OpenText Security Log Analytics

Comprehensive SIEM log management tool and security analytics solution eases compliance burdens, facilitates threat hunting, and accelerates forensic investigation

Benefits

- Improve efficiency with centralized log management
- Speed up threat hunting with high performance search
- Reduce administrative burden with simplified compliance and reporting
- Optimize cost and growth with the capability to store data at scale

As organizations strive to collect and store security data from a seemingly infinite number of sources, data monitoring and management has become increasingly difficult. Many solutions simply weren't built with security in mind, and inadvertently cause inefficiencies when implemented within the context of SIEM, security compliance, event logging, threat hunting, and forensic investigation. Logging, proactive threat mitigation, and forensic investigation are essential tasks in a modern SOC (Security Operations Center), and organizations need a solution that transcends the standards of today to be equipped for tomorrow.

OpenText™ Security Log Analytics (ArcSight Recon) is a comprehensive log management and security analytics solution for cybersecurity professionals who need to simplify log management and compliance while improving efficiency and effectiveness in proactive and reactive threat investigations. It combines the compliance, storage, and reporting needs of log management with the capabilities of big-data search and analysis. It is purpose-built for security event logs and is therefore more intuitive and accessible for security analysts, and will not require a DBA (database administrator) to operate. 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.

Improve efficiency with centralized log management

OpenText Security Log Analytics stores terabytes of machine data from any source including logs, clickstreams, sensors, stream network traffic, security devices, web servers, custom applications, social media, and cloud services. Store, search, monitor, and analyze data to gain centralized security intelligence from across your entire organization. For quick exploration of the data, an event detail panel allows investigation of individual and grouped events. The raw message view allows analysts to inspect original, unformatted event logs.

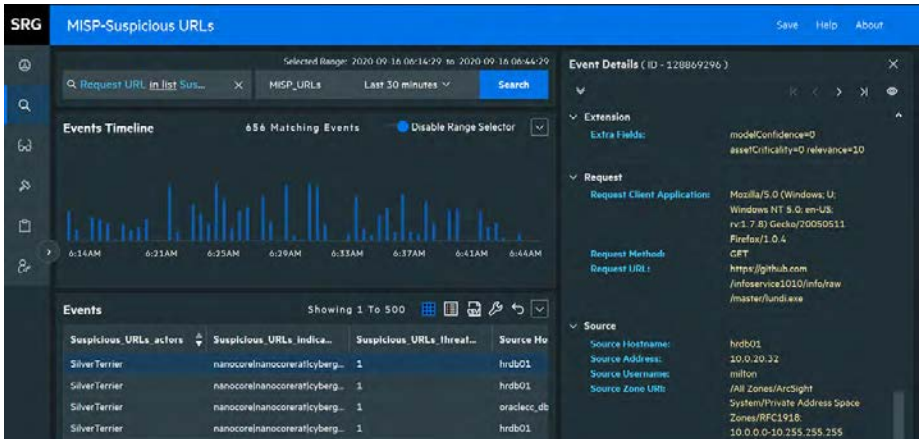

Figure 1. Event detail panel.

Figure 2.GDPR Reports.

Speed up threat hunting with high performance search

Sift through mountains of log data with minimal effort using OpenText Security Log Analytics' dynamic query suggestions and get results faster with its powerful big data analytics engine. Its columnar database responds to queries faster than traditional databases, enabling it to quickly and efficiently investigate millions of events. Storing clean, structured data in one centralized location accelerates investigation and improves the quality of results. Outlier detection provides visualizations to quickly identify deviations from baseline host behavior metrics. A user-friendly search interface displays a grid or message view, as well as a time-based histogram. The solution facilitates threat hunting in massive datasets, enabling security analytics at scale. It minimizes requirements for expertise and training, prioritizes abnormalities, and improves efficiency.

Reduce administrative burden with simplified compliance and reporting

Prepare compliance reports faster with OpenText Security Log Analytics' reporting content packages. Select the report wizard or choose a template to create crosstab reports, tables, or chart-based reports for your organization. After making your own customized reports, simultaneously email, upload, and publish the reports as needed. You can also schedule your reports to be automatically generated and delivered, even to multiple recipients at once.

