Network visibility to automatically detect and mitigate active cyber attacks in real time

The Ixia Visibility Architecture provides complete network access for Vectra Automated Threat Management software

**Joint Solution Benefits**

- Complete visibility of cyber threats inside the network. The Ixia Visibility Architecture delivers to Vectra all required traffic from anywhere in the network. All traffic – 100 percent – can be monitored, inspected and analyzed.
- Simplified deployment. The Ixia/Vectra solution is flexible enough to work in any network environment and can share access with deployed monitoring and security tools.
- Easily scalable. Additional 1G, 10G, 40G, or 100G ports can be added as needed and filters can be dynamically adjusted to meet any bandwidth requirements.
- Maximum efficiency. The Ixia solution filters and removes unneeded traffic so the Vectra platform always operates at full efficiency.

**Solution**

The Ixia Network Visibility Architecture and Vectra® Networks Automated Threat Management software work together to detect cyber attacks in progress amid the chatter of your network so security teams can quickly mitigate and prevent data loss.

Ixia Network Packet Brokers passively direct out-of-band network traffic from multiple network access points – like SPANs, taps and virtual taps (vTaps) – to the Vectra X-series platform for inspection and analysis. Traffic is aggregated from all network access points to provide comprehensive visibility.

Vectra then performs continuous analysis of internal network traffic to automatically detect all phases of persistent stealthy attacks, including hidden command-and-control communications, internal reconnaissance, botnet monetization, lateral movement, and data exfiltration.

**Network-based threat intelligence**

Vectra automates the real-time detection and analysis of active cyber attacks that evade perimeter security defenses and spread inside networks.

Vectra picks up where perimeter security leaves off by providing deep, continuous analysis of both internal (east-west) and Internet (north-south) network traffic to detect all phases of an attack during which hackers spy, spread, and steal inside your network.

The Vectra platform continuously listens, identifies, learns and follows latent attack behaviors to detect threats and anticipate a cyber criminal's next move. A unique combination of data science, machine learning and behavioral analysis enables Vectra to detect known and unknown zero-day threats without signatures or reputation lists.
Directs traffic to Vectra and other monitoring tools

The Ixia Network Packet Broker simultaneously aggregates traffic from multiple SPANs, taps and vTaps (also sold by Ixia) in the network and directs it to the Vectra platform. This ensures efficient access to asymmetric traffic across large heterogeneous networks.

Traffic that does not require analysis can be filtered out by Ixia’s Visibility Architecture to prevent Vectra resources from being unnecessarily consumed. With the Ixia Visibility Architecture, traffic from network access points can be shared with multiple monitoring tools. This eliminates common SPAN/tap shortages that occur when another tool is attached to a needed access point.

Additionally, by removing duplicate packets, Ixia Network Packet Brokers can enhance throughput capacity. The automation capability in the Ixia’ Visibility Architecture integrates seamlessly with Vectra to enable a wide range of applications, including:

- Load-balancing traffic across multiple Vectra input ports.
- Dynamically tightening filters as needed to ensure that critical transactions are always analyzed when total traffic spikes over 10 Gbps.
- Redirecting traffic among multiple Vectra platforms on a network to ensure high availability.
- Providing complete visibility into east-west traffic from virtual environments.

An intuitive GUI control panel makes Ixia Network Packet Brokers easy to set up and use. Simply drag-and-drop a virtual connection between SPANs/taps and the Vectra platform to make a live connection.

About Vectra Networks

Vectra® Networks is the leader in Automated Threat Management, which provides real-time detection of in-progress cyber attacks that evade perimeter security systems and spread inside networks. The company’s X-series Platforms and S-series Sensors continuously monitor internal network traffic to pinpoint cyber attacks as they happen. Vectra prioritizes attacks that pose the greatest business risk, enabling organizations to make rapid decisions on where to focus time and resources.

Vectra offers a wide range of critical threat-detection capabilities

Detects known and unknown threats in real-time anywhere in the network, including remote locations and network segment.

- Exposes encrypted and hidden attack communications without decrypting traffic.
- Reports threats throughout every phase of an advanced targeted attack.
- Reports are only one-click away and include threat severity and certainty scores, hosts that are under attack, and context about what attackers are doing.
- Identifies all attacks without relying on signatures or reputation lists and on all devices, operating systems and applications.
- Deploys in passive mode on a SPAN or a network tap.

Additional information about Vectra
Web: www.vectranetworks.com
Email: info@vectranetworks.com

About Ixia Visibility Architecture

Ixia’s Visibility Architecture provides complete network visibility into physical and virtual networks, improves network security and optimizes monitoring tool performance. Ixia solution ensures that each monitoring tool gets exactly the right data needed for analysis. This improves the way you manage your data center and maximizes return on investment. Our customers include large enterprises, service providers, educational institutions and government agencies.

For additional information:
http://www.ixiacom.com/solutions/visibility-architecture