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 Professional (CSAP)

(NFQ Level 6: Diploma in Advanced Cybersecurity)

(CompTIA A+, Security+, CySA+)

Course Overview

What would the world do if there were no security for personal or institutional data? The threat of data breaches is ever present and continues to affect many commercial and state enterprises so that effective measures that reduce the vulnerability of the systems they use and the likelihood of cyber attacks, are required. CompTIA has designed Cybersecurity course pathways to enable students to identify and fix security flaws/vulnerabilities, and prevent cyber-attacks. As attackers learn to circumvent traditional signature-based solutions, such as firewalls and anti-virus software, the scan-based approach in the IT security industry is becoming increasingly more important at organizational levels. This pathway will equip students to understand and tackle modern security issues associated with network systems and servers.

The CompTIA A+ course is designed to provide a basic understanding of hardware, networking, and computer systems as well as the relevant operational skills. This course containing relevant networking concepts also provides a platform for developing the next level of skills, such as Network+. The CompTIA Security+ provides a basic understanding of cybersecurity so that students can assess the vulnerability of an enterprise environment and implement the required security solutions, monitor, and secure cloud and IoT, maintain prominent laws and policies, and identify, analyze, and counter security incidents. CompTIA CySA+ applies behavioral analytics to networks in order to improve the overall security posture by identifying and combating malware and advanced persistent threats, increasing threat visibility across a wide range of attacks. This will provide the knowledge base for IT professionals to proactively defend and continuously improve organizational security.

Upon completion of A+, Security+ and CySA+ courses, enabling to gain the knowledge and skills required for managing the flow and the optimization of day-to-day cybercurity-related workplace activities, students will receive certification independently and/or stackable from CompTIA as well as NFQ Level 6 equivalent Cybersecurity professional certification from PCD. The learning materials provided will allow students to study for and pass CompTIA A+, Security+, and CySA+ exams, leading to their designation as a Cybersecurity and Network Security Analysis Professional.

Course format

The components making up this course are:

- CompTIA A+ 220-1001 (Core 1) and 220-1002 (Core 2)
- CompTIA Security+ SY0-601
- CompTIA CySA+ CS0-002

This pathway course is designed not only for beginners who are seeking foundational knowledge for reaching professional level (NFQ Level 6 equivalent) but also for intermediate learners intending to progress to the next level of diploma/degree from PCD and advanced certification courses from CompTIA such as CompTIA Security Analytics Expert (CSAE).

The course will be delivered as either Face-to-Face (in-classroom) or through a 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 students final certification as a Cybersecurity Analytics Professional.

Entry level

The course is designed for students, professionals, and avid learners having 0 to 2 years of experience in the field of IT. Students completed NFQ Level 5 equivalent at PCD can carry over their credentials to take remaining courses to get Level 6 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 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

Learning outcomes

This level 6 cybersecurity pathway will enable students to describe the basic 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.
- Understand basic networking concepts.
- Leverage and apply proactive threat intelligence to security support
- Manage vulnerability in organizational 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.
- Assess organizational security and response to incident procedures, such as basic threat detection, risk mitigation techniques, security controls, and basic digital forensics.
- Manage organizational risk and comply 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.
- Systems Analyst.
- Tier I and/or Tier II Support Specialist.
- Security Administrator.
- Helpdesk Manager / Analyst.
- Security Engineer/Analyst.
- DevOps/Software Developer.
- Security Analyst.
- Tier I - II SOC Analyst.
- Security Monitoring Engineer.
- Threat Intelligence Analyst.
- Security Engineer.
- Application Security Analyst.
- Incident Response Handler.
- Compliance Analyst.
- Threat Hunter

Credentials

Upon completion of A+, Security+ and CySA+ 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 Security Analytics Professional and will obtain a certificate/diploma of course completion from PCD with an Irish NFQ 6 equivalent credential. Besides they will also obtain the following stackable certification from CompTIA: CompTIA Security Analytics Professional.

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 PenTest+, Network+ and CASP+, enabling students to become a relevant professional and expert. Besides, students will have an opportunity to carry over credentials to complete NFQ Level 7 (Advanced Diploma/Graduation degree) at PCD.

Course duration

Standard: 12 months (Flexible: weekdays/weekends; mornings/afternoons/evenings)
Intensive: 1-2 weeks in each 3-month period to complete by 12 months.

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