EC-Council

CYBER SECURITY PROGRAMS

Over 1,200
Highly Qualified
Certified Instructors

145+
Countries

700+
Locations

Over 4,200
Classes Annually
in Cyber Security

www.eccouncil.org

Table of Contents

Tracks

Certifications

Academic Programs

Who We Are

The EC-Council group is made up of several entities that all help serve the same goal which is to create a better, safer cyber world through awareness and education. Our entities include International Council of eCommerce Consultants (EC-Council), iClass, EC-Council University, EC-Council Global Services (EGS), and EC-Council Conferences and Events.

EC-Council creates content (course materials and exams) and certification delivered through our channel of authorized training centers which consists of over 700 partners representing over 2,000 physical locations in more than 145 countries across the globe. We are the owner and developer of the world-famous Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI), EC-Council Certified Security Analyst (ECSA), and License Penetration Tester (LPT)(Master) programs.

Our certification programs are recognized worldwide and have received endorsements from various government agencies, including the United States Federal Government (via the Montgomery GI Bill), the National Security Agency (NSA), and the Committee on National Security Systems (CNSS). All these reputed organizations have Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI), EC-Council Disaster Recovery Professional (EDRP), EC-Council Certified Security Analyst (ECSA), Advanced Penetration Testing (APT) and Licensed Penetration Tester (LPT)(Master) programs for meeting the 4011, 4012, 4013A, 4014, 4015 and 4016 training standards for information security professionals. EC-Council has received accreditation from the American National Standards Institute (ANSI) for our coveted CEH, CCISO, CHFI, and CND programs. We have so far certified over 2,20,000 professionals in various e-business and cybersecurity skills.

iClass is EC-Council's direct certification training program. iClass delivers EC-Council certification courses through various training methodologies: instructor-led at client facilities, synchronous delivery through live, online instructor-led, and asynchronously through our streaming video platform. iClass course videos can also be loaded onto a mobile device, such as an iPad, and shipped to a client location.

> *"Our lives are dedicated to the mitigation and remediation of the cyber plague that is menacing the world today"*
>
> ***Jay Bavisi***
> ***President & CEO***
> ***EC-Council***

EC-Council University is a DEAC accredited university offering programs such as Bachelor of Science in Cyber Security, Master of Science in Cyber Security, and Graduate Certificate Program. EC-Council Global Services (EGS) is dedicated to helping organizations understand and manage their cyber-security risk posture effectively. EGS specializes in helping clients make informed business decisions to protect their organizations. EGS has over 20 dedicated cyber security practice areas informed by the best cyber security practitioners, each of whom have dedicated their lives to defending organizations from cyber-attacks.

EC-Council's Conference and Events Group is responsible for planning, organizing, and running conferences throughout the globe. TakeDownCon and Hacker Halted are IT security conferences that bring world renowned speakers together for keynotes, panels, debates, and breakout sessions. Conferences have been run in Dallas, Las Vegas, St. Louis, Huntsville, Maryland, Connecticut, Myrtle Beach, Miami, Atlanta, Iceland, Hong Kong, Egypt, Singapore, Mumbai, Dubai, Bahrain, London, Abu Dhabi and Kuala Lumpur.

Other events include CISO Summits, Global CISO Forums, and Executive Cocktail Receptions where EC-Council brings speakers and content to executive level IT Security Professionals.

The Global Cyberlympics competition is a "capture the flag" type competition with approximately 1,000 global participants. EC-Council brings the hackers together online for preliminary elimination rounds and then brings the top two teams (6-8 players per team) from each region to compete in the final head-to-head competition.

Pentagon trains workers to hack Defense computers

March 10, 2010 | By Larry Shaughnessy, CNN Pentagon Producer

The Pentagon is training people to hack into its own computer networks.

"To beat a hacker, you need to think like one," said Jay Bavisi, co-founder and president of the International Council of Electronic Commerce Consultants, or EC-Council. His company was chosen by the Pentagon to oversee training of Department of Defense employees who work in computer security-related jobs and certify them when the training is complete.

The idea behind the Pentagon's training is that thinking like a hacker can beat a hacker.

The Department of Defense does not consider this hacking.

"DoD personnel are not learning to hack. They are learning to defend the network against hackers," said spokesman Lt. Col. Eric Butterbaugh.

"EC-Council - Trusted worldwide for its end-to-end enterprise cyber security solutions for human capital development"

EC-Council at a Glance

EC-Council Group is a multidisciplinary institution of global Information Security professional services.

EC-Council Group is a dedicated Information Security organization that aims at creating knowledge, facilitating innovation, executing research, implementing development, and nurturing subject matter experts in order to provide their unique skills and niche expertise in cybersecurity.

Some of the finest organizations around the world such as the US Army, US Navy, DoD, the FBI, Microsoft, IBM, and the United Nations have trusted EC-Council to develop and advance their security infrastructure.

ICECC
International Council of E-Commerce Consultants
EC-Council Group

ECC
EC-Council Training & Certification
Division of Professional Workforce Development

EGS
EC-Council Global Services
Division of Corporate Consulting & Advisory Services

ECCU
EC-Council University
Division of Academic Education

EGE
EC-Council Global Events
Division of Conferences, Forums, Summits, Workshops & Industry Awards

ECF
EC-Council Foundation
Non-Profit Organization for Cyber Security Awareness Increase.

15+	40+	145+	350+	700+	3000+
YEARS EXPERIENCE	TRAINING & CERTIFICATION PROGRAMS	COUNTRIES	SUBJECT MATTER EXPERTS	TRAINING PARTNERS WORLDWIDE	TOOLS & TECHNOLOGIES

220,000+ CERTIFIED MEMBERS

Your Learning Options

Instructor-led Training

EC-Council has a large network of Accredited Training Centers (ATC) spread across 145 countries. Each center has a certified trainer to deliver the entire EC-Council program from a training facility in your city.

Online Training

iLearn online training is a distance learning program designed for those who cannot attend a live course. The program is for the people who have a very busy schedule and want to learn at their own pace through self-study. This modality is also available from our enterprise teams.

Mobile Learning

Our world class content is also available on a mobile device, allowing our students to learn on the go. This program is designed for those who are cannot attend a live course, but are keen to improve their cyber security skills. This modality is also available from our enterprise teams.

Computer-based Training

For people who work in secure facilities with limited or no access to the internet, we offer computer-based training (CBT) options delivered in an HD DVD format. The DVDs are an upgrade/add-on to the base iLearn program and are not sold independently. This modality is also available from our enterprise teams.

Hands-on Experience with the EC-Council Cyber Range (iLabs)

EC-Council iLabs allows students to dynamically access a host of virtual machines preconfigured with vulnerabilities, exploits, tools, and scripts from anywhere. Our simplistic web portal enables the student to launch an entire range of target machines and access them remotely with one simple click. It is the most cost-effective, easy to use, live range lab solution available. *Most of our courses are equipped with iLabs, but iLabs can be purchased independently as well.*

Customized Learning

Love a course we offer, but want it customized? No problem! EC-Council has a dedicated team to cater to your needs. We have access to the largest pool of EC-Council certified instructors via our ATC channel. Let us know where and when you want the training delivered, and we will arrange for an instructor and all that's required for a course to be taught at a location of your choice. Contact our accredited training partners for a custom solution.

