ABOUT US

The CCI is a robust, multi-agency effort to protect California from future cyber threats through training and research for government, academia, military, law enforcement, first responders and private entities. Our partners are the California National Guard and Cal Poly, San Luis Obispo.

The novel partnership among academia, industry and government offers immediate opportunities for local law enforcement, military personnel and even Cal Poly students as a part of its efforts to equip California to better protect its citizens.

As an extension of Cal Poly’s Cybersecurity Center, the CCI aims to educate the next generation cyber workforce and provide faculty and students with a new, hands-on research and learning environment. The CCI serves as an extended Learn by Doing space for Cal Poly students to explore new cyber technologies and train and test tactics side by side with law enforcement professionals and cyberforensics experts. The program helps shape California’s cyber standards and practices by offering an environment for cyberdefense innovation through advanced study and basic and applied research on emerging issues and technical challenges.

Learn more at cci.calpoly.edu.
<table>
<thead>
<tr>
<th>Course Roadmap</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection Seizure of Mobile Devices for Investigators Course</td>
<td>6</td>
</tr>
<tr>
<td>Ecosystem of Mobile Forensics Course</td>
<td>7</td>
</tr>
<tr>
<td>California Cyber Innovation Challenge</td>
<td>8</td>
</tr>
<tr>
<td>GenCyber Training Course</td>
<td>9</td>
</tr>
<tr>
<td>Strategies to Combat Human Trafficking</td>
<td>10</td>
</tr>
<tr>
<td>Intro to Vehicular Vulnerabilities Course</td>
<td>11</td>
</tr>
<tr>
<td>Advanced Vehicular Vulnerabilities Course</td>
<td>12</td>
</tr>
<tr>
<td>Cybersecurity Strategies for Decision Makers</td>
<td>13</td>
</tr>
<tr>
<td>Digital Forensics First Responders</td>
<td>14</td>
</tr>
<tr>
<td>Mobile Device Forensic Examiner Training</td>
<td>15</td>
</tr>
<tr>
<td>Bugbash Hackathon 2019</td>
<td>16</td>
</tr>
<tr>
<td>Certified Information Systems Security Officer</td>
<td>17</td>
</tr>
<tr>
<td>Certified Penetration Testing Engineer</td>
<td>18</td>
</tr>
<tr>
<td>Certified Penetration Testing Consultant</td>
<td>19</td>
</tr>
<tr>
<td>Certified Disaster Recovery Engineer</td>
<td>20</td>
</tr>
<tr>
<td>Certified Digital Forensics Examiner</td>
<td>21</td>
</tr>
<tr>
<td>Certified Network Forensics Examiner</td>
<td>22</td>
</tr>
<tr>
<td>Certified Secure Web Applications Engineer</td>
<td>23</td>
</tr>
<tr>
<td>Certified Incident Handling Engineer</td>
<td>24</td>
</tr>
<tr>
<td>Certified Vulnerability Assessor</td>
<td>25</td>
</tr>
<tr>
<td>Certified Security Leadership Officer</td>
<td>26</td>
</tr>
<tr>
<td>Certified Professional Ethical Hacker</td>
<td>27</td>
</tr>
<tr>
<td>Certified Information Systems Security Manager</td>
<td>28</td>
</tr>
<tr>
<td>Certified Information Systems Security Auditor</td>
<td>29</td>
</tr>
<tr>
<td>Certified Healthcare IS Security Practitioner</td>
<td>30</td>
</tr>
<tr>
<td>Certified Information Systems Risk Manager</td>
<td>31</td>
</tr>
<tr>
<td>Certified Security Principles +</td>
<td>32</td>
</tr>
<tr>
<td>Certified Virtualization Engineer</td>
<td>33</td>
</tr>
<tr>
<td>Certified Cloud Security Officer</td>
<td>34</td>
</tr>
<tr>
<td>Information Systems Certification and Accreditation Professional</td>
<td>35</td>
</tr>
<tr>
<td>Certified Security Awareness 1 &amp; 2</td>
<td>36</td>
</tr>
<tr>
<td>Information Systems 20 Controls</td>
<td>37</td>
</tr>
<tr>
<td>Certified Virtual Desktop Engineer</td>
<td>38</td>
</tr>
<tr>
<td>Certified IPv6 Security Specialist</td>
<td>39</td>
</tr>
<tr>
<td>Certified Virtualization Forensics Examiner</td>
<td>40</td>
</tr>
<tr>
<td>Certified Virtualization Principles</td>
<td>41</td>
</tr>
<tr>
<td>Certified PowerShell Hacker</td>
<td>42</td>
</tr>
<tr>
<td>Red Team vs Blue Team</td>
<td>43</td>
</tr>
<tr>
<td>Contact Us</td>
<td>44</td>
</tr>
<tr>
<td>Career Area</td>
<td>Fundamental</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Security Awareness</td>
<td>Certified Security Awareness 1</td>
</tr>
<tr>
<td>IS Management Leadership</td>
<td>Certified Security Principles Plus</td>
</tr>
<tr>
<td>Penetration Testing &amp; Hacking</td>
<td>Certified Vulnerability Assessor</td>
</tr>
<tr>
<td>Incident Handling</td>
<td>Certified Security Principles Plus</td>
</tr>
<tr>
<td>Forensics</td>
<td>Ecosystem of Mobile Forensics, Certified Security Principles Plus</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>Certified Security Principles Plus</td>
</tr>
<tr>
<td>Healthcare</td>
<td>Certified Security Principles Plus</td>
</tr>
<tr>
<td>Auditing</td>
<td>Certified Security Principles Plus</td>
</tr>
<tr>
<td>Cloud Security</td>
<td>Certified Virtualization Cloud Principles</td>
</tr>
<tr>
<td>Virtualization</td>
<td>Certified Virtualization Cloud Principles</td>
</tr>
<tr>
<td>IS Management Electives</td>
<td>Certified Information Systems Security Manager</td>
</tr>
<tr>
<td>Cyber Warfare</td>
<td>Red Team vs Blue Team</td>
</tr>
<tr>
<td>Career Area</td>
<td>Specialized</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Security Awareness</td>
<td>Cybersecurity Strategies for Decision Makers</td>
</tr>
<tr>
<td>IS Management Leadership</td>
<td>Information Systems 20 Controls, Cybersecurity</td>
</tr>
<tr>
<td></td>
<td>Strategies for Decision Makers</td>
</tr>
<tr>
<td>Penetration Testing &amp; Hacking</td>
<td>Certified Penetration Testing Engineer</td>
</tr>
<tr>
<td>Incident Handling</td>
<td>Certified Incident Handling Engineer</td>
</tr>
<tr>
<td>Forensics</td>
<td>Collection Seizure of Mobile Devices for</td>
</tr>
<tr>
<td></td>
<td>Investigators, Certified Virtual Forensics</td>
</tr>
<tr>
<td></td>
<td>Examiner</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>Certified Disaster Recovery Engineer</td>
</tr>
<tr>
<td>Healthcare</td>
<td>Certified Health Information Systems Security</td>
</tr>
<tr>
<td></td>
<td>Practitioner</td>
</tr>
<tr>
<td>Auditing</td>
<td></td>
</tr>
<tr>
<td>Application &amp; Secure Code</td>
<td>Certified Secure Web Application Engineer</td>
</tr>
<tr>
<td>Cloud Security</td>
<td>Certified Cloud Security Engineer</td>
</tr>
<tr>
<td>Virtualization</td>
<td>Certified Virtualization Systems Engineer</td>
</tr>
<tr>
<td>IS Management Electives</td>
<td>Information Systems Certification &amp; Accreditation Professional</td>
</tr>
<tr>
<td>Cyber Warfare</td>
<td></td>
</tr>
</tbody>
</table>
Best Practices - Collection Seizure of Mobile Devices for Investigators Course by The National Domestic Communications Assistance Center

