FlowIntelligence™ *IQ!* Analyst

Advanced Analytics for Cyber Security

bivio Networks

Solution Highlights

Speed

- Distributed search with concurrent queries across multiple cluster nodes
- Index on write, with all data fields indexed
- Schema on write of data, submit and receive query responses across multiple data indexes in minutes or less

Scale

- Collect and ingest data from many high-speed network sensors or third-party data sources simultaneously – 10's of millions of documents per second
- Retain, query and analyze data in a tiered architecture with Hot, Warm and Cold data nodes

Relevance

- Open, modern, extensible schema with data fields indexed using Elastic Common Schema (ECS)
- Enriched data for content and context
- Cross-source analysis of diverse data

Big Data Analysis for Cyber Security

The complexity of the cyber threat landscape can overwhelm the cyber analyst. The number of data sources and volumes of data that are available to the analyst creates additional pressures to provide an accurate analysis of the cyber terrain. Many cyber tools have implemented closed, custom analytics systems that create "analytic stovepipes" and the threat actors use that to their advantage in heterogeneous cyber security environments. In addition, the cyber security analyst must address multiple questions for the cyber security ecosystem, including:

- How can the organization effectively collect data from all cyber security and IT assets to provide a complete picture of the cyber terrain including threats and breaches, lateral threat movement and data exfiltration?
- How can the organization gain attack chain visibility to identify the phase of the breach for a threat and mitigation steps to resolve the event?
- How can the organization determine the specific IT assets are involved to formulate a mitigation concise strategy?
- How can the organization enrich the data collected with threat intelligence and GeoIP data to enhance the analysis process for higher fidelity and lower false positive alerts?
- How can the organization reduce the mean-time-to-detection, threat actor dwell time and mean-time-response?
- How can the organization leverage informed machine learning to detect sophisticated attacks, automate and prioritize the analysis process as well as reduce the threat actor's dwell time in the network?

IQ! Analyst is a key component of the FlowIntelligence™ suite of cyber tools. The solution breaks down the "stovepipes" with an open analytics system, collects data from any systems and it provides the Big Data Analysis for Cyber Security where it answers these questions and many others.

Functional Overview

IQ! Analyst enables organizations to gain visibility into the enterprise threat landscape and aids in rapidly mitigating threats or events that affect IT operations. Essential to this analytics solution is ***Speed, Scale and Relevance*** for mitigation of cyber threats. *IQ!* Analyst is an open analytics environment powered by Elastic®. It collects data from multiple sources including FlowIntelligence™ and third-party network sensors, Firewalls, EDR solutions, Identity and Access Management, Vulnerability Scanners, NetFlow sources, syslog, audit and file data source, windows logs, as well as numerous applications.

Speed

The analytics environment gains speed in the analysis process by performing index on write. This enables the analytic environment store data in an efficient and effective manner. When the data is stored, it utilizes a schema on write process that aids in accelerating queries across multiple data indexes. When queries are issued, it employs a distributed and concurrent process to retrieved data from multiple nodes. Leveraging a distributed ingest model, multiple nodes can ingest from high-speed data sources.

Scale

Extreme analytics scaling with high performance data ingest technology - 10's of millions of events, records and data elements or more per second. This equates to 100's of Terabytes and beyond per day. Collection from multiple sources is enabled with lightweight data harvesters for logs, event, statistics and network records from the entire enterprise. The solution unlike other vendors does not force an organization into a license scheme of "pay-by-the-Gigabit" or penalize for data retention. Many cyber threats take weeks, months or even years to fully develop and retaining data is crucial to fully understand the scope and complexity of a cyber threat. *IQ!* Analyst enables the organization to retain data with leveraging a tiered architecture for hot, warm and cold data that exceeds any other solution's capability and does not penalize them. It provides a lower Total Cost of Ownership.