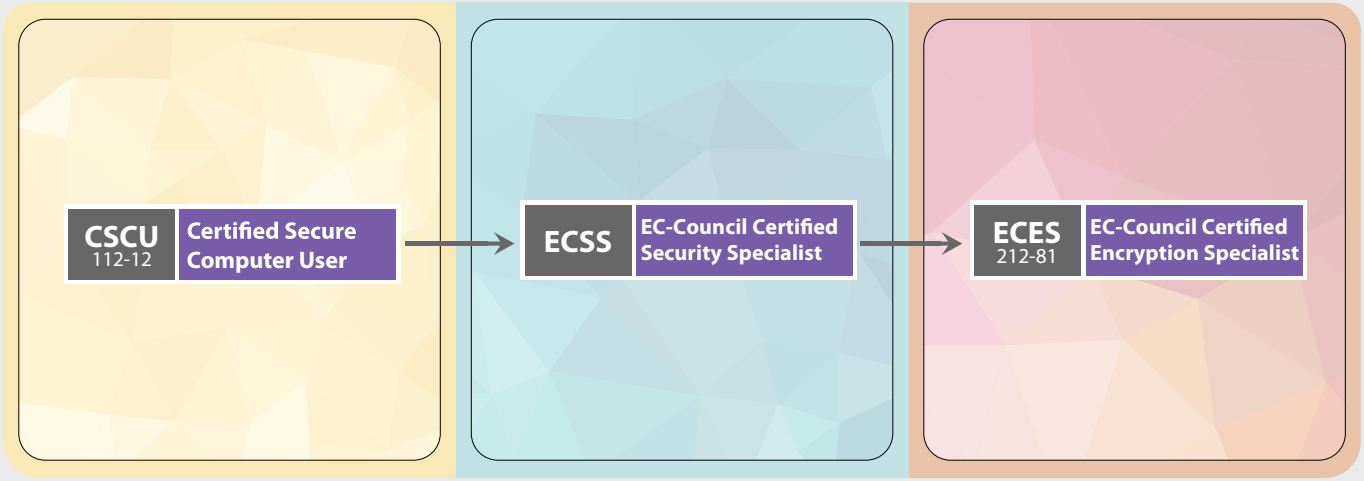
EC-Council client-site training includes official courseware, certification exam (ECC-Exam or VUE), iLabs, online labs (wherever available), and our test-pass guarantee.

Live Online Training

If self-study or self-paced learning does not fit into your personal learning style, we offer you our live online model, iWeek.

With iWeek, an instructor will teach you live online while you are seated in the comfort of your home. This training method gives you the freedom to get trained from a location of your choice. Individuals who choose this delivery method consistently attribute their choice to the preference of having a live instructor available for which questions can be asked and answered. We offer early-bird rates, group rates, and get even private courses delivered anytime.

Foundation Track



Target Audience

This track focuses on todays' computer users who use the internet extensively to work, study and play.

What will You Learn

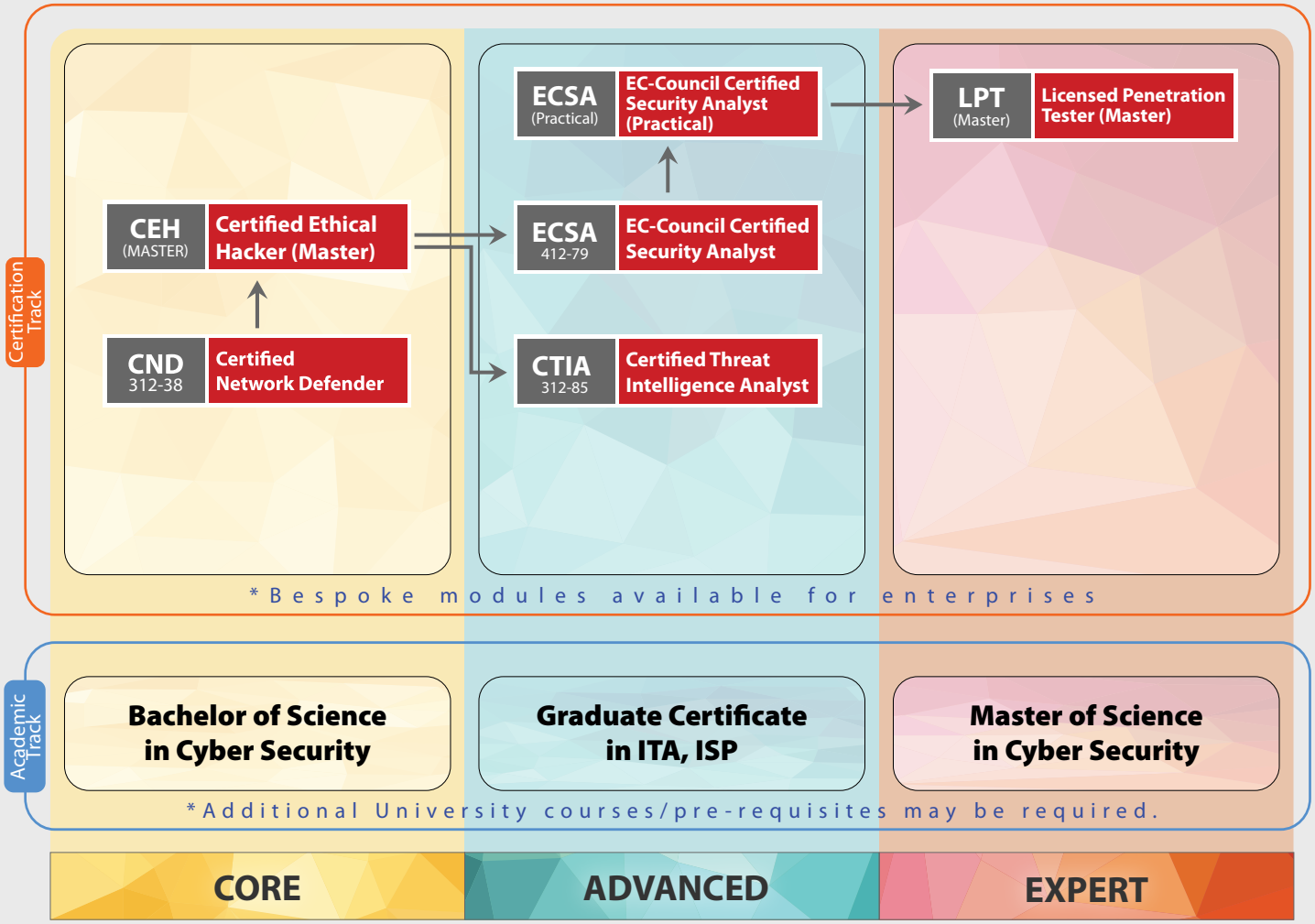
- Cloud Security
- Password Security
- Social Engineering Countermeasures
- Mitigating Identity Theft
- Email Security
- Safe Browsing
- Data Protection
- Physical Security
- Mobile Device Security
- Encryption
- Social Network Security
- Antiviruses Protection
- Disaster Recovery
- Internet Security
- Credit Card Security
- Monitoring Kids Online
- Wireless & Home Network Security
- OS Security

Our Certified Foundation Professionals are Employed at:

Caritas, Grant Thornton, IBM, PALADION, Poly technique Sousse, Unique Academy, Ministry of Defence, NTT DATA, ICT Group of Institutions, happiest minds, ingenia, icddr,b, DCB Bank, vodafone, UNP, RELIANCE, core4 factory, Nestlé, • • •

All credentials can be attained individually. Please refer to cert.eccouncil.org for the eligibility criteria.

