Area of Focus	Entry Level Requirements	Day-to-day job duties in a real company	Job titles (by level & years)
Governance & Risk Management (GRC)	Basics of risk, controls, policies; read ISO 27001/27002, NIST CSF/800-53; Excel & reporting; stakeholder comms; ability to write policies/standards; **nice-to-have certs:** Security+, ISO 27001 Foundation	Maintain risk register; collect control evidence; draft/maintain policies & standards; support internal/external audits; vendor/third-party risk questionnaires; track remediation & metrics; exception management	**Entry (0–2):** GRC Analyst I, Security Compliance Analyst, Risk Analyst **Intermediate (2–5):** GRC Analyst II, IT Auditor, Third-Party Risk Analyst **Advanced (5–8):** Senior GRC Analyst, Security Program Manager, Senior IT Auditor **Expert (8–12+):** GRC Manager/Lead, Head of GRC, Director of Risk & Compliance
Security Architecture & Design	Strong OS/network/cloud fundamentals; diagramming & design patterns; Zero Trust basics; threat modeling basics; **nice-to-have:** AWS/Azure/GCP fundamentals	Review solution designs; define security requirements; create reference architectures; perform threat modeling; choose controls & patterns; partner with platform/app/network teams; design reviews & sign-offs	**Entry (0–2):** Associate Security Architect, Junior Security Engineer (Architecture) **Intermediate (2–5):** Security Architect, Application Security Architect, Cloud Security Architect **Advanced (5–8):** Senior/Enterprise Security Architect **Expert (8–12+):** Principal/Chief Security Architect, Director of Security Architecture
Network & Infrastructure Security	TCP/IP, routing/switching, OS hardening; firewalls/IDS/IPS/VPN; Linux/Windows admin; scripting (Python/Bash/PowerShell); **nice-to-have:** Security+, CCNA	Operate firewalls/VPNs/NAC; network segmentation; server/network hardening & patching; log pipeline upkeep; IDS/IPS tuning; vuln remediation with infra teams; documentation/runbooks	**Entry (0–2):** Network Security Analyst, Security Operations Engineer (Infra) **Intermediate (2–5):** Network Security Engineer, Security Engineer (Infrastructure) **Advanced (5–8):** Senior Network Security Engineer, Infrastructure Security Lead **Expert (8–12+):** Principal/Staff Security Engineer (Network), Security Engineering Manager
Identity & Access Management (IAM)	AD/Azure AD basics; SSO/SAML/OAuth/OIDC; RBAC/least privilege; identity lifecycle; scripting for automation; **nice-to-have:** Okta/Azure AD associate cert	Provision/deprovision; app onboarding to SSO; MFA & conditional access policies; access reviews & role design; joiner/mover/leaver automation; directory hygiene; PAM operations & vaulting	**Entry (0–2):** IAM Analyst, Access Management Analyst **Intermediate (2–5):** IAM Engineer, SSO/Directory Engineer (Okta/Azure AD) **Advanced (5–8):** Senior IAM Engineer, IAM Architect, PAM Engineer **Expert (8–12+):** IAM Manager, Principal IAM Architect, Head of Identity
Application Security (DevSecOps)	SDLC & CI/CD basics; OWASP Top 10; code review fundamentals; know 1+ language; SAST/DAST/SCA tools; Git workflows	Triage & tune SAST/DAST/SCA; threat model features; enforce pipeline policies; secure-coding guidance & training; partner on vulns/PR reviews; manage bug bounty & vuln backlog; supply-chain security (deps, secrets)	**Entry (0–2):** AppSec Analyst, Junior Product Security Engineer **Intermediate (2–5):** Application Security Engineer, DevSecOps Engineer, Product Security Engineer **Advanced (5–8):** Senior AppSec/ProdSec Engineer, Team Lead, Security Champions Lead **Expert (8–12+):** Principal/Staff AppSec Engineer, AppSec Manager, Head of Product Security
Privacy & Data Security	Data lifecycle & classification; GDPR/CCPA basics; DLP concepts; encryption & key management basics; records retention; **nice-to-have:** CIPP/E, CIPT	Build data inventory/maps; run DPIAs/PIAs; tune DLP policies; coordinate data subject requests; advise on privacy-by-design; support key mgmt & tokenization; retention & deletion workflows; vendor privacy reviews	**Entry (0–2):** Privacy Analyst, Data Protection Analyst **Intermediate (2–5):** Privacy Program Manager, Data Security/DLP Engineer **Advanced (5–8):** Senior Privacy Manager/Specialist, Senior Data Protection Engineer **Expert (8–12+):** Data Protection Officer (DPO), Head of Privacy, Director of Data Security
