Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Certifications in the Field of Cyber Security

Canada

FOREWORD

The *Certifications in the Field of Cyber Security* is an UNCLASSIFIED publication. The guide provides information about many of the certifications available for prospective students and cyber security professionals. The intent is not to recommend any certification body or certification in particular, but to provide a listing of some of the different certifications that may help advance an individual's career in the field of cyber security.

Information is sourced from the websites of the certification bodies referenced in this guide.

Disclaimer: The Communications Security Establishment does not endorse or recommend any of the certification bodies or certifications listed in this document. Information provided is intended to be a general summary of publicly available information and is provided for informational purposes only.

REVISION HISTORY

Revision	Amendments	Date
1	First release	November 2020
2	New certifications added and training providers removed	July 2022

TABLE OF CONTENTS

Disclaimer: The Communications Security Establishment does not endorse or recommend any of the certification bodies or certifications listed in this document. Information provided is intended to be a general summary of publicly available information and is provided for informational purposes only.

LIST OF TABLES

1.0 INTRODUCTION

There continues to be a growing demand for qualified cyber security professionals and practitioners in Canada and around the world. With the increasing need for cyber security professionals, the value of Information Technology (IT) certification is also increasing. The right certification can give you an advantage over other job candidates. Organizations are looking for talent with superior training and real-world experience.

Obtaining a certification demonstrates to future employers that an individual is competent, skilled, and experienced in certain areas. Additionally, given the time and financial investment that many certifications require, some employers see certification as a measure of commitment to a career in the field.

Certifications are not only a great supplement to a professional's other qualifications; it can also lead to a salary increase. According to a study conducted by Global Knowledge, an individual with a certification can earn up to 15% more than those without it (1). Furthermore, maintaining certification often requires meeting continuing education requirements, ensuring that certificate holders are keeping up to date on the latest technologies and can continue to keep their organizations safe from emerging cyber security threats.

1.1 THE CANADIAN CENTRE FOR CYBER SECURITY

The Canadian Centre for Cyber Security (Cyber Centre), a part of the Communications Security Establishment (CSE), was officially launched in October 2018. The Cyber Centre's Academic Outreach and Cyber Skills Development team works with universities, colleges, educational associations, education ministerial boards and private sector educators to build cyber security talent and capacity in Canada. The team also works with educators to enhance the community's understanding of cyber security. Its mission is to ensure Canada is a global leader in cyber security by elevating cyber education.

1.2 PURPOSE

The primary audience for this guide is prospective cyber security students or professionals looking to advance their careers in the field. The guide highlights some of the more in-demand, globally recognized certifications offered by providers around the world. A complete list of certifications can be found at the end of the guide (Tables 1-14).

Disclaimer: CSE does not endorse or recommend any of the certification bodies or certifications listed in this document. Information provided is intended to be a general summary of publicly available information and is provided for informational purposes only.

Every effort has been made to ensure accuracy of information, however, due to the dynamic nature of curricula and cyber security, this guide will be reviewed on a regular basis to ensure it reflects the most current certification offerings. New certifications and other suggested changes can be submitted by email to academicoutreach-collaborationacademique@cyber.gc.ca.

2.0 GLOBALLY RECOGNIZED CERTIFICATIONS BODIES

The following highlights some of the more popular and well-known cyber certifications available, in alphabetical order. A more comprehensive list of certifications can be found in the attached tables. **CSE is not endorsing, supporting, or promoting any of the following certifications or certification bodies. This guide is solely for information purposes and should only be a starting point for anyone interested in obtaining a certification. We recommend that individuals do more in-depth research, while considering their own interests and career goals, time commitments and financial resources, before deciding which certification is right for them.**

It should also be noted that while most of the certification bodies are American, their certifications are recognized around the world. Furthermore, candidates can find training through local providers, and many of the certification exams can be written at local testing centres, such as Pearson VUE, or taken online in your own home.

2.1 CERTNEXUS

CertNexus offers certifications and micro-credentials in emerging technologies, such as Internet of Things (IoT), Artificial Intelligence (AI), and human-machine interfaces. Their four cyber security certifications are valid for three years.

- **The Certified First Responder** (CRF) certificate validates the knowledge and skills required to protect critical information and systems before, during, and after an incident.
- **Cyber Safe** certification demonstrates that the holder can identify the most common risks involved in using mobile and cloud technologies, and to protect themselves and their organizations from cyber threats.
- **Cyber Secure Coder** (CSC) certificate holders have learned about the vulnerabilities that undermine security, identification, and remediation of those vulnerabilities, as well as strategies for dealing with security defects.
- The **IRBIZ** micro-credential is for Information Technology (IT) leaders and executives who are responsible for complying with incident response legislation. Successfully completing the course and exam certifies that the candidate has the necessary skills to assess and respond to security threats, as well as operate a system and network security analysis platform.

A complete list of cyber security certifications offered by CertNexus can be found in Section 5.1.

2.2 CISCO SYSTEMS

Cisco Systems is a worldwide leader in networking hardware and solutions and most of today's Internet traffic travels over Cisco-build network pathways. Obtaining one of their certifications demonstrates that you know how to work with Cisco solutions. There are five levels of certification in Cisco's program:

- **Entry**: The starting point for individuals interested in starting a career as a networking professional.
- **Associate**: Individuals master the essentials needed to launch a career and expand job possibilities with the latest technologies.
- **Professiona**l: Individuals select a core technology track and a focused concentration exam to customize their professional level certification.
- **Expert**: Certification is accepted worldwide as the most prestigious certification in the technology industry.
- **Architect**: Demonstrates the architectural expertise of a network designer.

A complete list of cyber security certifications offered by Cisco Systems can be found in Section 5.2.

2.3 COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION

The **Computing Technology Industry Association** (CompTIA) issues certifications in over 120 countries with over 2.2 million recipients. The organization also releases 50 industry studies each year tracking trends and changes. They offer numerous certifications covering a wide range of IT fields, including cyber security. The renewal process includes meeting continuing education requirements and paying the annual fees.

- **CompTIA Advanced Security Practitioner** (CASP+) is a performance-based certification for practitioners, rather than managers, at the advanced skill level of cyber security. CASP+ recipients have advanced-level knowledge of risk management, enterprise security operations and architecture, as well as research and collaboration.
- **CompTIA Cyber Security Analyst** (CySA+) certification is a security analyst certification that covers advanced persistent threats in a post-2014 cyber security environment. It validates one's expertise in security analytics, intrusion detection, and response.
- **CompTIA PenTest+** is for cyber security professionals who are responsible for penetration testing and vulnerability management. Certification holders have demonstrated their up-to-date hands-on ability and knowledge to test devices in new environments, like cloud or mobile, as well as traditional desktops and servers.
- **CompTIA Security+** is an entry-level certification. Certificate holders are experts in threat management, cryptography, identity management, security systems, security risk identification and mitigation, network access control, and security infrastructure. Candidates must have 2 years' experience in network security and have already obtained their Network+ certification.

A complete list of cyber security certifications offered by CompTIA can be found in Section 5.3.

2.4 COUNCIL FOR REGISTERED ETHICAL SECURITY TESTERS

The **Council for Registered Ethical Security Testers** (CREST) is a not-for-profit organization that provides internationally recognized certification and accreditation for companies and individuals. It has chapters in the United Kingdom (UK), United States (US), Australia, Singapore, and Hong Kong. They provide examinations in Penetration Testing, Threat Intelligence, Incident Response, Security Architecture. The Incident Response has been approved by the UK's Government Communications Headquarters (GCHQ). CREST exams have three levels of accreditation for individuals:

- **Practitioner** - Entry into profession
- **Registered** - Competent to work independently without supervision
- **Certified** - Technically competent to run major projects and teams

A complete list of cyber security certifications can be found in Section 5.4.

2.5 CERTIFIED WIRELESS NETWORK PROFESSIONALS

Certified Wireless Network Professionals (CWNP) is a vendor-neutral wireless local area network (WLAN) certification program. CWNP offers four levels of enterprise WLAN certifications, from novice to expert. Their certification programs prepare IT professionals and WLAN administrators to specify, design, and manage WLAN infrastructure and applications.

- **Certified Wireless Network Expert** (CWNE) is the highest-level certification in the CWNP program. Certificate holders have the most advanced skills available in today's enterprise Wi-Fi market. Candidates must pass four certification exams, complete commercial WLAN deployments, provide three recommendations, meet experience and publication requirements, and pass a peer review by the CWNE Board of Advisors.
- **Certified Wireless Security Professional** (CWSP**)** is a professional level WLAN certification for the CWNP program that validates an individual's ability to assess the vulnerability of a network and help prevent attacks before they

happen, perform WLAN security audits and implement compliance monitoring solutions, and design a network's security architecture. Candidates must obtain Certified Wireless Network Administrator (CWNA) certification before they can earn CWNP certification.

A complete list of cyber security certifications offered by CWNP can be found in Section 5.5.

2.6 EC-COUNCIL

EC-Council is a cyber security technical certification board and operates in 145 countries. It is endorsed by the US Government, National Security Agency (NSA), and the Committee on National Security Systems (CNSS).

- The **Certified Ethical Hacker (ANSI)** credential certifies one's competence in the five phases of ethical hacking: reconnaissance, enumeration, gaining access, maintaining access, and covering tracks. Certification requires passing a 4-hour exam consisting of 125 questions.
- The **Certified Ethical Hacker (Practical)** designation targets the application of CEH skills to real-world security audit challenges and related scenarios. Candidates must complete a 6-hour exam featuring 20 case studies and obtain a 70% score.
- A **Certified Ethical Hacker (Master)** holds both the ANSI and Practical certifications.
- The **Computer Hacking Forensics Investigator (CHFI)** is another universally recognized certification that validates that the recipient is skilled in the areas of anti-hacking, digital forensics, and penetration testing.
- The **Certified Network Defender (CND)** certificate demonstrates a solid understanding of defensive security and the required expertise to secure data.
- The **EC Council Disaster Recovery Professional (EDRP)** certificate holders have the foundation for securing and restoring networks in the event of a disaster like malicious attacks.

