Advancing with ArcSight

ArcSight has advanced its security operations portfolio recently, and you can expect big improvements to your organization when it's fully utilized. Empower your team with ArcSight's end-to-end solution to maximize productivity and enjoy true cyber resilience.

ArcSight Versions at a Glance
Are you using the most updated version of ArcSight? Here some new capabilities you can utilize when you upgrade to the latest release:

ArcSight ESM

- CIRCL MISP integration
- MITRE ATT&CK dashboard
- SOAR offering, free of charge
- Global IDs
- Container-based deployment

ArcSight Intelligence

- Crowdstrike SaaS deployment
- Enhanced use case detection
- Reduced footprint
- Pluggable UX components
- Container-based deployment

ArcSight Recon

- 100+ out of the box reports and dashboards
- MITRE ATT&CK reports
- Outlier detection
- SOAR offering, free of charge
- Container-based deployment

SODP

- New SmartConnectors
- Container-based deployment
- Enhanced cloud connector support

You may have noticed that ArcSight has made several advancements lately, and you can expect additional changes in the future. ArcSight is determined to innovate and improve its capabilities, with an objective to provide the most complete and resilient security coverage available. These advancements span data collection, storage, analysis, cloud and SaaS offerings, and the integration of SOAR. ArcSight is moving fast, and in case you missed it, here are some of the areas ArcSight has enhanced recently:

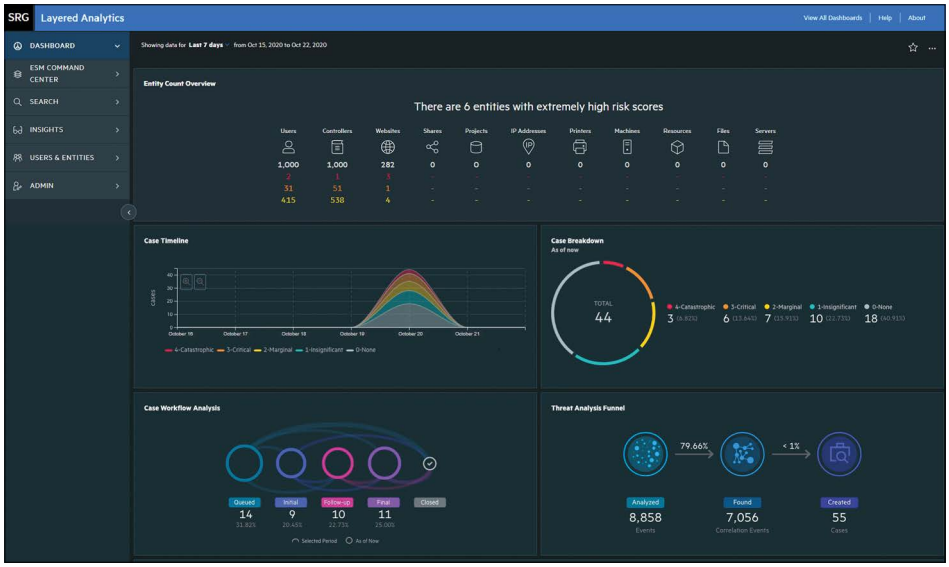

Figure 1. ArcSight's new UI integrated across all products

SIEM

ArcSight Enterprise Security Manager (ESM) is the crown jewel of ArcSight's security operations portfolio, and as such it will continue to drive major innovations, enhancements and integrations. ArcSight ESM continues to provide industry-leading real-time threat detection and response, allowing you to see and stop threats as they occur. Built to handle extremely high events per second (EPS), it can plow through mountains of incoming event logs. ESM monitors all your data sources and provides the highest level of enterprise security for your company. It is extremely customizable, allowing you to create company-specific rulesets to trigger instant alerts. Recent advancements include a new UI, tighter integration with ArcSight Intelligence, and acquisition and integration of a leading SOAR technology. ArcSight ESM enables both simple and complex automated responses that can be triggered on-demand or by specific alerts, without adding additional costs.

At a glance:

- Real-time threat detection
- High EPS thresholds
- Customizable and complex rulesets
- SOAR offering, free of charge
- New UI

Behavioral Analytics and AI

ArcSight Intelligence for behavioral analytics has been a major boost to ArcSight's security capabilities moving forward. Once installed, your organization can get valuable, actionable insights that might otherwise be missed. It informs you what normal user behavior looks like in your company, and instantly identifies and alerts you to the abnormal. There is no need to spend time creating rulesets because ArcSight Intelligence employs unsupervised machine-learning algorithms that do the work for you. It allows your company to sift through the flood of daily alerts and prioritize the few that need attention NOW.

