NCRIC 2020
Cybersecurity
Training Catalog

Contact
For more information, please contact Jimmy Baker

805.756.2948  jbaker30@calpoly.edu  www.calpoly.cci.edu/training
It is no longer a question of “IF” another cyber breach will happen in California, but “WHEN.” “California needs a comprehensive statewide strategy to uplift and upskill our workers to ensure technological advancements in AI, blockchain, big data, are creating jobs . . .,” stated Governor Newsom in his 2019 State of the State Address. The common factor in all cybercrime is the access of data. California is now in a transition with the convergence of machine data as well as traditional information technology all under the auspice of the Internet of Things. The level of sophistication and cyber attacks are on the rise in California, and so must the training for the existing and future California workforce. As the world’s fifth-largest economy, the State of California faces a myriad of challenges:

- 49,031 reported cybercrimes in 2018 by FBI
- 72,123 unfilled cyber positions according to cyberseek.org
- Multiple nation-states actively targeting the economy and citizens

Located on a secure military base halfway between San Francisco and Los Angeles, the California Cybersecurity Institute (CCI) offers NCRIC and their partners a variety of cybersecurity training courses. The cybersecurity certifications offered by the CCI are recognized by organizations such as:

- **ACCREDITED** by the NSA CNSS 4011-4016
- **MAPPED** to NIST / Homeland Security NICCS’s Cyber Security Workforce Framework
- **APPROVED** on the FBI Cyber Security Certification Requirement list (Tier 1-3)

Each course offers accommodates a class size of 20 students. Seating is limited. The following table provides an overview of the following courses offered to NCRIC and their partners.

<table>
<thead>
<tr>
<th>COURSE TITLE</th>
<th>COST PER PERSON FOR TRAINING AND CERTIFICATION EXAM</th>
<th>NUMBER OF DAYS</th>
<th>LOCATION</th>
<th>2020 CALENDAR DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certified Digital Forensics Examiner</td>
<td>$2,465</td>
<td>4</td>
<td>CI</td>
<td>February 17-20</td>
</tr>
<tr>
<td>Certified Information Systems Security Officer</td>
<td>$2,465</td>
<td>5</td>
<td>CI</td>
<td>March 9-13</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>September 14 - 18</td>
</tr>
<tr>
<td>Certified Professional Ethical Hacker</td>
<td>$2,465</td>
<td>4</td>
<td>CI</td>
<td>April 28 - May 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>November 17 -20</td>
</tr>
<tr>
<td>Certified Disaster Recovery Engineer</td>
<td>$1,972</td>
<td>4</td>
<td>CI</td>
<td>June 2-5</td>
</tr>
<tr>
<td>Certified Incident Handling Engineer</td>
<td>$2,465</td>
<td>4</td>
<td>CI</td>
<td>September 22-25</td>
</tr>
<tr>
<td>Red vs. Blue Team Training</td>
<td>$1,927</td>
<td>4</td>
<td>CCID</td>
<td>December 8-11</td>
</tr>
</tbody>
</table>
FREQUENTLY ASKED QUESTIONS

Cybersecurity Training Courses

WHY CHOOSE THE CALIFORNIA CYBERSECURITY INSTITUTE (CCI) FOR TRAINING?

✓ In partnership with CalPoly, the CCI curriculum is designed specifically to train California law enforcement, public safety, and government professionals in cybersecurity and forensics.
✓ CCI course prices come in several thousand dollars lower than comparable courses from other providers.
✓ Each CCI course price includes a Mile2 certification exam attempt and retest if needed.
✓ The in-person course sessions in this catalog are reserved for NCRIC members, so you will meet and learn alongside your regional peers.

HOW DO I PAY?

Attendees may pay online or via check made out to California Cybersecurity Institute. Please send your check to Cal Poly, Information Technology Services, 1 Grand Ave, San Luis Obispo, CA 93407, attention: James Baker CCI. If your organization receives the State Homeland Security Grant Program (SHSGP) funds, request a tracking number from CalOES. You will need your home agency to pay course fees. However, since CCI courses are already approved by the California Specialized Training Institute (CSTI), attendance, lodging, and per diem will be fully reimbursed for SHSGP recipients. Please contact Cal Poly’s James Baker at if you require an invoice at 805.756.2948 or NCRIC’s Alison Yakabe at 415.470.3628 for funding questions.

WHAT ARE THE LODGING OPTIONS?