Please join us for a free one-day training course designed to provide investigators and first responders with information related to the search and seizure of mobile devices encountered at a crime scene.

This training will help investigators and first responders identify mobile device digital evidence and associated media as well as take precautions to preserve the evidence. It also provides information related to the specialized and extensive analysis that may be conducted by forensic personnel in order to review data contained in the evidence. Finally, attendees will obtain a clear understanding of the required documentation and the potential for testimony related to the seizure of any digital evidence.

Topics Include:

- Crime Scene Investigation
- Evidence Collection/Preservation
- Mobile Device Identification
- Isolating and Protecting the Evidence
- Legal Perspectives of a Search
- Reporting and Testimony
- Practical Exercises
- Evidence Acquisition, Examination and Analysis

Location:
California Cybersecurity Institute, Camp San Luis Obispo*

Length:
TBD

2019 Course Dates:
TBD

*Camp San Luis Obispo requires a law enforcement ID or badge to enter the facilities.

For more information, contact us at cci@calpoly.edu or 805-756-1368

Learn more at cci.calpoly.edu/training.
ECOSYSTEM OF MOBILE FORENSICS

MSAB Instruction Lab: Cyber Forensics and Protection

MSAB is a global leader in mobile forensic technology. Its products are used by law enforcement, military, intelligence agencies and others in over 100 countries to investigate crime, gather intelligence and enforce laws. MSAB enables users to quickly extract and analyze mobile data and optimize the management of forensic systems. This course is designed as an introduction to the ecosystem of mobile forensics and an overview of the MSAB solution for law enforcement. Eligible students should have basic computer and mobile phone skills.

Attendees will receive learning opportunities, including:

• An immersive training exercise to learn how to extract, analyze and manage evidence from a mobile device.

• A tour of the Central Coast Forensics Lab and discussions.

• An update on CalECPA, the Electronic Communications Privacy Act.

• A demonstration of the MSAB Kiosk — designed to make it fast and easy for non-experts to do their own extractions, view the results and get actionable intelligence quickly.

• Learning by Doing with the California Cybersecurity Institute’s hands-on, immersive training program.

Cost:
The price to attend this training course is free to government, education and law enforcement.

Instructor:
TBD

Length:
TBD

2019 Course Dates:
TBD

* Government, military and law enforcement may stay on base at Camp San Luis Obispo at reduced rates compared to hotel venues in the surrounding area. Lunch will be provided.

For more information, contact us at cci@calpoly.edu or 805-756-1368
Learn more at cci.calpoly.edu/training.
CALIFORNIA CYBER INNOVATION CHALLENGE

Date: TBD  
Location: TBD

The California Cybersecurity Institute (CCI) of San Luis Obispo, California is excited to announce the launch of the 2019 California Cyber Innovation Challenge (CCIC). The CCIC is a statewide high school cybersecurity competition designed to introduce more students to the field of cybersecurity. It provides unique opportunities for businesses to proactively address their cybersecurity skills gaps while also expanding access to technology career pathways for all Californians. This year’s challenge will take place in a medical office scenario at the California Cybersecurity Institute and will focus on both the ethical and technical issues of a ransomware attack on a medical facility.

The CCIC begins with the spring 2019 regional qualifying rounds from which, along with an “at-large” selection process, 20 teams will be drawn to participate in the state championship round, June 23-25 at the CCI. This year’s competition highlights the challenges of securing healthcare information and devices due to the growing importance of protecting the progress of medical technology against impending cyberthreats.

Who can participate?

The CCIC is open to all California high schools. Last year’s event featured an immersive forensics training scenario with 16 cars, 64 high school students and team of professionals from government, industry and education. Learn more about this year’s event at [youtu.be/2x0GaW-2sCY](https://youtu.be/2x0GaW-2sCY).

For more information, contact us at cci@calpoly.edu or 805-756-1368. Learn more at cci.calpoly.edu/training.
GENCYBER

TRAINING COURSES

Cal Poly Faculty-Led Cybersecurity Training for High School and Middle School Teachers

When?
Training offered TBD
Practicum offered TBD and TBD. (Choose 3 consecutive days within the given time frame.)