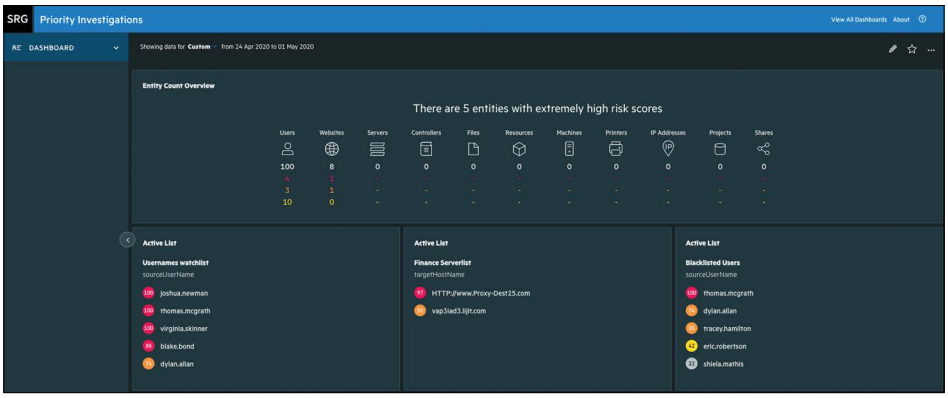

Figure 2. ArcSight Intelligence for behavioral analytics within ArcSight ESM

At a glance:

- Actionable behavioral insights
- Automated, unsupervised machine learning models
- Prioritized alerts

Data Storage and Analysis

ArcSight Recon is a major innovation in the SIEM industry. It is both a comprehensive log management solution and a security analytics solution rolled into one, easing compliance and accelerating forensic investigation for your security professionals. Recon is built for security event logs and is therefore more intuitive and accessible for security analysts, and it doesn't require a DBA to operate. It's developed with underlying Big Data technology that stores clean security data in its own security lake, which allows you search through mountains of data in a matter of seconds. It's also built to be the analytics engine to visualize and analyze your data, eliminating the need to buy a separate

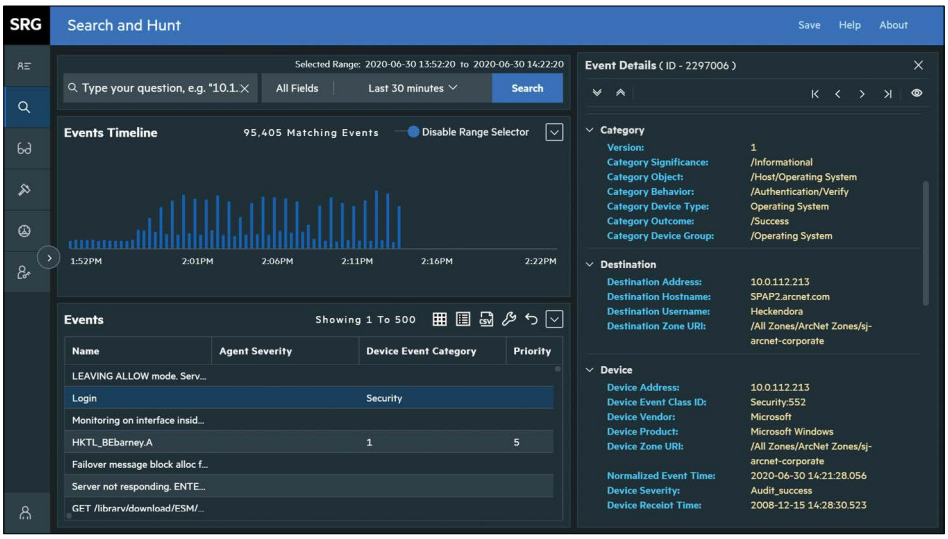

Figure 3. ArcSight Recon

product for your forensic analytics. 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. With ArcSight's recent acquisition of a leading SOAR company, Recon users have access to ArcSight SOAR with no additional costs.

