

ArcSight for Operational Efficiency

Intelligently adapt your SecOps resources for greater operational efficiency and a more resilient security organization. ArcSight enables your team with a unified platform that leverages layered analytics and automation to accelerate your threat detection, prioritization, and response.

ArcSight Operational Efficiency at a Glance

What sets ArcSight apart from other solutions?

Layered Analytics

The ArcSight platform combines real-time correlation, threat intelligence, behavioral analysis, advanced threat hunting and MITRE ATT&CK integration, to help you focus on the right threats.

Unified Solution

The ArcSight platform combines real-time correlation, threat intelligence, behavioral analysis, advanced threat hunting and MITRE ATT&CK integration, to help you focus on the right threats.

Automation

Establish an efficient human-machine team. Machine-driven analysis and automation will identify and begin responding to possible threats, to reduce and optimize analyst workloads.

SecOps Efficiency Challenges

Across the globe, operational efficiency has proven to be an elusive goal for cybersecurity teams like yours. The management of a security operations center is a heavy responsibility, with SOC managers being asked to defend their organizations from a flood of advanced threats, while being understaffed and supported by disjointed technologies. In a complex environment like this, limited resources are quickly overwhelmed. Alert fatigue and operational bottlenecks compromise your ability to efficiently detect and respond to threats, raising your organization's risk of oversight and breach to dangerously high levels. In order to achieve true cyber resilience, your security team needs a way to be both comprehensive and efficient.

Operational Efficiency with ArcSight

ArcSight enables your organization to proactively reduce its threat exposure and increase its operational efficiency by providing advanced security technologies that work together in a holistic end-to-end platform. ArcSight's intelligent layered analytics combines a first-in-class correlation engine, unsupervised machine learning, threat intelligence, advanced hunting, and SOAR, to enable your security team to quickly and accurately detect and respond to both known and unknown threats. It simultaneously reduces and optimizes the workload of your SOC team by providing contextualized, faster-than-human analysis, while automating repetitive tasks and response.



You can simplify security operations for your team and reduce their need to shift between resources and tools with ArcSight's unified data platform and common data storage. Its intuitive shared interface combines the insights from ArcSight's various analytical tools to provide platform-wide visibility and contextualized understanding of your threat environment from a single pane of glass. That same interface includes dashboards to help you easily monitor workflows and SOC metrics. And ArcSight's close integration with the MITRE ATT&CK framework, backed by supporting dashboards and pre-built content, will enable your security operations team to identify and fill the gaps in your organization's security environment, further supporting its cyber resilience.

Keep your SOC focused on what truly matters while staying efficient, flexible and quick to react. Empower your team with ArcSight's layered security analytics and automation platform.

Why ArcSight?

ArcSight is a holistic SecOps solution that enables SOC resilience. With ArcSight, your organization can intelligently adapt to talent shortages in the face of overwhelming incident volume, strangling bottlenecks and taxing incident fatigue, by sharpening resource focus on what truly matters. ArcSight enables faster, more accurate threat detection of both known and unknown threats with layered analytics, simplifies user experience with a unified interface, and accelerates response with native SOAR capabilities.

Features and Benefits

Combined Machine Learning: Your SOC is likely overwhelmed with alerts and false positives, wasting your analysts' valuable time and delaying response. ArcSight combines supervised machine learning from ArcSight Recon and unsupervised machine learning from ArcSight Intelligence to optimize your SOC's leads and focus your analysts' efforts on the threats that matter most.

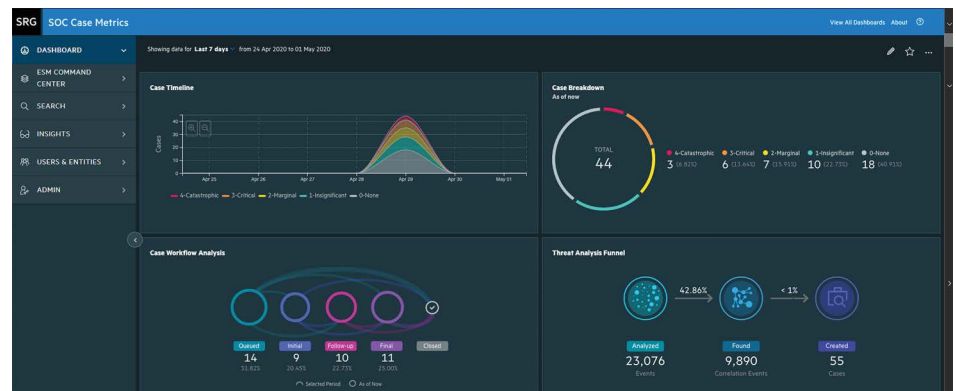


Figure 1. ArcSight helps you easily monitor workflows and SOC metrics.

