techskills

TEACHERS AND LECTURERS

Cyber Security careers: a guide for teachers and lecturers

Digital Resilience & Defence

Figures checked from 11 July 2026. Built from the TechSkills Career Matrix.

About this guide

This guide is for teachers and lecturers who advise students on careers in Cyber Security.

It is built from the TechSkills Career Matrix and Career Planner. Every pay, hiring and funding figure shows its source and the date it was checked. Where our data has a gap, the guide says so.

Areas of work covered	8
Apprenticeship standards listed	4
Produced by	TechSkills, techskills.org

Cyber Security at a glance

No.	Area of work	What it covers	Example roles	Pay range
01	Security Operations	Monitoring systems and responding to active threats in real-time.	SOC Analyst, Incident Responder, Threat Intel, Security Administrator	£34,000 to £75,000+
02	Offensive Security	Thinking like a hacker to find and fix vulnerabilities before the bad guys do.	Penetration Tester, Red Teamer, Bug Bounty Hunter, Vulnerability Analyst	£49,000 to £130,000+
03	Engineering & Architecture	Building systems that are 'Secure by Design' from the ground up.	Security Engineer, Security Architect, DevSecOps Engineer, Cryptography Lead	£50,000 to £150,000+
04	Governance & Risk	Managing the human, legal, and business side of digital trust.	GRC Analyst, Privacy Officer, Cyber Auditor, Risk Manager	£35,000 to £95,000+
05	Strategy & Leadership	Defining the security vision and protecting the organisation at executive level.	CISO, Head of Security, Cyber Strategist, Security Director	£78,000 to £200,000+
06	Emerging Cyber	Defending the next generation of technology from futuristic threats.	AI Security Lead, Quantum Security, IoT Architect, Zero Trust Specialist	£40,000 to £100,000+
07	Digital Forensics & Incident Response	Reconstructing digital evidence after a breach, tracing how attackers got in, what they touched, and building the case for legal or insurance action.	Digital Forensics Analyst, Incident Response Lead, Malware Analyst, eDiscovery Specialist	£26,000 to £71,000+
08	Cloud & Application Security	Embedding security into the software development lifecycle and cloud environments, rather than bolting it on afterwards.	Application Security Engineer, Cloud Security Engineer, DevSecOps Specialist, Product Security Lead	£45,000 to £105,000+

Pay ranges come from job advert data. The source for each range is shown with the area of work in the next section.

The areas of work, one by one

01 Security Operations

What it is	Monitoring systems and responding to active threats in real-time.
Example roles	SOC Analyst, Incident Responder, Threat Intel, Security Administrator
Skills used	Threat Hunting; SIEM Tools; Log Analysis; Incident Response
Who it suits	Analytical thinkers who thrive under pressure and enjoy investigative work.
Example of the work	Leading the response to a coordinated DDoS attack on a major platform.
What shows someone can do it	Ability to detect and triage a live security incident before it escalates into a full breach.
Sectors that hire	Financial Services, Government & Public Sector, Telecommunications, Retail & E-commerce, Critical National Infrastructure
Pay	£34,000 to £75,000+. Source: range across UK SOC Analyst to Threat Intel Analyst postings, IT Jobs Watch.

Apprenticeship route: Cyber Security Technician, Apprenticeship Route

What it is	Work first line cyber security support inside a real Security Operations Centre or Network Operations Centre under supervision, training on the job rather than starting with three years of full time study.
Example roles	Cyber Security Technician Apprentice, SOC Analyst Apprentice, Cyber Defend and Respond Apprentice
What suits this route	Comfortable training on the job with structured mentoring rather than lecture based study; Wants a paid route into cyber security, entering with GCSEs or A levels rather than a completed degree
Pay	£14,000 to £37,500+. Source: apprentice wage to qualified Junior Security Analyst pay, IT Jobs Watch/Glassdoor UK.

Standard	Reference	Level	Typical length	Checked
Cyber Security Technician	ST0865	Level 3	18 months	29 July 2026
Cyber Security Technologist (2021)	ST1021	Level 4	24 months	29 July 2026
Cyber Security Technical Professional (integrated degree)	ST0409	Level 6	48 months	29 July 2026

02 Offensive Security

What it is	Thinking like a hacker to find and fix vulnerabilities before the bad guys do.

