OpenText Enterprise Security Manager

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

Benefits

- Elevate security operations efficiency
- Reduce false positives through proven AI correlation
- Gain enterprise-wide cybersecurity event visibility
- Reduce threat exposure time
- Maximize return on SIEM investments

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.

Security teams must cut through noise, validate alerts quickly, and respond to real threats before they escalate. OpenText™ Enterprise Security Manager (ArcSight) helps your team do exactly that—by reducing false positives, improving detection accuracy, and giving analysts the context they need to make confident decisions in real time. Its capability has been proven in customer deployments.

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. Analysts are directed to cybersecurity threats in real time, helping them 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 the OpenText SIEM Open Data Platform (SODP) to enrich and analyze data from more than 450

"Every day we would spend up to three hours to manually identify and block malicious IP addresses. OpenText Enterprise Security Manager (ArcSight) has automated this process and reports back to us every 12 hours with a list of blocked IP addresses."

Read more ›

OpenText Security Services experts leverage extensive experience to identify security risks and implement programs to keep systems safe and protected.

Learn more ›

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. The FlexConnector framework supports the development of custom connectors to facilitate the ingestion and correlation of additional sources and more complex security use cases.

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. By automating and orchestrating triage, investigation, and response activities, you can reduce exposure time and ensure faster, more consistent security operations. Collaborate more effectively through a detailed case timeline gain clearer insight into performance with detailed KPI reporting. Visual workflow playbooks, out of-the box playbooks, and more than 120 integration plugins enable this critical SOAR capability.

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.

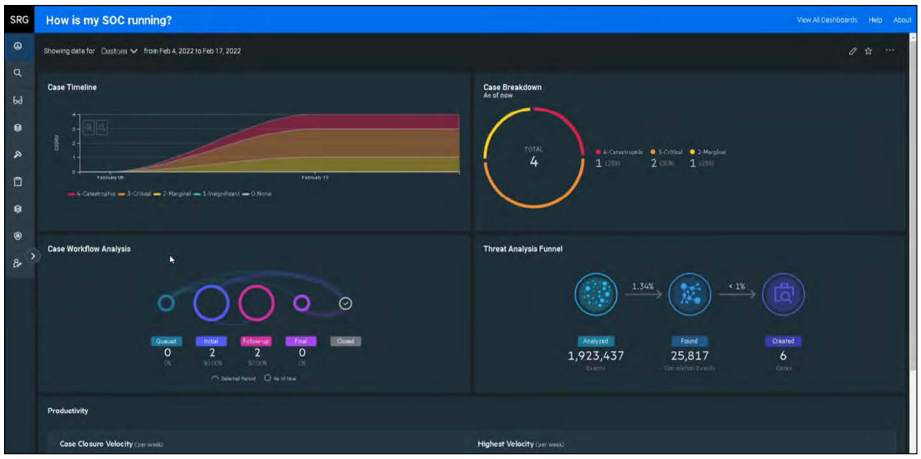


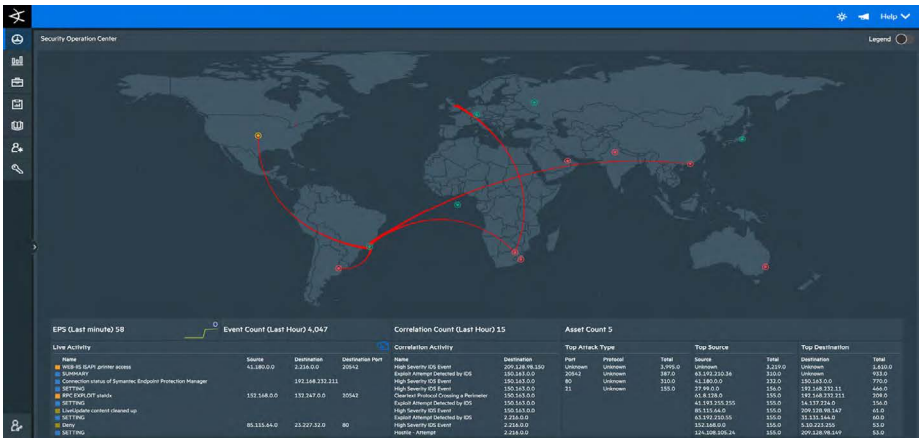
Figure 1. SOC metrics dashboards

Resources

Learn more ›

Read customer success stories ›

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.
AI-enabled correlation	Uses AI for predictive prioritization and decision making per NIST standards.
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™