EC-Council

CYBER SECURITY PROGRAMS

Over 1,500
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 E-Council Certified Ethical Hacker (CEH), EC-Council Computer Hacking Forensics Investigator (CHFI), EC-Council Certified Security Analyst (ECSA), and EC-Council License Penetration Tester (LPT) 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 EC-Council's Certified Ethical Hacking (CEH), EC-Council Network Security Administrator (ENSA), EC-Council Computer Hacking Forensics Investigator (CHFI), EC-Council Disaster Recovery Professional (EDRP), EC-Council Certified Security Analyst (ECSA) and EC-Council Licensed Penetration Tester (LPT) programs for meeting the 4011, 4012, 4013A, 4014, 4015 and 4016 training standards for information security professionals. EC-Council recently received accreditation from the American National Standards Institute (ANSI). We have so far certified over 2,00,000 professionals in various e-business and cyber security 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.

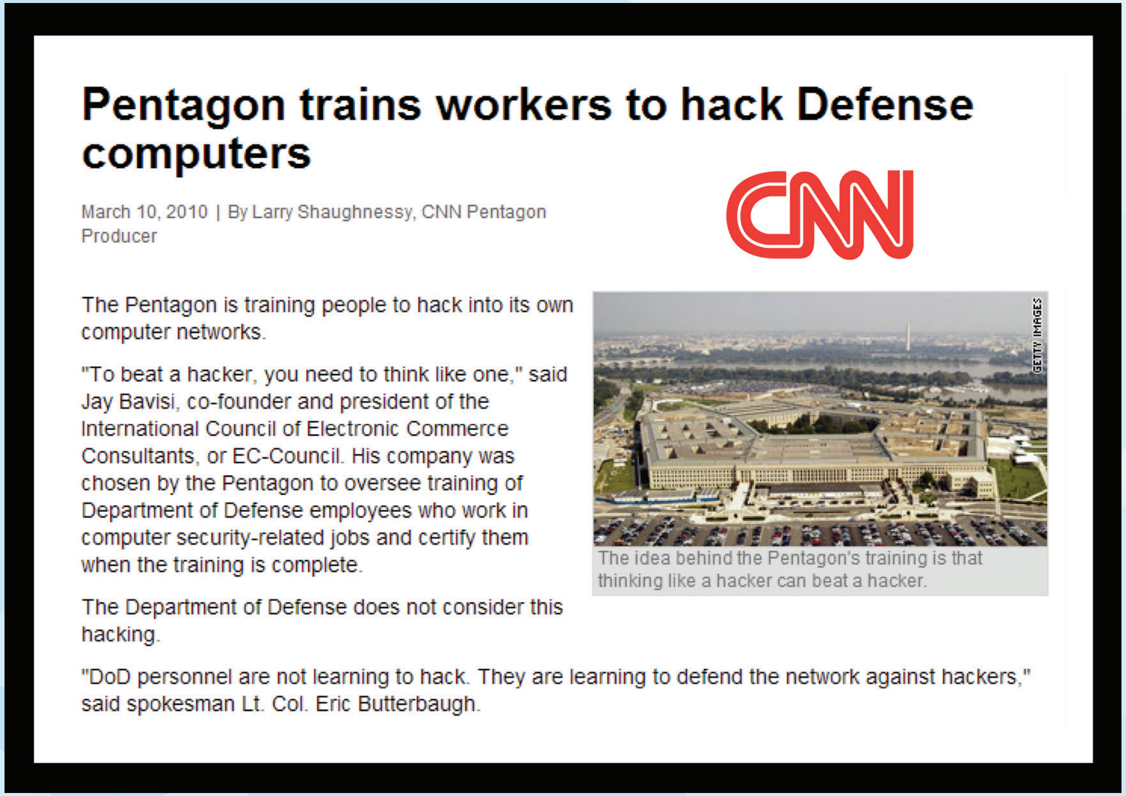
> *"Our lives are dedicated to the mitigation and remediation of the cyber plague that is menacing the world today"*
>
> ***Jay Bavisi***
> ***President & CEO***
> ***EC-Council***

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, 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

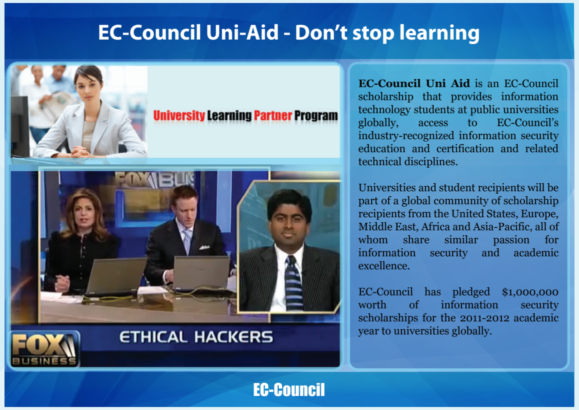
The Pentagon is training people to hack into its own computer networks.

"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 Uni-Aid - Don't stop learning

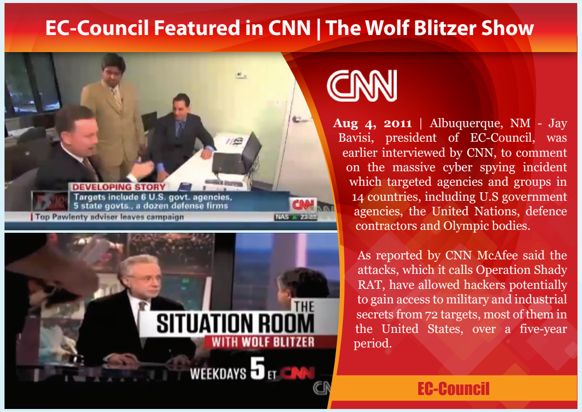
University Learning Partner Program
FOX BUSINESS
ETHICAL HACKERS

EC-Council Uni Aid is an EC-Council scholarship that provides information technology students at public universities globally, access to EC-Council's industry-recognized information security education and certification and related technical disciplines.

