Ixia Boosts Application and Threat Intelligence Processor

Written by Marco Attard
11 November 2016

Network security vendor Axia announces enhancements on the Application and Threat Intelligence Processor (ATIP), together with a centralised cloud management interface for ThreatARMOR appliances.

Part of the Security Fabric data distribution engine, the improved ATIP enables security and network professionals to extract metadata from network connections, including IOC, spanning URLs, Uniform Resource Identifiers, Session Initiation and Cisco Discovery Protocols, Domain Name System Text and User Agent. Such deeper context aware metadata allows for reporting tools to deliver analysis reports quickly and effectively, leading to improvements in MTTI and MTTR to threats and suspicious activity.

ATIP works with reporting solutions from the likes of Plixer, LiveAction, Splunk and Dynatrace to provide key insights in data breaches, without need for a specialised forensic monitor.

"Ixia is committed to leveraging and extending our decade-plus experience in advanced malware research to solve the key challenges facing network operators today," the company says. "We make significant investments in research that helps our customers to quickly identify inevitable security breaches with minimal investment of time and money."

A second Ixia announcements involves ThreatARMOR-- the threat intelligence gateway gets cloud-powered centralised management and mobile access to essential security information. The result is a convenient portal for the management of ThreatARMOR device deployments across the globe, with scalable management, log collection and centralised reporting of policy, inventory, licensing, device health, and synchronisation status, as well as aggregated blocking data.

ThreatARMOR Central Management requires zero setup, and Ixia provides hosting and data storage capabilities via the cloud. It is available to all ThreatArmor (1G or 10G) subscribers at no extra cost.

Go Ixia Enhances ATIP

Go Ixia Leverages the Cloud to Streamline Network Threat Intelligence