Vulnerability Assessment & Penetration Testing (VAPT)



Job Roles

- Information Assurance (IA) Security Officer
- Information Security Analyst/Administrator
- Information Security Manager/Specialist
- Information Systems Security Engineer/Manager
- Security Analyst
- Information Security Officers
- Information Security Auditors
- Risk/Vulnerability Analyst

Our Certified VAPT Professionals are Employed at:

Cisco, EY, Microsoft, accenture, Infosys, amazon, AIG, hp, Bank of America, Booz | Allen | Hamilton, Capgemini, Deloitte., NEC, bugcrowd, TATA, lastline, axiata, U.S. Army, Marriott, Hero

This track maps to NICE's Specialty Areas:

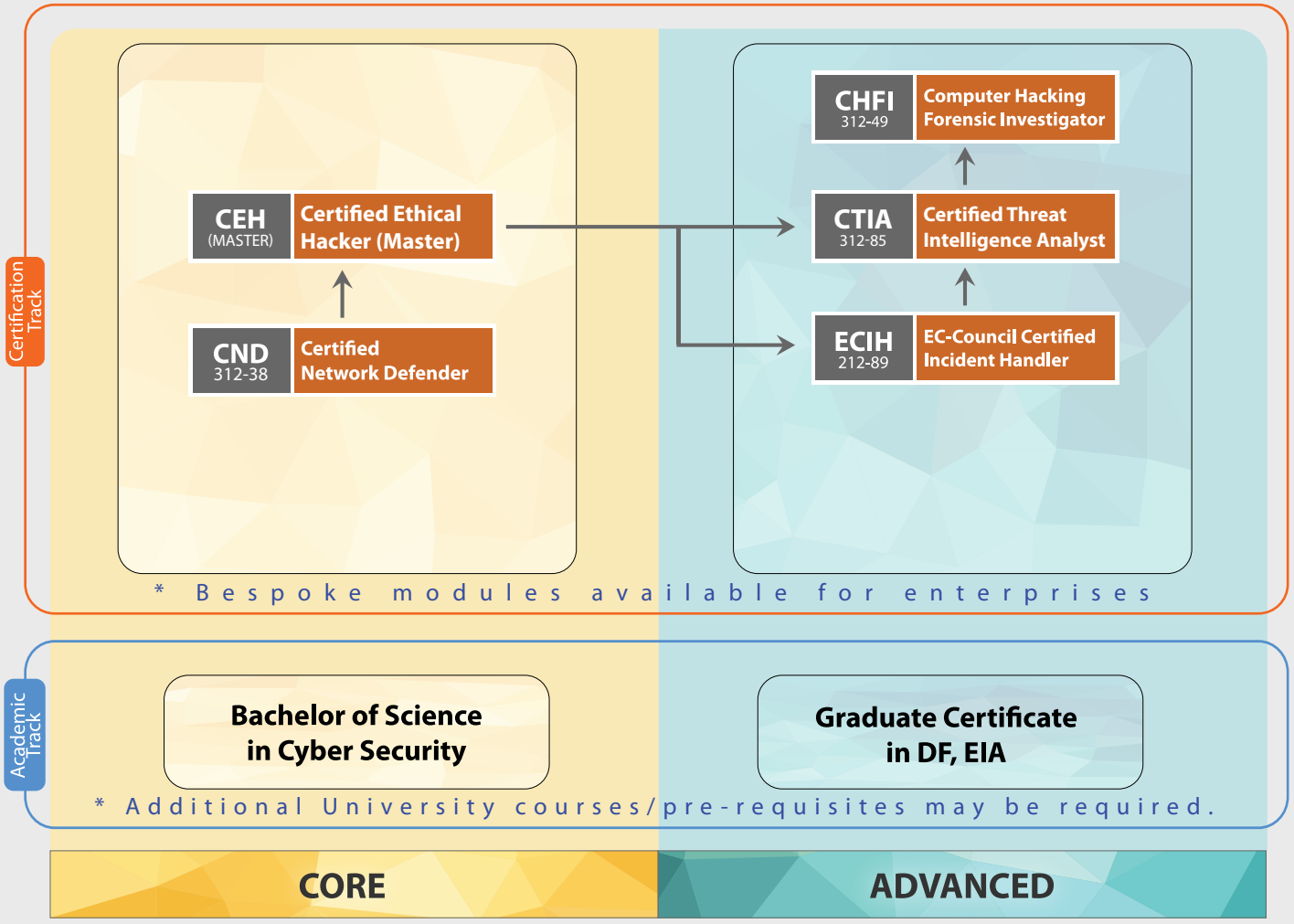
1. Protect and Defend (PR)
- a. Cybersecurity Defense Analysis (DA)
- b. Cybersecurity Defense Infrastructure Support (INF)
- c. Incident Response (IR)
- d. Vulnerability Assessment and Management (VA)

2. Securely Provision (SP)
- a. Test and Evaluation

3. Analyze (AN)
- a. Threat Analysis (TA)
- b. Exploitation Analysis (XA)

All credentials can be attained individually. Please refer to cert.eccouncil.org for the eligibility criteria.

Cyber Forensics



Job Roles

- Computer Forensic Analyst
- Computer Network Defense (CND)
- Forensic Analyst
- Digital Forensic Examiner

Our Certified Cyber Forensic Professionals are Employed at:

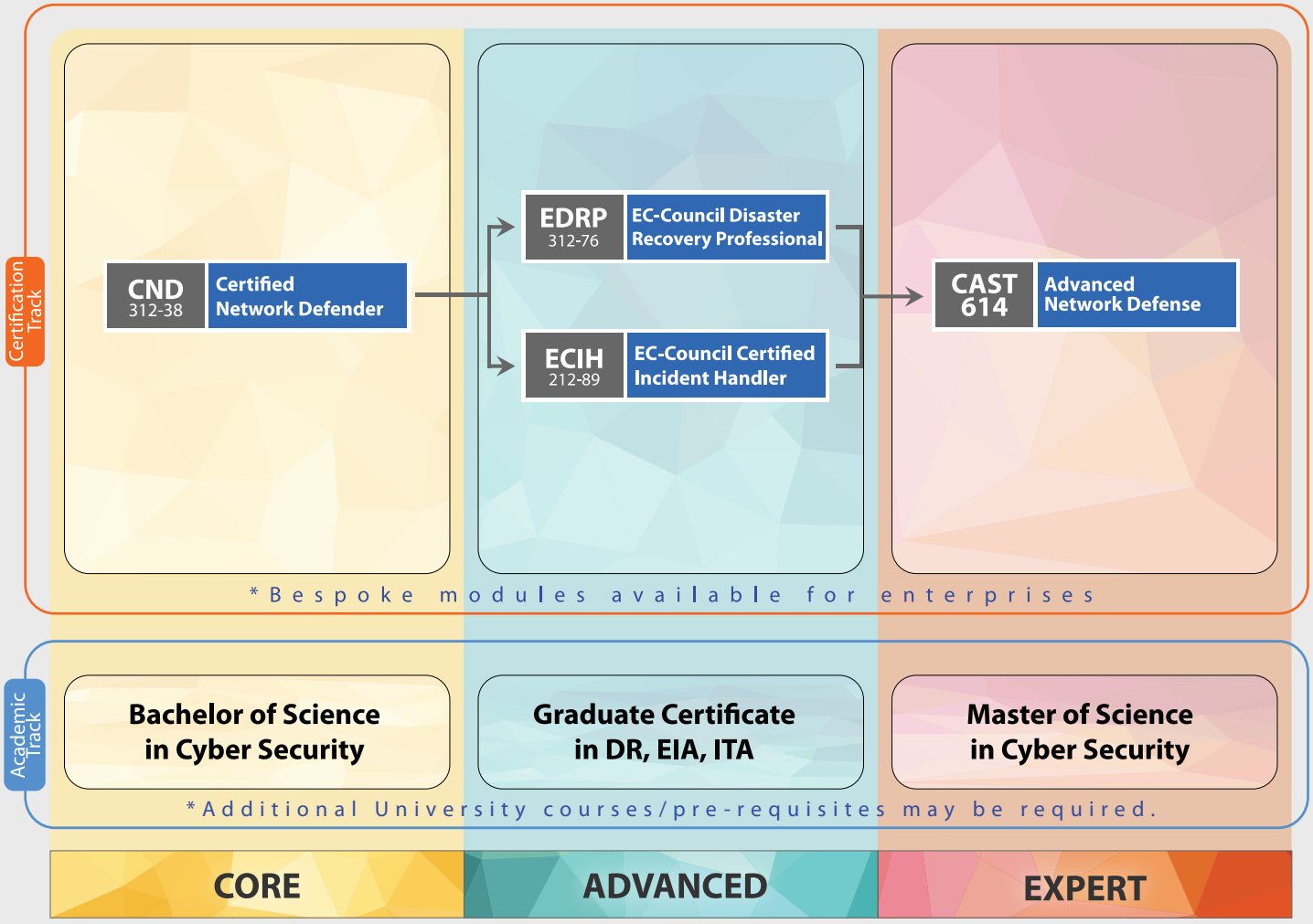
BARCLAYS, AIG, accenture, Infosys, U.S. ARMY, ICICI Bank, Bank of America, HDFC BANK, BMC SWITZERLAND, Telkom Indonesia, LEXINGTON MEDICAL CENTER, pwc, HSBC, WIPRO Applying Thought, ...

