FlowIntelligence™ Threat Analyst

bivio NETWORKS

Advanced Threat Fusion and Breach Detection-Prevention

Key Benefits

- Scalable network breach detection and prevention sensor up to 100Gbps

- Static, dynamic and custom PCRE-based analysis

-Threat fusion analysis with STIX, CYBOX and MAEC threat intelligence indicators

- Extreme scaling in PCRE-based analysis with HyperScan®

- Deep file inspection and malware analysis automation with effective machine learning

- Threat sharing, unified threat response and analytics environment

- Fully integrated, high performance, secure platform and sensor solution

- Integrated with FlowIntelligence analytics environment

- Integrated with enterprise management via Systems Management Center

- Embedded API's for threat sharing and active response

www.bivio.net

Network Threat Analysis 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 analysts to detect, mitigate and protect from Threat 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 fuse real time threat intelligence indicators for dynamic breach detection and analysis?

How to identify complex or advanced persistent threats and malware?

How can the security operations team 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 or alert on known malware embedded in network traffic?

How can the security operations team 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.

Key Capabilities

The FlowIntelligence™ Threat Analysis platform provides network breach detection-prevention and threat fusion analysis. The key capabilities include:

Advanced Threat Protection

Leverage multi-layered network breach defense with heuristics, threat fusion 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. PCRE rules can be applied globally or to specific customers or organizations via a VLAN or customer ID for multi-tenancy operations by cyber operators or managed service providers.

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. Perform analysis of SSL/TLS traffic and identify sessions that may contain threats with integrated JA3 feature set. 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 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.

Ease of Implementation

Threat Analyst operates in passive or transparent mode (in-line mode) and does not require an IP address for its packet collection interface(s). Simply provide a local IP address for the management and data interfaces, configure the destination for the log data, attach packet collection interface(s) to a network tap or span port and begin operations. Turn the platform on, configure the management interface, point log data to the destination analytics environment and your analyzing the cloud environment in hours, not days or weeks! It's just that simple!

Friction-less Updates

Rules, threat intelligence data and sensor application components are updated through the FlowIntelligence Cloud. Event definitions are accomplished through the user interface for automated updates. Operating environment and application updates are done on an "as needed" interval and typically the customer would be notified by Bivio Networks Technical Assistance Center to initiate a system update.

Distributed Operations

Threat Analyst features the ability to operate in an enhanced, distributed mode. The solution supports implementing physical and virtual collection platforms throughout the network and forwarding the network events via an embedded communications framework to a centralized logging process. New event definitions are sent via the framework to the collection workers for augmented analysis. Additionally, the collection workers share data among themselves to aid in advanced event identification.

Data Integration

Threat Analyst contains automated data integration via an API client to FlowIntelligence™ *IQ!* Analyst. It supports integration to third-party analytics via optional Splunk forwarder, S3, RSyslog or a Kafka message broker. Custom integration for other systems is also available through Bivio Networks' ExpertAssist™.

Open Architecture

Threat Analyst features an open sensor engine environment powered by Bivio Networks' version of *Suricata*®. It contains a plug-in architecture to add new application detection and analysis functionality to the ecosystem. It supports a framework-driven architecture for Configuration, File Analysis, Input, Intelligence, Logging, NetControl and Notice. This is supported with an open and extensible sensor engine with ability to add functionality via the plug-in architecture. Threat Analyst interfaces with third-party tools and solutions via the Open Data Layer Exchange (OpenDXL) API. Bivio Networks professional services teams can facilitate new or custom features and integration with ExpertAssist™.

"Next-generation IDS brings less false positives, more intelligence - An effective next-generation IDS can detect malicious attacks by integrating protection, analysis and response technologies, giving users better security intelligence." *Andy Briney, editor-in-chief of* Information Security *magazine*.

Threat Analyst Platforms

1, 5 and 10Gbs platform

25 & 40Gbs platform

Modular Chassis Architecure for performance scaling beyond 40Gbps

Threat Fusion

Threat Analyst supports threat intelligence indicators from commercial or private sources leveraging STIX, CYBOX and MAEC delivering threat fusion analysis. It utilizes information for IP Reputation, URL and Domain as well as Malware to execute dynamic analysis of network flows thereby significantly reducing the false positive aspects in the threat analysis process. This enables Threat Analyst to dynamically identify DDos, Botnet Command and Control, malware as well as many other critical threats.