Located at historic Camp San Luis Obispo, lodging is located on base within close proximity to the CCI. The government rate for overnight accommodations averages between $30-$70 per night. For other options, the City of San Luis Obispo is six miles away. Breakfast and lunch provided each day with course attendees. For more information on lodging and directions, please contact Cal Poly’s Christine Reed at 805.756.1368.
When
February 17-20, 2020
8:00AM-6:00PM

Where
Cal Poly's California Cybersecurity Institute at Camp
San Luis Obispo, Bldg. 631
San Luis Obispo, CA

Presenters
California Cybersecurity Institute, Mile 2, and Stronger

Cost
$2,465.00  / Cost of exam included in course price

Attendance
This instruction is designed for Active Peace Officers, Firefighters, State Investigators, Federal Agents, Military Investigative personnel, or other government employees working within the public safety / homeland security community. Attendees must be currently employed by a government agency.

Course Description
The Certified Digital Forensics Examiner (CDFE) 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. Mile2’s Certified Digital Forensics Examiner (CDFE) 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 prerequisite for this four-day training course is a minimum of 1 year with computers.
**Post & CSTI Certification**

CSTI Course Number: CP-M2CDFE1  
POST Course Number: 23419  

The CCI can accommodate and create custom POST-certified training to meet NCRIC’s current and future cyber training needs. Organizations receiving existing State Homeland Security Grant Program (SHSGP) funding can use those funds to reimburse.

**Registration**

Register Online at:  
https://www.eventbrite.com/e/85631180165  
Cal Poly will also accept checks. Please contact jbaker30@calpoly.edu for check instructions.

**Questions**

**Alison Yakabe**  
Lead Cyber Intelligence Analyst  
ayakabe@ncric.ca.gov  
415-470-3628

**Jimmy Baker**  
Account Coordinator  
Cal Poly California  
Cybersecurity Institute  
jbaker30@calpoly.edu  
805-756-2948

**Course Objectives**  
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 C)DFE exam. Certification exam is included with the cost of the course. Course attendees will work through the following modules:  
- **Module 0** - Introduction  
- **Module 2** - Incident Handling  
- **Module 3** - Computer Forensic Investigative Theory  
- **Module 4** - Computer Forensic Investigative Process  
- **Module 5** - Digital Acquisition  
- **Module 6** - Disks and Storages  
- **Module 7** - Digital Evidence Protocols  
- **Module 8** - Digital Evidence Presentation  
- **Module 9** – Computer Forensic Laboratory Protocols  
- **Module 10** - Computer Forensic Processing Techniques  
- **Module 11** - Specialized Artifact Recovery  
- **Module 12** - e-Discovery and ESI  
- **Module 13** - Mobile Device Forensics  
- **Module 14** - Digital Forensics Reporting

**Target Audience / Discipline**

This instruction is designed for Active Peace Officers, Firefighters, State Investigators, Federal Agents, Military Investigative personnel, or other government employees working within the public safety / homeland security community. Attendees must be currently employed by a government agency operating in the NCRIC’s Area of Responsibility (AOR). This instruction is designed for law enforcement professionals, attorneys, information systems managers, and security officers.

**About the CCI**

The CCI teaches Californians to protect California through cybercrime forensics and statewide tactical response training. The program helps shape California’s cyber standards and practices by offering an environment for cyber defense innovation through advanced study and basic and applied research on emerging issues and technical challenges. Learn more about the CCI and our training courses at www.cci.calpoly.edu
When

March 9-13, 2020  September 14-18, 2020 9:00AM-5:00PM

Where

Cal Poly’s California Cybersecurity Institute at Camp San Luis Obispo, Bldg. 631 San Luis Obispo, CA

Presenters

California Cybersecurity Institute, Mile 2, and Stronger

Cost

$2,465.00  
*Cost of exam included in course price

Attendance

This instruction is designed for technical professionals such as security officers, information systems managers, risk managers, auditors, information systems owners, information systems managers. Attendees must be currently employed by a government agency.

Course Description

The Certified Information Systems Security Officer certification training was a direct initiative of the DND – Department of National Defense of Canada in cooperation with the DOD – Department of Defense of the United States. The CISSO addresses the broad range of industry best practices, knowledge, and skills expected of a security manager/officer. The candidate will learn in-depth theory pertaining to the practical implementation of core security concepts, practices, monitoring, and compliance in the full panorama of IS management. Through the use of a risk-based approach, the CISSO is able to implement and maintain cost-effective security controls that are closely aligned with both business and industry standards. Whether you’re responsible for the management of a Cyber Security team, a Security Officer, an IT auditor or a Business Analyst, the CISSO certification course is an ideal way to increase your knowledge, expertise, and skill.