A complete list of cyber security certifications offered by EC-Council can be found in Section 5.6.

2.7 GLOBAL INFORMATION ASSURANCE CERTIFICATION

Global Information Assurance Certification (GIAC), founded by the SANS institute, specializes in technical and practical certification. Its certifications are linked to training courses provided by SANS and are recognized worldwide. Candidates for *Expert Status* certification are only required to pass an exam to obtain certification, which is valid for 4 years. To be eligible to renew at the end of the 4-year period, certificate holders must have 36 continuing education credits and pay the recertification fee or re-take the exam. Individuals wishing to pursue *Gold Status* certification must research and write a technical report or white paper. Gold Status indicates the holder has a deeper knowledge of a subject area.

- **GIAC Security Essential Certification** (GIAC) validates an individual's knowledge information security beyond the simple terminology and concepts. Recipients are skilled in active defense, cryptography, security policy and plans, incident handling, securing networks, etc.
- **GIAC Certified Intrusion Analyst** (GCIA) validates a practitioner's knowledge of network and host monitoring, traffic analysis, and intrusion detection. Certificate holders are qualified to configure and monitor intrusion detection systems, and to analyze network traffic.
- **GIAC Certified Incident Handler** (GCIH) demonstrates one's ability to detect, respond, and resolve computer security incidents using a wide range of essential security skills. An individual with GCIH certification has a solid understanding of common cyber-attack techniques and how to defend against them.

A complete list of cyber security certifications offered by GIAC can be found in Section 5.7.

2.8 INTERNATIONAL INFORMATION SYSTEMS SECURITY CERTIFICATION CONSORTIUM

The **International Information Systems Security Certification Consortium**, or (ISC)2, is a non-profit member organization that provides support to members with credentials, resources, and leadership to address cyber, information, software, and infrastructure security. It is a large IT Security organization, with more than 140,000 members worldwide, almost 6,000 of which are Canadian.

(ISC)2 offers one of the most popular cyber security certifications:

- **Certified Information Systems Security Professional** (CISSP) designation is often required for the most in-demand cyber security jobs and is considered the 'gold standard' of security certifications. Requirements for this advanced level certification include a minimum of 5 years of experience in at least two of (ICS)2's eight common body of knowledge domains, or 4 years of experience and a college degree or approved credentials. Candidates are also required to pass a 3-hour written exam. Re-certification is required every 3 years. To recertify, candidates must earn 120 continuing professional education credits within the three-year cycle and pay an annual fee.

A complete list of cyber security certifications offered by (ISC)2 can be found in Section 5.8.

2.9 ISACA

ISACA, formerly known as the Information Systems Audit and Control Association, is an international professional association focused on IT governance. It has more than 140,000 members and professionals holding ISACA certifications in 180 countries. Its 200+ chapters provide members with training, and networking and resource sharing opportunities.

Candidates must pass written exams to obtain any of ISACA's professional certifications, all of which are valid for three years. To maintain certification, credential holders are required to obtain at least 120 continuing professional education credits over the three-year period, and pay an annual membership fee, or re-take the exam. ISACA Cyber Security Certifications include the following:

- **The Certified Information Security Manager** (CISM) credential is aimed at leaders of Cyber Security teams, IT professionals responsible for managing, developing, and overseeing information security systems in enterprise-level applications, or for developing best organizational security practices. In addition to the written exam, candidates must have at least 5 years of security experience and submit a written application.
- **Certified in Risk and Information Systems Control** (CRISC) certification demonstrates the ability to identify, evaluate, and respond to IT risks. Candidates must have 3 years of professional-level risk management and control experience and perform the tasks of at least two CRISC domains. For this certification, education is not an acceptable substitute for work experience.
- **Cyber Security Nexus Practitioner** (CSX-P) recognizes individuals who can act as first responders for security incidents. Created in 2015, tests one's ability to perform globally validated cyber security covering the five core functions of the NIST Cyber Security Framework; Identify, Protect, Detect, Respond, and Recover. To obtain certification, candidates must pass a 4-hour performance-based exam consisting of simulated security incidents. At the end of the 3-year certification period, holders must take the latest version of the exam to recertify.

A complete list of cyber security certifications offered by ISACA can be found in Section 5.9.

2.10 ITSM SOLUTIONS

Built around NIST Cyber Security Framework (NCSF), **itSM Solutions** certifications validate that cyber security professionals have the baseline skills to design, build, test and manage a cyber security program using the NCSF.

Disclaimer: The Communications Security Establishment does not endorse or recommend any of the certification bodies or certifications listed in this document. Information provided is intended to be a general summary of publicly available information and is provided for informational purposes only.

- **NCSP Foundation:** For executives, business and IT professionals who need a basic understanding of NCSF to perform their jobs
- **NCSP Practitioner:** Teaches how to build and design a technology focused cyber security program and risk management program. Gives you a deeper understanding of the NCSF and how to adapt and operationalize it.

A complete list of cyber security certifications offered by itSM Solutions can be found in Section 5.10.

2.11 MCAFEE INSTITUTE

McAfee Institute offers several industry-recognized board certifications in the areas of cyber intelligence and investigations, digital forensics, and cryptocurrency investigations. Certificate holders come from some of the top law enforcement and government agencies like the U.S Air Force and Army, Federal Bureau of Investigation (FBI) and the New York Police Department (NYPD).

- **Certified Cyber Intelligence Professional** (CCIP) certification was developed in conjunction with the Department of Homeland Security' National Cyber Security Workforce Framework. Certification demonstrates that an individual can identify persons of interest, conduct timely cyber investigations, and prosecute cyber criminals. Candidates must hold a bachelor's degree or higher, and three years of experience in investigations, IT, fraud, law enforcement, forensics, criminal justice, law, and loss prevention.

A complete list of cyber security certifications offered by McAfee Institute can be found in Section 5.11.

2.12 OFFENSIVE SECURITY

Offensive Security is an international company that provides security counselling and training for technology companies, including practical performance-based certification programs, virtual lab access, and open-source projects.

- **Offensive Security Certified Professional** (OSCP) certification is considered one of the hardest to obtain due to its difficult exam. Candidates are required to successfully attack and penetrate live machines in a safe, lab environment over a 24-hour period. Because of its hands-on nature, it is intended for penetration testers with strong technical and ethical hacking backgrounds. Prior to attempting the exam, candidates must complete the Penetration Testing training course offered by Offensive Security. Obtaining the certificate also qualifies the recipient for 40 (ISC)2 continuing education credits. Unlike many of the other cyber security certifications, the OSCP certificate never expires.

A complete list of cyber security certifications offered by Offensive Security can be found in Section 5.12.

2.13 PECB

PECB is a certification body that provides education and certification under International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17024 (conformity assessment: general requirements for bodies operating certifications of individuals) on a wide variety of disciplines including information security and cloud security. They have a global network of distributers, trainers, and certified individuals in more than 150 countries. PECB is accredited by the International Accreditation Service (IAS) and the United Kingdom Accreditation Service (UKAS).

- **Certified Lead Ethical Hacker** credential demonstrates that you can lawfully assess the security of your organization's systems and find their vulnerabilities.

A complete list of cyber security certifications offered by PECB can be found in Section 5.13

2.14 SECO INSTITUTE

Security & Continuity Institute (SECO) is a European institute that offers high-level security and continuity certifications. The SECO certification program consists of seven different certification tracks, each focusing on a specific field of expertise, such as IT Security, Data Privacy, and Ethical Hacking. Tracks starts at the Foundation level, followed by Practitioner and Expert levels. Candidates can then apply for Certified Officer level certifications which are the highest achievable qualification in each certification track.

- **Ethical Hacking Foundation** (S-EHF) is an entry-level certification for professionals seeking to enter the career field. Certificate holders understand the fundamentals of ethical hacking and can perform basic penetration testing. While there are no prerequisites, it is recommended that candidates have a basic understanding of Linux.
- **Ethical Hacking Practitioner** (S-EHP) is aimed at professionals who already have solid knowledge of ethical hacking basics. It is recommended that candidates obtain S-EHF certification first. Obtaining certification demonstrates that an individual has a full understanding of the penetration testing process and is familiar with common penetration testing techniques.

A complete list of cyber security certifications offered by SECO can be found in Section 5.14.

3.0 CYBER CREDENTIALS COLLABORATIVE

Cyber Credentials Collaborative (C3) was created in 2011 to promote the benefits of certifications in the skills development of information security professionals around the world. C3 provides awareness of and advocacy for vendor-neutral credentials in information security, privacy, and other IT disciplines. By providing a forum for members to collaborate on issues of shared concern, C3 aims to advance IT careers, better prepare the workforce, and ensure that IT certifications are developed to meet the needs of government, private organizations, and educational institutions.

The below listed certification bodies are all members of C3:

- (ISC)2
- CertNexus
- CompTIA
- Global Information Assurance Certification
- ISACA

4.0 ACCELERATED CYBER SECURITY TRAINING

Rogers Cybersecure Catalyst, Ryerson University's national centre for innovation and collaboration in cyber security, recently partnered with SANS Institute to offer an intensive cyber security training and certification program. The Accelerated Cyber Security Training Program is designed to address the shortage of cyber security professionals in Canada. Students taking this 7-month program will earn three GIAC certifications:

- GIAC Foundational Cybersecurity Technologies (GFACT)
- GIAC Security Essentials Certification (GSEC)
- GIAC Certified Incident Handler (GCIH)

In addition to the certifications, participants will receive a Recognition of Completion form from Rogers Cybersecure Catalyst, career mentorship with experts, and connections with employers.

The program also aims to bring under-represented groups like Women, New Canadians and Displaced Workers into the industry by offering 4 streams: Royal Bank of Canada (RBC) Women in Cyber, RBC New Careers in Cyber, Rogers New Canadians in Cyber and Peel Region Young Workers in Cyber.

