www.syntechnx.com

TABLE OF CONTENTS

WHO AND WHAT WE TEACH

Credibility and trust play a critical role in determining how organizations choose their cyber-security personnel and providers.

Here at the SynTechNX Institute, we call our graduates cyber-security 'soldiers' because they are the most thoroughly battle-tested cyber-security graduates in the world. We use the soldier moniker because of the discipline and dedication required to drill through our training process and become a certified graduate (i.e., "boot camp").

The cyber-security challenges against all manners of attack, are growing exponentially every year, worldwide. From disgruntled employees or customers, to for-profit criminals, to corporate espionage to cyber-terrorists or government intrusion, we take pride in our graduates being cyber-security soldiers akin to the military equivalent of Army Rangers or Navy Seals.

SynTechNX Institute is fully dedicated to remaining cutting edge and up-to-date with the security challenges faced by all organizations today, which includes the frequency, complexity and distributed nature of attacks, and the lack of resource capacity and technical capability most organizations have to deal with these threats in a satisfactory manner.

The knowledge and experience SynTechNX Institute's experts and instructors have gained over the years make us the obvious choice for any IT professional that wishes to take Information Security seriously in a constantly dynamic world, where information is a prized commodity and cyber threats are the new enemy.

As with any higher learning organization, success is our ultimate goal. This means we believe that our success will only be measured in the quality of the service that our future graduates provide their employers and/or clients.

Our aim is to ensure that our graduates can counter any type of attack against that base and deliver a level of expertise and professionalism that is second to no other.

Welcome future cyber-security experts to SynTechNX Institute!

IMPORTANCE OF CYBER-SECURITY

Our Experience Works for You

Our experts establish, train and guide entire cyber units for varios sectors, leveraging the SynTechNX Groups vast operational experience and the in-depth knowledge of the Philippine nations TOP experts from diverse cyber realms.

To learn more about our Cyber Project, download….

A company data breach could cost millions of dollars and jeopardize the entire business. Investing in cyber-security awareness training for employees is important for every team member, and taking SynTechNX's courses could save you an enormous amount of time and money in the long run.

CYBER-SECURITY

Almost every action we take in modern life takes place, wholly or partly, in cyberspace. Our personal data and general preferences are scattered across the internet, assumed to be protected by complex mechanisms and entangled codes until they don't. The Cyber studies program trains students to understand the challenges posed by advanced technology, providing them with the tools to identify threats and manage them in manners of technological abilities and crisis management skills.

The world is now more reliant on technology than ever before. The emergence and growth of technology has had a positive impact on human life, but the convenience has, however, come with the risk of cyber attacks. If you use a tech device for whatever reason, then you're highly likely to be exposed to a cyber attack. You'll need to be protected, and that's where cyber security comes in.

Cyber security is the protection of electronic data and information. It's the defense of electronic systems on devices, like computers, cell phones, servers, and networks, from malicious attacks. Regardless of who you are, it's important to keep your data safe from unauthorized access.

Here are some reasons why cyber security is crucial:

1.There are different types of cyber attacks

No one is safe from the threat of cyber attacks. These attacks include malware, phishing, man-in-the-middle, and drive-by attacks. Scary right? Wait till you hear about crypto-jacking. This is where criminals could compromise your computer and use it to steal resources, such as Bitcoins and other digital currencies. If they can get to your computer, then they could easily steal your data. You need cyber security if you want to stand a chance against these threats.

2.Increase in cybercrimes

The fast development of technology, such as fast broadband, better gadgets, and cloud computing, has led to an increase in the number of connected devices. According to some surveys, there'll be about 21.1 billion networked devices in the world in 2021. This, with the development of the dark web, has created a fertile ground for cybercrime activities. Cyber security can, nonetheless, minimize your exposure. This link explains some ways of reducing risk in organizations.

3.Tech users are vulnerable

The fact that almost everyone on this planet is now more reliant on information and communication technology means, for cybercriminals, that there's a booming criminal opportunity. Factors like the enhancement of cloud storage and social media growth have left many exposed to cyber attacks. This makes cyber security more important than ever.

