



AuPI
AUSTRALIAN
POLYTECHNIC
INSTITUTE.

EC-Council Essential Series

*A Cyber Security workforce
development initiative*

N | D E E | H E D | F E

Network

Defense Essentials

Ethical

Hacking Essentials

Digital

Forensics Essentials

Future Your Career in Cyber Security

[Apply Now](#)

EC-COUNCIL | ACADEMIA
PARTNER



LETTER FROM CEO

"IF YOU ARE UNSURE WHERE TO START WITH A CYBER SECURITY CAREER, THE ESSENTIAL SERIES IS THE ANSWER. IT IS WELL EQUIPPED TO BUILD SOLID FOUNDATIONS AND BOOST YOUR CONFIDENCE TO COMBAT CYBER CRIMES."

EC-Council Essential Series is our cyber security workforce development initiative. This program will genuinely assist IT professionals in jump-starting their careers in cyber security. The essential series is the answer if you are unsure where to start with a global standard cyber security career.

There is an accelerating shortage of cybersecurity professionals across the globe, including in Australia. According to the federal Labour Market Information Portal (LIMP), demand for cyber security skills and services will grow at least 21% by May 2023, with a current growth rate of 38.9%. The 2022 LinkedIn Emerging Jobs Report listed Cyber Security Specialist as one of Australia's top two emerging jobs. And a recent federal government report estimated Australia would need another 11,000 cyber security specialists over the next decade. It's a fast-growing sector, and this offers tremendous job opportunities for IT professionals and aspiring cybersecurity enthusiasts. Current market reports contemplate that the unemployment rate in the cybersecurity field is close to 0%.

However, becoming a cyber security specialist is not easy. The field of cyber security encapsulates multi-disciplinary knowledge and skills. To be a cyber security expert, you need systematic planning, skill development, concurrency, hands-on experience, and, most importantly, hard work. AuPI is offering you the solution. An accredited certification course globally endorsed in the industry is the best way to start.

The EC-Council essential series is well equipped to build solid foundations and boost your confidence to combat cyber crimes. It consists of three critical building blocks of cyber security. These are a) Network Defence, b) Ethical Hacking, and c) Digital Forensics. Each course in the series is meticulous, detailed, and consists of all the learning resources in one place to build your career in cyber security

The EC-Council essential series is reasonably priced and offer super value. One payment of \$345 per course or \$945 for the entire series provides an enormous wealth of learning materials, hands-on practices, and academic support, including:

- Exam voucher;
- Exam Preparation Kit;
- Exam supervision (remote proctoring);
- Pre and Post assessments;
- 2-hours live orientation class;
- 12 months of access to all learning materials, including e-Book, video lectures, lab lectures, i-Lab, and exam preparation;
- Administrative support;
- Certificate of Completion

In addition to the above features, each course in the series is self-paced and 100% online. You can study anytime-anywhere from any device.

Our learning approach offers a solid commitment to and support for every learner as an individual. We believe in teamwork. Taking the AuPI's educational journey together, we can positively impact individuals, their professions and organisations, and broader local and global society.

I take this opportunity to thank you for choosing AuPI as your trusted learning partner. Please visit our website aupi.edu.au to find other courses.

We wish you all the best.

Best regards,

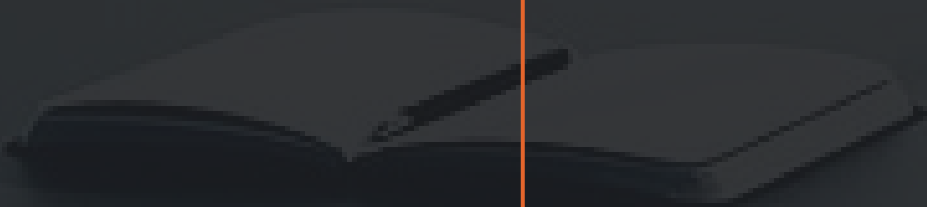


DR EHSAN AHMED, CEO

AUSTRALIAN POLYTECHNIC INSTITUTE
ceo@aupi.edu.au

TABLE OF CONTENTS

- 01** [About AuPI](#)
- 02** [Why AuPI?](#)
- 03** [About EC-Council](#)
- 04** [About the Essential Series](#)
- 05** [Course Outline](#)
 - [*Network Defence Essentials N|DE*](#)
 - [*Ethical Hacking Essentials E|HE*](#)
 - [*Digital Forensic Essentials D|FE*](#)
- 06** [Price](#)
- 07** [Cyber Security Career Pathway](#)