The Accelerated Cyber Security Training Program is funded by the Government of Canada, Rogers Communications and RBC.

5.0 CYBER SECURITY CERTIFICATION LISTINGS AND DESCRIPTIONS

The tables below offer a more fulsome list of the different cyber security certifications available to individuals, in alphabetical order.

Prior to attempting a certification exam, candidates can purchase training (in-class, online, or self-paced courses) and other exam preparation materials, such as practice exams, through the vendors and training providers. Some vendors also offer course bundles that include exam fees. To find out more about certification training options and providers, please visit the certification body website.

5.1 CERTNEXUS

Table 1 CertNexus Certification Listing and Descriptions[3]

Certification	Certification Overview	Intended Candidates

Certified First Responder (CFR)	• Validates a candidate's knowledge of analyzing threats, designing secure computing and network environments, proactively defecting networks and responding to/investigating cyber security incidents
	• Candidates should have 3-5 years of experience working in a computing environment protecting critical information systems before, during, and after an incident
	• Exam consists of 100 multiple choice questions
	• Valid for 3 years
	• 2 options for re-certification:
	  ○ Take the most recent version of the exam
	  ○ Earn 90 continuing educated credits within the 3 years and paying annual fees
		• System Administrators
		• Network Administrators
		• Incident Responders
		• Cyber Crime Investigators
		• IT Auditors
		• Security Analysts
		• Network Analysts
		• Information Systems Security Engineers

Certified IoT Security Practitioner (CIoTSP)	• Validates a candidate's knowledge, skills, and ability to secure network environments for IoT devices, analyze vulnerabilities and determine reasonable controls against threats and effectively monitor IoT devices and respond to incidents	• Network Administrators • Software Development Engineer

[3] Every effort has been made to ensure the accuracy of the information in this table; however, the information is subject to change at any time.

Disclaimer: The Communications Security Establishment does not endorse or recommend any of the certification bodies or certifications listed in this document. Information provided is intended to be a general summary of publicly available information and is provided for informational purposes only.

	• Candidates should have a fundamental understanding of IoT ecosystems • Exam consists of 100 multiple choice questions	• Solution Architects • Cyber Security Analysts • Web Developers • Cloud Engineers
Cyber Secure Coder (CSC)	• Demonstrates that a candidate has learned about the vulnerabilities that undermine security, identification and remediation of those vulnerabilities, and strategies for dealing with security defects • Candidates should have some programming experience (developing desktop, mobile, web, or cloud applications) • Exam consists of 80 multiple choice questions • Valid for 3 years	• Lead Developers • Junior Programmers • Application Testers • Quality Assurance Testers • Software Designers • Software Architects
CyberSafe	• Validates that a candidate can identify the most common risks involved in using mobile and cloud technologies, and to protect themselves and their organizations from cyber threats • No prerequisites for exam but candidates should have experience with basic technology (computers, smartphones, email, internet etc.) • Exam is only 10 questions and has no time limit	• Non-technical computer end-users
IRBIZ micro credential	• Certifies that a candidate has the necessary skills to assess and respond to security threats, and operation a system and network security analysis platform • Candidates should have a general understanding of cyber security • Exam consists of 10 multiple choice and true/false questions • Valid for 3 years	• IT leaders and Executives responsible for incident response legislation compliance

5.2 CISCO SYSTEMS

Table 2 Cisco Systems Certification Listing and Descriptions[4]

Certification	Certification Overview	Intended Candidates
Cisco Certified CyberOps Associate	• Certification prepares candidates to begin working with associate-level cyber security analysts within Security Operations Centres (SOC) • No prerequisites • Valid for 3 years • Recertification requires advancing to the next level of certification, earning continuing education credits, or a combination of both	• Cyber Security Analysts • SOC Team members
Cisco Certified CyberOps Professional	• New certification introduced in 2021 • Validates a candidate's knowledge of cloud computing security, risk management, and threat intelligence analysis • No prerequisites • Valid for 3 years • Recertification requires advancing to the next level of certification, earning continuing education credits, or a combination of both	• Information Security Analysts • Incident Responders • Incident Managers • Network Engineers
Cisco Certified Network Associate Security (CCNA Security)	• Validates a candidate's ability to develop a security infrastructure, recognize threats and vulnerabilities to networks, and mitigate security threats • Candidates should already have a valid Cisco CCENT, CCNA Routing and Switching, or any CCIE certification • Valid for 3 years • Recertification requires advancing to the next level of certification, earning continuing education credits, or a combination of both	• Network Administrators • Network Engineers

[4] Every effort has been made to ensure the accuracy of the information in this table; however, the information is subject to change at any time.

Disclaimer: The Communications Security Establishment does not endorse or recommend any of the certification bodies or certifications listed in this document. Information provided is intended to be a general summary of publicly available information and is provided for informational purposes only.

5.3 COMPTIA

Table 3 CompTIA Certification Listing and Descriptions[5]

Certification	Certification Overview	Intended Candidates
Advanced Security Practitioner (CASP+)	• Advanced level certification • The only performance-based certifications for practitioners rather than managers, at the advanced level of cyber security • Validates advanced-level competency in risk management, enterprise security operations and architecture, research and collaboration, and integration of enterprise security • Candidates require 10 years of experience in IT administration; 5 of which are hands-on technical security experience • Exam consists of 90 multiple choice and performance-based questions • Valid for 3 years • Renewal requires obtaining 75 continuing education credits during the 3-year period	• Security Architect • Technical Lead Analyst • Security Engineer • Application Security Engineer
Cyber Security Analyst (CySA+)	• Intermediate level cyber security analyst certification • The most up to date security analyst certification covering advanced persistent threats in a post-2014 cyber security environment • Validates a candidate's expertise in security analytics, intrusion detection, and response • Candidates should have 3-4 years of information security or related experience, and Network+ or Security+ certification, or equivalent knowledge • Approved by US Department of Defence • Exam consists of 85 multiple choice and performance-based questions • Valid for 3 years • Renewal requires obtaining 60 continuing education credits during the 3-year period	• IT Security Analyst • SOC Analyst • Cyber Security Specialist • Threat Intelligence Analyst • Security Engineer • Cyber Security Analyst

[5] Every effort has been made to ensure the accuracy of the information in this table; however, the information is subject to change at any time.

Disclaimer: The Communications Security Establishment does not endorse or recommend any of the certification bodies or certifications listed in this document. Information provided is intended to be a general summary of publicly available information and is provided for informational purposes only.

Network+	• Validates a candidate's knowledge and skills in designing and implementing functional networks • Prerequisites are A+ certification and 9-12 months of networking experience • Good to have for developing a career in IT infrastructure (troubleshooting, configuring, managing networks) • Exam consists of 90 multiple choice and performance-based questions • Valid for 3 years • Renewal requires obtaining 30 continuing education credits during the 3-year period	• Entry-level positions • Junior Network Administrator • Computer technician • Junior System Engineer
PenTest+	• Intermediate level certification • Validates a candidate's ability and knowledge to test devices in new environments, like cloud or mobile, as well as traditional desktops and servers • Candidates should have 3-4 years of hands-on information security or related experience • Exam consists of a maximum of 85 multiple choice and performance-based questions • Renewal requires obtaining 60 continuing education credits during the 3-year period	• Penetration Tester • Vulnerability Tester • Security Analyst • Network Security Operations
Security+	• Entry-level certification • Validates baseline cyber security skills needed to perform core security functions • Certificate holders are experts in threat management, network access control, and security infrastructure. • Candidates must have 2 years of experience in network security and obtained Network+ certification • Valid for 3 years • Renewal requires obtaining 50 continuing education credits during the 3-year period	• Systems Administrator • Network Administrator • Security Administrator • Junior IT Auditor • Penetration Tester • Security Engineer

5.4 COUNCIL FOR REGISTERED ETHICAL SECURITY TESTERS (CREST)

Table 4 CREST Certification Listing and Descriptions[6]

Certification	Certification Overview	Intended Candidates
Certified Infrastructure Tester	• Validates a candidate's ability to assess a network for flaws and vulnerabilities at the network and operating system layer • Exam consists of a multiple-choice written portion, and two 6 hour hands-on practical components • Valid for 3 years • To recertify, candidates must re-write the exam	• System Administrators • Penetration Testers • Information Security Managers • Incident Handlers
Certified Web Application Tester	• Assesses a candidate's ability to find vulnerabilities in bespoke web applications. • Exam consists of a multiple-choice written portion, and two 6 hour hands-on practical components • Valid for 3 years • To recertify, candidates must re-write the exam	• Penetration Testers • Ethical Hackers
CREST Certified Wireless Specialist (CCWS)	• Validates a candidate's knowledge and skills in performing traditional wireless security reviews, radio-frequency identification (RFID), Bluetooth and other wireless technologies • Prerequisite is successful completion of one of the core CREST certification exams • 2-part exam: 120 multiple choice questions and practical tasks • Valid for 3 years • To recertify, candidates must re-write the exam	• Senior professionals
Practitioner Security Analyst (CPSA)	• Entry-level certification	• System Administrators • Penetration Testers

[6] Every effort has been made to ensure the accuracy of the information in this table; however, the information is subject to change at any time.

Disclaimer: The Communications Security Establishment does not endorse or recommend any of the certification bodies or certifications listed in this document. Information provided is intended to be a general summary of publicly available information and is provided for informational purposes only.

