FlowIntelligence™ Threat Analyst

Advanced Breach Detection and Protection

bivio networks

Highlights

High Performance

- Blazingly fast with throughput at rates up to 100 Gbps full duplex
- 100's of thousands to millions of connections per second
- Millions to 10's of millions of simultaneous sessions analyzed
- 10's of thousands concurrent rules

Intelligent Operations

- Dynamic analysis with integrated threat intelligence indicators and automated rules from the FlowIntelligence™ Cloud
- Advanced file scanning and analysis framework with machine learning malware analysis engine

Open Architecture

- Open and extensible sensor engine with ability to add functionality via plug-in architecture
- Threat information sharing via embedded open data exchange API and message broker technology
- Interface with third-party tools and solutions via embedded SOAR and open data exchange API

Cyber Security as a Service

The rapid adoption of cloud-based applications and the reliance on the world-wide web to deliver services creates additional pressure on enterprise and service provider cyber analyst to detect, mitigate and protect from cyber threats. Cloud-based based applications, social media, Email and other applications all bring risk of an intrusion or breach in the network. Mobile users with Bring Your Own Device (BYOD), Internet-of-Things (IoT) and SCADA adds complexity and challenges for the security operations teams. They now have to address multiple questions for the network ecosystem, including:

- How to effectively operate and defend networks from external and internal threats?
- How to identify complex or advanced threats and malware?
- How can the cyber analyst implement dynamic analysis of the threat landscape?
- How can the organization protect users or subscribers from threats, web services or sites with poor reputation or know risks, identify potential applications that may be harmful to users or subscribers and block known malware embedded in network traffic?
- How can the cyber analyst perform automated deep file inspection and analysis for advanced malware detection?
- How can the organization ensure that network operations meet the data regulations and compliance requirements?

Bivio Networks' Threat Analyst is a key component of the FlowIntelligence™ solutions for effective defense of enterprise and service provider networks. It answers these questions plus provides proactive, dynamic breach detection and prevention capabilities.

Features and Capabilities

FlowIntelligence™ Threat Analyst provides advanced network breach detection and prevention. The features and capabilites are summarized below.

Embedded Advanced Threat Protection

Leverage multi-layered network breach defense with heuristics and malware analysis to identify and block advanced persistent threats to or from the enterprise. Implement custom whitelist/blacklist coupled with file and web reputation data for reputation analysis and blocking. Tune rules with Threat Risk and GeoIP location data for advanced network protection.

Deep Packet Inspection

Inspect network traffic and recognize threats to the environment. Analyze applications through layer 7 of the OSI model and identify activity that creates a security concern. Alert, log and block specific threats or events with rust-based analysis. Gain speed-to-decision and reduce the mean-time-to-detection utilizing dynamic analysis with threat intelligence indicators from the FlowIntelligence Cloud.

Malware Analysis

Protect users and subscribers from embedded malware in network flows. Automatically alert or block known web sites and URLs engaging in malware delivery. Perform deep file inspection to identify files in a network flow that may contain embedded malware. Interface with malware sandbox technology to deliver files of interest for indicators of compromise analysis.

File Scanning and Analysis Framework

Expose hidden or unknown threats to the enterprise through the File Scanning and Analysis Framework. Threat Analyst enables Deep File Inspection and unknown files can be presented to the *IQ!* machine learning-enabled malware analysis engine. Each file is analyzed and scored for benign, suspicious and malicious content. It addressed the unknow and zero-day threat for advanced network protection.

Automation and Orchestration

The sensor leverages an embedded workflow engine to automate many security and response functions. It contains a visual interface to implement custom workflows. Standard workflows include Deep File Inspection workflow and third-party integration with via embedded data exchange. Bivio Networks' professional services team can assist in developing additional custom workflows.

Ease of Implementation

Threat Analyst operates in transparent mode and does not require an IP address for either the outside or inside interface(s). Simply provide a local IP address for the management and data interfaces, configure the destination for the log data, place the system either inline or attach to a network tap-span port and begin operations. It's just that simple!

Scalable Operations

Threat Analyst scales up to 100 Gbps (Full duplex). Powered by BiviOS™ and the FlowIntelligence™ Adaptive Cyber Defense platforms, Threat Analyst features unparalleled performance. It the fastest network breach and prevention solution on the market today.

Friction-less Updates

Rules, Threat Intelligence data and sensor application components are updated through the FlowIntelligence Cloud. Rules and threat intelligence data can be updated as often as the cyber analyst desires in intervals as short as five (5) minutes. Typical rules updates are performed daily to pick-up additional rules that are developed and released. Operating environment and application updates are done on an "as needed" interval and typically the customer would be notified by the Bivio Networks Technical Assistance Center to initiate a system update.

Data Integration

Threat Analyst contains automated data integration via API client to FlowIntelligence™ *IQ!* Analyst. It supports integration to third-party analytics via optional Splunk forwarder or S3, and RSyslog or the integrated Kafka message broker. Custom integration is also available through the Professional Services team.

Open Architecture

Threat Analyst features an open sensor engine environment. It contains a plug-in architecture to add functionality to the ecosystem. Bivio Networks' professional services teams can facilitate new or custom features.

Rules Management and Multi-Tenancy Operations

Threat Analyst features embedded rule and sensor management. Through a web user interface, the cyber analyst can add, update or delete rules. They can also implement custom or targeted rules through this interface. Rules can be applied globally or to specific customers or organizations via a VLAN or customer ID for multi-tenancy operations by service providers.

Turn-Key Solution

Threat Analyst is delivered as a turn-key Network Breach Detection and Prevention solution on Bivio Networks FlowIntelligence Adaptive Cyber Defense platforms. The Adaptive Cyber Defense platforms permits the solution to scale from the small and medium enterprise to the Fortune 100 and Service Provider network speeds.

The feature-rich hardware platforms are designed with carrier-grade redundancy qualities to ensure non-stop operations. The solution incorporates an optical bypass switch for in-line operations to ensure mission-critical support for Bivio Networks' customers.

Scaling the sensor 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

Threat Analyst is comprehensive, advanced breach detection and prevention solution. It contains intelligent features for innovative detection of threats and malware to protect users and network subscribers. It is in an elite class for its performance, features and capabilities. Contact the Bivio Networks sales team to see how Threat 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 1000, 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, Inc.
4457 Willow Road, Suite 240
Pleasanton, CA 94588
Tel: +1 925 924 8600
www.bivio.net