Free career resource · Choosing a path

Cyber security career paths explained

Cyber security isn't one job. The six paths most beginners ask about are SOC analyst, governance risk and compliance (GRC), penetration testing, cloud security, security engineering and incident response. SOC and GRC roles are the most common first jobs. Penetration testing, cloud security and incident response usually come after a few years in IT or another security role.

By the Cyberend team · Published and updated 22 November 2026

THE SHORT ANSWER

- **Most common first jobs:** SOC analyst (monitoring and investigating alerts) and junior GRC or information security analyst (policies, risk and audits).
- **Usually a second step:** penetration testing, cloud security, security engineering and incident response tend to need experience in IT, development or a security operations team first.
- **Not all technical:** auditing (22%), governance (20%) and risk management (19%) were among the skills most often requested in UK cyber adverts in 2025 DSIT 2026.
- **Honest expectation:** none of these paths is quick to enter. Most people spend months learning and building evidence before their first role, and certifications help but don't guarantee a job.

The six paths at a glance

The UK Cyber Security Council, the profession's recognised professional body, describes 15 specialisms UK Cyber Security Council. Real job titles rarely map neatly onto one of them, so we've grouped them into the six paths people most often ask about.

SOC analyst

IN ONE LINE
Watch for attacks and investigate alerts

SUITS PEOPLE WHO
Like puzzles, patterns and working in a team on shifts

FIRST JOB?
Often a first job

MIDDLE ADVERTISED PAY
£55,000

GRC

IN ONE LINE
Policies, risk assessments and audits

SUITS PEOPLE WHO
Are organised, write clearly and like rules and process

FIRST JOB?
Often a first job

MIDDLE ADVERTISED PAY
£50,000 (small sample)

