ArcSight’s Latest and Greatest

New Features of ArcSight 2020.3 Release
ArcSight 2020.3: Simplifying Your SOC with SOAR, SaaS, and a Silent Installer

ArcSight is an automated, proactive end-to-end security operations solution that enables SOCs to intelligently adapt to talent shortages by elevating productivity. ArcSight 2020 offers faster, more accurate threat detection with layered analytics, while driving down total cost of ownership.

General Availability—ArcSight 2020.3
We are excited to announce the general availability of ArcSight 2020.3! ArcSight has made incredible strides in 2020 to help security teams like yours reduce their threat exposure and establish a cyber resilient SOC. The 2020.3 release delivers more resilient, faster, and broader end-to-end detection and response to threats across cloud, on-premises, and SaaS deployments.

The acquisition and integration of SOAR into the ArcSight family fills a key role in ArcSight’s end-to-end security operations offering, adding valuable orchestration, automation and response capabilities to ArcSight’s powerful layered analytics. With this new release, SOAR has been added as a native component to both ESM and Recon, at no additional charge.

Also essential to this release is the introduction of ArcSight’s first SaaS solution announced on October 30, 2020. Micro Focus launched ArcSight Intelligence as a Service to simplify adoption and management of behavioral analytics, with minimal barriers to entry. ArcSight Intelligence (previously "ArcSight Interset") works closely with ArcSight ESM, and as a SaaS it provides SIEM customers with an easy way to pair behavioral analytics with real-time correlation.

This release greatly simplifies ArcSight installation and deployment. A new silent install for containerized deployments installs and configures OS, storage and other prerequisites. It supports both simple single-node and highly available multi-node deployment of ArcSight Intelligence, ArcSight Recon, ArcSight Fusion, and Transformation Hub, based on simple, easy to understand deployment templates.

ArcSight 2020.3 features the releases of ArcSight SOAR 3.0, ArcSight Intelligence SaaS and 6.2, ArcSight ESM 7.4, ArcSight Fusion 1.2, ArcSight Recon 1.1, Transformation Hub 3.4, ArcMC 2.9.6, ArcSight SmartConnectors 8.1, and ArcSight Logger 7.1.1. The key features and improvements of our third ArcSight 2020 release are listed below. Please refer to the individual release notes (cited in this document) for more complete information.

Platform Highlights
- Automate responses to recognized threats in real-time via native SOAR capabilities offered with ArcSight ESM and ArcSight Recon.
- Deploy ArcSight components in the cloud natively, leveraging native Amazon Web Services and Microsoft Azure services, enabling you to reduce TCO and optimize infrastructure footprint.
- Gain enhanced insights with new integrations that pair behavioral analytics from ArcSight Intelligence (previously ArcSight Interset) with real-time correlation from ArcSight ESM.
- Deploy ArcSight with greater ease using the new silent installer for ArcSight’s containerized products. Supporting both simple single-node deployment, and highly available multi-node deployment of ArcSight Intelligence, ArcSight Recon, ArcSight Fusion, and Transformation Hub, it performs pre- and post-deployment checks and remediates prerequisites.
- Upgrade ArcSight with no downtime by performing rolling upgrades through the Master and Worker nodes in clusters of containerized products. Clusters deployed in highly available configurations continue to process events throughout the upgrade.
Access information more easily with new online documentation that supplements the traditional PDF guides and enables searching for relevant topics. Installation, configuration and administration of all containerized products is now covered by the new Administrator’s Guide for the ArcSight Platform.

Save resources with smaller deployment footprints. Avro- formatted event data is now supported across all ArcSight components, eliminating disk storage duplication, and reducing network transfer and compute overhead.

Navigate the UI more seamlessly with continued integration of the recently introduced ArcSight unified interface, called Fusion, by ArcSight components such as ESM, SOAR, Intelligence and Recon.

