ArcSight Recon

Micro Focus ArcSight Recon is a comprehensive SIEM log management tool and security analytics solution that eases compliance burdens and accelerates forensic investigation.

Product Highlights

Cyber-security has never been more important. More business is conducted online, more sensitive information is stored digitally, and more work is completed by remote workforces than ever before. Compliance mandates are getting stricter, all while bad actors develop increasingly sophisticated methods of infiltration.

As organizations strive to collect and store security data from a seemingly infinite number of sources, data monitoring and management has become increasingly difficult. Many solutions in the market simply weren't built with security in mind, and inadvertently cause inefficiencies when implemented within the context of SIEM, security compliance, event logging, and forensic investigation. Logging and forensic investigation are essential tasks in a modern SOC, and organizations need a solution that transcends the standards of today in order to be equipped for tomorrow.

ArcSight Recon is a comprehensive log management and security analytics solution that eases compliance burdens and accelerates forensic investigation for security professionals. It combines the compliance, storage and reporting needs of log management with the capabilities of big-data search and analysis. Recon is built for security event logs and is therefore more intuitive and accessible for security analysts, it won't require a DBA to operate. It helps hunt and defeat threats by unifying data logs from across organizations, processing billions of events, and quickly making

them available for search, visualization and reporting. Recon helps SOC engineers gain a deeper understanding of alerts across their organization and plays an important role in ArcSight's mission to deliver powerful layered analytics.

Key Benefits

Centralize Log Management

ArcSight Recon stores terabytes of machine data from any source (including logs, clickstreams, sensors, stream network traffic, security devices, Web servers, custom applications, social media, and cloud services). It enables you to store, search, monitor, and analyze data to gain centralized security intelligence from across your entire organization. For quick exploration of the data, Recon's event detail panel allows investigation of individual and grouped events. The raw message view allows analysts to inspect original, unformatted event logs. It was built with simplicity, usability and security in mind, and won't require a DBA to operate.

Key Features

- Event detail panel
- Raw message view
- Outlier detection
- User-friendly search bar
- Reporting content packages
- Unified ArcSight platform
- Single ID login

Key Benefits

- Centralize log management
- Hunt and defeat threats faster
- Report for compliance
- Store data at scale
- Integrate with your security environment

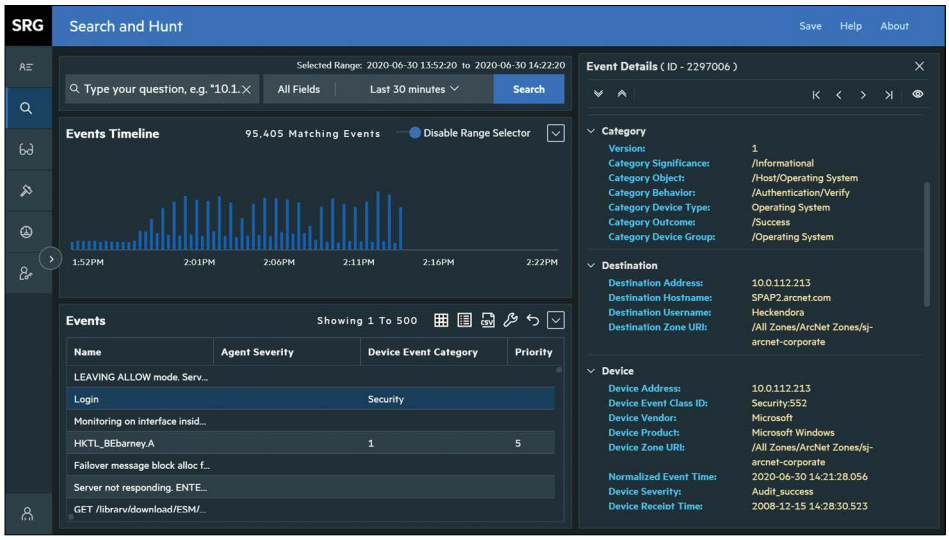

Figure 1. Event detail panel

Hunt and Defeat Threats Faster
Sift through mountains of log data with minimal effort using Recon's dynamic query suggestions and get results faster with its powerful security analytics technology. ArcSight Recon's columnar database responds to queries faster than traditional databases, enabling it to quickly and efficiently investigate millions of events. Storing clean, structured data in one centralized location accelerates investigation and improves the quality of results. Outlier detection provides visualizations to quickly identify deviations from baseline host behavior metrics. Recon's user-friendly search interface displays a grid or message view as well as a time-based histogram. It facilitates threat hunting in massive datasets, enabling security analytics at scale. It minimizes requirements for expertise and training, prioritizes abnormalities, and improves efficiency.

