opentext™ | Cybersecurity

Data Sheet

ArcSight Enterprise Security Manager

Real-time threat detection and response from a powerful, adaptable SIEM. ArcSight ESM provides massively scalable event collection, native threat intelligence, an industry-leading correlation engine, and native ArcSight SOAR.

When it comes to threat detection and response, every second matters. ArcSight Enterprise Security Manager (ESM) by OpenText dramatically reduces the time to detect, react, and triage cyber-security threats in real-time and at scale. ArcSight ESM is a powerful, intelligent SIEM (Security Information and Event Management) solution that leverages real-time event correlation analytics to help security teams detect and respond to internal and external threats. With native ArcSight SOAR by OpenText, it reduces response time from hours or days to minutes and gives Security Operation Centers (SOCs) the ability to address more threats without the need for additional headcount, through simplified SOC workflows and continuously updated threat packages available from the ArcSight Marketplace.

Key Benefits

Detect Threats in Real-Time with Operational Efficiency
ArcSight Enterprise Security Manager is a comprehensive real-time threat detection, analysis, workflow, and compliance management platform with data enrichment capabilities. ArcSight ESM detects and directs analysts to cyber-security threats, in real time, helping security operations teams respond quickly to threat indicators. By automatically identifying and prioritizing threats, teams avoid much of the cost, complexity and extra work associated with false positives. ESM gives SecOps teams the ability to have a centralized view of their environments, creating workflow efficiency for streamlined processes. Through improved detection, real-time correlation, workflow automation, and native ArcSight SOAR, SOC teams can resolve incidents quickly and accurately.

Enterprise-Wide Event Visibility
ArcSight ESM leverages advanced event collection technology from ArcSight Security Open Data Platform (SODP) by OpenText to enrich and analyze data from over 450 different security event source types. ArcSight SODP's SmartConnectors support every common event format (native Windows events, APIs, firewall logs, syslog, Netflow, direct database connectivity, etc.). ArcSight ESM also ingests data from the cloud. Beyond these, our FlexConnector framework supports the development of custom connectors to facilitate the ingestion and correlation of additional sources. More event sources means more visibility and the ability to develop more complex security use-cases specific to the needs of your organization.

Defend Against the Latest Threats with GTAP Threat Intelligence
Galaxy Threat Acceleration Program (GTAP) Basic is the native threat intelligence feed available to all ArcSight ESM users.

ArcSight ESM at a Glance

Detect Threats in Real-Time
Industry leading event correlation that scales to 100,000+ EPS, centralizes event log analysis to detect threats as they appear.

Native Threat Intelligence
Ensure ArcSight ESM stays up-to-date on the latest threats with ArcSight ESM's native TI feed: GTAP.

Content and Reporting
Default content provides MITRE ATT&CK mapping, modular dashboards, hundreds of adjustable correlation rules, and more.

MSP/MSSP-Ready
Supports multi-tenancy implementations for distributed security environments.

Native SOAR
Out-of-the-box ArcSight SOAR enables your team with automation, playbooks, incident management, SOC analytics, and more.

It automatically incorporates threat monitoring content into ArcSight ESM based on open-source threat intelligence data, providing greater coverage against modern threats and campaigns through increased visibility of industry threats. ArcSight ESM also integrates with many third-party and open-source threat intelligence feeds, and offers curated threat intelligence protection through GTAP Plus, our premium threat intelligence solution *(see "Add-Ons")*.

Automate Response with Native SOAR
ArcSight SOAR is considered to be a core part of modern security analytics, and as such provides it as a complementary, native solution. Backed by out-of-the-box playbooks and 120+ integration plugins, ArcSight SOAR effectively and efficiently automates and orchestrates triage, investigation, and response activities. It supports visual, workflow playbooks, detailed reporting on KPIs, and greater team collaboration through a detailed case timeline.