The prerequisites for this five-day training course are:

• 1 Year experience in at least 2 modules or
• 1 year in IS Management
**Course Objectives**

Upon completion, Certified Information Systems Security Officer students will not only be able to establish industry acceptable Cyber Security & IS management standards with current best practices but also be prepared to competently take the CISSO exam. The cost for this exam is included in your registration fees.

**Target Audience / Discipline**

This instruction is designed for Active Peace Officers, Firefighters, State Investigators, Federal Agents, Military Investigative personnel, or other government employees working within the public safety / homeland security community. Attendees must be currently employed by a government agency operating in the NCRIC’s Area of Responsibility (AOR). This instruction is designed for technical professionals such as security officers, information systems managers, risk managers, auditors, information systems owners, information systems managers.

**About the CCI**

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. Learn more about the CCI and our training courses at [www.cci.calpoly.edu](http://www.cci.calpoly.edu)

---

**Post & CSTI Certification**

CSTI Course Number: CP-M2CISSO1  
POST Course Number: 30558

The CCI can accommodate and create custom POST-certified training to meet NCRIC’s current and future cyber training needs. Organizations receiving existing State Homeland Security Grant Program (SHSGP) funding can use those funds to reimburse.

**Registration**

Register Online at:  
[https://www.eventbrite.com/e/85636482023](https://www.eventbrite.com/e/85636482023)

Cal Poly will also accept checks. Please contact jbaker30@calpoly.edu for check instructions.

**Questions**

Alison Yakabe  
Lead Cyber Intelligence Analyst  
ayakabe@ncric.ca.gov  
415-470-3628

Jimmy Baker  
Account Coordinator  
Cal Poly California Cybersecurity Institute  
jbaker30@calpoly.edu  
805-756-2948
PROFESSIONAL ETHICAL HACKER

Cybersecurity Training Course

When
April 28-May 1, 2020
November 17-20, 2020
8:00AM-6:00PM

Where
Cal Poly’s California Cybersecurity Institute at Camp
San Luis Obispo, Bldg. 631
San Luis Obispo, CA

Presenters
California Cybersecurity Institute, Mile 2, and Stronger

Cost
$2,465.00
*Cost of exam included in course price

Attendance
This instruction is designed for technical professionals such as security officers, information systems managers, risk managers, auditors, information systems owners, information systems managers. Attendees must be currently employed by a government agency.

Course Description
The Certified Professional Ethical Hacker (CPEH) vendor-neutral certification course is the foundational training to mile2’s line of penetration testing courses. 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. The CPEH 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 your company’s security posture, help implement controls to better secure your company’s network infrastructure and how to combat against hackers and viruses.

The prerequisites for this four-day training course are:
• 1 year of IT security experience
• 1 year of Networking Experience
Course Objectives

Upon completion, the Certified Professional Ethical Hacker candidate will be able to competently take the CPEH exam. Course attendees will work through the following modules:

- Module 1 – Introduction to Ethical Hacking
- Module 2 – Linux Fundamentals
- Module 3 – Protocols
- Module 4 – Cryptography
- Module 5 – Password Cracking
- Module 6 – Malware
- Module 7 – Security Devices
- Module 8 – Information Gathering - Passive Reconnaissance
- Module 9 – Social Engineering
- Module 10 – Active Reconnaissance
- Module 11 – Vulnerability Assessment
- Module 12 – Network Attacks
- Module 13 – Hacking Servers
- Module 14 – Hacking Web Technologies
- Module 15 – Hacking Wireless Technologies
- Module 16 – Maintaining Access and Covering

Target Audience / Discipline

This instruction is designed for Active Peace Officers, Firefighters, State Investigators, Federal Agents, Military Investigative personnel, or other government employees working within the public safety / homeland security community. Attendees must be currently employed by a government agency operating in the NCRIC’s Area of Responsibility (AOR). This instruction is designed for information system owners, security officers, ethical hackers, information owners, penetration testers, system owners and managers, and cybersecurity engineers.

About the CCI

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. Learn more about the CCI and our training courses at www.cci.calpoly.edu
DISASTER RECOVERY ENGINEER

Cybersecurity Training Course

When
June 2-5, 2020
9:00AM-5:00PM

Where
Cal Poly’s California Cybersecurity Institute at Camp San Luis Obispo, Bldg. 631
San Luis Obispo, CA

Presenters
California Cybersecurity Institute, Mile 2, and Stronger

Cost
$1,972.00
*Cost of exam included in course price

Attendance
This instruction is designed for technical professionals such as security officers, information systems managers, risk managers, auditors, information systems owners, information systems managers. Attendees must be currently employed by a government agency.

