MERIT CLASSES

The Michigan Cyber Range features a cybersecurity education experience based upon the National Institute of Standards and Technology National Initiative for Cybersecurity Education (NICE).

These training opportunities, including DoD approved baseline certifications, are offered both as private classes for your organization, and through our Cyber Range Hubs.

CERTIFICATION TRAINING - ISC2

CAP – CERTIFIED AUTHORIZATION PROFESSIONAL

The CAP certification is an objective measure of the knowledge, skills, and abilities required for personnel involved in the process of authorizing and maintaining information systems. Specifically, this credential applies to those responsible for formalizing processes used to assess risk and establish security requirements and documentation. Earning the CAP is a powerful way to validate your knowledge. It shows you thoroughly understand information security and risk management processes and procedures. You'll stand out and be more competitive.

CCFP – CERTIFIED COMPUTER FORENSICS PROFESSIONAL

CCFP addresses more experienced cyber forensics professionals who already have the proficiency and perspective to effectively apply their cyber forensics expertise to a variety of challenges. In fact, many new CCFP professionals likely hold one or more other digital forensics certifications. Given the varied applications of cyber forensics, CCFP professionals can come from an array of corporate, legal, law enforcement, and government occupations.

CCSP – CERTIFIED CLOUD SECURITY PROFESSIONAL

Instant credibility and differentiation. The CCSP positions you as an authority figure on cloud security. It's a quick way to communicate your knowledge and earn trust from your clients or senior leadership. Unique recognition. When you earn the CCSP, you achieve the highest standard for cloud security expertise. This certification is powered by the two leading non-profits focused on cloud and information security.

CISSP – CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL

As other CISSPs will tell you, this certification will raise your visibility and credibility, improve your job security, create new opportunities for you or even increase your salary — depending on your country and employer. Challenge yourself to grow and be better. The CISSP exam is a rigorous test of your knowledge. But well beyond the exam, the CISSP is about reaching a deeper, better and broader understanding of the common body of knowledge for cybersecurity. It's an exhilarating feeling to become a CISSP.

CSSLP – CERTIFIED SECURE SOFTWARE LIFECYCLE PROFESSIONAL

Instant credibility. The CSSLP proves you're a subject matter expert in application security. It shows you have desirable skills for employers around the world, giving you more opportunities. Increased compensation. While pay practices vary by employer, many CSSLPs find that this software security certification can lead to pay gains and "skill premiums." Relevant, new knowledge. Earning the CSSLP is a great way to expand your security knowledge, in addition to affirming your expertise. It offers continuing education, so you can keep your skills current and relevant.

HCISPP – HEALTHCARE INFORMATION SECURITY AND PRIVACY PRACTITIONER

The HCISPP is the only certification that proves you have the practical skills, foundational knowledge and experience in both security and privacy on an international level. It shows you know best practices and have real-world expertise in both healthcare information security and privacy. The HCISPP exam covers current, global topics. This ensures you're up-to-speed on evolving threats and regulations around the world. You're better prepared to protect your organization and patient data.

CERTIFICATION TRAINING - EC COUNCIL

C)NDA – CERTIFIED NETWORK DEFENSE ARCHITECT

This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. This course was specially designed for Government Agencies.

CCISO – CERTIFIED CHIEF INFORMATION SECURITY OFFICER

The Certified CISO (CCISO) program is the first of its kind training and certification program aimed at producing top-level information security executives. The CCISO does not focus solely on technical knowledge but on the application of information security management principles from an executive management point of view. The program was developed by sitting CISOs for current and aspiring CISOs. In order to sit for the CCISO exam and earn the certification, candidates must meet the basic CCISO requirements.

CEH – CERTIFIED ETHICAL HACKER$_A$

Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s). The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.

CHFI – COMPUTER HACKING FORENSIC INVESTIGATOR

The Computer Hacking Forensic Investigator course provides a strong baseline knowledge of key concepts and practices in the digital forensic domains relevant to today's organizations. CHFI provides its attendees a firm grasp on the domains of digital forensics. In the event of a cyber-attack or incident, it is critical investigations be carried out in a manner that is forensically sound to preserve evidence in the event of a breach of the law.