	• Validates a candidate's knowledge in assessing operating systems and common network services at a basic level • Candidates must demonstrate that they have the knowledge to perform basic infrastructure and web application vulnerability scans and interpret the results to locate security vulnerabilities. • Exam consists of multiple-choice questions • Valid for 3 years • To recertify, candidates must re-write the exam	• Information Security Managers • Incident Handlers
Registered Penetration Tester (CRT)	• Validates a candidate's ability to carry out basic vulnerability assessment and penetration testing tasks • During the exam, candidates are required to find known vulnerabilities across common network, application and database technologies; includes a multiple-choice section • Pre-requisite is the CPSA certification • Valid for 3 years • To recertify, candidates must re-write the exam	• System Administrators • Penetration Testers • Information Security Managers • Incident Handlers

5.5 CERTIFIED WIRELESS NETWORK PROFESSIONS (CWNP)

Table 5 CWNP Certification Listing and Descriptions[7]

Certification	Certification Overview	Intended Candidates
Certified Wireless Network Expert (CWNE)	• Advanced-level certification • Less than 200 CWNE certificate holders in the world • Validates that a candidate has mastered all the relevant to administer, install, configure, troubleshoot and design wireless networks, and has a deep understanding of protocol analysis, intrusion detection and prevention. • Candidates are required to have 3-years of experience related to Wi-Fi networks • Application requirements include endorsement from 3 people and written submissions (essays and publications) • Candidates must pass 4 exams and complete commercial WLAN deployments • Valid for 3 years • Renewal requires paying a renewal fee and obtaining 60 continuing education credits over a 3-year period	• Individuals in senior WLAN positions
Certified Wireless Security Professional (CWSP)	• Validates a candidate's ability to assess the vulnerabilities of a network, help prevent attacks before they happen, perform WLAN security audits, and implement compliance monitoring solutions. • Candidate must have already obtained Certified Wireless Network Administrator (CWNA) certification • Exam consists of 60 multiple choice questions • Valid for 3 years • Recertification requires having valid CWNA certification and passing the current version of the exam or pass the CWNE exam.	• IT Networking Professionals

[7] Every effort has been made to ensure the accuracy of the information in this table; however, the information is subject to change at any time.

Disclaimer: The Communications Security Establishment does not endorse or recommend any of the certification bodies or certifications listed in this document. Information provided is intended to be a general summary of publicly available information and is provided for informational purposes only.

5.6 EC COUNCIL

Table 6 EC Council Certification Listing and Descriptions[8]

Certification	Certification Overview	Intended Candidates
Certified Application Security Engineer (CASE)	• Two streams: JAVA and .NET • Validates that a candidate has the critical security skills and knowledge required throughout a typical software development life cycle (SDLC), focusing on the importance of the implementation of secure methodologies and practices in today's insecure operating environment • Candidates seeking certification without official training are required to have 2 years of work experience in information security and must apply for exam eligibility • Valid for 3 years • Exams consist of 50 multiple choice questions • To recertify, you must earn 120 continuing education credits during the 3-year period and pay annual fees	• Individuals responsible for developing, testing, managing, or protecting wide area of applications • Developers who want to become Application Security Engineers, Analysts or Testers
Certified Chief Information Security Officer (CCISO)	• Program recognizes the real-world experience necessary to succeed at the highest executive levels of Information Security • CCISO program is aimed at producing top-level information security executives • Candidates seeking certification without official training are required to have at least 5 years of work experience in each of the 5 CCISO domains and must apply for exam eligibility • Candidates attending official training require 5 years of work experience in at least 3 of the CCISO domains • Exam consists of 150 multiple choice questions	• Chief Information Security Officers

[8] Every effort has been made to ensure the accuracy of the information in this table; however, the information is subject to change at any time.

Disclaimer: The Communications Security Establishment does not endorse or recommend any of the certification bodies or certifications listed in this document. Information provided is intended to be a general summary of publicly available information and is provided for informational purposes only.

	• Valid for 3 years • To recertify, you must earn 120 continuing education credits during the 3-year period and pay annual fees	
Certified Cloud Security Engineer (CCSE)	• Validates a candidate's ability to create and implement security policies to safeguard cloud infrastructure and applications • Program provides both vendor-neutral and vendor-specific cloud security concepts • Candidates seeking certification without official training are required to have at least 2 years of work experience information security and must apply for exam eligibility • Exam consists of 125 multiple choice questions • Valid for 3 years • To recertify, you must earn 120 continuing education credits during the 3-year period and pay annual fees	• Cloud Analysts • Cyber Security Analysts • Network Security Administrators • Cloud Administrators and Engineers • Network and Cloud Management Operations Professionals
Certified Cybersecurity Technician (CCT)	• Entry-level cyber security credential for individuals starting a career in cyber security or IT • Validates a candidate's hands-on technical skills • No prerequisites • Exam consists of 60 multiple choice questions and 10 practical scenarios • Valid for 3 years • CCT is not part of the EC-Council Continuing Education (ECE) scheme. To recertify, a candidate must take the exam again	• Individuals seeking entry-level cyber security or information security roles • Cyber Security technicians • Network Engineers and Administrators • IT Support Specialists and Managers • Network Technicians and Coordinators
Certified Ethical Hacker (CEH) - ANSI	• Entry-level credential • Validates that a candidate knows how to look for weaknesses and vulnerabilities in target systems and use the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system • Candidates seeking certification without official training are required to have 2 years of work experience in information security and must apply for exam eligibility • This credential certifies individuals in the specific network security discipline of ethical hacking from a vendor-neutral perspective	• Information Security Officers • Information Assurance Security Officers, Managers, Engineers, or Specialists • Site Administrators

	• Exam consists of 125 questions • Valid for 3 years • To recertify, you must earn 120 continuing education credits during the 3-year period and pay annual fees	• Information Security Auditors • Risk/Threat/Vulnerability Analysts
Certified Ethical Hacker (CEH) - Master	• Candidate holds both the ANSI and Practical CEH certifications • Valid for 3 years • To recertify, you must earn 120 continuing education credits during the 3-year period and pay annual fees	• Security Officers • IT Auditors • Site Administrators
Certified Ethical Hacker (CEH) - Practical	• Validates a candidate's knowledge of ethical hacking techniques such as threat vector identification, network scanning, operating system (OS) detection, vulnerability analysis, system hacking, web application hacking, etc. • No perquisites, but this certification is usually the next step after obtaining the CEH ANSI • 6-hour exam features 20 case studies • Valid for 3 years • To recertify, you must earn 120 continuing education credits during the 3-year period and pay annual fees	• Information Security Analysts or Administrators • Information Assurance Security Officers, Managers, Engineers, or Specialists • Risk/Threat/Vulnerability Analysts • System Administrators • Network Administrators or Engineers
Certified Network Defender (CND) – ANSI	• Demonstrates that a candidate has the required expertise to protect, detect, and respond to threats on the network • Candidates seeking certification without official training are required to have 2 years of work experience in IT security and must apply for exam eligibility • Exam consists of 100 multiple choice questions • Valid for 3 years • To recertify, you must earn 120 continuing education credits during the 3-year period and pay annual fees	• Network and IT Administrators • Data Security Analyst • Network Engineers and Technicians

Certified Penetration Testing Professional (CPENT)	• Validates a candidate's ability to perform an effective penetration testing in an enterprise network environment that must be attacked, exploited, evaded, and defended • No prerequisites • 24-hour exam consists of a 100% practical assessment within the cyber range and the submission of a Penetration Testing report • Valid for 3 years • To recertify, you must earn 120 continuing education credits during the 3-year period and pay annual fees	• Penetration Testers • Ethical Hackers • Network Server and Firewall Administrators • Risk Assessment Professionals • Security Engineers and Analysts • Information Security Consultants
Certified Secure Computer User (CSCU)	• Validates that a candidate can identify information security threats and mitigate them effectively • No prerequisites • Exam consists of 50 multiple choice questions • Valid for 3 years • CSCU is not part of the EC-Council Continuing Education (ECE) scheme. To recertify, a candidate must take the exam again	• Anyone 13 and over who uses a computer for work, study, or play • End-users
Certified SOC Analyst (CSA)	• Validates a candidate's comprehensive understanding of the tasks required as a SOC Analyst • Program focuses on creating new career opportunities for candidates by providing them with in-demand technical skills, knowledge, and enhanced-level capabilities to dynamically contribute to a SOC team • Candidates seeking certification without official training are required to have 1 year of work experience in information security and must apply for exam eligibility • Exam consists of 100 multiple choice questions • Valid for 3 years • To recertify, you must earn 120 continuing education credits during the 3-year period and pay annual fees	• Tier I and Tier II SOC Analysts • Cyber Security Analysts • Future SOC Analysts • Network and Security Administrators or Engineers • Network Defence Analysts and Technicians

Certified Threat Intelligence Analyst (CTIA)	• Demonstrates that a candidate has the skills to identify and mitigate business risks by converting unknown internal and external threats into quantifiable threat entities and stop them in their tracks • Candidates seeking certification without official training are required to have 2 years of work experience in information security and must apply for exam eligibility • Exam consists of 50 multiple choice questions • Valid for 3 years • To recertify, you must earn 120 continuing education credits during the 3-year period and pay annual fees	• Ethical Hackers • Digital Forensic and Malware Analysts • Threat Intelligent Analysts • Incident Response Team Members • SOC Professionals • Security Practitioners, Engineers, Analysts, Architects, and Managers
Computer Hacking Forensics Investigator (CHFI) – ANSI	• Validates that a candidate has the necessary skills to proactively investigate complex security threats, allowing them to investigate, record, and report cybercrimes to prevent future attacks • Lab-focused, vendor-neutral program • Candidates seeking certification without official training must have 2 years of work experience in information security and must apply for exam eligibility • Exam consists of 150 multiple choice questions • Valid for 3 years • To recertify, you must earn 120 continuing education credits during the 3-year period and pay annual fees	• IT Managers • Digital Forensic Service Providers • Law enforcement personnel • Defence and Security personnel • Government Agencies
Digital Forensics Essentials (DFE)	• Entry-level credential helps candidates increase their competency and expertise in digital forensics and information security skills, thereby adding value to their workplace and employer • No prerequisites • Exam consists of 75 multiple choice questions • Valid for 3 years • DFE is not part of the EC-Council Continuing Education (ECE) scheme. To recertify, a candidate must take the exam again	• Individuals seeking entry-level cyber security or information security roles • Help Desk Technicians • Network Administrators • Network Technicians • Computer Support Specialists