Security Operations Center (SOC)	SIEM basics; log triage; EDR fundamentals; Windows/Linux/M365 logs; basic scripting; playbooks/runbooks; **nice-to-have:** CySA+	Monitor & triage alerts; investigate hosts in EDR; tune detection rules & use-cases; enrich with TI; ticketing & escalations; knowledge base upkeep; shift handovers & daily ops reporting	**Entry (0–2):** SOC Analyst Tier 1, MSSP Analyst **Intermediate (2–5):** SOC Analyst Tier 2, Threat Hunter, Detection Engineer **Advanced (5–8):** SOC Analyst Tier 3, Incident Handling Lead, SOC Engineer **Expert (8–12+):** SOC Manager, Head of Detection & Response, Director of SecOps
Incident Response (IR)	IR lifecycle (prepare/detect/contain/eradicate/recover/lessons); EDR/SIEM; host/network forensics basics; scripting; comms under pressure	Triage incidents; coordinate containment/eradication; acquire evidence; perform root-cause analysis; run tabletop exercises; maintain playbooks & comms templates; lead post-mortems & corrective actions	**Entry (0–2):** Incident Response Analyst, CSIRT Analyst **Intermediate (2–5):** Incident Responder, DFIR Analyst, Malware Analyst **Advanced (5–8):** Senior Incident Responder, IR Team Lead, D&R Engineer **Expert (8–12+):** IR Manager, Head of CSIRT, Director of Incident Response
Cloud Security	Cloud basics (AWS/Azure/GCP); cloud IAM, networking, logging; containers/K8s basics; CSPM/IaC scanning; **nice-to-have:** associate cloud cert	Review cloud designs & guardrails; implement policies (CIS benchmarks); remediate CSPM findings; IAM least-privilege reviews; KMS & secrets mgmt; container image/pipeline security; logging/monitoring enablement	**Entry (0–2):** Cloud Security Analyst, Junior Cloud Security Engineer **Intermediate (2–5):** Cloud Security Engineer, DevSecOps Engineer **Advanced (5–8):** Senior Cloud Security Engineer, Cloud Security Architect **Expert (8–12+):** Principal Cloud Security Engineer, Cloud Security Manager/Head of Cloud Security
Threat Intelligence (CTI)	ATT&CK, kill chain, IOCs/TTPs; OSINT tradecraft; basic malware/TLP; scripting for enrichment; strong writing/briefing	Collect & analyze intel; curate IOCs; integrate feeds with SIEM/EDR; produce strategic/tactical/operational intel reports; brief stakeholders; drive hunts & detection gaps; vendor & info-sharing participation (ISACs)	**Entry (0–2):** Threat Intelligence Analyst (Entry), CTI Researcher **Intermediate (2–5):** CTI Analyst, Threat Researcher, Malware Analyst **Advanced (5–8):** Senior CTI Analyst, Intelligence Lead, Collections Manager **Expert (8–12+):** CTI Manager, Head of Threat Intelligence, Principal Threat Researcher
Purple Teaming & Adversary Emulation	Offensive & defensive basics; ATT&CK mapping; scripting/automation (e.g., emulation frameworks); SIEM/EDR knowledge; measurement/metrics mindset	Plan purple exercises; emulate TTPs; coordinate with blue team; validate controls/detections; document gaps & recommendations; measure detection coverage; report outcomes to execs & engineering	**Entry (0–2):** Associate Purple Team Engineer, Detection Validation Engineer **Intermediate (2–5):** Purple Team Engineer, Adversary Emulation Engineer **Advanced (5–8):** Senior Purple Team Engineer, Detection Engineering Lead **Expert (8–12+):** Purple Team Lead/Manager, Director of Adversary Emulation
Digital Forensics	OS internals & filesystems; artifacts & timelines; memory/disk/mobile acquisition; chain of custody; reporting; **nice-to-have:** lab experience	Evidence acquisition (disk/mem/mobile); timeline & artifact analysis; write reports suitable for legal; tool validation & lab maintenance; support IR & HR/legal cases; testify when required	**Entry (0–2):** Forensics Technician, Junior DFIR Analyst **Intermediate (2–5):** Forensic Analyst, eDiscovery Analyst, Mobile Forensics Analyst **Advanced (5–8):** Senior Forensic Analyst, Forensic Examiner Lead **Expert (8–12+):** Forensics Manager, Principal Forensic Examiner
Security Assessment / Pentest / Red-Teaming	Networking, OS, and web basics; common vulns/exploitation; scripting (Python/PowerShell/Bash); reporting; **nice-to-have certs:** eJPT (entry), OSCP (advanced)	Scope engagements; perform web/network/cloud tests; develop & execute phishing/social-eng ops; document findings & risk; retesting & validation; red-team ops & purple exercises; client briefings	**Entry (0–2):** Associate Penetration Tester, Junior Security Consultant **Intermediate (2–5):** Penetration Tester, Security Consultant, Red Team Operator **Advanced (5–8):** Senior Penetration Tester, Offensive Security Engineer, Red Team Lead **Expert (8–12+):** Principal Consultant, Head of Offensive Security, Red Team Manager