Universities and student recipients will be part of a global community of scholarship recipients from the United States, Europe, Middle East, Africa and Asia-Pacific, all of whom share similar passion for information security and academic excellence.

EC-Council has pledged $1,000,000 worth of information security scholarships for the 2011-2012 academic year to universities globally.

EC-Council



EC-Council Featured in CNN | The Wolf Blitzer Show

DEVELOPING STORY
Targets include 6 U.S. govt. agencies, 5 state govts., a dozen defense firms
Top Pawlenty adviser leaves campaign
THE SITUATION ROOM
WITH WOLF BLITZER
WEEKDAYS 5 ET

Aug 4, 2011 | Albuquerque, NM - Jay Bavisi, president of EC-Council, was earlier interviewed by CNN, to comment on the massive cyber spying incident which targeted agencies and groups in 14 countries, including U.S government agencies, the United Nations, defence contractors and Olympic bodies.

As reported by CNN McAfee said the attacks, which it calls Operation Shady RAT, have allowed hackers potentially to gain access to military and industrial secrets from 72 targets, most of them in the United States, over a five-year period.

EC-Council

> *"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+
YEARS EXPERIENCE

40+
TRAINING & CERTIFICATION PROGRAMS

145+
COUNTRIES

350+
SUBJECT MATTER EXPERTS

700+
TRAINING PARTNERS WORLDWIDE

3000+
TOOLS & TECHNOLOGIES

200,000+ CERTIFIED MEMBERS

Your Learning Options

Instructor-led Training

EC-Council has a large network of enterprise teams 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 Learning

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.

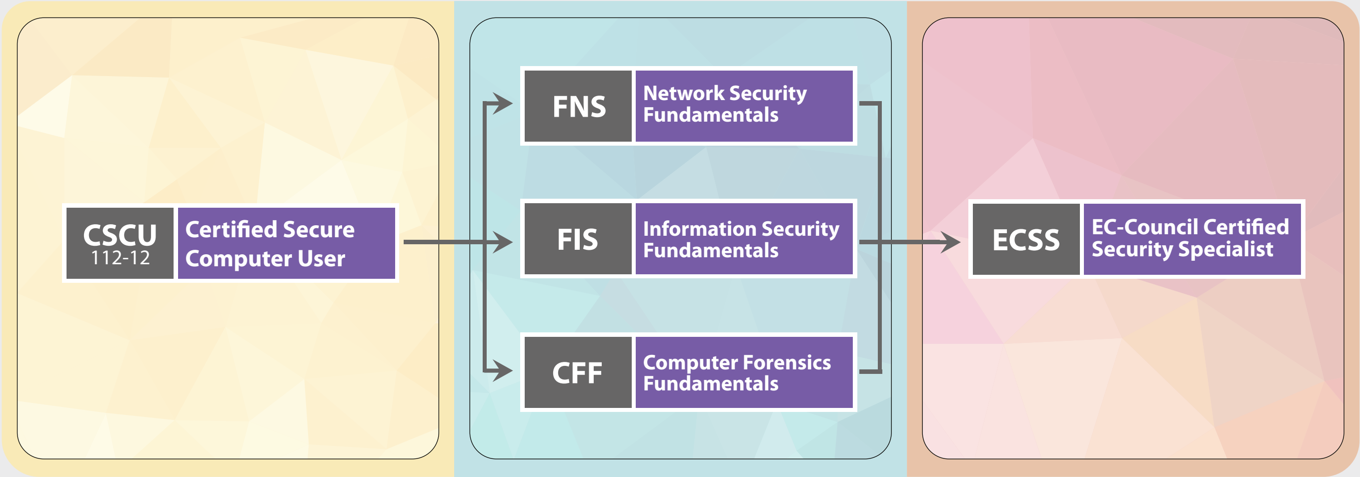
Customized Learning

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 and enterprise teams. 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 network of enterprise teams for a custom solution. EC-Council client-site training includes official courseware, certification exam (Prometric 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


CSCU
112-12
Certified Secure Computer User
FNS
Network Security Fundamentals
FIS
Information Security Fundamentals
CFF
Computer Forensics Fundamentals
ECSS
EC-Council Certified Security Specialist

Target Audience

This course is specifically designed for todays' computer users who use the internet extensively to work, study and play.

