# CompTIA Certification Coverage of ECSF Roles

This resource provides learners with a clear learning pathway by identifying the percentage of knowledge and skills alignment between CompTIA certifications and the roles defined in ENISA's European Cybersecurity Skills Framework (ECSF).

By presenting this alignment, learners can design their own customised learning journey while ensuring they meet the requirements outlined in the ECSF.

| ECSF Profile Title | Recommended Certification | Other Relevant Certifications |
|---|---|---|
| Chief Information Security Officer | CompTIA SecurityX CERTIFICATION Xpert Series | CompTIA Security+ CERTIFICATION Plus Series |
| Cyber Incident Responder | CompTIA CySA+ CERTIFICATION Plus Series | CompTIA Security+ CERTIFICATION Plus Series<br>CompTIA SecurityX CERTIFICATION Xpert Series |
| Cyber Legal, Policy & Compliance Officer | CompTIA SecurityX CERTIFICATION Xpert Series | CompTIA Security+ CERTIFICATION Plus Series |
| Cyber Threat Intelligence Specialist | CompTIA CySA+ CERTIFICATION Plus Series<br>CompTIA SecurityX CERTIFICATION Xpert Series | CompTIA Security+ CERTIFICATION Plus Series |
| Cybersecurity Architect | CompTIA SecurityX CERTIFICATION Xpert Series | CompTIA Cloud+ CERTIFICATION Plus Series<br>CompTIA Security+ CERTIFICATION Plus Series |
| Cybersecurity Auditor | CompTIA Security+ CERTIFICATION Plus Series | CompTIA SecurityX CERTIFICATION Xpert Series<br>CompTIA CySA+ CERTIFICATION Plus Series |
| Cybersecurity Educator | CompTIA Security+ CERTIFICATION Plus Series | CompTIA SecurityX CERTIFICATION Xpert Series |

| ECSF Profile Title | Recommended Certification | Other Relevant Certifications |
|---|---|---|
| Cybersecurity Implementer | CompTIA Security+ CERTIFICATION Plus Series | CompTIA SecurityX CERTIFICATION Xpert Series<br>CompTIA Cloud+ CERTIFICATION Plus Series |
| Cybersecurity Researcher | CompTIA Security+ CERTIFICATION Plus Series | CompTIA SecurityX CERTIFICATION Xpert Series |
| Cybersecurity Risk Manager | CompTIA SecurityX CERTIFICATION Xpert Series | CompTIA Security+ CERTIFICATION Plus Series |
| Digital Forensics Investigator | CompTIA Security+ CERTIFICATION Plus Series | CompTIA CySA+ CERTIFICATION Plus Series<br>CompTIA SecurityX CERTIFICATION Xpert Series |
| Penetration Tester | CompTIA PenTest+ CERTIFICATION Plus Series | CompTIA Security+ CERTIFICATION Plus Series<br>CompTIA Linux+ CERTIFICATION Plus Series |