This Track Maps to NICE's Specialty Areas:

1. **Securely Provision (SP)**
   a. Risk Management (RM)
   b. Test and Evaluation
2. **Operate and Maintain (OM)**
   a. Network Services (NET)
   b. Systems Administration (SA)
   c. Systems Analysis (AN)
3. **Oversee and Govern (OV)**
   a. Cybersecurity Management (MG)
4. **Protect and Defend (PR)**
   a. Cybersecurity Defense Analysis (DA)
   b. Cybersecurity Defense Infrastructure Support (INF)
   c. Incident Response (IR)
   d. Vulnerability Assessment and Management (VA)
5. **Analyze (AN)**
   a. Threat Analysis (TA)
   b. Exploitation Analysis (XA)

*All credentials can be attained individually. Please refer to cert.eccouncil.org for the eligibility criteria.

Network Defense and Operations



Job Roles

- Network Security Administrators
- Network Security Engineer/Specialist
- Network Defense Technicians
- Security Analyst
- Security Operator
- Computer Network Defense(CND) Analyst
- Cybersecurity Intelligence Analyst
- Enterprise Network Defense(END) Analyst

Our Certified Network Defense Professionals are Employed at:

FGB, IBM, KPMG, DISA, mitra solusi telematika, Ameriprise Financial, COMCAST, Florida State University, NCB الأهلي, IPDC Finance, Johnson Controls, sopra steria Consulting, Rockwell Automation, MAPFRE, • • •

This Track Maps to NICE's Specialty Areas:

1. Securely Provision (SP)
a. Risk Management (RM)
b. Test and Evaluation (TE)

2. Operate and Maintain (OM)
a. Network Services (NET)
b. Systems Administration (SA)
c. Systems Analysis (AN)

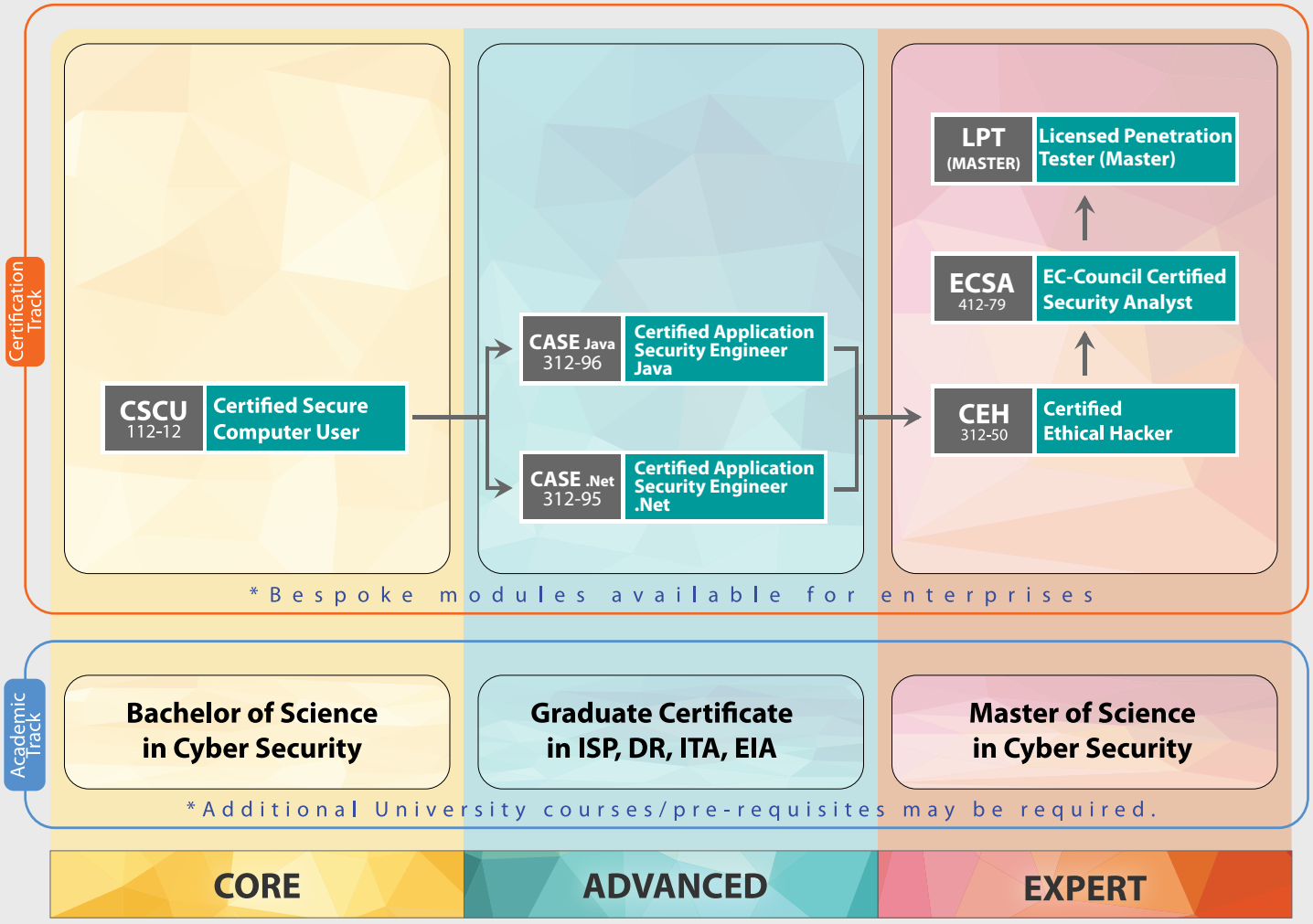
3. Oversee and Govern (OV)
a. Cybersecurity Management (MG)

4. Protect and Defend (PR)
a. Cybersecurity Defense Analysis (DA)
b. Cybersecurity Defense Infrastructure Support (INF)
c. Incident Response (IR)
d. Vulnerability Assessment and Management (VA)

5. Analyze (AN)
a. Threat Analysis (TA)

*All credentials can be attained individually. Please refer to cert.eccouncil.org for the eligibility criteria.

Software Security



Job Roles

- Secure Software Engineer
- Security Engineer
- Software Developer
- Software Engineer/Architect
- Systems Analyst
- Web Application Developer
- Application Security Tester

This Track Maps to NICE's Specialty Areas:

1. Securely Provision
a. Software Development (DEV)
b. Technology R&D (RD)

2. Operate and Maintain (OM)
a. Data Administration (DA)
b. Systems Analysis (AN)

3. Oversee and Govern (OV)
a. Cybersecurity Management (MG)

4. Protect and Defend (PR)
a. Cybersecurity Defense Analysis (DA)
b. Vulnerability Assessment

and Management (VA)

5. Analyze (AN)
a. Analyzes collected information to identify vulnerabilities and potential for exploitation.

Our Certified Software Security Professionals are Employed at:

WELLS FARGO, ITU, AIRBUS, TATA, axiata, BlueCross BlueShield, bol.com, alBaraka, Cognizant, Deloitte., EY Building a better working world, ecovadis 2007-2017 Supplier Sustainability Ratings, Infoblox Control Your Network, KASPERSKY lab, . . .