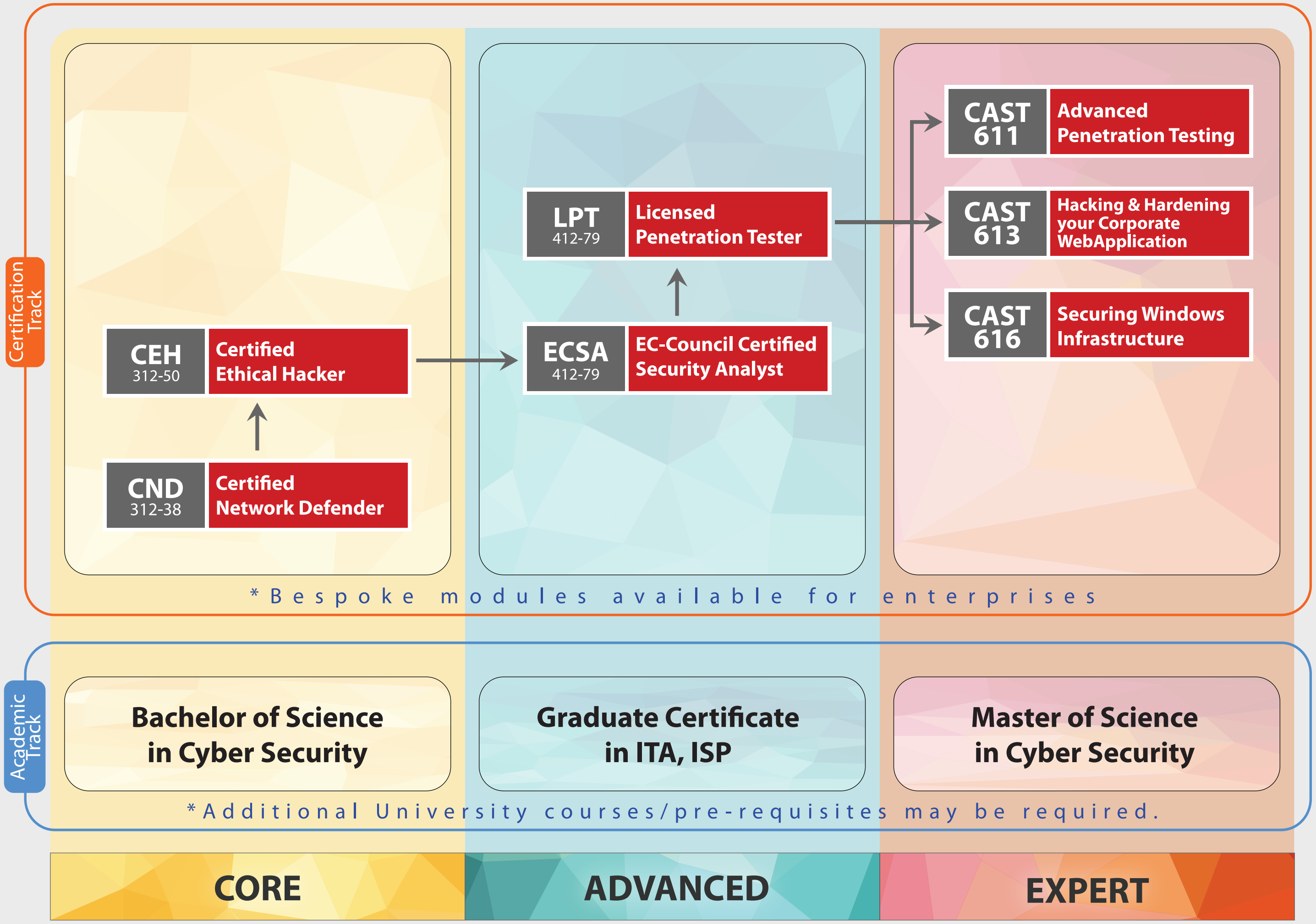
What will You Learn

- Cloud Security
- Password Security
- Social Engineering Countermeasures
- Mitigating Identity Theft
- Email Security
- Safe Browsing
- Data Protection
- Physical Security
- Mobile Device Security
- Data Backup
- 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 Microfinance Bank, Grant Thornton, IBM, PALADION, Poly technique, Unique Academy, Ministry of Defence, NTT Data, CIT Group of Institutions, happiest minds, ingenia, icddr,b, DCB Bank, vodafone, UNP, Reliance, core4 factory, Nestlé • • •

Vulnerability Assessment & Penetration Testing (VAPT)



Certification Track

CEH 312-50 Certified Ethical Hacker

CND 312-38 Certified Network Defender

ECSA 412-79 EC-Council Certified Security Analyst

LPT 412-79 Licensed Penetration Tester

CAST 611 Advanced Penetration Testing

CAST 613 Hacking & Hardening your Corporate WebApplication

CAST 616 Securing Windows Infrastructure

*Bespoke modules available for enterprises

Academic Track

Bachelor of Science in Cyber Security

Graduate Certificate in ITA, ISP

Master of Science in Cyber Security

*Additional University courses/pre-requisites may be required.

CORE

ADVANCED

EXPERT

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 CONSULTING.TECHNOLOGY.OUTSOURCING, Deloitte., NEC, bugcrowd, TATA, lastline, axiata, U.S. ARMY, Marriott, Hero

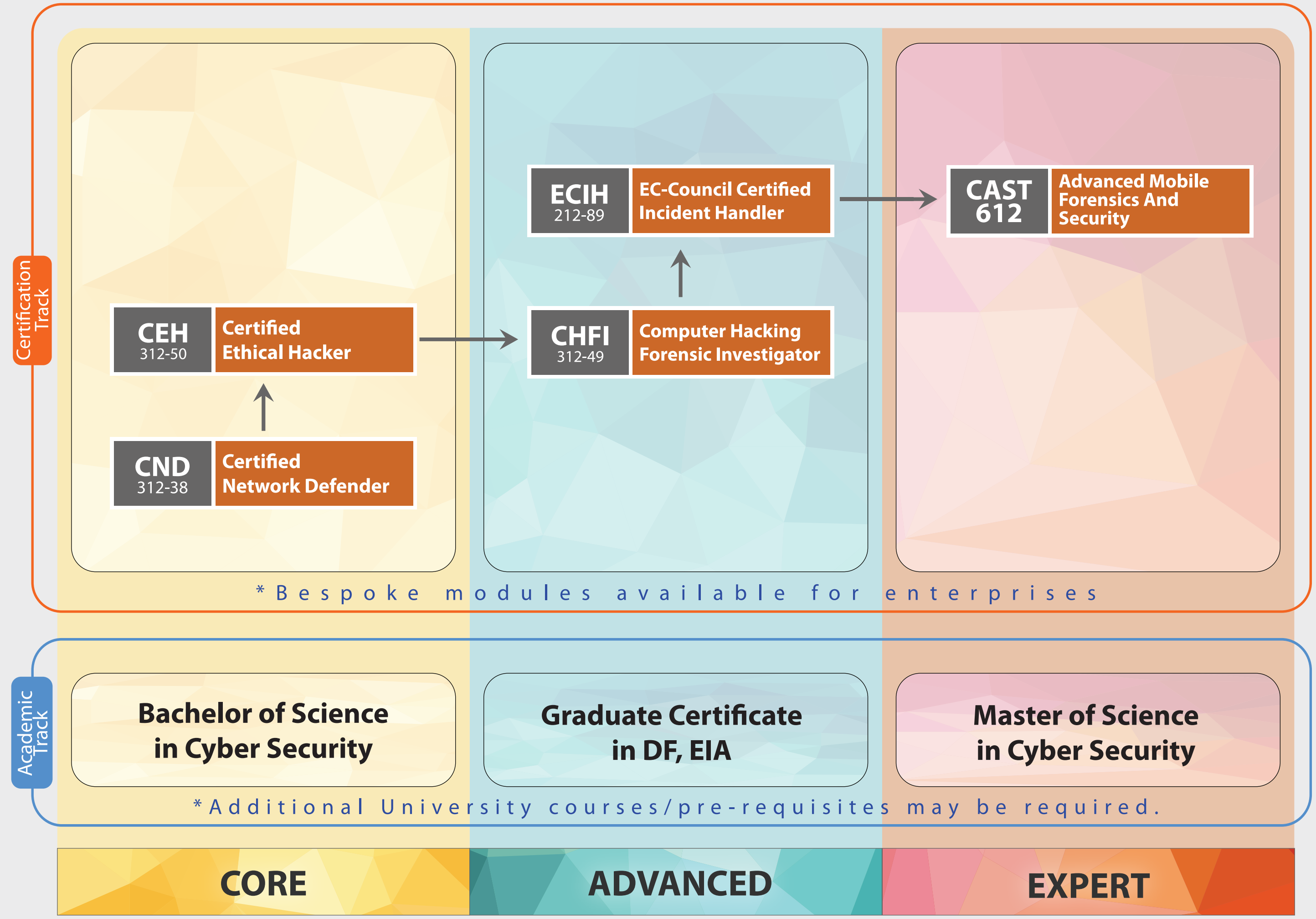
This Track Maps to NICE's Specialty Areas:

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)

Cyber Forensics


Certification Track

CEH 312-50 Certified Ethical Hacker

CND 312-38 Certified Network Defender

CHFI 312-49 Computer Hacking Forensic Investigator

ECIH 212-89 EC-Council Certified Incident Handler

CAST 612 Advanced Mobile Forensics And Security

*Bespoke modules available for enterprises

Academic Track

Bachelor of Science in Cyber Security

Graduate Certificate in DF, EIA

Master of Science in Cyber Security

*Additional University courses/pre-requisites may be required.

CORE

ADVANCED

EXPERT

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, h+k, BMC SWITZERLAND, BADAN INTELIJEN NEGARA REPUBLIK INDONESIA, Telkom Indonesia, LEXINGTON MEDICAL CENTER, pwc, du, HSBC, WIPRO Applying Thought, ...

This Track Maps to NICE's Specialty Areas:

1. Securely Provision (SP)
- a. Risk Management (RM)
- b. Test and Evaluation
- c. Systems Analysis (AN)

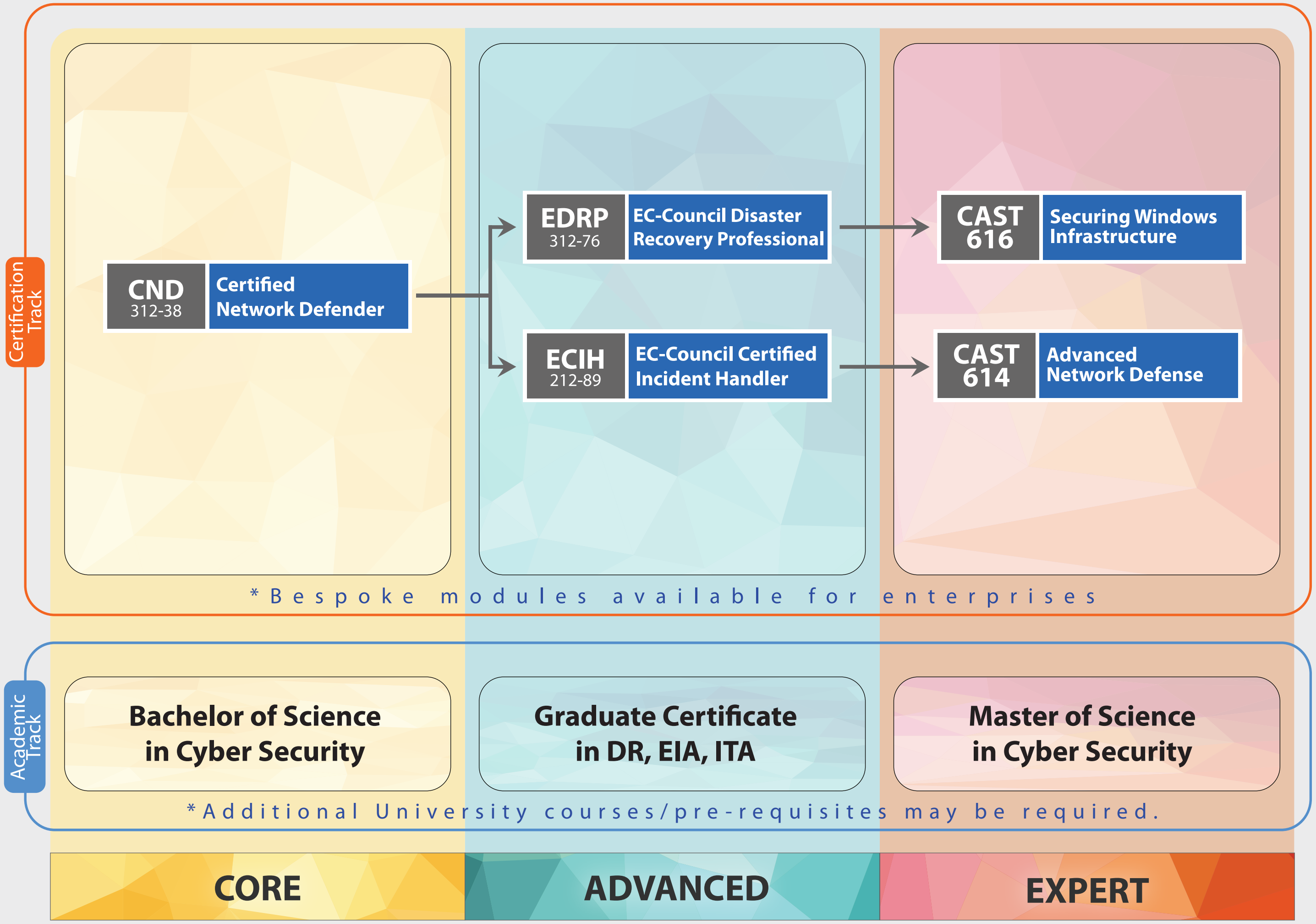
2. Operate and Maintain (OM)
- a. Network Services (NET)
- b. Systems Administration (SA)

