WHITE PAPER

IXIA 360^0 SECURITY

SECURITY SPANS DEVELOPMENT, DEPLOYMENT, AND OPERATION

Security is much more than layers of defense. It starts at the innermost core of your network. Whether your business builds products or simply relies on them, you need to decide at what point your application is 'good enough to deploy.' Every vulnerability your team does not catch in pre-deployment will end up becoming a patch once in operation. Your best option is good offense, a path often neglected.

When it comes to security, the industry focuses primarily on layers of defense against cyber-attacks. While a good defense is essential, it crumbles under pressure when not balanced with a good offense. Testing and training against realistic loads and cyberattacks before a product or service is deployed uncovers performance and security issues early. Prevent attacks from occurring in the first place and your operational costs will drop. Discovering vulnerabilities at earlier stages is much less expensive for both your products and your business.

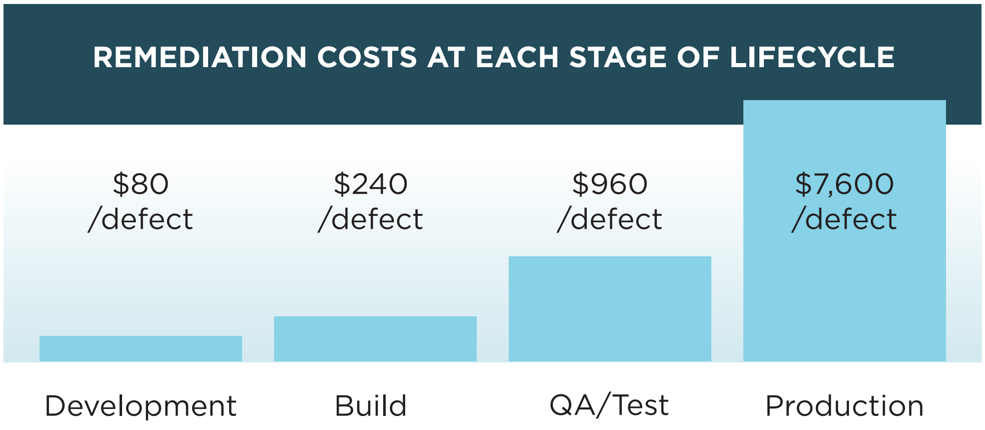
Research from Ponemon Institute found the later you identify a defect, the more it costs to fix. Creating patches for live services without affecting existing customer experiences is complex and costly. Catching defects earlier in the development process is much less expensive. Defects found in development, for instance, cost 11X less to resolve than those found during quality assurance (QA) testing, and 90x less than resolving them in live operation. Better load and attack testing in earlier stages of development and build leads to much more

"CYBERCRIME IS THE MODERN-DAY MAFIA."

BETHANY MAYER, CEO, IXIA

FORBES MAGAZINE, 2015

cost effective operations. And with the average cost of a breach at over $7M, the cost of avoiding a single breach is a fraction of the cost of additional testing.


REMEDIATION COSTS AT EACH STAGE OF LIFECYCLE

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

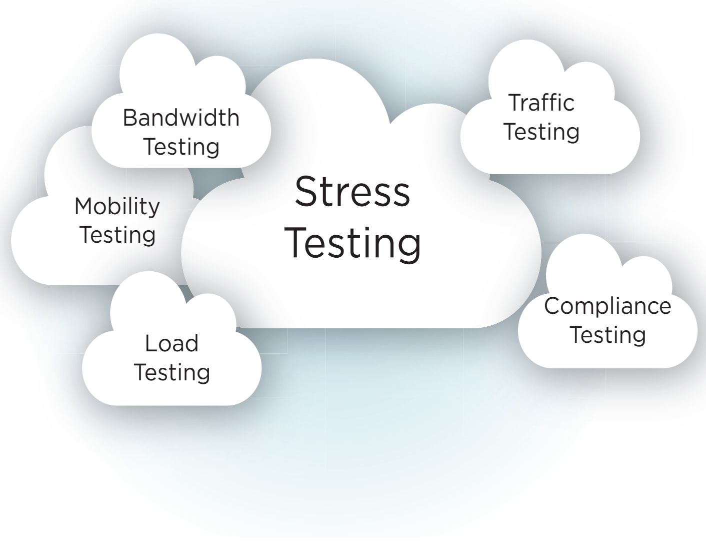
There are times when market or management pressures drive businesses to deploy a product with limited testing. The wider acceptance of 'beta releases' has driven many businesses to the conclusion that shortening the test cycle and 'fixing on the fly' is an acceptable trade. This can be a costly decision, especially if your application is as popular as you expect it to be. Once you have thousands, or millions of users relying on your application, implementing fixes become much more complicated.

Security industry leaders have estimated the annual cost of cybercrime to the global economy may be as high as $575B.   Cyber criminals are formidable: talented, well-informed entrepreneurs creating their own supply chains just like businesses. They understand they only need to find just one ingress point to get inside your application or network. From there, they still have to gather valuable data and move that data out of your network. You can monitor and trace each of these actions making robust monitoring just as important as vulnerability testing.

