PRUDENCE COLLEGE DUBLIN

Leading the transition towards a brighter future

Url: www.prudencecollege.ie
E-mail: info@prudencecollege.ie; Tel: +353 (0)1 254 8998; (0)87 466 9418

CompTIA Security Analytics Expert (CSAE)

(NFQ Level 7: Advanced Diploma/Ordinary Graduation)

(CompTIA A+, Network+, Security+, CySA+, PenTest+, CASP+)

Course Overview

Although the internet has improved people's lives through better and more accessible communication, and information exchange it has also had significant negative issues. Over recent years, cases of online fraud, cyber-bullying, racial abuse, gambling, and pornography have increased, warranting a need to create a greater awareness of the negative impacts of using the internet and to educate users on how to operate safely in cyberspace whilst ensuring the security of personal data. Consequently a workforce with the education and skills to identify cyber security flaws and their resolution is in high demand globally. The offered cybersecurity pathway course will equip students to identify and understand the issues associated with internet use and provide them with the experience and skills to tackle modern security issues associated with network systems and servers.

The CompTIA A+ certification is an entry-level/foundational qualification for the IT industry designed to provide a basic understanding of hardware, networking, and computer systems while gaining the relevant additional skills. The CompTIA Network+ delivers a fundamental understanding of networking from Local Area Network (LAN) management, and Internet Protocol (IP) tasks for performing hardware-software maintenance of Networks following the best security practices. The CompTIA Security+ provides a basic understanding of cybersecurity to assess the security position of an enterprise environment, identify appropriate security solutions, monitor and secure cloud and Internet of Things (IoT), maintain relevant policies and laws, as well as identify, analyze, and counter security incidents. The CompTIA CySA+ applies behavioral analytics to networks to improve the overall security posture by identifying and combating malware and advanced persistent threats, increasing threat visibility across a wide range of potential attacks, enhancing the ability of IT professionals to proactively defend and continuously improve organizational security. The CompTIA Pentest+ develops students' skill in the latest penetration testing methods and vulnerability assessments, enhances management skills needed to determine network resilience to attacks, and provides an understanding of legal and compliance requirements as well as vulnerability scanning, PenTest tools and technology, repair techniques, etc. The CompTIA Advanced Security Practitioner+ (CASP+) is an advanced-level cybersecurity certification for security architects and senior security engineers charged with leading and improving an enterprises cybersecurity readiness.

Upon completion of all courses, students will receive stackable certifications separately from CompTIA and an advanced diploma/ordinary graduation (accreditation is in progress) at NFQ level 7 equivalent from PCD. The learning materials provided will allow students to study for and pass both CompTIA A+, Network+, Security+, CySA+, CompTIA PenTest+, CompTIA CASP+ exams, leading to their qualification as a Cybersecurity and Network Security Analytics expert with further progression opportunities.

Course format

The two components making up this course are:

- CompTIA A+ 220-1001 (Core 1) and 220-1002 (Core 2)
- CompTIA Network+ N10-007
- CompTIA Security+ SY0-601
- CompTIA CySA+ CS0-002
- CompTIA PenTest+ PT0-002
- CompTIA CASP+ CAS-004

This course is designed not only for beginners who are seeking foundational knowledge for achieving expert level (NFQ Level 7 equivalent) but also for intermediate learners intending to progress to the next level of diploma/degree and advanced certification courses from CompTIA, such as CompTIA Security Infrastructure Expert (CSIE) and CompTIA Security Analytics Expert (CSAE).

The course will be delivered as either a Face-to-Face (in-classroom) or Virtual Classroom (instructor-led, real time) format and/or a Blended Learning environment. In addition to classes and hands-on training, course material/handouts will be accessible to students for further study either as hard copy (charge may apply) and/or online (Virtuline Hub). In addition, several sample tests, practical exercises/lab work, guided and self-paced study sessions, online problem-solving exercises etc. will be arranged by the instructor to assist in exam preparation and the student's final certification as a Cybersecurity Analytics Expert.

Entry level

The course is designed for students, professionals, and avid learners having 0 to 3 years of experience in the field of IT. Students who have completed NFQ Level 6 at PCD can carry over their credentials to take the remaining courses to obtain a Level 7 equivalent qualification.

Modules

CompTIA A+

Module 1: CompTIA A+ Hardware
Module 2: CompTIA A+ Networking
Module 3: CompTIA A+ Mobile Devices
Module 4: CompTIA A+ Hardware and Network Troubleshooting
Module 5: CompTIA A+ Windows Operating Systems
Module 6: CompTIA A+ Other Operating Systems and Technologies
Module 7: CompTIA A+ Security
Module 8: CompTIA A+ Software Troubleshooting
Module 9: CompTIA A+ Operational Procedures

CompTIA Network +

Module 1 / CompTIA Network+ Local Area Networks
Module 2 / CompTIA Network+ IP Addressing
Module 3 / CompTIA Network+ Internetworking
Module 4 / CompTIA Network+ Applications and Security
Module 5 / CompTIA Network+ Operations and Infrastructure

CompTIA Security+

Module 1: CompTIA Security+ Threats, Attacks, and Vulnerabilities
Module 2: CompTIA Security+ Architecture and Design
Module 3: CompTIA Security+ Implementation
Module 4: CompTIA Security+ Operations and Incident Response
Module 5: CompTIA Security+ Governance, Risk, and Compliance