EC Council Disaster Recovery Professional (EDRP)	• Validates a candidate's ability to plan, strategize, implement, and maintain a business continuity and disaster recovery plan • Candidates seeking certification without official training must have at least 2 years of work experience in information security and must apply for exam eligibility • Exam consists of 150 multiple choice questions • Valid for 3 years • To recertify, you must earn 120 continuing education credits during the 3-year period and pay annual fees	• IT Directors and CISOs • IT Risk Managers and Consultants • Business Continuity and Disaster Recovery Consultants • IT Professionals in Disaster Recovery, Business Continuity, and System Administration domains
EC-Council Certified Encryption Specialist (ECES)	• Entry-level certification that introduces professionals and students to the field of cryptography by learning the foundations of modern symmetric and key cryptography • Candidates seeking certification without official training must have at least 1 year of related work experience in information security and must apply for exam eligibility • Exam consists of 50 multiple choice questions • Valid for 3 years • To recertify, you must earn 120 continuing education credits during the 3-year period and pay annual fees	• Cryptanalysts • Cryptographers • Ethical Hackers • Penetration Testers
EC-Council Certified Incident Handler (ECIH) - ANSI	• Validates that a candidate has the knowledge and skills to effectively handle post breach consequences by reducing impact of the incident from both a financial and reputational perspective • Specialist-level program • Candidates seeking certification without official training must have at least 1 year of work experience in information security and must apply for exam eligibility • Exam consists of 100 multiple choice questions • Valid for 3 years • To recertify, you must earn 120 continuing education credits during the 3-year period and pay annual fees	• Risk Assessment Administrators • System Administrators and Engineers • Network and IT Managers • Application Security Engineers • Cyber Forensic Investigators and Analysts • SOC Analysts • Penetration Testers

Ethical Hacking Essentials (EHE)	• Entry-level credential covers ethical hacking and penetration testing fundamentals and prepares learners for a career in cyber security • No prerequisites • Exam consists of 75 multiple choice questions • Valid for 3 years • ECE is not part of the EC-Council Continuing Education (ECE) scheme. To recertify, a candidate must take the exam again	• Individuals seeking entry-level cyber security or information security roles • Help Desk Technicians • Network Administrators • Network Technicians • Computer Support Specialists
Industrial Control Systems and Supervisory Control and Data Acquisitions (ICS/SCADA) Cybersecurity	• Validates a candidate's knowledge of the foundations of security and ability to defend network architectures from attacks • Candidates seeking certification without official training are required to have 1 year of work experience in information security and must apply for exam eligibility • Exam consists of 75 multiple choice questions • Valid for 3 years • To recertify, you must earn 120 continuing education credits during the 3-year period and pay annual fees	• System Administrators and Engineers • SCADA Systems personnel • Business System Analysts who support SCADA interfaces • Security Consultants who perform security assessments of SCADA and/or ICS
Network Defense Essentials (NDE)	• Entry-level credential covers the fundamental concepts of information security and network defense, and is ideal for learners aspiring to pursue a career in cyber security • No prerequisites • Exam consists of 75 multiple choice questions • Valid for 3 years • NDE is not part of the EC-Council Continuing Education (ECE) scheme. To recertify, a candidate must take the exam again	• Individuals seeking entry-level cyber security or information security roles • Help Desk Technicians • Network Administrators • Network Technicians • Computer Support Specialists

5.7 GLOBAL INFORMATION ASSURANCE CERTIFICATION (GIAC)

Table 7 GIAC Certification Listing and Descriptions[9]

Certification	Certification Overview	Intended Candidates
GIAC Advanced Smartphone Forensics (GASF)	• Advanced-level certification • Validates a candidate is qualified to perform forensic examinations on devices such as mobile phones and tablets; and has an understanding of the fundamentals of mobile forensics, device file system analysis, mobile application behaviour, event artifact analysis and the identification and analysis of mobile device malware • Valid for 4 years • Exam consists of 75 questions • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Digital Forensic and Malware Analyst • Cyber Defense Forensic Analysts and Investigators • Penetration Testers • Exploit Developers • Threat Hunters
GIAC Assessing and Auditing Wireless Networks (GAWN)	• Advanced-level certification • Demonstrates knowledge of the different security mechanisms for wireless networks, the tools and techniques used to evaluate and exploit weaknesses, and techniques used to analyze wireless networks. • Exam consists of 75 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Auditors • Ethical Hackers • Penetration Testers • Network Security Professionals • Wireless System Engineers
GIAC Certified Detection Analyst (GCDA)	• Advanced-level certification • Validates a candidate's ability to collect, analyze, and tactically use modern network and endpoint data sources to detect malicious or unauthorized activity	• Security Analysts • Security Architects • Senior Security Engineers • SOC Engineers and Analysts

[9] Every effort has been made to ensure the accuracy of the information in this table; however, the information is subject to change at any time.

Disclaimer: The Communications Security Establishment does not endorse or recommend any of the certification bodies or certifications listed in this document. Information provided is intended to be a general summary of publicly available information and is provided for informational purposes only.

	• GCDA certificate holders are qualified for hands-on leadership positions that deal with Security Information and Event Management (SIEM) • Exam consists of 75 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Cyber Threat Investigators
GIAC Certified Enterprise Defender (GCED)	• Advanced-level certification • Validates a candidate's knowledges and abilities in the areas of defensive network infrastructure, packet analysis, penetration testing, incident handling, and malware remove • Exam consists of 115 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Incident Responders • Penetration Testers • SOC Engineers and Analysts • Network Security Professionals
GIAC Certified Forensic Analyst (GCFA)	• Advanced-level certification • Validates that a candidate has the knowledge, skills, and ability to conduct formal incident investigations and handle advanced incident handling scenarios • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Incident Response Team Members • SOC Analysts • Federal Agents and Law Enforcement Professionals • Digital Forensics Analysts
GIAC Certified Forensic Examiner (GCFE)	• Intermediate-level certification • Validates a candidate's knowledge of computer forensics analysis, including core skills needed to collect and analyze data from Windows systems • Exam consists of 115 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Information Security professionals • Law enforcement members • Digital Forensics and Malware Analysts • Cyber Defense Forensic Analysts and Investigators

GIAC Certified Incident Handler (GCIH)	• Intermediate-level certification • Demonstrates one's ability to detect, respond, and resolve computer security incidents using a wide range of essential security skills • Exam consists of 100-150 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Incident Response Team Members • Cyber Defence Incident Responder
GIAC Certified Intrusion Analyst (GCIA)	• Advanced-level certification • Validates a candidate's knowledge of network and host monitoring traffic analysis, and intrusion detection • Certificate holders are qualified to configure and monitor intrusion detection systems, and to analyze network traffic • Exam consists of 100-150 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Individuals who are responsible for network and host monitoring, traffic analysis, or intrusion detection • Threat Hunters • Security Operations Centre Analysts • Incident Response team members
GIAC Certified Web Application Defender (GWEB)	• Advanced-level certification • Demonstrates that a candidate has mastered the security knowledge and skills needed to deal with common web application errors that lead to most security problems. • Exam consists of 75 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Application Developers • Application Security Analysts • Application Architects • Penetration Testers • Individuals in roles requiring Payment Card Industry (PCI) compliance
GIAC Certified Windows Security Administrator (GCWN)	• Advanced-level certification • Validates a candidate's ability to secure Windows clients and servers, and knowledge of configuring and managing the security of Microsoft operating systems and applications	• Individuals responsible for installing, configuring, and securing Microsoft Windows clients and servers

	• Exam consists of 75 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	
GIAC Continuous Monitoring Certification (GMON)	• Advanced-level certification • Validates a candidate's ability to deter intrusions and quickly detect anomalous activity • Exam consists of 115 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Security Architects • SOC Analysts and Managers • Technical Security manager • Security Engineers
GIAC Critical Controls Certification (GCCC)	• Advanced-level certification • The only certification that is based on the Critical Security Controls, a prioritized, risk-based approach to security. • Validates a candidate's knowledge and skills to implement and execute the Critical Security Controls recommended by the Council on Cybersecurity and perform audits based on the standard. • No prerequisites • Exam consists of 75 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• IT Administrators • Network Security Engineers • Security Vendors • Security Auditors, Chief Information Officers (CIOs), and Risk Officers
GIAC Critical Infrastructure Protection (GCIP)	• Advanced-level certification • Validates a candidate has the knowledge and skills needed to understand the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) regulations and plan practical implementation strategies to achieve regulatory compliance. • Exam consists of 75 questions • Valid for 4 years	• Security Operations Analysts • Team Leaders and Managers • Incident Response Analysts • ICS Cyber Security Practitioners

	• Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	
GIAC Cyber Threat Intelligence (GCTI)	• Advanced-level certification • Validates a candidate's ability to understand and analyze complex threat analysis scenarios; identify, create, and validate intelligence requirements through threat modelling • Exam consists of 75 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Incident Response Team members • Threat Hunters • Intelligence Analysts
GIAC Defending Advanced Threats (GDAT)	• Advanced-level certification • Validates that a candidate has advanced knowledge of how adversaries penetrate networks and what security controls are effective to stop them. • Exam consists of 75 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Security Architects • Security Engineers • Technical Security Managers
GIAC Defensible Security Architecture (GDSA)	• Advanced-level certification • Validates that a candidate's real-world, hands-on skills dealing with network-centric and data-centric approaches to defensible security architecture, hardening applications across the Transmission Control Protocol/Internet Protocol (TSP/IP) stack, and secure environment creation with private, hybrid, or public clouds • Exam consists of 75 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Security Architects • Network Engineers • Security Analysts • Cyber Threat Investigators • Senior Security Engineers • Security Analysts
GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)	• Advanced-level certification	• Vulnerability Testers • Security Analysts

Disclaimer: The Communications Security Establishment does not endorse or recommend any of the certification bodies or certifications listed in this document. Information provided is intended to be a general summary of publicly available information and is provided for informational purposes only.