All credentials can be attained individually. Please refer to cert.eccouncil.org for the eligibility criteria.

Governance

Master of Science in Cyber Security

Graduate Certificate in:

- **Information Security Professional**
- **Information Analyst**
- **Information Technology Analyst**
- **Disaster Recovery**
- **Digital Forensics**

Job Roles

- Chief Information Security Officer (CISO)
- Chief Security Officer (CSO)
- Information Security (IS) Director
- Information Assurance (IA) Program Manager

Our Certified CCISO Professionals are Employed at:

marta, U.S. Army, Akamai, MUFG Bank of Tokyo-Mitsubishi UFJ, Santander, BOFI Federal Bank, Chase, Chemical Bank, Generali, Government of South Australia, KPMG, Malwarebytes, Police Department, Arrow, Polycom, Rockwell Collins, Tadawul, The Bancorp, GE, HSBC, ICF, Juniper Networks, L'Oréal, Rabobank, vodafone, Telstra, ...

This Track Maps to NICE's Specialty Areas:

1. Securely Provision (SP)
- a. Risk Management (RM)
- b. Technology R&D (RD)
- c. Systems Requirements Planning (RP)

2. Oversee and Govern (OV)
- a. Legal Advice and Advocacy (LG)
- b. Training, Education, and Awareness (ED)
- c. Cybersecurity Management (MG)
- d. Strategic Planning and Policy (PL)
- e. Executive Cybersecurity Leadership (EX)
- f. Acquisition and Program/Project Management (PM)

3. Collect and Operate (CO)
- a. Cyber Operational Planning (PL)

**All credentials can be attained individually. Please refer to cert.eccouncil.org for the eligibility criteria.*

Certified Secure Computer User (CSCU)

Course Description

CSCU provides individuals with the necessary knowledge and skills to protect their information assets.

This course covers fundamentals of various computer and network security threats such as identity theft, credit card fraud, phishing, virus and backdoors, emails hoaxes, loss of confidential information, hacking attacks, and social engineering.

Key Outcomes

- Fundamentals of various computer and network security threats
- Understanding of identity theft, phishing scams, malware, social engineering, and financial frauds
- Learn to safeguard mobile, media and protect data
- Protecting computers, accounts, and social networking profiles as a user
- Understand security incidents and reporting

Exam Information

- Exam Title: Certified Secure Computer User
- Exam Code: 112-12
- Number of Questions: 50
- Duration: 2 Hours
- Availability: ECC Exam Portal
- Test Format: Multiple Choice
- Passing Score: 70%

Course Outline

- Introduction to Security
- Securing Operating Systems
- Malware and Antivirus
- Internet Security
- Security on Social Networking Sites
- Securing Email Communications
- Securing Mobile Devices
- Securing Cloud
- Securing Network Connections
- Data Backup and Disaster Recovery

EC-Council Certified Security Specialist (ECSS)

Course Description

EC-Council Certified Security Specialist (ECSS) is an entry level security program covering the fundamental concepts of information security, computer forensics, and network security. It enables students to identify information security threats which reflect on the security posture of the organization and implement general security controls.

This program will give a holistic overview of the key components of information security, computer forensics, and network security. This program provides a solid fundamental knowledge required for a career in information security.

Key Outcomes

- It facilitates your entry into the world of Information Security
- It provides professional understanding about the concepts of Information Security, Network Security, and Computer Forensics
- It provides best practices to improve organizational security posture
- It enhances your skills as a Security Specialist and increases your employability

Exam Information

- Exam Title: EC-Council Certified Security Specialist
- Exam Code: ECSS
- Number of Questions: 50
- Duration: 2 hours
- Availability: ECC Exam Portal
- Test Format: Multiple Choice
- Passing Score: 70%

Course Outline

- Information Security Fundamentals
- Networking Fundamentals
- Secure Network Protocols
- Information Security Threats and Attacks
- Social Engineering
- Hacking Cycle
- Identification, Authentication, and Authorization
- Cryptography
- Firewalls
- Intrusion Detection System
- Data Backup
- Virtual Private Network
- Wireless Network Security
- Web Security
- Ethical Hacking and Pen Testing
- Incident Response
- Computer Forensics Fundamentals
- Digital Evidence
- Understanding File Systems
- Windows Forensics
- Network Forensics and Investigating Network Traffic
- Steganography
- Analyzing Logs
- E-mail Crime and Computer Forensics
- Writing Investigative Report

EC-Council Certified Encryption Specialist (ECES)

Course Description

The EC-Council Certified Encryption Specialist (ECES) program introduces professionals and students to the field of cryptography. The participants will learn the foundations of modern symmetric and key cryptography including the details of algorithms such as Feistel Functions, DES, and AES.

Key Outcomes

- Develop skills to protect critical data in organizations with encryption
- Develop a deep understanding of essential cryptography algorithms and their applications
- Make informed decisions about applying encryption technologies
- Save time and cost by avoiding common mistakes in implementing encryption technologies effectively
- Develop working knowledge of cryptanalysis

Exam Information

- Exam Title: EC-Council Certified Encryption Specialist
- Exam Code: 212-81
- Number of Questions: 50
- Duration: 2 hours
- Availability: ECC Exam Portal
- Test Format: Multiple Choice
- Passing Score: 70%

Course Outline

- Introduction and History of Cryptography
- Symmetric Cryptography and Hashes
- Number Theory and Asymmetric Cryptography
- Applications of Cryptography
- Cryptanalysis

Certified Network Defender (CND)

Course Description

CND is the world's most advanced network defense course that covers 14 of the most current network security domains any individuals will ever want to know when they are planning to protect, detect, and respond to the network attacks.

The course contains hands-on labs, based on major network security tools and to provide network administrators real world expertise on current network security technologies and operations.

Key Outcomes

- Knowledge on how to protect, detect, and respond to network attacks
- Network defense fundamentals
- Application of network security controls, protocols, perimeter appliances, secure IDS, VPN, and firewall configuration
- Intricacies of network traffic signature, analysis, and vulnerability scanning

Exam Information

- Exam Title: Certified Network Defender
- Exam Code: 312-38
- Number of Questions: 100
- Duration: 4 hours
- Availability: ECC Exam Portal
- Test Format: Multiple Choice
- Passing Score: Please refer to
- Passing Score: Please refer to https://cert.eccouncil.org/faq.html

Course Outline

- Computer Network and Defense Fundamentals
- Network Security Threats, Vulnerabilities, and Attacks
- Network Security Controls, Protocols, and Devices
- Network Security Policy Design and Implementation
- Physical Security
- Host Security
- Secure Firewall Configuration and Management
- Secure IDS Configuration and Management
- Secure VPN Configuration and Management
- Wireless Network Defense
- Network Traffic Monitoring and Analysis
- Network Risk and Vulnerability Management
- Data Backup and Recovery
- Network Incident Response and Management

Certified Ethical Hacker (C|EH)

Course Description

C|EH is the world's most advanced certified ethical hacking course that covers 20 of the most current security domains any individual will ever want to know when they are planning to beef-up the information security posture of their organization.

The accredited course provides the advanced hacking tools and techniques used by hackers and information security professionals.

