Partner Data Sheet

splunk>

Website

www.splunk.com

Company Overview

Splunk provides the leading platform for Operational Intelligence. Customers use Splunk to search, monitor, analyze and visualize machine data.

Product Overview

Splunk offers the leading platform for Operational Intelligence. It enables the curious to look closely at what others ignore—machine data—and find what others never see: insights that can help make your company more productive, profitable, competitive and secure.

Solution Highlights

- Splunk Core
- Splunk Enterprise Security
- Splunk Cloud size of your network.

Next Generation Security Solutions

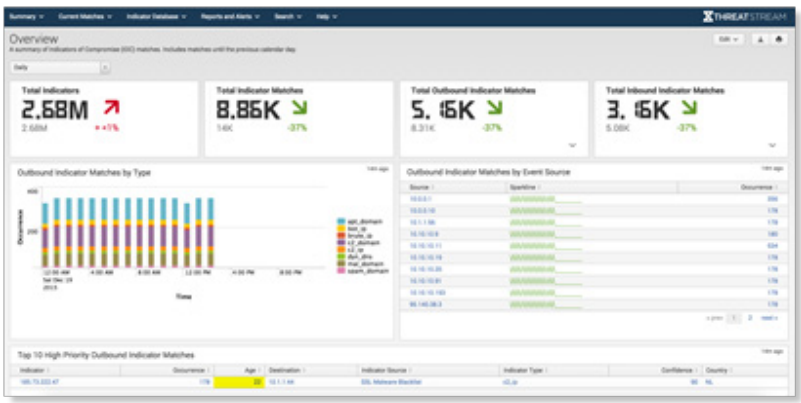
The threat landscape is continually expanding and organizations are under continuous attack and overwhelmed with alerts. Thousands of incidents occur each day and security professionals only have time to deal with dozens. This creates operational chaos. Security teams need next-generation security solutions 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 Splunk 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 Splunk instance enriched with factors such as risk score to add context and relevance to the delivered information.

Benefits of the Joint Offering

The Anomali Splunk App provides seamless, automated integration of indicator data to deliver real-time threat intelligence to your Splunk instance so you can start using the threat feeds in meaningful ways more efficiently and more effectively than ever before.



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 Splunk

- Search, monitor and analyze any machine data for powerful new insights.
- Use cloud to have all the features of Splunk Enterprise with all the benefits of SaaS.
- Rapidly explore, analyze and visualize data in Hadoop to unlock the business value of big data.
- Log search and analysis for small IT environments as a cloud service or software.

Prioritized Information

The Anomali Splunk integration provides analysts with prioritization of what they're seeing in their Splunk instance making them far more effective and efficient.

Enrichment

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.

Seamless

Anomali's Splunk App adds real-time threat intelligence to event data in your Splunk 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 Anomali Splunk App 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.

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 Splunk

Splunk is a market-leading platform that powers Operational Intelligence. Splunk pioneers innovative, disruptive solutions that make machine data accessible, usable and valuable to everyone. More than 11,000 customers in over 110 countries use Splunk software and cloud services to make business, government and education more efficient, secure and profitable.

For more information contact Anomali sales at info@anomali.com

ANOMALI

2317 Broadway, 3rd Floor, Redwood City, CA 94063 USA
1-844-4-THREATS | info@anomali.com | www.anomali.com