Managed SIEM

BlueVoyant®

INTRODUCTION

"BlueVoyant offers the private sector exceptional cyber defense capabilities through our unique data assets, world-class threat intelligence experts, and managed security services. Helping to defend businesses around the world against well-developed cyber attackers, we excel in delivering unparalleled visibility and insights for our customers. At our core, we believe in providing resource-constrained organization of all sizes with the same level of cybersecurity previously only available to the largest and most well-defended businesses and government agencies."

Jim Rosenthal, CEO | Former Chief Operating Officer of Morgan Stanley
Past Chairman of the Securities Industry and Financial Markets Association and its Cybersecurity Committee.

OUR SERVICES

Threat Intelligence

Managed Security Services

Professional Services

About BlueVoyant

A first-things-first cybersecurity company focused on delivering best-of-breed technology and outstanding customer service to businesses around the world. We believe in the democratization of cybersecurity - offering robust solutions and tools to businesses previously ignored and under-served. Through our advanced Threat Intelligence, Managed Security Services, and Professional Services, we excel in intelligence gathering, cybersecurity defense, and detection of attacks with response coupled with remediation. With global SOCs, we are prepared to protect the world over from well-financed threat actors and their newest tools of attack. Learn more at www.bluevoyant.com

Managed SIEM

BlueVoyant Managed SIEM provides Security Information and Event Management using industry leading tools, with simplified pricing, that is amplified by our expert customization, so that the system you're using will fit the needs of your business.

We believe in democratizing next-generation cybersecurity by delivering services that offer the same level of protection enjoyed by large enterprises, available to small- to mid-sized businesses at a fraction of the cost. Moreover, we provide advanced security capabilities, including User and Entity Behavioral Analytics (UEBA) **natively** within our platform. Additionally, we take the complexity out of ingesting, normalizing, and storing your data, using advanced data management tools to increase efficiency and decrease costs traditionally associated with leading SIEM technologies.

The BlueVoyant Security Platform, inclusive of Splunk®, correlates and analyzes network logs in near real-time, aggregating disparate data and applying the latest threat intelligence. This delivers clean, normalized, searchable information that identifies critical security threats, without noisy alerts.

BlueVoyant simplifies and right-sizes the implementation of our SIEM solution by tuning the system to your unique environment, using the same expertise and design principles from the largest and most sophisticated Security Operations Centers in the world. We effectively reduce the number of resources required to manage your security program while increasing your efficacy in monitoring threats.

As a data aggregation, search, and reporting system, SIEM can help you maximize your existing platform investments and improve the return on your technology and resource investments.

Cybersecurity professionals spend

25% **of their time responding to**

false positives

BlueVoyant®

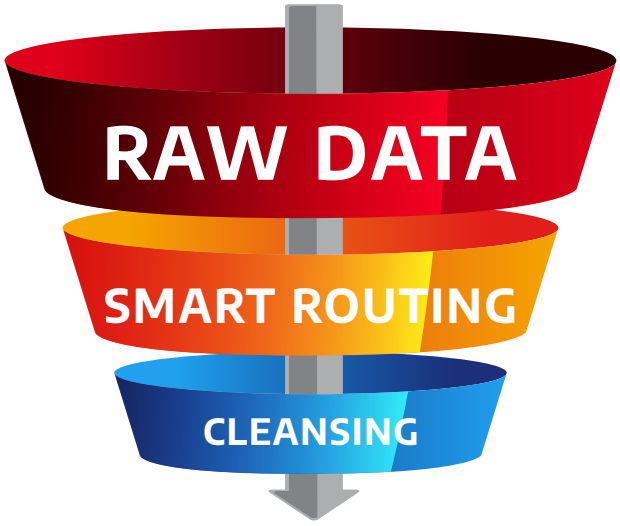
Overview

Ingest & Aggregation: Connecting, filtering, and sorting all log data into the BlueVoyant platform for a "single-pane-of-glass" view at your information. At this step we remove data with no security value (including data with Privacy risks) before we ingest into our environment.

Baseline and Alert: We assess "normal" activity on your network and apply incident type classifications for easy identification and categorization.

Coordinate & Consult: We work with you to develop additional customizations to your environment.

Analyze & Share: Generate custom reports that you can share with stakeholders to show your existing cybersecurity posture, and create dashboards to pro-actively track risks and policy adherence.



The starting price of a cybercrime tool kit on the Dark Web =

$1 USD

Cybersecurity Ventures

The cost of cybercrime is $2.1 TRILLION USD globally in 2019

Juniper Research

Set Up

Team deploys your unique, single tenant Splunk® instance using BlueVoyant's platform.

