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 Secure Infrastructure Specialist (CSIS)

(NFQ Level 5: Diploma in Secure Infrastructure)

(A+, Security+)

Course Overview

In an ever-expanding world, every sector is adapting to faster information exchange and more powerful security measures. Troubleshooting and the maintenance of computer systems, servers, and networks are also key supporting requirements for all information technology (IT) work. The CompTIA A+ course is designed to provide a basic understanding of hardware, networking, and computer systems while gaining the relevant additional skills. 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.

Completing both A+ and Security+ courses will provide the knowledge and relevant applications required for managing the flow and the optimization of day-to-day workplace activities based on different requirements. The added advantage is to take ***Network+*** to become a CompTIA Secure Infrastructure Specialist (CSIS). This will also enable a student to receive CompTIA certification independently and attain a diploma at NFQ level 5 equivalent to obtain a Cybersecurity Specialist certification from PCD. The learning materials provided by this course will allow a student to study for and pass all of CompTIA A+ and Security+ exams, leading to their designation as a Secure Infrastructure and Cybersecurity Specialist.

Entry level

The course is designed for students, professionals, and avid learners from any demographic having 0 to 2 years of experience in the field of IT.

Course format

The two courses contained in this path are:

- CompTIA A+ 220-1001 (Core 1) and 220-1002 (Core 2)
- CompTIA Security+ SY0-601
- CompTIA Network+ N10-008 (*Extra course for attaining CSIS*)

This course is designed not only for beginners who are seeking foundational knowledge to reach intermediate level (NFQ Level 5 equivalent) but also for intermediate learners who are intending to progress to advanced certification courses such as CSIS, CompTIA Network Security Professional (CNSP) and CompTIA Secure Cloud Professional (CSCP) from CompTIA.

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 for the students' final certification.

Modules

CompTIA A+	CompTIA Security+
Module 1: CompTIA A+ Hardware	Module 1: CompTIA Security+ Threats, Attacks, and Vulnerabilities
Module 2: CompTIA A+ Networking	Module 2: CompTIA Security+ Architecture and Design
Module 3: CompTIA A+ Mobile Devices	Module 3: CompTIA Security+ Implementation
Module 4: CompTIA A+ Hardware and Network Troubleshooting	Module 4: CompTIA Security+ Operations and Incident Response
Module 5: CompTIA A+ Windows Operating Systems	Module 5: CompTIA Security+ Governance, Risk, and Compliance
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	

Learning outcomes

This cybersecurity pathway will enable students to know and get hands-on training on the fundamentals of computing, networking, and cybersecurity and their applications. 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.
- 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/Cloud Engineer
- Security Engineer/Analyst
- DevOps/Software Developer
- IT Auditors.
- IT Project Manager.
- Tier III Specialist.

Credentials

After completion of A+ and Security+ exams, CompTIA will issue digital certification badge(s) from Credly and grant the respective stackable certification(s) automatically via certmetrics. Students will obtain a course completion certificate from PCD with an Irish NFQ Level 5 equivalent credentials, which can be carried over to take the remaining courses to obtain a Level 6 equivalent qualification, and/or a global recognized certification to become a CSIS by taking the Network+. The CompTIA credential will not only make you workplace ready but also facilitate further progress by taking other courses such as CompTIA CySA+ and CASP+ to become a relevant professional and expert.

Course duration

Standard: 6-9 months (Flexible: weekdays/weekends; mornings/afternoons/evenings)
Intensive: 1-2 weeks in each 3-month period to complete by 6 or 9 months.

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