FlowIntelligence™ Cyber Analyst

bivio networks

Cloud Event Monitoring and Traffic Analysis

Key Benefits

Deep Visibility

- *Collect network flows and analyze network applications through Layer 7 of the OSI model from the enterprise*
- *Analyze Cloud traffic (DNS, FTP, SIP, DHCP, SMTP, HTTP/HTTPs, SMB, ModBus & DNP3, etc.)*
- *Centralized and distributed analysis environments*
- *More than 3000 types of network events tracked*
- *Generate metadata for network events with more than 50 embedded log types and hundreds of metadata objects*
- *Investigate data with associated BGP, MPLS and VLAN tags*
- *Identify network and application anomalous behavior including known embedded malware*
- *Integrate threat intelligence indicators for dynamic analysis*

Cloud Monitoring as a Service

The complexity of operating a private or hybrid cloud with networks, applications and services creates additional pressure on enterprise cloud operators. FlowIntelligence™ Cyber Analyst monitors cloud environments and identifies network events that affects overall performance and operations. It provides detailed information on cloud-based applications such as DNS, Social Media, Email, SCADA and Internet of Things (IoT) which brings the risk of an unwanted or undesirable events 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 cloud ecosystem including:

How to effectively collect and analyze every session in the network?

How to identify anomalous behavior of applications and users or subscribers in the cloud?

How can the organization implement dynamic analysis of the cloud ecosystem?

How can cloud operators automate the blocking or shunting process for risky or unwanted network traffic?

How can the organization ensure that network operations meet the data regulations and compliance requirements?

How can the organization analyze SSL/TLS traffic?

Bivio Network's FlowIntelligence™ Cyber Threat Analyst is a key component for the effective operation of private and hybrid clouds. It answers these questions plus provides proactive, network and cloud intelligence capabilities for effective operations.

Key Capabilities

The FlowIntelligence™ Cyber Analysis platform provides deep cloud analysis and enables enforcement of organizational policies for cloud access, services and applications. The key capabilities include:

Deep Packet Inspection

Cyber Analyst inspects network traffic and analyze applications through layer-7 of the OSI model. It logs events as well as identifies network activity that creates an operational concern. The solution leverages the LDAP to identify users and correlate them to the network activity. Analyst can investigate, alert and log specific events through python-based event analysis to gain deep insight into private and hybrid cloud operations with the Cyber Analyst technology.

Performance and Operational Analysis

Probe traffic from north-south as well as east-west network links. Collect flow metadata on every session within the sensor's scope which enables the cloud and network operations team to identify performance issues and network bottlenecks. Proactively uncover anomalous applications behaviors and network issues before they significantly affect cloud operations. Validate cloud operational and security policies. With the ability to collect more than 60 log types with throusands of metadata objects and 300 or more events tracked, rich analysis of the cloud ecosystem is possible to identify abnormalities in applications, subnets and networks.

Cyber Analyst identifies security threats with its deep file inspection process. Each embedded file is analyze against known malware hash values and alerts the operators during a event. It analyzes events related to DNS and rapidly identifies "spoofing" events.

Cloud Policy Control

Analyze network flows for policy control violations and identify applications as well as users or subscribers who are violating acceptable use policies. Rapidly target unauthorized applications and eliminate those from the cloud ecosystem with the embedded OpenFlow client. This provides the ability to interface with packet brokers and Software Defined Networks (SDN) to block or shunt unwanted or undesired cloud activity.

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 the packet collection interface to a network tap or span port and begin operations. Turn 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

Events, threat intelligence and platform components are automatically updated through the FlowIntelligence Cloud. The embedded package manager automatically updates event definitions through the user interface. Threat intelligence is updated with an embedded client. The 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

Cyber 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 communication framework to the collection workers for augmented analysis. Additionally, the collection workers share data among themselves to aid in advanced event identification.

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, S3, RSyslog or a Kafka message broker. Custom integration for other systems is also available through Bivio Networks' ExpertAssist™.

Open Architecture

Cyber Analyst features an open sensor engine environment powered by *Zeek*™. 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 plug-in architecture. Cyber Analyst interfaces with third-party tools and solutions via the Open Data Layer Exchange (OpenDXL) API. The Bivio Networks professional services teams can facilitate new or custom features and integration with ExpertAssist™.

"There was a time when every household, town, farm or village had its own water well. Today, shared public utilities give us access to clean water by simply turning on the tap; cloud computing works in a similar fashion. Just like water from the tap in your kitchen, cloud computing services can be turned on or off quickly as needed. Like at the water company, there is a team of dedicated professionals making sure the service provided is safe, secure and available on a 24/7 basis. When the tap isn't on, not only are you saving water, but you aren't paying for resources you don't currently need." –**Vivek Kundra**, Federal CIO, United States Government,

Cyber Analyst Platforms

1, 5 and 10Gbs platform

25Gbs platform

Modular Chassis Architecture - up to 100Gbps

Safe and Secure Cloud Operations

Operating safe and secure cloud environments requires a deep insight into the applications and subscribers that traverse the cloud. It requires the cloud operator to monitor and identify anomalous activity, take action to mitigate events and ensure the cloud is safe in the shared environment. This is exactly what Cyber Analyst does - It analyzes applications in the cloud including DNS, SMTP, HTTP & HTTPS, SSL/TLS as well as many others to ensure it these applications are operating or being used appropriately. It also analyzes user or subscriber behavior, determines whether they are utilizing the cloud environment in a safe, consistent and approved manner. It identifies known malware that can affect the cloud environment. This analyst never sleeps - so you can rest assure that 24/7, Cyber Analyst will ensure your organization has a safe, secure and available cloud environment.

Turn-key Solution

Cyber Analyst is provided as a turn-key cloud monitoring and network traffic analysis solution on Bivio Networks FlowIntelligence™ adaptive cyber defense platforms. These platforms provide the scaling for operating the solution at speeds reaching 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 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 clouds 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

Cyber Analyst is a comprehensive, advanced deep packet inspection and cloud monitoring solution. It contains intelligent features for innovative detection of network applications and events to aid cloud operators. It is in an elite class for its performance, features and capabilities. Contact 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, 8-5PST 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 cyber analysis team to develop custom detection rules, events and threat intelligence indicators for use in the FlowIntelligence suite of tools.

Platform Specifications:

Features	Virtual Cyber Platform	1-10Gbps	25Gbps	Modular Chassis Architecture
Operating Speeds	1, 5 & 10 Gigabits per second (Full Duplex)	1, 5 & 10 Gigabits per second (Full Duplex)	25 Gigabits per second (Full Duplex)	Up to 100 Gigabits per seconds (Full Duplex)
Network Interface	4 x vNIC (1 & 10Gbps)	2 x 1Gbe RJ45 Copper or 2 x 1/10 SFP+ Optical or Copper Interfaces	2x25 Gigabits QSFP28 interfaces	Packet Interface Module with 2 x 100 Gigabit Ethernet and 1 x 40 Gigabit QSFP interfaces
Data Interfaces	2 x vNIC	2 x 1Gbe RJ45 Copper or 2 x 1/10 SFP+ Optical or Copper Interfaces	2 x 1/10 SFP+ Optical or Copper Interfaces	Data Offload Module with 2 x 100 Gigabit Ethernet and 1 x 40 Gigabit QSFP interfaces
Management Interface	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	N/A	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 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. Contact your Bivio Networks account team for specific information.			
Virtual Platforms	Licensing for the virtual platform is based on an annual subscription for 1, 5 & 10Gb operations. Contact your Bivio Networks account team for information and technical specifications.			

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