opentext™ | Cybersecurity

Service Flyer

ArcSight SaaS with Real-Time Threat Detection

Empower your SOC team to be cybersecurity heroes that can focus on terminating threats, rather than maintaining hardware. Effortlessly detect and respond to cyberthreats in real-time with ArcSight SaaS.

ArcSight SaaS with Real-Time Threat Detection at a Glance

Detect Threats in Real-Time

Industry leading event correlation that centralizes event log analysis to detect 'known' threats as they appear.

Native SOAR

Enable your team to efficiently respond to threats with automation, playbooks, incident management, SOC analytics, and more.

Native Threat Intelligence

Stay up-to-date on the latest threats with ArcSight's native threat intelligence feed.

Content and Reporting

Backed by MITRE ATT&CK mapping, modular dashboards, hundreds of adjustable correlation rules, and more.

Evolve with ArcSight SaaS

Simplify your SecOps, increase time to value, and reduce infrastructural workloads, onboarding, and education times, with ArcSight SaaS. Let your SOC team be threat hunters; leave system administration behind.

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.

The ArcSight SaaS by OpenText platform provides a no-hassle security experience by eliminating the need to buy, install and manage severs and by simplifying security operations 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. With auto-updates, you and your team can run on the most cutting-edge ArcSight solutions and immediately benefit from their capability enhancements.

ArcSight SaaS is an intelligent, holistic security operations stack with real-time threat detection, SOAR, behavioral analytics, 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, alerts, and automated actions. Backed by 20+ years of experience, ArcSight SaaS enables your Security Operations Center (SOC) with an industry leading SIEM focused on operational efficiency and 360° threat analysis to reduce business risk and streamline your real-time cyber defense.

Streamline Your SecOps with 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 detects and directs analysts to cybersecurity threats in real time, with dynamic event risk scoring and prioritization that help 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 enables your SecOps team to react quickly and accurately to threat indicators and cyber incidents.

Enterprise-Wide Event Visibility

ArcSight SaaS with Real-Time Threat Detection leverages advanced event collection technology through ArcSight's SmartConnectors to consolidate, enrich, and analyze data from over 450 different security event source types. SmartConnectors support every common event format (native Windows and Linux events, APIs, firewall logs, syslog, Netflow, direct database connectivity, etc.). ArcSight also ingests data from the cloud (AWS, Azure, GCP, Microsoft 365, and more). Beyond these, our FlexConnector framework supports the development of custom connectors to facilitate the ingestion and correlation of additional sources. More event sources means more visibility and the ability to develop more complex security use-cases specific to the needs of your organization.

Automated Response with Native SOAR

ArcSight considers 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, 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.

Defend Against the Latest Threats with GTAP Threat Intelligence

Galaxy Threat Acceleration Program (GTAP) Basic is the native threat intelligence feed available to all ArcSight SaaS with Real-Time Threat Detection users through the GTAP SmartConnector. It automatically incorporates threat monitoring content into ArcSight based on open-source threat intelligence data, providing greater coverage against modern threats and campaigns through increased visibility of industry threats. ArcSight also integrates with many third-party and open-source threat intelligence feeds, and offers curated threat intelligence protection through GTAP Plus, ArcSight's premium threat intelligence solution.

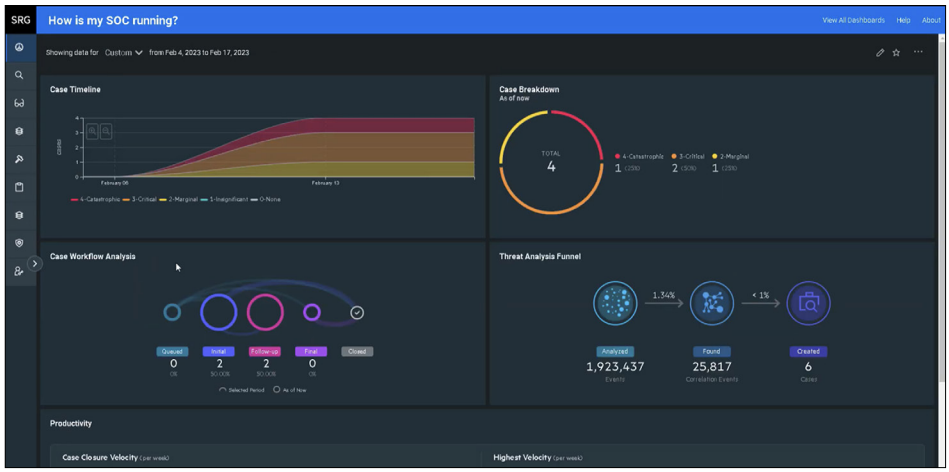

Figure 1. SOC metrics dashboard

Intelligent and Dynamic Event Risk Scoring and Prioritization

ArcSight's unique priority formula for Real-Time Threat Detection consists of criteria that each event is evaluated against to determine its relative importance, or priority, to your network. The calculation incorporates many data points, such as open ports and imported vulnerability scan results from third-party solutions. For example, a given attack might be known to exploit a certain vulnerability. If the targeted system exposes that vulnerability and the attacked port is open on the asset, then ArcSight SaaS can assume that the attack is likely to succeed and will prioritize it.

Hypothesis-Driven Threat Hunting with ArcSight Search

Threat hunting is an analyst-centric process that enables security operations teams to uncover hidden advanced threats. It supplements ArcSight's real-time detection capabilities and expands on the effectiveness of the solution by leveraging a collaboration of people, technology, and process to uncover top-tier attackers. ArcSight SaaS empowers threat hunters by turning data into insights and actions with ArcSight Search, a core component of the platform.