	• Validates a candidate's ability to find and mitigate significant security flaws in systems and networks • Exam consists of 55-75 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Vulnerability Assessment Analysts
GIAC Information Security Fundamentals (GISF)	• Introductory-level certification • Validates a candidate's knowledge of security's foundation, computer functions and networking, introductory level cryptography, and cyber security technologies • Exam consists of 75 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Management • Information Security Officers • System Administrators • Professionals who need an introduction to cyber security fundamentals
GIAC Information Security Professional (GISP)	• Intermediate-level certification for Managers and Leaders • Validates a candidate's knowledge of the 8 domains of cyber security knowledge, asset security, communications and network security, identity and access management, security and risk management, security assessment and testing, security engineering, security operations, and software development security. • Candidate should have some experience in information systems and networking • Exam consists of 250 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• System Administrators • Security Administrators • Network Administrators • Security Managers
GIAC Mobile Device Security Analyst (GMOB)	• Advanced-level certification • Validates a candidate's to properly secure mobile devices that are accessing vital information • Demonstrates knowledge of assessing and managing mobile device and application security, and mitigating against malware and stolen devices • Exam consists of 75 questions	• Information Security Analysts • Penetration Testers • Ethical Hackers • Network and System Administrators

Disclaimer: The Communications Security Establishment does not endorse or recommend any of the certification bodies or certifications listed in this document. Information provided is intended to be a general summary of publicly available information and is provided for informational purposes only.

	• Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	
GIAC Network Forensic Analyst (GNFA)	• Advanced-level certification • Validates a candidate's ability to perform examinations employing network forensic artifact analysis • Exam consists of 50 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Law Enforcement members • Digital Forensic and Malware Analysts • Cyber Defence Analysts • Incident Response team members • SOC team members
GIAC Penetration Tester (GPEN)	• Advanced-level certification • Validates a candidate's ability to properly conduct a penetration test, using best practice techniques and methodologies • Exam consists of up to 115 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Penetration Tester • Exploit Developers • Network Security personnel • Ethical Hackers
GIAC Response and Industrial Defence (GRID)	• Advanced-level certification • Demonstrates that a candidate understands the Active Defence Approach, ICS-specific attacks, and how these attacks inform mitigation strategies • Exam consists of 75 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Industrial Control System Incident Response Team leads and members • Security Operations Centre Team leads and Analysts • Active Defenders
GIAC Reverse Engineering Malware (GREM)	• Advanced-level certification • Validates a candidate's knowledge and skills to reverse-engineer malware that targets common platforms such as Microsoft Windows and web browsers • Exam consists of 75 questions	• System and Network Administrators • Auditors • Security Managers

	• Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Forensic Investigators
GIAC Security Essentials Certification (GSEC)	• Entry-level certification • Validates an individual's knowledge of information security beyond simple terminology and concepts • Recipients are skilled in active defense, cryptography, security policy and plans, incident handling and securing networks. • Exam consists of 180 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Security Professionals
GIAC Security Expert (GSE)	• Less than 250 GSE certificate holders in the world • Validates that a candidate has mastered the wide variety of skills required by top security consultants and practitioners • Prerequisites are GSEC, GCIH, GCIA with 2 Gold certifications • Exam consists of 2 parts: 24 virtual machine-based hands-on questions and a practical lab • Valid for 4 years • Recertification requires taking the current version of the exam • Renewing GSE certification renews all other active GIAC certifications	• Top Security Consultants and Practitioners
GIAC Security Leadership (GSLC)	• Advanced-level certification for Managers and Leaders • Validates a candidate's knowledge of governance and technical controls focused on protecting, detecting, and responding to security issues • Exam consists of 115 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Managers/Supervisors of Information Security teams • IT Managers

GIAC Systems and Network Auditor (GSNA)	• Advanced-level certification for Managers and Leaders • Validates a candidate's ability to apply basic risk analysis techniques and to conduct technical audits of essential information systems • Exam consists of 115 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Technical staff responsible for securing and auditing information systems • Auditors • Network Administrators • Managers of Audit or Security teams
GIAC Web Application Penetration Tester (GWAPT)	• Advanced-level certification • Validates a candidate's ability to better secure organizations through penetration testing and thorough understanding of web application security issues • Demonstrates knowledge of web applications exploits and penetration testing methodologies • Exam consists of 75 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Penetration Testers • Vulnerability Testers • Security Analysts • Vulnerability Assessment Analysts • Ethical Hackers • Website Designers
Global Industrial Cyber Security Professional (GICSP)	• Advanced-level certification • Assesses a candidate's base level of knowledge and understanding across a diverse set of professionals who engineer or support control systems and share responsibility for the security of these environments • No perquisites • Exam consists of 115 questions • Valid for 4 years • Renewal requires taking the current version of the exam; or obtaining 36 continuing education credits over the 4-year period	• Security Engineers • Industry Managers • Security Analysts

5.8 INTERNATIONAL INFORMATION SYSTEMS SECURITY CERTIFICATION CONSORTIUM

Table 8 (ISC)2 Certification Listing and Descriptions[10]

Certification	Certification Overview	Intended Candidates
Certified Cloud Security Professional (CCSP)	• Co-developed with Cloud Security Alliance (CSA) • Recognizes IT and information security leaders who have the knowledge and skills with cloud security architecture, design, operations, and service orchestration • Candidates require a minimum of 5 years work related experience in IT; at least 3 of those years must be in information security and 1 year in one of the 6 domains of CCSP Common Body of Knowledge • Exam consists of 125 multiple choice questions • Valid for 3 years • Recertification requires obtaining 90 continuing education credits during 3-year period	• Enterprise Architect • Systems Engineer • Systems Architect • Security Administrator • IT and Information Security Leaders

Certified Information Systems Security Professional (CISSP)	• Advanced-level certification
	• Candidates require a minimum of 5-years related work experience in at least 2 of the 8 (ISC)2 common body of knowledge of domains; or 4-years of work experience and a college degree or other approved credential
	• Exam consists of 100-150 item computer adaptive testing
	• Valid for 3 years
	• Recertification requirements include obtaining 120 continuing professional education credits during the 3-year period
	• Three concentrations are also available to those possessing valid CISSP certification:
	  ○ CISSP-ISSAP (Architecture)
	  ○ CISSP-ISSEP (Engineering)
	  ○ CISSP-ISSMP (Management)
		• Chief Information Security Officer
		• Chief Security Officer
		• Security Analyst/Auditor
		• Director of Security
		• IT Director/Manager

[10] Every effort has been made to ensure the accuracy of the information in this table; however, the information is subject to change at any time.

Disclaimer: The Communications Security Establishment does not endorse or recommend any of the certification bodies or certifications listed in this document. Information provided is intended to be a general summary of publicly available information and is provided for informational purposes only.

Healthcare Information Security and Privacy Practitioner (HCISPP)	• Validates knowledge and skills to implement, manager, or assess security and privacy controls for healthcare and patient information • Designed for practitioners and consultants in healthcare information security and privacy • Candidates require a minimum of 2-years work experience • Exam consists of 125 multiple choice questions • Valid for 3 years • Recertification requires obtaining 60 continuing education credits during the 3-year period	• Compliance Officer • Medical Records Supervisor • Practice Manager • Information Security Manager • Health Information Manager
Systems Security Certified Practitioner (SSCP)	• Global IT security certification • Entry-level certification • Demonstrates that the holder has the technical skills and knowledge to implement, monitor, and administer an IT infrastructure. • Designed for practitioners in operational IT roles or in information security • Candidates must have 1 year of cumulative work experience in one or more of the 7 domains of SSCP Common Body of Knowledge; a 1-year experience waiver will be granted to candidates who hold a bachelor's or master's degree in Cyber Security • Exam consists of 125 multiple choice questions • Valid for 3 years • Recertification requires obtaining 60 continuing education credits during the 3-year period	• Network Security Engineer • Systems Administrator • Security Analyst • Systems/Network Analyst • Security Consultant • IT Administrators, Directors, or Managers

5.9 ISACA

Table 9 ISACA Certification Listing and Descriptions[11]

Certification	Certification Overview	Intended Candidates
Certified Cybersecurity Practitioner (CSX-P)	• New certification created in 2015 • Recognizes individuals who can act as first responders for security incidents • The only certification that tests one's ability to perform globally validated cyber security covering the 5 core functions of the NIST Cyber Security Framework; Identify, Protect, Detect, Respond, and Recover • Candidates must pass a performance-based exam consisting of simulated security incidents. • Valid for 3 years • Recertification requirements include obtaining 120 hours of continuing professional education during 3-year period	• Security Practitioners • Incident Handlers
Certified in Risk and Information Systems Control (CRISC)	• Recognizes those who identify, evaluate, and manage risk through the development, implementation, and maintenance of information systems controls • Candidates must have 3-years of professional-level risk management and control experience, no education substitutes • Valid for 3 years • Recertification requirements include obtaining 120 hours of continuing professional education during a 3-year period	• IT and Business professionals • Risk and Compliance professionals • Business Analysts • Project Managers • Security directors
Certified Information Security Manager (CISM)	• Management focused certification • Recognizes candidates who manage, design, oversee, and assess an enterprise's information security	• Information security managers and directors • IT Security Analysts • Risk Analysts • IT Auditor

[11] Every effort has been made to ensure the accuracy of the information in this table; however, the information is subject to change at any time.

Disclaimer: The Communications Security Establishment does not endorse or recommend any of the certification bodies or certifications listed in this document. Information provided is intended to be a general summary of publicly available information and is provided for informational purposes only.