At a glance:

- Log storage and analytics in one
- Built on big-data search technology
- Data-lake for security events
- SOAR offering, free of charge

Data Collection and Distribution

ArcSight is dedicated to expanding and enhancing the Security Open Data Platform (SODP) to collect, organize, enrich and distribute your security data. Continuous innovation of Connectors convert an ever-increasing number data types into Common Event Format (CEF), which allows your analysts to use your data quickly and easily. ArcSight's many partner integrations

let you leverage existing security solutions, increase your ROI, and lets you expand your security coverage at will. ArcSight's open infrastructure lets you use what you already have, while gaining the benefits of organized and centralized data.

At a glance:

- Security-specific data platform for SIEM
- Real-time alerts and analysis
- Hundreds of connectors, partner content, and integrations
- Increase ROI of existing solutions

SOAR

ArcSight SOAR is a leading Security Orchestration, Automation and Response Platform (SOAR) which combines orchestration of both technology and people, automation and incident management into a seamless experience. ArcSight SOAR helps security teams improve their efficiency in responding to cyberattacks in security operations by automating repetitive tasks, improving efficiency, filling employee skills gaps, and governing incident data.

At a glance:

- SOAR offered to ESM and Recon customers
- No additional cost
- Automation
- Incident governance

MITRE and Threat Intelligence Feeds

ArcSight is committed to keeping your company secure with the most up-to-date threat intelligence available. With automated integrations like MITRE ATT&CK and MISP CIRCL, as well as partner integrations with companies like Anomali, Ixia and LookingGlasss, your company is equipped with the most up-to-date protections available. ArcSight makes it easier for you to assess your overall security posture by incorporating the MITRE ATT&CK Framework into ArcSight's reports and dashboards. Learn how much coverage ArcSight provides within the MITRE ATT&CK Framework at **mitre.microfocus.com**.

At a glance:

- MITRE ATT&CK and MISP CIRCL integration
- Threat intelligence from partners: Anomali, IXIA, LookingGlass, CyCraft, Eclectic iq, IntSights, InQuest, Recorded Future, ThreatConnect, etc.

Cloud and SaaS

Cloud-native and SaaS deployments of your SIEM software are more important than ever if you want to reduce your hardware and infrastructure footprint. ArcSight is dedicated to providing cloud-native and SaaS deployments of its software within Azure and AWS to assist in this endeavor. ArcSight Intelligence components are already available as SaaS, and more SaaS components are in development for the near future.

At a glance:

- AWS deployment for ESM, Logger, ArcMC, SmartConnectors
- Azure deployment for ArcMC, Transformation Hub, SmartConnectors
- SaaS deployment for ArcSight Intelligence
- More cloud-native and SaaS components in development

Contact us at **CyberRes.com**
Like what you read? Share it.

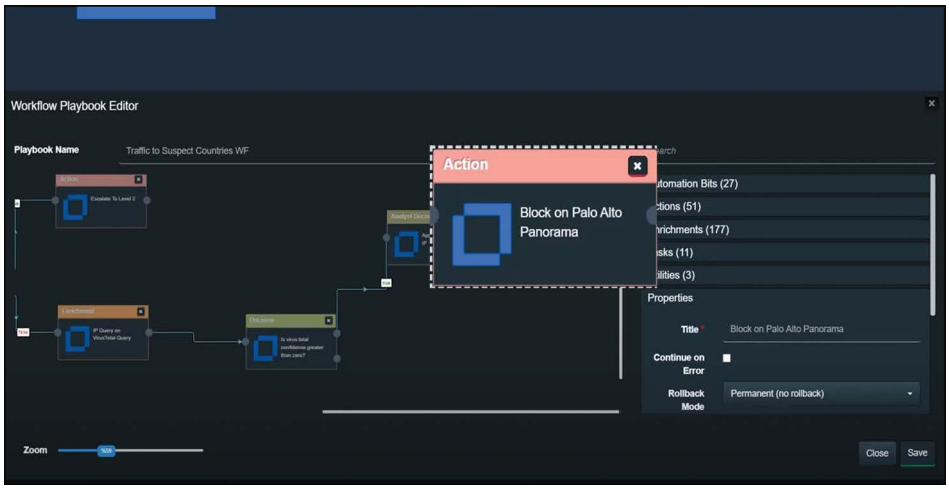

Figure 4. ArcSight SOAR, free of charge for ArcSight ESM and Recon customers

CyberRes
A Micro Focus Line of Business