ixia

Cyber Range Training Services

Table of Contents

Train Like You Fight 2

The Global Cyber Range Imperative 3

Why Traditional Approaches Have Failed 3

A Pragmatic Strategy for Arming and Training Elite Cyber Warriors 3

Training Next-Generation Cyber Warriors with Advanced Cyber Range Training 4

Real-World Cyber Ranges 5

Ixia's BreakingPoint Cyber Ranges 6

Cyber Range Targets 6

Service Operations Module 7

Service Defensive Operations Module 7

Cyber Range Simulation Learning Module 7

Cyber Range Training 8

Train Like You Fight

Organizations worldwide face a dangerous shortage of Cyber Warriors with the skills required to defend against cyber terrorism. This urgent situation is made worse by the weaknesses and vulnerabilities that continue to pervade critical IT infrastructures — despite billions of dollars invested in cyber security measures.

Addressing these problems requires Internet-scale simulation environments, along with a comprehensive training curriculum and proven methodologies, to develop elite Cyber Warriors and simulate attacks on IT infrastructures. Military commanders, defense contractors, and even commercial analysts such as Gartner refer to these environments as “Cyber Ranges.”

Although Cyber Ranges are a necessity for training Cyber Warriors, in recent years the old approach to building them has been exposed as a costly and futile exercise. Flagship Cyber Range projects relying on that outmoded approach have wasted years and hundreds of millions of dollars merely to study the problem.

Yet Ixia BreakingPoint has harnessed patented network processor technology to deliver a better approach — one that creates an Internet-scale Cyber Range environment from a single 7-inch-high device. This breakthrough invention removes the obstacles that once prevented the widespread deployment of Cyber Ranges for arming and training Cyber Warriors.

Leveraging its Cyber Range experience, Ixia has formulated a strategy for preparing organizations to defend their interests by assessing, educating, and training elite Cyber Warriors and equipping them to harden the resiliency of critical network and data center infrastructures.

Cyber Range Training Services

The Global Cyber Range Imperative

Those who do not remember the lessons of the past are doomed to repeat them. Yet today the same complacency that has led to catastrophic losses so many times is placing the world’s leading nations at risk, this time in the fifth battle space—the cyber domain. Without urgent action and investment to harden the resiliency of national cyber defenses, the impacts of cyber attacks will continue to multiply.

Just as every military and police force needs a firing range to hone weapons skills and battle tactics, every Cyber Warrior needs access to a Cyber Range. Only with an Internet-scale, operationally-relevant, and ever-current Cyber Range can organizations produce the empirically-valid war-gaming scenarios necessary to develop IT staff skills and instincts for offensive and defensive action. Similarly, the only way to understand the resiliency of IT infrastructures is to assault every element within them using the high-stress, real-world conditions created in the controlled environment of a Cyber Range.

Why Traditional Approaches Have Failed

Unfortunately, the enormity of today’s cyber security crisis has outstripped the unmanageable, inefficient approach of traditional Cyber Range models. At one organization, leaders were struggling to scale to the performance necessary to replicate a realistic environment. The organization had followed the old Cyber Range model to build out a lab filled with hundreds of servers cabled together to simulate the load of 15,000 users — with limited application coverage. Its mission, however, required 250,000 users to exercise target devices across the full complement of today’s applications.

The traditional Cyber Range model involves massive investments in hardware, software licenses, electricity, and real estate. It also requires dozens of skilled professionals to set up, configure, integrate, and maintain. It then requires dozens more network and security professionals with the knowledge to continually research and create an evolving mix of sophisticated attacks.

Rather than use cost-effective, adaptive, and scalable technology that is now readily available, too many organizations and government agencies have answered the Cyber Range challenge by throwing money, outmoded hardware, and expensive consultants at it. That approach is destined to fail, however, because it will never keep pace with the rapid evolution of cyber threats.

A Pragmatic Strategy for Arming and Training Elite Cyber Warriors

Drawing on its years of experience in delivering breakthrough Cyber Range innovations to military organizations and global enterprises, Ixia has developed a pragmatic and sustainable strategy for arming organizations to assess, educate, and certify a national force of Cyber Warriors to carry out information assurance (IA), information operations (IO), and mission assurance (MA) duties. The same innovative technology and scalable approach used for training Cyber Warriors can be leveraged to assess and harden IT infrastructure resiliency.