Where?
Training is located in San Luis Obispo at the California Cybersecurity Institute and Cal Poly campus.

What’s Included?
Only basic computer literacy is required. Morning courses include learning about web security, network security, secret communication and forensics. In the afternoon, hands-on labs are held focusing on topics in python programming, password hacking, social engineering and forensics analysis.

Breakfast and lunch are included.

A stipend of up to $2,000 is offered to attending teachers.

Continuing education credits available (six CEUs).

Post-training support including faculty and student on-site support in the attending teacher’s school; startup resources for cybersecurity high school clubs including Cal Poly student support, startup funding, activities, curriculum, Cal Poly facility tours, etc.

For more information, contact us at cci@calpoly.edu or 805-756-1368.
The CCI is launching its own training, titled “Strategies to Combat Human Trafficking.” This course will teach attendees about the following topics:

- **IMPACT** of mobile forensics on human trafficking cases as well as the CalECPA’s impact on how law enforcement, prosecutors and decision-makers fight modern-day slavery.

- **REAL-LIFE** human trafficking through immersive training exercises that represent actual scenes, including brothels or illicit massage businesses laced with cyber evidence on varying electronic devices.

- **EMOTIONAL** engagement and skills required to process the difficult emotions that arise in response to human trafficking crimes.

- **BASIC** mobile forensics concepts that drastically change the way evidence is collected and retrieved. In addition, attendees will review evidence resembling current cases under prosecution.

- **ACTIONS** for attendees to implement in their community, state, country and world.
VULNERABILITIES

Intro Course: Are your vehicles safe from hackers?

Organizations spend a great deal of time, money and resources protecting their physical infrastructures from cyberbreaches but neglect the vehicles their teams use in the field. This one-day course introduces individuals with basic computer skills to the security vulnerabilities accessible to hackers in any vehicle, any time and anywhere. This hands-on, immersive training program teaches participants to discover where security vulnerabilities may exist through a Learn by Doing experience. Attendees also gain an understanding of how to identify and enumerate common field equipment used by modern police forces.

In this course, students will gain insight into the following:

• Penetration testing of wiring, antennas, infotainment systems and radios.

• Software that operates your vehicles (most vehicles today have millions of lines of code).

• The security risk of mobile phones that enter your car.

• Accessible passwords to hackers in your vehicle.

• How to tell if your vehicle has been compromised.

• Digital attacks on drivers in your community.

Prerequisites:
This entry-level course is designed for both technical personnel and decision-makers who require an introduction to vehicular vulnerabilities.

Length:
All Day

Course Dates:
Monday, March 18, 2019
TBD
TBD

For more information, contact us at cci@calpoly.edu or 805-756-1368

Learn more at cci.calpoly.edu/training.

* Government, military and law enforcement may stay on base at Camp San Luis Obispo at reduced rates compared to hotel venues in the surrounding area. Lunch will be provided.
Advanced Course: Are your vehicles safe from hackers?

Organizations spend a great deal of time, money and resources protecting their physical infrastructures from cyberbreaches but neglect the vehicles their teams use in the field. This four-day, comprehensive training course introduces individuals to the security vulnerabilities accessible to hackers in any vehicle, any time and anywhere. Course attendees will run live-testing on fleet vehicles in our secure testing bays. This hands-on, immersive training program teaches participants to discover where security vulnerabilities may exist through a Learn by Doing experience. Attendees also gain an advanced understanding of how to identify and enumerate common field equipment used by modern police forces.

In this course, students will gain insight into the following:

- Penetration testing of wiring, antennas, infotainment systems and radios.

- Software that operates your vehicles (most vehicles today have millions of lines of code).

- The security risk of mobile phones that enter your car.

- Passwords accessible to hackers in your vehicle.

- How to tell if your vehicle has been compromised.

- Digital attacks on drivers in your community.

Prerequisites:
This advanced course is designed for those already working in the cybersecurity field or those with a technology background who want to learn more about vehicular vulnerabilities.

Length:
All Day

Course Dates:
Tuesday, March 19 - Friday, March 22, 2019
TBD
TBD

For more information, contact us at cci@calpoly.edu or 805-756-1368

Learn more at cci.calpoly.edu/training.

* Government, military and law enforcement may stay on base at Camp San Luis Obispo at reduced rates compared to hotel venues in the surrounding area. Lunch will be provided.
With the explosion of cybersecurity threats, business leaders need affordable and practical solutions.

Nearly 50 million Californians have had their records breached during the past four years, according to the Attorney General in the 2016 California Data Breach Report. Most of the exploited vulnerabilities that enabled these breaches were compromised more than a year after the solution to patch those vulnerabilities became publicly available.

Through a combination of lecture and hands-on exercises, this class aims to instruct students in these topics:

**CYBERSECURITY BASICS**
Learn cybersecurity fundamentals, including vocabulary, common threats and mitigation approaches.

**THE EVOLVING THREAT**
Understand the range of cybersecurity threats, both current and emerging.

**CYBERSECURITY BEST PRACTICES**
Observe how the best organizations deal with the evolving threat.

**THE RIGHT TOOLS AND TACTICS**
Use hands-on exercises to choose the right tools and actions that can help shield your organization from malicious content, based on your budget.

For more information, contact us at cci@calpoly.edu or 805-756-1368
Learn more at cci.calpoly.edu/training.

Registration opens for this class TBD. To reserve a spot, please contact cci@calpoly.edu.
This eight-hour course is designed as an introduction for first responders (officers, investigators and supervisors) who have basic computer skills and need to learn the basics of identifying, preserving and collecting digital evidence.

This class will provide training on the standards of preserving digital evidence for court, introduction to computer and component identification, legal issues related to the search and seizure of digital evidence, an overview of the phases of digital forensics, data authentication, and the preservation and collection of digital evidence. The course includes hands-on training in the collection of digital evidence, including storage media and evidence authentication.

This course is POST certified– Presenter 1348, Cal Poly’s Cybersecurity Institute.

