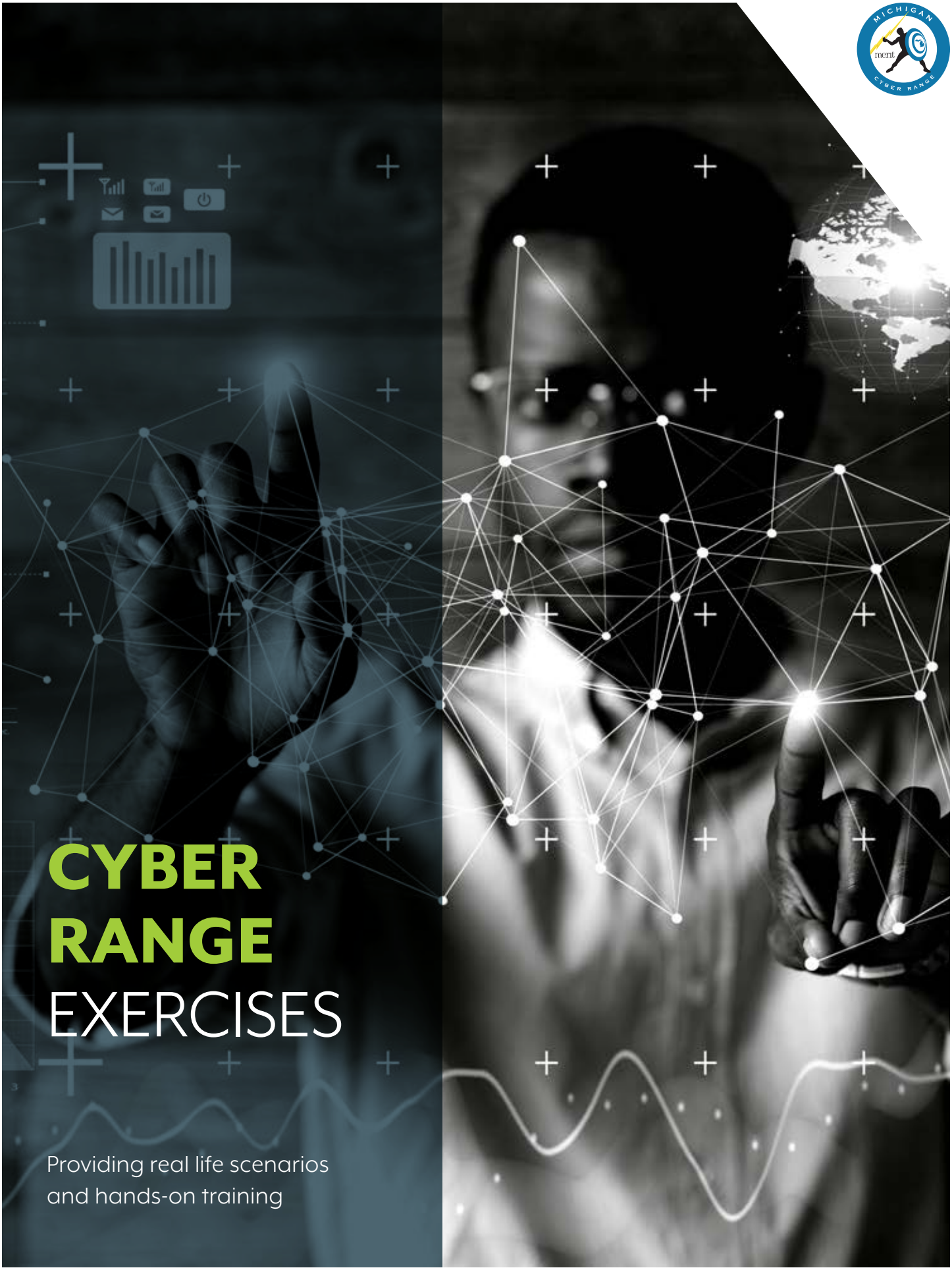

CYBER RANGE EXERCISES

Providing real life scenarios
and hands-on training

Michigan Cyber Range exercises offer an affordable, hands-on training environment, which provides real life scenarios that teach users to detect and mitigate cyber attacks.

These exercises complement other elements of cybersecurity training by challenging participants to apply the skills they've learned in classes and on-the-job training in realistic settings.

All teams can participate in Michigan Cyber Range exercises virtually – there is no requirement to be onsite. User experience is augmented through the use of our scoreboard and 3D visualization of the Alphaville training environment.

