Ixia Cyber Range Services

Training Next-Generation Cyber Warriors with Advanced Cyber Range Services

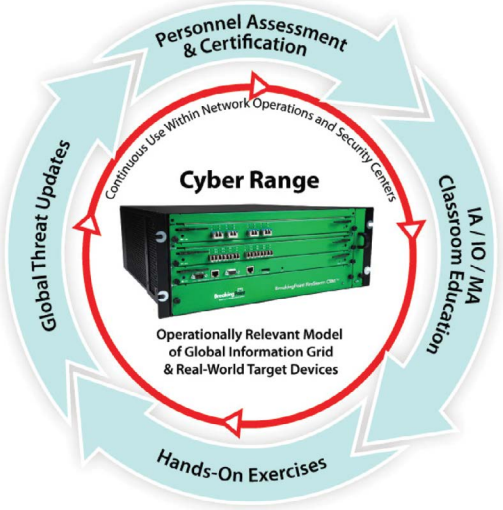
Too many organizations and government agencies have answered the cyber defense challenge by arming their networks with firewalls, intrusion prevention systems (IPSs), and other defenses. Though this satisfies a rudimentary network security checklist, this approach has no hope of keeping pace with the 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 Service 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 services include both pre-built and customized war-game scenarios to ensure the highest security for your particular network.

Our Cyber Range Service leverages BreakingPoint™ Actionable Security Intelligence (ASI) to generate realistic application traffic and exploits, using pre-configured and custom Internet and target simulations. The service generates 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
  - Population and country user base
  - Mobile subscriber user base
  - Data of interest or "needle in a haystack" for data loss prevention (DLP)
  - Enterprise and IT services
  - Internet IPv4 and IPv6 infrastructure

Our Cyber Range Service 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



Real-world cyber ranges are central to the making of elite cyber warriors

including attack and exploit vectors and target simulations, defensive operations from a network/security operations centers (NOC/SOC) perspective, and lab exercises.

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.

Ixia's BreakingPoint Cyber Ranges

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 realistic 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 service leverages real-world security and network infrastructures to simulate the day-to-day operations that are conducted at data centers, NOCs, and SOCs. 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. Application servers include mail servers, web servers, database servers, and voice servers.

Service Operations Module
The service operations module leverages 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

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

For more information see http://www.ixiacom.com

Successful operations require collaboration and information exchanges between operational nodes and their personnel. The service leverages multiple frameworks to capture the information exchanges and operational activities at operation centers. Ixia's Cyber Range Service trains students 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 200+ application protocols, transport protocols, and network protocols. Our cyber range simulation learning module leverages 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 Services are offered at Ixia's Cyber Defense Academy™ or on-site at your location.