Relevance

Unlike other solutions, *IQ!* Analyst indexes every data field presented to the analytics environment. This enables complete metadata analysis by utilizing a common, modern, open and extensible schema powered by Elastic Common Schema (ECS). This creates relevance of the data where other solutions fall short. Enrichment of data in the cyber hunt process means that the analyst gains deeper insight into cyber threats. Adding threat intelligence indicators to the data increase the relevance to identify threats, campaigns and potentially actors or sources of cyber threats. Additionally, geospatial information such as latitude and longitude information based on the IP address and Autonomous System Number (ASN) enables the analyst to perform targeted analysis. Other information such as vulnerability data, server and endpoint data, LDAP and Windows user data can be incorporated in the analysis process for greater content and context. This reveals where an attack originated, how a compromise occurred, which resources were compromised, and more.

Open Architecture

IQ! Analyst is an open analytics environment. It provides the single pane of glass into the data from the enterprise and allows the analyst to collect, index, normalize, query, analyze, visualize and pivot on multiple data elements. It ingests data from multiple sources to include syslog, .csv, textual and JSON data.

Secure

The analytics application resides on a Red Hat Enterprise Linux operating system that is capable of meeting the most stringent certification requirements from the US Government. It is a STIG-ready operating system to meet the Department of Defense standards and Bivio proactively maintains the operating environment with periodic updates as a part of the continuing support function. The analytics environment also implements security for secure transport of the data and role-based access control. Finally, field-level security can be leveraged to protect sensitive data.

Gain the advantage over the adversary by leveraging global threat intelligence to enrich the network traffic metadata and enable rapid threat identification with key records of interest. Utilizing GeoIP information enables Geo-Spatial analysis of the threats, events, campaigns and actors which includes mapping of complex data.

Reduce the mean-to-detection, dwell time and mean-time-to-response. Rapidly detect, identify and mitigate zero-day attacks, network breaches and data exfiltration issues while minimizing false positives.

Full attack chain visibility with low false positives and high-fidelity alerts. Identify and analyze the attack chain based on Mitre ATT&CK® model. Leverage on-line references to gain clarity on the individual attack phases and suggested response process.

Robust API for inbound and outbound integration. Collect data from non-traditional sources with generic data harvesters. Provide data for north-bound analytics systems and manager-of-manager systems.

Automated data integration via API client on FlowIntelligence™ Threat Analyst, Cyber Analyst, Deception Analyst and *IQ!* Sandbox solutions. Implement data harvesters for enterprise assets to perform flow collection, log analysis, system audit and windows event logging. Logging and audit modules are available for many popular applications. Custom modules are also available through the Professional Services team.

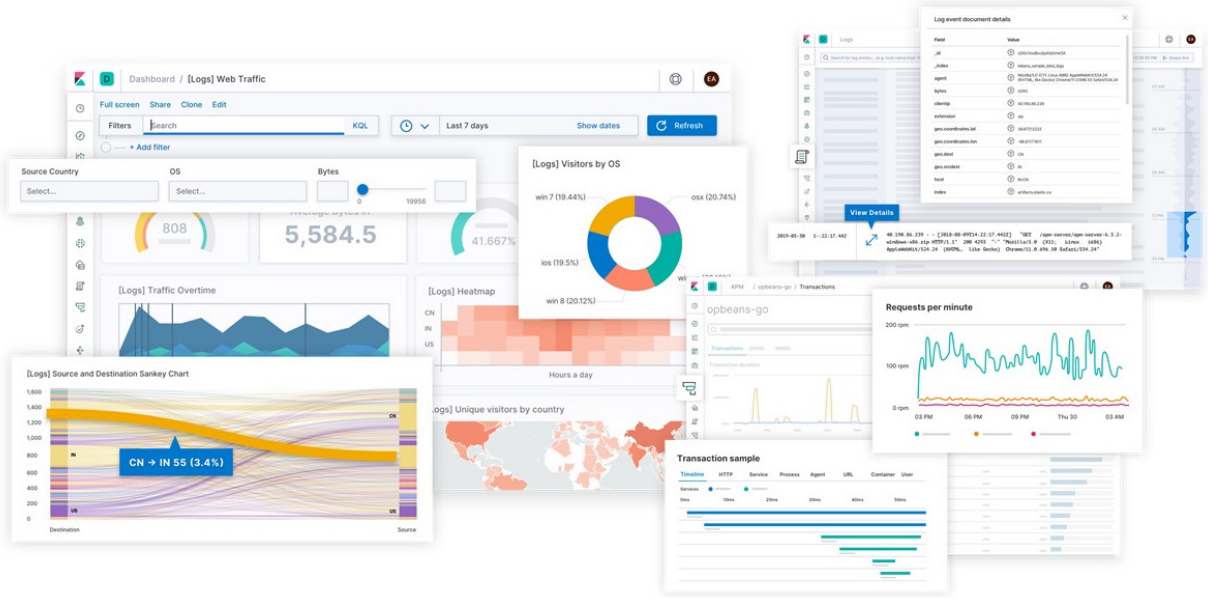
Analyze data using informed machine learning to detect sophisticated attacks. Leverage the enrichment process to find the "nuggets" for anomaly detection with unsupervised algorithms, continuous analysis model, timeline series analysis, population outliers and forecasting. The machine learning engine contains more than 70 embedded models for advanced analysis to aid the analyst in automating the cyber hunt process.