Example roles	Penetration Tester, Red Teamer, Bug Bounty Hunter, Vulnerability Analyst
Skills used	Ethical Hacking; Exploit Dev; Python; Social Engineering
Who it suits	Creative problem solvers who enjoy the 'puzzle' of breaking systems.
Example of the work	Conducting a 'Red Team' exercise to simulate a breach of a bank's system.
What shows someone can do it	Ability to find and responsibly report an exploitable vulnerability before a real attacker does.
Sectors that hire	Financial Services, Government & Public Sector, Aerospace & Defence, Technology & Software, Professional & Consulting Services
Pay	£49,000 to £130,000+. Source: Penetration Tester to Red Team postings, IT Jobs Watch; Bug Bounty pay too variable to include.

03 Engineering & Architecture

What it is	Building systems that are 'Secure by Design' from the ground up.
Example roles	Security Engineer, Security Architect, DevSecOps Engineer, Cryptography Lead
Skills used	Secure Coding; Cloud Security; IAM; Encryption
Who it suits	System builders who enjoy the bridge between engineering and security.
Example of the work	Designing the secure identity system for a new government portal.
What shows someone can do it	Ability to design systems that are secure by default, rather than patched after the fact.
Sectors that hire	Financial Services, Government & Public Sector, Technology & Software, Healthcare & Life Sciences, Telecommunications
Pay	£50,000 to £150,000+. Source: Security Engineer to Enterprise Security Architect postings, IT Jobs Watch; Cryptography Lead via Cryptography Engineer proxy, Glassdoor UK.

Apprenticeship route: Operational Technology (OT) Security

What it is	Secures the operational technology behind critical national infrastructure: the industrial control and SCADA systems that run water treatment, power generation and manufacturing. Involves visiting live sites to assess and harden real plant equipment alongside the engineers who run it, not just monitoring a screen from a desk.
Example roles	OT Security Engineer, ICS Security Analyst, Industrial Cyber Security Consultant

What suits this route	Understands how the physical process works, not just the network protecting it; Comfortable visiting industrial sites and working around live plant equipment; Can translate between the engineers who run the plant and the analysts who watch the network; A background in a trade or industrial engineering is a genuine advantage: it is far easier to teach that person the security software than to teach a computer scientist how a water treatment plant actually runs
Pay	£36,000 to £100,000+. Source: range across real UK OT security job postings, analyst to consultant level.

Standard	Reference	Level	Typical length	Checked
Cyber Security Technician	ST0865	Level 3	18 months	30 July 2026
Automation and Controls Engineering Technician	ST0662	Level 4	48 months	30 July 2026

04 Governance & Risk

What it is	Managing the human, legal, and business side of digital trust.
Example roles	GRC Analyst, Privacy Officer, Cyber Auditor, Risk Manager
Skills used	Risk Assessment; Compliance; Auditing; Privacy Law
Who it suits	Detail-oriented thinkers interested in law, policy, and business strategy.
Example of the work	Auditing a company's global data handling to ensure GDPR compliance.
What shows someone can do it	Ability to translate legal and regulatory requirements into practical, auditable controls.
Sectors that hire	Financial Services, Insurance, Legal Services, Healthcare & Life Sciences, Government & Public Sector
Pay	£35,000 to £95,000+. Source: GRC Analyst to IT Auditor postings, IT Jobs Watch/Glassdoor; cross-checked against ONS Risk managers median £54,619.

05 Strategy & Leadership

What it is	Defining the security vision and protecting the organisation at executive level.
Example roles	CISO, Head of Security, Cyber Strategist, Security Director
Skills used	Strategic Planning; Board Comms; Budget Mgmt; Crisis Leadership
Who it suits	Experienced leaders who can translate technical risk into business value.
Example of the work	Developing a 5-year cyber resilience strategy for a multi-national.
What shows someone can do it	Ability to set and defend a multi-year security strategy and budget at board level.
Sectors that hire	Financial Services, Government & Public Sector, Critical National Infrastructure, Professional & Consulting Services, Telecommunications

Pay	£78,000 to £200,000+. Source: Head of Security to CISO postings, IT Jobs Watch/Glassdoor UK; top CISO pay exceeds £270,000.