CompTIA CySA+

Module 1: CompTIA CySA+ Threat and Vulnerability Management
Module 2: CompTIA CySA+ Software and Systems Security
Module 3: CompTIA CySA+ Security Operations and Monitoring
Module 4: CompTIA CySA+ Incident Response
Module 5: CompTIA CySA+ Compliance and Assessment

CompTIA Pentest+

Module 1: CompTIA PenTest+ Topic Planning and Scoping
Module 2: CompTIA PenTest+ Information Gathering and Vulnerability Identification
Module 3: CompTIA PenTest+ Attacks and Exploits
Module 4: CompTIA PenTest+ Penetration Testing Tools
Module 5: CompTIA PenTest+ Reporting and Communication

CompTIA CASP+

Module 1: CompTIA CASP+ Topic Security Architecture
Module 2: CompTIA CASP+ Security Operations
Module 3: CompTIA CASP+ Security Engineering and Cryptography
Module 4: CompTIA CASP+ Governance, Risk, and Compliance

Learning outcomes

This level 7 cybersecurity pathway will enable students to describe the advanced contents of networking and security and allow to diagnose security issues at relevant systems. This includes how to**:**

- Demonstrate baseline security skills for IT support professionals.
- Configure device operating systems, including Windows, Mac, Linux, Chrome OS, Android and iOS and administer client-based as well as cloud-based (SaaS) software.
- Troubleshoot and problem solve core service and support challenges while applying best practices for documentation, change management, and scripting.
- Support basic IT infrastructure and networking.
- Configure and support PC, mobile and IoT device hardware.
- Implement basic data backup and recovery methods and apply data storage and management best practices.
- Identify basic network theory concepts and major network communications methods.
- Describe bounded network media.
- Identify unbounded network media and the major types of network implementations.
- Identify TCP/IP addressing, and data delivery methods and the major services deployed on TCP/IP networks, and implementation of routing technologies.
- Identify the infrastructure of a WAN implementation.
- Identify the components used in cloud computing and virtualization.

- Describe basic concepts related to network security, prevention of security breaches, and responding to security incidents.
- Leveraging and applying proactive threat intelligence to security support
- Vulnerability management organization and activities.
- Apply security solutions to infrastructure management and explain software and hardware assurance best practices.
- Apply the concept of security to support organizational risk mitigation and understand the importance of frameworks, policies, procedures, and controls.
- Analyze data as part of ongoing security monitoring activities and make configuration changes to existing controls to improve security.
- Apply appropriate incident response procedures, analyze potential indicators of danger, and use basic digital forensic techniques.
- Identify the components used in cloud computing and virtualization.
- Describe basic concepts related to network security, prevention of security breaches, and responding to security incidents.
- Identify the components of a remote network implementation, the tools, methods, and techniques used in managing a network.
- Describe troubleshooting of issues on a network.
- Describe attacks, and vulnerabilities on the Internet from newer custom devices IoT and embedded devices
- Identity Administration, access management, PKI, basic cryptography, wireless, and end-to-end security.
- Organizational security assessment and incident response procedures, such as basic threat detection, risk mitigation techniques, security controls, and basic digital forensics.
- Organizational risk management and compliance to regulations, such as PCI-DSS, SOX, HIPAA, GDPR, FISMA, NIST, and CCPA.

Job Opportunities

- Field Service Technician.
- Help Desk Technician.
- IT Specialist.
- Technical Support Specialist.
- IT Support Manager.
- Junior Network Administrator.
- Junior Systems Engineer.
- Network Support Specialist.
- Systems Analyst.
- Tier I and/or Tier II Support Specialist.
- Security Administrator.
- Systems Administrator.
- Helpdesk Manager/Analyst.
- Network Engineer.
- Security Engineer/Analyst.
- DevOps/Software Developer.
- Security analyst.
- Tier I - II SOC analyst.
- Network Security Engineer.
- Threat Intelligence Analyst.
- Security Engineer.
- Application Security Analyst.
- Network Incident Handler
- Compliance Analyst.
- Threat Hunter.
- Security Architect.
- Senior Security Engineer.
- SOC (Security Operation Center) Manager.
- Security Analyst.
- Security Analyst Engineer.
- Security Infrastructure Engineer.

Credentials

Upon completion of A+, Network+, Security+, CySA+, PenTest+, CASP+ exams, CompTIA will issue digital certification badge(s) from Credly and grant the respective stackable certification(s) automatically via certmetrics. Student will have the global recognition as a Network Security Analytics Expert and will obtain a certificate of course completion from PCD with an Irish NFQ 7 equivalent credential (Advanced Diploma/Graduation degree to BSc in Cybersecurity, additional accreditation is in progress). Besides they will also obtain the following stackable certification from CompTIA:

- CompTIA IT Operations Specialist.
- CompTIA Secure Infrastructure Specialist.

- CompTIA Security Analytics Professional.
- CompTIA Network Security Professional.
- CompTIA Network Vulnerability Assessment Professional.
- CompTIA Security Infrastructure Expert.
- CompTIA Security Analytics Expert

The CompTIA credentials will not only make students workplace ready but also facilitate further progress by allowing students to take other advanced courses such as CompTIA Data+, CompTIA Project+, and CompTIA Cloud Essentials+, enabling to become a relevant professional and expert.

Course duration

Standard: 24 months (Flexible: weekdays/weekends; mornings/afternoons/evenings)
Intensive: 1-2 weeks in each 3-month period to complete by 24 months.

- A semisterwise class routine will be available a month before starting the classes.
- A minimum number of students' enrolment is required to start the course.