ArcSight
An HP Company

Industry

SIEM

Website

www.hpe.com

Company Overview

Hewlett Packard Enterprise draws on decades of enterprise security experience and powers much of the world's security intelligence to uncover vulnerabilities, identify threats and neutralize them so that, instead of simply reacting, you can proactively counter your adversary.

Product Overview

The ArcSight SIEM solution is a comprehensive threat detection and compliance management platform with a flexible architecture allowing organizations to easily scale out their existing deployments.

Solution Highlights

ArcSight is an Enterprise security management software that combines event correlation and security analytics to identify and prioritize threats in real time and remediate incidents early.

A Holistic Approach to Security Intelligence

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

Benefits of the Joint Offering

Anomali's ArcSight content adds real-time threat intelligence to event data in your ArcSight 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 ArcSight 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.

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 ArcSight

- Prioritize security events

- Protect your business

- Flexible architecture

- Speed to value and simplified SIEM

- Real-time correlation

- Non-stop compliance

- Security information ecosphere

- Easily expand the size and breadth of a deployment.

Integrated Context

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

ArcSight ESM content is delivered through the Anomali Link software. Anomali Link talks directly with the ESM API to deliver rules, dashboards and other configurations.

Active Channels are core part of working in ArcSight. Anomali provides various Active Channels, but there are two key Active Channels for viewing Anomali data.

Real-world Content

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

About Anomali

Anomali™ is the pioneer of an enterprise class threat intelligence platform, combining comprehensive threat data collection, prioritization, and analytics with secure collaboration in a vetted community. Offering the broadest enterprise security infrastructure integration available, the ThreatStream platform enables organizations to proactively identify and combat cyber threats targeting their operations. www.anomali.com

About Hewlett Packard Enterprise

Hewlett Packard Enterprise has been in the innovation business for more than 75 years. HPE's vast intellectual property portfolio and global research and development capabilities are part of an innovation roadmap designed to help organizations of all sizes – from global enterprises to local startups – transition from traditional technology platforms to the IT systems of the future. HPE makes IT environments more efficient, productive and secure, enabling fast, flexible responses to a rapidly changing competitive landscape. HPE enable organizations to act quickly on ideas by delivering infrastructure that can be easily composed and recomposed to meet shifting demands, so they can lead in today's marketplace of disruptive innovation.

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

ANOMALI