



Company:
Cyber Intelligence Sdn Bhd

Industry: Cyber Security
Solution & Service Provider

Key Issues:

- To simulate real-life scenarios for cyber security professionals to develop network security skills as part of IT Security
- To help organizations test and validate their systems to ensure greater resiliency in their network infrastructure and operations

Solutions:

- Ixia BreakingPoint

Results:

- Delivers a real-world learning experience for IT security training
- Helps uncover difficult-to-detect weaknesses in network infrastructure
- Allows organizations to benchmark the performance of IT security teams
- Enables a more proactive approach to defense
- Helps organizations comply with the security assurance requirements of their industries

CYBER INTELLIGENCE PARTNERS WITH IXIA



RAISE THE BAR IN IT SECURITY TRAINING AND NETWORK RESILIENCY VALIDATION

A Cyber Range has been set up at International Islamic University Malaysia (IIUM), the world’s premier Islamic university, to expose IT professionals to “real-world” attack scenarios through the cyber equivalent of military war games. The aim is to help them develop and hone their skills in network security.

Organizations can also make use of the Cyber Range to test and validate their systems to ensure greater resiliency in their network infrastructure and operations. These goals are in line with efforts under the Malaysian National Cyber Security Policy (NCSP) to improve the resiliency of the Critical National Information Infrastructure (CNII) against cybercrime, terrorism, and information warfare. They are also in line with efforts to reduce the number of information security incidents through improved awareness and skill building. CyberSecurity Malaysia (CSM), Malaysia’s national cyber security agency, which operates under the Ministry of Science, Technology and Innovation (MOSTI), aspires to train and certify 10,000 cyber security professionals by 2020.



CHALLENGES

Cyber Range Malaysia is part of the CSM-IIUM Cyber Security Centre of Excellence, which launched in July 2016 as a collaboration among CSM, IIUM, and Cyber Intelligence Sdn. Bhd. (CI).

In addressing these training needs, CI's approach involves providing participants with a close-to-live learning environment to help them better visualize the threat landscape. It deploys network simulation equipment so that network topologies can be configured to mirror the actual infrastructure environment in an organization. However, CI realized it lacked the ability to generate attack traffic, simulating real-world attack scenarios.

"Only with an Internet-scale, operationally-relevant, and ever-current Cyber Range can organizations produce the empirically valid cyber war-gaming scenarios necessary to develop IT staff skills and instincts for defensive action," says Professor Mohamed Ridza Wahiddin, PhD, DSc, Deputy Rector of Research and Innovation at IIUM.

In searching for a solution to plug this gap, CI partnered with Ixia®. Ixia's BreakingPoint® is being used in some of the largest cyber ranges around the world, such as the U.S. Defense Advanced Research Projects Agency National Range. The partnership between CI and Ixia, and the collaboration among CI, CSM, and IIUM marks the first time this technology has been deployed at an institute of higher learning in Malaysia.

With a state-of-the-art infrastructure now in place for IT security training, CI will offer its associate-level cyber defense course to those who would like to increase their security operations proficiency, add to their skillset in cyber security, or take on cyber-security related roles.

This can include system/network administrators, information security officers/information security managers, C-level IT professionals, security auditors, and governance and compliance officers. The



"Cyber Range Malaysia will be an important contributor toward nurturing more highly-skilled cyber security experts for Malaysia and its neighboring countries"

— Naavin Vasshudave, Chief Operations Officer, of Cyber Intelligence Sdn Bhd

"One of the key challenges in training security professionals is to assess how well they identify and respond to an attack and defend their network in a real-world scenario"

— Dr. Amirudin Abdul Wahab, CEO of CyberSecurity Malaysia

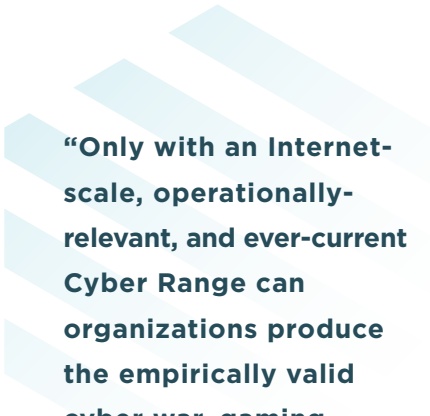
associate course, called Certified Cyber Defender Associate (CCDA) is certified by IIUM and endorsed by CSM.