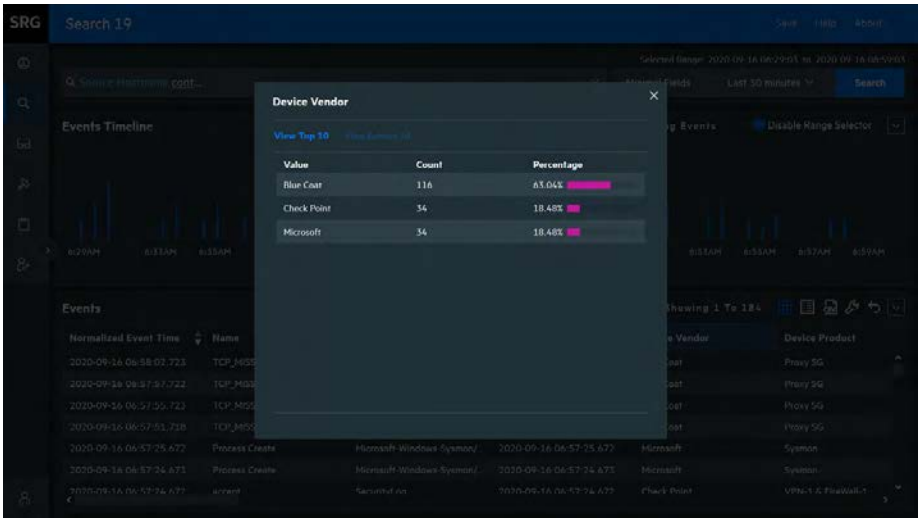

Figure 3. Histogram of vendor device values.

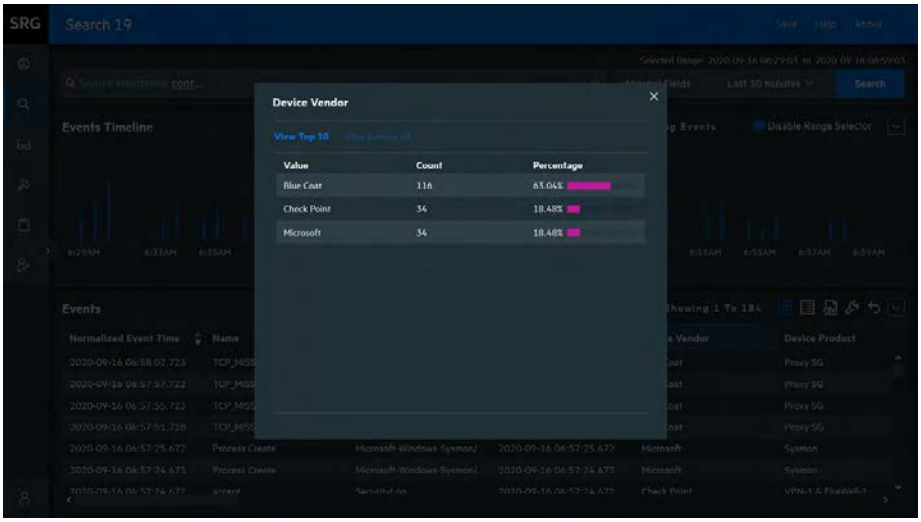

Figure 4. Pre-built MITRE ATT&CK content.

Pre-built content for FIPS 140-2, GDPR, PCI and IT-GOV compliance packages are now available, and more reporting templates are expected in subsequent releases.

Moreover, the solution comes with more than 100+ out-of-the-box reports/dashboards, including MITRE ATT&CK, Cloud, OWASP, and data modeler content. It also supports external data sources such as, Text/Excel/Directory/Elastic search/JDBC, Rest JSON, XML. With the MITRE ATT&CK content, you can quickly see how much coverage you have against the tactics and techniques within the framework, and the reports show your tailored results in the context of MITRE techniques.

Optimize cost and growth with the capability to store data at scale

Store data more efficiently with OpenText Security Log Analytics' event aggregation and log compression. It cost-effectively stores your security event log data, thanks to impressive compression ratios. OpenText SmartConnectors allow aggregation and filtering of events for additional log storage savings. Whether you choose to deploy with one node or multiple, it is built to scale with your needs.

Resources

St Mary MacKillop College Canberra embraces enterprise-grade cyber resilience with OpenText Cybersecurity suite of solutions.

Read more ›

OpenText Security Log Analytics is a scalable, high performance, comprehensive, and cost-effective log management, compliance, and threat hunting solution developed for security professionals by security experts with more than 20 years of domain expertise. Its holistic approach uniquely unifies robust big data ingestion (collect, normalize, aggregate, and enrich) from more than 480 sources across sprawling and diverse infrastructure with advanced security analytics and a native SOAR for elevating threat investigation and response' effectiveness and efficiency.

OpenText™ Security Log Analytics