Turn-key Solution

Threat Analyst is provided as a turn-key advanced breach detection-prevention and network threat fusion solution on Bivio Networks FlowIntelligence™ adaptive cyber defense platforms. Bivio Networks delivers both physical and virtual platforms supporting north-south and east-west threat analysis at speeds up to 100Gbps. The heart of the platform includes a robust, secure Linux operating environment and BiviOS®, Bivio Networks unique packet processing middleware technology for lossless packet processing. The physical platforms provide many key features for high availability operations including redundant hardware components, automated applications management and data interfacing for the enterprise or service provider operator. The FlowIntelligence™ adaptive cyber defense platforms permits the solution to scale from the small and medium enterprise to the Fortune 100 and Service network speeds. The feature-rich hardware platforms are designed with carrier-grade redundancy qualities to ensure non-stop operations and each platform is managed by Systems Management Center. Scaling the threat analysis 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 a comprehensive, advanced threat fusion and breach detection-prevention solution. It contains intelligent features for innovative detection of network threats and malware to aid security operation teams with cyber analysis. It is in an elite class for its performance, features and capabilities. Contact Bivio Networks sales team to see how Threat Analyst can enhance your cyber security operations team.

Recommended Expert Services

ExpertSupport™ aids organizations with proactive support for critical systems. ExpertSupport provides comprehensive software and hardware support to organizations with standard Monday through Friday, 8-5PST or ExpertSupport Plus with 24-hour, seven days a week that can include advanced replacement of a failed module. ExpertAssist™ delivers on-site services with engineering and consulting that provides installation or more detailed and complex technical services. ExpertAnalyst™ enables organizations to leverage Bivio's Threat analysis team to develop custom detection rules, events and threat intelligence indicators for use in the FlowIntelligence suite of tools.

Platform Specifications:

Features	Virtual	1-10Gbps	25 & 40Gbps	Up to 100Gbps
Operating Speeds	1,5 & 10Gbps	1, 5 & 10 Gigabits per second	25 & 40 Gigabits per second	Modular Chassis Architecture for speed up to 100 Gigabits per seconds
Network Interface	4x vNIC's (1 or 10Gbps)	4x 1Gbe RJ45 Copper or 4 x 1/10 SFP+ Copper or Optical Interfaces	2 x 25 Gigabits QSFP28 interfaces or 2 x 40Gbps QSFP Interfaces	Packet Interface Module with 2 x 100 Gigabit Ethernet and 1 x 40 Gigabit QSFP interfaces
Data Interfaces	2 x vNIC's	2 x 1Gbe RJ45 Copper	2 x 1/10Gbe SFP+ Copper or Optical interfaces	Data Offload Module with 2 x 100 Gigabit Ethernet and 1 x 40 Gigabit QSFP interfaces
Management Interfaces	2 x vNIC's	2 x 1Gbe RJ45 Copper		
Local Storage Capacity (Max)	N/A	30 TB SSD Fast Read	M.2 Dual 480GB (Raid-1) Boot and Operating System Storage. 100TB SSD Fast Read Data storage	M.2 Dual 480GB (Raid-1) Boot and Operating System Storage. 384TB SSD Fast Read
Power	N/A	Dual 120/240vac, 750w Hot-swappable PSU's	Dual 240VAC, 2000w Hot-swappable PSU's	Six (6) Grid 240VAC, 3000w Hot-swappable PSU's with Grid Redundancy
Cooling	N/A	Five (5) hot swap fans standard, Eight (8) - Maximum	Six (6) hot swap fans	Four (4) Front, Five (5) Rear hot swappable fans
Chassis Size	N/A	1.69" x 18.98 x 31.8" (One Physical Rack Unit)	3.4" x 17.08 x 32.09" (Two Physical Rack Units)	12.10" x 18.98" x 32.16" (Seven Physical Rack Units)
System Weight		48.3lbs	80.7lbs	~400lbs (fully loaded chassis)
Safety Compliance	US/Canada: UL/CSA 60950-1			
Electromagnetic Compliance	USA/Canada: FCC Part 15 and GR-1089 Europe: EC Directive, EC Council Directive 2004/108/EC, ETSI EN300 386, EN55022, EN 55024 International: CISPR 22 Class A and CISPR 24			
Hardware/Software support	Annual hardware/software support for the physical platform and operating environment – must be included at time of purchased. Contact your Bivio Networks account team for specific information on levels of support available.			
Licensing – Application, events, threat intelligence license	Licensing for Application, events and threat intelligence data is an annual subscription. The virtual platform is an annual subscription license. Contact your Bivio Networks account team for specific information.			

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, control and operate customer networks. Bivio is privately held and headquartered in the San Francisco Bay area with office locations worldwide. More information is available at www.bivio.net.

bivio NETWORKS

Contact Information

Bivio Networks, Inc.
4457 Willow Road, Suite 240
Pleasanton, CA 94588
Tel: +1 925.924.8600
Fax: +1 925.924.8650
www.bivio.net