Course Description
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 answer is found in the vendor-neutral Certified Disaster Recovery Engineer (CDRE) certification course. Disaster recovery and business continuity planning is the process of having a professional work with a business to prepare processes, policies, and procedures to follow 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 (CDRE) 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.
The prerequisites for this four-day training course is a minimum of 1 year of Information Systems or IS Management

**Course Objectives**
Upon completion, Certified Disaster Recovery Engineer students will be able to establish industry acceptable DR & BCP standards with current best practices and policies. Students will also be prepared to competently take the CDRE exam. Course attendees will work through the following modules:

- Welcome to Disaster Recovery Training
- Business Impact Analysis
- Risk Analysis
- Design & Development Phase (BCP Strategies)
- IT Recovery Strategies
- Testing and Exercise
- Maintenance and Updating
- Pandemics
- Case Studies and Templates

**Target Audience / Discipline**
This instruction is designed for Active Peace Officers, Firefighters, State Investigators, Federal Agents, Military Investigative personnel, or other government employees working within the public safety / homeland security community. Attendees must be currently employed by a government agency operating in the NCRIC’s Area of Responsibility (AOR). This instruction is designed for information system owners, security officers, ethical hackers, information owners, penetration testers, system owners and managers, and cybersecurity engineers.

**About the CCI**
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. Learn more about the CCI and our training courses at [www.cci.calpoly.edu](http://www.cci.calpoly.edu)
INCIDENT HANDLING ENGINEER

Cybersecurity Training Course

When
September 22-25, 2020
8:00AM-6:00PM

Where
Cal Poly’s California Cybersecurity Institute at Camp San Luis Obispo, Bldg. 631
San Luis Obispo, CA

Presenters
California Cybersecurity Institute, Mile 2, and Stronger

Cost
$2,465.00  / Cost of exam included in course price

Attendance
This instruction is designed for Active Peace Officers, Firefighters, State Investigators, Federal Agents, Military Investigative personnel, or other government employees working within the public safety / homeland security community. Attendees must be currently employed by a government agency.

Course Description
The Certified Incident Handling Engineer (CIHE) 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.

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 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.
Graduates of the mile2 Certified Incident Handling Engineer (CIHE) 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 CIHE certifications. The prerequisites for this four-day training course are:

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

Course Objectives

Upon completion of the Certified Incident Handling Engineer course, students will be able to confidently undertake the CIHE certification examination (recommended). The cost for this exam is included in your registration fees. Students will enjoy an in-depth course that is continuously updated to maintain and incorporate the ever changing security world. This course offers up-to-date proprietary laboratories that have been researched and developed by leading security professionals from around the world.

Target Audience / Discipline

This instruction is designed for Active Peace Officers, Firefighters, State Investigators, Federal Agents, Military Investigative personnel, or other government employees working within the public safety / homeland security community. Attendees must be currently employed by a government agency operating in the NCRIC’s Area of Responsibility (AOR).

About the CCI

The CCI teaches Californians to protect California through cybercrime forensics and statewide tactical response training. The program helps shape California’s cyber standards and practices by offering an environment for cyber defense innovation through advanced study and basic and applied research on emerging issues and technical challenges. Learn more about the CCI and our training courses at [www.cci.calpoly.edu](http://www.cci.calpoly.edu)
RED VS. BLUE TEAM
Cybersecurity Training Course

**When**

December 8-11, 2020
9:00AM-5:00PM

**Where**

Cal Poly's California Cybersecurity Institute at Camp San Luis Obispo, Bldg. 631
San Luis Obispo, CA

**Presenters**

California Cybersecurity Institute, Mile 2, and Stronger

**Cost**

$1,972.00 / Cost of exam included in course price

**Attendance**

This instruction is designed for Active Peace Officers, Firefighters, State Investigators, Federal Agents, Military Investigative personnel, or other government employees working within the public safety / homeland security community. Attendees must be currently employed by a government agency.

**Course Description**

The Ultimate Red vs. Blue Team Course is built on intense hands-on sessions that emulate real-world cyberattack and defense scenarios (Four in total). The Ultimate Red vs. Blue Team Course was developed around principles and behaviors used to combat malicious hackers who use advanced persistent threat techniques. Attendees will expect to learn not only some of the latest hacking attacks but also blue team counter responsive controls.

