opentext™ | Cybersecurity

Article

ArcSight's Latest and Greatest

New Features of ArcSight 2023.1

ArcSight 2023.1: Real-Time Detection Takes ArcSight SaaS to the Next Level

General Availability—ArcSight 2023.1 release

OpenText Cybersecurity is excited to announce the availability of OpenText™ ArcSight 2023.1, a historic release that marks the launch of Real-Time Threat Detection on the ArcSight SaaS platform and the start of a new chapter for ArcSight users, who now have the full power of the ArcSight portfolio available to them in a cloud-hosted environment. We are proud to provide cybersecurity teams with one of the market's few truly complete SIEM as a Service (SaaS) solutions, backed by real-time threat detection, SOAR, threat intelligence, behavioral analytics, search, log management and compliance capabilities.

This release comes at a critical time for SOCs (Security Operations Centers). Defending against modern cyberthreats is a major challenge for security teams, who face off against increasingly complex threats while monitoring an ever-expanding attack surface. As the list of potential threats grows longer and the shortage of skilled security professionals continues to take its toll, security teams are seeing their workloads increased as they faithfully strive to limit their organization's threat exposure. And to make things worse, many teams find themselves having to dedicate a significant amount of time and energy to system administration, maintenance, and updates for their security tools.

ArcSight understands these challenges, and with the 2023.1 release, demonstrates its commitment to providing industry-leading security solutions that are responsive to today's ever-changing threat landscape. ArcSight 2023.1 enables you to simplify your security operations and reduce your threat exposure time with real-time detection, native SOAR, enhanced search, new integrations, and more.

By offering real-time threat detection on SaaS, ArcSight advances beyond typical SIEM market offerings to provide you with a truly complete SIEM as a Service solution. The combination of real-time

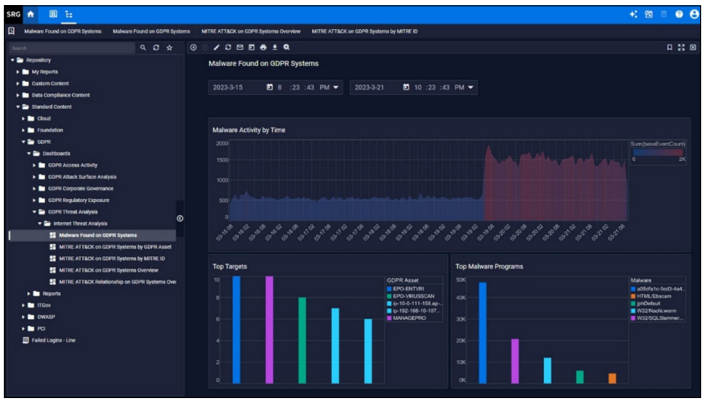

Figure 1. GDPR dashboard within ArcSight SIEM as a Service

detection and automated response enables your security team to quickly detect and respond to known threats, helping you to achieve your mean time to detect (MTTD) and mean time to respond (MTTR) goals and, more importantly, reducing your organization's overall cyber risk and threat exposure.

With OpenText™ ArcSight SaaS, the security operations experience is simplified by eliminating the need to buy, install, and manage servers. With infrastructural workloads, maintenance, and learning curves reduced through SIEM as a Service, your team of analysts gets their time back so they can focus on being the efficient threat hunters and cybersecurity heroes they long to be.

Backed by 20 years of experience in the SIEM space, ArcSight is proud to provide you and your team with a portfolio of cutting-edge solutions, fully deployable on both SaaS and off-cloud environments, that empower your team to tackle modern threats with 360° threat analysis and streamlined real-time cyber defense.

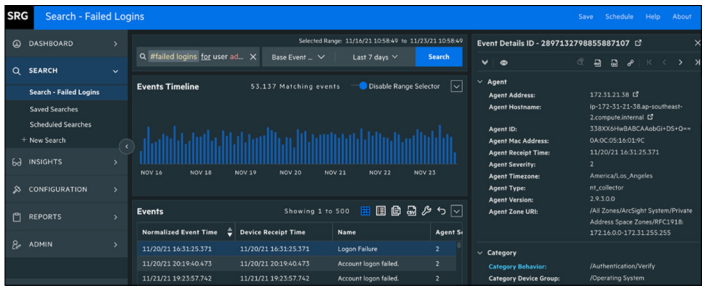

Figure 2. ArcSight SIEM as a Service event detail panel

ArcSight SaaS Real-Time Threat Detection

Responding to threats with speed and efficiency is essential to security operations. 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 Real-Time Detection acts as a comprehensive data collection and real-time threat analysis solution to alert SOC analysts to known threats as they occur. Backed by native SOAR (more on that below) and a native threat intelligence feed (GTAP) that provides up-to-date information on the latest threats and malicious campaigns, OpenText™ ArcSight SaaS Real-Time Threat Detection enables security teams to react quickly and accurately to threat indicators and cyber incidents before damage is done. Dynamic event risk scoring and prioritization help analysts to avoid false positives and focus on the highest-priority threats. ArcSight SaaS Real-Time Threat Detection also enables organizations with enhanced threat visibility, dashboards, compliance support, MITRE ATT&CK integration, and more, to provide them with a clearer view of their security posture.