	• Candidates require a minimum of 5-years of information security experience gained within the 10-year period before writing the exam • Written application is required • Exam consists of 150 questions / 4 hours long • Valid for 3 years • Recertification requirements include obtaining 120 hours of continuing professional education during 3-year period	• Information Systems Security Manager
Certified Information Systems Auditor (CISA)	• Globally recognized certification • Validates a candidate's audit experience, skills and knowledge, and ability to assess vulnerabilities, report on compliance and institute controls within the enterprise • Candidates require 5 years of professional information systems (IS) auditing, control or security work experience; some education substitutes • Exam consists of 150 questions • Certificate holders are required to take at least 120 hours of continuing education during the 3-year period	• IS audit control, assurance, and security professionals

5.10 ITSM SOLUTIONS

Table 10 itSM Solutions Certification Listing and Descriptions[12]

Certification	Certification Overview	Intended Candidates
NIST Cyber Security Professional (NCSP) Foundation	• Entry-level certification • Validates that a candidate has the knowledge and ability to operationalize the NIST Cyber Security Framework • No prerequisites but basic computing skills and security knowledge are recommended • Exam consists of 40 multiple choice questions	• Security, IT, Risk Management professionals • Auditors • Other professions who need to understand the basics of cyber security, the components of the NIST Cyber Security Framework and how it aligns to risk management
NCSP Practitioner	• Validates a candidate's skills and abilities to design, build, test, manage, improve a cyber security program based on NCSF • Candidates must complete the NCSF Foundation training/exam before attempting the exam • Exam consists of 65 multiple choice questions	• IT and Cyber Security Professionals

[12] Every effort has been made to ensure the accuracy of the information in this table; however, the information is subject to change at any time.

Disclaimer: The Communications Security Establishment does not endorse or recommend any of the certification bodies or certifications listed in this document. Information provided is intended to be a general summary of publicly available information and is provided for informational purposes only.

5.11 MCAFEE INSTITUTE

Table 11 McAfee Institute Certification Listing and Descriptions[13]

Certification	Certification Overview	Intended Candidates
Certified Counterintelligence Threat Analyst (CCTA)	• Validates a candidate's ability to identify and investigate cyber criminals, conduct cyber counterintelligence investigations to mitigate threats, and investigate and prosecute hackers and cyber criminals • Prerequisites: Bachelor's degree or higher and 3 years of experience in a related field, or associate degree and 4 years of experience • Candidates must pass a background check • Exam consists of 200 questions • Valid for 2 years • To renew, candidates must pay a renewal fee and obtain continuing education credits	• Individuals in cyber security, law enforcement, loss prevention roles
Certified Cyber Intelligence Investigator (CCII)	• Validates a candidate's ability to conduct cyber investigations, utilize methodologies to prosecute cyber criminals, apply mobile and digital forensics, recognize fraud and hacking, and develop intelligence gathering • Perquisites: Bachelor's degree or higher and 1 year of experience in a related field, or an associate degree and 2 years of experience • Candidates must pass a background check • Exam consists of 200 questions • Valid for 2 years • To renew, candidates must pay a renewal fee and obtain continuing education credits	• Individuals in cyber security, law enforcement, loss prevention roles

[13] Every effort has been made to ensure the accuracy of the information in this table; however, the information is subject to change at any time.

Disclaimer: The Communications Security Establishment does not endorse or recommend any of the certification bodies or certifications listed in this document. Information provided is intended to be a general summary of publicly available information and is provided for informational purposes only.

Certified Cyber Intelligence Professional (CCIP)	• Validates a candidate's ability to conduct cyber investigations, utilize methodologies to prosecute cyber criminals, design and implement a cyber program, understand mobile and digital forensics, and recognize fraud and hacking • Perquisites: Bachelor's degree or higher and 3 years of experience in a related field, or an associate degree and 4 years of experience • Candidates must pass a background check • Exam consists of 200 questions • Valid for 2 years • To renew, candidates must pay a renewal fee and obtain continuing education credits	• Individuals in cyber security, law enforcement, loss prevention roles
Certified Expert in Cyber Investigations (CECI)	• Validates a candidate's ability to recognize and identify cyber criminals, conduct cyber counterintelligence investigations to mitigate threats, protect an organization's assets and information, and investigate and prosecute hackers and cybercriminals • Prerequisites: Bachelor's degree or higher and 4 years of experience in a related field, or an associate degree and 6 years of experience • Candidates must pass a background check • Exam consists of 200 true/false, multiple choice, and scenario-based questions. • Valid for 2 years • To renew, candidates must pay a renewal fee and obtain continuing education credits	• Individuals in cyber security, law enforcement, loss prevention roles

5.12 OFFENSIVE SECURITY

Table 12 Offensive Security Certification Listing and Descriptions[14]

Certification	Certification Overview	Intended Candidates
Offensive Security Certified Expert (OSCE)	• Demonstrates that a candidate has a mastery of advanced penetration testing skills; analyze, correct, modify, and port exploit code; and craft binaries to evade antivirus software • Candidates should have prior knowledge of Windows exploitation techniques, Linux experience, and a solid understanding of TCP/IC and networking • Candidates must complete the *Cracking the Perimeter* course before attempting exam • Exam has a 48-hour time limit and consists of hands-on penetration testing in an isolated virtual private network (VPN); must also submit a comprehensive test report	• Penetration Testers • Security Professionals
Offensive Security Certified Professional (OSCP)	• Validates the knowledge and skills needed to identify vulnerabilities and execute organized attacks in a controlled and focused manner • Intended for penetration testers with strong technical and ethical hacking backgrounds, and a solid understanding of TCP/IP networking • Candidates must first complete the *Penetration Testing* training course • Certification is hard to obtain due to its notoriously difficult exam • Candidates must pass a 24-hour exam where they are required to attack and penetrate live machines in a safe lab environment; must also submit a comprehensive penetration test report • Certification never expires	• Penetration Testers • Network Administrators • Network Security Professionals
Offensive Security Exploitation Expert (OSEE)	• Requires significant time investment • Validates a candidate's ability to analyze vulnerable software, find problematic code, develop sophisticated exploits under various modern Windows operating systems	• Penetration Testers

[14] Every effort has been made to ensure the accuracy of the information in this table; however, the information is subject to change at any time.

Disclaimer: The Communications Security Establishment does not endorse or recommend any of the certification bodies or certifications listed in this document. Information provided is intended to be a general summary of publicly available information and is provided for informational purposes only.

	• Candidates should have experience in developing windows exploits and understand how to operate a debugger • Candidates must complete the *Advanced Windows Exploitation* course before attempting the exam • Candidates should obtain OSCE certification first • Exam consists of developing and documenting exploits during a 72-hour period; must also submit a comprehensive penetration test report • Certification qualifies the recipient for 40 (ISC)2 continuing education credits • Certification never expires	
Offensive Security Web Expert (OSWE)	• Validates that a candidate has practical knowledge of web application assessment and hacking process; and ability to review advanced source code in web applications, identify vulnerabilities, and exploit them • Candidates should have familiarity with coding languages and Linux, ability to write scripts, experience with web proxies, a general understanding of web app attack vectors, theory and practice, and a solid understanding of TCP/IP and networking • Candidates are required to take the *Advanced Web Attacks and Exploitation* course before attempting the exam • 48-hour exam consisting of hands-on web application assessment in an isolated VPN network; successful candidates must also submit an assessment report • Certification never expires	• Penetration Testers • Web Application Security Specialists • Software Engineers • Web Developers
Offensive Security Wireless Professional (OSWP)	• Validates a candidate's ability to identify existing encryptions and vulnerabilities in Institute of Electronic Engineers (IEEE) 802.11 networks, circumvent security restrictions and recover encryption keys in use • Candidates must have a solid understanding of TCP/IP and the Open Systems Interconnection (OSI) model, familiarity with Linux • Candidates must complete the *Offensive Security Wireless Attacks* course before attempting the exam • 4-hour exam requires that candidate to conduct wireless info gathering, and implement various attacks to get access to the target networks; must also submit a penetration test report	• Network Administrators • Penetration Testers

	• Certification never expires	

5.13 PECB

Table 13 PECB Certification Listing and Descriptions[15]

Certification	Certification Overview	Intended Candidates
Certified Lead Ethical Hacker	• Validates a candidate's knowledge of information gathering tools and techniques, threat modeling and vulnerability identification, exploitation techniques, reporting, etc. • Candidates are required to have knowledge of information security concepts and principles and advanced skills in operating systems • Candidates are required to have 2 years of penetration testing and cyber security experience. • Candidates are required to sign the PECB Code of Ethics and the PECB CLEH Code of Conduct • 6-hour open book exam consists of 2 parts: the candidate must first compromise 2 or more target machines through penetration testing, then document the process in a written report • Valid for 3 years Renewal requirements include demonstrating that you have are still performing tasks related to the certification, meeting the required number of Continuing Professional Development (CPD) credits, and paying the annual maintenance fee	• Individuals responsible for the security of information systems • Information Security team members
Computer Forensics Foundation	• Validates a candidate's knowledge of the fundamental principles and concepts of computer forensics and computer forensics processes • No prerequisites • Candidates are required to sign the PECB Code of Ethics • 1-hour open book exam consists of 5 essay type questions • Valid for 3 years	• Individuals interested in pursuing a career in Computer Forensics

[15] Every effort has been made to ensure the accuracy of the information in this table; however, the information is subject to change at any time.

Disclaimer: The Communications Security Establishment does not endorse or recommend any of the certification bodies or certifications listed in this document. Information provided is intended to be a general summary of publicly available information and is provided for informational purposes only.