With ArcSight Search, you're enabled to do the following:

- Enjoy the ease of threat hunting with visualizations, fast and detailed search, reports, and dashboards to hunt for threats before damage is done.
- Run many parallel searches at high speed.
- Encourage your teams to adopt exploratory search approaches and creative mindsets.
- Benefit from the advantage of easy-to-use transparent results for decision-making.

Dashboards and Visualizations with ArcSight Reports

ArcSight SaaS comes with 100+ out-of-the-box reports and dashboards, including cloud, OWASP, data modeler, and MITRE ATT&CK. ArcSight's prebuilt and customizable reports and dashboards, available as part of ArcSight Reports (another core component of the ArcSight SaaS platform), enable you to decrease the time needed to visualize and share your security posture, improve your understanding of your security environment, and achieve enterprise-wide threat visibility.

Easier Compliance with ArcSight Reports

Compliance regulations aren't meant to increase the workload of a SOC. They're meant to help organizations improve their security posture. This is why the compliance module for ArcSight SaaS is designed specifically for cybersecurity. ArcSight Reports reduces the pain and complexity of compliance reporting with simple, customizable reports and dashboards. With policy-driven data collection and retention, and out-of-the-box content, it is easy to run efficient compliance reports so your team can be audit-ready at a moment's notice.

Additional Feature Highlights

- **Active Lists**—Dynamic in-memory lists capable of holding millions of entries, these can act as watch lists for monitoring suspicious traffic or behavior, with the ability to use active lists in any correlation rule.
- **Schedule reports**—Automated reporting can prepare reports and deliver results automatically to key stakeholders.
- **ArcSight 360° Analytics Dashboards**—ArcSight's unifying analytics UI connects all components of the ArcSight SaaS platform and supports customizable widget-based dashboards to visualize SOC metrics.

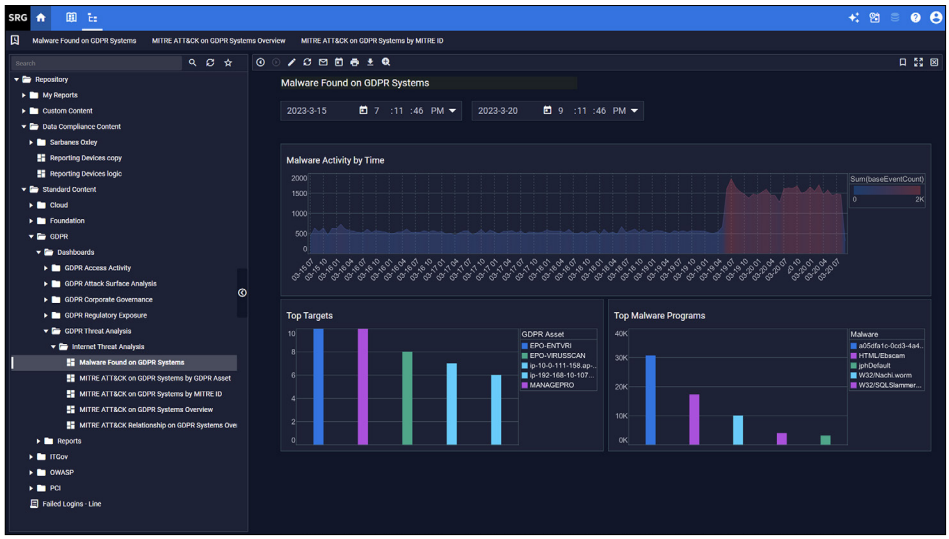

Figure 2. GDPR dashboard within ArcSight Reports

- **MITRE ATT&CK Dashboards**—Get a real-time view of all MITRE ATT&CK related events happening in your environment, the top threat techniques facing your SOC, and a clear image of your organization's ability to detect individual techniques.
- **Data Security**—Protect your data integrity with immutable data storage.

Transition from ArcSight ESM

ArcSight SaaS with Real-Time Detection is the natural successor of ArcSight Enterprise Security Manager (ESM). Thousands of customers have been drawn to ArcSight ESM over the years for its market-leading real-time detection capabilities. But architectural maintenance has always been a necessary evil for SIEM solutions like ArcSight ESM, especially when deployed off-cloud. With ArcSight SaaS, SOC teams can ditch the drawbacks of time-consuming maintenance while maintaining the enterprise-wide threat visibility that ESM users have come to hold dear. Furthermore, ArcSight SaaS comes with native SOAR and enhanced case management and reporting capabilities over what was available with ArcSight ESM.

Why Transition from ESM to ArcSight SaaS?

- **Eliminate** version lag. Benefit from the latest ArcSight SaaS capabilities as they come online.
- **Simplify** migration, by easily exporting/importing your rules and content from ESM to ArcSight SaaS.
- **Alleviate** analyst fatigue with automated response, native threat intelligence, and reduced maintenance.
- **Avoid** capability deficit—ESM, although supported, will no longer receive feature upgrades.

Why ArcSight SaaS?

ArcSight SaaS is a scalable and powerful next-gen SIEM platform that enables security teams to leave behind maintenance and administration so they can focus on their true passion: finding and eliminating threats. The ArcSight SaaS platform is a

Connect with Us
www.CyberRes.com

comprehensive solution developed for security professionals by security experts. It takes a holistic approach to security intelligence, uniquely unifying big data collection, event monitoring, threat detection, and response. Customers are enabled by advanced security analytics technologies, including hunt, investigation, UEBA, SOAR, and real-time detection, to execute a powerful, layered analytics approach to secure their enterprise against modern threats.

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.

761-000100-001 | O | 04/23 |