Penetration testing

IN ONE LINE
Test systems for weaknesses, with permission

SUITS PEOPLE WHO
Are deeply technical, persistent and write good reports

FIRST JOB?
Rarely a first job

MIDDLE ADVERTISED PAY
£65,000

Cloud security

IN ONE LINE
Secure systems in AWS, Azure or Google Cloud

SUITS PEOPLE WHO
Already work with cloud, infrastructure or code

FIRST JOB?
Rarely a first job

MIDDLE ADVERTISED PAY
£75,000

Security engineering

IN ONE LINE
Build and run the security tools and controls

SUITS PEOPLE WHO
Enjoy building, automating and fixing systems

FIRST JOB?
Sometimes a first job

MIDDLE ADVERTISED PAY
£60,000

Incident response

IN ONE LINE
Contain and investigate breaches when they happen

SUITS PEOPLE WHO
Stay calm under pressure and like investigation

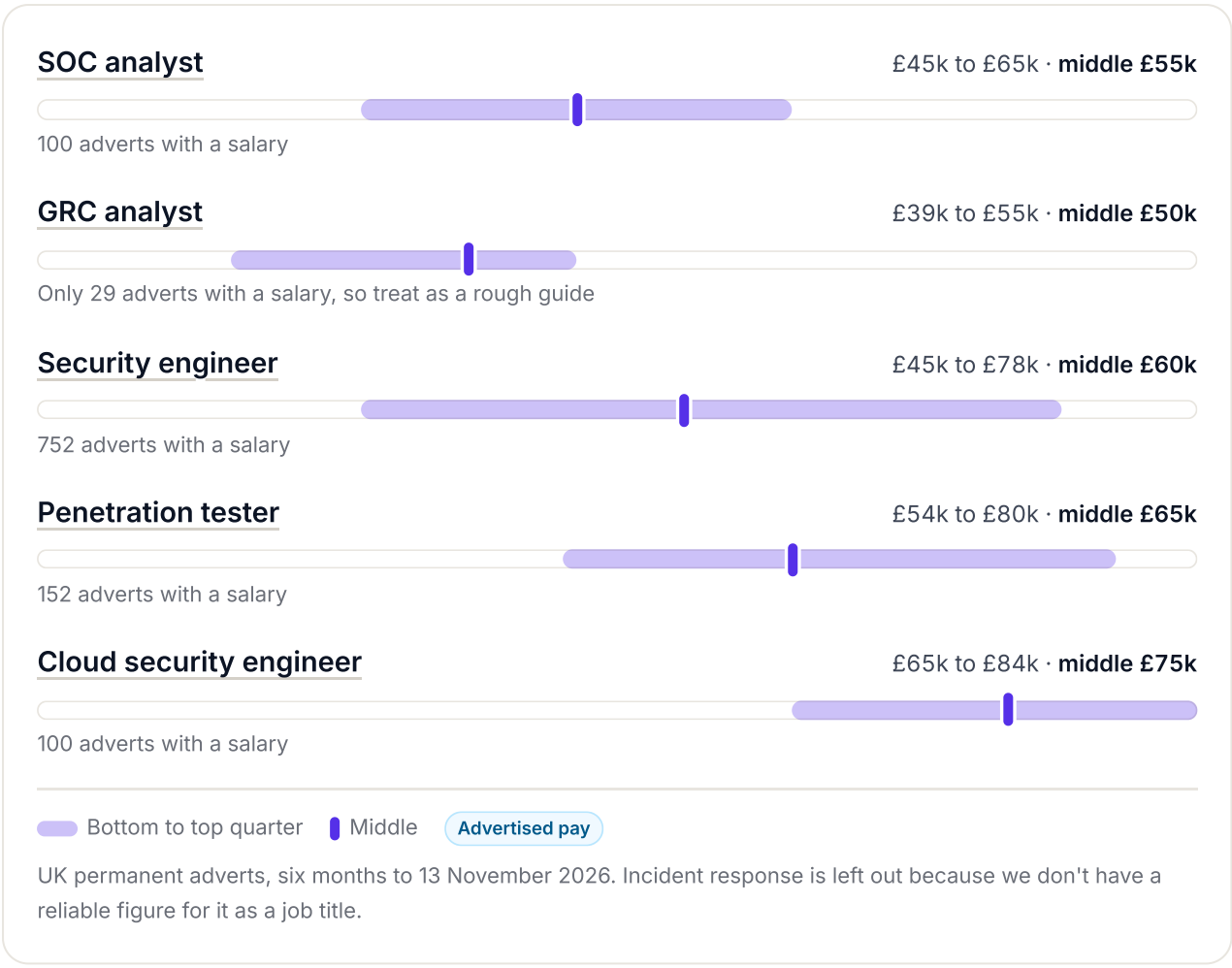
FIRST JOB?
Rarely a first job

MIDDLE ADVERTISED PAY
No reliable figure

Pay is the middle advertised salary for each job title across all experience levels, from IT Jobs Watch.

Advertised pay compared

Each bar runs from the bottom quarter to the top quarter of advertised salaries for that job title, with a marker at the middle. These cover every advert with the title, junior to senior, so starting pay is usually below the bar IT Jobs Watch.



UK permanent adverts, six months to 13 November 2026. Incident response is left out because we don't have a reliable figure for it as a job title.

KEY TAKEAWAY

Higher-paid paths are mostly second or third jobs. If you need a first role, SOC and GRC are the realistic targets, and our **entry-level jobs guide** shows what starting salaries look like.

SOC analyst

Often a first job | **Middle advertised pay: £55,000**

Suits people who like puzzles, patterns and working in a team on shifts

A security operations centre (SOC) is the team that watches an organisation's systems for signs of attack. Analysts work through alerts from security tools, decide which are real, investigate the suspicious ones and escalate genuine incidents. It's the most common technical first job in cyber security, and it maps onto the Council's Network Monitoring and Intrusion Detection and Secure Operations specialisms UK Cyber Security Council.