E)CES – EC-COUNCIL CERTIFIED ENCRYPTION SPECIALIST

A person successfully completing this course will be able to select the encryption standard that is most beneficial to their organization and understand how to effectively deploy that technology. This course is excellent for ethical hackers and penetration testing professionals as most penetration testing courses skip cryptanalysis completely., better and broader understanding of the common body of knowledge for cybersecurity. It's an exhilarating feeling to become a CISSP.

ECIH – EC-COUNCIL CERTIFIED INCIDENT HANDLER

The EC-Council Certified Incident Handler program is designed to provide the fundamental skills to handle and respond to the computer security incidents in an information system. The course addresses various underlying principles and techniques for detecting and responding to current and emerging computer security threats. Students will learn how to handle various types of incidents, risk assessment methodologies, and various laws and policy related to incident handling.

ECSA – EC-COUNCIL CERTIFIED SECURITY ANALYST

The ECSA penetration testing course provides you with a real world hands-on penetration testing experience and is a globally accepted hacking and penetration testing class available that covers the testing of modern infrastructures, operating systems and application environments while teaching the students how to document and write a penetration testing report.

ENSA – EC-COUNCIL NETWORK SECURITY ADMINISTRATOR

The EC-Council Network Security Administrator (ENSA) certification verifies candidate's network security skills and knowledge from defensive perspective while the CEH certification looks at the security from an offensive view. An ENSA should have fundamental skills to analyze the internal and external security threats against a network, and to develop security policies that will protect an organization's information. Certified professionals should know how to evaluate network and Internet security issues and design, and how to implement successful security policies and firewall strategies.

L)PT – LICENSED PENETRATION TESTER

EC-Council's prestigious endorsement as a licensed penetration testing professional, allows successful candidates to practice penetration testing and consulting internationally. You will need to demonstrate a mastery of the skills required to conduct a full blackbox penetration test of a network provided to you by EC-Council on our cyber range, iLabs. You will follow the entire process taught to you through Ethical Hacking and Security Assessment, taking you from reconnaissance, scanning, enumeration, gaining access, maintaining access, then exploiting vulnerabilities that you will have to seek out in a network that only a true professional will be able to break.

CERTIFICATION TRAINING - CompTIA

A+ – COMPTIA A+

Held by over 1 million IT professionals worldwide, CompTIA A+ is the most essential IT certification for establishing an IT career. If you're new to the IT industry, this will help you put your best foot forward. And if you're already an IT professional, the CompTIA A+ certification validates your skills and can boost your career.

N+ – NETWORK+

The stakes are high. Data networks are more crucial for businesses than ever before. They are the lifeline to the critical financial, healthcare and information services that need to function at the highest, most secure level. With a CompTIA Network+ certification, you will possess the key skills to troubleshoot, configure and manage these systems and keep your company productive..

S+ – SECURITY+

IT security is paramount to organizations as cloud computing and mobile devices have changed the way we do business. With the massive amounts of data transmitted and stored on networks throughout the world, it's essential to have effective security practices in place. That's where CompTIA Security+ comes in. Get the Security+ certification to show that you have the skills to secure a network and deter hackers and you're ready for the job.

SKILL BASED TRAINING - MILE2

C)DFE – CERTIFIED DIGITAL FORENSICS EXAMINER

The Certified Digital Forensics Examiner vendor neutral certification is designed to train Cyber Crime and Fraud Investigators whereby students are taught electronic discovery and advanced investigation techniques. This course is essential to anyone encountering digital evidence while conducting an investigation. The Certified Digital Forensics Examiner course will benefit organizations, individuals, government offices, and law enforcement agencies interested in pursuing litigation, proof of guilt, or corrective action based on digital evidence.

