CASE STUDY

Modern Embedded Analytics platform for SIEM application

intellicus

Overview

The company is one of the world's largest enterprise software providers. Their vast range of solutions includes analytics and big data management, application delivery management, IT operations management, log management, among others. Over 45+ years, they have partnered with more than 40,000 businesses. They have successfully assisted the digital transformation journey for their customers and serve 98 out of fortune 100 companies.

The organization was looking for a modern analytics platform that could become a part of their log management application's workflow and assisted their customers to perform forensic investigation on logs. They wanted to integrate secure, high-performance analytics capabilities into their solution

Business Challenges & Requirements

The organization's log management solution helps their customers record, monitor, and track logs from all their connected devices, streaming networks, syslog, custom applications, social media, and cloud services. It further helps the customers connect more than 480 varied data sources to assimilate security data. The company needed an embedded analytics solution that could collate and process these logs and translate them into useful information in the form of reports and dashboards.

They were looking for a solution that would:

- Get tightly coupled to their application, with similar UI and customer experience.
- Connect to their proprietary big database management system.
- Smoothly process data from more than 480 data sources.
- Enhance the querying process and provide dynamic query suggestions that would minimalize the efforts needed to query events and logs.
- Provide pre-formatted, built-in reporting content, reports and dashboards for end users such as vulnerability overview reports, device monitoring dashboard, compliance, safety, and accountability reports etc.
- Analyze billions of events per day from across the organization.
- Monitor security logs and events in real-time.
- Perform risk assessments concerning vulnerabilities, device upgrades etc.
- Correlate data logs, issues and learnings from disparate data sources and bring out trends for timely identification of upcoming threats.
- Process data with data science environments like python to bring out predictive and what-if insights. Provide report formats and workflows that follow compliance and regulatory guidelines such as PCI, SOX, HIPAA.
- Automate the complete reporting process so as no human intervention is needed, and the reports can reach recipients at a prescribed time.
- Generate alert notifications whenever an anomaly occurs.
- Follow the product's user authentication and authorization workflow.

Intellicus Solution

Intellicus is effortlessly embedded into the log management application and has become a part of its workflow. It has provided a similar UI and user experience that has enabled faster user adoption amongst the company's customers. Intellicus seamlessly connects to its proprietary data source to provide high-volume, high-performance reporting. It collates data that the application collects from various sources and builds a centralized reporting interface on top of it.

The application can store years of data. Intellicus simplifies the reporting process for this high volume of data. Intellicus helps them to provide pre-formatted built-in reporting content, reports and dashboards formats that quickens the analytics process of their customers. These pre-built report formats follow compliance, data privacy, and regulation guidelines, thereby decreasing the time required to document for compliance.

Intellicus helps in analyzing billions of events per day, corelating these data points and in bringing out critical information. The users can perform risk assessments, monitor logs, threat hunting, and analyze devices security data in real-time. Intellicus offers built-in data science actions and helps the users bring out predictive and what-if insights in simple steps. They can bring out correlations from historical data, detect threats and timely act on these inputs.

Intellicus has seamlessly embedded into the application's security workflow. It manages the authentication and authorization mechanisms seamlessly, without exposing any data or user information to the outside world.

Intellicus helps users create threshold points and generate alert notifications whenever an anomaly occurs. Users do not have to fret for critical intelligence at the right time as Intellicus has automatized their reporting process.

Business Benefits

- Seamless integration into the security applications' complex architecture with a similar look and feel.
- Ability to read and analyze billions of events per day.
- Connectivity to the proprietary big data platform. Built-in reports, dashboards that follow all the required compliance norms.
- Alert notifications to timely act on critical data inputs.
- Forecasts and trends to efficiently hunt threats.