Training Next-Generation Cyber Warriors with Advanced Cyber Range Training

Organizations and government agencies have answered the cyber defense challenge by arming their networks with firewalls, intrusion prevention systems (IPSs), and other defenses. Though this satisfies a rudimentary network security checklist, this approach on its own has no hope of keeping pace with the rapid evolution and scale of cyber threats, and is destined to fail. Effective cyber security is the product of melding trained people, or Cyber Warriors, and automated systems into a unified defense.

Ixia's Cyber Range Training delivers structured training and war-gaming exercises to prepare Cyber Warriors at both public and private organizations to defend their critical infrastructures, enterprises, and communications networks. With a comprehensive Cyber Warrior curriculum, commanders, government officials, and CIOs can educate and train their personnel through a wide range of exercises at increasing levels of difficulty to evaluate expertise and certify capabilities. Our training includes both pre-built and customized war game scenarios to ensure the highest security for your particular network.

Our Cyber Range Training leverages Ixia BreakingPoint™ Actionable Security Intelligence (ASI) to generate realistic application traffic and exploits, using pre-configured and custom Internet and target simulations. During training, we will generate the following traffic and simulations to create an Internet-scale Cyber Range environment:

- Realistic target simulations
- Realistic exploit simulations
- Realistic evasion simulations
- Realistic traffic simulation
  - Internet IPv4 and IPv6 infrastructure
  - Enterprise and IT services
  - Population and country user base
  - Data of interest or "needle in a haystack" for data loss prevention (DLP)
  - Mobile subscriber user base

Our Cyber Range training was developed with an emphasis on real-world operations and self-enabling. The training objective is to instruct students on how to conduct offensive and defensive operations, taking into account personnel roles and responsibilities in a Cyber Range environment. Learning modules cover offensive operations, including attack and exploit vectors and target simulations, defensive operations from a network/security operations centers (NOC/SOC) perspective, and lab exercises.

Cyber Range Training Services

Real-World Cyber Ranges

A true Cyber Range environment allows Cyber Warriors to conduct offensive operations against enemy targets connected to networks, and defensive operations to protect critical infrastructure components connected to networks. We implement a Cyber Range environment with multiple components, including computer servers, computer clients, routers, and switches that simulate your real infrastructure components and targets. While many Cyber Ranges are hardware intensive, requiring hundreds of servers and clients, we implement a more cost-effective virtual environment.

Image Source: US Air Force

Ixia's BreakingPoint Cyber Ranges

Ixia BreakingPoint-based Cyber Ranges provide an environment that allows Cyber Warriors to:

- Conduct cyberspace operations to ensure freedom of action in cyberspace, while denying the same to adversaries
- Simulate critical infrastructure components, including computer servers and clients
- Simulate and conduct offensive operations against enemy targets
- Simulate and conduct defensive operations to protect critical infrastructure components.

Cyber Range Targets

To simulate theater operations, Ixia developed a realistic set of targets for multiple geographical areas of responsibilities (AOR). Ixia's Cyber Range targets map to the following geographical AORs:

- Asia Pacific targets
- North America targets
- Europe targets

To simulate real-world operations, the training will leverage available real-world security and network infrastructures to simulate the day-to-day operations that are conducted at data centers, NOCs, and SOCs. Possible infrastructure components include application-level firewalls, intrusion detection systems (IDS), intrusion protection systems (IPS), SYSLOG servers, DLP appliances, routers, switches, network management systems, and application servers. Possible application servers include mail servers, web servers, database servers, and voice servers.

Service Operations Module

The Service Operations Module leverages Ixia BreakingPoint ASI platforms using pre-configured or custom simulations that target private and public infrastructure components and assets. During the lab exercises students will generate target traffic using the following simulations:

- Country of Interest Traffic
- Country of Interest Targets

This will cover real-world traffic scenarios, to include:

- Application traffic simulations with mixes of different protocols
- Reconnaissance activities
- Denial of Service (DoS) attacks, including:
  - IP layer
  - Transport layer
  - Application layer
- Distributed Denial of Service (DDoS) attacks, including:
  - IP layer
  - Transport layer
  - Application layer
- Worm exploits
- Application exploits
- Common Vulnerabilities and Exposures exploits
- Malware

Note: This list will be customized for each customer, based on need.