4.Cloud storage needs protection

Sensitive information, like banking details and passwords, can now be stored on the cloud, increasing their risk of theft. Also, the growth of social media has led to an increase in identity fraud. The truth is that whether you're an individual, a small business, a large organization, or even a government, you're at risk of being targeted for cybercrime. You may, therefore, want to consider cyber security.

5.It could save millions of dollars

According to recent studies, the average cost of cybercrimes for an organization was about USD$13 million last year. Research also revealed a sharp increase in information breaches, including financial information, health records, trade secrets, personal data, and intellectual property. You'd rather pay a little for cyber security and save big on your organization's protection than lose a fortune through industrial espionage.

6.Enables credibility

Cyber attacks often make online platforms, like websites, unpleasant or inaccessible. That could result in a bad reputation, which might be difficult to undo. Cyber security is, hence, important for the protection of your platform from such risks. It could also help protect customers from potential hackers.

7.Viruses can harm you or business

Computer viruses can spread like wildfire. These could cause severe problems for you and your business if not controlled. Computer viruses are capable of corrupting your files and systems. It's essential, therefore, to take cyber security seriously as it could save your computer systems from viruses.

8.The dark web

Technology has developed, so has the dark web strengthened its sophistication. It has provided a haven for cybercriminals and resulted in an increased threat on surface Internet use. These vulnerabilities have heightened the significance of cyber security. Our certification programs are recognized worldwide and have received endorsements from various government agencies including the US Federal Government via the Montgomery GI Bill, and the US Government National Security Agency (NSA) and the Committee on National Security Systems (CNSS) certifying EC-Council's Certified Ethical Hacking (CEH), Network Security Administrator (ENSA), Computer Hacking Forensics Investigator (CHFI), Disaster Recovery Professional (EDRP), Certified Security Analyst (E|CSA) and Licensed Penetration Tester(LPT) program for meeting the 4011, 4012, 4013A, 4014, 4015 and 4016 training standards for information security professionals and most recently EC-Council has received accreditation from the American National Standards Institute (ANSI).

CYBER SECURITY SALARY RATE

Information Security Manager

According to our 2019 Tech & Digital Marketing Salary Guide, this role tops the list of highest-paid cyber-security jobs with an average salary range of $125,000 to $215,000. Information Security Managers play a key role in avoiding security disasters by identifying any areas that might make your information systems vulnerable. These are the professionals who are tasked with assessing current security measures and mitigating future attacks against your company's computers, networks, and data.

Cyber-security Engineer

The Cyber-security Engineer position also nets one of the highest salaries in the security industry, with average cyber-security salaries ranging from $120,000 to $200,000. Companies invest in these professionals for their skill sets and experience as they are primarily responsible for multiple security engineer functions, including designing, developing, and implementing secure network solutions to defend against advanced cyberattacks, hacking attempts, and persistent threats.

Application Security Engineer

Another one of the highest-paid cyber-security jobs, Application Security Engineers, make on average between $120,000 to $180,000. If your company uses software solutions provided or hosted by third party organizations like AWS or Microsoft's Azure or even if you custom build your own solutions, hiring an Application security engineer is crucial. These professionals will be tasked with securing all software and business applications used throughout your workforce and ensuring that all privacy and compliance constraints are built into the software and followed.

Cyber-security Analyst

The average cyber-security salary for this position falls between $90,000 and $160,000, and they are worth every penny. These security professionals help create, plan, and carry out security measures to keep your infrastructure secure. They have the knowledge and experience to work with Penetration Testers and Information Security Managers to mitigate and avoid cyber attacks that could cripple your bottom line and are especially equipped to identify vulnerabilities before hackers have a chance.

Penetration Tester

Penetration Testers, commonly called Pen Testers or Ethical Hackers, on average, make between $80,000 to $130,000. A McAfee survey showed that security managers believe hiring ethical hackers offers a company a valuable understanding of logic used by hackers and skills critical to cyber-security . Does your company conduct quarterly, monthly, or daily security tests? If so, then these are the professionals you need to invest in attracting and retaining. Penetration Testers complete various, in-depth tests across your computer systems, networks, and even web applications to identify vulnerabilities that can be exploited by cybercriminals.

