WHITE PAPER

APPLICATION AND THREAT INTELLIGENCE RESEARCH CENTER

COMPLEXITY CREATES VULNERABILITY

The modern application is complex. We know because at Ixia, we have been testing equipment, networks, and applications for decades. As an enterprise, you rely on your development teams to have depth of knowledge across a wide range of technology areas that includes application and threat vulnerabilities. Tracking the latest message board alerts—from the operating system, to the software development environment, to threat and connectivity attack methods— requires multiple focused teams. You have one team and it is under constant pressure to fix bugs faster to meet delivery schedules. But you have a failsafe way to make sure apps rushed to completion do not introduce vulnerabilities...right?

Vulnerabilities come from lots of places. For instance, one operating system kernel or driver update can have ripple effects to several related software elements. Did that just create the possibility of a buffer overflow that hackers can exploit? One unpatched security vulnerability can create a pathway directly into your application database. Did you just open the door to your customer data? You need the ability to validate the entire security ecosystem to protect against this kind of change.

VULNERABILITIES COME FROM A LOT OF PLACES. FIND THEM BEFORE THEY DO.

Many security providers offer threat intelligence—the tracking of attacker profiles, methods, and attack vectors. Some vendors offer application intelligence—the monitoring of applications in action. Both are critical to your operation and more intertwined than they may appear on the surface.

IXIA'S APPLICATION AND THREAT INTELLIGENCE (ATI) RESEARCH CENTER

Ixia knows test, how applications should perform, and security. We have deep knowledge concerning the challenges of maintaining a network solution that facilitates high-speed data moving through a network, along with the security and performance issues which inevitably arise. That is why we created the ATI Research Center, an elite group of top application and security researchers from around the globe. Their expertise spans software development, reverse engineering, vulnerability assessment and remediation, malware investigation, and intelligence gathering.

Our Ixia ATI Research Center combines proficiency in cybersecurity threats and application protocol behavior. This unique combination takes network security to a whole new level, looking at it the exact same way as a cybercriminal, from every direction. Ixia uses this combination of application and threat intelligence across its test, visibility, and security solutions to:

- Create realistic applications attacks – from protocols, through loading, through threats
- Block malicious inbound and outbound communications
- Collect ongoing intelligence on new threats
- Identify unknown applications
- Detect traffic geolocation

These capabilities combine to go far beyond simple signature recognition. They proactively defend against attack patterns and reduce your attack surface by finding product vulnerabilities before and after you launch to the market. The ATI Research Center leverages the knowledge of hundreds of Ixia engineers and decades of knowledge across test, protocols, networks, and security.

IXIA ATI REASEARCH CENTER COMBINES PROFICIENCY IN CYBERSECURITY THREATS AND APPLICATION PROTOCOL BEHAVIOR.

ATI GLOBAL IMPACT

The intelligence produced by the ATI Research Center supports a wide range of Ixia products including our Application and Threat Intelligence Processor (ATIP), ThreatARMOR, BreakingPoint, IxLoad, IxChariot, and IxNetwork. ATI data sources are used in the test products we provide to every major security vendor, network equipment manufacturer (NEM), and service provider in the industry. Top ranked security vendors all leverage the outputs of the ATI research to verify their own products and applications run strong.

We augment the knowledge of how applications perform in service provider and enterprise networks with threat intelligence data gathered from our network security products.

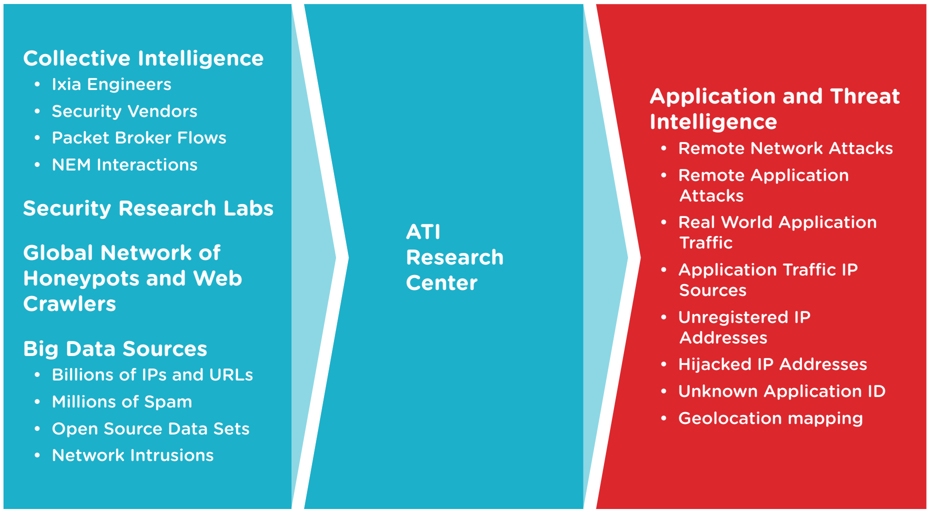
The combination gives the ATI Research Center a powerful understanding of how hackers exploit vulnerabilities missed before product launch or once they are in a live network. We partner with leading developers, monitor alerts across every layer of the OSI stack, and actively research threats around the globe to keep our application and threat intelligence feeds up to date with the latest data.