Australian Polytechnic Institute (AuPI) is a nationally accredited education provider in Australia (RTO Code: 45820). We meticulously select and offer a narrow range of courses exceedingly desirable in the current job market. Our learning approaches are pragmatic and designed to foster the application of knowledge, workplace skills, and job readiness. AuPI will ensure learning outcomes with the real-world skills you need for a successful career. This philosophy is our motto of being **Future Your Career ...**

ABOUT AUPI



FUTURE YOUR CAREER...

Our students are at the centre of everything we do. We design our courses focusing on supporting individual study choices and lifestyles. We ensure flexibility, accessibility and the best learning experience for our students. There are several unique features we offer to our students, including:

WHY AUPI?



Simple Learning Structure



24/7 Virtual Lab



Learn in Small Bite



Study Anytime-Anywhere



Learn from Industry Experts



On Any Device

ABOUT

EC-Council

The International Council of E-commerce (EC-Council) is known as the world's largest technical cyber security certification body. It is also recognised for being the creators of the globally recognised Certified Ethical Hacker (CEH) standards, coining the phrase "Ethical Hacking" back in 2001 when hacking was still considered a "bad" word.

Over 20 years, EC-Council has produced over 20 career-focused, tactical cyber security certifications widely recognised, accredited, and valued by industry, government, and ministries worldwide.

Some of the finest organisations worldwide, 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.

EC-Council's sole purpose is to build and refine the cybersecurity profession globally. The organisation helps individuals, organisations, educators, and governments address global workforce problems by developing and curating world-class cybersecurity education programs and corresponding certifications.

EC-Council provides cybersecurity services to some of the largest businesses around the world. Trusted by 7 of the Fortune 10, 47 of the Fortune 100, the Department of Defense, the global intelligence community, NATO, and more than 2,000 of the best universities, colleges, and training companies, EC-Council's programs have proliferated through 140 countries. They have set the bar in cybersecurity education. ECCouncil is an ANSI 17024-accredited organisation and has earned recognition from the DoD under Directive 8140/8570, in the UK by the GCHQ, CREST, and a variety of other authoritative bodies that influence the entire profession. Best known for the Certified Ethical Hacker program, we are dedicated to equipping more than 230,000 information-age soldiers with the knowledge, skills, and abilities required to fight and win against black hat adversaries.

EC-Council Accreditation & Recognition



DoD
Department of Defense
Directive 8570



ACE
American Council on Education



CNSS
Committee on National Security
Systems



ANSI 17024
American National Standards Institute



Veteran Affairs
Department of Veteran Affairs US



NCSC
National Cyber Security Centre



NICE Mapped
National Initiative for Cybersecurity
Education



US Army
US Army Credentialing Assistance

ABOUT THE ESSENTIAL SERIES

WHAT IS ESSENTIAL SERIES?

EC-Council's Essentials Series is a set of professional certified courses accredited globally. These courses teach learners various techniques across industry verticals, such as securing networks, mitigating cyber risks, conducting forensic investigations, and more. You must sit for a certified exam and pass to get the certificate for each course. There are three courses in the essential series:

- Network Defense Essentials (N|DE).
- Ethical Hacking Essentials (E|HE).
- Digital Forensics Essentials (D|FE).

These courses are well-equipped to help students and early career cybersecurity professionals to choose their area of competency or select a specific interest in cybersecurity.