Benefit from up-to-date and secure underlying components. The platform has been certified on Red Hat Enterprise Linux 8.2, CentOS 8.2, with current releases of Java runtime, Kubernetes, Docker, CDF, PostgreSQL, Apache Kafka Client, Apache Tomcat, and the Confluent platform (which includes Apache Kafka, Schema Registry and ZooKeeper). Component libraries include current vulnerability compliance, and ciphers are up-to-date.

Component Highlights
ArcSight SOAR 3.0

ArcSight SOAR connects people, processes, and technology to help security engineers run day-to-day security operations efficiently. By providing tactical automation and orchestration through a single pane of glass, it enables SecOps teams to ramp up their output despite a growing cyber skills gap and an increasing volume of complex attacks and alerts.

Key Highlights
- Unified look and feel with ArcSight and single sign-on through Fusion
- Full and semi automation of incident creation, triage, investigation, and response activities orchestrate the machine and human elements from an intuitive interface
- Scenario and playbook automation can be customized to efficiently address your SOC’s unique needs with workflows and automation bits written in Python language
- Incident Management Service Desk provides faster, more collaborative incident response, and increases analyst efficiency
- Customizable case management of incident fields, severity, classification, and UI
- 110+ integration plugins from 70+ vendors for centralized investigation and response activities from a single pane of glass, eliminating the need to switch between tools
- Task delegation and precise access control allows both lower and higher-level analysts to work on sensitive tasks safely and seamlessly
- Detailed incident timeline records and visualizes incidents while promoting accountability and collaboration in an easy-to-understand visualization
- KPI monitoring records SLAs, workloads, analyst activities and automated operations, and reports them in ArcSight’s shared Fusion interface
- Deploy with greater ease using the new silent installer, which performs pre- and post-deployment checks, remediates prerequisites, and supports both single-node and multi-node deployment
- No additional license fee for ESM and Recon customers

ArcSight Intelligence SaaS
ArcSight Intelligence evolves to meet your enterprise’s growing threat needs by simplifying adoption of behavioral analytics via a SaaS deployment model. This release reduces and optimizes resource requirements from prior releases. With multiple integration points into ArcSight,
gain ingest flexibility for seamless integration and threat coverage. The ArcSight Intelligence SaaS offering provides a simplified service initiative to minimize exposure by reducing your enterprise’s attack surface.

**Key Highlights**

- **Avoid heavy resource requirements** typically associated with SaaS analytics implementations
- **Quicker time to value** with seamless integration points into existing ArcSight solutions
- **Broad event source coverage** provided by well-known SmartConnectors
- **Detect threats in real-time** through seamless integration with ArcSight’s real-time correlation engine and auto-populated Active Lists with analytics results
- **Threat-based risk scores** rank entity-specific threats using configurable rules

**ArcSight Intelligence 6.2** *(previously ArcSight Interset)*

**Key Highlights**

- **Support for additional Connectors** allowing analytics to be performed on events from additional VPNs and introducing support for repositories
- **Fusion** is now accessible from ArcSight Intelligence, easing navigation between the two tools for an improved analyst experience
- **Deploy with greater ease** using the new silent installer which performs pre- and post-deployment checks, remediates prerequisites, and supports both single-node and multi-node deployment

**ArcSight ESM 7.4**

**Key Highlights**

- **ArcSight SOAR** is now a native solution within ESM, pairing real-time detection with automated threat response
- **New MITRE ATT&CK dashboard** visualizes your organization’s ability to detect MITRE ATT&CK techniques, to clearly convey where your organization is covered and, more importantly, where it’s not
- **Web-based Command Center expands Active List visibility** beyond the ArcSight Console, allowing your security team to more easily monitor users and/or systems flagged by ArcSight’s correlation engine

