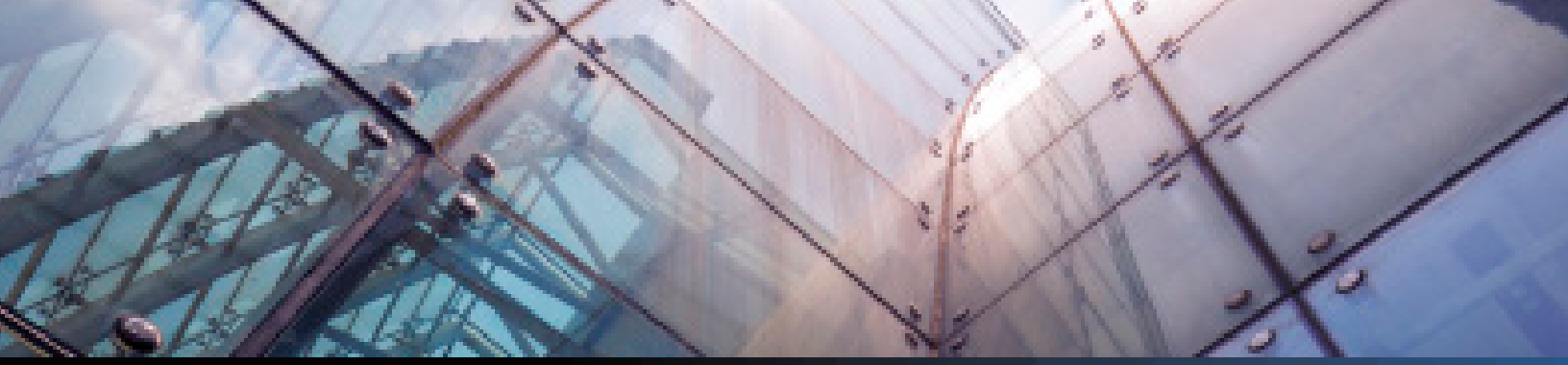


Partner Data Sheet

accelops

Industry

SIEM

Website

www.accelops.com

Company Overview

AccelOps offers the industry's first software to monitor both performance and security (SIEM) of IT infrastructure and applications from a common cloud-generation platform.

Product Overview

AccelOps brings together Network Operations Center (NOC) and Security Operations Center (SOC) analytics (SIEM and PAM) into a comprehensive, real-time, cross-correlated "Single-Pane-of-Glass" view into an organization's network.

Solution Highlights

- The AccelOps patented unified analytics platform is the industry's first to integrate and cross-correlate data and analytics that has historically been procured and managed in divergent organizational silos.

- Control threats to network security, performance, and regulatory compliance, by dramatically decreasing the time it takes to identify, isolate, remediate and prevent future threats

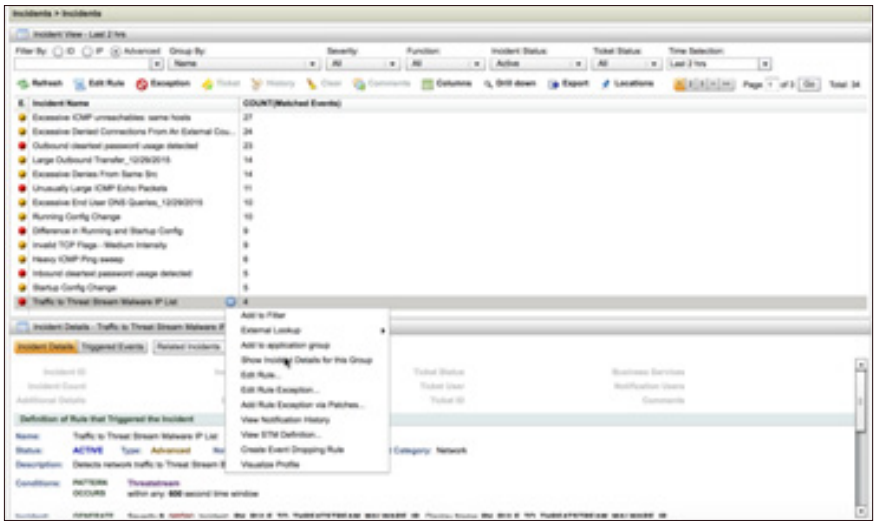
ANOMALI

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 AccelOps 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 AccelOps instance enriched with factors such as risk score to add context and relevance to the delivered information



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 AccelOps

- Cloud Security
- Performance and Availability Monitoring
- Big Data Analytics
- Managed Service Providers (MSPs)
- Asset Discovery and Change Management
- Cloud and Virtualizations Monitoring
- IT Operations Management

Benefits of the Joint Offering

Anomali's AccelOps content adds real-time threat intelligence to event data in your AccelOps 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 AccelOps 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 and domains, but is enriched with factors such as risk score to add context and relevance to the delivered information.

Automated Integration

The Anomali AccelOps integration is quick and easy. A small piece of software, OpticLink, automatically delivers threat intelligence with the relevant context on a regularly scheduled basis to be picked up by the AccelOps Blocked Lists at the time interval you specify. Configuration is normally only necessary during the initial installation.

Correlation

Anomali AccelOps CMDB, Rules, and Dashboard provide seamless, automated integration of indicator data to deliver real-time threat intelligence to your AccelOps instance so you can start using the threat feeds in meaningful ways more efficiently and more effectively than ever before.

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 AccelOps

The AccelOps solution is fundamentally changing the way organizations are able to control threats to network security, performance, and regulatory compliance, by dramatically decreasing the time it takes to identify, isolate, remediate and prevent future threats. The AccelOps patented unified analytics platform is the industry's first to integrate and cross-correlate data and analytics that has historically been procured and managed in divergent organizational silos. Anything less is putting you and your organization at risk.

ANOMALI

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