Network Security Engineer

Rounding out this list of the highest-paid cyber-security jobs, the average salary for the Network Security Engineer role now ranges between $125,000 to $185,000. Much like the Cyber-security Engineer position, this is a multifaceted position; tasked with maintaining your LAN, WAN and server architecture while also maintaining and monitoring virtual networks, firewalls, email security and web protocols, security, and programs. When it comes to a business's computer network, you can never be too secure, and this role helps guarantee your company's network is safe and secure.

COURSE LIST & COURSE TRACKS

COURSE LIST	DURATION	CERTIFYING BODY
Cyber-security in-depth course – Mandatory for all students	12 Weeks	SynTechNX

COURSE LIST	DURATION	CERTIFYING BODY
Certified Blockchain Professional - CBP	Week 1	EC-Council
Certified Chief Information Security Officer - CCISO	Week 2	EC-Council
Certified Ethical Hacker - CEH	Week 3	EC-Council
Certified Incident Handler - ECIH	Week 4	EC-Council
Certified Network Defender - CND	Week 5	EC-Council
Certified Penetration Testing Professional - CPENT	Week 6	EC-Council
Certified Project Management - CPM	Week 7	EC-Council
Certified Secure Computer User - CSCU	Week 8	EC-Council
Certified SOC Analyst - CSA	Week 9	EC-Council
Computer Hacking Forensics Investigator - CHFI	Week 10	EC-Council

Your Learning Options

Instructor-led Training
SynTechNX has a certified trainer to deliver the entire EC-Council program from a training facility in your city.

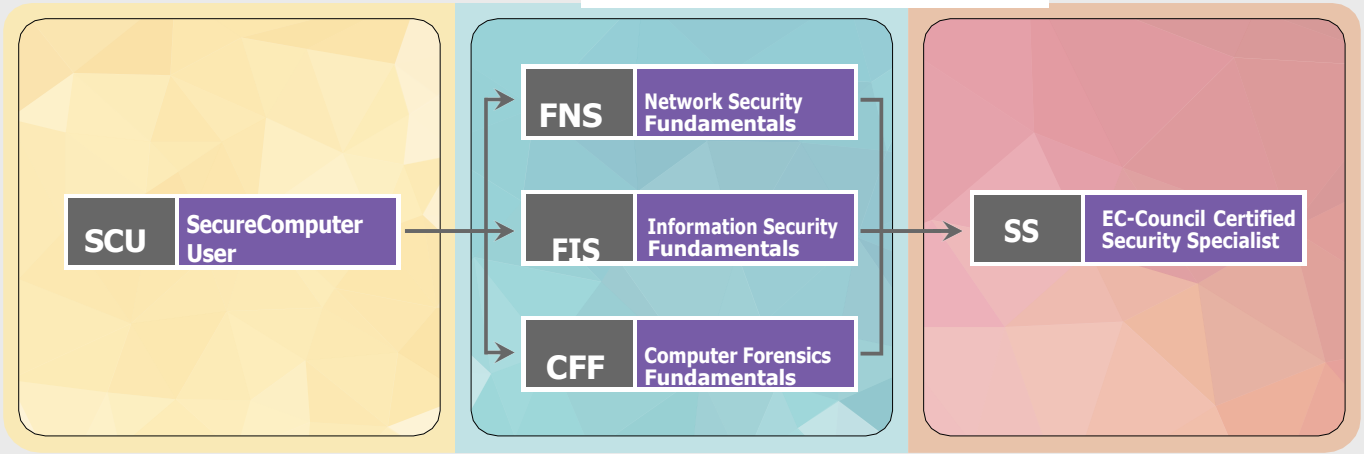
Online Learning
iLearn online training is a distance learning program designed for those who cannot attend a live course. The program is for the people who have a very busy schedule and want to learn at their own pace through self-study. This modality is also available from our enterprise teams.

Computer-based Training
For people who work in secure facilities with limited or no access to the internet, we o er 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 Cyber Range (iLabs)
SynTechNX offers EC-Council iLabs that 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.