Course: 22317, Cyber Security & High Tech Threats.

This course will be taught on the following dates:

• TBD

NOTE: The cost of this course may be covered by funds from the Homeland Security Grant Program. Funds may cover the cost of registration, travel, lodging, per-diem, backfill or overtime.

For more information, contact us at cci@calpoly.edu or 805-756-1368
Learn more at cci.calpoly.edu/training.
This course is designed to provide the foundational knowledge and hands-on skills needed to become a mobile device forensics examiner. This vendor-neutral, immersive training course will teach students how to access critical data stored on mobile devices and understand how popular forensic software extracts data from these locations. The class will focus on the forensics process, identifying where data resides and how to extract that data manually. Therefore, this course will benefit forensic examiners, detectives, investigators, information security professionals and law enforcement officers who desire to specialize in mobile device forensics. Lawyers, paralegals, IT auditors and IT professionals involved in civil proceedings and the electronic discovery process will also benefit from taking this course. The training is calculated to prepare students who are seeking the Mobile Device Forensics Examiner (MDFE) certification — one of only two industry leading vendor-neutral mobile device forensics certifications.

To ensure your success in this course, you should be able to perform basic Microsoft Windows operations and be familiar with basic forensics concepts. This course was written as an introduction to mobile device forensics and is beneficial at all levels, from beginners to advanced.

For more information, contact us at cci@calpoly.edu or 805-756-1368
Learn more at cci.calpoly.edu/training.
BUG BASH

HACKATHON 2019

Join the California Cybersecurity Institute, Bugcrowd,

Date: TBD
Time: TBD
Location: California Cybersecurity Institute
          Camp San Luis Obispo
          10 Sonoma Avenue, Building 631
          San Luis Obispo, CA 93405

For more information, contact us at cci@calpoly.edu or 805-756-1368.
Learn more at cci.calpoly.edu/training.
NOTE: The cost of this course may be covered by funds from the homeland security grant program. Funds may cover the cost of registration, travel, lodging, per-diem, backfill or overtime.

(CSTI Course Number: CP-M2CISSO1)
Certified Penetration Testing Engineer

The vendor-neutral Certified Penetration Testing Engineer, or C)PTE, certification course is built firmly upon proven, hands-on penetration testing methodologies utilized by our international group of penetration testing consultants.

The C)PTE presents information based on the five key elements of penetration testing: information gathering, scanning, enumeration, exploitation and reporting. The latest vulnerabilities are 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 in order to reduce the risk associated with using the internet. Students will use the latest tools such as Saint, Metasploit through Kali Linux and Microsoft PowerShell.

Mile2 goes far beyond simply teaching you to “hack.” The C)PTE was developed around principles and behaviors used to combat malicious hackers and focuses on professional penetration testing rather than “ethical hacking.”

In addition to utilizing ethical hacking methodologies, students will learn penetration testing methodologies using advanced persistent threat techniques. Course participants will go through a complete penetration test from A to Z. They will also learn to create their own assessment report and apply their knowledge immediately in the workforce. With this in mind, the C)PTE certification course is a complete upgrade from the EC-Council CEH. The C)PTE exam is taken anytime and anywhere online through Mile2’s MACS system, which makes the exam experience easy and mobile. Students do not need to take the C)PTE course to attempt the C)PTE exam.

NOTE: The cost of this course may be covered by funds from the Homeland Security Grant Program. Funds may cover the cost of registration, travel, lodging, per-diem, backfill or overtime.

(CSTI Course Number: CP-M2CPTE1)
Certified Penetration Testing Consultant

The vendor-neutral Certified Penetration Testing Consultant course is designed for IT security professionals and network administrators who are interested in conducting penetration tests against large network infrastructures similar to large corporate networks, service providers and telecommunication companies. Instead of focusing on operating system-level penetration testing, this course covers techniques on how to attack and prevent underlying network infrastructure and protocols.

The training starts with basic packet capturing and analyzing by using both commercial and open-source tools. From there, the student continues with Layer2 attack vectors, Layer3 based attacks (including both IPv4 and IPv6 stacks) and routing protocol attacks (i.e., OSPF, BGP, etc.). Then, the student jumps to service provider-level attacks related to commonly used MPLS, how to use relays and pivots, and VPN attacks (including IPSEC protocol suite and SSL attacks).

Finally, the class covers NIDS/NIPS evasion and implementation techniques. This course has in-depth lab exercises after each module. Students may spend over 16 hours performing labs that emulate a real-world penetration testing model. Students will use a myriad of traditional and cutting-edge penetration testing tools (including GUI, command line, Windows and Linux) as they make their way through Mile2’s time-tested methodology.

Students will be prepared to take the C)PTC exam.

NOTE: The cost of this course may be covered by funds from the Homeland Security Grant Program. Funds may cover the cost of registration, travel, lodging, per-diem, backfill or overtime.

(CSTI Course Number: CP-M2CPTC1)
Certified Disaster Recovery Engineer

When a business is hit by a natural disaster, cybercrime or any other disruptive tragedy, how should the organization react? What if the network infrastructure is taken down? Will the business be able to continue operations? How much will it cost if the business is down during repairs?

The answers are found in the vendor-neutral Certified Disaster Recovery Engineer certification course. Disaster recovery and business continuity planning is the process of working professionally with a business to prepare processes, policies and procedures for application in the event of a disruption. The goal is to keep a business’ critical operations running which, today, relies heavily on its IT infrastructure.

The comprehensive Certified Disaster Recovery Engineer course goes beyond traditional BCP training — which prepares students for industry certification in business continuity planning — to present 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 developed by leading risk management professionals.

Students will be prepared to take the CDRE exam.

NOTE: The cost of this course may be covered by funds from the Homeland Security Grant Program. Funds may cover the cost of registration, travel, lodging, per-diem, backfill or overtime.

