opentext™ | Cybersecurity

Flyer

ArcSight SIEM as a Service (SaaS)

Elevate your security operations with ArcSight SaaS, designed to enhance your cyber resilience with advanced detection, response, and investigation tools delivered in a secure SaaS environment.

ArcSight SaaS at a Glance

Protect

Protect your organization in a scalable environment with intelligent tools to empower your SOC pros.

Detect

Leverage multiple threat detection technologies to reduce your risk. Detect known threats in real-time, and respond with native SOAR. Discover unknown, elusive threats with behavioral analytics and advanced threat hunting.

Evolve

Simplify your SecOps with SaaS deployments for superior threat hunting to decrease attacker dwell time and increase SOC efficiency.

Welcome to ArcSight SaaS

Securing your organization can be complicated and time consuming due to the growing complexity of managing on-premises servers and networks, a cybersecurity talent shortage, and the increased dangers of the expanding threat landscape. Managing and upgrading SecOps systems can add to the difficulty of maintaining a secure organization and be a distraction from your core business. To improve the experience of managing SecOps, we bring you OpenText™ ArcSight SaaS to simplify the security experience.

ArcSight SaaS provides a no-hassle security experience by removing the need to buy, install, and manage servers, simplifying your security experience to empower your SecOps team. The ArcSight team takes care of all the servers, hardware, and maintenance on your behalf to eliminate security infrastructure concerns and to free up time for your team to focus on stopping cyberthreats in their tracks.

Not only does the ArcSight team take care of server infrastructure, but painful version upgrades are also a thing of the past with ArcSight SaaS. New releases are automatically applied to your SaaS instance, so you always have the latest and greatest features at no additional expense to you.

Our pricing model makes managing SOC costs simple and easy. The model promotes pricing transparency designed to reduce EPS overage fees. This pricing model can significantly reduce unexpected pricing variations, making budgeting predictable and simple.

Using ArcSight SaaS enables virtually infinite scalability to grow with your organization, so you don't have to worry about expanding your security storage or computing. In contrast, on-premises deployments can require significant resources, time, and money to expand in order to accommodate your growing business.

ArcSight SaaS Capabilities

ArcSight SaaS features a range of solutions that work together to fit the needs of your SOC with industry-leading real-time threat detection, a native threat intelligence feed, native SOAR, intuitive log management, advanced behavioral analytics, long-term data retention for compliance, reporting, customizable dashboards and visualizations, outlier and anomaly detection, and more.

Real-Time Threat Detection

Faster threat detection and response are critical to reducing threat exposure time and the risk of breach. There are many useful threat detection technologies in the market today, but real-time event correlation from a SIEM is still the fastest method to uncover and escalate known threats in a cyber environment. It alerts analysts to threat-correlated events in real-time, rather than making them wait on batched searches. ArcSight has been a long-time market leader in real-time threat detection and is now one of the few vendors to offer this capability in the SaaS space.

ArcSight SaaS with Real-Time Threat Detection is a comprehensive data collection and real-time threat analysis solution with a native threat intelligence feed and native SOAR. The SIEM solution can ingest event data from over 450 different source types, including cloud-based sources. It then correlates the events to detect and direct analysts to cybersecurity threats in real time. With dynamic event risk scoring and prioritization, ArcSight SaaS helps analysts to avoid much of the cost, complexity and extra work associated with false positives. Further supported by native case management and automated response, ArcSight SaaS enables your SecOps team to react quickly and accurately to threat indicators and cyber incidents.

Native SOAR

ArcSight considers Security Orchestration, Automation and Response (SOAR) to be a core part of modern security analytics, and as such provides it as a complementary, native solution. Backed by out-of-the-box playbooks and 120+ integration plugins, OpenText(TM) ArcSight SOAR effectively and efficiently automates and orchestrates triage, investigation, and response activities. It supports visual workflow playbooks, detailed reporting on KPIs, and greater team collaboration through a complete case timeline.

Log Management

ArcSight SaaS makes SIEM log management simple with centralized log analysis tools and hypothesis-driven threat hunting tools to improve threat hunting efficiency. Data can be integrated from a large variety of sources including logs, clickstreams, sensors, stream network traffic, security devices, web servers, custom applications, social media, cloud services and more to improve your data monitoring. Use search and filter capabilities to find exactly what you are looking for to increase the efficacy of threat hunting efforts.

Forensic investigations are made easy with fast on-demand search capabilities within terabytes of data to enable quick and efficient investigation. Optimized for speed, it uses a columnar database reducing time spend waiting for results to load. Search fast, get results faster. ArcSight SaaS also has the capability to run many parallel searches at high speed and to schedule critical searches, so you never lose time while waiting for search results.

ArcSight SaaS provides a statistical analysis method called outlier detection to enhance search and hunt abilities. Outlier detection is an advanced log management capability that enables threat hunters to perform statistical analysis on historical data to find outliers that may indicate potential threats.