06 Emerging Cyber

What it is	Defending the next generation of technology from futuristic threats.
Example roles	AI Security Lead, Quantum Security, IoT Architect, Zero Trust Specialist
Skills used	AI Security; Quantum Crypto; IoT Defence; Zero Trust
Who it suits	Pioneers who want to build the defences of the future.
Example of the work	Securing a fleet of autonomous drones from signal hijacking.
What shows someone can do it	Ability to anticipate and defend against attack surfaces that don't exist yet, from AI systems to quantum-era cryptography.
Sectors that hire	Aerospace & Defence, Technology & Software, Automotive, Critical National Infrastructure, Telecommunications
Pay	£40,000 to £100,000+. Source: IoT Architect, Zero Trust and AI Engineer postings, IT Jobs Watch; Quantum Security proxied via Quantum Computing Engineer, Glassdoor UK.

07 Digital Forensics & Incident Response

What it is	Reconstructing digital evidence after a breach, tracing how attackers got in, what they touched, and building the case for legal or insurance action.
Example roles	Digital Forensics Analyst, Incident Response Lead, Malware Analyst, eDiscovery Specialist
Skills used	Forensic Imaging; Malware Analysis; Chain of Custody; Log Correlation
Who it suits	Patient investigators who enjoy piecing together a story from fragments of evidence.
Example of the work	Turns a breach into a documented, actionable, and legally sound investigation.
What shows someone can do it	Ability to reconstruct an attack timeline from digital evidence that holds up in court or before a regulator.
Sectors that hire	Financial Services, Government & Public Sector, Legal Services, Insurance, Critical National Infrastructure
Pay	£26,000 to £71,000+. Source: Digital Forensics Analyst to Incident Response Lead postings, IT Jobs Watch/Glassdoor; eDiscovery Specialist narrower niche, £25,000–£39,000.

08 Cloud & Application Security

What it is	Embedding security into the software development lifecycle and cloud environments, rather than bolting it on afterwards.
Example roles	Application Security Engineer, Cloud Security Engineer, DevSecOps Specialist, Product Security Lead
Skills used	Secure SDLC; Cloud Security Posture; Container Security; SAST/DAST Tooling
Who it suits	Engineers who want security built in from the first line of code, not added last.
Example of the work	Prevents vulnerabilities from ever reaching production in cloud-native environments.
What shows someone can do it	Ability to catch vulnerabilities in code and cloud configuration before they reach production.
Sectors that hire	Technology & Software, Financial Services, Retail & E-commerce, Telecommunications, Government & Public Sector
Pay	£45,000 to £105,000+. Source: Application Security to DevSecOps Engineer postings, IT Jobs Watch; Product Security Lead via Glassdoor UK proxy, £43,000–£93,000.

Routes into the field

Route	What it is	Cost and pay
Apprenticeships	Earn while they train through structured learning that combines workplace experience with recognised development.	their employer (or the government, via the apprenticeship levy and co-investment) pays for all their training and assessment costs directly to the provider, they are never billed for tuition, and they don't take out a loan for it. Apprentices are paid at least the apprentice minimum wage of £8.00 an hour.
Degrees	Build strong technical foundations through longer-form study with opportunities to specialise and progress academically.	Covers their tuition fees in full, paid directly to their university or college, not means-tested, so every eligible student can borrow the same amount regardless of household income. Repayments under Plan 5 are 9% of income above £25,000 a year, and the loan is written off after 40 years.
Bootcamps & Intensive Training	We don't currently have any Tech Industry Gold accredited bootcamp providers - accelerate their move into tech via the government's own Skills Bootcamps programme instead: free, flexible courses up to 16 weeks, built around employability.	Free to the learner. Up to 16 weeks. Available across England.
Flexible Learning (Apprenticeship Units)	Build relevant tech skills through shorter, flexible learning without committing to a full programme from the start.	Shorter, flexible training. Focused, in-demand skills. Aligned to employer needs. Can build toward larger qualifications.