Key Outcomes

- Thorough introduction to ethical hacking
- Exposure to threat vectors and countermeasures
- Addresses emerging areas of IoT, cloud and mobile hacking
- Prepares you to combat Trojans, malware, backdoors, and more
- Enables you to hack using mobile

Exam Information

- Exam Title: Certified Ethical Hacker (ANSI)
- Exam Code: 312-50 (ECC EXAM), 312-50 (VUE)
- Number of Questions: 125
- Duration: 4 hours
- Availability: ECC Exam Portal, VUE
- Test Format: Multiple Choice
- Passing Score: Please refer to https://cert.eccouncil.org/faq.html

Course Outline

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking
- Cloud Computing
- Cryptography

Certified Ethical Hacker (Practical)

Course Description

C|EH Practical is a six-hour, rigorous exam that requires you to demonstrate the application of ethical hacking techniques such as threat vector identification, network scanning, OS detection, vulnerability analysis, system hacking, web app hacking, etc. to solve a security audit challenge.

This is the next step after you have attained the highly acclaimed Certified Ethical Hacker certification.

Key Outcomes

- Mastery of Ethical Hacking skills.
- Demonstrate the application of the knowledge to find solutions to real-life challenges.
- Commitment to code of ethics.
- Validate essential skills required in the ethical hacking domains.

Exam Information

- Exam Title: Certified Ethical Hacker (Practical)
- Number of Practical Challenges: 20
- Duration: 6 hours
- Availability: Aspen - iLabs
- Test Format: iLabs Cyber Range
- Passing Score: 70%

C|EH (Practical) Credential Holders Can

- Demonstrate the understanding of attack vectors
- Perform network scanning to identify live and vulnerable machines in a network.
- Perform OS banner grabbing, service, and user enumeration.
- Perform system hacking, steganography, steganalysis attacks, and cover tracks.
- Identify and use viruses, computer worms, and malware to exploit systems.
- Perform packet sniffing.
- Conduct a variety of web server and web application attacks including directory traversal, parameter tampering, XSS, etc.
- Perform SQL injection attacks.
- Perform different types of cryptography attacks.
- Perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems etc.

Certified Threat Intelligence Analyst (CTIA)

Course Description

C|TIA is a method-driven program that uses a holistic approach, covering concepts from planning the threat intelligence project to building a report to disseminating threat intelligence. These concepts are highly essential while building effective threat intelligence and, when used properly, can secure organizations from future threats or attacks.

This program addresses all the stages involved in the Threat Intelligence Life Cycle. This attention to a realistic and futuristic approach makes C|TIA one of the most comprehensive threat intelligence certifications on the market today.

Key Outcomes

- Enable individuals and organizations with the ability to prepare and run a threat intelligence program that allows evidence-based knowledge and provides actionable advice about existing and unknown threats
- Ensure that organizations have predictive capabilities rather than just proactive measures beyond active defense mechanism
- Empower information security professionals with the skills to develop a professional, systematic, and repeatable real-life threat intelligence program
- Differentiate threat intelligence professionals from other information security professionals
- Provide an invaluable ability of structured threat intelligence to enhance skills and boost their employability

Exam Information

- Exam Title: Certified Threat Intelligence Analyst
- Exam Code: 312-85
- Number of Questions: 50
- Duration: 2 hours
- Availability: EC-Council Exam Portal
- Test Format: Multiple Choice
- Passing Score: 70%

Course Outline

- Introduction to Threat Intelligence
- Cyber Threats and Kill Chain Methodology
- Requirements, Planning, Direction, and Review
- Data Collection and Processing
- Data Analysis
- Intelligence Reporting and Dissemination

ECSA™
EC-Council Certified Security Analyst

EC-Council Certified Security Analyst (ECSA)

Course Description

ECSA is a globally accepted hacking and penetration testing program 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.

This program takes the tools and techniques covered in C|EH to next level by utilizing EC-Council's published penetration testing methodology.

Key Outcomes

- Introduction to security analysis and penetration testing methodologies
- In-depth vulnerability analysis, network penetration testing from external and internal evading firewalls and IDS
- Learn to own web applications and databases, and take over cloud services
- Analyze security of mobile devices and wireless networks
- Present findings in a structured actionable report

Exam Information

- Exam Title: EC-Council Certified Security Analyst
- Exam Code: 412-79
- Number of Questions: 150
- Duration: 4 hours
- Availability: ECC Exam Portal
- Test Format: Multiple Choice
- Passing Score: 70%

Course Outline

- Penetration Testing Essential Concepts (Student Introduction)
- Introduction to Penetration Testing and Methodologies
- Penetration Testing Scoping and Engagement Methodology
- Open-Source Intelligence (OSINT) Methodology
- Social Engineering Penetration Testing Methodology
- Network Penetration Testing Methodology – External
- Network Penetration Testing Methodology – Internal
- Network Penetration Testing Methodology – Perimeter Devices
- Web Application Penetration Testing Methodology
- Database Penetration Testing Methodology
- Wireless Penetration Testing Methodology
- Cloud Penetration Testing Methodology
- Report Writing and Post Testing Actions

EC-Council Certified Security Analyst (Practical)

Course Description

ECSA (Practical) is a 12-hour, rigorous practical exam built to test your penetration testing skills.

The candidates are required to demonstrate the application of the penetration testing methodology that is presented in the ECSA program, and are required to perform a comprehensive security audit of an organization, just like in the real world. You will start with challenges requiring you to perform advanced network scans beyond perimeter defenses, leading to automated and manual vulnerability analysis, exploit selection, customization, launch, and post exploitation maneuvers.

Key Outcomes

- Test your ability to perform threat and exploit research, understand exploits in the wild, write your own exploits, customize payloads, and make critical decisions
- Create a professional pen testing report with essential elements

Exam Information

- Exam Title: EC-Council Certified Security Analyst (Practical)
- Number of challenges: 8
- Duration: 12 hours
- Availability: Aspen- iLabs
- Test Format: iLabs cyber range
- Passing Score: 5 out of 8 challenges and submission of an acceptable penetration testing report

ECSA (Practical) Credential Holders Can

- Perform advanced network scans beyond perimeter defenses, leading to automated and manual vulnerability analysis, exploit selection, customization, launch and post exploitation maneuvers.
- Customize payloads
- Make critical decisions at different phases of a pen-testing engagement
- Perform advanced network scans beyond perimeter defenses
- Perform automated and manual vulnerability analysis
- Customization, launch, and post exploitation maneuvers
- Perform a full fledged Penetration Testing engagement
- Create a professional pen-testing report
- Demonstrate the application of penetration testing methodology presented in the ECSA program

EC-Council Certified Incident Handler (ECIH)

Course Description

The ECIH 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.

The comprehensive training program will make students proficient in handling as well as responding to various security incidents such as network security incidents, malicious code incidents, and insider attack threats.

Key Outcomes

- Principals, processes and techniques for detecting and responding to security threats/ breaches
- Liaison with legal and regulatory bodies
- Learn to handle incidents and conduct assessments
- Cover various incidents like malicious code, network attacks, and insider attacks

Exam Information

- Exam Title: EC-Council Certified Incident Handler
- Exam Code: 212-89
- Number of Questions: 50
- Duration: 2 hours
- Availability: ECC Exam Portal
- Test Format: Multiple Choice
- Passing Score: 70%

Course Outline

- Introduction to Incident Response and Handling
- Risk Assessment
- Incident Response and Handling Steps
- CSIRT
- Handling Network Security Incidents
- Handling Malicious Code Incidents
- Handling Insider Threats
- Forensic Analysis and Incident Response
- Incident Reporting
- Incident Recovery
- Security Policies and Laws

Computer Hacking and Forensic Investigator (CHFI)

Course Description

CHFI is a comprehensive course covering major forensic investigation scenarios, enabling students to acquire hands-on experience.

The program provides a strong baseline knowledge of key concepts and practices in the digital forensic domains relevant to today's organizations. Moreover, CHFI provides firm grasp on the domains of digital forensics.

