



■ Technical ● Process

Training  
Support

Track

Foundation

Intermediate

Advanced

**RED**

**COURSES FOR THE ATTACKERS** External or internal security experts who simulate real-world cyber threats to test an organisation's defences, vulnerabilities, and incident response capabilities.

**BLUE**

**COURSES FOR YOUR ORGANISATION'S DEFENDERS** in-house security professionals responsible for maintaining and monitoring the security infrastructure.

**CompTIA Security +** ■

A practical course covering network security, compliance, operational security, cryptography, application data and host security, threats and vulnerabilities, and identity management. **Prerequisites:** CompTIA Network+ course, or CISCO ICND1, or equivalent.

**Cyber Matters** ●

Introduction to security and cyber related topics, covers fundamentals of security, areas it is applied and the importance policy integration. **Prerequisites:** None but a general appreciation of IT business functions.

**CompTIA PenTest+** ■

Verifies that learners have skills to plan and scope an assessment, understand legal / compliance requirements, perform vulnerability scanning / penetration testing, analyse data, and effectively report and communicate results. **Prerequisites:** Network+, Security+ or equivalent knowledge. 3 years hands-on information security experience or equivalent.

**CompTIA CySA+** ■

Focusses on frameworks and technologies used to and protect IT systems. CySA+ is an IT workforce certification that applies behavioural analytics to networks and devices to prevent, detect and combat cybersecurity threats. **Prerequisites:** CompTIA S+ course or equivalent.

**Certified Ethical Hacker** ■

Industry leading qualification that equips individuals for a career in penetration testing or red team deployment. Covers required theory and hands on experience through in-depth labs and exercises. **Prerequisites:** Knowledge of Networking and Security. 2 years' IT work experience, Linux, or Unix familiarity.

**RESILIA® Combined (Foundation & Practitioner)** ●

Incorporates best-practice security into existing management systems to improve immunity and increase robustness, to help prevent, detect, and recover from attacks. **Prerequisites:** None, knowledge of ITIL is advantageous.

**Certified Information Systems Security Professional (CISSP)** ●

A globally recognised Information Security standard. CISSP reviews the entire information security landscape and technologies, addressing the eight knowledge domains of the common body of knowledge (CBK). **Prerequisites:** Two domains in the CBK, for 5 years or more (4 years with relevant industry or degree level certification). Associate status can be achieved without full experience.

**CompTIA Advanced Security Practitioner (CASP+)** ■

Advanced hands-on, performance-based certification for practitioners. Certified professionals figure out how to implement solutions within cybersecurity policies and frameworks. **Prerequisites:** 10 years' IT administration, 5 years hands-on tech experience, CompTIA S+ / CYSA+.

**Certified Information Security Manager (CISM)** ●

Prepares delegates for the CISM exam and covers all associated job practices. Covers key syllabus areas and concepts / process that someone performing this job must understand. **Prerequisites:** Understanding core concepts of Information Security. Cyber Matters, CompTIA Security+, RESILIA or equivalent.

Coaching & Consultancy