CompTIA

| CompTIA Security+<br>CERTIFICATION<br>Plus Series | CompTIA Cloud+<br>CERTIFICATION<br>Plus Series | CompTIA Linux+<br>CERTIFICATION<br>Plus Series | CompTIA CySA+<br>CERTIFICATION<br>Plus Series | CompTIA PenTest+<br>CERTIFICATION<br>Plus Series | CompTIA SecurityX<br>CERTIFICATION<br>Xpert Series |
|---|---|---|---|---|---|
| **SECURITY GENERALIST** | **CLOUD SYSTEMS ADMINISTRATION** | **LINUX ENGINEERING** | **CYBER DEFENCE, INCIDENT RESPONSE** | **PENETRATION TESTING** | **SECURITY ARCHITECT** |
| The CompTIA Security+ certification exam will verify the successful candidate has the knowledge and skills required to assess the security posture of an enterprise environment and recommend and implement appropriate security solutions; monitor and secure hybrid environments, including cloud, mobile, and IoT; operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance; identify, analyse, and respond to security events and incidents. | CompTIA Cloud+ validates your skills in cloud infrastructure, making it the industry standard for professionals working in multi-cloud environments. With this certification, you'll cover critical areas such as cloud architecture, deployment, operations, security, DevOps fundamentals, and troubleshooting. CompTIA Cloud+ equips you with the hands-on skills you need to excel in cloud operations and advance your career in the growing field of cloud computing. | CompTIA Linux+ covers an evolving job role that focuses more on how Linux powers the cloud. The exam includes cutting edge technologies that help automate and orchestrate business processes, including infrastructure as code and containers. | The CompTIA Cybersecurity Analyst (CySA+) certification verifies that successful candidates have the knowledge and skills required to detect and analyse indicators of malicious activity, understand threat intelligence and threat management, respond to attacks and vulnerabilities, perform incident response, and report and communicate related activity. | The CompTIA PenTest+ will certify the successful candidate has the knowledge and skills required to plan and scope a penetration testing engagement within compliance requirements, conduct enumeration and reconnaissance activities, analyse vulnerabilities, launch attacks, exfiltrate data and produce a written report with remediation techniques. | SecurityX (formerly CASP+) covers the technical knowledge and skills required to architect, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterprise while considering the impact of governance, risk, and compliance requirements. |
| **Required experience** | **Required experience** | **Required experience** | **Required experience** | **Required experience** | **Required experience** |
| 1-2 years in IT related field, with strong networking skills or Network+ equivalent. | 2-3 years of system administration or equivalent experience | 12 months in IT related field, with experience working with Linux. A+ and Network+ recommended. | 3-4 years experience in IT, 1 year experience in hands-on security environment. Security+ or equivalent knowledge recommended. | 3-4 years experience in IT, 1 year experience in hands-on security environment. Security+ or equivalent knowledge recommended. | 5+ years of hands-on experience in a security environment. Security+, CySA+ and PenTest+ recommended. |
| **Jobs that typically use Security+** | **Jobs that typically use Cloud+** | **Jobs that typically use Linux+** | **Jobs that typically use CySA+** | **Jobs that typically use PenTest+** | **Jobs that typically use SecurityX** |
| • Security Specialist<br>• Security Administrator<br>• Security Analyst<br>• Security Engineer | • Senior Systems Administrator<br>• Systems Engineer<br>• Cloud Specialist<br>• Network Engineer<br>• Cloud Architect<br>• DevOps<br>• Security Administrator<br>• Systems Architect | • Linux Administrator<br>• Linux Engineer<br>• Cybersecurity Engineer<br>• Systems Administrator | • Security Analyst<br>• Threat Intelligence Analyst<br>• Security Engineer<br>• Compliance Analyst | • Penetration Tester<br>• Security Consultant<br>• Information Security Engineer<br>• Cloud Penetration Tester | • Security Architect<br>• SOC Manager<br>• Cyber Risk Analyst<br>• Senior Security Engineer<br>• Director of Security<br>• Chief Information Officer<br>• Chief Information Security Officer<br>• IT Architect<br>• IT Risk Manager |
| **Domains covered** | **Domains covered** | **Domains covered** | **Domains covered** | **Domains covered** | **Domains covered** |
| 1. General Security Concepts<br>2. Threats, Vulnerabilities, and Mitigations<br>3. Security Architecture<br>4. Security Operations<br>5. Security Program Management and Oversight | 1. Cloud Architecture<br>2. Cloud Deployment<br>3. Cloud Operations<br>4. Cloud Security<br>5. DevOps Fundamentals<br>6. Troubleshooting | 1. System Management<br>2. System Security<br>3. Scripting, Containers, and Automation<br>4. Troubleshooting | 1. Security Operations<br>2. Vulnerability Management<br>3. Incident Response and Management<br>4. Reporting and Communication | 1. Engagement Management<br>2. Reconnaissance and Enumeration<br>3. Vulnerability Discovery and Analysis<br>4. Attacks and Exploits<br>5. Post-exploitation and Lateral Movement | 1. Governance, Risk, and Compliance<br>2. Security Architecture<br>3. Security Engineering<br>4. Security Operations |