Detect and Analyze Advanced Attacks

The Ixia network visibility architecture provides complete network access for the RSA NetWitness® Logs and Packets solution.

Challenge

The sophistication of threat actors and the expanding attack surface make it nearly impossible for security teams to discover and understand compromises quickly enough to respond before they impact the business.

To detect advanced attacks, logs need to be combined with other data types such as network packet, endpoint, and cloud data. RSA NetWitness Logs and Packets discovers attacks missed by log-centric SIEM and signature-based tools with the only solution that can correlate network packets with other security data.

Joint Solution Overview

RSA NetWitness Logs and Packets combined with Ixia's network packet brokers and Taps provides pervasive visibility with advanced analytics – including real-time behavior analytics - to detect and investigate sophisticated attacks.

The Ixia solution and RSA NetWitness work together to capture and analyze network packet traffic in a scalable solution that can accurately and efficiently monitor networks of any size. Ixia network packet brokers passively direct out-of-band network packet data from multiple access points to the RSA NetWitness Logs and Packets solution for comprehensive analysis.

Visibility is Provided Across:

- Data Sources - Full Packet Capture, NetFlow Logs and Endpoint
- Threat Vectors – Endpoint, Network and Cloud
points, such as SPANs, taps, and virtual taps (also sold by Ixia), in the network to RSA NetWitness for capture. Traffic is aggregated from all needed access points in the network to provide comprehensive visibility.

RSA NetWitness Logs and Packets unique architecture captures and enriches data sources with security context in real-time. Additionally, threat intelligence is applied to the enriched data to identify high risk indicators as APT domains, suspicious proxies or malicious networks. This method of processing large data sources in real-time provides analysts with security insight into their entire environment from on-premise to cloud.

**Ixia Delivers Complete Packet Access**

Ixia Network Packet Brokers (NPBs) sit between access points in the network that require monitoring and the NetWitness appliance, simultaneously aggregating traffic from multiple SPANs and taps and directing corresponding packets and Netflow records to RSA for analysis. Traffic is aggregated from all needed access points in the physical and virtual network for comprehensive visibility.

**Visibility, Analysis and Action**

RSA NetWitness Logs and Packets captures and enriches full network packet data alongside other data types, such as logs, NetFlow and endpoint. RSA NetWitness Logs and Packets captures full network packets, which means an attack can be reconstructed to fully understand the full scope of the attack and in turn implement an effective remediation plan to stop the attacker from achieving their objective.

**Ixia Complements RSA NetWitness by:**

- Eliminating SPAN/Tap by allowing traffic from a single network access point to be shared with multiple monitoring tools
- Providing access to all needed physical and virtual network traffic;
- Enabling efficient access to asymmetric traffic across large heterogeneous networks;
- Improving tool utilization by filtering out traffic not needed for analysis;
- Load-balancing traffic across multiple NetWitness appliances to scale and monitor networks of any size

---

**Figure 1. Ixia and RSA Deployment**
For example, in a Spear Phishing attack, the attacker implements a series of steps across the kill chain. By using RSA NetWitness Logs and Packets, a security operations team will have full visibility across the kill chain. Attacker’s actions are fully reconstructed with RSA NetWitness Logs and Packets and this helps the security operations team to put an effective remediation plan in place.

The ability to process the data in real-time as indicated above enables security operations team to detect earlier and investigate more effectively and faster. For example, in a Spear Phishing attack, the attacker implements a series of steps across the kill chain. By using RSA NetWitness Logs and Packets, a security operations team will have full visibility across the kill chain.

About RSA

RSA helps more than 30,000 customers around the world take command of their security posture by partnering to build and implement business-driven security strategies. With RSA’s award-winning cybersecurity solutions, organizations can effectively detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. For more information, go to www.rsa.com.

About Ixia

Ixia provides testing, visibility and security solutions, strengthening physical and virtual network elements for enterprises, governments, service providers, and network equipment manufacturers. Customers worldwide trust Ixia to verify their designs, optimize their performance, and ensure protection of their networks to make their networks stronger.