ot opentext™

OpenText Enterprise Security Manager

Accelerate effective threat detection and response with real-time correlation and native SOAR

Benefits

- Elevate security operations efficiency
- Gain enterprise-wide cybersecurity event visibility
- Reduce threat exposure time
- Maximize return on SIEM investment

The complexity and volume of cyberthreats require substantial investment in advanced technologies and skilled personnel, which can strain financial resources. Additionally, the constant evolution of cyberthreats demands continuous updates and training, disrupting operations and increasing the risk of potential breaches if not managed effectively.

OpenText™ Enterprise Security Manager (ArcSight Enterprise Security Manager) is for security operations teams that need to significantly reduce false positives and find and respond to threats that matter in real time. Its capability has been proven in customer deployments and independent MITRE ATT&CK framework evaluation for SIEMs.

Elevate security operations efficiency

OpenText Enterprise Security Manager is a comprehensive threat detection, analysis, workflow, and compliance management platform with data enrichment capabilities and native SOAR. It detects and directs analysts to cybersecurity 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. SecOps teams have a centralized view of their environments, creating workflow efficiency for streamlined processes.

Gain enterprise-wide cybersecurity event visibility

Leverage advanced event collection technology from OpenText Security Open Data Platform (SODP) to enrich and analyze data from more than 450 different security event source types. OpenText SODP's SmartConnectors support every

common event format (native Windows events, APIs, firewall logs, syslog, Netflow, direct database connectivity, etc.). OpenText Enterprise Security Manager also ingests data from the cloud. Beyond these, its FlexConnector framework supports the development of custom connectors to facilitate the ingestion and correlation of additional sources. More event sources mean more visibility and the ability to develop more complex security use cases specific to your organization's needs.
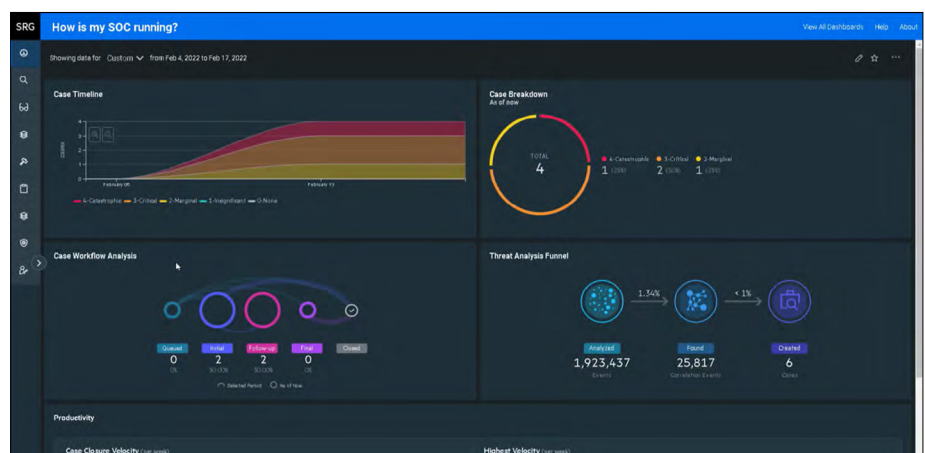
Reduce threat exposure time

SOAR is a core part of modern security analytics, and as such, comes as a complementary, native solution with OpenText Enterprise Security Manager. Backed by out-of-the-box playbooks and more than 120 integration plugins, this critical SOAR capability reduces exposure time by automating and orchestrating triage, investigation, and response activities. It supports visual, workflow playbooks; detailed reporting on KPIs; and greater team collaboration through a detailed case timeline.

Maximize return on SIEM investment

OpenText Enterprise Security Manager integrates with many third-party security tools, such as EDRs, ticketing systems, and identity repositories to help you maximize your return on investment. These can be viewed on OpenText Marketplace. It 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 and deployed on other systems or shared to other business units or the OpenText community.

In tiered architectures, multiple OpenText Enterprise Security Manager instances can be set to automatically sync content systems dynamically. OpenText Marketplace and the OpenText Enterprise Security Manager Default Content packages are continuously updated with new security use cases, rules, and supported products, which can be easily deployed to help you alert and triage defenses current with relevant threats while realizing a greater return on your investment.

OpenText Enterprise Security Manager enables real-time threat detection through the power of extensive data connectivity, robust data processing and enrichment, proven real-time correlation, rich content, solid MITRE ATT&CK framework support, and native SOAR to improve security operations efficiency and help analysts do more in less time, with less stress.

SOC metrics dashboard

Product features	Description
Real-time correlation	Analyzes 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	Evaluates each event against a unique priority criteria formula to determine its relative importance, or priority, to your network.
Categorization and normalization	Converts collected raw event logs into a universal format and helps you quickly identify situations that require investigation or immediate action.
MITRE ATT&CK dashboards	Provides a real-time view of all MITRE ATT&CK-related events, such as the top threat techniques and an organization's ability to detect individual techniques.
Workflow automation	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.
Integration with OpenText Security Log Analytics	Integrates with OpenText™ Security Log Analytics to support extremely fast and intuitive search and data visualization within the security operations environment.

SOC Dashboard with World Map

opentext™