Security Information & Event Management (SIEM)

SIEM solutions are rapidly evolving to enable more accurate identification of unusual and malicious activity. BlueVoyant engages deep human expertise to turn volumes of data and alerts into actionable intelligence.

Managing a SIEM takes time and expertise that most resource-constrained organizations do not have. The complexity and cost of SIEM keeps many organizations from pursuing it.

The BlueVoyant Managed SIEM solution gives you a single tenant Splunk® custom log ingestion, hosted by BlueVoyant. You get:

- Custom data/log collection and analysis
- Dedicated and fully managed infrastructure
- Custom support for correlations and content
- Hands-on access to data

Perform Searches

In addition to BlueVoyant's services, your team can perform their own searches, develop correlations, execute log collection, facilitate analysis, and detect threats on-premise and/or in the cloud.

We can help you maximize your existing platform investments to improve your return on investment. View content dashboards, correlations, data models, and architecture to manage your security program successfully.

Fully Managed SIEM

Managed SIEM monitors on-premise and cloud environments with Splunk® Enterprise Platform. Our experts can help IT make sense of the data.

We help you analyze millions of data points to identify and respond to threats before they wreak havoc on your network. We utilize orchestrations, playbooks, and automations to accelerate enrichment and expedite incident responses.

Monitoring of Splunk On-Prem

If you already have Splunk deployed on prem, we can monitor security alerts 24x7 from our SOC. We start by quickly assessing your instance's capabilities and then rapidly enhancing them so that you get the most from your Splunk® investment.

Want to move your on-prem Splunk to the cloud? We provide migration and full hosting and management via our Managed SIEM offering.

KEY FEATURES & BENEFITS

ADVANCED THREAT INTELLIGENCE
Our proprietary, open-source, and dark web intelligence is leveraged to expedite triage and enrich investigations conducted by the SOC. **Greater threat intelligence translates into faster identification and remediation of security events.**

TECHNOLOGY, ACCESS, AND VALUE
BlueVoyant's technology platform leverages Splunk® Enterprise - a dedicated and fully managed infrastructure. **Access best in class tech, with full data access; creating a new and enhanced value for you at a lower cost.**

24/7 SECURITY OPERATIONS CENTERS
The BlueVoyant SOC monitors the collection of cyber security data and is ready to respond to anomalies. **The SOC can respond to security events 24/7, giving you peace of mind that breaches won't go unnoticed.**

CUSTOM CORRELATIONS
BlueVoyant experts help you to generate custom correlations and content. **Our fully trained and certified experts set your IT staff up for success and allow you to make sense of all the disparate data.**

COMPLIANCE
Prepare documentation quickly and easily with the BlueVoyant technology platform. **You'll have access to all necessary data required for meeting audit collection and legal notification requirements.**

WAVELENGTH™, CLIENT PORTAL
We allow unprecedented visibility of our work so you can examine what we are doing on your behalf. **You have full event visibility and access to at-a-glance insights and compliance reports.**

SUPPORT TO ON-PREM SPLUNK INSTANCES
If you want to extract additional value from your on-prem Splunk instance by moving to our **fully managed Cloud**, we can perform migrations for you. We can also provide you with a Health Check for your Splunk instance and full remediation capability. Our SOC can also **monitor security alerts from your on-prem Splunk® and give you 24x7 coverage.**