Key Outcomes

- Comprehensive forensics investigation process
- Forensics of file systems, operating systems, network and database, websites, and email systems
- Techniques for investigating on cloud, malware, and mobile
- Data acquisition and analysis as well as anti-forensic techniques
- Thorough understanding of chain of custody, forensic report, and presentation

Exam Information

- Exam Title: Computer Hacking Forensic Investigator
- Exam Code: 312-49 exam
- Number of Questions: 150
- Duration: 4 hours
- Availability: ECC Exam Portal
- Test Format: Multiple Choice
- Passing Score: Please refer to https://cert.eccouncil.org/faq.html

Course Outline

- Computer Forensics in Today's World
- Computer Forensics Investigation Process
- Understanding Hard Disks and File Systems
- Data Acquisition and Duplication
- Defeating Anti-Forensics Techniques
- Operating System Forensics
- Network Forensics
- Investigating Web Attacks
- Database Forensics
- Cloud Forensics
- Malware Forensics
- Investigating Email Crimes
- Mobile Forensics
- Forensics Report Writing and Presentation

Certified Application Security Engineer (CASE) Java

Course Description

The **CASE Java** program is designed to be a hands-on, comprehensive application security training course that will help software professionals create secure applications. It trains software developers on the critical security skills and knowledge required throughout a typical software development life cycle (SDLC), focusing on the importance of the implementation of secure methodologies and practices required in today's insecure operating environment.

Key Outcomes

- Security Beyond Secure Coding - Challenging the traditional mindset where secure application means secure coding
- Testing and credentialing secure application development across all phases of the SDLC
- CASE Program maps to many Specialty Areas under "Securely Provision category" in the NICE 2.0 Framework
- Covers techniques such as Input Validation techniques, Defense Coding Practices, Authentications and Authorizations, Cryptographic Attacks, Error Handling techniques, and Session Management techniques, among many others

Exam Information

- Exam Title: Certified Application Security Engineer (Java)
- Exam Code: 312-96
- Number of Questions: 50
- Duration: 2 hours
- Availability: ECC Exam Portal
- Test Format: Multiple Choice
- Passing Score: 70%

Course Outline

- Understanding Application Security, Threats, and Attacks
- Security Requirements Gathering
- Secure Application Design and Architecture
- Secure Coding Practices for Input Validation
- Secure Coding Practices for Authentication and Authorization
- Secure Coding Practices for Cryptography
- Secure Coding Practices for Session Management
- Secure Coding Practices for Error Handling
- Static and Dynamic Application Security Testing (SAST & DAST)
- Secure Deployment and Maintenance

Certified Application Security Engineer (CASE) .Net

Course Description

CASE goes beyond just the guidelines on secure coding practices but include secure requirement gathering, robust application design, and handling security issues in post development phases of application development.

This makes CASE one of the most comprehensive certifications for secure software development in the market today. It's desired by software application engineers, analysts, testers globally, and respected by hiring authorities.

The hands-on training program encompasses security activities involved in all phases of the Secure Software Development Life Cycle (SDLC): planning, creating, testing, and deploying an application.

Key Outcomes

- Ensure that application security is no longer an afterthought but a foremost one.
- It lays the foundation required by all application developers and development organizations, to produce secure applications with greater stability and fewer security risks to the consumer.
- Ensure that organizations mitigate the risk of losing millions due to security compromises that may arise with every step of application development process.
- Helps individuals develop the habit of giving importance to security sacrosanct of their job role in the SDLC, therefore opening security as the main domain for testers, developers, network administrator etc.

Exam Information

- Exam Title: Certified Application Security Engineer (.NET)
- Exam Code: 312-95
- Number of Questions: 50
- Duration: 2 hours
- Availability: ECC Exam Portal
- Test Format: Multiple Choice
- Passing Score: 70%

Course Outline

- Understanding Application Security, Threats, and Attacks
- Security Requirements Gathering
- Secure Application Design and Architecture
- Secure Coding Practices for Input Validation
- Secure Coding Practices for Authentication and Authorization
- Secure Coding Practices for Cryptography
- Secure Coding Practices for Session Management
- Secure Coding Practices for Error Handling
- Static and Dynamic Application Security Testing (SAST & DAST)
- Secure Deployment and Maintenance

APT
Advanced Penetration Testing

Advanced Penetration Testing

Course Description

In the Advanced Penetration Testing Course, you are presented with minimal network information along with a Scope of Work (SOW). The course was created to provide you with advanced concepts that will help when it comes to attempting the LPT (Master) Certification exam.

The last module of the course includes an SOW for each of the various networks we have created for the course. This, combined with the composition of various ranges, mimics a professional penetration test. Time is limited and you will be required to identify the attack surface followed by the weaknesses of the machines that are on the network.

Key Outcomes

- Prepare you for the LPT (master) exam.
- Learn professional security and penetration testing skills.
- Show advanced concepts like scanning against defenses, pivoting between networks, deploying proxy chains, and using web shells.

Course Outline

- Introduction to Vulnerability Assessment and Penetration Testing
- Information Gathering Methodology
- Scanning and Enumeration
- Identify Vulnerabilities
- Exploitation
- Post Exploitation
- Advanced Tips and Techniques
- Preparing a Report
- Practice Ranges

The Licensed Penetration Tester (Master) Credential– LPT(Master)

Course Description

The LPT (Master) credential is developed in collaboration with SMEs and practitioners around the world after a thorough job role, job task, and skills-gap analysis.

The LPT (Master) practical exam is the capstone to EC-Council's entire information security track, right from the CEH to the ECSA Program. The LPT (Master) exam covers the skill-sets, technical analysis and report writing, required to be a true professional penetration tester.

Key Outcomes

LPT Demonstrates

- Mastery of penetration testing skills
- Ability to perform repeatable methodology
- Commitment to code of ethics
- Ability to present analysed results through structured reports

Exam Information

- Live Online
- Fully Proctored
- 3 Levels
- 9 Challenges
- 18 Hours

Testimonials

"Converting fear into confidence with $LPT_{(Master)}$"

by Adithya Naresh

"Proud to attain the $LPT_{(Master)}$ credential"

by Ali Isikli

"$LPT_{(Master)}$: Extremely challenging and one of the toughest exams"

by Mark Horvat

"Real-life penetration testing with $LPT_{(Master)}$"

by Moustafa Mohamed Mohsen

CAST
Center for Advanced Security Training

CAST 614 – Advanced Network Defense

Course Description

CAST 614 is an advanced course offering you the opportunity to deep dive into the crucial practical aspects of enterprise network security.

It covers fundamental areas of fortifying your defenses by discovering methods of developing a secure baseline and how to harden your enterprise architecture from the most advanced attacks. Once a strategy for a fortified perimeter is denied, the course moves on to defending against the sophisticated malware that is on the rise today, and the importance of live memory analysis and real time monitoring.

Key Outcomes

- Stage a strong defense against popular security threats
- Fortify your organization with a good foundation of risk protection methods
- Apply latest references and guidance on best practices in the field of cybersecurity
- Secure your enterprise architecture from a medium threat level and build towards more sophisticated threats

Exam Information

- Exam Title: CAST 614 - Advanced Network Defense
- Number of Questions: 50 (Written) and 10 (Practical)
- Duration: 90 minutes (Written) and 60 minutes (Practical)
- Availability: ECC Exam Portal
- Passing Score: Written Exam (60%) and Practical Exam (70%)

Course Outline

- Firewalls
- Advanced Filtering
- Firewall Configuration
- Hardening: Establishing a Secure Baseline
- Intrusion Detection and Prevention
- Protecting Web Applications
- Memory Analysis
- Endpoint Protection
- Securing an Enterprise

EC-Council Disaster Recovery Professional™

EC-Council Disaster Recovery Professional (EDRP)

Course Description

The EDRP course identifies vulnerabilities and takes appropriate countermeasures to prevent and mitigate failure risks for an organization. It also provides the networking professional a foundation in disaster recovery course principles, including preparation of a disaster recovery plan, assessment of risks in the enterprise, development of policies and procedures, an understanding of the roles and relationships of various members of an organization, implementation of a plan, and recovering from a disaster.