Apprenticeships: Explore Apprenticeships

Degrees: Find Degrees

Bootcamps & Intensive Training: Find a Skills Bootcamp (gov.uk)

Flexible Learning (Apprenticeship Units): Explore Flexible Learning

Who pays for an apprenticeship	Employers with an annual pay bill over £3 million pay into the apprenticeship levy, topped up by government, to fund training. Smaller employers get most of the cost covered through government co-investment, and from the 2026/27 funding year, training for under-25s at these smaller, non-levy-paying employers is fully funded.
Apprentice minimum wage	£8.00 an hour: the National Minimum Wage apprentice rate, which applies if they're under 19, or 19+ and in the first year of their apprenticeship (from 1 April 2026). Once they're 19+ and past their first year, they move to the normal age-based National Minimum Wage (up to £12.71/hour for ages 21+ from April 2026), many employers pay well above the legal minimum.

Funding sources: gov.uk: Apprenticeship funding rules and assessment plan guidance, 2026 to 2027 (checked 20 July 2026); gov.uk: Student finance for undergraduates, gov.uk: Repaying your student loan; gov.uk: How interest is calculated, Plan 5 (checked 20 July 2026). Rates change each year, so confirm current figures on gov.uk before quoting them.

Apprenticeship standards in this career family

Reference	Standard	Level	Typical length
ST0865	Cyber Security Technician	Level 3	18 months
ST0662	Automation and Controls Engineering Technician	Level 4	48 months
ST1021	Cyber Security Technologist (2021)	Level 4	24 months
ST0409	Cyber Security Technical Professional (integrated degree)	Level 6	48 months

ST0865 Cyber Security Technician First line cyber security support, monitoring threats and working within a Security Operations Centre or Network Operations Centre under supervision.

ST0662 Automation and Controls Engineering Technician An equally real route in from the engineering side: understanding automation and control systems first, then moving into securing them.

ST1021 Cyber Security Technologist (2021) Has a Cyber Defend and Respond pathway that maps directly onto SOC monitoring and incident response work, with typical job titles including Secure Operations Centre (SOC) Analyst.

ST0409 Cyber Security Technical Professional (integrated degree) The integrated degree apprenticeship BT's own cyber security apprentices complete, alongside GCHQ and NCSC's CyberFirst Degree Apprenticeship route.

Pay and hiring

Level	Median pay	25th to 75th percentile	Salaries in sample	Source	Period
Junior	£37,500	£33,750 to £41,250	2	IT Jobs Watch: Junior Security Analyst (UK)	6 months to 11 Jul 2026
Mid-level	£55,000	£40,000 to £65,000	343	IT Jobs Watch: Security Analyst (UK)	6 months to 11 Jul 2026
Senior	£60,000	£40,000 to £79,250	6,777	IT Jobs Watch: Cyber Security (UK, all levels)	6 months to 11 Jul 2026

A small sample makes a figure indicative only. The hiring note below says where that applies.

Hiring	83% of employers of cyber security professionals expected to recruit during 2026, against a persistent UK-wide skills shortfall (around 3,800 professionals a year) and 49% of businesses reporting they lack basic cyber skills in-house. The junior-specific figures above are based on an extremely small sample (2 salaries), treat that band as indicative only, not precise.
Remote working	38.2% of UK cyber/IT security job postings were listed as remote or flexible (Jan-Apr 2026), though only around 23% of professionals currently work fully remote versus roughly 31-40% who would prefer to, a real gap between employer offers and candidate preference.
Fastest growing skill	Cloud security (Azure) now appears in over two-thirds of UK Security Analyst postings, alongside growing employer interest in AI/LLM security and AI governance as genuinely emerging specialisms.