C)DRE – CERTIFIED DISASTER RECOVERY ENGINEER

The comprehensive Certified Disaster Recovery Engineer course goes beyond traditional BCP training -preparing students for industry certification in Business Continuity planning, and presenting the latest methodologies and best practices for real-world systems recovery. Students will receive a solid foundation of instruction that will enable them to create meaningful business continuity plans. This course offers up-to-date information that has been developed by leading risk management professionals.

C)IHE – CERTIFIED INCIDENT HANDLING ENGINEER

The Certified Incident Handling Engineer vendor neutral certification is designed to help Incident Handlers, System Administrators, and any General Security Engineers understand how to plan, create and utilize their systems in order to prevent, detect and respond to attacks. Furthermore, students will enjoy numerous hands-on laboratory exercises that focus on topics, such as reconnaissance, vulnerability assessments using Nessus, network sniffing, web application manipulation, malware and using Netcat plus several additional scenarios for both Windows and Linux systems.

C)ISA – CERTIFIED INFORMATION SYSTEMS AUDITOR

Earning the CISA designation helps assure a positive reputation as a qualified IS audit, control and/or security professional, and because the CISA program certifies individuals who demonstrate proficiency in today's most sought-after skills, employers prefer to hire and retain those who achieve and maintain their designation. Learn how to decode the technical situation and report on compliance using accurate, non-technical facts. Learn how to avoid the common pitfalls so you can remain safe from liability.

C)ISM – CERTIFIED INFORMATION SECURITY MANAGER

The Certified Information Systems Security Manager covers the skills and knowledge to assess threat analysis and risks, Risk & incident management, Security programs and CISO roles, IS security strategy and frameworks, Audit and Risk management creation of policies, compliance and awareness, as well as DR and BCP development, deployment and maintenance. The Certified Information Systems Security Manager will receive in-depth knowledge.

C)ISSO – CERTIFIED INFORMATION SYSTEMS SECURITY OFFICER

The C)ISSO course addresses the broad range of industry best practices as well as the knowledge and skills expected of a security leader. The C)ISSO candidate learns BOTH the theory and the requirements for practical implementation of core security concepts, practices, monitoring and compliance. Through the use of a risk-based approach, the C)ISSO is able to implement and maintain cost-effective security controls that are closely aligned with not only business requirements but global industry standards.

C)NFE – CERTIFIED NETWORK FORENSICS EXAMINER

The C)NFE takes a digital and network forensic skill set to the next level by navigating through over twenty modules of network forensic topics. The CNFE provides practical experience through our lab exercises that simulate real-world scenarios that cover investigation and recovery of data in network, Physical Interception, Traffic Acquisition, Analysis, Wireless Attacks and SNORT. The course focuses on the centralizing and investigating of logging systems as well as network devices.

C)PEH – CERTIFIED PROFESSIONAL ETHICAL HACKER

The CPEH certification training enables students to understand the importance of vulnerability assessments by providing industry knowledge and skills in Vulnerability Assessments. In doing so, the CPEH student is able to understand how malware and destructive viruses function. In addition, the CPEH course helps students learn how to implement counter response and preventative measures when it comes to a network hack.

C)PTC – CERTIFIED PENETRATION TESTING CONSULTANT

The vendor neutral Certified Penetration Testing Consultant course is designed for IT Security Professionals and IT Network Administrators who are interested in conducting Penetration tests against large network infrastructures similar to large corporate networks, Services Providers and Telecommunication Companies.

C)PTE – CERTIFIED PENETRATION TESTING ENGINEER

The C)PTE presents information based on the 5 Key Elements of Pen Testing; Information Gathering, Scanning, Enumeration, Exploitation and Reporting. The latest vulnerabilities will be discovered using these tried and true techniques. This course also enhances the business skills needed to identify protection opportunities, justify testing activities and optimize security controls to reduce risk associated to working with the internet.

C)SLO – CERTIFIED SECURITY LEADERSHIP OFFICER

The C)SLO course was designed to give management an essential understanding of current security issues, best practices, and technology. Because a security officer or manager understands the value of security, he or she is prepared to manage the security component of an information technology security projects. A C)SLO candidate can be seen as the bridge between the cyber security team and operations as well as business management.