Maximize Your ROI through Integrations and Content
ArcSight ESM integrates with the rest of the ArcSight portfolio and a large number of third-party security tools (EDRs, ticketing systems, identity repositories, etc.) to help you maximize your return on investment. These can be viewed on the ArcSight Marketplace by OpenText. ArcSight ESM also comes with hundreds of adjustable out-of-the-box correlation rules and dashboards. Custom content (rules, trends, dashboards and reports) can also be created to address practically any security use case, and can then be easily packaged up and deployed on other systems or shared to other business units or the OpenText community. In tiered architectures, multiple ArcSight ESMs can be set to automatically sync content systems dynamically. ArcSight Marketplace and the ArcSight ESM Default Content packages are continuously updated with new security use cases, rules, and supported products

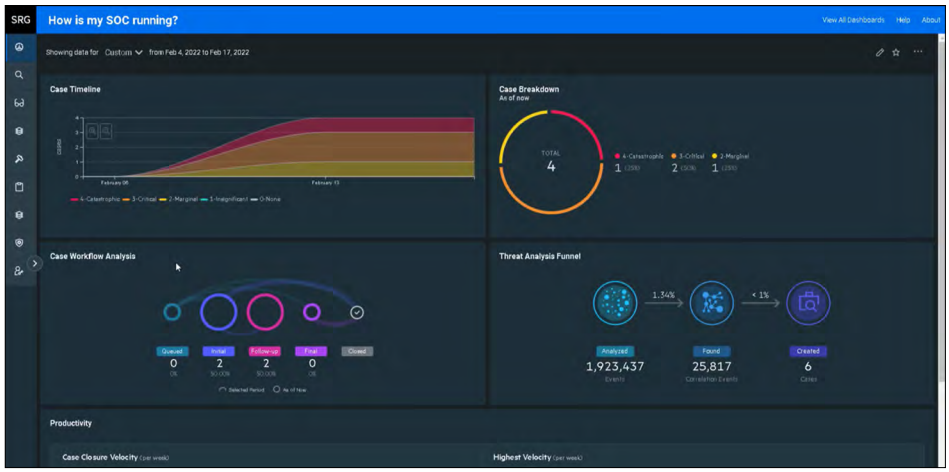

Figure 1. SOC metrics dashboard

that can be easily deployed to help you alert and triage defenses current with relevant threats while realizing a greater return on your investment.

Key Features

Powerful Real-Time Correlation
ArcSight ESM correlates events and alerts to identify high priority threats within your environment. The powerful correlation engine can analyze huge volumes of event data (100,000+ events per second) in real-time to accurately escalate threats that violate the internal rules set within the platform.

Intelligent and Dynamic Event Risk Scoring and Prioritization
ArcSight ESM's unique priority formula consists of criteria that each event is evaluated against to determine its relative importance, or priority, to your network. The calculation incorporates many data points, such as the defined network and asset model, open ports and imported vulnerability scan results from third-party solutions. For example, a given attack might be known to exploit a certain vulnerability. If the targeted system exposes that vulnerability and the attacked port is open on the asset, then ArcSight ESM can assume that the attack is likely to succeed and will prioritize it.

Categorization and Normalization
Categorization and normalization convert collected raw event logs into a universal format for use across the ArcSight Platform. We use the Common Event Format (CEF), a de facto industry standard developed by ArcSight from expertise gained over decades of building 300+ connectors across dozens of security and network technology categories. Data categorization and normalization helps you quickly identify situations that require investigation or immediate action to focus your attention on the most urgent, high-risk threats.

Workflow Automation
When a case is created, ArcSight ESM automatically fetches artifacts from the detected event, builds the case scope, classifies it, consolidates it, maps it to the MITRE ATT&CK framework, and assigns it to an analyst or analyst group. Automated triage prioritizes alerts and can close false positives automatically. Playbooks can be setup to be triggered automatically or run manually. ArcSight ESM's built-in case management system enables triage to run efficiently and effectively and tracks all activities on a case timeline. By tracking SLAs and analyst response time metrics, SOC teams can reduce their mean time to respond and escalate

incidents to the appropriate personnel for resolution. ArcSight ESM also integrates with many third-party ticketing systems.