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

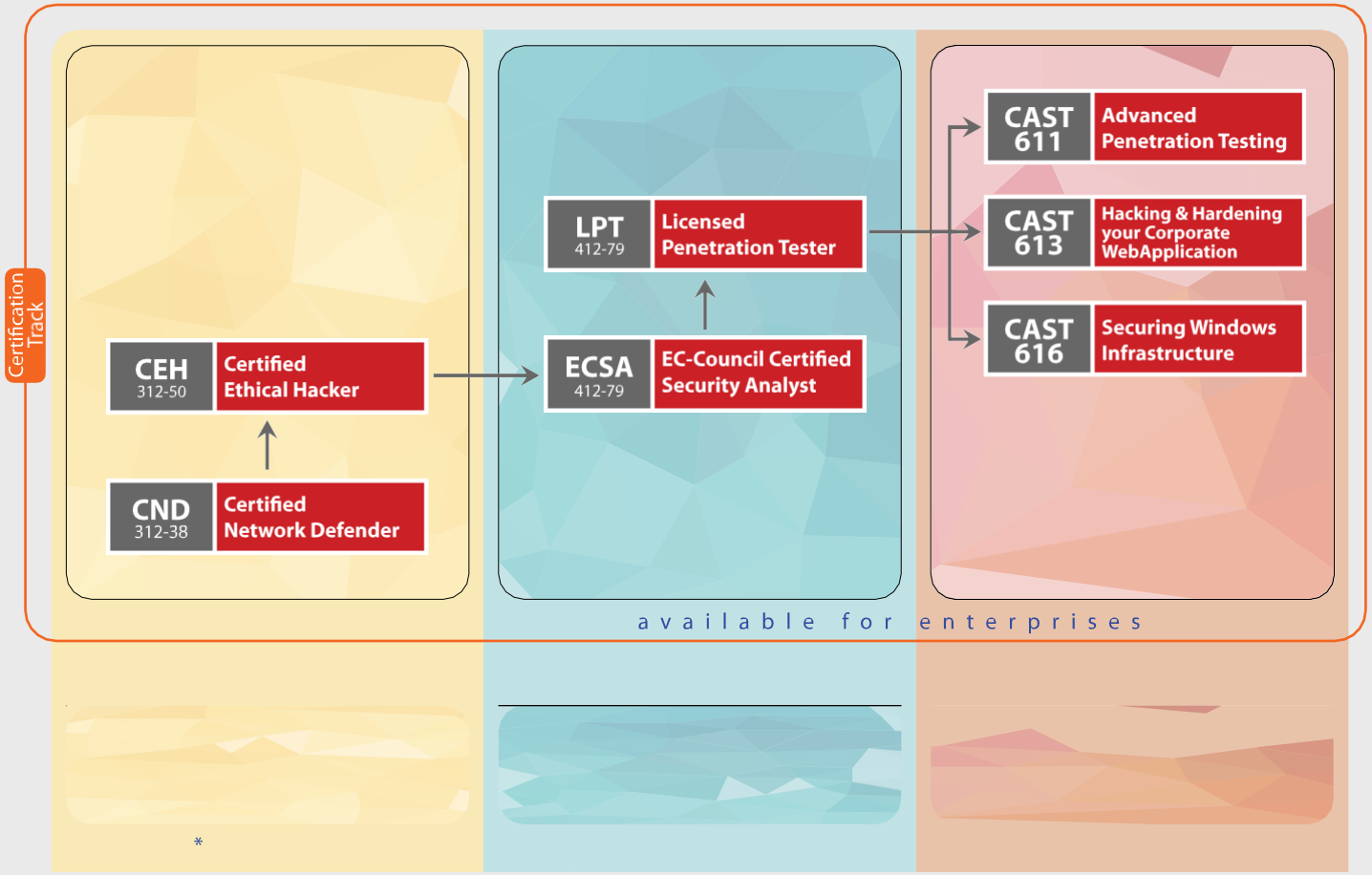


Target Audience

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

Our Graduates Professionalsare employed at:

VulnerabilityAssessment & Penetration Testing (VAPT)



