New England Regional Cyber Range Opens At Devens

Devens, MA – October 2017 - New England Regional Cyber Range, the only regionally-based independently owned cyber range, announced today the opening of the new facility at the Devens Innovation Center. This new facility was created to support the training and education of cyber security professionals. The range is aligned with the Massachusetts State DLCS (Digital Literacy and Computer Science) curriculum framework. The range will include cyber warfare training, incident response simulations and reverse engineering classes.

Joe Provost, managing partner and owner of Syncstate stated, “This state-of-the-art training and development facility is comprised of Live, Virtual, and Simulated (LVS) technologies. It is being used to address the critical skills gap and need for highly specialized cyber security individuals within the New England region with a specific focus on Massachusetts.”

The Cyber Range

The range provides a realistic copy of the Internet, several corporate networks, hacker sites, nation state actors, simulated users, and other tools and technologies designed for training and exercises, product testing, threat modeling, and software testing and development.

The training scenarios and exercises combine both commercial and open source technologies. Syncstate and its partners makes use of this platform to model threat events pulled directly from the headlines. The combined effects immerse individuals into complicated cyber warfare activities to train how to properly detect, respond, and mitigate a variety of threats. “We use the same hacking tools and tactics as the adversary. You will be required to protect the business processes and systems while working in a contested environment,” said Provost.

Who Uses The Range And Why

The training programs and exercises are built for both the technical expert and senior management person alike. The total immersion means your organization will be able to complete end-to-end incident response plan testing as well as prepare for advanced cyber warfare activities. It provides the capability for any organization to train. Using the range means that you’re not restricted to a simple table top exercise or an environment not representative of your particular company.

The environment provides everything you need, right down to the workstations. This ensures that your own systems will not be infected or damaged.

Benefits of the NECYR include:

- Real world network environments (organization specific)
- Network forensics and incident response training
- Vulnerability research and reverse engineering
- Open source data collection and intelligence production
- Offensive cyber warfare training
- Capture-the-Flag Events
- Individual training plan development
- Software development and testing (IV&V)

Threat Modeling and Simulation

There are a variety of scenarios that your team can participate in. Threat Modeling provides a unique approach to attack vectors and tactics that will be used against any network. Internal Red Teams will study your environment to better understand the potential threats. Events and attacks are adjusted for each exercise scenario to ensure it is a true representation of current and potential threats to any business.

Fusion Center Layout

The cyber range is connected to several threat feeds. The information displayed across several different image sources and control panels provides a rich visual environment. The Fusion Center can be specifically tailored to represent a Security Operations Center (SOC) to support complex cyber security exercises to a Business Intelligence (BI) Center for senior leaders to exercise crisis communications (media, interviews).

The new Remote Connection Pod means that facilities that are geographically separate can actively participate in large scale exercises and testing scenarios. Universities who participate can provide hands-on experience for the student body that would not otherwise be available.

Training and Exercises

For the experts - the Incident Response and Network Forensics exercise is for senior managers (CISO) and their technical staff to train the handling of events that occurred over a period of time but have just been discovered.

The scenarios can be modified to represent a government organization, financial institution, manufacturing facility, or hospital. The environment would include typical web applications, credit card services, internal and external services and other common ports and protocols normally found in any business network today.

Organizational Specific Exercise – This industry specific exercise is about Quest Star Hospital and their remote offices. You will be required to control and defend business and hospital systems, office specific applications, and third party systems that are cyber dependent.

This program and other exercise programs are designed to educate your organization and increase their ability to properly identify and mitigate impacts to critical business systems. The combination of cyber related incidents and skills to communicate issues between organizational groups will be improved. This improvement will help your business build confidence during day-to-day operations as well as improve the ability to handle difficult situations when critical decision-making under pressure is needed.

Tailored Cyber Warfare Exercises – The range makes it possible to create a custom cyber exercise and operating environment. This type of exercise demands careful and thoughtful planning, preparation, and targeted evaluation. This is critical to create the custom environment.

Requests for this level of granularity are reviewed on a case-by-case basis. The range can be tailored to represent specific networks, systems, and services to conduct live cyber warfare exercises. Contact Range Operations to discuss your specific needs.

Operating Hours:
Monday-Friday: 0800am – 1730pm (EDT)
Saturday: 0900am – 1200am (EDT)
Sunday: Closed

Phone: (978) 875 - 2832
Email: info@necyrange.com
Website: http://www.necyrange.com