(CSTI Course Number: CP-M2CDRE1)
In the vendor-neutral Certified Digital Forensics Examiner or CDFE certification course, designed to train cybercrime and fraud investigators, students are taught electronic discovery and advanced investigation techniques. This course is essential to anyone encountering digital evidence while conducting an investigation.

Mile2’s Certified Digital Forensics Examiner training teaches the methodology for conducting a computer forensic examination. Students will learn to use forensically sound investigative techniques in order to evaluate the scene, collect and document all relevant information, interview appropriate personnel, maintain chain of custody and write a findings report. 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.

Upon completion, Certified Digital Forensics Examiner students will be able to establish industry acceptable digital forensics standards with current best practices and policies. Students will also be prepared to competently take the CDFE exam.

NOTE: The cost of this course may be covered by funds from the Homeland Security Grant Program. Funds may cover the cost of registration, travel, lodging, per-diem, backfill or overtime.

(CSTI Course Number: CP-M2CDFE1)
Certified Network Forensics Examiner

The Certified Network Forensics Examiner, or CJNFE, vendor-neutral certification was developed for a U.S. classified government agency. The CJNFE takes digital and network forensic skills to the next level by navigating through more than 20 modules of network forensic topics.

The CJNFE provides practical experience through lab exercises that simulate real-world scenarios that cover investigation and recovery of data in a network, physical interception, traffic acquisition, analysis, wireless attacks and Snort.

The course focuses on the centralization and investigation of logging systems as well as network devices.

Students will be prepared to take the CJNFE exam.

NOTE: The cost of this course may be covered by funds from the Homeland Security Grant Program. Funds may cover the cost of registration, travel, lodging, per-diem, backfill or overtime.

(CSTI Course Number: CP-M2CNFE1)
Organizations and governments fall victim to internet-based attacks every day. In many cases, cyberattacks could be thwarted, but hackers, organized criminal gangs and foreign agents are able to exploit weaknesses in web applications.

The secure web programmer knows how to identify, mitigate and defend against all attacks through designing and building systems resistant to failure. The secure web application developer knows how to develop web applications that are not subject to common vulnerabilities as well as how to test their applications and validate that they 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 standards. The student will be able to design, develop and test web applications providing reliable web services that meet functional business requirements and satisfy compliance and assurance needs.

The Certified Secure Web Application Engineer course is delivered by high-level Open Web Application Security Project (OWASP) experts. Students can expect to obtain real-world security knowledge that enables them to recognize vulnerabilities, exploit system weaknesses and help safeguard against application threats.

Students will be prepared to take the C)SWAE exam.

NOTE: The cost of this course may be covered by funds from the Homeland Security Grant Program. Funds may cover the cost of registration, travel, lodging, per-diem, backfill or overtime.

(CSTI Course Number: CP-M2CSWAE1)
Certified Incident Handling Engineer

The Certified Incident Handling Engineer, or C)IHE, vendor-neutral certification is designed to help incident handlers, system administrators and general security engineers understand how to plan, create and utilize their systems in order to prevent, detect and respond to attacks.

In this in-depth training, students will learn step-by-step approaches used by hackers globally, the latest attack vectors and how to safeguard against them, incident handling procedures (including developing the process from start to finish and establishing your incident handling team), strategies for each type of attack, recovering from attacks and much more.

Furthermore, students will enjoy numerous hands-on laboratory exercises focusing on topics such as reconnaissance, vulnerability assessments using Nessus, network sniffing, web application manipulation, malware and Netcat. Students will also be exposed to additional scenarios for both Windows and Linux systems.

BENEFITS OF THE C)IHE COURSE

Graduates of the Mile2 Certified Incident Handling Engineer training obtain real-world security knowledge that enables them to recognize vulnerabilities, exploit system weaknesses and help safeguard against threats. This course covers the same objectives as the SANS Security 504 training and prepares students for the GCIH and C)IHE certifications.

Students will be prepared to take the C)IHE exam.

NOTE: The cost of this course may be covered by funds from the Homeland Security Grant Program. Funds may cover the cost of registration, travel, lodging, per-diem, backfill or overtime.

(CSTI Course Number: CP-M2CIHE1)
The vendor-neutral Certified Vulnerability Assessor, C)VA, certification course helps students understand the importance of vulnerability assessments by providing intricate knowledge and skills in the vulnerability assessment arena. The C)VA course focuses on vulnerability assessments and provides fundamental knowledge of general VA tools as well as popular exploits familiar to an IT engineer. Students will receive fundamental information such as the importance of a vulnerability assessment and how it can help an engineer prevent serious break-ins to your organization. After the C)VA course, students will be well versed in basic malware and viruses and how they can infiltrate an organization’s network. Students will also learn how to assess a company’s security posture and perform a basic vulnerability test to help secure the organization’s networking infrastructure.

Students will be prepared to take the C)VA exam.

NOTE: The cost of this course may be covered by funds from the Homeland Security Grant Program. Funds may cover the cost of registration, travel, lodging, per-diem, backfill or overtime.

(CSTI Course Number: CP-M2CVA1)
Certified Security Leadership Officer

The vendor-neutral Certified Security Leadership Officer, or C)SLO, certification course was designed for middle- and upper-level managers as well as all engineers who seek to increase their knowledge in the security arena. The C)SLO course was intended to give management an essential understanding of current security issues, best practices and technology. When a security officer or manager understands the value of security, he/she is prepared to manage the security component of information technology security projects.

A C)SLO candidate can be seen as the bridge between the cybersecurity team and operations as well as business management. Essential topics covered in this management track are extremely detailed and include the following: network fundamentals and applications, hardware architecture, information assurance, foundations, computer security policies, contingency and continuity planning, business impact analysis, incident handling, architect approaches to defense, cyberattacks, vulnerability assessment and management, security policies, web security, offensive and defensive information warfare, culminating with management practicum.

Students will be prepared to take the C)SLO exam.

NOTE: The cost of this course may be covered by funds from the Homeland Security Grant Program. Funds may cover the cost of registration, travel, lodging, per-diem, backfill or overtime.