Skills and certifications

Skills employers ask for

Skill	Importance	Demand	Time to learn	Route
Security Fundamentals & Threat Concepts	Critical	Very High, in 90% of postings	3-4 weeks	All routes
Networking & Linux Fundamentals	Critical	Very High	4-6 weeks	All routes
SIEM (Security Information and Event Management) & Log Analysis	High	Medium, in 12% of postings	3-4 weeks	All routes
Cloud Security (Azure)	High	Very High, in 68% of postings	3-4 weeks	All routes
Information Security & Governance, Risk and Compliance (GRC)	Medium	Medium, in 11% of postings	2-3 weeks	All routes
Assess and Harden Industrial Control System (ICS) / SCADA (Supervisory Control and Data Acquisition) Security	Critical	High	Built up on the job after an initial cyber security or engineering apprenticeship, deepening over 1-2+ years	Apprenticeship

Security Fundamentals & Threat Concepts: Introduction to Cybersecurity Cisco Skills for All

Security Fundamentals & Threat Concepts: Professor Messer's Security+ training videos Professor Messer

Networking & Linux Fundamentals: Networking Basics Cisco Networking Academy

Networking & Linux Fundamentals: Introduction to Linux Cisco Skills for All

SIEM (Security Information and Event Management) & Log Analysis: Security Onion documentation Security Onion

SIEM (Security Information and Event Management) & Log Analysis: Wazuh documentation Wazuh

Cloud Security (Azure): Microsoft Certified: Security, Compliance, and Identity Fundamentals Microsoft Learn

Information Security & Governance, Risk and Compliance (GRC): ISO/IEC 27001 overview ISO

Assess and Harden Industrial Control System (ICS) / SCADA (Supervisory Control and Data Acquisition) Security: Secure Connectivity Principles for Operational Technology NCSC / CISA / FBI

Security Fundamentals & Threat Concepts: Share of UK Security Analyst job postings mentioning cybersecurity as a core competency. Networking & Linux Fundamentals: Universally cited as foundational in cyber security career guidance; not separately broken out as a keyword percentage since it's assumed baseline rather than a differentiator. SIEM (Security Information and Event Management) & Log Analysis: Share of UK Security Analyst job postings explicitly mentioning SIEM as a keyword (likely an undercount, since many postings describe the task without naming the tool). Cloud Security (Azure): Share of UK Security Analyst job postings mentioning Azure. Information Security & Governance, Risk and Compliance (GRC): Share of UK Security Analyst job postings mentioning Information Security/ISO 27001 explicitly. Assess and Harden Industrial Control System (ICS) / SCADA (Supervisory Control and Data Acquisition) Security: No dedicated OT/ICS security apprenticeship standard exists on the England register yet, this is entered via the general Cyber Security Technician standard (ST0865) or from an Automation and Controls Engineering Technician (ST0662) background, then built up on the job, per this domain's own framing in capability-matrices.ts. IT Jobs Watch's 'Operational Technology' keyword page shows a £62,500 median (148 salaries), treat as indicative since no dedicated OT/ICS job-title page exists yet. NCSC (the UK's National Cyber Security Centre) has published joint guidance with CISA (its US equivalent, the Cybersecurity and Infrastructure Security Agency) and the FBI on securing OT connectivity, reflecting sustained UK national-security priority in this area.

Certifications

Certification	Provider	Cost	Time	Level	Recognised	Best stage
CompTIA Security+	CompTIA	Approx. $425-439 / £330-350 for a single exam voucher (correct at time of writing, CompTIA raised prices in June 2026, check comptia.org for current pricing)	6-10 weeks part-time	Beginner	High	Before you apply
ISC2 Certified in Cybersecurity (CC)	ISC2	$199 exam fee for new candidates (correct at time of writing), ISC2's free '1 Million Certified in Cybersecurity' enrolment programme closed to new sign-ups after hitting its target, so this is no longer free unless you already hold an unexpired voucher code from that programme	3-5 weeks part-time	Beginner	Medium	Before you apply
ISA/IEC 62443 Cybersecurity Fundamentals Specialist	ISA (International Society of Automation)	Approx. $2,000 for the certificate course and exam, around $1,600 for ISA members (correct at time of writing, check isa.org for current pricing)	1-2 weeks part-time	Intermediate	Niche	Before you apply
GIAC Global Industrial Cyber Security Professional (GICSP)	GIAC (Global Information Assurance Certification, the certifying body run by SANS)	$999 for a first attempt / $899 for a retake (exam fee, correct at time of writing, check giac.org/pricing for current pricing); renewal is $499 every 4 years. The optional SANS ICS410 prep course runs $8,000+, a genuinely significant cost most entry-level candidates won't take on straight away	Several months of study, longer if pairing with the optional SANS ICS410 course	Advanced	Niche	Early career (0-2 years)

Professional standard

UK Cyber Security Council publishes the Standard for Professional Competence and Commitment (SPCC).

