The Cybersecurity Career Tree

Every career path in cybersecurity — explained simply.

AUTHOR	Babashaheer
VERSION	1.0
DATE	April 2026
SERIES	Cybersecurity Career Series — Document 02 of 06
COVERS	All 8 major cybersecurity career branches in one document

Ethical Hacking · Forensics · Malware · Network Sec · AppSec · Cloud Sec · SOC / Blue Team · GRC

Contents

1.	How to Use This Document	**3**
2.	The Cybersecurity Career Tree — Visual Overview	**3**
3.	Ethical Hacking & Penetration Testing	**4**
4.	Digital Forensics & Incident Response	**5**
5.	Malware Analysis & Reverse Engineering	**6**
6.	Network Security	**7**
7.	Application Security (AppSec)	**8**
8.	Cloud Security	**9**
9.	Security Operations (SOC / Blue Team)	**10**
10.	Governance, Risk & Compliance (GRC)	**11**
11.	How to Choose Your Path	**12**
12.	References	**13**

Baba Shaheer Gutappa
Digitally signed by Baba Shaheer Gutappa
Date: 2026.04.16 12:06:17 +01'00'

1. How to Use This Document

This document gives you a complete map of the cybersecurity field. Eight major career branches are covered — each one explained with what it involves, what skills it needs, which certifications to aim for and what kind of person tends to thrive in it.

You do not need to read it cover to cover. Use it as a reference. Find the branch that sounds most like you, then move on to the dedicated document in this series for that specific path. Each branch in this series gets its own detailed document with a full learning roadmap, tool guide and job hunting advice.

> Document 01: Making a Career in Ethical Hacking (already published)
> **Document 02: This document — the career tree overview**
> Documents 03–06: One deep-dive per career branch (coming next)

2. The Cybersecurity Career Tree — Visual Overview

Cybersecurity is not one job. It is a field with many distinct specialisms, each with its own tools, skills and career trajectory. The diagram below maps out the major branches. Think of the trunk as the common foundation — networking, operating systems and security fundamentals — that every branch grows from.