Fastest industry time for dynamic analysis and actionable results. Detect and respond to threats before attackers have a chance to steal your valuable data or disrupt information technology operations in the enterprise. Fast search across multiple datasets decreases the mean-time-to-detection thereby reducing threat actor's dwell time and the organizations risk to exposure from an incident, ultimately saving money by rapidly mitigating a cyber breach.

Finding the adversaries hiding in plain sight is the most challenging problem for cyber analyst and trying to discern the threat from all the noise inside an enterprise network is extremely difficult. *IQ!* Analyst filters the noise by allowing custom or unique plain language queries across multiple data indexes to ask the hard question "Who or what shouldn't be in my network".

Leverage role-based access control to invite users and stakeholders into specific spaces. Multi-user operation gives users access to individual "workspaces" with distinct content for each user or class of users.

Monitor and maintain health of the analytics environment. Perform real time health checks of the data collectors and the analytics cluster with embedded health checks. Rapidly resolve any issues with either a data harvester or a cluster node and minimize data loss issues.



Visualizations that Cyber Analyst Love

IQ! Analyst provides the ability to query and visualize the data. It contains hundreds of pre-defined visual representations for the data elements associated with each data harvester and it enables the analyst to rapidly assess information from those data sources. With the analytics environment, the analyst can select one or more data elements and combine those into a unique visualization. Vega provides the ability to create custom visualizations and Bivio Networks' solutions engineers can also deliver additional customization of the analytics visualization environment. The visualization engine provides multiple types of geospatial views to include bar charts, line and area charts, circular charts, dot and scatter plots, distributions, geographic maps, heat maps, tree diagrams, network diagrams and many others. Organizations can infuse their brand into the analytics with Canvas. This enables security teams build visualizations and dashboards as well as easily share key performance indicators data for various stakeholders.

Turn-key Solution

IQ! Analyst is delivered as a turn-key analytics solution on Bivio Networks Atlas Cloud Applications platforms. Atlas Cloud Applications platforms permits the solution to scale from the small and medium enterprise to the Fortune 100 global operations. The supporting hardware platforms are designed as hyper-converged solutions with carrier-grade redundancy features to ensure non-stop operations. The analytics operating environment incorporates its own redundancy in the software architecture to ensure mission-critical support for Bivio Networks' customers. Scaling the analytics environment for each organization is done by our Solutions Architects. They can perform a comprehensive analysis to identify, design and deliver a complete solution to meet the organization's requirements.

Summary

When Speed, Scale and Relevance of cyber security data matters, *IQ!* Analyst delivers a robust, open and extensible analytics solution to meet these requirements. This solution truly enables the cyber hunt process and provides clarity to find, mitigate and eliminate cyber threats. Contact your Bivio Networks' sales team to see how *IQ!* Analyst can enhance your cyber security operations team.

About Bivio Networks

Bivio Networks is a leading provider of network systems for securing, monitoring and controlling critical network infrastructure. Bivio's global customer base includes Fortune 500, worldwide government agencies and service providers. Bivio's products enable customers and partners, who include application developers and systems integrators, to develop and deploy leading solutions to secure, monitor and control customer networks. Bivio is privately-held and is headquartered in the San Francisco Bay Area.

bivio NETWORKS

Bivio Networks, Inc.
4457 Willow Road, Suite 240
Pleasanton, CA 94588
Tel: +1 925 924 8600
www.bivio.net