	• Renewal requirements include demonstrating that you have are still performing tasks related to the certification, meeting the required number of Continuing Professional Development (CPD) credits, and paying the annual maintenance fee	
ISO/IEC 27032 Foundation	• Validates an individual's knowledge of the fundamental cyber security principles and concepts, and understanding of the approaches, methods, and techniques used in cyber security • No prerequisites • Candidates are required to sign the PECB Code of Ethics • 1 hour exam consists of 40 multiple choice questions • Valid for 3 years • Renewal requirements include demonstrating that you have are still performing tasks related to the certification, meeting the required number of Continuing Professional Development (CPD) credits, and paying the annual maintenance fee	• Cyber security and Information Security professionals • Individuals interested in pursuing a career in cyber security
ISO/IEC 27032 Lead Cybersecurity Manager • Certified Provisional • Certified • Certified Lead • Certified Senior Lead	• Validates a candidate's knowledge of the fundamental principles and concepts of cyber security, roles and responsibilities of stakeholders, cyber security risk management, attack mechanisms and cybersecurity controls, information sharing and coordination, integrating a cyber security program in business continuity management, and cyber security incident management and performance measurement • Candidates are required to have a fundamental understanding of ISO/IEC 27032 and comprehensive knowledge of cyber security • Candidates are required to sign the PECB Code of Ethics • 3-hour open book exam consists of 12 essay type questions • Candidates who pass the exam can apply for 1 of 4 credentials based on the number of years of work experience, cyber security experience, and total number of hours of cyber security activities • Valid for 3 years • Renewal requirements include demonstrating that you have are still performing tasks related to the certification, meeting the required number of Continuing Professional Development (CPD) credits, and paying the annual maintenance fee	• Cyber security and Information Security Professionals • Individuals responsible for developing and/or managing a cyber security program

Lead Cloud Security Manager • Certified Provisional • Certified • Certified Lead • Certified Senior Lead	• Validates a candidate's knowledge of the principles and concepts of cloud computing, cloud computing risk management and incident management, cloud security testing, monitoring, and continual improvement, etc. • Candidates are required to have a fundamental knowledge and understanding of ISO/IEC 27019 and ISO/IEC 27018 and general knowledge of cloud computing systems • Candidates are required to sign a PECB Code of Ethics • 3-hour open book exam consists of 80 multiple choice questions • Candidates who pass the exam can apply for 1 of 4 credentials (based on the number of years of work experience, cyber security experience, and total number of hours of Central Configuration Setting Management System (CCSMS) project activities • Valid for 3 years • Renewal requirements include demonstrating that you have are still performing tasks related to the certification, meeting the required number of Continuing Professional Development (CPD) credits, and paying the annual maintenance fee	• Cloud Security and Information Security Professionals • Individuals responsible for maintaining and managing a cloud security program Cloud Security Expert Advisors
Lead Forensics Examiner • Certified Provisional • Certified • Certified Lead	• Validates a candidate's knowledge of the fundamental principles and concepts of computer forensics, digital forensics lab requirements, computer crime investigation and forensics examinations, and maintaining chain of evidence • Candidates are required to have knowledge of computer forensics • Candidates are required to sign the PECB Code of Ethics • 3-hour exam open book exam consists of 14 essay type questions • Candidates who pass the exam can apply for 1 of 3 credentials (based on the number of years of work experience, cyber security experience, and total number of hours of forensics activities • Valid for 3 years • Renewal requirements include demonstrating that you have are still performing tasks related to the certification, meeting the required number of Continuing Professional Development (CPD) credits, and paying the annual maintenance fee	• Computer Forensics specialists and consultants • Cyber Security professionals • Cyber Intelligence Analysts • Law Enforcement professionals • Electronic Data Analysts

Lead Pen Test Professional • Certified Provisional • Certified • Certified Lead	• Validates a candidate's knowledge of the fundamental principles and concepts in penetration testing, technical foundation of penetration testing, testing types, and analyzing results and the reporting process • Candidates are required to have a fundamental understanding of penetration testing and comprehensive knowledge of cyber security • Candidates are required to sigh the PECB Code of Ethics • 3-hour exam consists of 150 multiple choice questions • Candidates who pass the exam can apply for 1 of 3 credentials (based on the number of years of work experience, pen testing experience, and total number of hours of pen testing activities • Valid for 3 years • Renewal requirements include demonstrating that you have are still performing tasks related to the certification, meeting the required number of Continuing Professional Development (CPD) credits, and paying the annual maintenance fee	• IT Professionals • Auditors • IT and Risk Mangers • Penetration Testers • Ethical Hackers

5.14 SECO INSTITUTE

Table 14 SECO Institute Certification Listing and Descriptions[16]

Certification	Certification Overview	Intended Candidates
Certified Ethical Hacker (S-EHE)	• Program is currently being re-designed	• N/A
Dark Web Foundations	• Entry-level certification • Developed by the Netherlands Organisation for Applied Scientific Research in collaboration with the International Criminal Police Organization (INTERPOL) • Demonstrates that a candidate understands how to use the dark web in a secure way • Exam consists of 40 multiple choice questions • Valid for life and is not subject to re-certification requirements	• IT Security Professionals • Law Enforcement • Policy makers and Government Officials
Ethical Hacking Foundations (S-EHF)	• Entry-level certification • Validates that a candidate has an in-depth understanding of basic penetration testing techniques and possesses fundamental hacking skills • Exam consists of 40 multiple choice questions • Valid for life and is not subject to re-certification requirements	• Web Developers • Computer Software Engineers • Security Administrator • Network Engineer • Ethical Hackers
Ethical Hacking Leader (S-EHL)	• Highest achievable qualification in the Ethical Hacking certification track • Demonstrates that a candidate has excellent penetration testing skills and experience in leading penetration tests • Candidates must have expert-level knowledge (SECO Expert level certificate or equivalent) and at least 3 years of relevant work experience • No exam • Valid for 1 year	• Professionals who seek to validate the expertise they have built up through hands-on work experience

[16] Every effort has been made to ensure the accuracy of the information in this table; however, the information is subject to change at any time.

Disclaimer: The Communications Security Establishment does not endorse or recommend any of the certification bodies or certifications listed in this document. Information provided is intended to be a general summary of publicly available information and is provided for informational purposes only.

	• To renew, candidates must pay annual membership fees and obtain 40 continuing education credits during the year	
Ethical Hacking Practitioner (S-EHP)	• Validates that a candidate has a full understanding of the penetration testing process and familiarity with common penetration testing techniques • Candidates should have a good understanding of ethical hacking fundamentals • S-EHF certificate (or equivalent) is recommended • 3-part exam: 10 multiple choice questions, 5 essay type questions and 1 case study • Valid for 1 year • To renew, candidates must pay annual membership fees and obtain 20 continuing education credits during the year	• Web Developers • Security Administrators • Network Engineers • Computer Software Engineers • Aspiring Penetration Testers
IT Security Expert/SOC (S-ITSE/SOC)	• Validates that a candidate has acquired the knowledge and skills necessary to assume responsibility for threat detection, analysis and response, and can improve an organization's overall security poster • Candidates should have a basic understanding of TCP/IP, operating system fundamentals and common security concepts, and 2 years of experience in a SOC • Prerequisite is the S-ITSP or equivalent • Candidates can choose 1 of 2 specializations: SOC Manager or IT Security Manager • Valid for 1 year • To renew, candidates must pay annual membership fees and obtain 40 continuing education credits during the year	• Individuals that want to become Tier I/Tier II Soc Analysts • Future SOC Managers • System Engineers • Security Analysts
IT Security Foundation (S-ITSF)	• Entry-level certification • Validates that a candidate has a basic understanding of computer architecture, common hardware vulnerabilities and security measures • No prerequisites and suitable for beginners with basic understanding of computers and technology • Exam consists of 40 multiple choice questions • Valid for life and not subject to re-certification requirements	• Network or System Administrator • Individuals looking to start a career in IT Security

IT Security Practitioner (S-ITSP)	• Validates a candidate's technical competencies in vulnerability management, firewall and network security, security architecture and penetration testing • Candidates should have a good understanding of fundamental IT security terms, concepts and principle • IT Security Foundation certificate (or equivalent) is recommended • Exam includes 10 multiple choice questions, 5 open questions, and 1 case study • Valid for 1 year • To renew, candidates must pay annual membership fees and obtain 60 continuing education credits during the year	• Security Administrators • Security Analysts • Security Architects • Security Auditors • Future SOC Analysts

6.0 SUPPORTING CONTENT

6.1 LIST OF ABBREVIATIONS

Term	Definition
AI	Artificial Intelligence
(ICS)2	International Information Systems Security Certification Consortium
C3	Cyber Credentials Collaborative
CCSMS	Central configuration setting management system
CNSS	Committee on National Security Systems
CompTIA	Computing Technology Industry Association
CREST	Council for Registered Ethical Testers
CSA	Cloud Security Alliance
CSE	Communications Security Establishment
CWNP	Certified Wireless Network Professionals
Cyber Centre	Canadian Centre for Cyber Security
GIAC	Global Information Assurance Certification
GCHQ	Government Communications Headquarters
IAS	International Accreditation Service
IEC	International Electrotechnical Commission
ICS	Industrial control systems
IEEE	Institute of Electronic Engineers
INTERPOL	International Criminal Police Organization
IoT	Internet of Things
IS	Information System
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
IT	Information technology
NERC CIP	North American Electric Reliability Corporate Critical Infrastructure Protection
NICCS	National Initiative for Cyber Security Careers and Studies
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating system
OSI	Open systems interconnection
PCI	Payment card industry
RBC	Royal Bank of Canada

RFID	Radio frequency identification
SCADA	Supervisory control and data acquisitions
SDLC	Software development life cycle
SECO	Security and Continuity Institute
SIEM	Security Information and Event Management
SOC	Security Operations Centre
TSP/IP	Transmission control Protocol/Internet Protocol
UKAS	United Kingdom Accreditation Service
VPN	Virtual private network
WLAN	Wireless local area network

6.2 REFERENCES

Number	Reference
1	Steve Morgan. "10 Hot Cybersecurity Certifications for IT Professionals to Pursue in 2020", *Cyber Crime Magazine.* 24 May, 2020. https://cybersecurityventures.com/10-hot-cybersecurity-certifications-for-it-professionals-to-pursue-in-2019/