Multi-Tenancy

ArcSight ESM allows distributed business units to utilize one simplified SecOps view. With multi-tenancy capabilities and access control permissions configurable down to the event level, enterprises can use a centralized set of management abilities including rule-based thresholds and a unified permissions roles, rights, and responsibilities matrix. Tenants of a single deployment are assigned a unique tenant identifier, and data from tenants is always isolated (secure data separation). Unique rules, reports, and dashboards can be customized and made accessible to target system owners and stakeholders.

Integration with ArcSight Intelligence

ArcSight Intelligence by OpenText delivers powerful behavioral analytics backed by unsupervised machine learning to help you detect insider threats, zero-day attacks, and advanced persistent threats (APTs). By integrating ArcSight Intelligence with ArcSight ESM, you gain a layered analytics approach that detects both known and unknown threats, providing your organization with greater security coverage. Furthermore, integration enhances each solution with greater threat context. For example, risk scores for ArcSight ESM alerts are optimized by factoring in the behavioral risk scores of any entities associated with those alerts. Users can also build correlation rules based on anomalous behavior detected by Intelligence.

Integration with ArcSight Recon

ArcSight ESM integrates with ArcSight Recon by OpenText to support extremely fast and intuitive search and data visualization within the security operations environment. ArcSight Recon is a next-gen log management, compliance, hunt, and investigation solution built on an advanced analytics platform to serve the evolving needs of security teams. Combining ArcSight ESM and ArcSight Recon allows SOC personnel to detect and understand unknown security threats within their enterprise through intelligent visualizations, to quickly remediate any impact or pre-emptively mitigate these threats before damage is done.

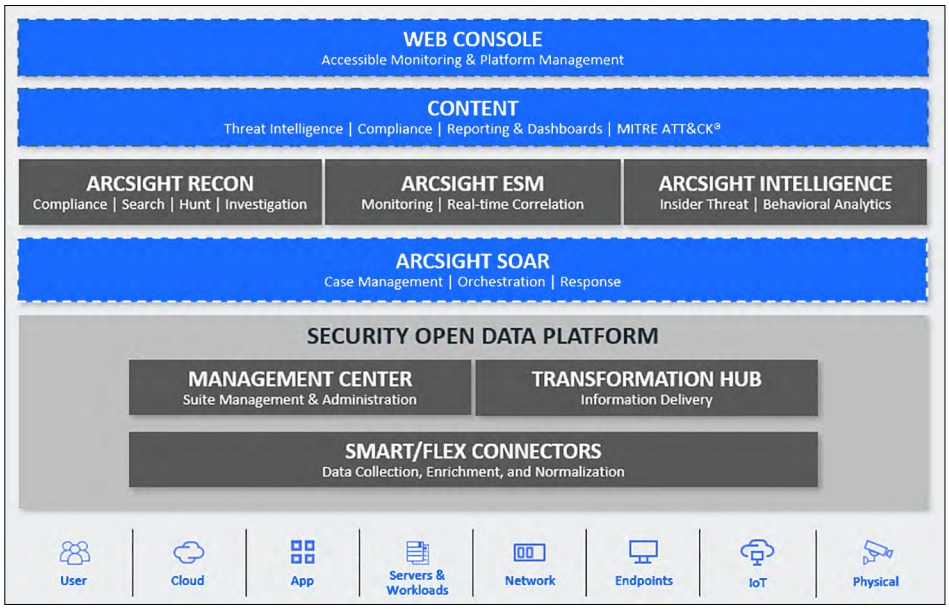

Figure 2. The ArcSight portfolio

Additional ESM Features

Other Features

- **Active Lists**—Dynamic in-memory lists capable of holding millions of entries, these can act as watch lists for monitoring suspicious traffic or behavior, with the ability to use active lists in any correlation rule.
- **Schedule reports**—And deliver results automatically to key stakeholders.
- **APIs**—Share event and case data from ArcSight ESM with ArcSight REST by OpenText-based APIs and Swagger integration.
- **ArcSight Fusion by OpenText Dashboards**—ArcSight's web-based Fusion UI connects all components of the ArcSight platform and supports customizable widget-based dashboards to visualize SOC metrics.
- **MITRE ATT&CK Dashboards**—Get a real-time view of all MITRE ATT&CK related events happening in your environment, the top threat techniques facing your SOC, and a clear image of your organization's ability to detect individual techniques.
- **Data Security**—Protect your data integrity with immutable data storage.
- **Active Directory Integration**—Manage your ArcSight ESM user and group memberships through your AD users and groups.
- **Distributed Correlation**—This mode allows users to deploy multiple instances of correlators and aggregators to increase processing speed and improve correlation fidelity with more contextual event analysis.

