Analytics Driven Security Management

Multiple Data Source Connectivity

Real-Time Insights & Alerts

Predictions of Breaches & Threats

intellicus

SIEM customers are now demanding deeper insights from their data. They need a solution that goes beyond simple information and event management to deliver real-time alerts and predict different patterns of malicious activities. Intellicus seamlessly integrates with different SIEM tools to collate and analyze data across the enterprise. Analytics-driven SIEM with Intellicus enables IT teams to monitor threats in real time and respond quickly to incidents to evade or minimize the damage.

Multiple Data Sources

Intellicus can read and analyze data coming from multiple assets like machine data sources, business applications, and proprietary data sources. It enables you to capture insights from across your infrastructure in a single screen.

Real-Time Monitoring

Intellicus monitors data logs real time and sends out alerts to all stakeholders instantly. It can read 5000 events per second, or more, depending on device capacity. Whether the data comes from weblogs, application usage or digital transactions, real-time monitoring with Intellicus enables rapid action on breaches. Intellicus presents real-time insights as actionable, responsive dashboards. Users can click and act upon a value, right from the dashboard.

Machine Learning and Predictive Analytics

Intellicus can collect data from different sources and identify multiple patterns in that data using machine learning algorithms. On basis of these patterns, Intellicus can predict the next threat or attack. These predictions help in alerting the teams and enable them to address future threats today.

Risk Assessment

Intellicus reports correlation and probability of any malicious activity as it occurs. It also empowers IT teams find anomalies at the aggregation level and then drill down into details. With Intellicus, users can set multiple conditions to track breaches.Intellicus processes data on basis of these conditions and alerts the users when any set condition is met. Intellicus further simplifies analytics by presenting these insights as highly interactive reports and dashboards. Users get 360 degree analysis in a single screen and can further drill down to points of interest.

IT departments can benefit from Intellicus by:

- Tracking user activity
- Tracking traffic sources to identify suspicious visits
- Analyzing malware activity
- Analyzing firewall activity
- Tracking access and authentication

© Intellicus Technologies.

info@intellicus.com | www.intellicus.com