**ArcSight Fusion 1.2**

**Key Highlights**

- **ArcSight SOAR integration** enables users to access SOAR through Fusion (and vice-versa)
- **ArcSight Intelligence** is now accessible from Fusion, easing navigation between the two tools for an improved analyst experience
- **Deploy with greater ease** using the new silent installer which performs pre- and post-deployment checks, remediates prerequisites, and supports both single-node and multi-node deployment

**ArcSight Recon 1.1**

**Key Highlights**

- **ArcSight SOAR** has been added as a native solution within Recon, pairing threat-hunting with automated threat response
- **Improved event details** include unique sharable event URLs, export options, integration with “nslookup” and “whois”, and the ability to select field values to search for similar events
- **New user preferences** for search parameters, display formats and limits
- **Independent retention periods per storage group** for up to 10 groups, allows sets of logs to be retained for different periods and improves search performance
- **Deploy with greater ease** using the new silent installer which performs pre- and post-deployment checks, remediates prerequisites, and supports both single-node and multi-node deployment

**Transformation Hub 3.4**

**Key Highlights**

- **Cloud-native deployment** to leverage AWS cloud services
- **Unified storage support** for high-performance SmartConnectors and event routing
- **Updated libraries** for RHEL and CentOS, Azul Java, PostgreSQL, Apache Kafka Client, and the Confluent Platform
Deploy with greater ease using the new silent installer which performs pre- and post-deployment checks, remediates prerequisites, and supports both single-node and multi-node deployment.

ArcSight Management Center 2.9.6

Key Highlights
- Host status exceptions dashboard shows fatal, critical and warning exceptions
- Device status report export option for locally cached status data
- Cloud-native T-Hub deployment and configuration in AWS
- Updated libraries for RHEL and CentOS, Azul Java, Apache Tomcat

ArcSight SmartConnectors 8.1

Key Highlights
- SmartConnector improvements increase throughput for all event formats
- Enhanced AWS support for Security Hub and S3
- New SmartConnectors for OKTA
- New FlexConnectors for Microsoft Threat Protector (MTP), Microsot 365 Defender
- Azure support for Security Center

ArcSight Logger 7.1.1

Key Highlights
- Maintenance release to enhance security and performance of Logger software

ArcSight Documentation

Release Notes
- ArcSight Platform 20.11
- ArcSight ESM 7.4
- ArcSight Intelligence 6.2
- ArcSight Recon 1.1
- ArcSight SOAR 3.0

ArcSight Fusion 1.2
- Transformation Hub 3.4
- ArcSight Management Center 2.9.6
- ArcSight SmartConnectors 8.1
- ArcSight Logger 7.1.1

Is Your ArcSight Version Up to Date?

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Newest Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ArcSight ESM</td>
<td>7.4</td>
</tr>
<tr>
<td>ArcSight Intelligence (ArcSight Interset)</td>
<td>6.2</td>
</tr>
<tr>
<td>ArcSight Recon</td>
<td>1.1</td>
</tr>
<tr>
<td>ArcSight SOAR</td>
<td>3.0</td>
</tr>
<tr>
<td>ArcSight Fusion</td>
<td>1.2</td>
</tr>
<tr>
<td>ArcSight Logger</td>
<td>7.1.1</td>
</tr>
<tr>
<td>ArcSight Investigate</td>
<td>3.1</td>
</tr>
<tr>
<td>Transformation Hub</td>
<td>3.4</td>
</tr>
<tr>
<td>ArcSight Management Center</td>
<td>2.9.6</td>
</tr>
<tr>
<td>ArcSight SmartConnectors</td>
<td>8.1</td>
</tr>
</tbody>
</table>

Watch our on-demand webinar Wrapping up ArcSight 2020, where ArcSight Director of Product Management Michael Mychalczuk goes over the key takeaways of ArcSight 2020.3, including the importance of SaaS and SOAR in your security toolkit. He also reflects on the progress made during 2020 to deliver a truly end-to-end SecOps solution, before touching on the future of ArcSight and its ability to help your organization achieve true cyber resilience.

Learn more at www.microfocus.com/secops