

Cyber Range Training Services





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.

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.

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

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.

Cyber Range Simulation Learning Module

Ixia Cyber Ranges simulate millions of users and thousands of servers and clients with over 375 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

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