Add-Ons

GTAP Plus

GTAP Plus is a premium, curated threat intelligence feed for ArcSight ESM that incorporates insights from OpenText™

> **“With ArcSight, we don’t just detect real attacks quickly, but we also automate orchestrated responses in near-real time. The flexibility of ArcSight helps us intelligently adapt for the future.”**
>
> **Dmitriy Ryzhkov**
> Senior Information Security Analyst
> NPC Ukrenergo

Connect with Us
www.opentext.com

Cybersecurity Galaxy’s threat research network and provides ArcSight users with proactive defenses. It increases your coverage against modern threats and threat campaigns by providing greater visibility, reducing false positives, and enhancing threat response. GTAP Plus works to eliminate blind spots and powers advanced implementation of ATT&CK and D3FEND countermeasures to help stop breaches before they occur.

High Availability (HA)
Provides an optimized performance environment with multiple ArcSight ESM systems, with automatic failover capabilities should the primary system experience any communication or operational problems.

Compliance Insight Packages (CIPs)
Ease the burden of audits and compliance with ArcSight CIPs. These packages provide essential foundations for compliance with various regulations through a bundle of rules, dashboards, data monitors, active channels, automation, reports, and more. Packages are available for GDPR, NERC, HIPAA, ITGOV, FISMA, PCI, and SOX.

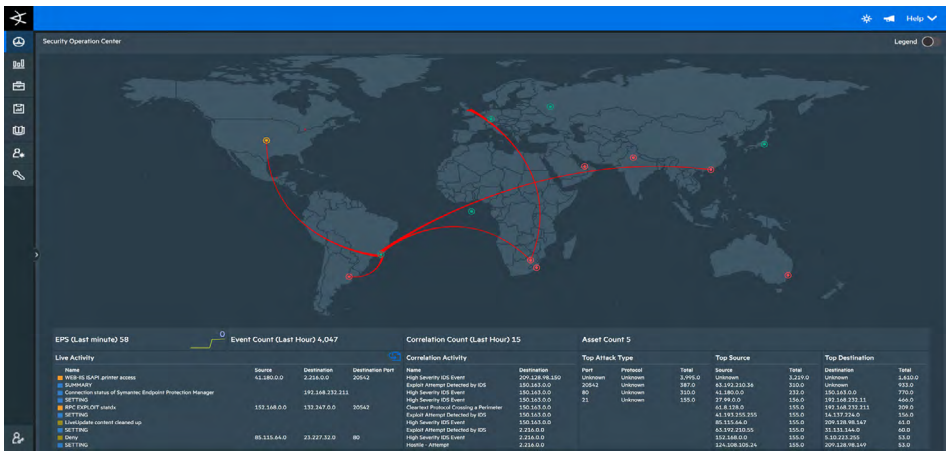

Figure 3. SOC Dashboard with World Map

Voltage SecureData Enterprise Add-on
Using Voltage SecureData Enterprise by OpenText technology, ArcSight applies Format Preserving Encryption (FPE) to retain correlation capabilities without exposing sensitive data like social security numbers or credit card numbers to analysts or ArcSight users.

ArcSight Marketplace
Through the ArcSight Marketplace, users can access hundreds of supporting content packages from our partners, community, and security experts. This includes both free and paid content, with ArcSight-verified apps, rulesets, dashboards, integrations, connectors, and more to further enhance your ArcSight usage.

Learn more at
www.microfocus.com/arcsightesm

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

760-000042-003 | O | 10/23 | © 2023 Open Text