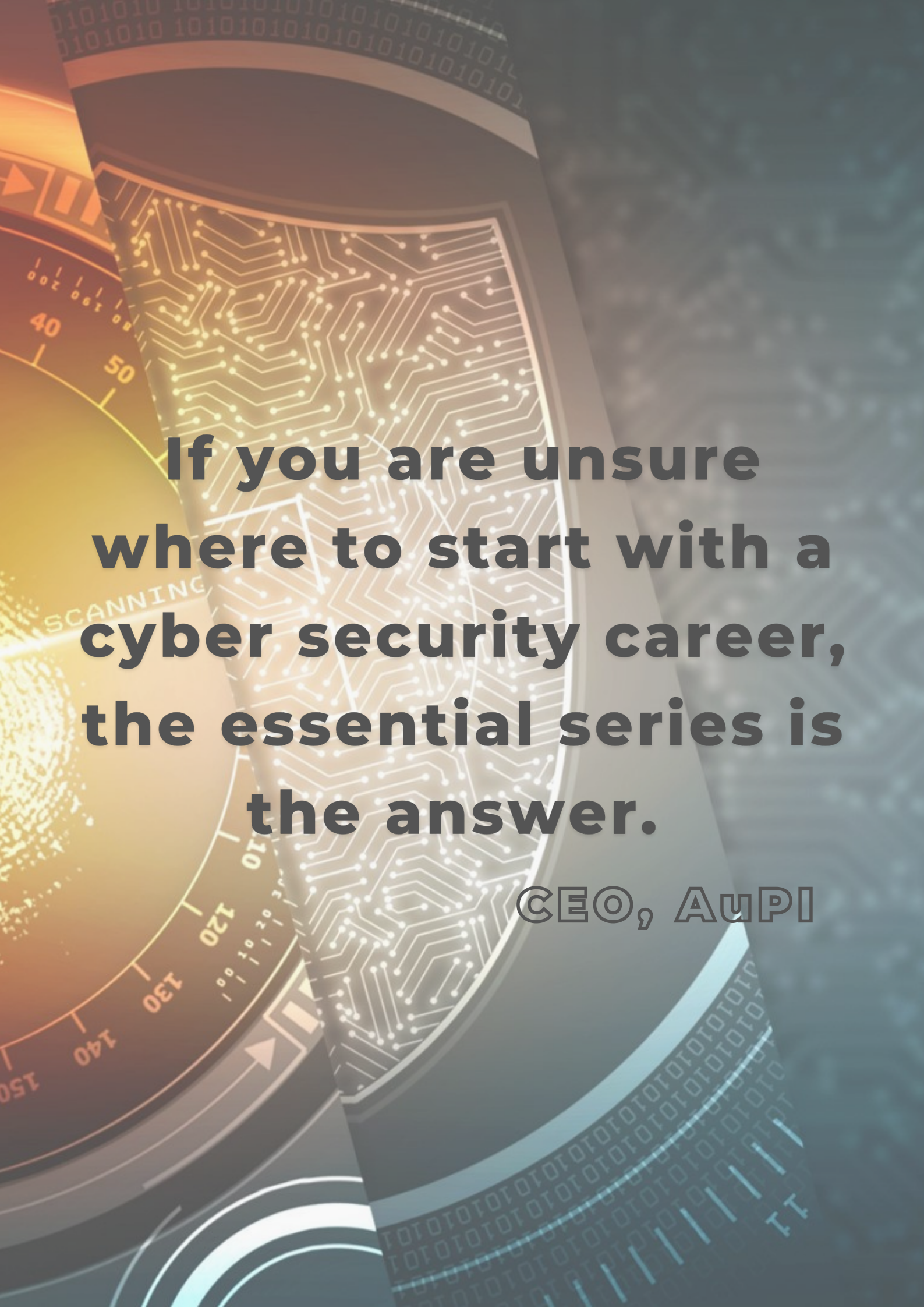
WHAT ARE THE BENEFITS?

Industry experts designed the Essentials Series to provide an unbiased approach to learning and exploring industry best practices. It empowers individuals to:

- Gain foundational knowledge in cybersecurity
- Practice essentials skills such as how to defend networks and investigate them
- Challenge industry-recognised exams and earn cybersecurity credentials to build and further your career

WHO SHOULD ATTEND THESE COURSES?

EC-Council's Essentials Series programs and certifications build and validate candidates' skills for their cybersecurity future. It is ideal for IT professionals seeking to foray into the exciting world of cybersecurity. Cybersecurity enthusiasts and students will find the program interesting, challenging, and valuable.



**If you are unsure
where to start with a
cyber security career,
the essential series is
the answer.**

CEO, AuPI

[View Course](#)



COURSE OUTLINE

Course Overview

N|DE entails a holistic overview of the critical components of network security with virtual labs for hands-on experience. This includes 12 essential topic areas in network security, covering fundamental network security concepts, including IoT, cryptography, and PKI.

By completing this certification course, you will be able to implement the basics of network security and establish the first line of defence for your workplace.

This course is designed for those interested in learning the various fundamentals of network security and who aspire to pursue a career in network security. It's an ideal stepping stone to transforming your career into a cyber security specialist.