Ixia ATI Research Center operates a worldwide, distributed network of honeypots and web crawlers to actively identify known and unknown malware, attack vectors, and application exposures.

In addition, the team regularly finds and discloses zero-day vulnerabilities. We correlate this data with real world events, validate reported findings, and then push actionable intelligence to customers with continuous updates.

The ATI data feeds produce actionable security intelligence on application vulnerabilities as well as threats across networks, endpoints, mobile devices, virtual systems, web, and email. The ATI feeds automate the gathering and analysis of a wide range of threat intelligence data from sources including:

- Billions of IPs and URLs
- Millions of spam
- Millions of malware attacks
- Open source data sets
- Millions of network intrusions



Collective Intelligence

- Ixia Engineers
- Security Vendors
- Packet Broker Flows
- NEM Interactions

Security Research Labs

Global Network of Honeypots and Web Crawlers

Big Data Sources

- Billions of IPs and URLs
- Millions of Spam
- Open Source Data Sets
- Network Intrusions

ATI Research Center

Application and Threat Intelligence

- Remote Network Attacks
- Remote Application Attacks
- Real World Application Traffic
- Application Traffic IP Sources
- Unregistered IP Addresses
- Hijacked IP Addresses
- Unknown Application ID
- Geolocation mapping

TOP RANKED SECURITY VENDORS ALL LEVERAGE THE OUTPUTS OF THE ATI RESEARCH TO VERIFY THEIR OWN PRODUCTS AND APPLICATIONS RUN STRONG.

The majority of NEMs and service providers validate their hardware and systems by leveraging our application intelligence, which includes:

- Programming methods of communication protocols, common practices to introduce weaknesses, and loading profiles of the widest range of traffic types
- Deconstructing application protocols and packaging them for use in real world user simulation testing
- Using a deep knowledge of protocols to fuzz applications and look for specific types of weaknesses as well as find unknown, zero-day vulnerabilities

The unique combination of application plus threat intelligence ensures resilient networks, and better performing and secure applications.

ATI: MORE RESILIENT SECURITY + BETTER PERFORMANCE

Threat intelligence providers and security vendors typically focus on the symptom, not the disease. They address how to identify and block the high-level threat without addressing the door which the threat exploited to enter originally. Those typically come from a vulnerability in the network or application. Stronger applications lead to better performance and just as importantly, more resilient security.

You need to know if the application and service you are providing is stable and secure. You need expertise to fully assess your application's stability as well as its security. Testing massive scale at high speeds across multiple data types requires breadth of application expertise. Knowing the latest threat attacker exploits, identities, and methods requires depth of threat intelligence.

The combination of application plus threat intelligence expertise can mean the difference between delivering a product that significantly grows your market share versus one that brings your business to its knees.

THE UNIQUE COMBINATION OF APPLICATION PLUS THREAT INTELLIGENCE ENSURES RESILIENT NETWORKS.

IXIA WORLDWIDE HEADQUARTERS
26601 AGOURA RD.
CALABASAS, CA 91302

(TOLL FREE NORTH AMERICA)
1.877.367.4942

(OUTSIDE NORTH AMERICA)
+1.818.871.1800
(FAX) 818.871.1805

WWW.IXIACOM.COM

IXIA EUROPEAN HEADQUARTERS
IXIA TECHNOLOGIES EUROPE LTD
CLARION HOUSE, NORREYS DRIVE
MAIDENHEAD SL6 4FL
UNITED KINGDOM

SALES +44 1628 408750
(FAX) +44 1628 639916

IXIA ASIA PACIFIC HEADQUARTERS
101 THOMSON ROAD,
#29-04/05 UNITED SQUARE,
SINGAPORE 307591

SALES +65.6332.0125
(FAX) +65.6332.0127