The service operations module instructs students on how to develop attack vectors with multiple evasion techniques. During the attack and exploit lab exercises, students will perform the following exercises targeting multiple infrastructure components:

- Generate realistic security exploits
- Generate fuzzing traffic with invalid and malformed data
- Generate evasions to bypass security countermeasures

Successful operations require collaboration and information exchanges between operational nodes and their personnel. The training leverages multiple frameworks to capture the information exchanges and operational activities at operation centers. Ixia's Cyber Range Training shows students how to develop the following operational views to support their enterprise operations:

- High-level operational concept graphic
- Operational node description
- Operational information exchange matrix
- Organizational relationship chart
- Operational activity model

Service Defensive Operations Module

The Service Defensive Operations Module includes an overview of the day-to-day activities that are performed at data centers, NOCs, and SOCs. The student will learn how to use operational activity models and operational information exchange matrixes in support of defensive operations. The module also covers how incident response teams (IRT) react to network and security events. During the operations lab exercises, students will perform the following exercises:

- Monitor enterprise traffic
- Monitor network devices
- Monitor security devices
- Respond to network and security events
- Reconfigure network and security devices

Cyber Range Simulation Learning Module

Ixia Cyber Ranges simulate millions of users and thousands of servers and clients with over 245 application protocols, transport protocols, and network protocols. Our Cyber Range Simulation Learning Module leverages Ixia BreakingPoint ASI platforms to simulate critical infrastructure components that can represent anything from financial, utilities, telecommunications, and industrial computer servers to military weapon systems.

Cyber Range Training

Course Code 985-2503 - 3 days

985-2504 - 5 days, includes all of 985-2503, and an additional 2 days of hands-on Operational Scenarios, described below

Level: Advanced

Prerequisites: Students should have a good understanding of TCP/IP and traffic flows. In addition, students may be working with routers, switches, firewalls, and IDS/IPS devices, and security information event management (SIEM), so should have a working knowledge of these products. Students will take on roles of managing the network and security devices during the class, so should have an understanding of these roles.

Synopsis: This course will give students an understanding of offensive and defensive cyber security methods. Students will gain knowledge and skills in reacting to a myriad of cyber security and application traffic flows. Students will be put through Operational Scenarios that include malicious and non-malicious traffic in a safe, secure environment.

Objectives:

Upon successful completion, students will be able to:

- Determine best practices for defensive cyber security mechanisms
- Build a Cyber Range to use as a continual learning tool
- Understand cyber security attacks and how they affect network and security devices
- Configure the Ixia BreakingPoint system to run application and security traffic
- Create Operational Scenarios

Day 1:

- Cyber Range Fundamentals
  - Overview of a Cyber Range and different environments that include Cyber Range Security Operations Center, Cyber Range penetration testing tools, and Cyber Range integrated with a Learning Management System (LMS)
- Network Neighborhood
  - Overview of Network Neighborhood and how to model operational environments
  - Setting up different Network Neighborhoods to include switch, router, and core (virtual) router environments
  - Labs to learn how to setup basic Network Neighborhoods
  - Labs to setup country- and region-specific Network Neighborhoods
- Super Flows
  - Describe what flows, Super Flows, and Application Profiles are and how to build them
  - Super Flow test cases to describe different protocols and how they can be used to build specific application traffic
  - Labs to build Super Flow traffic, as well as putting the Super Flows into an Application Profile

Day 2:

- Critical Infrastructure Servers
  - Building simulated critical infrastructure servers and the traffic being generated
- Client Simulator
  - Overview of Client Simulator test component
  - Adding Super Flows to Client Simulator scenarios
  - Labs to create and run Client Simulator Super Flows previously created
- Application Simulator
  - Overview of Application Simulator test component
  - Adding Application Profiles to Client Simulator scenarios
  - Labs to create and run Application Simulator using different Application Profiles
- Strike Lists
  - Vulnerability detection and reporting
  - Strike List overview
  - Strike List terms
  - Default Strike Lists
  - Fuzzers
  - Labs to configure Strike Lists
- Security
  - Security test component configuration
  - Adding Strike Lists to Security scenarios
  - Evasion Profiles
  - Labs to configure Security test scenarios

Cyber Range Training

Day 3:

- Session Sender
  - Session Sender test component configuration
  - Session Sender test phases
  - What constitutes a session
  - Labs to create Session Sender test scenarios
- Stack Scrambler
  - Stack Scrambler test component configuration
  - Header fields that can be modified
  - Labs to create Stack Scrambler traffic flows
- Reconnaissance Activities
  - PING sweeps
  - Port scans
- IP Layer Attacks
  - ICMP flood
  - ICMP flood with fragments
  - ICMP flood from different clients to different targets
- Transport Layer Attacks
  - UDP flood
  - UDP flood with fragments
  - UDP flood from different clients to different targets
  - TCP SYN flood
  - TCP SYN ACK flood
  - TCP PUSH flood
  - TCP Session attack (all of these can be done multiple times with different Evasion profiles)
- Introduction to Application Layer Attacks, Malware and CVE Attacks

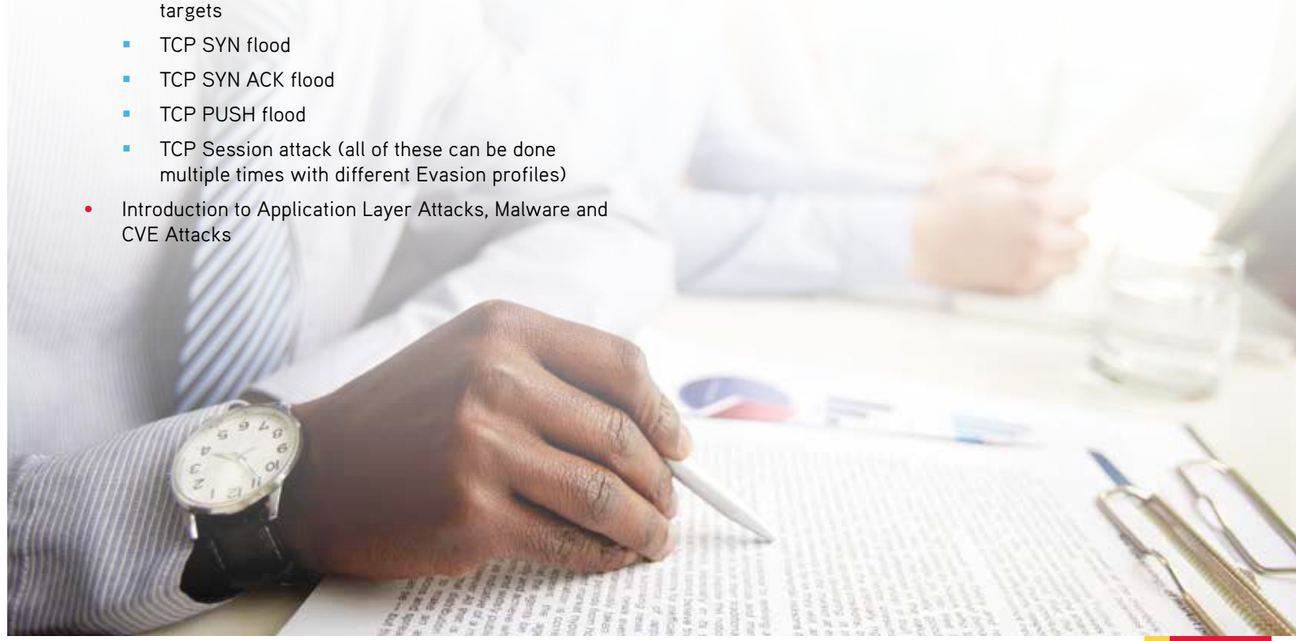
Day 4:

- Application Layer Attacks
  - DNS based attacks
  - HTTP fragmentation attacks
  - Excessive Verb (POST)
  - Excessive Verb (GET)
- Malware
  - Run a mix of the over 35,000 pieces of live malware in different combinations depending on the targets
- CVE attacks
  - Run a mix of over 6000 pieces of CVE attacks

Day 5:

- Review the skills learned throughout the first four days of class
- Practice those skills using the equipment that has been gathered for the customer's specific requirements
- Spend additional time designing customer specific scenarios using techniques learned during the week
- Run through those scenarios with a qualified Cyber Range Instructor available as a guide and mentor

Cyber Range Training is offered at Ixia's Cyber Defense Academy™ or on-site at your location.



Contact Ixia Today

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
21 Serangoon North Avenue 5
#04-01
Singapore 554864
Sales +65.6332.0125
Fax +65.6332.0127

915-4036-01 Rev. A, May 2014