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)

Network Defense and Operations



Certification Track

CND 312-38 Certified Network Defender

EDRP 312-76 EC-Council Disaster Recovery Professional

ECIH 212-89 EC-Council Certified Incident Handler

CAST 616 Securing Windows Infrastructure

CAST 614 Advanced Network Defense

* Bespoke modules available for enterprises

Academic Track

Bachelor of Science in Cyber Security

Graduate Certificate in DR, EIA, ITA

Master of Science in Cyber Security

* Additional University courses/pre-requisites may be required.

CORE

ADVANCED

EXPERT

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 بنك الخليج الأول, IBM, KPMG, DISA, mitra solusi telematika, Ameriprise Financial, COMCAST, Florida State University 1851, 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)

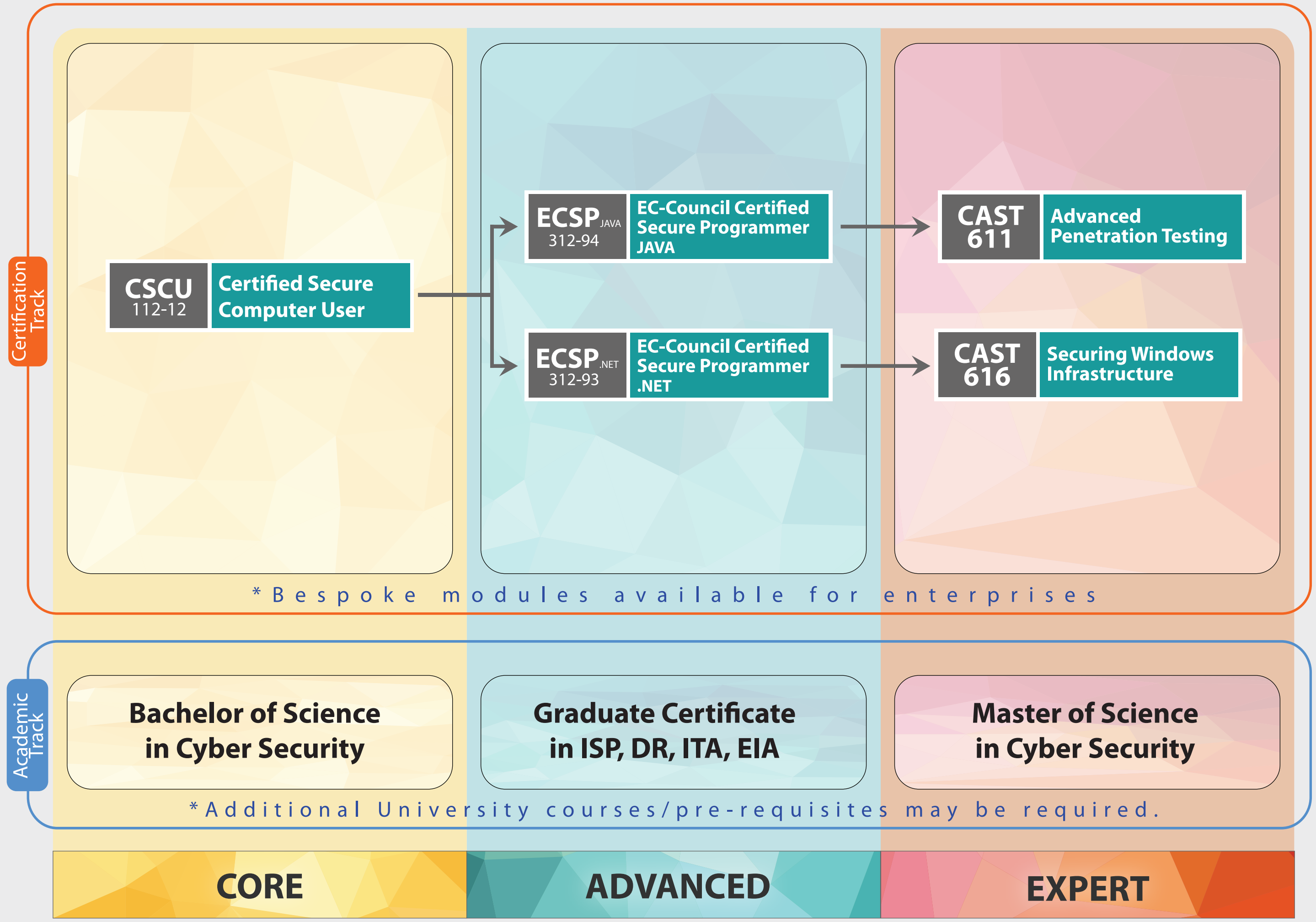
2. Operate and Maintain (OM)
- a. Network Services (NET)
- b. Systems Administration (SA)
- c. Systems Analysis (AN)

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)

Software Security



Certification Track

CSCU 112-12 Certified Secure Computer User

ECSP JAVA 312-94 EC-Council Certified Secure Programmer JAVA

ECSP .NET 312-93 EC-Council Certified Secure Programmer .NET

CAST 611 Advanced Penetration Testing

CAST 616 Securing Windows Infrastructure

*Bespoke modules available for enterprises

Academic Track

Bachelor of Science in Cyber Security

Graduate Certificate in ISP, DR, ITA, EIA

Master of Science in Cyber Security

*Additional University courses/pre-requisites may be required.