WHAT MAKES GOOD SECURITY?

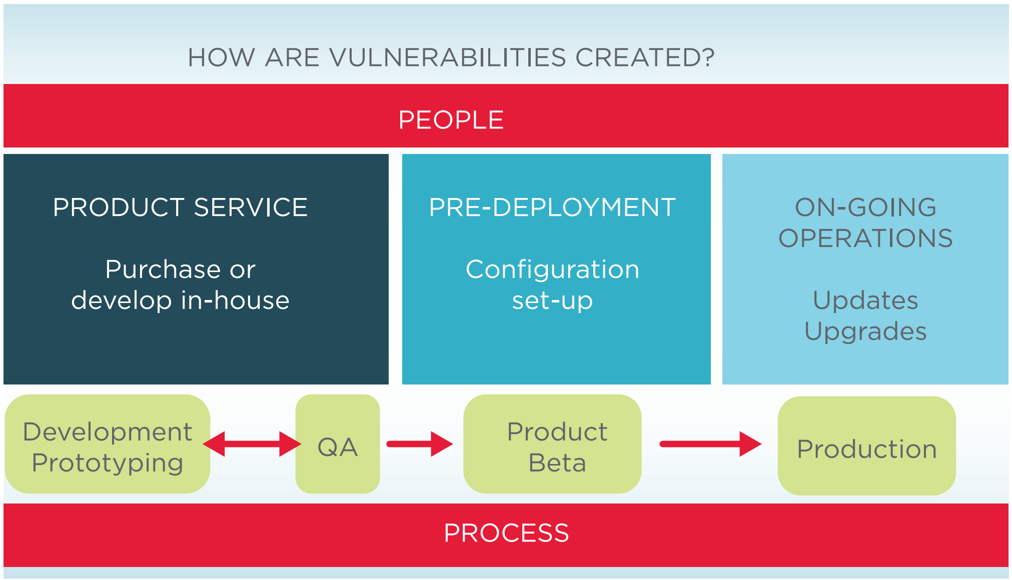
A good defense integrates firewalls, IDS/IPS, anti-bot and antivirus software to detect and block threats preying on vulnerabilities. Manufacturers design most of these tools to protect your network from attacks. Adding defensive layers is absolutely necessary and smart, but only addresses the symptoms, not the disease. Attacks occur because of a system or application feature that can be exploited. Identifying and fixing those issues is good practice for security offense.

Offense: Untapped Potential



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

THE ROOTS OF THE PROBLEM


HOW ARE VULNERABILITIES CREATED?

PEOPLE

PRODUCT SERVICE
Purchase or develop in-house

PRE-DEPLOYMENT
Configuration set-up

ON-GOING OPERATIONS
Updates
Upgrades

Development Prototyping ↔ QA → Product Beta → Production

PROCESS

As we have noted, vulnerabilities can come from exploiting product features, system commands, or compliance issues. They can also come from exploiting people or process. For instance, employees who tape their passwords to their monitors or pop in USB sticks they found in the parking lot; IT support people who accidentally leave a support back door to the network open; or security teams that are not trained on how to deal with an attack once it is in action. They can also come from issues ranging from how products or services were installed in your network or how they are configured. They can even be exploited because they did not deploy the latest patch or upgrade right away.

From product development through deployment through operation, vulnerabilities can come from products, people, or processes.   Whether your business builds products or relies on them to provide services, you need to validate your product/service as well as the people and processes at every stage.

MANY COMPANIES STILL USE COPIES OF LIVE PRODUCTION DATA IN TESTING ENVIRONMENTS... WITHOUT ANY CONTROL OVER HOW THE DATA IS HANDLED..."

SC MAGAZINE UK

DECEMBER, 2015

IXIA'S IxSECURE ARCHITECTURE: SECURITY THAT STARTS AT THE FOUNDATION

Network equipment manufacturers, network security vendors, service providers and enterprises use Ixia's IxSecure security architecture to validate their products and monitor their operations from early-on product conception, through development and deployment, and during live operation. At the core of Ixia's security architecture is the Application and Threat Intelligence (ATI) Research Center.

Our ATI Research Center is what ties insight from testing with insight from monitoring. Staffed by more than 900 engineers, our test business needs to emulate the latest trends in protocols, communication methods, and application behaviors.   To accurately test network integrity, we also monitor threats from around the globe, map the world's IP addresses, and continuously verify known bad sites to bolster our visibility and defense products. The result is an ATI research center that understands the evolving complexities of product development, the breadth of application behaviors, and the latest threats in the market – all in one intelligence stream.

Ixia is the only company with the insight and access to create combined application and threat intelligence that can be used to validate products during deployment, plus validate their operation in production.

IxSECURE: A 360 APPROACH TO PROTECTING YOUR NETWORK

Multiple products and services combine to address four major challenges throughout the security lifecycle: develop, train, monitor, and defend.

