com

Features	★★★★★
Documentation	★★★★★
Value for money	★★★★★
Performance	★★★★★
Support	★★★★★
Ease of use	★★★★★

OVERALL RATING ★★★★★

Strengths Trusted Circles is a collaborative community platform that acts as an additional stream of information ingested by the platform.

Weaknesses None that we found.

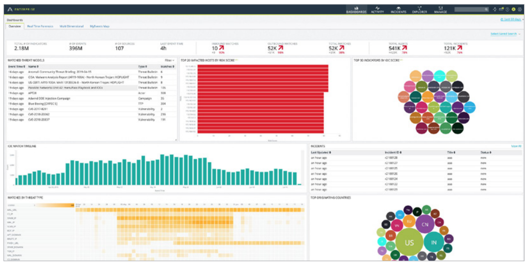
Verdict Anomali Altitude is an integrated suite designed to enable organizations to identify serious threats, investigate adversaries, and respond efficiently and effectively.

ANOMALI®

info@anomali.com
www.anomali.com

Anomali

Anomali Altitude™



Anomali Altitude is an integrated suite designed to help organizations identify serious threats, investigate adversaries and respond efficiently and effectively. Organizations also can import their own data directly into the platform, via STIX, or through email. Visibility into threats and events enhance threat detection capabilities. Automated threat detection, analysis and operations improve response efficiency and effectiveness.

SC MEDIA BEST BUY

Anomali added software development kits to the platform for feeds, enrichments and integrations. And, the product includes assistance in the development of SDKs. Available as a cloud service or on-premises, Anomali Altitude offers enterprises a single, centralized environment for the collection, management, integration and analysis of all cyber threat intelligence.

Threats and events receive a severity level score as well as a confidence score. Analysts can delve into each event for more information, such as whether an active threat is underway, what type of threat it is and the like. The solution shows all ingested data and matches it to each indicator of compromise. The solution provides comprehensive analysis through the collaboration between internal and external cyber threat intelligence groups. New investigations can be created and assigned to a user or work group.

ThreatStream passes gathered intelligence through machine intelligent algorithm that uses it to produce threat feeds. It uses this information to generate scores, which combined human research eliminates the possibility of flagging false positives or duplicates.

ThreatStream includes sandboxing capabilities. So, for example, if an attachment comes with an email, an analyst can use the onboard sandbox to detonate the information. We found it easy to pivot throughout the platform to identify all the details around an attachment and any associated threats or events.

Retrospective searches compare specific domains with present and historical log information to correlate events with data ingested through the platform. The product can also ingest and leverage asset data. Vulnerabilities show where detections and patches occur to provide a big picture perspective. CrowdStrike provides actor details along with motivations and industries targeted in addition to descriptions, associations, attachments and historical information.

Dashboards include some unique pieces of information, like sightings (changes in presentation of an item or an event). Bidirectional communication with SIEM technology and populated attacks show matched data in a 3D global map based on threat intelligence and where it originates. Anomali Altitude also matches threat types to an environment based on log data.

Organizations can add individual widgets to the dashboard and customize per user login. The solution can export all data to PDFs with a variety of reporting options. A fully searchable help feature built into the platform assists analyst with anything they may need.

A Visualization Entities Map harvests data and enrichments that are customizable. Organizations can import and publish observables within the platform for easy research capabilities or further use of that information.

A standout among the Anomali offerings, the Trusted Circle collaborative community platform allows analysts to share intelligence that serves as an additional stream of information ingested by the platform.

Starting price is $50,000. Basic no-cost support offerings include 24/7 for subscription duration. Fee-based support options are available. Phone, email and website support include FAQs and a knowledgebase.

— Katelyn Dunn
Tested by Matthew Hreben