Security Orchestration and Automated Response: ArcSight's native SOAR capabilities aid your analysts by automating repetitive tasks and initiating swift threat response. With SOAR, you'll reduce the workload facing your analysts and enable them to more efficiently focus on their most critical tasks.

Centralized User Interface: With fragmented security tools running independently, your analysts are unable to gain a holistic view of your entire threat landscape, hindering swift threat detection and response. ArcSight's various components share a centralized user interface to enable your SOC with a single pane of glass that reduces "swivel-chair syndrome" and wasted time, allowing your analysts to find and react to threats with both speed and accuracy.

Identification of Known and Unknown Threats: Accurately detecting both known and unknown threats is key to stopping attacks before they take place. ArcSight helps you protect your organization from community-known threats with real-time correlation, and from unknown threats with advanced behavioral analytics and threat hunting.

Contextual Threat Insights: To efficiently detect threats, your security team needs more than just siloed investigations and

alerts. By merging the insights from multiple analysis tools onto a single UI, ArcSight's layered analytics provide your team with greater context behind each threat alert and risky user. This cross validation and insight enrichment significantly increases the accuracy of your SOC in separating real threats from false positives, allowing your team to quickly prioritize and address the riskiest threats.

Integration with Threat Intelligence: ArcSight's real-time correlation can detect documented threats faster than any other security technology. Integration with threat intelligence feeds, such as those provided by MISP and Anomali, help keep ArcSight's correlation rules up-to-date so that they can detect the latest attacks in today's evolving threat landscape (including zero-day attacks).

MITRE ATT&CK Integration: The MITRE ATT&CK Framework provides SOCs with a global knowledge base of malicious cyber tactics and techniques, to help organizations better understand cyber threats, and identify their organizational security gaps. ArcSight has worked MITRE ATT&CK directly into its product offering, with dashboards that map ingested security events to MITRE techniques, to provide you with a real-time view of the top threat techniques facing your SOC, and to give you a clear, birds-eye view of your overall threat exposure and security

“By taking a different approach to visualizing our risk themes, embracing modern, business-enabling technologies such as ArcSight, and establishing an advanced SOC, we have experienced a 30% reduction in alarms, ensuring our resources are directed most effectively.”

MR. JACOB JACOB
Specialist Cyber Security
Dubai Electricity and Water Authority

Contact us at [CyberRes.com](https://www.cyberres.com)
Like what you read? Share it.



coverage. Micro Focus also offers its own [MITRE ATT&CK Navigator](#) to direct users to the content and solutions they need to fill their security gaps.

Unified Platform: Siloed security solutions waste time and add complexity to your SOC, requiring your analysts to manage multiple data stores, and to move between various tools and interfaces. ArcSight simplifies SecOps by uniting an end-to-end solution on a single platform, complete with a unified data platform, common storage, layered analytics, and a shared intuitive interface.

Hundreds of Connectors: Through ArcSight's SmartConnectors, you can collect, normalize, aggregate, and enrich data from over 480 different data source types. The structured approach to data, using a common event

format, enables you to efficiently search, monitor, and analyze your data to gain valuable security intelligence from across your entire organization.

Open Architecture: An open architecture gives you greater interoperability for increased coverage. With out-of-the-box connector support for over 480 different data sources, and a custom connector creation tool, you can collect, normalize, aggregate and enrich data from across your organization. Further, with over 100 partner integrations, ArcSight enables you to leverage your existing security solutions, increase their ROI, and expand your security coverage at will. ArcSight's open architecture lets you use what you already have, while gaining the benefits of normalized, centralized data.