Every organisation requires a stable and efficient network security architecture that protects its critical assets and information systems from emerging security threats. However, as the Internet and computer networks continually grow, network security has become a slippery ground and possible gateway to cyber-attacks. Securing information and data in our digital landscape has become increasingly important with the increased use of emerging technology. Research shows that fundamental network security knowledge and simple steps can significantly reduce an organisation's cyber-attack vulnerability.

What you will learn and can apply

After successful completion of this course, you should be able to:

1. Discuss fundamental concepts of network security.
2. Discuss access control principles, terminologies, and models.
3. Examine various administrative network defence controls.
4. Examine various physical network defence controls.
5. Examine various technical network defence controls.
6. Comprehend fundamental virtualisation concepts, and suggest security best practices.
7. Explain wireless network fundamentals.
8. Discuss mobile device connection methods, and review general security guidelines and best practices for mobile platforms.
9. Discuss the working of IoT devices, application areas, communication models and IoT security best practices.
10. Discuss cryptography and PKI techniques, and use various cryptography tools to protect information.
11. Discuss data security concepts, and compare different data backup concepts and technologies.
12. Discuss the need and advantages of network traffic monitoring.

Tools you will learn

Docker Bench for security, AWS, Miradore MDM, HashCalc, MD5 calculator, HashMyFiles, VeraCrypt, Data Recovery Wizard, and Wireshark

Mode of Delivery

Online and self-paced (anytime, anyplace and on any device)

Certification Exam

Exam Length : 2 Hours
Exam Format : Multiple Choice Questions
of Questions : 75
Passing Score : 70%



COURSE OUTLINE

Course Overview

E|HE provides foundational knowledge and skills in ethical hacking. There are 12 modules and add-on labs covering fundamental ethical hacking concepts, including emerging technologies like IoT and OT, cloud computing, etc.

Anyone who uses a device connected to the Internet is susceptible to hacking. According to ACSC, "Hacking" refers to unauthorized access to a system or network, often to exploit a system's data or manipulate its normal behaviour. These hackers use their skills for a particular goal, such as gaining fame by bringing down a computer system, stealing money, or making a network unavailable. On the other hand, "Ethical Hackers" are skilled individuals who are granted access to the network by the authorities and then report vulnerabilities in the system. With ethical hacking skills, Cyber Security professionals will be able to minimise the impact of the potential threat and reduce the chances of a successful attack. Training in ethical hacking can help network defenders develop this mindset.

Learning ethical hacking can play a vital role in securing the systems and data from threats and attacks. As an ethical hacker, you can: conduct investigations and analyses of the target systems to identify any security or system vulnerabilities from the hacker's point of view and suggest a remedy. If you learn Ethical Hacking, your chances of securing a cybersecurity career will increase within an industry recruiting 3.5 million unfilled cybersecurity jobs globally.

However, being an ethical hacker is not easy and requires a lot of studying tools, techniques, penetration testing, and, most importantly, hard work. The course Ethical Hacking Essentials is an ideal pathway and building block to transform your career from novice to cybersecurity expert. This course is designed to learn the fundamentals of ethical hacking and aspire to pursue a cybersecurity specialist career.

[View Course](#)



What you will learn and can apply

After successful completion of this course, you should be able to:

1. Discuss the key issues plaguing the information security world and review various security laws and regulations.
2. Comprehend Cyber Kill Chain Methodology, hacking and ethical hacking concepts, hacker classes, different phases of a hacking cycle, and assess essential ethical hacking tools.
3. Examine various information security threats and vulnerabilities, identify different types of malware and perform vulnerability assessments.
4. Explain and use different password cracking, social engineering, insider threats, and identity theft techniques, and discuss their countermeasures.
5. Examine various network-level attacks, including sniffing, denial-of-service, and session hijacking, and discuss their countermeasures.
6. Examine various application-level attacks, including webserver exploitation, OWASP top-10 attacks, and SQL injection, and discuss their countermeasures.
7. Discuss different types of wireless encryption, examine wireless threats and attacks, and suggest countermeasures.
8. Describe various mobile platform attack vectors, mobile device management, mobile security guidelines, and identify essential mobile security tools.
9. Discuss IoT and OT concepts, examine various IoT and OT threats and attacks, and suggest countermeasures.
10. Describe various Cloud computing technologies, examine cloud computing threats and attacks, and identify security techniques.
11. Discuss the fundamentals of penetration testing, its benefits, strategies, and phases, and examine guidelines for penetration testing.