Compliance

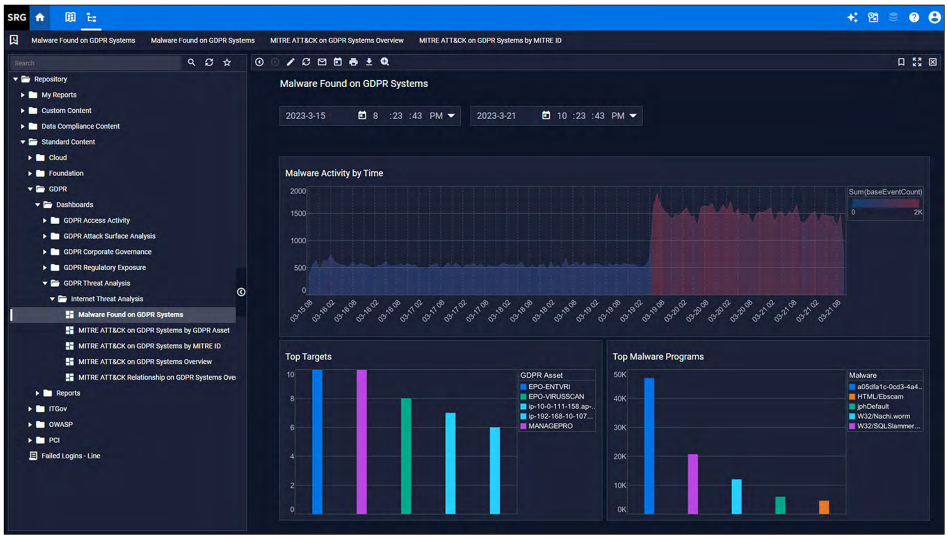
With data regulations worldwide becoming increasing strict, compliance features such as long-term data retention, safeguards for protected data (PII, PHI, HIPAA, GDPR, etc.), and executive reporting are essential to any SIEM. ArcSight SaaS handles compliance with ease with customized data retention schedules and pre-built reports to quickly communicate information to threat hunters and executives alike. Rest assured that when that breach happens, ArcSight SaaS can improve response time to governmental regulations and reduce costs to comply to local laws.

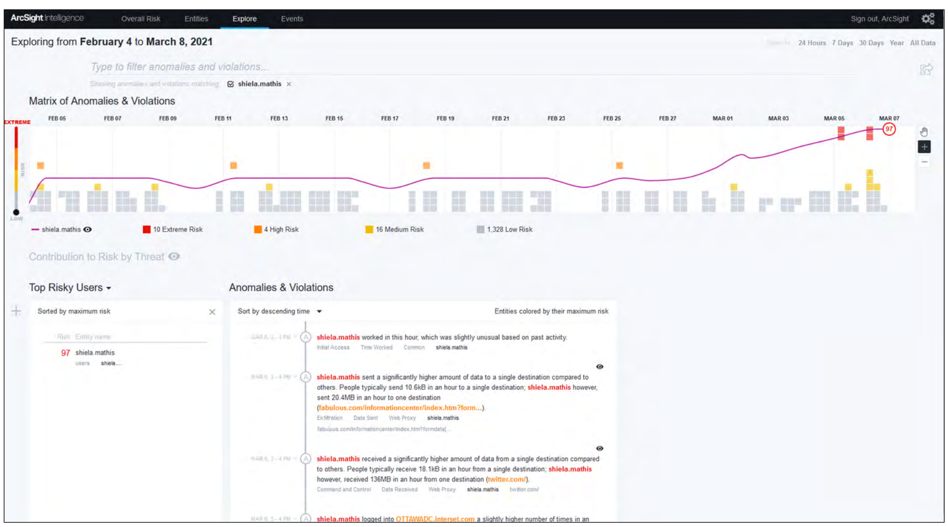
Dashboards and Reports

Intuitive visualizations turn data into actionable insights in ArcSight SaaS with modern dashboards for viewing trends at-a-glance. Enjoy customized visuals and personalized dashboards that can be purpose built for specific use cases including executive reporting, trend analysis, and more.

Behavioral Analytics

Designed to detect even the most subtle of threats, ArcSight SaaS comes with behavioral analytics to enhance your threat detection capabilities, shedding light on elusive threats that often fly under the radar. ArcSight SaaS behavioral analytics is powered by adaptive unsupervised machine learning, a branch of artificial intelligence (AI), that monitors entities on your network such as users, machines, devices, web addresses and more for anomalous behavior that may indicate a breach from outside attackers or malicious insiders.



