FlowIntelligence™ Cyber Analyst

Advanced Deep Packet Inspection and Cyber Intelligence

bivio networks

Highlights

Deep Visibility

- Collect network flows and analyze network applications through Layer 7 of the OSI model from the enterprise
- Centralized and distributed analysis
- Generate metadata for network events with more than 60 log types
- Identify suspicious or malicious files embedded in network flows

Dynamic Analysis

- Dynamic analysis with integrated threat intelligence indicators and enhanced events from the FlowIntelligence™ Cloud
- Identify network and application anomalous behavior
- Identify cover channels and events related to cyber campaigns
- 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 Intelligence as a Service

The complexity of networks, applications and services creates additional pressure on enterprise and service provider cyber analyst to identify network events as well as detect, mitigate and protect from cyber threats. Network-based based applications, social media, Email, SCADA and Internet of Things (IoT) all bring risk of an unwanted or undesirable event in the network. Identifying external and internal threats, lateral movement from a network event as well as data exfiltration adds complexity and challenges for the security operations teams. They now have to address multiple questions for the network ecosystem, including:

- How to effectively collect and analyze every session in the network?
- How to identify complex or advanced events, threats and malware?
- How to identify internal threat actors and related events, lateral movement of threats and the scope of their movement?
- 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' Cyber 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, cyber intelligence capabilities.

Features and Capabilities

FlowIntelligence™ Cyber Analyst provides advanced deep packet inspection and cyber intelligence. The features and capabilites are summarized below.

Deep Packet Inspection

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

Cyber Intelligence

Analyze traffic from north-south as well as east-west network links. Collect metadata on every session within the sensor's scope, enable the cyber hunt process with the rich log data that is available and expose hidden events or threats. Identify anomalous behaviors for applications, covert network channels and activity based on cyber campaigns.

Malware Analysis

Protect users and subscribers from embedded malware in network flows. Automatically alert on users connecting to 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. Cyber 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 addresses 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

Cyber Analyst operates in passive 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. It's just that simple!

Scalable Operations

Cyber Analyst scales up to 100Gbps operating speed. Powered by BiviOS™ and the FlowIntelligence™ Adaptive Cyber Defense platforms, Cyber Analyst features unparalleled performance. It the fastest network security monitor solution on the market today.

Friction-less Updates

Events, threat intelligence data and sensor application components are updated through the FlowIntelligence Cloud. Event definitions are accomplished through the user interface for automated updates. Threat intelligence data can be updated as often as the cyber analyst desires in intervals as short as five (5) minutes. 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.

Data Integration

Cyber Analyst contains automated data integration via an 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

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

Distributed Operations

FlowIntelligence Cyber Analyst features the ability to operate in an enhanced, distributed mode. The solution supports implementing 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.

Turn-Key Solution

Cyber Analyst is delivered as a turn-key deep packet inspection and cyber intelligence 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 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

Cyber Analyst is comprehensive, advanced deep packet inspection and cyber intelligence solution. It contains intelligent features for innovative detection of network events, 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 Cyber Analyst can enhance your cyber security operations team.

Recommended Services

ExpertSupport™ aids organizations with proactive support for critical systems. ExpertSupport provides comprehensive software and hardware support to organizations with standard Monday through Friday, 8-5 PST 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 services to provide installation or more detailed and complex technical services.

ExpertAnalyst™ enables organizations to leverage Bivio Networks' cyber analysis team to develop custom detection rules, events and threat intelligence indicators for use in the FlowIntelligence suite of tools.

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