WHAT YOU'D DO

- Triage alerts in a SIEM (security information and event management) tool such as Microsoft Sentinel or Splunk

- Check suspicious emails, logins and files, and decide whether they are harmless or malicious
- Escalate real incidents to senior analysts or incident responders, with clear notes
- Tune detection rules so the team isn't buried in false alarms
- Often work shifts, including nights and weekends, in teams that run around the clock

SKILLS EMPLOYERS ASK FOR

- Networking and how Windows, Active Directory and Linux work
- SIEM tools: named in 29% of SOC analyst adverts, Splunk in 20% **IT Jobs Watch**
- MITRE ATT&CK (15%), PowerShell (14%) and Python (11%)
- Security clearance: mentioned in 35% of SOC adverts, so check eligibility before applying
- Clear writing, because every investigation ends in notes someone else has to act on

REALISTIC WAYS IN

- Junior or trainee SOC analyst roles, sometimes with in-house training
- The Level 4 Cyber security technologist apprenticeship, which has a defending and responding option **Skills England**
- A year or two in IT support or on a service desk, then an internal move or a junior SOC role
- CompTIA Security+ is the certification most often named in junior SOC adverts (15% of all SOC adverts) **CompTIA**, but practical evidence matters as much

UK PAY EVIDENCE

SOC analyst adverts: middle £55,000, bottom quarter £45,000 or less, across all levels
IT Jobs Watch

Advertised pay

The National Careers Service puts information security analyst pay at £35,000 for starters to £76,000 for experienced staff **National Careers Service**

Official guidance

WHERE IT LEADS

STAGE 1

Junior or trainee SOC analyst



STAGE 2

SOC analyst, then senior analyst

STAGE 3

Threat hunter or detection engineer

STAGE 4

Incident responder or SOC manager

Roles this path leads to include senior analyst, threat hunter, detection engineer, incident responder or SOC manager. Security operations manager adverts have a middle advertised salary of £77,500 IT Jobs Watch. Our **SOC analyst salary guide** goes into pay at each level.

See live UK SOC and defence roles →

Governance, risk and compliance (GRC)

Often a first job | **Middle advertised pay: £50,000 (small sample)**

Suits people who are organised, write clearly and like rules and process

GRC is the part of cyber security that decides what an organisation should protect, how much risk it can accept, and whether it's following its own rules and the law. It's less hands-on with technology day to day, and it's in demand: governance and risk management was the specialism most UK cyber businesses employed people in, at 42% of firms surveyed DSIT 2025.

The most requested skills across all UK cyber adverts in 2025 show how much of the field is governance, audit and risk:



Share of 34,932 UK cyber security adverts from 2025 naming each skill DSIT 2026.

WHAT YOU'D DO

- Write and update security policies and check people are following them
- Run risk assessments and keep the risk register up to date
- Gather evidence for audits and certifications such as ISO 27001 and Cyber Essentials
- Check that suppliers meet the organisation's security requirements
- Explain security risks to managers in business terms, not technical ones

SKILLS EMPLOYERS ASK FOR

- ISO/IEC 27001, named in 20% of UK cyber adverts in 2025 **DSIT 2026**
- Auditing (22%), governance (20%) and risk management (19%)
- UK frameworks such as Cyber Essentials **NCSC** and the NCSC Cyber Assessment Framework **NCSC**
- Clear writing, organisation and the confidence to challenge colleagues politely
- Enough technical understanding to know what a control actually does

REALISTIC WAYS IN

- Junior GRC, information security, IT risk or compliance analyst roles
- Graduate schemes in risk or technology consulting, which often accept any degree subject
- The risk analysis option of the Level 4 Cyber security technologist apprenticeship **Skills England**
- Moving across from audit, compliance, legal, finance, data protection, quality or project roles, where the habits are similar

UK PAY EVIDENCE

GRC analyst adverts: middle £50,000, bottom quarter £39,000 or less. Only 29 adverts quoted a salary, so treat this as a rough guide **IT Jobs Watch**

Advertised pay

WHERE IT LEADS

STAGE 1

Junior GRC or information security analyst

↓

STAGE 2

GRC lead

↓

STAGE 3

Information security manager

STAGE 4

Head of information security or CISO

For some

Roles this path leads to include GRC lead, information security manager, head of information security and, for some, chief information security officer (CISO). Information security manager adverts have a middle advertised salary of £75,000 IT Jobs Watch.