ArcSight SaaS Real-Time Threat Detection is the natural successor of OpenText™ ArcSight Enterprise Security Manager (ESM). For years, ArcSight users have benefited from ESM's market-leading real-time detection capabilities in off-cloud environments where architectural maintenance is an unfortunate necessity. With the launch of Real-Time Threat Detection on 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. Additionally, ArcSight SaaS delivers enhanced reporting and case management capabilities, and opens the door for further SIEM enhancements moving into the future.

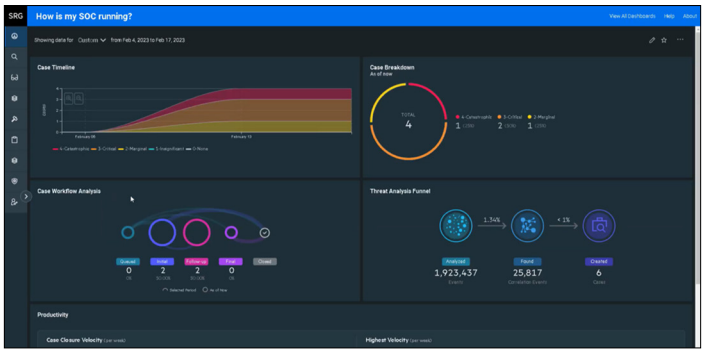

Figure 3. SOC Metrics dashboard within Real-Time Threat Detection

ArcSight SaaS SOAR

OpenText™ Security Orchestration, Automation, and Response (SOAR) is an essential aspect of modern security analytics as it enables organizations to respond to threats swiftly and cohesively. It is critical to efficient security operations as it reduces false positives, automates response, and facilitates team collaboration.

Since the launch of ArcSight SOAR (off-cloud) in 2020, ArcSight has provided SOAR as a complementary, native solution. And in December 2022, ArcSight brought its SOAR to the SaaS world, as a native component of the ArcSight SaaS platform. With 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 detailed case timeline.

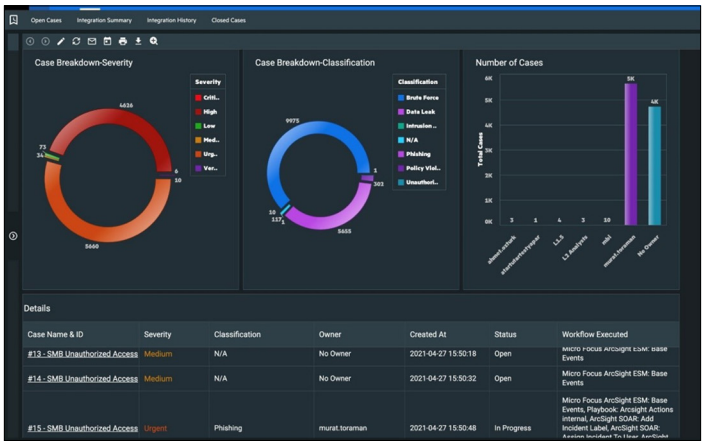

Figure 4. ArcSight SOAR reports and dashboards

SOAR is closely aligned with Real-Time Threat Detection and will handle all case management and automated response for the OpenText™ ArcSight SaaS platform. By detecting threats in real-time, prioritizing the riskiest threats, and then turning SOAR lose on those threats with automated response and a coordinated team effort, ArcSight reduces threat exposure while enhancing operational efficiency.

Latest ArcSight News and Recognitions

- Press Release: ArcSight Closes Out 2022 Strong with Solid Ratings and Innovation News
- ArcSight Recognized as Leader and Fast Mover in GigaOm Radar for SIEM
- ArcSight Scores 10/10 in this Competitive Benchmark Evaluation Focused on MITRE ATT&CK

ArcSight 2023.1 features new releases of:

- ArcSight SIEM as a Service (SaaS)
- OpenText™ ArcSight Platform 23.1
- OpenText™ ArcSight ESM 7.6.4
- OpenText™ ArcSight Intelligence 6.4.4
- OpenText™ ArcSight Recon 1.5.1
- ArcSight SOAR 3.5
- OpenText™ ArcSight GTAP 2.0
- OpenText™ Transformation Hub 3.7
- OpenText™ ArcSight Management Center 3.2
- OpenText™ ArcSight SmartConnectors 8.4.1
- OpenText™ ArcSight Logger 7.2.2

The key features and improvements of our ArcSight 2023.1 release are listed below. Please refer to the individual release documentation *(cited at the end of this article)* for more complete information.