(CSTI Course Number: CP-M2CSLO1)
Certified Professional Ethical Hacker

The vendor-neutral Certified Professional Ethical Hacker, or C)PEH, certification course is the foundation to Mile2’s line of penetration testing courses. The C)PEH certification training enables students to understand the importance of vulnerability assessments by providing industry knowledge and skills. In doing so, the C)PEH student is able to understand how malware and destructive viruses function. In addition, the C)PEH course helps students learn how to implement counterattacks and preventative measures when it comes to a network hack. The course provides in-depth labs that focus on both open-source and commercial-based tools with industry best practices. These hands-on labs emulate real-world hacking scenarios and equip the candidate to assess a company’s security posture, help implement controls to better secure a company’s network infrastructure, combat against hackers and/or viruses, etc.

Students will be prepared to take the C)PEH exam.

NOTE: The cost of this course may be covered by funds from the Homeland Security Grant Program. Funds may cover the cost of registration, travel, lodging, per-diem, backfill or overtime.

(CSTI Course Number: CP-M2CPEH1)
Certified Information Systems Security Manager

The Certified Information Systems Security Manager, or C)ISSM, certification course trains and certifies managers of information systems who have experience with information, security risk, security, compliance, and incident management of systems. If you are lacking experience in one or two of these areas, we recommend taking our C)ISSO or Certified Information Systems Security Officer certification course first. Since this is a specialized course, we expect our students to be familiar with these subjects before coming to the course.

The C)ISSM certification course is designed to train and certify an information systems professional to comply with a high standard of excellence in the following areas:

- Information security governance
- Information risk management and compliance
- Information security program development and management
- Information security incident management

While we provide thorough training in these four critical areas of information systems security management, most who take the C)ISSM course have professional experience in all four of these areas. A gap of experience in some of these fields can be bridged by achieving our C)ISSO or Certified Information Systems Security Officer certification.

Students will be prepared to take the C)ISSM exam.

NOTE: The cost of this course may be covered by funds from the Homeland Security Grant Program. Funds may cover the cost of registration, travel, lodging, per-diem, backfill or overtime.

(CSTI Course Number: CP-M2CISSM1)
Many organizations require an Information System Auditor’s expert knowledge when it comes to identifying critical issues and providing effective auditing solutions. The knowledge and course content provided in the vendor-neutral Certified Information Systems Security Auditor, or C)ISSA, certification course will not only cover ISACA’s exam, but will also provide a measurable certification that demonstrates proficiency in the IS auditing field.

The C)ISSA certification course covers the skills and knowledge to assess vulnerabilities, report on compliance and implement controls for private and public enterprises. Students will receive in-depth knowledge in topics that pertain to the following: IS audit, control and assurance. This course is designed for IT professionals in the following job roles: IT consultants, auditors, managers, security policy writers, privacy officers, information security officers, network administrators, security device administrators, and security engineers.

Students will be prepared to take the C)ISSA exam.

NOTE: The cost of this course may be covered by funds from the Homeland Security Grant Program. Funds may cover the cost of registration, travel, lodging, per-diem, backfill or overtime.

(CSTI Course Number: CP-M2CISSA1)
Certified Healthcare IS Security Practitioner

The vendor-neutral Certified Healthcare Information Systems Security Practitioner certification course covers the skills and knowledge needed to implement the best IT healthcare practices as well as regulatory compliance and standards in the healthcare industry.

Because of growing industry regulations and privacy requirements in the healthcare industry, Mile2 developed the Certified Healthcare Information Systems Security Practitioner, or C)HISSP, certification. The C)HISSPs have become vital in managing and protecting healthcare data. They are tasked with protecting patient information by implementing, managing and assessing proper IT controls for patient health information integrity.

Students will be prepared to take the C)HISSP exam.

NOTE: The cost of this course may be covered by funds from the Homeland Security Grant Program. Funds may cover the cost of registration, travel, lodging, per-diem, backfill or overtime.

(CSTI Course Number: CP-M2CHISSP1)
Certified Information Systems Risk Manager

The vendor-neutral Certified Information Systems Risk Manager certification is designed for IT and IS professionals involved with risk identification, risk assessment, risk evaluation, risk response, risk monitoring, IS control design and implementation and IS control monitoring and maintenance.

The Certified Information Systems Risk Manager training will elevate the professionals’ understanding in identifying and evaluating entity-specific risks as well as risks associated with enterprise business objectives by equipping the practitioner to design, implement, monitor and maintain risk-based, efficient and effective IS controls.

The Certified Information Systems Risk Manager covers five critical subjects: risk identification, assessment and evaluation, risk response, risk monitoring, IS control design and implementation and IS control monitoring and maintenance.

Students will be prepared to take the C)ISRM exam.

NOTE: The cost of this course may be covered by funds from the Homeland Security Grant Program. Funds may cover the cost of registration, travel, lodging, per-diem, backfill or overtime.

(CSTI Course Number: CP-M2CISRM1)
Certified Information Systems Risk Manager

Mile2’s Certified Security Principles + course provides the skills necessary to apply and implement technical knowledge of security concepts in today’s security environment.

Students will gain an in-depth knowledge of systems security, access control, network infrastructure, assessments and audits, cryptography and organizational security across all vendor products. These skills have become increasingly important due to additional safeguards such as intrusion detection systems, physical access control and multi-factor authentication becoming standard methods of protection. Students are given real-world scenarios to reinforce the material covered and will learn how to apply the concepts to their daily operations.

Students will be prepared to take the C)SP+ exam.

NOTE: The cost of this course may be covered by funds from the Homeland Security Grant Program. Funds may cover the cost of registration, travel, lodging, per-diem, backfill or overtime.

(CSTI Course Number: CP-M2CSP+)

Length:
Five days

Prerequisites:
• Basic Windows user skills
• A fundamental understanding of computer and networking concepts

Audience:
• IT professionals with networking and administrative skills in Windows-based transmission control protocol/internet protocol (TCP/IP) networks and familiarity with other operating systems (e.g., Linux).