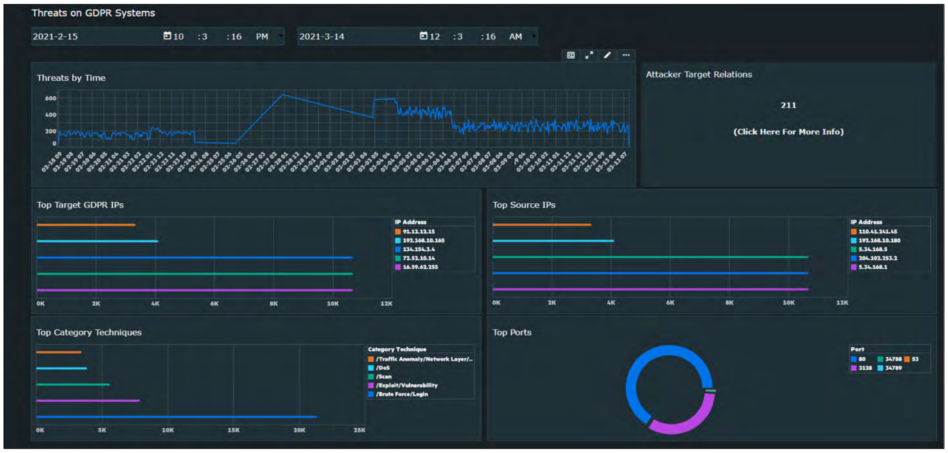


The AI engine powering the behavioral analytics capabilities enables continuous adaptive baselining that improve threat detection effectiveness. Baselining allows ArcSight to compare an individual's normal behavior to how that individual is currently behaving. This comparison between expected norms to current behavior allows ArcSight to surface anomalies that may indicate threats.

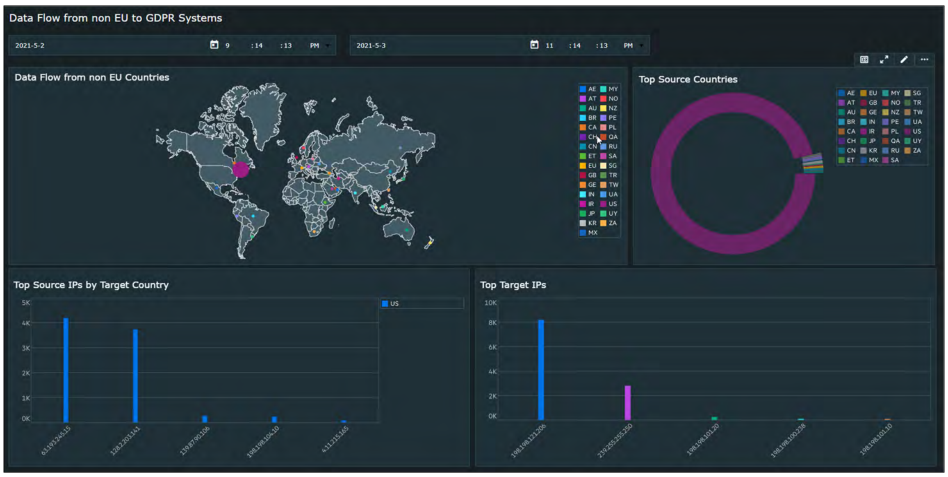
ArcSight SaaS behavioral analytics improves SOC analysts threat hunting efficiency by running automatically on your system, surfacing entities that are exhibiting anomalous behavior that may indicate cyber threats. ArcSight SaaS features explainable machine learning results with clear explanations of why anomalies and threats are raised as potential breaches to speed validation and investigation stages. This in turn improves analyst efficiency and enables them to investigate more potential threats.

Outlier Analytics

ArcSight SaaS contains outlier analytics with tools that enable SOC analysts to analyze data sources for outliers that may indicate unusual or suspicious behavior. While similar to behavioral analytics, outlier detection can be used on a wider array of data sources and is only used on-demand as opposed to being automated. Outlier analytics puts the power of statistics and machine learning in the hands of SOC analysts as they look to uncover lurking threats.



Connect with Us
www.opentext.com



Intelligent Threat Hunting

The capabilities in ArcSight SaaS enable both hypothesis-based and analytics-driven threat hunting to improve threat landscape coverage and threat detection effectiveness. Incredibly fast search and hunt functions enable SOC analysts to perform hypothesis-based threat hunting by looking through security logs and using filtering tools to find indicators of threats. SOC analysts can also leverage modern machine learning through behavioral analytics and outlier analytics to perform analytics-driven threat hunting. Analytics generates quick threat leads that can then be investigated and, if needed, resolved.

Threat Hunting Service

Offered with ArcSight SaaS is a threat hunting service provided by the ArcSight team as a compliment to your existing threat hunting program. This service focuses on finding the most difficult attacks: insider threats and advanced persistent threats using behavioral analytics. With over 50 years of combined experience, the tenured ArcSight threat hunting team has a proven track record of detecting malicious threats that jeopardize the cyber defense of organizations worldwide.

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

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

761-000052-003 | O | 10/23 |