See live UK governance, risk and compliance roles →

Penetration testing

Rarely a first job | Middle advertised pay: £65,000

Suits people who are deeply technical, persistent and write good reports

Penetration testers, sometimes called ethical hackers, are hired to attack systems with permission and report the weaknesses before criminals find them. It's the path that attracts most beginners, and one of the hardest to start in: most testers spent time in IT, development or a SOC first. The Council calls this specialism Security Testing UK Cyber Security Council.

Only test what you're allowed to

Accessing or testing a computer system without permission is a criminal offence under the Computer Misuse Act 1990 legislation.gov.uk, even if you mean well. Practise only on your own equipment, deliberately vulnerable labs and platforms that give you permission.

WHAT YOU'D DO

- Test networks, web applications and cloud setups within an agreed scope and time window
- Use tools such as Burp Suite and Nmap, and check their findings by hand
- Write reports that explain each weakness, how serious it is and how to fix it
- Talk findings through with clients, often to non-technical people
- Keep learning constantly, because techniques change quickly

SKILLS EMPLOYERS ASK FOR

- Strong networking, Linux and Windows knowledge, and how web applications work

- Scripting, usually Python or Bash, to automate repetitive tasks
- Report writing, which is a large part of the job and often underestimated
- In the UK, CREST's CPSA and then CRT exams. CRT is the minimum standard for testers on the government's CHECK scheme **CREST**
- For government CHECK work, SC clearance and a Council professional title **NCSC**

REALISTIC WAYS IN

- Two or more years in IT, networking, development or a SOC, then a junior tester role
- A small number of graduate schemes at security consultancies
- Showing skill through capture the flag (CTF) events and practice labs, written up and linked from your CV
- Moving into testing inside an employer you already work for, starting with vulnerability scanning

UK PAY EVIDENCE

Penetration tester adverts: middle £65,000, bottom quarter £54,375 or less, mostly experienced roles **IT Jobs Watch**

Advertised pay

WHERE IT LEADS

STAGE 1

IT, networking, development or SOC role

Usually two or more years

↓

STAGE 2

Junior penetration tester

↓

STAGE 3

Senior tester or CHECK team leader

↓

STAGE 4

Red team, consultant or head of offensive security

Roles this path leads to include senior tester, CHECK team leader, red team operator, security consultant or head of offensive security.

See live UK penetration testing roles →

Cloud security

Rarely a first job | **Middle advertised pay: £75,000**

Suits people who already work with cloud, infrastructure or code

Most organisations now run at least some of their systems in Amazon Web Services, Microsoft Azure or Google Cloud. Cloud security specialists make sure those environments are set up safely: who can access what, how data is protected and how problems are spotted. It is rarely a first job, because you need to understand the cloud platform itself before you can secure it.

WHAT YOU'D DO

- Review cloud accounts for risky settings, such as storage open to the internet
- Design and manage identity and access, so people only have the permissions they need
- Write infrastructure as code (for example Terraform) with security checks built in
- Set up logging and alerts so the SOC can see what happens in the cloud
- Advise development teams on building securely

SKILLS EMPLOYERS ASK FOR

- Hands-on experience with at least one platform. Microsoft Azure appeared in 16% of UK cyber adverts in 2025 **DSIT 2026**
- Identity and access management, networking and encryption basics
- Automation (15% of adverts) and scripting in Python or PowerShell
- Vendor certifications, starting with fundamentals such as Microsoft SC-900 **Microsoft Learn**, then the platform's security specialty exams

REALISTIC WAYS IN

- Cloud support, cloud engineering, DevOps or systems administration roles first, then specialising in security
- Security engineering or SOC roles that look after cloud systems
- Graduate technology schemes that rotate through cloud teams

UK PAY EVIDENCE

Cloud security engineer adverts: middle £75,000, bottom quarter £65,000 or less. These are almost all experienced roles **IT Jobs Watch**

Advertised pay

WHERE IT LEADS

STAGE 1

Cloud support, DevOps or systems administration

↓

STAGE 2

Cloud security engineer

↓

STAGE 3

Senior cloud security engineer

↓

STAGE 4

Cloud security architect or head of cloud security

Roles this path leads to include senior cloud security engineer, cloud security architect or head of cloud security. Security architect adverts have a middle advertised salary of £85,000 **IT Jobs Watch**.