*Certification exam is included with the cost of the course.
Certified Virtualization Engineer

This fast-paced, high-energy, hands-on course provides not only the foundation needed for a top performing software defined data center, but also provides the latest in virtualization and cloud technologies that gives engineers and administrators the knowledge and skills they need to design and manage the data center for tomorrow’s needs.

This course will cover topics including design, installation, configuration, best practices, performance monitoring, and everything in between.

Students will be prepared to take the C)VE exam.

NOTE: The cost of this course may be covered by funds from the Homeland Security Grant Program. Funds may cover the cost of registration, travel, lodging, per-diem, backfill or overtime.

(CSTI Course Number: CP-M2CVE1)
Cloud use now dominates the work environment and is continuing to increase. Current statistics show 79 percent of business workloads are using cloud technology, 41 percent public cloud and 38 percent private cloud, according to a Rightscale 2017 State of the Cloud Report. Cybersecurity has evolved, bringing a new set of standards and issues that must be addressed in order for organizations to securely use cloud technology. Understand the issues and complexity of running a cloud strategy through a hands-on, in-depth cloud course that will prepare students for practical application and provide information to pass the Certified Cloud Security Officer certification exam.

This course focuses on the implementation of cloud security, auditing and compliance issues. It also focuses on the core knowledge areas tailored around the six domains in the C)CSO examination. This is managed by a unique delivery of the C)CSO knowledge domains along with the hands-on labs that allow for a deeper understanding of the data set at every layer of the cloud stack.

This relevant course will introduce many topics on technology used in the cloud, from implementing a VMware vRealize cloud and using a new, key management solution to various vendors, including VMware, Amazon AWS, and Microsoft Azure.

Students will be prepared to take the C)CSO exam.

NOTE: The cost of this course may be covered by funds from the Homeland Security Grant Program. Funds may cover the cost of registration, travel, lodging, per-diem, backfill or overtime.

(CSTI Course Number: CP-M2CCSO1)
Information Systems Certification and Accreditation Professional

Mile2’s vendor-neutral Information Systems Certification and Accreditation Professional certification training quantifies the process of certifying, reviewing and accrediting an information system by IT professionals.

This certification is designed to provide, through its contents and referenced resources, a complete guide to establishing a certified and accredited information system in any organization.

This course was created as a standard to measure the set of skills that specific members of an organization are required to have for the practice of certifying, reviewing and accrediting the security of information systems. Specifically, this training was designed for the individuals responsible for creating and implementing the processes used to evaluate risk and institute security baselines and requirements. These critical decisions are essential in making sure that the security of the information systems outweighs the potential risks to an organization from any internal or external threats.

Students will be prepared to take the ISCAP exam.

NOTE: The cost of this course may be covered by funds from the Homeland Security Grant Program. Funds may cover the cost of registration, travel, lodging, per-diem, backfill or overtime.

(CSTI Course Number: CP-M2ISCAP1)
Certified Security Awareness 1 & 2

The Mile2 vendor-neutral Certified Security Awareness 1 certification course is intended for anyone that uses the internet on a computer. Attendees will understand the security threats as well as the countermeasures associated with these attacks. Also, 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 a company’s community. The social engineering portion of the class is designed to teach the participants the skills used by social engineers to facilitate the extraction of information from an organization using technical and non-technical methods.

Computer fraud, black-hat hacking and cyber-terrorists – these phrases describe an innovative generation of criminals that use over-the-wire technology to attack, steal from and terrorize us. However, the best tool in their arsenal is not new. It is only used by the most experienced, dangerous and boldest hackers.

The Mile2 Certified Security Awareness 1 program has innovative training for students on how attacks are performed, the skills necessary to perform an attack, how to train people to identify an attack and, most importantly, how to train internal targets, so that the training is effective and lasts.

Upon completion, the Certified Security Awareness 1 & 2 candidate will not only be able to competently take the CSA1 & CSA2 exams but will also understand basic cybersecurity knowledge to keep companies’ IP and IT infrastructure safe.

NOTE: The cost of this course may be covered by funds from the Homeland Security Grant Program. Funds may cover the cost of registration, travel, lodging, per-diem, backfill or overtime.

(CSTI Course Number: CP-M2CSS1)
Mile2’s Information Systems 20 Controls course covers the most important security controls and their methodologies as outlined by the U.S. Department of Defense and other major players in the cybersecurity sector who understand how attacks work and how to prevent them. Students are trained to improve security in networks by implementing the top 20 security controls. When it comes to security controls, prevention is ideal but detection is a must. The top 20 controls do both.

Experts began to compile the top 20 security controls list (Consensus Audit Guidelines) in 2008 after many U.S. defense industry companies suffered a severe loss of data due to various cyberattacks. As these attacks continued to rise, many federal cyberattacks and defense experts were compelled to collaborate with each other. Their understanding and knowledge of these malicious attack techniques were being used against both government and corporate industries alike. This collaboration resulted in the top 20 list of known security controls needed to ensure the integrity of organizational assets. The CAG project was led by John Gilligan, who served as chief information officer for both the U.S. Air Force and the U.S. Department of Energy. In a statement, Gilligan said that, “It was obvious that organizations should implement these controls.” He also said, “If you know that attacks are being carried out, you have a responsibility to prioritize your security investments to stop those attacks.”

Our instructors have real-world experience and will show you the value of what you are learning in proprietary case studies. Students will be prepared to take the IS20 certification exam after this course. As a result of this course and exam, attentive students are prepared to lead future security projects because they will have a plan for exactly what needs to be done to secure a network.
Certified Virtual Desktop Engineer

This course introduces virtualization professionals to VMware Horizon View 7 Suite. VMware professionals will learn to install and configure Horizon View and its many components as well as how to design a basic EUC environment utilizing the products. After the completion of this course, the delegate is expected to be above VCP-DT level.

Students will be prepared to take the CVVDE Exam.

