EC-Council Certified Incident Handler

Courseware

EC-Council

EC-Council New Mexico
101C Sun Ave NE
Albuquerque, NM 87109

NOTICE TO THE READER

Foreword

A dramatic upsurge in cyber threat incidents has taken place in recent times. Nowadays, most organizations are concerned about data breaches that occur due to targeted cyberattacks, malware campaigns, zero-day vulnerabilities, and ransomware attacks. The WannaCry and Petya/NotPetya ransomware attacks in 2017 and SamSam ransomware attacks in 2018 reminded the entire global cybersecurity community that cyber threats can surprise organizations at any moment and may arise from unexpected sources. According to the *Sophoslabs 2019 Threat Report*, SamSam ransom payments reached a total of $6.5 million by November 2018. This very thorough ransomware attack significantly raised the stakes for companies by charging ransoms from $10,000 to more than $50,000, per attack; and this is far from being the only example: Apart from SamSam, other ransomware attacks like BitPaymer, Ryuk, Dharma, GandCrab, and so on have created havoc in the global arena.

Some organizations have the resources and skills to protect their IT infrastructure against such threats. However, many organizations still lack the ability to appropriately handle cyberattacks. It does not matter if an organization installs state-of-the-art security software solutions or spends thousands of dollars on security mechanisms; the fact remains that no organization is completely secure. To better defend itself, an organization must be aware of the possibility of such an attack before one actually takes place—and must also be well equipped to handle such incidents effectively. This is where the incident handling and response process comes into play. An effective cyber defense policy requires skilled incident handling and response personnel who can not only detect the incidents but also contain them rapidly and eradicate them completely. Security incursions are inevitable, so organizations need incident handlers who can prepare security policies and plans in order to tackle incidents appropriately and efficiently to reduce their impact.

EC-Council Certified Incident Handler (ECIH) is a well-regarded cyber security incident response training program that teaches a structured approach to effective incident handling and response.

In the current complex and ever-changing threat landscape, ECIH is an essential program for those who deal with security incidents on a daily basis. The course addresses various underlying principles and techniques for detecting and responding to both current and emerging cyber security threats. Students will learn how to handle various types of incidents, risk assessment methodologies, and the assorted laws and policies related to incident handling. After completing the course, students will be able to create incident handling and response policies and deal with different types of security issues such as malware incidents, email security incidents, network security incidents, web application security incidents, cloud security incidents, and insider threat-related incidents. In addition, students will learn about computer forensics and its role in handling and responding to incidents. The course also covers incident response teams, incident reporting methods, and incident recovery techniques in detail.

About EC-Council

The International Council of Electronic Commerce Consultants, better known as EC-Council, was founded in late 2001 to address the need for well-educated and certified information security and e-business practitioners. EC-Council is a global, member-based organization composed of industry and subject matter experts working together to set the standards and raise the bar in information security certification and education.

EC-Council first developed the Certified Ethical Hacker (CEH) program with the goal of teaching the methodologies, tools, and techniques used by hackers. Leveraging the collective knowledge of hundreds of subject-matter experts, the CEH program has rapidly gained popularity around the world and is now delivered in more than 145 countries by more than 950 authorized training centers. Considered the benchmark for many government entities and major corporations around the globe, more than 200,000 information security practitioners have been trained through CEH.

Shortly after launching CEH, EC-Council developed the Certified Security Analyst (ECSA) program. The goal of the ECSA program is to teach groundbreaking analysis methods to be applied while conducting advanced penetration testing. The ECSA program leads to the Licensed Penetration Tester (LPT) certification. The Computer Hacking Forensic Investigator (CHFI) program was developed using the same design methodologies and has become a global standard in certification for computer forensics. EC-Council, through its impressive network of professionals and huge industry following, has also developed a range of other leading programs in information security and e-business. EC-Council certifications are viewed as the essential certifications needed when standard configuration and security policy courses fall short. Providing a true, hands-on, tactical approach to security, individuals armed with the knowledge disseminated by EC-Council programs are tightening security networks around the world and beating hackers at their own game.

Other EC-Council Programs

Security Awareness: Certified Secure Computer User

C|SCU
Certified | Secure Computer User

The purpose of the CSCU training program is to provide students with the necessary knowledge and skills to protect their information assets. This class will immerse students in an interactive learning environment where they will acquire fundamental understanding of various computer and network security threats such as identity theft, credit card fraud, online banking phishing scams, viruses and backdoors, email hoaxes, sexual predators and other online threats, loss of confidential information, hacking attacks, and social engineering. More importantly, the skills learnt from the class help students take the necessary steps to mitigate their security exposure.

Network Defense: Certified Network Defender

Students enrolled in the Certified Network Defender course will gain a detailed understanding of network defense and develop their hands-on expertise to perform in real-life network defense situations. They will gain the depth of technical knowledge required to actively design a secure network within your organization. This course provides a fundamental understanding of the true nature of data transfer, network technologies, and software technologies so that students may understand how networks operate, how automation software behaves, and how to analyze networks and their defense.