See live UK security engineering and cloud roles →

Security engineering

Sometimes a first job | Middle advertised pay: £60,000

Suits people who enjoy building, automating and fixing systems

Security engineers build and run the defences: firewalls, endpoint protection, identity systems, email filtering and the pipelines that feed the SOC. Where a SOC analyst responds to alerts, an engineer makes sure the tools that raise them work. Job titles vary a lot, from security engineer to infrastructure security or identity and access management engineer.

WHAT YOU'D DO

- Deploy and configure security tools across an organisation's devices and networks
- Automate routine work, such as patch checks or account reviews, with scripts
- Manage identity systems such as Microsoft Entra ID and multi-factor authentication
- Work with IT teams to fix weaknesses found by testers and scanners

- Keep documentation and diagrams up to date

SKILLS EMPLOYERS ASK FOR

- Systems administration on Windows and Linux, and solid networking
- Scripting in Python, PowerShell or Bash
- Cloud platforms, especially Azure (16% of UK cyber adverts) DSIT 2026
- Experience with specific products named in the advert, such as a firewall or endpoint tool

REALISTIC WAYS IN

- From IT support, systems administration, network engineering or software development
- The security engineering option of the Level 4 Cyber security technologist apprenticeship Skills England
- Graduate schemes in technology or cyber, which often include an engineering rotation

UK PAY EVIDENCE

Security engineer adverts: middle £60,000, bottom quarter £45,000 or less, from 752 adverts quoting a salary IT Jobs Watch

Advertised pay

WHERE IT LEADS

STAGE 1

IT support, systems, networking or development

↓

STAGE 2

Security engineer

↓

STAGE 3

Senior or lead engineer

↓

STAGE 4

Cloud or detection engineer, or security architect

Roles this path leads to include senior or lead engineer, cloud security engineer, detection engineer, or security architect (middle advertised salary £85,000) IT Jobs Watch.

See live UK security engineering roles →

Incident response

Rarely a first job | **Middle advertised pay: No reliable figure**

Suits people who stay calm under pressure and like investigation

When a serious attack gets through, incident responders take over: they work out what happened, stop it spreading, remove the attacker and help the organisation recover. The work is high pressure and often happens out of hours. Incident Response is one of the Council's 15 specialisms UK Cyber Security Council, and it was named in 18% of UK cyber adverts in 2025 DSIT 2026.

WHAT YOU'D DO

- Lead or support the response to live incidents such as ransomware or a compromised email account
- Collect and analyse evidence from computers, logs and memory
- Work out how the attacker got in and what they touched
- Write timelines and reports for managers, lawyers or regulators
- Run practice exercises and improve the organisation's response plan

SKILLS EMPLOYERS ASK FOR

- Strong log analysis and Windows internals, often learned in a SOC
- Digital forensics tools and techniques
- Calm, clear communication with stressed people, and careful note-taking
- Willingness to be on call

REALISTIC WAYS IN

- Most responders start as SOC analysts and move up as they handle more serious incidents
- Digital forensics roles, including in policing, are another route
- Specialist incident response consultancies hire some juniors, but usually after a SOC or forensics role

UK PAY EVIDENCE

We don't have a reliable UK pay figure for incident responder as a job title. Because most responders come up through the SOC, the SOC analyst and security operations manager figures above are the closest guide.

WHERE IT LEADS

STAGE 1

SOC analyst or digital forensics role

STAGE 2

Incident responder

STAGE 3

Senior responder or DFIR consultant

STAGE 4

Threat hunter or SOC manager

Roles this path leads to include senior incident responder, digital forensics and incident response (DFIR) consultant, threat hunter or SOC manager.