Title	Code	What it recognises
Associate Cyber Security Professional	ACSP	Building knowledge, skills and experience in an early cyber security career.
Practitioner Cyber Security Professional	PraCSP	Applying cyber security expertise independently and effectively.
Principal Cyber Security Professional	PriCSP	Leading teams, projects and specialist practice.
Chartered Cyber Security Professional	ChCSP	Influencing organisations, standards and the wider profession.

Entry title	Associate Cyber Security Professional (ACSP), launched April 2026. The Council's entry-level professional registration, for people at the start of their cyber security careers who are either in an early-career cyber role or ready for their first one. Achieving it lets someone join the UK Cyber Security Professional Register and use the ACSP post-nominal.
Keeping a title	Staying on the UK Cyber Security Professional Register isn't a one-off achievement: applying for a title requires committing to the Council's code of ethics, and 75 hours of Continuing Professional Development over three years (25 hours a year) is required to keep a title current.
Used by employers	This is already a real employer requirement, not a theoretical framework: the NCSC's CHECK scheme (which approves penetration-testing providers for government and critical national infrastructure work) now requires, for every new applicant, at least one proposed CHECK Team Leader to hold a UK Cyber Security Council Professional Title in the Security Testing specialism at Principal level or above, confirmed directly on the NCSC's own CHECK scheme page.

UK Cyber Security Council, The Standard for Professional Competence and Commitment

UK Cyber Security Council, Standard for Professional Competence and Commitment (primary PDF, v4.2, October 2024)

UK Cyber Security Council, The Professional Titles

UK Cyber Security Council, Cyber Security Specialisms (incl. Security Testing)

NCSC, CHECK penetration testing: information for providers

For teachers and lecturers

Area of work	Who it suits	Example roles	Apprenticeship standards
Security Operations	Analytical thinkers who thrive under pressure and enjoy investigative work.	SOC Analyst, Incident Responder, Threat Intel, Security Administrator	ST0865 Level 3, ST1021 Level 4, ST0409 Level 6
Offensive Security	Creative problem solvers who enjoy the 'puzzle' of breaking systems.	Penetration Tester, Red Teamer, Bug Bounty Hunter, Vulnerability Analyst	None listed in the Matrix yet
Engineering & Architecture	System builders who enjoy the bridge between engineering and security.	Security Engineer, Security Architect, DevSecOps Engineer, Cryptography Lead	ST0865 Level 3, ST0662 Level 4
Governance & Risk	Detail-oriented thinkers interested in law, policy, and business strategy.	GRC Analyst, Privacy Officer, Cyber Auditor, Risk Manager	None listed in the Matrix yet
Strategy & Leadership	Experienced leaders who can translate technical risk into business value.	CISO, Head of Security, Cyber Strategist, Security Director	None listed in the Matrix yet
Emerging Cyber	Pioneers who want to build the defences of the future.	AI Security Lead, Quantum Security, IoT Architect, Zero Trust Specialist	None listed in the Matrix yet
Digital Forensics & Incident Response	Patient investigators who enjoy piecing together a story from fragments of evidence.	Digital Forensics Analyst, Incident Response Lead, Malware Analyst, eDiscovery Specialist	None listed in the Matrix yet
Cloud & Application Security	Engineers who want security built in from the first line of code, not added last.	Application Security Engineer, Cloud Security Engineer, DevSecOps Specialist, Product Security Lead	None listed in the Matrix yet

The Who it suits column comes from the Career Matrix. It is a starting point for a conversation, not an assessment.