Students will learn how to protect, detect, and respond to the network attacks as well as learning about network defense fundamentals, the application of network security controls, protocols, perimeter appliances, secure IDS, VPN, and firewall configuration. Students will also learn the intricacies of network traffic signature, analysis, and vulnerability scanning, which will help in designing improved network security policies and successful incident response plans. These skills will help organizations foster resiliency and operational continuity during attacks.

Ethical Hacking: Certified Ethical Hacker

The Certified Ethical Hacker (CEH) program is the core of any information security professional's most desirable training system. CEH is the first part of a three-part EC-Council Information Security Track, which helps students master hacking technologies. You will become a hacker—but an ethical one!

As the security mindset in any organization must not be limited to the silos of a certain vendor, technology, or piece of equipment, this course was designed to provide students with an understanding of the tools and techniques used by hackers and information security professionals alike to break into an organization's systems. As we put it, "To beat a hacker, you need to think like a hacker."

This program will immerse students in the hacker mindset so they will be able to defend against future attacks. It puts students in the driver's seat, using an innovative, hands-on learning environment to immerse them in a systematic ethical hacking process.

Here, students will be exposed to an entirely different way of achieving optimal information security posture in an organization—by hacking it! Students will scan, test, hack, and secure their own systems. They will be taught the five phases of ethical hacking and how to approach a target and succeed at breaking in every time. The five phases include reconnaissance, gaining access, enumeration, maintaining access, and covering their tracks.

Penetration Testing: EC-Council Certified Security Analyst

The EC-Council Certified Security Analyst (ECSA) course complements the Certified Ethical Hacker (CEH) certification by exploring the analytical phase of ethical hacking. While the CEH certification exposes the learner to hacking tools and technologies, the Certified Security Analyst course takes it a step further, exploring how to analyze the outcomes of using these tools and technologies. Through the use of groundbreaking penetration testing methods and techniques, this pen-testing security training course helps students perform the intensive assessments required to effectively identify and mitigate risks to IT infrastructure security.

This makes the Certified Security Analyst "Penetration Training" a relevant milestone toward achieving EC-Council's Licensed Penetration Tester certification, which also teaches the business aspects of penetration testing. The Licensed Penetration Tester certification standardizes the knowledge base for penetration testing professionals by incorporating the best practices followed by experienced experts in the field. The objective of becoming a Certified Security Analyst is to help experienced security professionals add value to their credentials and skills by providing security training that will help them analyze the outcomes of their vulnerability assessments. Penetration Testing Training leads the learner into the advanced stages of ethical hacking.

Penetration Testing: Licensed Penetration Tester (Master)

The LPT (Master) is the world's first fully online, remotely proctored LPT (Master) practical exam, which challenges the candidates through a grueling 18 hours of performance-based, hands-on examinations. These are divided into three six-hour practical exams that will test candidates' perseverance and focus by forcing them to outdo themselves with each new challenge. The exam requires the candidates to demonstrate a methodical approach to testing and validating security defenses. The LPT (Master) exam is developed in close collaboration with subject-matter experts and practitioners around the world after a thorough job role, job task, and skills-gap analysis.

Computer Forensics: Computer Hacking Forensic Investigator

Computer Hacking Forensic Investigator (CHFI) is a comprehensive course covering major forensic investigation scenarios. It enables students to acquire crucial hands-on experience with various forensic investigation techniques. Students learn how to utilize standard forensic tools to successfully carry out a computer forensic investigation, preparing them to better aid in the prosecution of perpetrators.

EC-Council's CHFI certifies individuals in the specific security discipline of computer forensics from a vendor-neutral perspective. The CHFI certification bolsters the applied knowledge of law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of network infrastructures.

Management: Certified Chief Information Security Officer

The Certified Chief Information Security Officer (CCISO) program was developed by EC-Council to fill a knowledge gap in the information security industry. Most information security certifications focus on specific tools or practitioner capabilities. When the CCISO program was developed, no certification existed to recognize the knowledge, skills, and aptitudes required for an experienced information security professional to perform the duties of a CISO effectively and competently. In fact, at that time, many questions existed about what a CISO really was and the value this role adds to an organization.

The CCISO Body of Knowledge helps to define the role of the CISO and clearly outline the contributions this person makes in an organization. EC-Council enhances this information through training opportunities conducted as instructor-led or self-study modules to ensure candidates have a complete understanding of the role. EC-Council evaluates the knowledge of CCISO candidates with a rigorous exam that tests their competence across five domains with which a seasoned security leader should be familiar.

ECIH Exam Information

ECIH Exam Details	
Exam Title	**EC-Council Certified Incident Handler (ECIH)**
Exam Code	**212-89**
Availability	**EC-Council Exam Portal** (please visit **https://www.eccexam.com**)
Duration	**3 Hours**
Questions	**100**
Passing Score	Please refer to **https://cert.eccouncil.org/faq.html**

Please visit **https://cert.eccouncil.org** for more information.

Table of Contents