The prerequisites for this four-day training course are an understanding of the following:

- Networking
- Scanning and Vulnerabilities
- Networking Technologies
- TCP/IP
- Microsoft packages
- Basic Knowledge of Linux is essential
**Course Objectives**

The Red vs. Blue Team is a scenario-based, hands-on lab experience. The goal is to put together items learned in Mile2’s cyber range based on both a Windows and Linux infrastructure. The four-day course consists of two days of hands-on labs using Kali Linux and Microsoft PowerShell and two days (four scenarios) ranging from intermediate to advanced problem sets.

Graduates of the Red vs. Blue Team scenario-based events will:
1. Become more versed with tools and applications, such as Metasploit, Kali Linux, and Microsoft PowerShell.
2. Allow individuals to piece together a team that will focus on attack-based skillsets.
3. Be able to assess their current penetration testing and incident response teams.
4. Have a strong understanding as to how to help prevent and defend against cyber-attacks.

**Target Audience / Discipline**

This instruction is designed for Active Peace Officers, Firefighters, State Investigators, Federal Agents, Military Investigative personnel, or other government employees working within the public safety / homeland security community. Attendees must be currently employed by a government agency operating in the NCRIC’s Area of Responsibility (AOR). This instruction is designed for anyone looking to learn about security, penetration testers, Microsoft administrators, security administrators, and cybersecurity engineers.

**About the CCI**

The CCI teaches Californians to protect California through cybercrime forensics and statewide tactical response training. The program helps shape California’s cyber standards and practices by offering an environment for cyber defense innovation through advanced study and basic and applied research on emerging issues and technical challenges. Learn more about the CCI and our training courses at [www.cci.calpoly.edu](http://www.cci.calpoly.edu)
CAL POLY
Cal Poly is a nationally ranked, four-year, comprehensive public university located in San Luis Obispo, halfway between San Francisco and Los Angeles on California’s Central Coast. Known for its Learn by Doing approach, small class sizes and open access to expert faculty, Cal Poly is a distinctive learning community whose 21,000 academically motivated students enjoy an unrivaled, hands-on educational experience that prepares them to lead successful personal and professional lives. Cal Poly is consistently ranked a top university for academics, value and graduate salaries.
www.calpoly.edu

CCI
The California Cybersecurity Institute teaches Californians to protect California through cybercrime forensics and statewide tactical response training. The program helps shape California’s cyber standards and practices by offering an environment for cyber defense innovation through advanced study and basic and applied research on emerging issues and technical challenges.

The CCI is a public-private partnership bringing together the best subject matter experts to address the “cyber” needs of the State of California. Under this effort, we employ the California Polytechnic State University pedagogy “Learn by Doing” to create live-immersive scenarios that are real, current, and relevant. This training provides an accurate context of particular challenges as well as tactical exercises that ensures retention and proper deployment of solutions.
www.cci.calpoly.edu/training

MILE 2
Mile 2, Stronger, and the CCI have a standing public-private relationship and provide cyber training to government, academia, military, and law enforcement. Mile2® develops and delivers proprietary vendor-neutral professional certifications for the cybersecurity industry. Mile2® administers cybersecurity certification exams through the MACS (Mile2 Assessment and Certification System) system via Mile2.com. Mile2® cybersecurity training certification courses teach the fundamental and advanced principles of cybersecurity. Training courses follow a certification track that leads to advanced hands-on skills training for penetration testing, disaster recovery, incident handling, and network forensics. Mile2® also provides Information Assurance training certification that meets military, government, private sector, and institutional specifications.
www.mile2.com

STRONGER
Mile 2, Stronger, and the CCI have a standing public-private relationship and provide cyber training to government, academia, military, and law enforcement. At Stronger International, we provide expert consulting, onsite, live-remote, and cloud-based virtual training to organizations and individuals who want to enhance their IT security and increase their overall IT knowledge. Our consultants and trainers work with clients of all sizes in the public and private sector to help identify, prevent, and remediate against all forms of cybercrime. We also teach basic skills enhancement and compliance training to increase your organization’s knowledge asset value. When it comes to protecting your company, there’s no such thing as safe enough. In a world where damaging cybercrime is committed every two seconds, it’s not a question of if you will be attacked, only when.
www.stronger.tech

805.756.2948  jbaker30@calpoly.edu  www.calpoly.cci.edu/training