ArcSight’s Latest and Greatest

New Features of ArcSight 2020.3 Release
ArcSight 2020.3: Simplifying Your SOC with SOAR, SaaS, and CDF

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

With the close of 2020, we are excited to announce the general availability of ArcSight 2020.3! This year, ArcSight has made incredible strides to help security teams like yours reduce their threat exposure and establish a cyber resilient SOC. The 2020.3 release delivers on this goal by simplifying your security operations through SaaS, SOAR, and CDF.

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. ArcSight SOAR’s integrations with ArcSight ESM prior to acquisition significantly accelerated the assimilation of SOAR capabilities within ArcSight, enhancing user experience and streamlining processes. With this new release, SOAR has been added as a native component to both ESM and Recon, at no additional charge.

The next key aspect of this release is the announcement of ArcSight’s first SaaS solution. On October 30, 2020, Micro Focus launched ArcSight Intelligence as a Service to simplify adoption and management of behavioral analytics, with minimal barrier to entry. ArcSight Intelligence as a Service works closely with ArcSight ESM and provides SIEM customers with an easy way to pair behavioral analytics with real-time correlation.

It’s also worth noting that updates to ArcSight’s hybrid deployment capabilities have come with this release, for both running in, and monitoring events from, popular cloud platforms such as AWS and Azure.

Finally, another central theme of this release is ArcSight’s advancements in simplifying installation and deployment. With ArcSight 2020.3 you can install in minutes, configure in hours, and achieve value in days. A new silent install via containerized deployment (CDF) installs and configures OS, storage and other prerequisites, and performs pre- and post-deployment evaluations. It supports both simple, single-node deployment, and multi-node, high-availability deployment of ArcSight Intelligence, ArcSight Recon, ArcSight Fusion, and Transformation Hub.

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, and ArcSight SmartConnectors 8.1. Below are listed the key features and improvements of our third ArcSight 2020 release. Please refer to the individual release notes (cited in this document) for more complete information.
analyst augmentation, collaborative investigation and response through an intuitive interface.

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

**Key Highlights**
- **Unified look and feel** with ArcSight and single sign-on through Fusion
- **Full and semi automation** of incident creation, triage, investigation, response, etc.
- **Scenario and playbook automation** can be customized to efficiently address your SOC’s unique needs
- **Collaborative incident response** for faster reaction and increased efficiency
- **Customizable case management** of incident fields, severity, classification, and UI
- **110+ integration plugins** from 70+ vendors for centralized investigation and response, without needing to move between tools
- **Task delegation** allows teammates with lower access levels to safely work on cases
- **Detailed incident timeline** records and visualizes incidents while promoting accountability and collaboration
- **KPI monitoring** of SLAs, workloads, analyst activities and automated operations
- **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 the adoption of behavioral analytics via SaaS. This release removes heavy resource requirements for on-premise delivery so you can gain the power of ArcSight Intelligence with ease. With known 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**
- **Removed heavy resource requirements** associated with analytics solutions with SaaS implementation
- **Decreased time to value** with multiple integration points into existing ArcSight solutions
- **Ingest flexibility** with well-known SmartConnector library for CEF support
- **Seamless integration** with ArcSight’s real-time correlation engine and auto-populated Active Lists with analytics results
- **Flexible content** with configurable rules to identify a variety of Entities based on Risk score

**ArcSight Intelligence 6.2**

**Key Highlights**
- **Additional data sources for ingestion** with enhanced satisfaction of potential use cases
- **Integration with Fusion UI** for easier analyst navigation through a single-pane-of-glass
- **Streamlined data ingestion** that eliminates the storage duplication and compute overhead. This enables smaller footprint deployments to save on investment and resources

**ArcSight ESM 7.4**

**Key Highlights**
- **ArcSight SOAR** has been added as 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 more clearly convey where your organization is covered (and where it’s not)
- **Active list visibility** expands beyond the ArcSight Console to the web-based ArcSight Command Center, allowing your security team to more easily monitor any users and/or systems flagged by ArcSight’s correlation engine
- **Event Throughput dashboard** now includes Pre-Aggregation EPS details
- **Performance improvements** to lists, including enhanced diagnostics, optimization choices, and more
ArcSight Fusion 1.2

Key Highlights
- Integration with ArcSight SOAR enables users to access SOAR through Fusion (and vice-versa)
- ArcSight Intelligence is also now accessible from Fusion (and vice-versa), further facilitating layered analysis through a single interface point
- Container deployment of Fusion via CDF allows for simplified installation and deployment (both multi-node and single-node)

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
- User preferences for search parameters, display formats and limits
- Storage group support for up to 10 groups, with a retention period per group
- Simplified deployment for both multi-node and all-in-one form factors

Transformation Hub 3.4

Key Highlights
- Cloud-native deployment to leverage AWS cloud services
- Simplified deployment for multi-node clusters, for both CDF and Vertica clusters
- 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

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
- Avro routing enhancements allow events to be forwarded and consumed from ESM or Logger
- Updated libraries for RHEL and CentOS, Azul Java, Apache Tomcat

ArcSight SmartConnectors 8.1

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

ArcSight Logger 7.1 (ArcSight 2020.2)

Key Highlights
- Enhanced search UI provides a new navbar, exporting, field summary and saved searches
- Persisted search results that can be loaded on UI for monitoring
- Definable Logger Roles allow administrators to tune Logger resources based on role
- Logger peer monitoring enables editing of Logger peer status for searches
- Data forwarding to Transformation Hub and other Kafka-based message buses
- Cloud integration allows Logger to forward data to AWS for archiving
- RHEL 8.1 is supported
- Updated libraries for MySQL, PostgreSQL
- Unified platform updates to enable routing, filtering and storage for all ArcSight products
- Storage Improvements for more data in the same disk space

ArcSight Documentation

Release Notes
- ArcSight ESM 7.4
- ArcSight Intelligence 6.2
- ArcSight Recon 1.1
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](http://www.microfocus.com/secops)