Tools you will learn

L0phtCrack, Netcraft, SQL Injection Detection Tool, Web Application Security Scanner, ARP Spoofing Detection Tools

Certification Exam

Exam Length : 2 Hours
Exam Format : Multiple Choice Questions
of Questions : 75
Passing Score : 70%

Mode of Delivery

Online and self-paced - anytime, anyplace and on any device



[View Course](#)



COURSE OUTLINE

Course Overview

D|FE provides foundational knowledge and skills in digital forensics. There are 12 modules and add-on labs covering fundamental digital forensics concepts, such as dark web forensics, investigating web application attacks, and more.

Digital devices such as cell phones, tablets, gaming consoles, laptops and desktop computers have become an indispensable part of modern society. With the proliferation of these devices in our everyday lives, there is a tendency to use information derived from them for criminal activities. A recent statistical report on cybercrimes reveals that the digital forensics market will grow from \$4.62B in 2017 to \$9.68B by 2022, with an annual compound growth rate of almost 16%.

Unlike the other two courses in the essential series, the security approach in Digital Forensic differs. While Network Defence and Ethical Hacking focus on preventive measures, Digital Forensic focuses on reactive measures.

Digital forensic investigators face challenges such as extracting data from damaged or destroyed devices, locating individual items of evidence among vast quantities of data, and ensuring that their methods capture data reliably without altering it. The process integrates many stakeholders, including legal professionals, law enforcement bodies, policymakers, businesses, education providers, and the government.

Becoming a Digital Forensic expert is hard work and requires a systematic knowledge-building approach. This course can genuinely help you and will be an effective stepping tool to develop your expertise in digital forensics. The course encapsulates various fundamental and technical aspects of digital forensics to start your professional journey as a cyber security specialist.

What you will learn and can apply

After successful completion of this course, you should be able to:

1. Discuss the fundamental concepts of computer forensics, digital evidence, and forensic readiness, identify a forensic investigator's roles and responsibilities, and review legal compliance issues in computer forensics.
2. Examine the computer forensic investigation process and its phases.
3. Describe different disk drives, characteristics, and logical structure, understand Windows, Linux, and Mac boot processes, and examine various file systems and formats.
4. Discuss data acquisition concepts, types, format, and methodology.
5. Examine various anti-forensics techniques and identify countermeasures.
6. Examine various volatile and non-volatile information gathering techniques for Windows, Linux, and Mac systems, including Windows memory and registry analysis, cache, cookie, history analysis, and metadata investigation.
7. Explain network forensics fundamentals and event correlation, and perform network traffic investigation.
8. Comprehend web server logs and perform web application forensics to detect and investigate various attacks on web applications.
9. Discuss the working of the dark web and email systems, and perform Dark Web, TOR browser, and email forensics.
10. Discuss malware forensics fundamentals and list and perform different types of malware analysis.

Tools you will learn

Linux, Windows, Sleuth Kit, Wireshak,
Splunk, TOR browser, ESEDatabaseView

Mode of Delivery

Online and self-paced - anytime, anyplace
and on any device

Certification Exam

Exam Length : 2 Hours
Exam Format : Multiple Choice Questions
of Questions : 75
Passing Score : 70%

PRICE

The EC-Council Essential series is a cyber security workforce development initiative by Australian Polytechnic Institute. It is reasonably priced to attract early career cybersecurity professionals and help them progress toward advanced level certified courses.

One payment of \$345 per course or \$945 for the entire series provides an enormous wealth of learning materials, hands-on practices, and academic support, including:

- Exam voucher
- Exam Preparation Kit
- Exam supervision
- All assessments
- Live orientation class
- 12 months of access to all learning materials
- e-Book
- Video lectures
- 24/7 virtual Lab
- Administrative support;
- Certificate of Completion