Release Highlights for ArcSight SIEM as a Service (SaaS)

Real-Time Threat Detection

KEY HIGHLIGHTS

- **Streamline real-time threat detection** by alerting analysts to threat-correlated events as they appear, leveraging ArcSight's market-leading correlation technology.
- **Dynamic risk scoring and prioritizatio**n enable your analysts to focus on the highest-risk threats first, while shutting down false positives.
- **Native SOAR** through the ArcSight SaaS Core Platform facilitates automated response, playbooks, SOC analytics, and more.
- **Advanced case management** through SOAR integration.
- **Enhanced reporting** with 100+ pre-built and customizable reports and dashboards that help to visualize your security posture.
- **Efficient compliance module** reduces the burden on your compliance team in addressing regulatory requirements.
- **Search and Hunt capabilities** extend the reach of your real-time threat detection team and complement the core real-time detection functionality of the solution.

SOAR

KEY HIGHLIGHTS

- **The introduction of SOAR capabilities** within the ArcSight SIEM as a Service (SaaS) base platform offering. This enables every ArcSight SaaS customer to enjoy the benefits of automated triage, investigation and response without an additional license or fee.
- **New integration plugins** focused on the following areas:
  - **Endpoint Protection/EDRs:** Microsoft Defender for Endpoints, CrowdStrike
  - **Threat Intelligence Databases:** CyberRes Galaxy, FraudGuard, Intezer
  - **Cloud Services:** AWS Network FW, Azure Security Groups, AWS Lambda
- **Integrations with Microsoft Teams and Slack** to support ChatOps and include non-SOC organizational units and end users in investigation and response activities.
- **Productivity and Case Load dashboard widgets** provide visibility around analyst teams' workloads and performance.
- **Coming Soon:** Additional integrations with SentinelOne EDR, Microsoft Defender for Cloud Apps, BMC Helix Remedyforce, Sailpoint, Domaintools, Netskope, and Cisco Umbrella

Log Management and Compliance

KEY HIGHLIGHTS

- **Tamper-resistant event storage** enforces the immutability of events once they are received from data sources.
- **New search operators** such as 'wheresql' provide powerful threat hunting capabilities for complex searches.
- **Search operator chaining** allows for the construction of a complex query statement by chaining together multiple search operators into a single query instead of implementing separate queries.
- **Enhanced search capabilities** that provide analysts with more options to view data, e.g., linear or log scale; the ability to drill down on matching events by clicking on a histogram bar; the ability to select an event and open the event inspector, etc.

- **The Search Home tab** provides a high-level view of your search activity providing a list of all your session (non-saved) searches as well as widgets that show the state of saved search queries, saved search criteria, saved search results, field sets, and lookup lists.
- **Data Processing Monitoring dashboard** that contains a Database Event Ingestion Timeline widget useful for monitoring the rate of event ingestion into the database.

Behavioral Analytics

KEY HIGHLIGHTS

- **Data ingest** optimizations.
- **Security updates** to address potential vulnerabilities.
- **General bug fixes**.

ArcSight GTAP Basic 2.0 (Released November 2022)

KEY HIGHLIGHTS

- **No additional charge** for ArcSight customers; allows you to get coverage with a base-level of threat intelligence content.
- **Plug and play SmartConnector** makes it easy to get started with threat intelligence.
- **Automated response via SOAR** means less work for your analysts after threat intelligence is implemented.

ArcSight GTAP+ 2.0 (Released November 2022)

KEY HIGHLIGHTS

- **Premium threat intelligence** curated by the OpenText Galaxy team helps you make better-informed decisions with more concrete information.
- **Richer threat intelligence** gives you 30+ enrichment fields to provide granular context of individual threats in the feed.
- **Auto-blocking** high-confidence IoCs to reduce busywork for your analysts, and provide instantaneous coverage.
- **Plug and play SmartConnector** makes it easy to get started with threat intelligence.
- **Automated response via SOAR** means less work for your analysts once threat intelligence is implemented.

Release Highlights for the ArcSight Platform (On-Prem/Off-Cloud)

ArcSight ESM 7.6.4

KEY HIGHLIGHTS

- **Currency updates** to Java, SQL, Kafka, and OS.
- **Stability, security, and performance** enhancements.
- **General bug fixes**.