Shared Data Platform and Storage: ArcSight leverages the Security Open Data Platform to ingest and distribute data as needed, across the ArcSight platform and with any integrated 3rd party solutions. ArcSight Recon's powerful storage solution enables SOCs with a single data repository that can be used by each of the ArcSight platform's various components, to allow users to collect their data once, store it once, but use it many times across multiple ArcSight solutions.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
T1208 Drive-by-Compromise	T1094 Command and Scripting Interpreter	T1098 Account Manipulation	T1548 Abuse Elevation Control Mechanism	T1548 Abuse Elevation Control Mechanism	T1180 Remote Force	T1087 Account Discovery	T1210 Exploitation of Remote Services	T1340 Active Collected Data	T1071 Application Layer Protocol
T1170 Exploit Public-Facing Application	T1003 Exploitation for Client Execution	T1197 BITS Jobs	T1134 Access Token Manipulation	T1134 Access Token Manipulation	T1548 Credentials from Password Stores	T5010 Application Window Discovery	T1534 Internal Spearphishing	T1123 Audio Capture	T1090 Communication Through Removable Media
T1133 External Remote Services	T1599 File Process Communication	T1547 Root or Logon Auxiliary Execution	T1547 Root or Logon Auxiliary Execution	T1197 BITS Jobs	T1312 Exploitation for Credential Access	T1217 Browser Bookmark Discovery	T1370 Lateral Tool Transfer	T1119 Automated Collection	T1132 Data Encoding
T1200 Hardware Address	T1106 Native API	T1007 Root or Logon Initialization Scripts	T1007 Root or Logon Initialization Scripts	T1540 OperatingSystem/Device File or Information	T1187 Forced Authentication	T1482 Domain Trust Discovery	T1543 Remote Service Session Hijacking	T1115 Clipboard Data	T1001 Data Obfuscation
T1564 Phishing	T1053 Scheduled Task/Job	T1174 Browser Extensions	T1543 Create or Modify System Process	T1006 Direct Volume Access	T1056 Input Capture	T1083 File and Directory Discovery	T1001 Remote Services	T1213 Data from Information Repositories	T1566 Dynamic Resolution
T1091 Replication Through Removable Media	T1329 Shared Modules	T1534 Compromised Client Software Binary	T1346 Event Triggered Execution	T1480 Execution Guardrails	T1557 Man-in-the-Middle	T1046 Network Service Scanning	T1091 Replication Through Removable Media	T1008 Data from Local System	T1373 Encrypted Channel
T1195 Supply Chain Compromise	T1072 Software Deployment Tools	T1336 Create Account	T1066 Exploitation for Privilege Escalation	T1111 Exploitation for Defense Evasion	T1554 Hostly Authentication Process	T1338 Network Share Discovery	T1072 Software Deployment Tools	T1029 Data from Network Shared Drive	T1008 Fatback Channels
T1149 Trusted Relationship	T1569 System Service	T1543 Create or Modify System Process	T1484 Group Policy Modification	T1222 File and Directory Permissions Modification	T1040 Network Sniffing	T1040 Network Sniffing	T1080 Taint Shared Content	T1028 Data from Removable Media	T1105 Ingress Tool Transfer
T1078 Valid Accounts	T1304 User Execution	T1544 Event Triggered Execution	T1574 Hijack Execution Flow	T1484 Group Policy Modification	T1005 OS Credential Dumping	T1001 Password Policy Discovery	T1550 Use Alternate Authentication Material	T1074 Data Staged	T1104 Multi-Stage Channels
T1047 Windows Management Instrumentation	T1123 External Remote Services	T1055 Process Injection	T1584 Hide Artifacts	T1222 File and Directory Permissions Modification	T1586 Shell or Forge Windows Tickets	T1120 Peripheral Device Discovery	T1114 Email Collection	T0998 Non-Application Layer Protocol	T1571 Protocol Tunneling
T1574 Hijack Execution Flow	T1053 Scheduled Task/Job	T1053 Scheduled Task/Job	T1574 Hijack Execution Flow	T1574 Hijack Execution Flow	T1539 Shell Web Session Coerce	T1069 Permission Groups Discovery	T1056 Input Capture		
T1137					T1111				

Figure 2. ArcSight's MITRE ATT&CK dashboards give you a real-time view of the top threat techniques facing your SOC