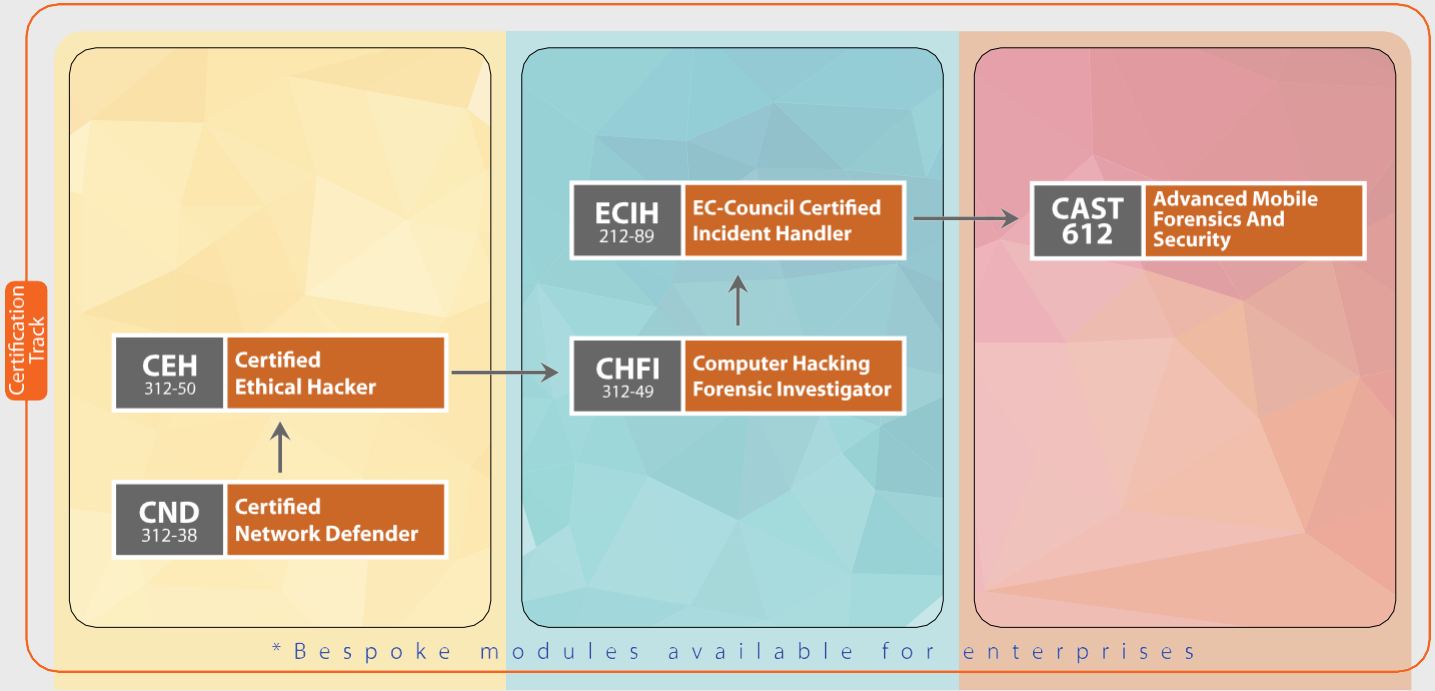
Job Roles

- 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 Graduates Professionals are employed at:

cisco, EY, Microsoft, accenture, Infosys, amazon, AIG, hp, Bank of America, Booz | Allen | Hamilton, Capgemini, Deloitte., NEC, bugcrowd, TATA, lastline