Notes on your students

Activities for lessons and clubs

Activity	What students do	Level	Time	Skills shown
Home SOC (Security Operations Centre) Lab	A small virtualised Security Operations Centre environment (e.g. using VirtualBox/VMware with a Kali Linux attacker machine, a deliberately vulnerable target VM, Virtual Machine, a simulated computer running inside your real one, and a SIEM, or Security Information and Event Management tool, like Security Onion or Wazuh collecting activity logs from both), demonstrating end-to-end detection of a simulated attack.	Intermediate	15-20 hours	Networking & Linux Fundamentals, SIEM & Log Analysis, Security Fundamentals & Threat Concepts
SIEM (Security Information and Event Management) Dashboard	Building on the Home SOC Lab, configure custom dashboards and alert rules in your SIEM (Security Onion/Wazuh both support this) that surface a specific realistic threat pattern, e.g. repeated failed logins or unusual outbound traffic.	Intermediate	8-12 hours	SIEM & Log Analysis, Cloud Security (Azure)
Vulnerability Assessment	Run a real, free vulnerability scanner (OpenVAS or Nessus Essentials, both free for personal/small-scale use) against your own home lab environment, then write a professional-style report ranking findings by severity with realistic remediation recommendations.	Beginner	8-10 hours	Security Fundamentals & Threat Concepts, Information Security & Governance, Risk and Compliance (GRC)
Cyber Security Helpdesk Ticket Log	A log kept over several weeks of real cyber security helpdesk requests you processed at work, recording how each one protected the confidentiality, integrity and availability of the organisation's digital information (the CIA triad), with your mentor's sign-off on each entry as part of your portfolio of evidence for ST0865 Duty 3.	Beginner	4-6 weeks of off-the-job (OTJ) training time, a couple of hours logged per week	Security Fundamentals & Threat Concepts, Information Security & Governance, Risk and Compliance (GRC)
Security Monitoring and Escalation Shift Log	A shift log built up over several weeks of real information security incidents and events you monitored, identified and escalated at work, following your employer's procedures and referenced against ST0865 Duty 5 and Duty 18 (or Duty 18 and Duty 20 of the Cyber Defend & Responder option on ST1021), with each escalation decision reviewed and signed off by your mentor as part of your portfolio of evidence.	Intermediate	6-8 weeks of on-the-job monitoring, logged as it happens during your off-the-job (OTJ) training time	SIEM & Log Analysis, Security Fundamentals & Threat Concepts

Activity	What students do	Level	Time	Skills shown
ICS/SCADA Security Assessment Log	Under supervision, or using a training/simulation environment, assess a small industrial control system or SCADA (Supervisory Control and Data Acquisition) test rig against a recognised security framework such as IEC 62443 (the international standard for securing industrial control systems), recording the vulnerabilities identified, the hardening steps applied and the outcome, with your mentor's or trainer's sign-off on each entry.	Advanced	8-12 hours	Assess and Harden Industrial Control System (ICS/SCADA) Security
Industrial Site Security Walkdown Report	Carry out a physical and cyber security walkdown of a real or training industrial site or rig, documenting network segmentation, physical access controls and any insecure remote-access points found, then write up findings and recommended fixes for review by your mentor.	Intermediate	6-10 hours	Assess and Harden Industrial Control System (ICS/SCADA) Security

These are the portfolio projects used in the TechSkills Career Planner. Each is meant to produce work a learner can show an employer.

Where to find out more

National Careers Service Careers advice, job profiles, information and resources. (Department for Education. Checked 1 November 2026.)

Find an apprenticeship Register a profile, search vacancies and apply for an apprenticeship. Applicants must be 16 or over. (GOV.UK. Checked 1 November 2026.)

Skills Bootcamps For people updating their skills to progress in their current job or move into a different role. (JobHelp, GOV.UK. Checked 1 November 2026.)

Skills England: apprenticeship search Skills England's apprenticeship search. (Skills England. Checked 1 November 2026.)

NCSC: cyber skills The National Cyber Security Centre's cyber skills pages. (National Cyber Security Centre. Checked 1 November 2026.)

