INTERACTIVE CYBERSECURITY WORKSHOPS

From entry level to C-suite, the Michigan Cyber Range offers a range of strategic and technical seminars and interactive workshops. Topics range from cyber crimes and cyber warfare, secure coding and scripting, IT employee management and more.

Completely customizable, our workshops are available as private engagements at your location, via telepresence or at Merit headquarters in Ann Arbor, Michigan. These workshops can supplement workforce development programs and certifications and can also be used as a segue to hands-on exercises and tabletop exercises.

MICHIGAN CYBER RANGE WORKSHOPS

A PCI COMPLIANCE ROADMAP

DURATION: 4 HOURS

Understand the requirements of PCI compliance and build a framework for your organization in this introductory session. PCI SAQs, six control objectives, evidence gathering and how to define scope will be covered.

THREAT AT YOUR DOORSTEP: CYBERSECURITY FOR EXECUTIVES

DURATION: 4 OR 8 HOURS

Threat At Your Doorstep is comprised of several 50-minute modules focusing on the current threat landscape, social engineering, critical controls, common attack vectors and more. Participants receive an in-depth overview of the types of various hackers, the nature and role of training programs and warning signs of an attack. Attendees will also participate in a phishing demonstration.

CENTERS FOR INTERNET SECURITY 20 CRITICAL SECURITY CONTROLS

DURATION: 4 HOURS

Organizations will learn to prioritize actions to improve enterprise security posture using a threat-focused approach, rather than regulatory compliance. This workshop offers a lens for focusing activity on improving the areas which will have the largest impact on security by concentrating on specific threats and how they can be used to exploit security weaknesses.

INCIDENT RESPONSE WORKSHOP

DURATION: 4 HOURS

Build an incident response plan for your organization. The IR Workshop is based on the National Institute of Standards and Technology (NIST) 800 framework for managing computer security incidents. Attendees will learn the format of an IR plan, how to determine a reportable incident, roles of a response team and more. Participants will leave the workshop with a drafted incident response plan.

Any company that must comply with the North American Electric Reliability Corporation (NERC) critical infrastructure protection (CIP) cybersecurity standards should attend, as well as accounting firms, emergency managers, government officials and police personnel.

This workshop can be tailored to instruct on development and testing for NERC CIPv6.

POLICY MANAGEMENT

DURATION: 4-8 HOURS

The Policy Management Workshop is designed to provide valuable insight about the development of governance within an organization, ways to create policy training and awareness within your staff and the establishment of policies that align to data regulations.

During the workshop attendees will complete policy management templates and will gain an understanding of a formal policy organization structure. A hands-on portion of the event allows groups and individuals to practice crafting, or improve upon an already existing policy, standards and procedure guide.

PROTECTING IOT

DURATION: 4 HOURS

From hardware and software configuration to end-user security, there are multiple potential vulnerabilities in the IoT space. The growing demand of new device technology often means that security is a secondary concern. With the global rise in hacking attempts, organizations must develop IoT security frameworks, secure programming best practices and end-user education.

In this introductory session on IoT, attendees will gain an understanding of how to apply IoT frameworks for increased security in manufacturing and consumer products.

HOW TO IMPLEMENT RISK MANAGEMENT IN YOUR CYBERSECURITY PROGRAM

DURATION: 4 HOURS

Develop a roadmap for tracking and addressing risks throughout your development lifecycles. This workshop discusses implementation of NIST's (National Institute of Standards and Technology) Risk Management Framework to reduce overall risk in your organization.

GO PHISH

DURATION: 50 MINUTES

Phishing attempts, the tactics employed to trick users into sharing personal information, passwords and credit card numbers, are growing in frequency and sophistication. This demonstration illustrates the ease and speed of phishing attempts and arms attendees with tactics to protect their personal data.

WIFI HACKING DEMO

DURATION: 50 MINUTES

This workshop demonstrates the ease with which hackers can fake a wireless access point, while tricking users into believing they are connecting to a legitimate network. Watch as traffic is manipulated within the audience during the presentation, and gain an understanding of the different types of approaches hackers can use.

MUSKETEER

DURATION: 4-8 HOURS

This workshop is a guided version of our Capture The Flag Exercise, which is a challenge designed to cover the spectrum of cybersecurity. Participants will use open source tools to fire off live attacks on networked systems in real time.

Participants should have basic computer skills, familiarity with the command line, understanding of IP addressing and DNS and familiarity with basic security concepts. A proctor will be onsite to solve technical problems and to assist participants who get stuck. They will be pointed in the right direction, but not given the answer outright.

CYBERSECURITY WORKSHOPS K-12

DURATION: 50 MINUTES

K-12 focused presentations discuss social engineering, critical controls for IT managers, cybersecurity from a hacker's vantage point, OWASP 10 and SANS Top 20 Controls, securing endpoints and applications and IT risk management. Any individual in the K-12 arena will benefit from gaining an understanding in beginning an onsite security program through this workshop. Contact us to develop a custom program for your organization!

SECURITY ON A SHOESTRING

DURATION: 4 HOURS

With the cost of security products and services skyrocketing, how can organizations afford to protect themselves?

Larger organizations are able to purchase the necessary equipment and hire security staff, but small and medium sized businesses have difficulty keeping up. Hackers are very aware of this trend and are now targeting these smaller organizations with gaps in their security plan in the hopes of pulling off a successful breach.

Gartner is predicting that prices will continue to rise for security protection and firewall services. The industry could see as much as $170 billion in growth over the next four years.

ALPHA SCOUT

DURATION: 2 HOURS

This workshop, aimed at executives, is a guided demonstration of Capture the Flag, led by a Cyber Range Analyst. This session is ideally completed through a two-hour hands-on BYOD workshop utilizing the Alphaville training environment, however, it can also be executed in a lecture-style session.

merit.edu | sales@merit.edu

The Michigan Cyber Range prepares cybersecurity professionals to detect, prevent and mitigate cyber-attacks in a real world setting. Certification courses, hands-on exercises and workshops are hosted on the range, the nation's largest unclassified private cloud.

The Michigan Cyber Range is hosted and facilitated by Merit Network.