The program is also in line with CSM's efforts to address the chronic shortage of manpower in this sphere. The introduction of the CCDA program enables participants to advance their IT security skills or make a midcareer switch to specialize in IT security.

Five key benefits to participants getting CCDA certified include:

- Developing a deep understanding and advanced skills to defend their organization and formulate defense strategies against sophisticated cyber-attacks.
- Learning to formulate defense responses using vulnerability management systems, next-generation firewalls, intrusion prevention systems, URL filters, anti-spyware systems, anti-virus systems, anti-Distributed Denial of Service (DDoS) systems, data filters and file blocking systems, and advanced application-based protection systems.
- Developing the ability to correlate information from the sources mentioned and collaborate with other team members to further develop a comprehensive cyber defense strategy.
- Boosting earning capability.
- Improving credibility in terms of their information security qualifications and experience

For organizations, Cyber Range Malaysia also plays a key role in identifying and plugging gaps in their IT security, especially in the area of network resiliency through a service offering called Testing as a Service (TaaS). This is key in optimizing IT investments in security while minimizing test investments. When testing security devices needs to be done quickly and correctly the first time, CI's TaaS delivers a fast, accurate, and reliable means of validating the proper function of security infrastructures and devices when they are needed most.



“Only with an Internet-scale, operationally-relevant, and ever-current Cyber Range can organizations produce the empirically valid cyber war-gaming scenarios necessary to develop IT staff skills and instincts for defensive action,”

— Professor Mohamed Ridza Wahiddin, PhD, DSc, Deputy Rector of Research and Innovation at IIUM.



CI's TaaS Security Assessments:

- Validate what you know, and uncover what you do not: Bad things happen in “blind spots.” We find them fast.
- Measure system performance: Repeatable testing of competing devices helps you select the best next-gen firewall (NGFW), Intrusion Prevention System (IPS), and other security elements for your company's needs.
- Determine resiliency to attack: Planned attacks test how well you'll react to the real ones—and real attacks will happen. Ixia generates advanced Denial of Service (DoS) attacks to pinpoint the vulnerabilities savvy attackers will use to bring down services.

Two of the main Security Assessments conducted in Cyber Range Malaysia are DoS assessments and NGFW assessments. CI's network-based assessments generate real attacks to help evaluate defenses against volumetric attacks designed to degrade performance. CI DoS assessments span three critical areas to uncover and pinpoint areas of vulnerability. Emulating actual attacks in a controlled manner helps strengthen defenses, improve response times, and minimize the impact on end-users as real attacks occur. Individual device assessments provide fast, easy “bakeoffs” between competing solutions. CI NGFW assessments measure seven critical aspects of device performance, so security professionals can make “apples-to-apples” comparisons to find the best solution for their company's needs.

“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,”

— Sivanathan Subramaniam,
Chief Executive Officer of
Cyber Intelligence Sdn Bhd

“Much of the security effort in organizations has been focused on testing and hardening the security on the server side, for example, through penetration tests. But, little has been done to address resiliency issues on the network side,”

— Naveen Bhat,
Managing Director, Ixia, Asia Pacific

SOLUTION

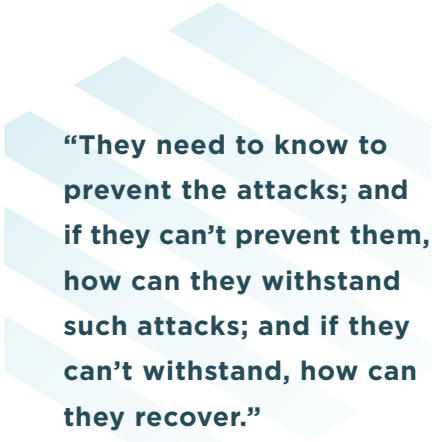
Powered by Ixia's BreakingPoint, Cyber Range Malaysia helps address these issues. This technology agnostic solution works with any networking products to pinpoint weaknesses in the devices, the network, or the data center before they can be exploited. It does this by bombarding network components, such as routers, switches, firewalls, and servers with extreme loads of application and malicious traffic at up to 40 Gbps and monitoring the effects over time.