Our SOC investigates every alert, tuning and providing custom configurations to the system, ensuring limited operational interruption.

You provide requests for custom correlations and visualizations - BlueVoyant sets up your environment to provide you with best in class detection and response, while still leaving you with hands-on access to your data.

Have Splunk® On-Prem? We can help you enhance and provide 24x7 monitoring

BlueVoyant®

HOW WE'RE DIFFERENT

Rapid assessment of unusual and malicious activity can be achieved with any SIEM solution. What differentiates BlueVoyant's Managed SIEM is the team of experts who can turn your data avalanche into a meaningful data story that spells out what, how, and why something happened.

The time, resources, and expertise required to manage the complexity of SIEM can seem daunting. By engaging BlueVoyant to manage your SIEM, you can gain access to a custom, down-market priced Splunk®, single-tenant hosted log ingestion system.

Use Managed SIEM to consult with our CyberIntel Experts to develop unique searches, custom correlations, and track threats on-premise and in the cloud.

Gain the edge on threat actors by having real-time visibility into all of your network logs minus all of the false, duplicate, and noisy alerts that come with "off the shelf" solutions.

Let BlueVoyant deliver a solution that helps by developing content dashboards, correlations, data models, and an architecture that you can use to effectively manage your security program. You can maximize your current investments while increasing your awareness without additional internal support.

CORE FUNCTIONS

- 24x7 Advanced Threat Detection
- Full Investigation
- Expert Response
- Comprehensive searchability
- Compliance Reporting

FEATURES

» Simple, Headcount-based Pricing
» 365 Days of Searchable Logs
» Security Monitoring and Incident Response
» Advanced Threat Intelligence
» Log Aggregation, Search and Reporting
» Over 2 Dozen Dashboards and Reports Off the Shelf
» Report Customization and SIEM Engineering Support
» Normalization of Data
» Filtered Notifications and Alerts
» SOC Automations for Remediation
» Threat Response Playbooks
» Custom Correlations and Data Reporting
» 24/7 SOC - Fast Time to Respond

BlueVoyant®

WORKING WITH US

Have you experienced a breach? Our incident response team can help. Contact us 24/7.

In the event of an incident - BlueVoyant's Professional Services team can work with you to seamlessly generate custom forensic reports and an alert set based on analytics that match a rule set that indicates a security issue.

We are a company that mutually reinforces your business through our unique business units. This allows you to choose the security that is robust, relevant and right-sized to your present needs and as they scale.

LEADING YOUR TEAM

Managed SIEM is supported by expert Security Analysts who operate 24/7, across multiple locations within Security Operations Centers (SOC). Customers leverage Wavelength™, BlueVoyant's client portal, to access real-time information about alerts and to track remediation on incidents.

This web based portal enables approved client employees to interact with BlueVoyant's security operations center analysts, view all detected assets, and if applicable, view vulnerabilities. Dashboards provide a snapshot of real time security posture.

GENERATING RESULTS

Reports are available through Wavelength™ and include client environment content related to alerts, incidents, indicators, assets, and vulnerabilities.

Updates on the threat landscape, sectorial, and intelligence summary reports are developed by the BlueVoyant Threat Fusion Cell - an elite team of Security Analysts and threat researchers focused on identifying and prioritizing information about threats using BlueVoyant proprietary and open source intelligence.

WORKING FASTER

Orchestration and automation allow the SOC to accelerate triage, reduce false positives, and improve mean-time to resolve. FFIEC and NCUA-ACET automations help financial institutions manage the growing number of security compliance management challenges that impact operations. Mandatory risk assessments and compliance reports are burdensome, but BlueVoyant has automated many of the compliance controls to reduce the time-intensive reporting process.

KEEPING IT SIMPLE

Through a single pane of glass, you can address all of your data and respond faster to anomalies and incidents. BlueVoyant's services all work independently but are mutually reinforced. If you require remote endpoint protection with NGAV, or threat hunting - our Managed Detection and Response service can help neutralize incidents and increase your antivirus blocking and detection.

Whether you need increased threat intelligence, managed security services, cyber forensics with incident response, or proactive services to become better prepared - BlueVoyant provides exceptional intelligence and cyber defense.

The average cost of a data breach by 2020 will be $150 Million and the global cost of ransomware will reach

$20 Billion by 2021

Juniper Research & Cybersecurity Ventures