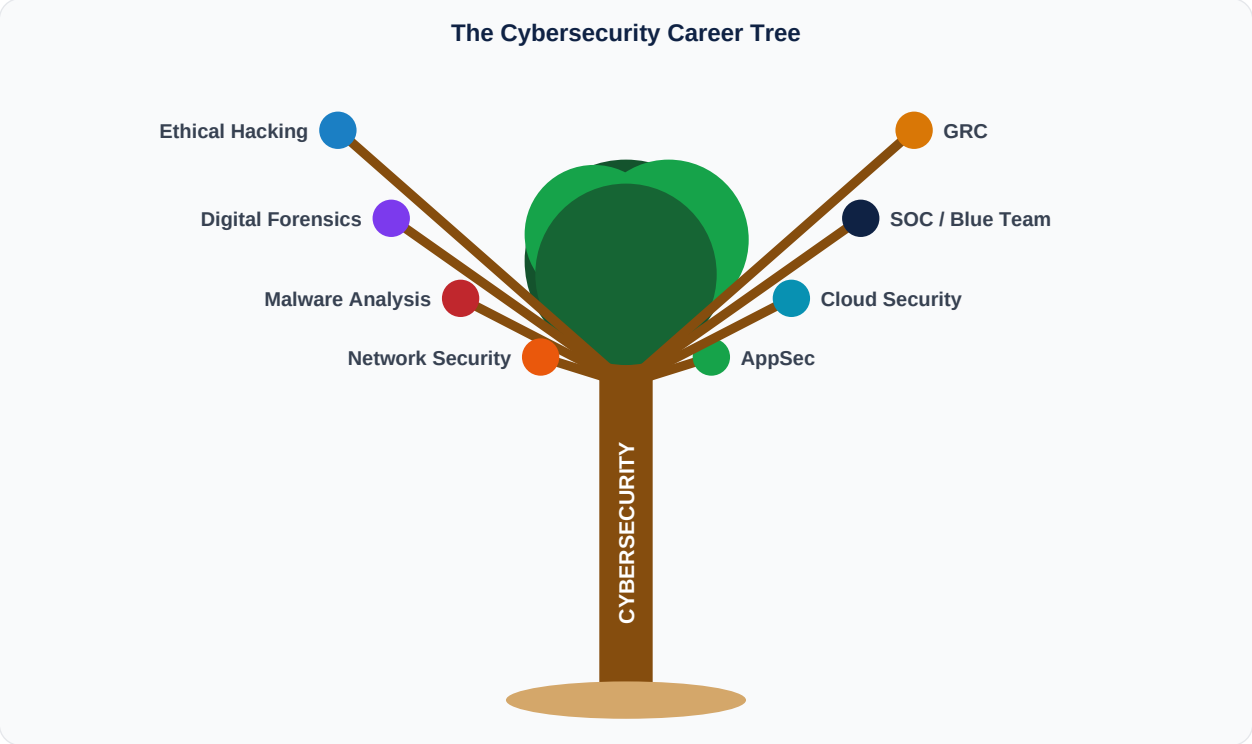


Figure 1: The cybersecurity career tree. Each branch is a distinct career path. All branches share the same foundational trunk.

3. Ethical Hacking & Penetration Testing

Ethical Hacking & Penetration Testing

Ethical hackers are paid to break into systems before real attackers do.

All levels | £30k–£95k+

Ethical hackers are paid to break into systems before real attackers do. You simulate cyberattacks — against networks, web applications, physical premises or staff — using the same techniques a real adversary would use. Everything is documented, reported and used to help the organisation fix its weaknesses. This is an offensive security discipline: you are always thinking like an attacker.

A Typical Day Involves...

- Running Nmap scans and enumeration
- Testing web apps for OWASP Top 10 flaws
- Writing exploitation scripts in Python
- Privilege escalation on compromised hosts
- Writing client reports and findings
- Researching new CVEs and techniques

Work Environment

- Consulting firm or in-house team
- Mix of remote and client on-site
- Short engagements (days to weeks)
- Collaborative — debrief calls with clients
- Continuous self-study required

Key Skills Required

Certifications to Target	Who Suits This Path?
CompTIA Security+	Problem-solvers
CEH (EC-Council)	Lateral thinkers
eJPT	Self-starters
OSCP (Offensive Security)	Detail-oriented
CREST CRT/CCT	Enjoy hands-on labs

Already covered in depth: see Document 01 — Making a Career in Ethical Hacking.

4. Digital Forensics & Incident Response

Digital Forensics & Incident Response

Digital forensics professionals investigate cybersecurity incidents after they happen.

All levels | £28k–£80k+

Digital forensics professionals investigate cybersecurity incidents after they happen. When a company is breached, infected with ransomware or suspects insider fraud, a forensics analyst is called in to piece together exactly what happened — which systems were accessed, what data was taken, how the attacker got in and what evidence can be preserved for legal proceedings. DFIR (Digital Forensics and Incident Response) is a reactive discipline: you clean up and investigate the scene.

A Typical Day Involves...

- Acquiring forensic disk images
- Analysing Windows event logs
- Recovering deleted files and artefacts
- Memory forensics with Volatility
- Writing forensic investigation reports
- Testifying as an expert witness

Work Environment

- Incident response firms or law enforcement
- Often called out at short notice
- High-pressure, deadline-driven
- Works with legal teams and police
- Strong documentation culture

Key Skills Required

Certifications to Target	Who Suits This Path?
CompTIA Security+	Methodical thinkers
CHFI (EC-Council)	Detail-obsessed
GCFE / GCFA (GIAC)	Calm under pressure
EnCE (EnCase)	Interest in law
CREST CPIA	Patient investigators

5. Malware Analysis & Reverse Engineering

Malware Analysis & Reverse Engineering

Malware analysts take malicious software apart to understand how it works.

Mid–Senior

£35k–£85k+

Malware analysts take malicious software apart to understand how it works. When a new virus, ransomware strain or backdoor is discovered, someone has to figure out what it does, how it spreads, what it communicates with and how to detect and remove it. This is one of the most technically demanding branches of cybersecurity — it requires strong programming knowledge, patience and an almost obsessive attention to detail. Reverse engineers work at the lowest level of software, often reading raw assembly code.