It also features unprecedented scalability, with the ability to produce Internet-scale scenarios and traffic from millions of users. "Instead of having hundreds of thousands of servers and users, you can now simulate up to 90 million concurrent TCP/IP sessions on one BreakingPoint system," says Bhat.

Delivers an Authentic Learning Experience for IT Security Training

By simulating real traffic and attacks on the Cyber Range, BreakingPoint enables Cyber Range Malaysia to provide an authentic learning experience.

"As far as possible, we try to expose our students to different IT security scenarios. In a cyber-exercise, we get them to play different roles. For example, we use Ixia BreakingPoint to pump in attack traffic, and the student playing the role of defender will handle incident response. We want to see their reaction or what action they will take. Since attacks cannot be introduced on a live network, the real-life conditions have to be simulated to train IT security professionals for these attacks," says Bhat. "They need to know to prevent the attacks; and if they can't prevent them, how can they withstand such attacks; and if they can't withstand, how can they recover. This is the cycle, and Cyber Range trains them to handle these situations."



"They need to know to prevent the attacks; and if they can't prevent them, how can they withstand such attacks; and if they can't withstand, how can they recover."

— Naveen Bhat,
Managing Director, Ixia, Asia Pacific

Helps Uncover Difficult-to-Detect Weaknesses in the Network Infrastructure

On the other side of security infrastructure, Ixia's BreakingPoint picks up the traffic so that the organization can monitor how much of the attack gets propagated down to the internal network. With this, BreakingPoint Storm™ generates a Resiliency Score™ to indicate the performance of discrete components, as well as the network as a whole, under high-stress, hostile conditions.

Using the BreakingPoint Resiliency Score, the organization can identify problem areas and remediate through tuning and configuration changes. The Resiliency Score provides a deterministic, scientific, and repeatable measurement of resiliency both at the network and device levels. With this information, organizations can evaluate and select the most appropriate network equipment for their critical infrastructure.

Allows Organizations to Benchmark the Performance of their IT Security Teams

The Resiliency Score is also useful for organizations that want to benchmark the performance of their IT security team. Once they know where their improvement areas are, the organizations can take measures to address weaknesses, such as improving their incident response procedures, increasing the competency of the IT security staff in handling attacks. "We can set up a controlled environment that simulates their infrastructure, and organizations can evaluate how they deal with cyberattacks," says Navin.

Ixia BreakingPoint helps organizations adopt a more proactive approach to IT security by making sure their policies are effective in detecting these attacks. For example, a distributed DoS (DDoS) attack will not be picked up by the firewall, because firewalls usually look at the IP address, while a DDoS attack can come from all directions. Neither will it be picked up through deep packet inspection, because a DDoS packet looks like a normal data packet with no malware or viruses. What is different about a DDoS attack is the sheer number of requests that are being sent to a server, which subsequently hangs when it is overwhelmed

by the workload. By simulating a DDoS attack on the Cyber Range, organizations can fine-tune their policies to detect if there is an abnormal number of concurrent attempts to access the server so that remedial action can be taken before the server crashes.

Organization

Established in 2010, Cyber Intelligence Sdn Bhd is an information security service and solution provider. Since its inception, CI has won multiple awards, including the Malaysian Cyber Security Awards 2015 for Training & Education Provider of the Year and Finalist of APICTA 2015 for Best of Security. Its information security solutions and services are being used by many enterprises across many verticals, such as telco, financial, healthcare and government. CI, in partnership with CyberSecurity Malaysia (CSM) and International Islamic University Malaysia (IIUM) is the builder and operator of Cyber Range Malaysia and exclusively delivers and manages the government sanctioned Next-Gen Cyber Defender training program and all Testing As A Service (TaaS) activities.

ABOUT IXIA

Ixia provides testing, visibility and security solutions, strengthening applications across physical and virtual networks for enterprises, governments, service providers, and network equipment manufacturers.

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