See live UK SOC and incident response roles →

How to choose a path

You don't need to choose for life, and many people move between these paths. But employers respond better to someone who can say “I want to be a SOC analyst, and here's what I've done about it” than to “I want to get into cyber”. A few honest questions help:

Do you enjoy hands-on technology?

If you like taking things apart, scripting and fixing computers, look at **SOC**, **security engineering** or, longer term, **penetration testing** or **cloud security**.

Are you happier with people, process and writing?

GRC uses those strengths, and many career changers from audit, admin, compliance and teaching do well there.

Can you work shifts?

Many SOC roles involve nights and weekends. Some don't, so check the advert.

Can you get security clearance?

A lot of UK defence and government security work needs it, which normally means several years' UK residence. Our **first job guide** explains how it works.

What do you already know?

Your existing experience is usually the shortest bridge. A network engineer is closer to security engineering than to GRC, and an auditor is the other way round.

TRY BEFORE YOU CHOOSE

Spend a few weeks on free introductory material for two paths, such as a beginner SOC lab and a beginner ISO 27001 course, and notice which one you want to keep doing.

How cyber security careers progress

Most careers follow a similar shape whatever the specialism. Prospects describes the same pattern for analysts, from entry-level to senior analyst or consultant and, with extensive experience, to head of cyber security Prospects.

STAGE 1

Junior role

Learn the basics under supervision

↓

STAGE 2

Analyst, engineer or consultant

Two to five years building depth

↓

STAGE 3

Senior specialist or leadership

Go deeper technically, or lead a team

The UK Cyber Security Council also awards professional titles at four levels UK Cyber Security Council. They're aimed at people with experience rather than beginners, but

they're worth knowing about: some government work, such as CHECK penetration testing, now requires them NCSC.

STAGE 1
Associate

↓

STAGE 2
Practitioner

↓

STAGE 3
Principal

↓

STAGE 4
Chartered

What experience pays

The pay figures above cover every advert with each title, junior to senior. For a fuller picture by experience level, region and employer, see our **UK cyber security salary guide**.

Other cyber security specialisms

The six paths above aren't the whole field. The Council's framework also covers these specialisms UK Cyber Security Council, several of which are reachable from other careers:

Cyber threat intelligence

Researching attackers and their methods. Suits people with research, analysis or language skills.

Digital forensics

Recovering and analysing evidence from devices, often for police investigations.

Identity and access management

Making sure only the right people can reach systems and data.

Vulnerability management

Finding, prioritising and tracking fixes for weaknesses across an organisation.

Data protection and privacy

Keeping personal data safe and lawful. A natural move from legal or data protection work.

Secure system development and architecture

Designing and building software and systems that are secure from the start.

Audit and assurance, and cryptography

Checking that controls work, and designing the encryption that protects communications.

Not sure where to start?

The free Cyberend beginner roadmap covers the computer and network basics every path needs, how to choose a direction, and a 12-week plan to follow.

Get the free roadmap

Common questions

Which cyber security career is easiest to get into?

None is easy, but SOC analyst and junior GRC roles are the most common first jobs, and both have apprenticeship routes. Many people also start in IT support and move across, which takes longer but is often more reliable.

Do I need to be able to code?

Not for every path. GRC roles rarely need it. SOC and engineering roles benefit from basic scripting in Python or PowerShell, and cloud security and penetration testing need more. You can start without it and learn as you go.

Can I become a penetration tester straight away?

It's possible but uncommon. Most penetration testers had IT, development or SOC experience first. If testing is your goal, a SOC or IT role plus regular practice in legal labs and CTF events is a realistic route.

Is GRC a real cyber security job?

Yes. Governance and risk management was the specialism most UK cyber businesses employed people in DSIT 2025, and auditing, governance and ISO 27001 were among the skills most requested in 2025 adverts DSIT 2026.

How much do cyber security jobs pay in the UK?