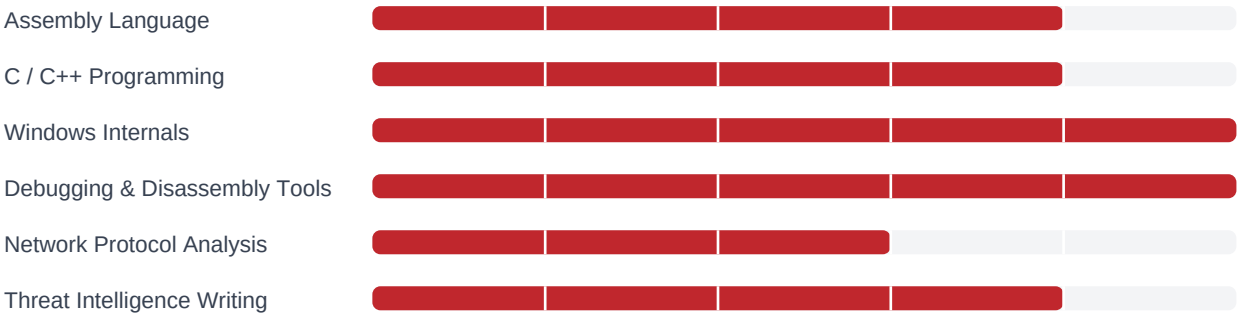
A Typical Day Involves...

- Static analysis of suspicious binaries
- Dynamic analysis in sandboxed VMs
- Disassembling code in Ghidra/IDA Pro
- Writing YARA detection rules
- Producing threat intelligence reports
- Tracking malware families and campaigns

Work Environment

- Threat intelligence or AV vendors
- Government / GCHQ / intelligence roles
- Mostly desk-based, deep focus work
- Small specialist teams
- Very high technical depth required

Key Skills Required



Certifications to Target	Who Suits This Path?
GREM (GIAC Reverse Engineering Malware)	Deep technical mindset
CHFI (EC-Council)	Programmers moving into security
Malware Unicorn courses (free)	Puzzle-solvers
CompTIA Security+	Extreme patience
TCM Security PMAT	Research-oriented

6. Network Security

Network Security

Network security professionals design, implement and monitor the security of an organisation's network infrastructure.

All levels | £28k–£75k+

Network security professionals design, implement and monitor the security of an organisation's network infrastructure. This includes configuring firewalls, intrusion detection and prevention systems (IDS/IPS), VPNs, network segmentation and monitoring tools. Unlike ethical hacking, this is primarily a defensive discipline — you are building and maintaining the walls, rather than looking for gaps in them. It overlaps significantly with network engineering, and many network security professionals start their careers as network engineers or administrators.

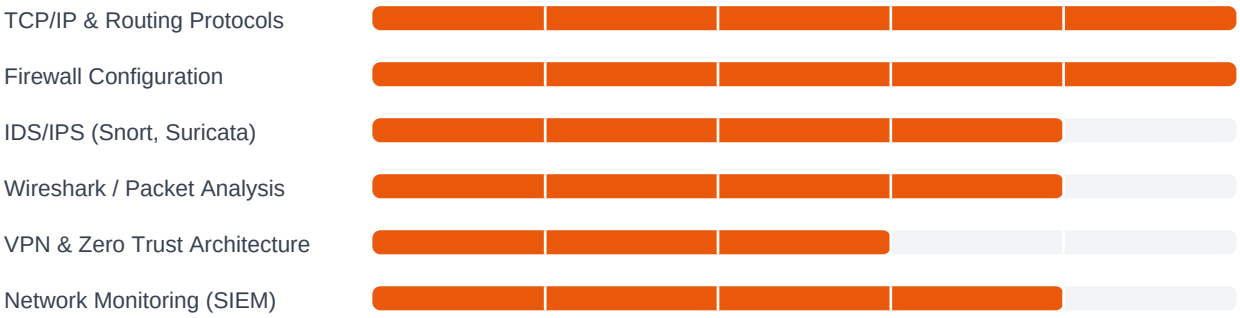
A Typical Day Involves...

