BlueVoyant

Managed SIEM with Splunk® Enterprise

BlueVoyant Experts Can Help You Leverage Splunk® Enterprise to Analyze Your Data and Respond to Threats Before They Wreak Havoc

As the nature of cyber attacks constantly changes, so does our commitment to keep ahead of them. SIEM solutions are rapidly evolving to enable more accurate identification of unusual and malicious activity. However, it takes deep, human expertise to turn the volume of data and alerts into actionable intelligence.

Managing SIEM takes time, resources and expertise that resource-constrained organizations do not have. The complexity of managing SIEM solutions is beyond their capability.

The BlueVoyant Managed SIEM solution gives you access to a dedicated Splunk® Enterprise environment, hosted by BlueVoyant, enabling hands-on access to data. In addition to BlueVoyant's services, your team can perform their own searches, develop correlations and execute log collection, facilitate analysis and detect threats on-premise and/or in the cloud.

The BlueVoyant Technology Platform correlates and analyzes network logs in real time, aggregating disparate data and applying the latest threat intelligence to filter background noise and identify security threats that really matter. We can help you maximize your existing platform investments to improve your return on investment.

Leverage the BlueVoyant Technology Platform, and our deep expertise, to maximize your Splunk investment. Our experts and platform deliver the right content dashboards, correlations, data models and architecture to manage your security program successfully.

BlueVoyant Managed SIEM monitors on-premise and cloud environments with Splunk® Enterprise Platform, supported by BlueVoyant experts.

Managed SIEM can help you maximize existing platform investments while improving your visibility into threat activity, giving resourced-constrained teams access to a powerful platform for advanced security protection.

Reduce the frustrations and complexities of managing Splunk® Enterprise with BlueVoyant's team of SIEM experts.

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. Delivered as intelligence reports with new detections outlined with classifications of threat indicators.

Benefit: Greater threat intelligence translates into faster identification and remediation of security events. It also reduces the risk of data loss and business disruption due to successful attacks.

ROBUST TECHNOLOGY PLATFORM

BlueVoyant Technology Platform leverages Splunk® Enterprise: A dedicated and fully managed infrastructure, giving you access to best-of-breed, scaled, search and SIEM platform.

Benefit: We put the security large enterprises can afford within your reach. Your company isn't required to purchase or maintain expensive cybersecurity tools or hire expert staff.

24/7 SECURITY OPERATIONS CENTERS

BlueVoyant SOC monitors the collection of cyber security data and is ready to respond to anomalies that are highlighted automatically through the Platform and our proprietary Threat Intelligence data set.

Benefit: Our Platform allows our experts to prioritize alerts, detecting the most likely threat behavior, giving our analysts time to focus on the alerts that matter. Plus, the SOC can respond to security events 24/7 giving you peace of mind that breaches can't spread unnoticed.

ACCESS TO SIEM EXPERTS

Contact BlueVoyant experts for security questions and to generate custom correlations and content.

Benefit: Our fully trained and certified experts set your IT staff up for success and allow you to make sense of all the data.

BlueVoyant

THOROUGH DOCUMENTATION

Compliance documentation and reporting is easy; the BlueVoyant Technology Platform can provide all necessary data to the meet audit collection and legal notification requirements. You can meet compliance requirements from audit trail collection and reporting.

Benefit: Generate any compliance report with easily accessed data.

WAVELENGTH™, CLIENT PORTAL

Our Client Portal, Wavelength™, is always available. We allow unprecedented visibility to our clients to examine the work we are doing on your behalf.

Benefit: Wavelength™ gives you full event visibility and access to at-a-glance insights, compliance reports, and complete network visibility so you know what we know. You can see live what we're working on.

Why Clients choose Managed SIEM (Splunk® Enterprise)

Clients choose Managed SIEM (Splunk® Enterprise) to gain access to BlueVoyant experts who can help them make sense of the data on-premise or in the cloud.

The BlueVoyant SIEM/Log Management security information and event management software is designed to automatically monitor for traces of malicious actions that could be buried in log files together with other legitimate entries.

We help you analyze millions of data points to identify and respond to threats before they wreak havoc on your network. Utilize BlueVoyant's orchestration, playbook, and automations to accelerate enrichment and response action.

We put the security large enterprises can afford within your reach and help set your IT staff up for success.

For more information please visit:
www.bluevoyant.com

Secure your business now:
sales@bluevoyant.com