ArcSight SIEM as a Service Log Management and Compliance

Empower your security operations with ArcSight SIEM as a Service.

ArcSight SaaS at a Glance

Centralize Log Management

Store, search, monitor, and analyze data to gain centralized security intelligence across your organization.

Report for Compliance

Policy-driven data collection and retention. Be audit-ready at all times.

Hunt for Threats Fast

Efficiently hunt for threats with outlier detection, a powerful and fast search engine, and visualizations.

Evolve with ArcSight SaaS

Simplify your SecOps with SaaS, increase time to value, and reduce infrastructural workloads, onboarding, and education times. Focus on your primary mission and core competencies.

Welcome to ArcSight SIEM as a Service

Defending your organization from today's evolving threat landscape can be complicated and time consuming. With the effect of rapid digitalization and the increase in remote workers, the threat landscape is increasing significantly and adding to the workload of security professionals. Managing infrastructure workloads and software updates brings an additional challenge for security operations and distracts security analysts from their core responsibilities of detecting and defending their organization from possible attacks.

ArcSight SaaS provides a no-hassle security experience by eliminating the cost of buying, installing, and managing servers and simplifying and empowering security operations. There is minimal up-front cost when switching to SaaS and little to no maintenance cost. The ArcSight team takes care of all the servers, hardware, and maintenance on behalf of the customer to eliminate security infrastructure concerns. With auto-updates, customers can run on the latest and greatest versions and benefit from the capability improvements immediately.

ArcSight SaaS is an intelligent, holistic security operation stack with log management, and compliance capabilities in a scalable, no-hassle environment. It provides a very detailed view into exactly what is happening in an organization by turning data into visualizations and actions.

ArcSight SaaS combines the compliance, storage, and reporting needs of log management with the capabilities of big data search and analysis. It is built for security event logs and is therefore more intuitive and accessible for security analysts.

Log Management

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, creating inefficiencies when implemented within the context of SIEM.

ArcSight SaaS makes SIEM log management simple with policy-driven data collection, centralized log management, and hypothesis-driven threat hunting tools that improve efficiency and reduce the time spent hunting for threats. Data can be collected from many sources—including logs, sensors, ream network traffic, security devices, web servers, custom applications, social media, cloud services, and more to improve your data monitoring.

ArcSight SaaS's columnar database responds to queries faster than traditional databases, enabling it to investigate millions of events quickly and efficiently. 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.

With big data analytics, reports, dashboards, search visualizations, and prebuilt content, ArcSight SaaS helps you gain full visibility into your security environment. ArcSight SaaS

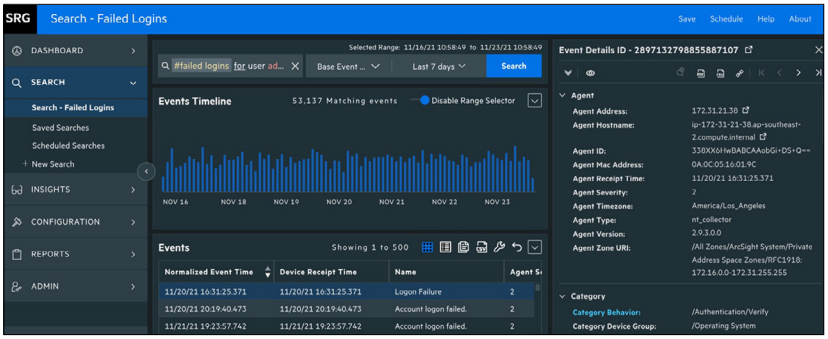

Figure 1. Event detail panel

has been optimized for speed and search performance, empowering security teams with a super-fast and powerful search engine to provide a deeper understanding of alerts across your organization. ArcSight SaaS uses a columnar database that reduces time spent waiting for search results to load. It also makes forensic investigations easier with smart search features such as autofill, search suggestions, filters, raw event details, saved and scheduled searches, search on historic data, parallel searches, reports, and dashboards.

Hypothesis-Driven Threat Hunting

Threat hunting is an analyst-centric process that enables organizations to uncover hidden advanced threats missed by automated preventive and detective controls. It leverages the collaboration of people, technology, and process in uncovering top-tier attackers. ArcSight SaaS empowers threat hunters by turning data into insights and actions.

- Enjoy the ease of threat hunting with outlier detection, visualizations, fast and detailed search, reports, and dashboards to hunt for threats before damage is done.
- Identify the anomalous activities with outlier detection to quickly identify deviations from baseline host behavior metrics and deep dive into what is going on in your environment with smart, fast search and hunt.
- Run many parallel searches at high speed. Never waste time while waiting for search results.
- Encourage your teams for exploratory search approaches and creative mindsets.
- Benefit from the advantage of easy-to-use transparent results for decision-making.

Compliance

Compliance regulations aren't meant to increase the workload of a SOC (Security Operations Center). They are meant to help organizations improve their security posture. That is the reason ArcSight SaaS's compliance module is designed specific to cybersecurity. ArcSight SaaS compliance module reduces the pain and complexity of compliance reporting with simpler, customizable reports and dashboards. With policy-driven data collection and retention, and 100+ out-of-the-box reports and dashboards, it is easy to run efficient compliance reports, and help compliance teams be audit-ready at all times.

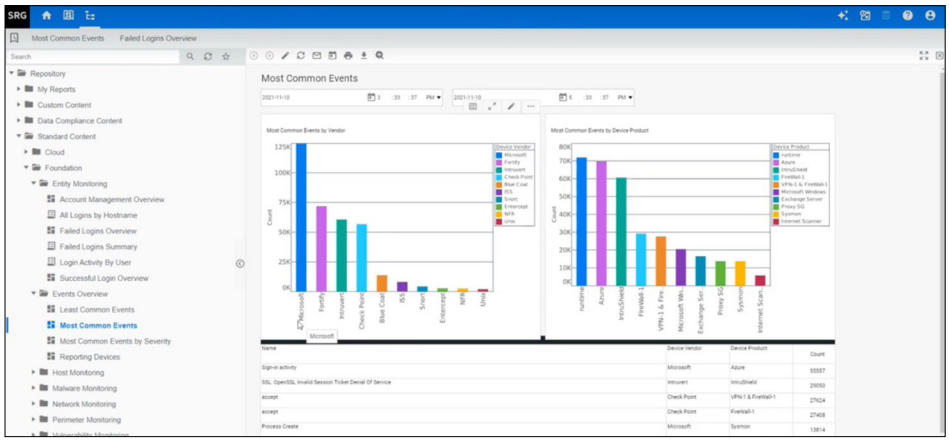

Figure 2. Turn data into visualizations with ArcSight SaaS

Dashboards and Visualizations

ArcSight SaaS comes with 100+ out-of-the-box reports/dashboards, including cloud, OWASP, and data modeler. Its prebuilt and customizable reports and dashboards enable you to have a better understanding of your security environment, turn data into visualizations for full visibility into your security environment, and decrease the time to create reports and dashboards.

Why ArcSight SaaS?

The next-gen SIEM platform ArcSight SaaS 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. ArcSight SaaS provides log management, compliance automation and assurance, and intelligent threat hunting to provide a powerful, layered analytics approach that empowers enterprises on SaaS.

Learn more at **www.microfocus.com/en-us/cyberres/saas/secops**

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

CyberRes
A Micro Focus Line of Business