ArcSight's Latest and Greatest

New Features of ArcSight 2020.2 Release

www.microfocus.com

Article

Security

ArcSight 2020.2: Culminating 20 Years in SIEM with Layered Analytics and a Unified Platform

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 2020.2

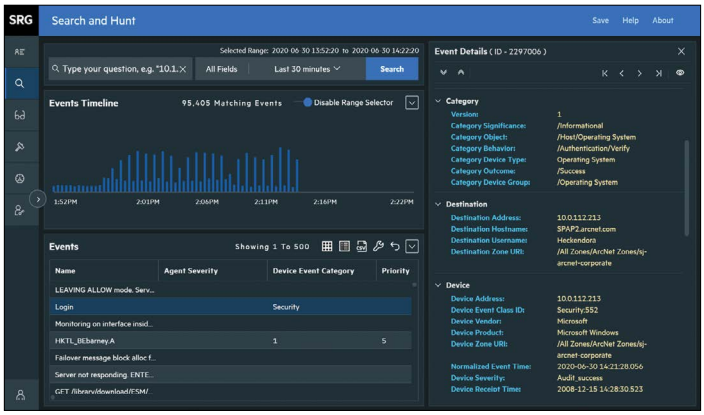
We are excited to announce the general availability of our Micro Focus ArcSight 2020.2 release! After 20 years in the SIEM space, ArcSight has evolved into a single, Intelligent SOC platform that delivers real-time correlation, behavioral analytics, and advanced threat hunting. This release marks a significant accomplishment in our mission to make SecOps more **simple**, **open** and **intelligent**.

ArcSight 2020.2 offers SOCs a **simple** approach through a holistic SecOps platform benefiting from a shared UI and a unified storage solution. ArcSight Recon, our new threat hunting and log management solution, consolidates the collection and storage of security event data into a single repository that can be used for all your SecOps needs. Recon joins ESM and Interset on Fusion, our new ArcSight UI. Further, Interset's new release marks its first general availability within the ArcSight family, and fully integrates the behavioral analytics solution into the ArcSight architecture.

Our team works tirelessly to provide a solution that is **open** to your ever-expanding security environment. Cloud integration in particular has been greatly expanded in this release, ArcSight now features cloud-native deployments and enhanced support for Microsoft Azure and AWS.

ArcSight continues to improve the **intelligence** of its layered analytics by combining machine learning, correlation, and powerful threat hunting. With its intuitive interface and unified platform, ArcSight improves your SOC's ability to find and react to threats in your organization.

ArcSight 2020.2 features the releases of ArcSight Recon 1.0 (Next generation Logging/Investigate solution), ArcSight Interset 6.1, ArcSight ESM 7.3, ArcSight Fusion 1.1 (our new UI), ArcSight Logger 7.1, Transformation Hub 3.3, ArcMC 2.9.5 and SmartConnectors 8.0. Below are listed the key features and improvements of our second ArcSight 2020 release. Please refer to the individual release notes (cited in this document) for more complete information.



ArcSight Recon 1.0

ArcSight Recon is a comprehensive log management and search solution that eases compliance burdens and accelerates forensic investigation for security professionals. It combines the compliance, storage and reporting needs of log management with the capabilities of big-data

search and analysis. Recon is built for security event logs and is therefore more intuitive and accessible for security analysts, it won't require a DBA to operate. It helps hunt and defeat threats by unifying data logs from across organizations, processing billions of events, and quickly making them available for search, visualization and reporting. Recon helps SOC analysts gain a deeper understanding of alerts across their organization and plays an important role in ArcSight's mission to deliver powerful layered analytics.

Key Highlights

- **User-friendly search** displays grid or message views, time-based histogram, dynamic query suggestions and search time horizons, UI dark theme, and syntax highlighting
- **Raw message view** allows analysts to inspect original, unformatted event logs
- **Event detail panel** allows detail inspection for selected events
- **Unified platform** updates to enable routing, filtering and storage for all ArcSight products
- **Reporting content packages** to create, edit and publish reports
- **MITRE ATT&CK reports** are available as pre-built content
- **Outlier detection** visualizes deviations from baseline host behavior metrics
- **Single ID** and password to access all products within the ArcSight suite

ArcSight Interset 6.1

This release provides unmatched visibilty with a layered analytics approach through ArcSight architecture alignment including analytical engine, storage, and data movement components. This release allows customers to have an easier path to adding in the complete set of Interset capabilities, which are complimentary to ArcSight's real-time correlation engine. There have been multiple improvements to performance focused around more efficient results, and simplified deployment through a unified platform.