**Length:**
Five days

**Prerequisites:**
- 2+ years experience with VMware vSphere

**Audience:**
- This course targets VDI professionals that are new to VMware Horizon Suite, but are already proficient with vSphere 5.x or 6.x based virtual infrastructure and the configuration of DRS, HA and other Cluster related features. Also, provides performance insights for experienced users.
Certified IPv6 Security Specialist

Are you ready for the coming storm? According to our team of security experts, the implementation of IPv6 will likely produce another Wild West across the internet.

The ease at which a hacker can steal your data on an IPv6 environment is plain scary. Internet protocols are not written with security in mind; they focus on functionality. If we are not aware of the pitfalls of IPv6, we will see the financial loss due to hacking skyrocket, like the old days before we properly secured IPv4.

Students will be prepared to take the C)Ipv6 Exam.

Length:
Two days

Prerequisites:
• Understanding of existing IP protocols such as ICMP, TCP, UDP and others
• Knowledge of existing switching technologies such as Cisco or Juniper

Audience:
• Network Administrators
• Network Engineers
• DataCenter Engineers
• Security Engineers
• CTO’s
• CIO’s
• IT Managers
• IT Professionals
This course takes two enormously challenging areas facing IT security professionals today—incidence response and virtualization—and attempts to meld these together.

Forensics is at the heart of incidence response; therefore, this training will focus on how to gather evidence relating to an incident—the what, when, where, who and why of an incident—within today’s common virtual environments. Additionally, the course will take a deep dive into the virtual infrastructure, to contrast the various virtual entities against their physical counterparts. This will allow for a clear demonstration of the forensically-relevant differences between the virtual and physical environments. The course uses a lab-centric, scenario-based approach to demonstrate how to forensically examine relevant components of a virtual infrastructure for specific use cases.

Students will be prepared to take the CVFE Exam.

**Length:**
Five days

**Prerequisites:**
- Must have a digital or computer forensics certification or equivalent knowledge

**Audience:**
- Virtual Infrastructure Specialists
- Architects
- Engineers
- Administrators
- Forensic Investigators
Certified Virtualization Principles

Most companies are already virtual and many are looking into furthering virtualization into the cloud and implementing desktop virtualization. However, many companies continue to look at the competing virtualization platforms in the market wondering if they have made the right choice.

This hands-on course is designed for IT and sales professionals to dive into the key components of virtualization and compare the key players in the market space. The course will answer the following questions: what features does each platform have, which platforms actually work, and how can I decide which one is right for me based on ROI/TCO?

Students will be prepared to take the CJVP Exam.
CALIFORNIA CYBERSECURITY INSTITUTE

Certified PowerShell Hacker

This course is an intense few days covering the keys to hacking with PowerShell. We know that most companies have an Active Directory infrastructure that manages authentication and authorization to most devices and objects within the organization. Many use PowerShell to speed up and simplify management, which only makes sense. Did you know that a large percentage of hacks over the last year included PowerShell based attacks? Well they did, which is why we spend 4 days learning how to hack like the pros using nothing but what is already available to us in Windows or now in open source code on Mac and Linux! The course is based on real world implementations of a windows infrastructure along with real world penetration testing techniques. You will leave with a real strong skill set to help test your windows environment like never before. An attendee will also walk away with a strong skill set on how to help prevent these attacks from happening in the first place!

Here are just a few things you will take away from this course:

- Detailed lab manual
- VMs for performing labs on your own
- New ideas on testing your own AD infrastructure
- Attacks you can use immediately
- How to secure against PowerShell attacks

Students will be prepared to take the C)PSH Exam.

Length:
Four days

Prerequisites:
- General Understanding of Pen Testing
- General Understanding of Active Directory
- General Understanding of scripting and programming

Audience:
- Penetration Testers
- Microsoft Administrators
- Security Administrators
- Active Directory Administrators
- Anyone looking to learn more about security
Red Team vs Blue Team

The Red Team vs. Blue Team is a scenario-based, hands-on lab experience. The goal is to put together skills learned during Mile2 courses and apply them in this environment. It consists of two days with four scenarios ranging from easy to intermediate to advanced problem sets.

As a Blue Team individual, you will be given approximately 45 minutes to review the target systems within your scenario and potentially patch vulnerabilities. NOTE: You cannot disable any services on the system, but you can patch them. You are authorized to change the default credentials for the user “playerone,” however, that password will be given to the Mile2 range monitor. NOTE: If credentials are changed after the start of the Red Team portion, there will be a timeout period up to 15 minutes.

As a Red Team individual, you will be given three hours to attempt to exploit other students’ machines. The intent for the Red Team is to gain access to other systems in the network and place their name or team name in the flag.txt file in the root/administrator directory.

Upon completion, graduates of the Mile2 Red Team vs. Blue Team scenario-based events allow for individuals to piece together a team that will attack based on skillset. This allows for managers to assess their current penetration testing and incident response teams to ensure they are able to attack vulnerabilities and defend against attacks.

Length:
Two days

Prerequisites:
• 12 months minimum of experience in networking technologies
• Sound knowledge of TCP/IP
• Knowledge of Microsoft packages
• Basic knowledge of Linux is essential

Red Team vs Blue Team Scenarios:
• Scenario 1 – Kali vs. Proximo and Gracchus
• Scenario 2 – Kali vs. Priscus and Verus
• Scenario 3 – Kali vs. Maximus and Quintus
• Scenario 4 – Kali vs. Tetraites and Commodus
CONTACT US

Martin Minnich
Program Director
California Cybersecurity Institute
Phone: 540-903-4004
Email: mminnich@calpoly.edu

Rob Swift
Division Manager
Central Coast Cyber Forensic Lab
Phone: 805-464-7808
Email: rqswift@co.slo.ca.us

Christine Reed
Administrative Support Coordinator
California Cybersecurity Institute
Phone: 805-756-1368
Email: cci@calpoly.edu

Jimmy Baker
Interim Director for Industry Outreach
California Cybersecurity Institute
Phone: 805-756-2948
Email: jbaker30@calpoly.edu