- Configuring and managing firewalls
- Reviewing IDS/IPS alerts
- Network segmentation and VLAN design
- Packet capture and traffic analysis
- VPN setup and management
- Responding to network-level incidents

Work Environment

- Corporate IT teams or MSSPs
- Mostly office/remote — operational role
- On-call rotation is common
- Works closely with network engineers
- Long-term infrastructure projects

Key Skills Required



Certifications to Target	Who Suits This Path?
CompTIA Network+	Networking background
CompTIA Security+	Structured methodical workers
Cisco CCNA Security	Enjoy operational roles
PCNSA (Palo Alto)	Good at documentation
Fortinet NSE certifications	Problem diagnosticians

7. Application Security (AppSec)

Application Security (AppSec)

Application security specialists focus on making software secure — both during development and after deployment.

Mid–Senior

£35k–£90k+

Application security specialists focus on making software secure — both during development and after deployment. Where a penetration tester might find a SQL injection vulnerability in a live application, an AppSec engineer works with the development team to make sure it never gets built in the first place. This involves threat modelling, secure code review, integrating security tooling into CI/CD pipelines (DevSecOps), and training developers to write code that is harder to exploit. AppSec sits at the intersection of software development and security.

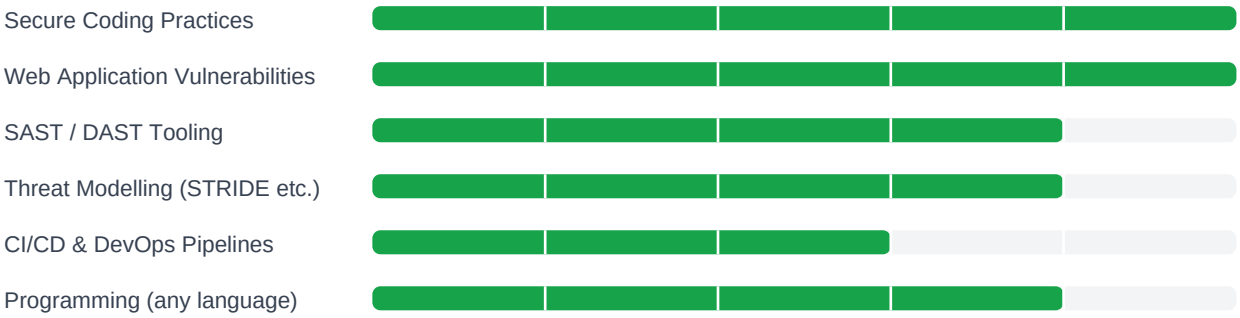
A Typical Day Involves...

- Secure code review (SAST tools)
- Threat modelling new features
- Running DAST scans on live apps
- Integrating security into CI/CD
- Developer security training
- Triaging vulnerability scanner output

Work Environment

- Software companies or financial sector
- Embedded in development teams
- Agile / sprint-based work environment
- Mix of technical and advisory work
- Fast-paced, product-focused

Key Skills Required



Certifications to Target	Who Suits This Path?
GWEB (GIAC Web App Defender)	Developers moving into security
CSSLP (ISC2)	OWASP-curious engineers
PortSwigger Web Academy (free)	Enjoy code review
CompTIA Security+	Strong communicators
OSWE (Offensive Security)	Team-oriented

8. Cloud Security

Cloud Security

Cloud security is the fastest-growing specialism in cybersecurity right now.

Mid–Senior

£45k–£100k+

Cloud security is the fastest-growing specialism in cybersecurity right now. As organisations move their infrastructure to AWS, Microsoft Azure and Google Cloud, they need people who understand how to secure that environment. Cloud security is not just 'security but in the cloud' — the attack surface, the tools and the threat model are all different from traditional on-premise security. Misconfigurations are the leading cause of cloud breaches (Gartner, 2023): an S3 bucket left publicly readable, an IAM role with excessive permissions, or a storage account with no encryption can expose millions of records in minutes.

A Typical Day Involves...