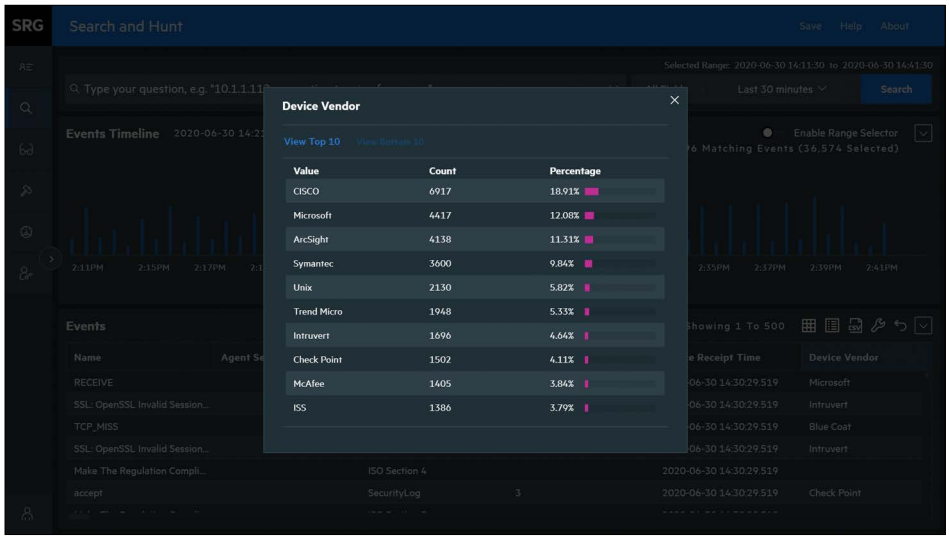

Figure 2. Histogram of vendor device values

Report for Compliance
Prepare compliance reports faster with Recon's reporting content packages. Select the report wizard or choose a template to create crosstab reports, tables, or chart-based reports for your organization. Pre-built content for FIPS 140-2 compliance is available, with more reporting templates expected in subsequent releases. MITRE ATT&CK content within Recon helps align your organization's compliance and security efforts.

Store Data at Scale
Store data more efficiently with Recon's event aggregation and log compression. ArcSight Recon cost-effectively stores your security event log data, thanks to its impressive compression ratios. ArcSight SmartConnectors allow aggregation and filtering of events for additional log storage savings. Whether you choose to deploy with one node or multiple, ArcSight Recon is built to scale with your needs.

Integrate with Your Security Environment
Disparate, unstructured storage delays investigation and limits the ability to connect patterns or multi-stage attacks. Gain a complete view of security events by integrating with and consolidating your existing security operations solutions. ArcSight Recon leverages the Security Open Data Platform (SODP) architecture that allows you to collect, normalize, aggregate, and enrich data from over 480 source types. With the ArcSight 2020.2 release, collection and storage of data has been consolidated to a single unified storage platform. Recon empowers teams to securely store data on its structured data lake for data exploration.

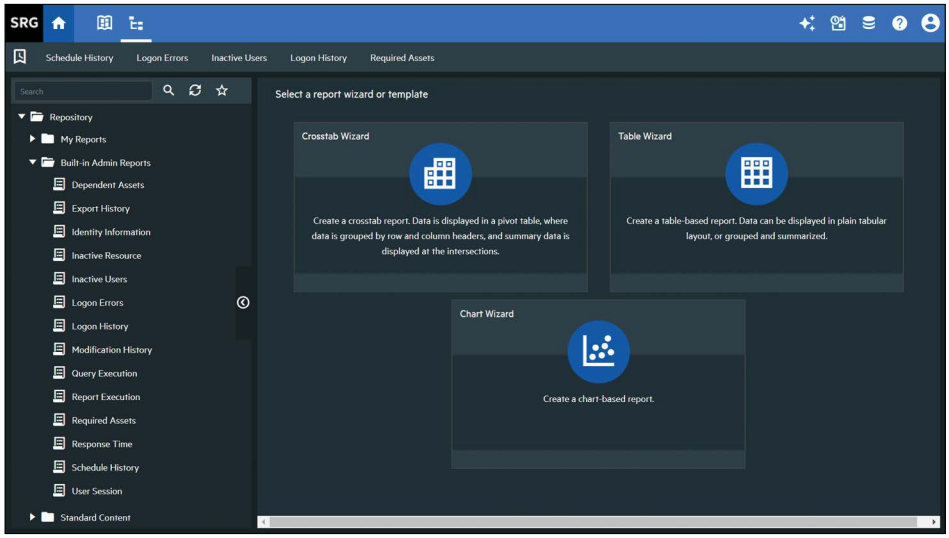

Figure 3. Creating reports

Collect once, store once, and use your data often. With this unification you can now navigate between ArcSight ESM, ArcSight Interset and ArcSight Recon with a simple click of a button. ArcSight's single ID login (customizable) saves time when toggling between any of the ArcSight portfolio products. For organizations that utilize multiple solutions, Recon can also integrate with leading security tools to provide quick investigation, streamlined workflows and fast response times.

Why ArcSight?

The ArcSight next-gen SIEM platform is scalable and powerful. It is a comprehensive solution developed for security professionals by security experts. It takes a holistic approach to security intelligence, uniquely unifying Big Data collection, network, user and endpoint monitoring and forensics with advanced security analytics technologies, including hunt, investigation, and UEBA solutions. It provides real-time threat detection and response, compliance automation and assurance, and IT operational intelligence to provide a powerful layered analytics approach that enables the self-defending enterprise. While many vendors claim to provide a robust SIEM solution, the ArcSight team has the security expertise, experience, and leadership that few vendors can match. Our next-gen solution, proven methodologies, and 20 years of experience with some of the largest, most complex SOCs in the world make Micro Focus uniquely qualified to help you achieve greater security posture and operational excellence.

Learn more at
www.microfocus.com/en-us/cyberres/secops/arcsight-recon

Contact us at **CyberRes.com**
Like what you read? Share it.

CyberRes
A Micro Focus line of business