Cyber Forensics



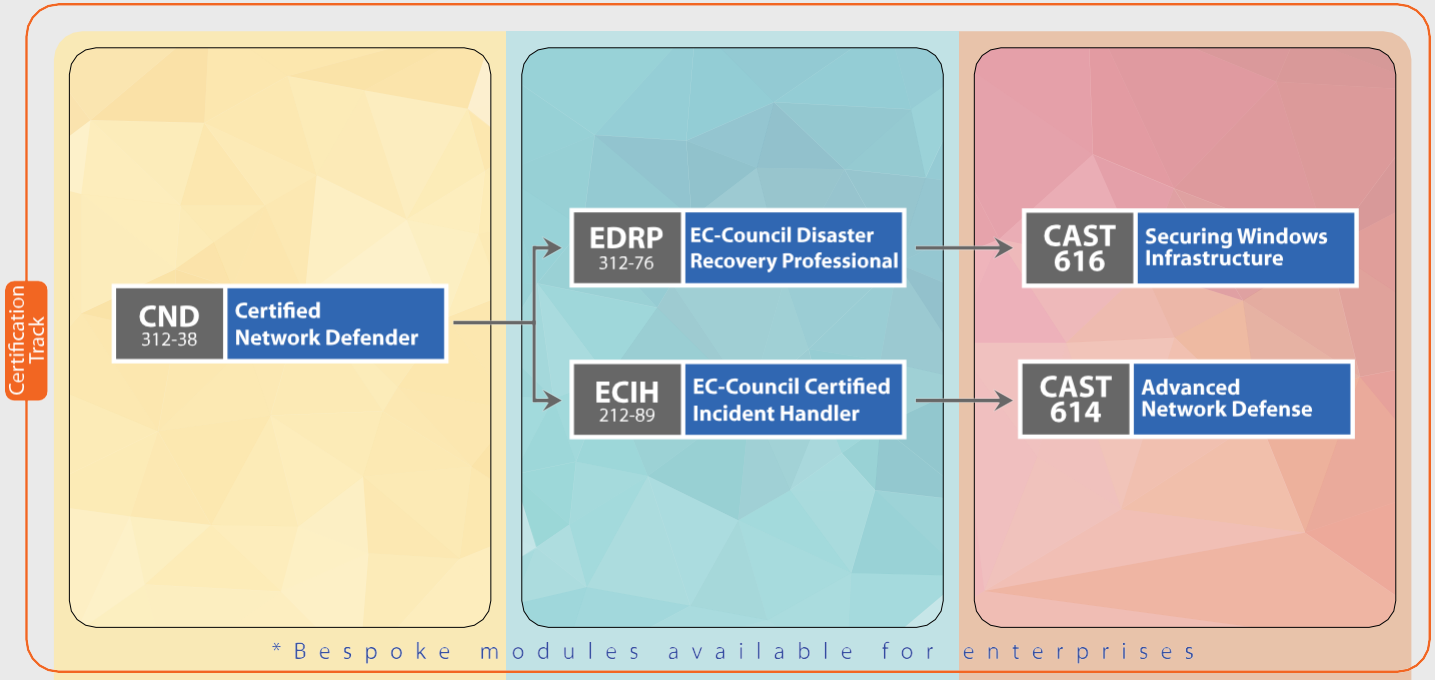
Job Roles

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

Our Certified Cyber Forensic Professionals are Employed at:

BARCLAYS, AIG, Infosys, U.S. ARMY, ICICI Bank, Bank of America, HDFC BANK, BMC SWITZERLAND, LEXINGTON MEDICAL CENTER, pwc