C)SAP – CERTIFIED SECURITY AWARENESS PRINCIPLES

Certified Security Awareness Principles certification course is intended for anyone that uses a computer on the internet. Attendees will understand the security threats as well as the countermeasures associated with these attacks. Employees will learn that the weakest link in any security program is a poorly trained department. This course teaches general security awareness as well as how to develop a strong security culture within your company's community.

C)SWAE – CERTIFIED SECURE WEB APPLICATION ENGINEER

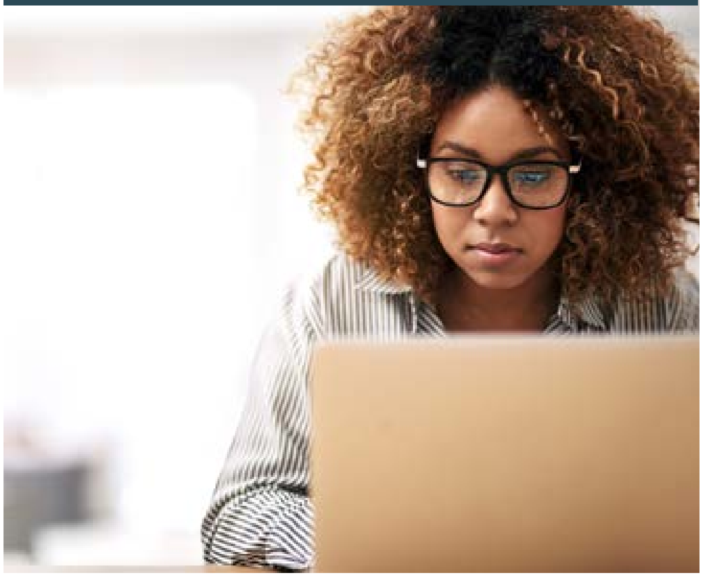
The Secure Web programmer knows how to identify, mitigate and defend against all attacks through designing and building systems that are resistant to failure. The secure web application developer knows how to develop web applications that aren't subject to common vulnerabilities, and how to test and validate that their applications are secure, reliable and resistant to attack. The vendor neutral Certified Secure Web Application Engineer certification provides the developer with a thorough and broad understanding of secure application concepts, principles and standard

C)VME – CERTIFIED VIRTUAL MACHINE ENGINEER

The Certified Virtual Machine Engineer course is designed for those who need to understand virtualization and the impacts it can have on an organization. This high impact course provides not only the foundational level of knowledge needed for an efficient datacenter. It also provides the most recent in virtualization and cloud technologies which gives the Certified Virtual Machine Engineer the knowledge and skills necessary to design and manage the datacenter effectively.

C)WSE – CERTIFIED WIRELESS SECURITY ENGINEER

The Certified Wireless Security Engineer is prepared to identify those risk that wireless networks present for a business and to create and implement a plan to mitigate those risk. The C)WSE course will give students real-world experience with solving security vulnerabilities in wireless networks.



CPTE AND CPTC BOOT CAMP

The “Ultimate” Penetration Testing & Ethical Hacking 7 Day Boot-Camp provides the latest and greatest penetration testing tools right in Mile2’s customary Cyber Range.

IS20 SECURITY CONTROLS

IS20 Controls certification course covers proven general controls and methodologies that are used to execute and analyze the Top Twenty Most Critical Security Controls. This course allows the security professional to see how to implement controls in their existing network(s) through highly effective and economical automation. For management, this training is the best way to distinguish how you’ll assess whether these security controls are effectively being administered or if they are falling short to industry standards.

SKILL BASED TRAINING - CISCO

CCNP – CISCO CERTIFIED NETWORK PROFESSIONAL

IS20 Controls certification course covers proven general controls and methodologies that are used to execute and analyze the Top Twenty Most Critical Security Controls. This course allows the security professional to see how to implement controls in their existing network(s) through highly effective and economical automation. For management, this training is the best way to distinguish how you’ll assess whether these security controls are effectively being administered or if they are falling short to industry standards.

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.