CORE

ADVANCED

EXPERT

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)

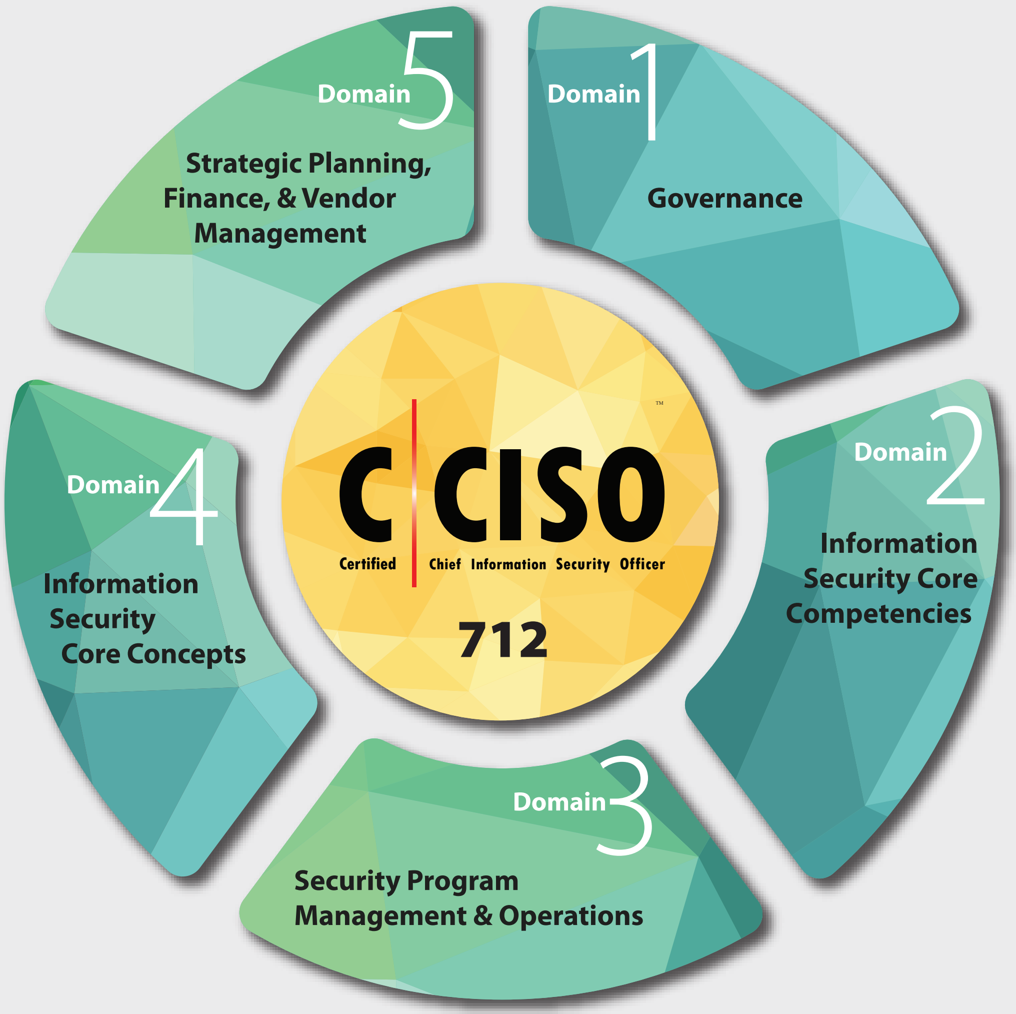
4. Protect and Defend (PR)
   a. Cybersecurity Defense Analysis (DA)
   b. Vulnerability Assessment and Management (VA)

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, Infoblox CONTROL YOUR NETWORK, KASPERSKY lab . . .

Governance



Domain 5
Strategic Planning, Finance, & Vendor Management
Domain 1
Governance
Domain 2
Information Security Core Competencies
Domain 3
Security Program Management & Operations
Domain 4
Information Security Core Concepts
C|CISO
Certified Chief Information Security Officer
712

Job Roles

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

Master of Science in Cyber Security

Graduate Certificate in:

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

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 City of New York
ARROW
Polycom
Rockwell Collins
تداول 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)

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 name: CSCU (112-12) exam
- Number of questions: 50
- Passing score: 70%
- Test duration: 2 Hours
- Test format: Multiple choice
- Test delivery: EC-Council exam portal

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 the cloud
- Securing network connections
- Data backup and disaster recovery

CND
Certified Network Defender

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: CND
- Exam code: 312-38
- Number of questions: 100
- Duration: 4 hours
- Availability: ECC exam
- Test format: Interactive multiple choice questions

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

CEH Certified Ethical Hacker™

Certified Ethical Hacker (CEH)

Course Description

CEH is the world's most advanced certified ethical hacking course that covers 18 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 counter measures
- Addresses emerging areas of cloud and mobile hacking
- Prepares you to combat Trojans, malware, backdoors and more
- Enables you to hack using mobile

Exam Information

- Number of questions: 125
- Test duration: 4 Hours
- Test format: Multiple choice
- Test delivery: ECC exam, VUE
- Exam prefix: 312-50 (ECC exam),
  312-50 (VUE)

Course Outline

- Introduction to ethical hacking
- Foot printing and reconnaissance
- Scanning networks
- Enumeration
- Sniffing
- System hacking
- Malware threats
- Social engineering
- Denial of service
- Session hijacking
- Hacking web applications
- SQL injection
- Hacking wireless networks
- Hacking web servers
- Hacking mobile platforms
- Evading IDS, Firewalls, and Honeypot
- Cloud computing
- Cryptography

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 CEH to next level by utilizing EC-Council's published penetration testing methodology.