\$345

Per Course

or

\$945

The Entire Series

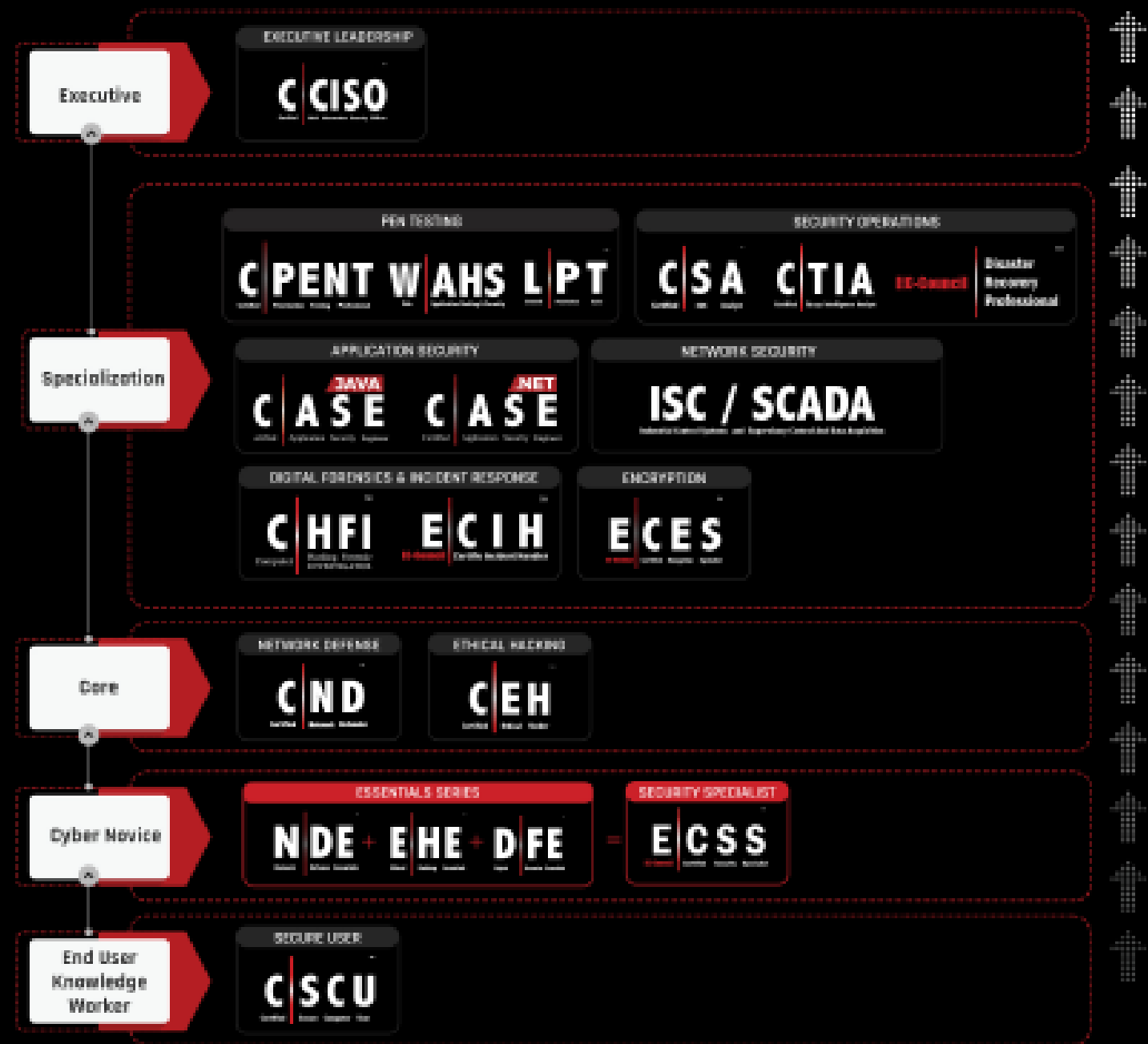
In addition to the above features, each course in the series is self-paced and 100% online. You can study anytime-anywhere from any device.

[Apply Now](#)



Your Pathway to a Promising Career in Cybersecurity

EC-Council certifications help professionals secure their careers in cybersecurity. These certifications have helped thousands of professionals further their careers in Fortune 500 companies. Students can choose between following the certification path or learning in-demand skills of their choice to become future cybersecurity professionals.



This is a suggested learning pathway only. Programs can be taken independently in any order depending on job role requirements and existing skill sets.

*If you haven't
been hacked
means you don't
know!*

CEO, AUPI



+61 432 898 942



enrol@aupi.edu.au



Sydney, NSW 2567, Australia



AuPI
AUSTRALIAN
POLYTECHNIC
INSTITUTE.



Future Your Career

aupi.edu.au

RTO Code: 45820