- Auditing IAM roles and permissions
- Reviewing cloud security posture (CSPM)
- Hunting for misconfigured S3/Blob storage
- Reviewing serverless function security
- Cloud incident response and log analysis
- Writing cloud security architecture docs

Work Environment

- Tech companies, financial sector, consulting
- Highly remote-friendly role
- Fast-moving — cloud platforms change constantly
- Works with DevOps and platform engineering
- High commercial demand and short supply

Key Skills Required

Certifications to Target	Who Suits This Path?
AWS Security Specialty	Cloud engineers adding security
Microsoft SC-100 / AZ-500	Fast learners
Google PCSE	Comfortable with constant change
CCSP (ISC2)	Remote workers
CompTIA Cloud+	High earners

9. Security Operations — SOC & Blue Team

Security Operations Centre (SOC) / Blue Team

The Security Operations Centre is the organisation's frontline defence.

Entry–Senior | £22k–£65k+

The Security Operations Centre is the organisation's frontline defence. SOC analysts monitor systems 24 hours a day, seven days a week, looking for signs of attack. When an alert fires — a login from an unusual country, a spike in outbound traffic, a suspicious process running on a server — the SOC analyst investigates, determines whether it is a real threat, and escalates or responds accordingly. The SOC is often the first career entry point into cybersecurity. Tier 1 roles are accessible with relatively modest experience, and the work builds real-world threat analysis skills quickly.

A Typical Day Involves...

- Triaging SIEM alerts (Splunk, Sentinel)
- Investigating phishing emails
- Threat hunting using IOCs
- Escalating incidents to Tier 2/3
- Writing incident tickets and reports
- Reviewing EDR alerts (CrowdStrike, SentinelOne)

Work Environment

- MSSP or in-house SOC
- Shift work — 24/7 coverage required
- Team-based, structured environment
- Fast decision-making under pressure
- Good starting point for many other paths

Key Skills Required

Certifications to Target	Who Suits This Path?
■ CompTIA Security+	■ Good under pressure
■ SC-200 (Microsoft Sentinel)	■ Enjoy shift work
■ BTL1 (Blue Team Labs Online)	■ Analytical mindset
■ CySA+ (CompTIA)	■ Strong communicators
■ GCIA / GCIH (GIAC)	■ Looking for a structured start

10. Governance, Risk & Compliance (GRC)

Governance, Risk & Compliance (GRC)

GRC professionals ensure that organisations manage cybersecurity risk systematically and comply with the regulations and standards that apply to them.

All levels | £30k–£100k+

GRC professionals ensure that organisations manage cybersecurity risk systematically and comply with the regulations and standards that apply to them. This includes implementing frameworks like ISO 27001 and NIST, conducting risk assessments, writing security policies, preparing for audits, managing third-party supplier risk and ensuring GDPR compliance. GRC is the least technical branch of cybersecurity in terms of hands-on hacking — but it is no less important. Regulatory fines and reputational damage from compliance failures cost organisations as much as technical breaches. GRC professionals are increasingly in demand and often progress into senior leadership roles (CISO, DPO, Head of Risk).

A Typical Day Involves...

- Writing and reviewing security policies
- Conducting risk assessments
- Preparing for ISO 27001 audits
- Managing third-party supplier risk
- GDPR compliance and data mapping
- Security awareness programme management

Work Environment

- Financial services, healthcare, government
- Office or remote — minimal shift work
- Works with legal, HR and senior leadership
- Strong writing and communication focus
- Pathway to CISO or DPO roles

Key Skills Required

Certifications to Target	Who Suits This Path?
CISM (ISACA)	Strong writers
CISSP (ISC2)	Policy-minded thinkers
ISO 27001 Lead Implementer/Auditor	Non-technical background welcome
CRISC (ISACA)	Leadership ambitions
BCS Practitioner Certificate in Info Security	Risk-aware mindset

11. How to Choose Your Path

The most common question from people entering cybersecurity is: which path should I take? There is no single correct answer. The right path is the one that matches how your brain works, what kind of work you can sustain over years and what kind of environment you want to be in. Below are a few honest questions to help you narrow it down.