It depends heavily on the role and experience. Advertised pay for the paths here ranges from a middle figure of £50,000 for GRC analysts to £75,000 for cloud security engineers, across all levels. Starting pay is lower: see the **entry-level jobs guide**.

Sources and method

The descriptions of each path draw on the UK Cyber Security Council's Cyber Career Framework, which defines 15 recognised specialisms, and on official UK careers profiles. Which skills employers ask for comes from the government's 2026 cyber skills report (34,932 UK cyber job adverts from 2025) and from IT Jobs Watch's analysis of SOC analyst adverts.

Pay figures are advertised salaries from IT Jobs Watch (UK permanent adverts, six months to 13 November 2026) and cover every advert with that job title, so they include experienced and senior roles. They are not starting salaries. Where we have no reliable figure for a job title, we say so rather than estimate. For starting pay on named graduate schemes and apprenticeships, see the **entry-level jobs guide**.

The career routes under each path show common next steps named in this guide and its sources. They are typical, not fixed: plenty of people skip stages or move sideways between paths.

UK Cyber Security Council: Cyber Career Framework Professional or certifying body

The profession's 15 recognised specialisms, such as Incident Response, Security Testing and Governance and Risk Management, with typical tasks, skills and routes in from other careers.

UK Cyber Security Council: Professional registration Professional or certifying body

The Associate, Practitioner, Principal and Chartered professional titles for experienced cyber security practitioners.

Department for Science, Innovation and Technology: Cyber security skills in the UK labour market 2026

Advertised pay

Research by Ipsos and Perspective Economics, published 29 September 2026. Pay figures come from 34,932 UK core cyber job adverts in 2025 (Lightcast), of which 8,481 stated a salary.

Department for Science, Innovation and Technology: Cyber security skills in the UK labour market 2025

Official guidance

A survey of 209 UK cyber sector businesses (fieldwork 2024) on which Cyber Career Framework specialisms their staff work in.

IT Jobs Watch: UK permanent job title salary statistics Advertised pay

Salaries quoted in UK permanent IT job adverts in the six months to 13 November 2026, by job title. Licensed under CC BY-NC-SA 4.0.

National Careers Service: Job profile: IT security co-ordinator (information security analyst)

Official guidance

The official England careers profile for security analyst work: day-to-day tasks, skills and routes in.

Prospects (Jisc): Job profile: Cyber security analyst

Official guidance

The UK graduate careers service's profile of the role, including typical career progression.

Skills England: Cyber security technologist (2021), Level 4 apprenticeship standard ST1021

Official guidance

The current Level 4 cyber apprenticeship in England: options, typical duration and job titles.

CREST: CREST Registered Penetration Tester (CRT): FAQs

Professional or certifying body

The CRT exam, its CPSA prerequisite, its three-year validity and its role as the minimum standard for CHECK team members.

National Cyber Security Centre: Assured CHECK Scheme Standard

Official guidance

Requirements for penetration testers on government CHECK tests, including professional titles and SC clearance.

CompTIA: CompTIA Security+

Professional or certifying body

The vendor-neutral entry-level security certification: what it covers and how the exam works.

Microsoft: Microsoft Certified: Security, Compliance, and Identity Fundamentals (SC-900)

Professional or certifying body

Microsoft's introductory security certification, with free self-paced learning paths.

National Cyber Security Centre: Cyber Essentials

Official guidance

The UK government-backed scheme setting five basic technical controls for organisations.

National Cyber Security Centre: Cyber Assessment Framework

Official guidance

The NCSC's framework for assessing how well organisations that run essential services manage cyber risk.

legislation.gov.uk: Computer Misuse Act 1990

Official guidance

The UK law that makes accessing or testing computer systems without permission a criminal offence.

Every figure and link in this guide was checked against its source on 22 November 2026. Live job listings update every few hours.

This is a PDF copy of a free Cyberend guide. Read it online, with today's live UK cyber security jobs, at cyberend.io/resources/cyber-security-career-paths.