ArcSight Intelligence 6.4.4

KEY HIGHLIGHTS

- **Security** enhancements.
- **General bug fixes**.

ArcSight Recon 1.5.1

KEY HIGHLIGHTS

- **Tamper-resistant Event Storage** enforces the immutability of events once they are received from data sources.
- **New search operators** such as 'wheresql' provide powerful threat hunting capabilities for complex searches.
- **Search operator chaining** allows for the construction of a complex query statement by chaining together multiple search operators into a single query instead of implementing separate queries.
- **Enhanced search capabilities** that provide analysts with more options to view data, e.g., linear or log scale; the ability to drill down on matching events by clicking on a histogram bar; the ability to select an event and open the event inspector, etc.
- **The Search Home tab** provides a high-level view of your search activity providing a list of all your session (non-saved) searches as well as widgets that show the state of saved search queries, saved search criteria, saved search results, field sets, and lookup lists.
- **Data Processing Monitoring dashboard** that contains a Database Event Ingestion Timeline widget useful for monitoring the rate of event ingestion into the database.

ArcSight SOAR 3.5

KEY HIGHLIGHTS

- **New Integration Plugins for SOAR:**
  - **CyberRes Galaxy Threat Accelerator** plugin for enriching IP addresses, domains, files, and URLs from the OpenText Galaxy threat intelligence database.
  - **Microsoft Defender for Endpoint** plugin for stopping attacks, isolating machines from network, searching and managing Defender alerts.
  - **CrowdStrike Falcon Integration** plugin for searching IOCs across the network and isolating suspicious endpoints from the network.
  - **AWS Network Firewall** plugin for managing AWS network firewall policies and rules as part of threat response.
  - **Azure Network Security Groups** plugin for managing Azure network security groups and rules as part of response activities.
  - **Intezer Malware Analysis** plugin for analyzing suspicious files on Intezer Malware analysis service.

  - **FraudGuard** plugin for managing custom blacklists & whitelists and querying reputation scores from FraudGuard.io.
  - **AWS Lambda Integration** plugin for invoking Lambda functions on customer cloud environments.
- **Plugin improvements** for Okta, Azure Active Directory and McAfee Web Gateway integration plugins facilitate device-related enrichments and actions, permission listings, group actions, and version compatibility.
- **Productivity and Case Load dashboard widgets** provide visibility around analyst teams' workloads and performance.

ArcSight GTAP Basic 2.0 and GTAP+ 2.0 (Released November 2022)

KEY HIGHLIGHTS

- See GTAP notes from the ArcSight SIEM as a Service section.

ArcSight Transformation Hub 3.7

KEY HIGHLIGHTS

- Performance improvements and minor bug fixes.
- Detailed documentation available here.

ArcSight Management Center 3.2

KEY HIGHLIGHTS

- Performance improvements and minor bug fixes.
- Detailed documentation available here.

ArcSight SmartConnectors 8.4.1

KEY HIGHLIGHTS

- Performance improvements and minor bug fixes.
- Detailed documentation available here.

ArcSight Logger 7.2.2

KEY HIGHLIGHTS

- **Maintenance release** addressing security vulnerabilities and other issues found in Logger 7.2.1.
- **Exporting search events** is processed 8.42 times faster when compared to the previous release.
- **Time synchronization** is now handled by NTP instead of Chrony. This improvement, previously released as a standalone patch, is now integrated into the product.
- **Coming Soon: Logger 7.3**, focused on security vulnerability fixes, OBC updates, and library updates.

ArcSight Documentation

User Guides, Release Notes, and More

- ArcSight SIEM as a Service (SaaS) 23.3.1
- ArcSight Platform 23.1
- ArcSight ESM 7.6.4
- ArcSight Intelligence 6.4.4
- ArcSight Recon 1.5.1
- ArcSight SOAR 3.5
- ArcSight GTAP 2.0
- Transformation Hub 3.7
- ArcSight Management Center 3.2
- ArcSight SmartConnectors 8.4.1
- ArcSight Logger 7.2.2

Is Your ArcSight Version up to Date?

Product Name	Newest Version
ArcSight SIEM as a Service	Always updated
ArcSight Platform	23.1
ArcSight ESM	7.6.4
ArcSight Intelligence	6.4.4
ArcSight Recon	1.5.1
ArcSight SOAR	3.5
ArcSight GTAP	2.0
ArcSight Transformation Hub	3.7
ArcSight Management Center	3.2
ArcSight SmartConnectors	8.4.1
ArcSight Logger	7.2.2

Learn more at
www.arcsight.com

Connect with Us

www.CyberRes.com

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.

772-000001-008 | O | 04/23 | © 2023 Open Text