If you ask yourself this...	...it might point you towards
Do I enjoy breaking things and figuring out how they work?	Ethical Hacking / Penetration Testing
Am I drawn to investigating what went wrong after an incident?	Digital Forensics & Incident Response
Do I find low-level programming and how software works at a binary level fascinating?	Malware Analysis & Reverse Engineering
Am I comfortable in an operational role managing infrastructure day to day?	Network Security
Do I write code and want to make it more secure?	Application Security (AppSec)
Am I already working with cloud platforms and want to add security knowledge?	Cloud Security
Do I want a structured team role with clear processes as my entry point?	SOC / Blue Team
Do I prefer strategy, policy and communication over hands-on technical work?	GRC

Table 1: Self-assessment questions to help identify your cybersecurity career branch

A few things worth knowing

- **You will not be stuck in one lane.** Many cybersecurity professionals work across more than one area, or move between branches as their career develops. Starting in the SOC and moving to penetration testing, or starting in network security and specialising in cloud, are very common progressions.
- **Technical is not the only path.** GRC and security management roles are genuinely valued and well paid. Not everyone needs to become a penetration tester to have a successful cybersecurity career.
- **The foundations are the same.** Whatever branch you choose, the starting point is the same: networking, operating systems, and basic security principles. Get those right first.
- **Practical evidence matters.** In every branch, employers respond to people who can demonstrate what they have done — labs, certs, personal projects, write-ups. Credentials alone are rarely enough.

Salary Summary by Branch (UK, 2024)

Career Branch	Junior	Mid-level	Senior / Lead
Ethical Hacking / Pentesting	£30–45k	£50–75k	£75k–£95k+

Career Branch	Junior	Mid-level	Senior / Lead
Digital Forensics	£28–40k	£45–65k	£65k–£80k+
Malware Analysis	£35–48k	£50–70k	£70k–£90k+
Network Security	£28–40k	£45–65k	£65k–£80k+
AppSec	£35–50k	£55–75k	£75k–£95k+
Cloud Security	£45–60k	£65–80k	£80k–£110k+
SOC / Blue Team	£22–32k	£35–50k	£55k–£70k+
GRC	£30–42k	£48–65k	£65k–£100k+

Table 2: UK salary ranges by cybersecurity career branch (CW Jobs, 2024; Reed, 2024)

12. References

1. CW Jobs (2024) *Technology Salary Survey 2024.* Available at: https://www.cwjobs.co.uk/salary-checker [Accessed: 10 April 2026].

2. DSIT (2024) *Cyber Security Skills in the UK Labour Market 2024.* Department for Science, Innovation and Technology. Available at: https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2024 [Accessed: 10 April 2026].

3. Gartner (2023) *Cloud Security: The Most Common Cause of Breaches Is Misconfiguration.* Available at: https://www.gartner.com/en/documents/cloud-misconfiguration [Accessed: 11 April 2026].

4. GIAC (2024) *Certifications Overview.* Available at: https://www.giac.org/certifications [Accessed: 11 April 2026].

5. ISC2 (2023) *Cybersecurity Workforce Study 2023.* Available at: https://www.isc2.org/Research/Workforce-Study [Accessed: 11 April 2026].

6. ISACA (2024) *CISM and CRISC Certification Overview.* Available at: https://www.isaca.org/credentialing [Accessed: 12 April 2026].

7. National Cyber Security Centre (NCSC) (2024) *Cyber Security Careers.* Available at: https://www.ncsc.gov.uk/section/education-skills/careers [Accessed: 12 April 2026].

8. Offensive Security (2024) *OSCP, OSWE and OSED Certifications.* Available at: https://www.offensive-security.com [Accessed: 12 April 2026].

9. OWASP Foundation (2021) *OWASP Top Ten 2021.* Available at: https://owasp.org/Top10/ [Accessed: 12 April 2026].

10. Reed (2024) *Cybersecurity Salary Guide UK 2024.* Available at: https://www.reed.co.uk/career-advice/cybersecurity-salary [Accessed: 13 April 2026].

11. TryHackMe (2024) *SOC Analyst, Red Teaming and Other Learning Paths.* Available at: https://tryhackme.com/paths [Accessed: 13 April 2026].

Document prepared by **Babashaheer**. Version 1.0 — April 2026. Cybersecurity Career Series — Document 02 of 06.