Unlike our competitors, Michigan Cyber Range exercises are wholly contained within the secure Michigan Cyber Range and are extremely affordable for organizations of all sizes and can be customized to meet your scheduling and organizational needs:

- Game-based problem solving, more effective than book learning
- Flexible scheduling with ½ day to week-long exercises
- Facilitated by Cybersecurity Experts
- Some exercises are self-paced
- Customize teams to the needs of your organization
- Training takes place at a Cyber Range facility or your site
- **All exercises mapped to NICE FEMA ICS standards.**

CYBER RANGE EXERCISES

CAPTURE THE FLAG

DURATION: 4-8 HOURS
SKILL LEVEL: INTERMEDIATE

Capture the Flag, or CTF, is a challenge designed to cover the spectrum of cybersecurity. From Python scripting and web application hijacking to penetrating SCADA networks, reverse engineering and database hacking, the exercise challenges participants' technical skills. Attendees will also learn to become better defenders by using open source tools.

Participants will use open source tools to fire off live attacks on networked systems in real time. A self-paced exercise, the CTF is a means to assess individual skills across a broad range of systems.

Teams and individuals can play from any location in a complete Capture the Flag environment. This means that nobody can prevent another's ability to capture a flag or achieve a challenge. User experience is augmented through the use of our scoreboard and 3D visualization of the Alphaville environment. This is ideal for Capstone activity.

CTF participants should have basic computer skills, familiarity with the command line, understanding of IP addressing and DNS, familiarity with basic security concepts, problem solving skills, and resourcefulness. Participants will not know all the solutions to problems encountered in the CTF. The solutions will require research outside of the game.

PLEASE NOTE:

Participants are shown how to access to the CTF and how to interact with the environment. A proctor is onsite to solve technical problems only. No assistance in how to solve challenges is offered. All participants must hold intermediate to advanced cybersecurity and programming skills in order to succeed in the exercise.

CYBER SENTINEL PASSIVE

DURATION: 8 HOURS

SKILL LEVEL: NEWLY FORMED CYBER IR TEAMS WITH INTERMEDIATE SKILLS

Cyber Sentinel Passive is a hands-on foundational Incident Response exercise that maps to the NIST 800 standards. Sentinel will lay the groundwork for establishing and strengthening your Incident Response teams, assigning team member roles and assessing your organization's readiness to an actual incident. Newly formed teams should participate in this exercise - Cyber Range Analysts will leave forensic clues for your participants to work through as a team.

Teams will need to quickly distinguish between precursors, indicators and false positives to secure the network and conduct forensic analysis. Problem solving and tool selection play an integral role in progressing through the exercise as while utilizing various open source tools to enumerate actual threats. Traditionally, this exercise is not scripted, and requires players to simulate their actions and policies as they would in defending a live network against passive adversaries.

- Preparation and IR planning
- Detection and analysis
- Containment, eradication and recovery
- Post-incident activity

CYBER SENTINEL ACTIVE

DURATION: 8 HOURS
SKILL LEVEL: INTERMEDIATE – ADVANCED EXISTING CYBER INCIDENT RESPONSE TEAMS

Cyber Sentinel Active is a version of Cyber Sentinel that is intended to strengthen and assess the response capability of an organization's already established Incident Response team. This exercise is intended for established teams who understand their current roles during an incident.

Your preexisting cyber incident response teams will play against one or more Red Teams to secure your network and conduct forensic analysis.

PAINTBALL

DURATION: 8 HOURS

SKILL LEVEL: INTERMEDIATE – ADVANCED

The Stampede challenge is a multi-team-based engagement, which challenges the penetration and defense skills across the spectrum of cybersecurity. Similar to Capture The Flag, teams use open source tools to fire off live attacks on networked systems in real time.

Teams compete against each other in the Alphaville environment with the goal of penetrating, controlling, and securing as many systems as possible.

TABLE TOP EXERCISE

DURATION: 8 HOURS

SKILL LEVEL: NOVICE - EXECUTIVES

Table Top Exercises test and validate an organization's ability to handle cyber incidents, and execute procedures at an organizational level.

Executives and employees from within finance, human resources, IT and legal departments should attend. Table Top exercises are designed to facilitate discussion around policies and procedures.

CYBER DEFENSE EXERCISE (RED VS. BLUE)

DURATION: 8 HOURS

SKILL LEVEL: INTERMEDIATE – ADVANCED

The Cyber Defense Exercise scenario is a force-on-force cyber exercise that challenges cybersecurity professionals with a live, thinking, adapting adversary.

This exercise is completely customizable - your teams can attack, defend or both. Cyber Defense Exercise takes place in a subset of our larger Alphaville Training environment. Teams are assessed based on learning objectives in an after-action review.

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.