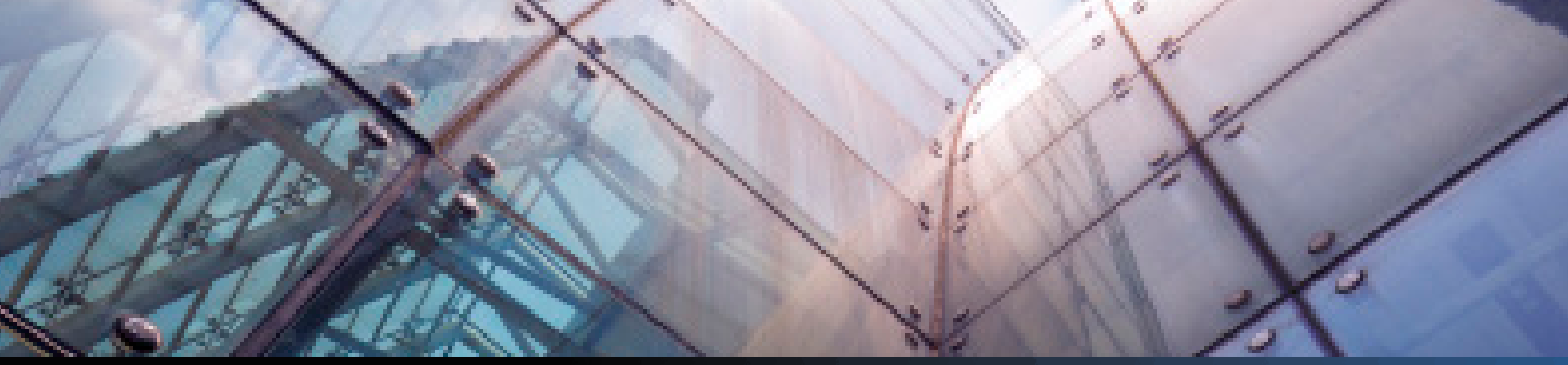


Partner Data Sheet

RSA Security Analytics

Industry

Security, Operations, and Compliance

Website

www.rsa.com

Company Overview

RSA provides more than 30,000 customers around the world with the essential security capabilities to protect their most valuable assets from cyber threats.

Product Overview

RSA Security Analytics discovers attacks missed by log-centric SIEM and signature-based tools with the only solution that can correlate network packets with other security data.

Solution Highlights

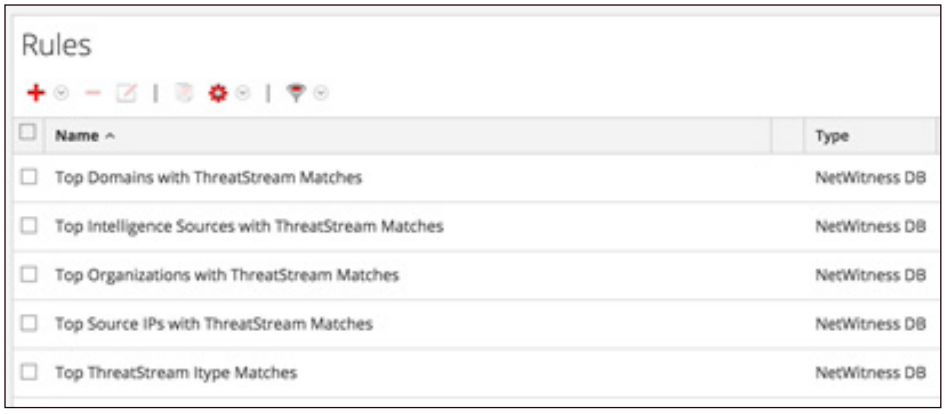
- Be one step ahead of advanced attacks
- Detect and analyze advanced attacks
- Empowering security teams like never before

Next Generation Security Solutions

The threat landscape is continually expanding and organizations are under continuous attack and overwhelmed with alerts. Thousands of incidents occur each day and security professionals only have time to deal with dozens. This creates operational chaos. Security teams need next-generation security solutions to help them respond faster, defend proactively and invest smarter.

Just-in-Time Intelligence

Threat intelligence is continuously gathered, categorized, risk ranked (for severity and confidence) in Anomali's ThreatStream platform and then delivered in real-time to your RSA Security Analytics instance for detection of security threats in your enterprise infrastructure for the security and threat intelligence teams to quickly see high priority threats to your business. Each of the selected IOCs for integration into your RSA Security Analytics instance enriched with factors such as risk score to add context and relevance to the delivered information



ANOMALI

Benefits of Anomali

- Easy-to-use interface to view threat information received through STIX/TAXII feeds.
- Analyze and correlate data into actionable information: SIEM rules, reports, and dashboards.
- Pinpoint IOCs - quickly search for a specific indicator, search for an indicator type over a time range, and drill-down into details.
- Eliminate unnecessary, duplicative and irrelevant indicators - before they enter your infrastructure.
- Identify and prioritize the events that matter now - without DIY scripting.
- Machine-to-Machine learning algorithms scale to accommodate thousands of IOCs per minute across your environment.

Benefits of RSA

- Improve threat detection, investigations and response by consuming network flow data, full packet capture (PCAP), logs, and endpoint data, as well as information from other security systems, external threat intelligence and IT assets.
- Designed to enable forensic investigations that make it simpler for security teams to determine the root cause of an incident.
- The RSA Live service provides machine-readable threat intelligence thus making the intelligence actionable immediately.
- When used together, the combined solution provides security teams with visibility, threat detection and response capabilities from endpoints to the cloud.

Benefits of the Joint Offering

Anomali's RSA Security Analytics content adds real-time threat intelligence to event data in your RSA Security Analytics deployment. Threat intelligence is continuously gathered, categorized, risk ranked (for severity and confidence) in Anomali's ThreatStream platform and then delivered in real-time to your RSA Security Analytics instance for monitoring and detection of security threats in your enterprise infrastructure for the security and threat intelligence teams to quickly see high priority threats to your business. The intelligence is based on common industry-accepted Indicators of Compromise (IOC) such as source and destination IP addresses, email addresses, domains, URLs, and so on, but is enriched with factors such as risk score to add context and relevance to the delivered information.

Automated Integration

The Anomali RSA Security Analytics integration is quick and easy. A small piece of software, Anomali Link, automatically delivers threat intelligence with nearly a dozen meta fields on a regularly scheduled basis to be picked up by the RSA Security Analytics Live Feeds. Configuration is normally only necessary during the initial installation.

Correlation

RSA Security Analytics Rules and Reports are easily added into the instance to correlate our lists against events sent into the Concentrator. These correlations are then shown in the Alerts field within the Investigation page.

Extended Functionality

Our integrated External Lookup also enables your analysts to have access to more information about the Alert than ever before by taking analysts to the ThreatStream details page showing every related aspect and impact of the Indicator of Compromise in question.

About Anomali

Anomali delivers earlier detection and identification of adversaries in your organizations network by making it possible to correlate tens of millions of threat indicators against your real time network activity logs and up to a year or more of forensic log data. Anomali's approach enables detection at every point along the kill chain, making it possible to mitigate threats before material damage to your organization has occurred.

About RSA

RSA provides more than 30,000 customers around the world with the essential security capabilities to protect their most valuable assets from cyber threats. With RSA's award-winning products, organizations effectively detect, investigate, and respond to advanced attacks; confirm and manage identities; and ultimately, reduce IP theft, fraud, and cybercrime. RSA's product suite provides comprehensive visibility into networks, endpoints, and identities delivered through the industry's most effective and complete investigative workbench for detecting attacks and initiating response.

ANOMALI

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