Key Outcomes

- Introduce 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:

- Test format: Multiple choice
- Number of Questions: 150
- Passing Score: 70%
- Test Duration: 4 Hours

Penetration testing:

- Complete ECSA Practical Cyber Range Challenges in thirty Days
- Submit report within thirty Days completion of challenges
- Passing Criteria: 70 / 100 (Max)

Course Outline

- Security analysis and penetration testing methodologies
- TCP IP packet analysis
- Pre-penetration testing steps
- Information gathering methodology
- Vulnerability analysis
- External network penetration testing methodology
- Internal network penetration testing methodology
- Firewall penetration testing methodology
- IDS penetration testing methodology
- Web application penetration testing methodology
- SQL penetration testing methodology
- Database penetration testing methodology
- Wireless network penetration testing methodology
- Mobile devices penetration testing methodology
- Cloud penetration testing methodology
- Report writing and post-test actions

ECIH™
EC-Council | Certified Incident Handler

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

- Credit towards certification: ECIH 212-89 exam
- Test format: Multiple choice
- Test delivery: ECC exam, VUE

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

CHFI™ Computer Hacking Forensic INVESTIGATOR

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

- Number of Questions: 150
- Passing Score: 70%
- Test Duration: 4 hours
- Test Format: Multiple choice
- Test Delivery: ECC exam portal

Course Outline

- Computer forensics in today's world
- Computer forensics investigation process
- Understanding hard disks and file systems
- 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
- Data Acquisition and Duplication

ECSP JAVA™
EC-Council Certified Secure Programmer

EC-Council Certified Secure Programmer (ECSP) Java

Course Description

The **ECSP Java** program is a comprehensive course that provides hands-on training covering Java security features, policies, strengths, and weaknesses. It helps developers understand how to write secure and robust Java applications, and provides advanced knowledge in various aspects of secure Java development that can effectively prevent hostile and buggy code.

Key Outcomes

- Introduces Java security architecture and common security threats
- Secure software development lifecycle (SDLC)
- Common threats and mitigation approaches
- Detailed coverage of input validation, output encoding, authentication and authorization, and other secure coding practices
- Thorough understanding of Sandbox, JVM, Bytecode Verifier, Security Manager, and JSF (Java Security Framework)

Exam Information

- Number of questions: 50
- Passing score: 70%
- Test duration: 2 Hours
- Test format: Multiple choice
- Test delivery: EC-Council exam center
- Exam prefix: 312-94

Course Outline

- Java security principles and secure coding practices Java Security Platform, Sandbox, JVM, Class loading, Bytecode verifier, Security Manager, security policies, and Java Security Framework
- Secure SDLC, threat modelling, software security frameworks, and secure software architectures
- Best practices and standards and guidelines for secure file input/output and serialization
- Java input validation techniques, validation errors, and best practices
- Java exceptions, erroneous behaviors, and the best practices to handle or avoid them
- Secure authentication and authorization processes
- Java Authentication and Authorization Service (JAAS), its architecture, Pluggable Authentication Module (PAM) Framework, and access permissions through Java Security Model
- Secure Java concurrency and session management
- Core security coding practices of Java Cryptography that includes Encryption, Key Generator and implementation of Cipher Class,
- Digital signatures, secret keys, and key management
- Various Java application vulnerabilities

ECSP .NET
EC-Council Certified Secure Programmer

EC-Council Certified Secure Programmer (ECSP) .Net

Course Description

The **ECSP .Net** program covers identification of security flaws and implementation of security countermeasures throughout the software development lifecycle to improve the overall quality of products and applications. This course is purposefully built with a number of labs with three days of training, offering participants critical hands on time to fully grasp the new techniques and strategies in secure programming.

Key Outcomes

- Introduces .Net security architecture and common security threats
- Secure software development lifecycle (SDLC)
- Common threats and mitigation approaches
- Detailed coverage of input validation, output encoding, authentication and authorization, and other secure coding practices

Exam Information

- Number of questions: 50
- Passing score: 70%
- Test duration: 2 Hours
- Test format: Multiple choice
- Test delivery: EC-Council exam center
- Exam prefix: 312-93

Course Outline

- .Net Application Security, ASP.Net Security Architecture common security threats to .Net framework
- Security attacks on .Net framework and Secure SDLC
- Common threats to .Net assemblies and stack walking processes
- Input validation
- Authorization and authentication processes and common threats
- Various security principles for session management
- Importance of cryptography in .Net, different types of cryptographic attacks in .Net
- Symmetric and asymmetric encryption, hashing concepts, digital certificates, digital and XML signatures
- Principles of secure error handling, different levels of exception handling, and various .Net logging tools
- File handling concepts

EC-Council Licensed Penetration Tester (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

Hands-on Challenge

- Penetration testing of LPT Practical Cyber Range with ten challenges
- Complete challenges in five Days from day of activation
- Submit report within thirty Days of activation
- Passing Criteria: 70 / 100 (Max)

Testimonials

"My overall experience was really good and taught me great skills. LPT (Master) is a must for every cyber security specialist and I guarantee it's worth a try"

Adithya Naresh

"A certification is always a nice thing to show to other parties, but when you have a credential like the LPT (Master), you can proudly say that this is just not another multiple-choice exam. It proves that you can actually do an end-to-end penetration test of world-class quality!"

Ali Isikli

"The LPT (Master) certification allows people like me to speak from a sense of authority. When presenting penetration testing results to clients you have a sense of security that what you are saying is accurate and real when you are backed up by a certification such as this."

Mark Horvat

"The ECSA program also gave me the correct professional experience in how to interact with my customers in a professional manner before, during, and after completing my service to them."

Moustafa Mohamed Mohsen

CAST

Center for Advanced Security Training

CAST 611 - Advanced Penetration Testing

Course Description

The **CAST 611– Advanced Penetration Testing** is a specialized training program covering key information security domains, at an advanced level. Students completing this course will gain in-depth knowledge about information gathering, scanning, enumeration, exploitation and post exploitation, data analysis and reporting, and a number of advanced techniques.