Develop: Pressure-Test to Be Sure

Using copies of live production data—or testing in live production environments is tremendously risky. Ixia's solutions let you perform in-depth assessments that include generating realistic mixes of application and attack traffic to see how proposed designs fare, and scale, in live scenarios. Industry-leading products such as IxNetwork, IxLoad, IxVeriWave, IxVM, and BreakingPoint test everything from Layer 2/3 infrastructures and Layer 4-7 service delivery to wireless performance, virtualized data centers, security, and compliance.

"Development" never stops. New features, updates, patches are constantly occurring at the application, network, and wireless connection levels. Continuing to validate performance and security integrity during upgrades, maintenance and other changes ensures you are constantly passing valuable feedback to your internal developers, vendors, and service providers.

Train: Don't Take Anything for Granted

Every professional athlete trains continuously on and off the field. How much on the field training, do you give your professional security team? Do they know what to do when an attack occurs? When it comes to training, you need to make sure your team has the skillsets to address every stage of the security lifecycle. This includes knowing how to stress designs and configurations during beta testing before bringing products into production, knowing what to look for when monitoring, and knowing how to limit your network's attack surface.

When it comes to validating application performance, IxChariot and IxLoad can simulate combinations of traffic patterns to test your application and network integrity, ensuring you optimize your configurations. When you want to test your network against attack scenarios, BreakingPoint is the industry's gold standard for creating realistic attacks against your network, clouds, and applications.

For preparing your team to handle real-time attack events, Ixia offers a full "cyber range" environment and exercises to help walk through a range of RED Team, BLUE Team attack scenarios encouraging your own team to find vulnerabilities and learn how to defend.

Monitor: Keep ROI High and the Back Door Closed

You cannot secure what you cannot see. Ixia's visibility solutions streamline and advance performance and security monitoring with the industry's widest array of proactive and reactive tools. Physical and virtual taps (vTaps) provide real-time visibility to live data streams. Network Packet Brokers

(NPBs) intelligently filter and load-balance data through your monitoring infrastructures. In addition, NPBs actively authenticate traffic to help simplify filtering. They validate that application traffic is being sourced from a valid site by inspecting both clear and encrypted traffic and flagging anomalies for security analysis tools.

Underneath all of your security tools are bypass switches, and not all are alike. A proper bypass switch reinforces your security posture by safeguarding the flow of good traffic against device, link, and power failures. Heartbeats sent back and forth between these intelligent switches and tools in the network verify that your tools are working properly and route traffic to alternate paths when one goes offline.

For active testing of live networks, IxChariot tools add proactive monitoring validating performance at every network end point for seamless operation as application loads and requirements change. Together, this combination of monitoring tools ensures performance is as expected, that you safeguard your organization and your applications perform optimally.

Defend: Shrink Your Network Attack Surface

Security tools protect you from attacks in any direction. But if your organization does not do business everywhere, why would you open your doors to them? For instance, if you knew that an IT address was a proven phishing site, why would you let it on your network? You would not.   Simply preventing unneeded and unwanted traffic from touching your network dramatically reduces risk, minimizes the cycles spent responding to attacks, and saves your security team from having to deal with 'alert overload.'

In addition to our active monitoring tools, Ixia offers ThreatARMOR, an appliance that sits in front of your firewall and blocks known bad, unregistered, and hijacked IP addresses. A powerful game changer, ThreatARMOR instantly and dramatically reduces your network attack surface by blocking known bad traffic from gaining access to the network. Using feeds from Ixia's ATI Research Center, ThreatARMOR gets continuously validated bad IP addresses from around the world and blocks them. It also provides simple mechanisms to block entire geographies where you have no business.   And, if your network is already infected, ThreatARMOR blocks those internal bots from communicating out.

GOOD SECURITY IS GOOD FOR YOUR BOTTOM LINE AND YOUR TOP LINE

So what is the impact in terms of financial benefits to your IT operations? Just deploying better defenses like ThreatARMOR can eliminate up to 33 percent of known bad false positives, which would have to be investigated by your security team. In a large organization, security teams average 21,000 hours per year on chasing false positive security alerts. That translates into 157 weeks saved for your business. With an average salary of $100k, that is an annual savings of $300k – an ROI of 15x.

Add on Cyber Range training and network packet brokers and the ROI continues to grow. It all adds up to efficiency in your operations, which is important as your network expands.

GOOD OFFENSE

- In Development: Test for stability and security continuously before and after you launch
- In Training: Stress test your application and prepare your team for the unexpected

GOOD DEFENSE

- In Monitoring: Give your security tools a fighting chance with pre-filtered high-speed access to your data streams
- In Defending: Help make defense easier by reducing your attack surface and maximizing your security tools

It is no longer a matter of if you will be targeted by cybercriminals, but when and how often. Learn how you can make defending your network easier with Ixia's security solutions and IxSecure architecture at http://www.ixiacom.com/solutions/network-security-test.

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) 1.818.871.1805
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