Key Outcomes

- Introduction to business continuity, risk management, and disaster recovery
- Disasters and emergency management, and applicable regulations
- DR planning process, preparation, recovery of systems and facilities
- Incident response and liaison with public services and regulatory bodies
- Exposure to various services from government and other entities

Exam Information

- Exam Title: EC-Council Disaster Recovery Professional
- Exam Code: 312-76
- Number of Questions: 150
- Duration: 4 hours
- Availability: ECC Exam Portal
- Test Format: Multiple Choice
- Passing Score: 70%

Course Outline

- Introduction to Disaster Recovery and Business Continuity
- Business Continuity Management (BCM)
- Risk Assessment
- Business Impact Analysis (BIA)
- Business Continuity Planning (BCP)
- Data Backup Strategies
- Data Recovery Strategies
- Virtualization-Based Disaster Recovery
- System Recovery
- Centralized and Decentralized System Recovery
- Disaster Recovery Planning Process
- BCP Testing, Maintenance, and Training

EC-Council

Certified Chief Information Security Officer (C|CISO)

Course Description

The C|CISO certification is an industry-leading program that recognizes the real-world experience necessary to succeed at the highest executive levels of information security. Bringing together all the components required for a C-Level positions, the C|CISO program combines audit management, governance, IS controls, human capital management, strategic program development, and the financial expertise vital for leading a highly successful IS program.

The C|CISO Training Program can be the key to a successful transition to the highest ranks of information security management.

Key Outcomes

- Establishes the role of CISO and models for governance
- Core concepts of information security controls, risk management, and compliance
- Builds foundation for leadership through strategic planning, program management, and vendor management

Exam Information

- Number of Questions: 150
- Duration: 2.5 hours
- Test Format: Multiple Choice

Domains

- Governance
- Security Risk Management, Controls, & Audit Management
- Security Program Management & Operations
- Information Security Core Competencies
- Strategic Planning, Finance, & Vendor Management

EC-COUNCIL UNIVERSITY
ACCREDITED. FLEXIBLE. ONLINE.

Bachelor of Science in Cyber Security (BSCS)

Course Description

The **Bachelor of Science in Cyber Security (BSCS)** prepares students the knowledge for careers in cyber security and assurance. The program consists of topical areas dealing with computer security management, incident response, and security threat assessment, etc.

Key Outcomes

- Knowledge and hands-on experience on various foundational cyber security concepts
- Some of the key topics include security management and incident response, security threat assessment and risk management, legal and regulatory issues and compliance
- Cyber defense and cyber warfare, implementation of security controls, and auditing
- Capstone Project

Graduation Requirements

- Completion of 60 credit hours of 300/400 level courses in which the candidate earned a cumulative GPA of 2.5 or better
- Satisfactory completion of the summative capstone course
- All degree requirements must be completed within four years from the date the student enrolls in the University and begins the program

Courses

- CIS 300 Fundamentals of Information Systems Security
- CIS 301 Legal Issues in Cyber Security
- CIS 302 Managing Risk in Information Systems
- CIS 303 Security Policies and Implementation Issues
- CIS 304 Auditing IT Infrastructures for Compliance
- CIS 308 Access Control
- CIS 401 Security Strategies in Windows Platforms and Applications
- CIS 402 Security Strategies in Linux Platforms and Applications
- CIS 403 Network Security, Firewalls, and VPNs
- CIS 404 Hacker Techniques, Tools, and Incident Handling
- CIS 405 Internet Security: How to Defend Against Online Attackers
- CIS 406 System Forensics, Investigation, and Response
- CIS 407 Cyberwarfare
- CIS 408 Wireless and Mobile Device Security
- CIS 410 Capstone Course
- COM 340 Communication and Technical Writing
- MTH 350 Introduction to Statistics
- PSY 360 Social Psychology
- BIS 430 Ethics for the Business Professional
- ECN 440 Principles of Microeconomics
- MGT 450 Introduction to Project Management

EC-COUNCIL UNIVERSITY
ACCREDITED. FLEXIBLE. ONLINE.

Graduate Certificate Programs

Course Description

EC-Council University's Graduate Certificate Program focuses on the competencies necessary for information assurance professionals to become managers, directors, and CIOs. Students will experience not only specialized technical training in a variety of IT security areas, but will also acquire an understanding of organizational structure and behavior, the skills to work within and across that organizational structure, and the ability to analyze and navigate its hierarchy successfully. Each certificate targets skills and understandings specific to particular roles in the IT security framework of an organization. The certificates can be taken singly or as a progressive set of five, each building on the one before it to move students from IT practitioner skill levels to IT executive skill levels.

Key Outcomes

- Preparation for industry recognized certifications
- NSA program mappings
- Executive leadership development
- Masters level education
- Promoting critical thinking
- Ethical practice
- Scholarship & research

Certificate Requirements

- Completion of mandated credit hours of courses in which the candidate earned a cumulative GPA of 2.5 or better
- All certificate requirements must be completed within **six months-one year** from the date the student enrolls in the university and begins the program

Specializations

- Security Analyst
- Enterprise Security Architect
- Digital Forensics
- Incident Management and Business Continuity
- Executive Leadership in Information Assurance

EC-COUNCIL UNIVERSITY
ACCREDITED. FLEXIBLE. ONLINE.

Master of Science in Cyber Security (MSCS)

Course Description

The **Master of Science in Cyber Security (MSCS)** Program prepares information technology professionals for careers in cyber security and assurance. The program consists of topical areas dealing with computer security management, incident response, and cyber security threat assessment, which require students to be the creators of knowledge and inventors of cyber security processes, not merely users of information. Additionally, students will receive instruction in leadership and management in preparation for becoming cyber security leaders, managers, and directors.

Key Outcomes

- Application of cyber security technical strategies, tools, and techniques to secure data and information for a customer or client
- Adherence to a high standard of cyber security ethical behavior
- Use of research in both established venues and innovative applications to expand the body of knowledge in cyber security
- Application of principles of critical thinking to creatively and systematically solve the problems and meet the challenges of the everchanging environments of cyber security
- Mastery of the skills necessary to move into cyber security leadership roles in companies, agencies, divisions, or departments

Graduation Requirements

- Completion of thirty-six (36) credits of 500 level courses in which the candidate earned a cumulative GPA of 3.0 or better
- Satisfactory completion of the summative capstone course
- All degree requirements must be completed within four years from the date the student enrolls in the university and begins the program

Courses

- ECCU 500 Managing Secure Network Systems
- MGMT 502 Business Essentials
- ECCU 501 Ethical Hacking & Countermeasures
- ECCU 502 Investigating Network Intrusions and Computer Forensics
- ECCU 503 Security Analysis and Vulnerability Assessment
- ECCU 504 Foundations of Organizational Behavior for the IT Practitioner
- ECCU 505 Introduction to Research and Writing for the IT Practitioner
- ECCU 506 Conducting Penetration and Security Tests
- ECCU 507 Linux Networking and Security
- ECCU 509 Securing Wireless Networks
- ECCU 510 Secure Programming
- ECCU 511 Global Business Leadership
- ECCU 512 Beyond Business Continuity
- ECCU 513 Disaster Recovery
- ECCU 514 Quantum Leadership
- ECCU 515 Project Management in IT Security
- ECCU 516 The Hacker Mind: Profiling the IT Criminal
- ECCU 517 Cyber Law
- ECCU 518 Special Topics
- ECCU 519 Capstone

EC-Council | Westcon Comstor Academy

www.eccouncil.org