Network Defense and Operations

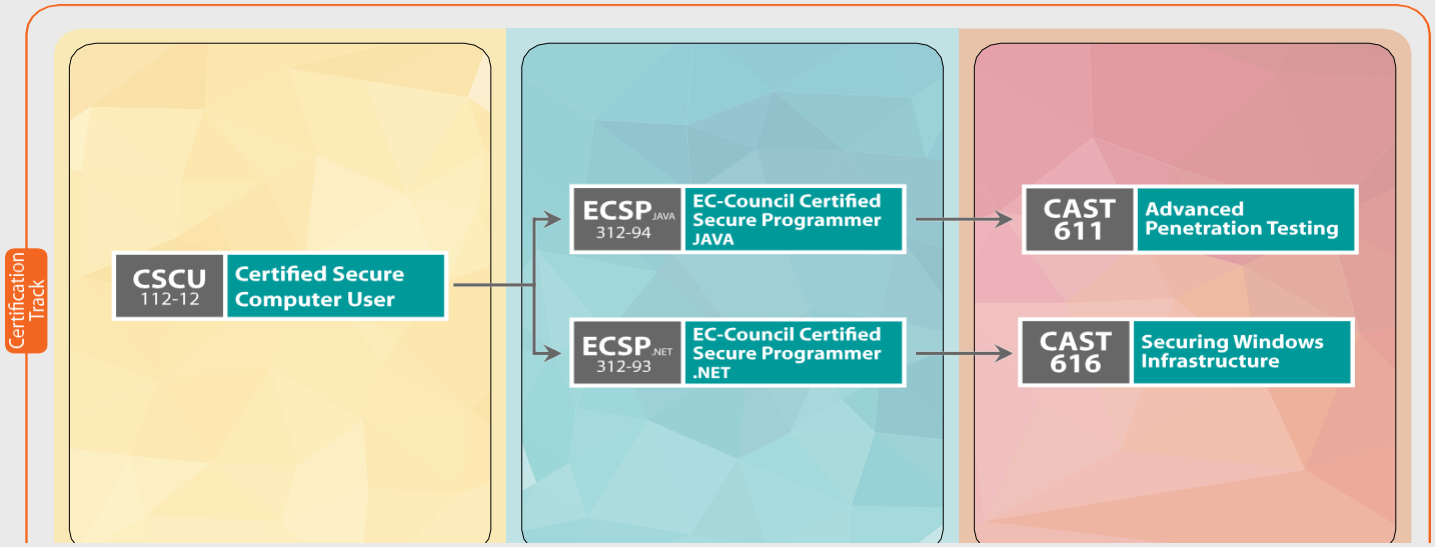


Job Roles

- 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:

Software Security



JobRoles

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

Our Graduates 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

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.

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

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

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, andrespond 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

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

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 informationsecurity posture of their organization.

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

Key Outcomes

- Thorough introduction to ethical hacking
- Exposure to threat vectors and counter measures
- Addresses emerging areas of cloud andmobile hacking
- Prepares you to combat Trojans, malware, backdoors and more

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

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, networkpenetration testing from external and internal evading firewalls and ids

Course Outline

- Security analysis and penetration testingmethodologies
- TCP IP packet analysis
- Pre-penetration testing steps
- Information gathering methodology
- Vulnerability analysis
- External network penetration testingmethodology
- Internal network penetration testingmethodology
- Firewall penetration testing methodology
- IDS penetration testing methodology

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 attackthreats.

Course Outline

- Introduction to incident response andhandling
- 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

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 conductassessments

Computer Hacking and Forensic Investigator (CHFI)

Course Description

CHFI is a comprehensive course covering major forensic investigation scenarios, enabling students toacquire 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 investigationprocess
- Forensics of file systems, operating systems,network and database, websites, and email systems
- Techniques for investigating on cloud,malware, and mobile

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

Licensed Penetration Tester (LPT)

Course Description

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

Key Outcomes

LPT Demonstrates

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

Course Outline

- Understanding hard disks and file systems
- Network forensics
- Investigating web attacks
- Database forensics
- Cloud forensics

1

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 informationsecurity management.

Key Outcomes

- Establishes the role of CISO and models forgovernance
- Core concepts of information security controls, risk management, and compliance

Course Outline

- Governance
- Security risk management, controls, andaudit management
- Security program management andoperations
- Information security core concepts
- Strategic planning, finance, and vendormanagement

TESTIMONIAL

"My IT-department just finished training at SynTechNX, I definitely would recommend SynTechNX Training Institute and would encourage students to study hard and inform themselves as much as possible about the several academic opportunities the Institution offers. SynTechnx takes the educational mission to heart, here you will find people that will support you and guide you on the path to your Cyber-security."

Alexander L.

IT marketing head ASEAN region.

"Most of my employees has the best skillet in Cyber security, when you check on their background, most of the trained at SynTechnx Training Institute. The training at SynTechNX definitely it is top of the line"

Alexander L.

South East Asia Information Systems chairman

"As a young CEO, I always look for the best skillet available; SynTechNX has always produced and assisted my company to get their top cream cyber-security engineers "

Derrick R.

ASEAN strategic IT officer