Key Highlights

- **Joining the ArcSight architecture** allows Interset to simplify deployment with more efficient and enriched analytics
- **Enhanced use case detection** through the exercising of additional models
- **Reduced footprint** by more accurately sizing environments and resources
- **Integration with Recon** for a unified user experience
- **Simplified and intuitive installation** through the Micro Focus Container Deployment Framework
- **Improved analytics flexibility** through the updated risk engine which sets the stage for enhanced feedback features, investigation and hunting experiences
- **Unified and extensible user experience** through personalized dashboards and Jump and Search features which suit different personas and use cases, using ArcSight UI components, in one view
- **Pluggable UX components** for a customizable environment both within and outside the product for a more holistic view

ArcSight ESM 7.3

Key Highlights

- **Greater ArcSight Fusion adoption**, including the option for SecOps administrators to access ArcSight Command Center directly from the new Fusion UI for simpler SIEM management
- **Interactive API documentation** through Swagger integration supports a standards-based approach to REST APIs
- **Performance improvements** to lists, actor data, and list update speeds
- **Consolidated Remote Storage** (through ArcSight Recon) enables ESM to forward its events to a unified storage repository to be used across the ArcSight SecOps platform
- **Avro Ingestion** from Transformation Hub, in addition to ESM Binary format

ArcSight Fusion 1.1

Key Highlights

- **Build your own widgets** with Fusion's Widget SDK (Software Development Kit) and publish them through the ArcSight Marketplace
- **ArcSight Recon support** with new widgets to convey system health of the Recon infrastructure
- **Localization** to support French, Japanese, Korean, Russian and Chinese languages

ArcSight Logger 7.1

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

Transformation Hub 3.3

Key Highlights

- **Cloud-native deployment** available to leverage Azure services and capabilities
- **Unified Platform** updates to enable routing, filtering and storage for all ArcSight products
- **CDF Doctor** available for troubleshooting features of CDF
- **ZSTD compression** is supported, performs better than GZIP compression
- **Updated libraries** for RHEL and CentOS

ArcSight Management Center 2.9.5

Key Highlights

- **Cloud support** for Transformation Hub and Connectors in Azure
- **Unified Platform** updates to enable routing, filtering and storage for all ArcSight products
- **Updated libraries** for RHEL and CentOS, PostgreSQL, Azul Java
- **Connector support** for latest release v8.0
- **ZSTD compression** is supported, performs better than GZIP compression

SmartConnectors 8.0

Key Highlights

- **Cloud-native support** for Azure and AWS, including connectors for AWS S3 and Security Hub
- **Un-obfuscated parsers** allow access to parser definitions
- **Updated support** for newest Micro Focus Security, Risk and Governance products
- **Improved Connector Load Balancer** to increase security
- **ZSTD compression** is supported, performs better than GZIP compression
- **Customizable roles** to tailor memory allocations for Connectors (with Logger)
- **Updated libraries** for RHEL and CentOS

ArcSight Investigate 3.1—(ArcSight 2020.1)

Key Highlights

- **Enhanced integration** with SmartConnectors and Transformation Hub to ingest and route logs at scale
- **Container deployments** (CDF) can roll upgrades through the ArcSight Investigate cluster all at once, completing in hours what used to take days
- **New guided queries** assist in searching your data
- **Pre-built charts and visualizations** to optimize investigation
- **Host Profiler dashboard** provides fast insights into host behavior
- **Outlier detection** for network traffic identifies hosts deviating from baseline behavior
- **Domain Generation Algorithm** (DGA) helps identify activity using Investigate's pre-defined visualizations
- **Data Quality Dashboard** helps to identify data quality concerns

ArcSight Documentation

Release Notes

- ArcSight ESM 7.3
- ArcSight Fusion 1.1
- ArcSight Interset 6.1
- ArcSight Recon 1.0
- ArcSight Logger 7.1
- Transformation Hub 3.3
- ArcSight Management Console 2.9.5
- ArcSight SmartConnectors 8.0
- ArcSight Investigate 3.1 (ArcSight 2020.1 release)

Is Your ArcSight Version Up to Date?

Product Name	Newest Version
ArcSight ESM	7.3
ArcSight Fusion	1.1
ArcSight Interset	6.1
ArcSight Recon	1.0
ArcSight Logger	7.1
ArcSight Investigate	3.1
Transformation Hub	3.3
ArcMC	2.9.5
SmartConnectors	8.0

Watch ArcSight Specialist Gene Marrero and ArcSight Director of Product Management Mike Mychalczuk as they discuss the journey of SIEM and the features of the 2020.2 release. We also have exciting news about our recent SOAR acquisition available in our security blog.

Learn more at
www.microfocus.com/secops

Contact us at:
www.microfocus.com

Like what you read? Share it.