UK Cyber Security Council The Council's website. It publishes the Standard for Professional Competence and Commitment and the professional titles described in this guide. (UK Cyber Security Council. Checked 1 November 2026.)

General notes

Sources and checking

The figures in this guide were checked on dates from 11 July 2026 to 1 November 2026. Each source below shows its own date.

Skills England: ST0865 Cyber Security Technician Checked 29 July 2026

Skills England: ST0662 Automation and Controls Engineering Technician Checked 30 July 2026

Skills England: ST1021 Cyber Security Technologist (2021) Checked 29 July 2026

Skills England: ST0409 Cyber Security Technical Professional (integrated degree) Checked 29 July 2026

UK Cyber Security Council, The Standard for Professional Competence and Commitment

UK Cyber Security Council, Standard for Professional Competence and Commitment (primary PDF, v4.2, October 2024)

UK Cyber Security Council, The Professional Titles

UK Cyber Security Council, Cyber Security Specialisms (incl. Security Testing)

NCSC, CHECK penetration testing: information for providers

National Careers Service, Department for Education Checked 1 November 2026

Find an apprenticeship, GOV.UK Checked 1 November 2026

Skills Bootcamps, JobHelp, GOV.UK Checked 1 November 2026

Skills England: apprenticeship search, Skills England Checked 1 November 2026

NCSC: cyber skills, National Cyber Security Centre Checked 1 November 2026

UK Cyber Security Council, UK Cyber Security Council Checked 1 November 2026

- gov.uk: Apprenticeship funding rules and assessment plan guidance, 2026 to 2027 (checked 20 July 2026)
- gov.uk: National Minimum Wage and National Living Wage rates (checked 20 July 2026)
- gov.uk: Student finance for undergraduates (checked 20 July 2026)
- gov.uk: Repaying your student loan; gov.uk: How interest is calculated, Plan 5 (checked 20 July 2026)
- IT Jobs Watch: Cyber Security / Security Analyst / Junior Security Analyst (UK) (checked 11 July 2026)
- Robert Walters: Cybersecurity Trends Shaping Hiring in 2026 (UK Market Update) (checked 11 July 2026)
- GDPR Course: Cyber Security Skills Gap Statistics UK (checked 11 July 2026)
- IT & Cyber Security Job Market Report (UK), Learning People, Jan 2026 (checked 11 July 2026)
- IT Jobs Watch: Security Analyst skills (UK), 6 months to 11 Jul 2026 (checked 11 July 2026)
- Professor Messer Security+ curriculum (checked 11 July 2026)
- Cisco Networking Academy course structure (checked 11 July 2026)
- IfATE/Skills England: Cyber Security Technician (ST0865), Automation and Controls Engineering Technician (ST0662) (checked 31 July 2026)
- SANS Institute: State of ICS/OT Security 2025 (Jason D. Christopher, November 2025) (checked 31 July 2026)
- NCSC/CISA/FBI: Secure Connectivity Principles for Operational Technology (checked 31 July 2026)
- ISA: ISA/IEC 62443 Cybersecurity Fundamentals Specialist programme (checked 31 July 2026)
- GIAC: Global Industrial Cyber Security Professional (GICSP) certification (checked 31 July 2026)
- IT Jobs Watch: 'Operational Technology' (UK keyword postings), 6 months to 30 Jul 2026 (checked 31 July 2026)
- IT Jobs Watch: Security Analyst skills (UK), 6 months to 11 Jul 2026 (70.05% of postings) (checked 11 July 2026)
- Nucamp: Top In-Demand Cybersecurity Jobs for Beginners in the UK (checked 11 July 2026)
- ISC2 official CC certification page (checked 11 July 2026)

- ISC2: 'Easier Than Ever: Register for Your Free ISC2 Certified in Cybersecurity Exam' (2024, programme now closed to new enrolments) (checked 11 July 2026)
- ISA: ISA/IEC 62443 Cybersecurity Certificate Programme page (checked 31 July 2026)
- GIAC: GICSP certification page (checked 31 July 2026)
- GIAC: certification pricing page (checked 31 July 2026)