Key Outcomes

- Introduces a comprehensive process for a security test, producing findings and report for an enterprise class setting
- Complemented with Cyber Ranges that progresses in difficulty and reflect an enterprise level architecture, with defenses to defeat and challenges to overcome
- Exposure to evasion techniques

Exam Information

- Based on practical results
- 60 questions
- 75 minutes
- Open book, note and access to range is allowed during the test
- 70% minimum required to pass

Course Outline

- Information gathering and OSINT
- Scanning
- Enumeration
- Vulnerability analysis
- Exploitation
- Post exploitation
- Advanced techniques
- Data analysis and reporting

CAST
Center for Advanced Security Training

CAST 612 – Advanced Mobile Forensics and Security

Course Description

The **CAST 612 – Advanced Mobile Forensics and Security** focuses on what today's mobile forensics practitioner requires. Some of the advanced areas this course covers are the intricacies of manual acquisition (physical vs. logical) and advanced analysis using reverse engineering, understanding how the popular Mobile OSs are hardened to defend against common attacks and exploits.

Key Outcomes

- Advanced concepts of forensic imaging of mobile devices, including logical, file, and storage system
- Data carving and analysis
- Bypassing pattern and password locks
- Reverse engineering of Apps and DB analysis

Exam Information

- Onsite workshop

Course Outline

- Mobile forensics challenges
- Mobile forensics process
- Mobile hardware design and architectures
- Mobile OS architecture, boot process, and file systems
- Mobile threats and security
- Mobile evidence acquisition and analysis
- Mobile application reverse engineering
- Mobile forensics reporting and expert testimony

CAST
Center for Advanced Security Training

CAST 613 – Hacking and Hardening Corporate Web Apps

Course Description

The **CAST 613 – Hacking and Hardening Corporate Web Apps** is a course designed with the average security unaware programmer in mind. The course is designed with more than 50% involving hands-on coding labs. The ideal participant should have a development background, coding, or architecting background either currently or previously.

Key Outcomes

- Advanced techniques of hacking and hardening a Website/Web App
- Key concepts of cryptography, TLS, user account management, and session management
- Reducing the attack surface with disclosure controls as well as mitigation of XSS, SQLi, and CSRF, etc.

Exam Information

- Exam Title: CAST 613 - Hacking and Hardening your Corporate Web Application
- Exam Code: CAST613
- Number of Questions: 50
- Duration: 2 hours
- Availability: EC-Council Exam Portal
- Passing Score: 70%

Course Outline

- Cryptography decryption
- Account management
- Parameter diddling
- Transport layer protection
- Cross site scripting
- Cookies
- Internal implementation disclosure
- SQL injection
- Cross site attacks

CAST
Center for Advanced Security Training

CAST 614 – Advanced Network Defense

Course Description

The **CAST 614 – Advanced Network Defense** will enable you to evaluate advanced hacking methods of defense fortification, bringing you closer to establishing perfect security best practices and methodologies you can apply to secure environments. It will cover fundamental areas of fortifying your defenses by discovering methods of developing a secure baseline and hardening your enterprise architecture from the most advanced attacks.

Key Outcomes

- Get introduced to concepts of advanced firewall controls and hardening of systems
- Understand intrusions, detection and prevention
- Defending web applications, end points, and critical infrastructure systems

Exam Information

- Onsite workshop

Course Outline

- Firewalls
- Advanced filtering
- Firewall configuration
- Hardening: establishing a secure baseline
- Intrusion detection and prevention
- Protecting web applications
- Memory analysis
- Endpoint protection
- Securing wireless

CAST
Center for Advanced Security Training

CAST 616 – Securing Windows Infrastructure

Course Description

The **CAST 616 – Securing Windows Infrastructure** focuses on the key aspects of Windows Infrastructure Security. It is designed with the single purpose of providing infosec professionals complete knowledge and practical skills necessary for ensuring the security of their network infrastructure, that is fast becoming, if already not, a top priority and a major challenge for most organizations.

Key Outcomes

- Key aspects of Windows infrastructure security
- Architecture and its interconnected nature in an enterprise system
- Application of best practices to secure with a holistic framework

Exam Information

- Three-day technical workshop

Course Outline

- Windows 7 & 8 hardening
- Windows Server 2008 R2 / Windows Server 2012 hardening
- Hardening Microsoft network roles
- Windows high availability
- Data and application security
- Monitoring, troubleshooting and auditing Windows
- Automating Windows hardening
- Organizational security

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

- Number of questions: 50
- Test duration: 2 hours
- Test format: Multiple choice
- Test delivery: ECC exam portal

Course Outline

- Introduction to disaster recovery and business continuity
- Nature and causes of disasters
- Emergency management
- Laws and acts
- Business continuity management
- Disaster recovery planning process
- Risk management
- Facility protection
- Data recovery
- System recovery
- Backup and recovery
- Centralized and decentralized system recovery
- Windows data recovery tools
- Linux, Mac and Novell Netware data recovery tools
- Incident response
- Role of public services in disaster
- Organizations providing services during disasters
- Organizations providing disaster recovery solutions
- Case studies

C|CISO Certified Chief Information Security Officer

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

- Exam Format : Multiple Choice
- Total number of questions : 150
- Exam duration : 2.5 Hours
- Required passing score : 72%

Course Outline

- Governance
- Security risk management, controls, and audit management
- Security program management and operations
- Information security core concepts
- Strategic planning, finance, and 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
- ENG 340 English communications
- 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 and 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

Courses

- Information security professional
  - ECCU 500 Managing secure network systems
  - ECCU 501 Ethical hacking and Countermeasures
  - ECCU 505 Research and writing for the IT practitioner
  - Digital forensics
  - Disaster recovery
  - Executive information assurance
  - IT Analyst

EC-COUNCIL UNIVERSITY
ACCREDITED. FLEXIBLE. ONLINE.

Master of Science in Cyber Security (MSS)

Course Description

The **Master of Science in Cyber Security (MSS)** 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 and 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

www.eccouncil.org