Cybersecurity RoadMap

Techpal Security Team

https://techpal.club/

https://blog.peneter.com/

Entry To Security

- Self study (needs time, Patient, Pasion)
- Academic(Listed below)

- MS in Cyber Security Operations and Leadership
- MS in Cybersecurity Engineering
- MS in Computer Science
- MS in Computer Engineering
- MS in Information Assurance
- MS in Information Technology

Skillset

- IT Skills
- Network Engineering knowledge
- Programming Language
- Solve Problem

Cybersecurity Branches

- Information Security Analysts (day-to-day security operations) → SIEM/SOAR
- Application Security (Software/Web/Database/Cloud/Code/DevOps)
- Mobile OS/Application Security/Cryptocurrency/Blockchain Developer
- Penetration Testing and Security Assessment (Red/Blue/Purple)
- Network and Infrastructure Security (SMB/Enterprise/OT/CIS)
- Digital Forensics and Incident Response (DFIR)
- Security Researchers (Protocol design/assessment) → Academia/Big Techs R&D (limited)

Information Security Analyst & Security Compliance Analyst

Information security analysts have the responsibility of creating plans and strategies for preventing cyber attacks. They are essentially the protectors of sensitive information, and they ensure that policies are being followed. Their main jobs include monitoring systems and networks, detecting threats, analyzing and assessing issues, and generally protecting IT infrastructure from criminal activity. Once they have found a threat, they will determine whether to resolve or escalate it, based on the defined security policies/protocols. Since the role of an information security analyst is technical, they generally have a bachelor's degree in a subject such as computer science or programming. Popular Terms: VPN, IDS/IPS/IDP, SIEM, SOAR, CASB, EDR, NAC, Sandbox, ZTNA, GRC, CIS, GDPR, ISO-27001, Risk Assessment, Threat Intelligence.

Security Software Developer & Application/Cloud/DevSecOps Engineer

If you're a big fan of coding and love the idea of creating software, this job will suit you. It combines the technical knowledge of writing and developing software with an interest in security. To succeed in this role, you'll need to understand software in and out, from its design, testing and implementation. You'll be able to make changes to existing programs, carry out upgrades and integrate security protocols into old applications. It's important that you can work well in a team, as you will often be developing software collaboratively and working with IT colleagues. If you're interested in becoming a software developer, you can try Software Development with Python and Java, aimed at beginners to programming and development, where you will gain an understanding of multiple coding languages.

Security of Mobile Applications and Blockchain Developer

Blockchain developers create and develop innovative systems as a response to challenges such as hacking. It is their job to ensure the security of digital transactions by recording and storing blockchain data using secure methods such as cryptography. They often operate on multiple systems and know several different programming languages, as blockchain technology and smart contracts can be very complex. Some important skills that blockchain developers need include blockchain architecture, knowledge of data structures, web development, smart contract development and cryptography. Reader's Digest named blockchain developer as one of the most in-demand jobs for 2021.

Pen Tester (Red/Blue/Purple Teaming)

If you're interested in learning more about cyber criminals and how they work, you might want to become an ethical hacker or pen-tester. It is their job to carry out advanced penetration tests on a company's system and check if there are any weaknesses or breaches in their security. By stepping into the mind of a cyber criminal, ethical hackers assess the security of computer systems and fix any problems that they find so that real hackers can't penetrate the system. They create preventative measures to stop hackers before they've even begun. Certified ethical hackers or pen testers don't need a degree, but they usually have some form of certification. (CEH/OSCP/LPT)

Network Security (SOC) Engineer

As you can see from their job titles, network security engineers are responsible for dealing with computer networks. They are technical experts, and it is their job to set up networks, look after them and offer technical support to users of the network. There are both hands-on and computer-based aspects to this role. Network engineers can perform installations and maintenance tasks on aspects of network components such as routers, switches and firewalls, but they also look after software by monitoring network activity, configuring systems, and troubleshooting problems.

Cyber Security Architect/Project Manager (Professional Services)

As the job title reveals, security architects are responsible for creating and designing security for a system. They also develop architecture patterns and new security approaches for technologies. If you have an analytical mind, enjoy designing programs and love working with data, this might be the perfect role for you. Security architects may be in charge of designing IT security infrastructure, but they will also be involved in its creation, implementation and management. It’s important that they have great communication skills as they will need to educate staff on security policies, provide specialist advice to teams, recommend approaches to stakeholders and help review the work of others. You’ll need a bachelor’s degree for this job, but it’s worth also keeping in mind that around 30% of employees for this position also request a relevant masters degree.

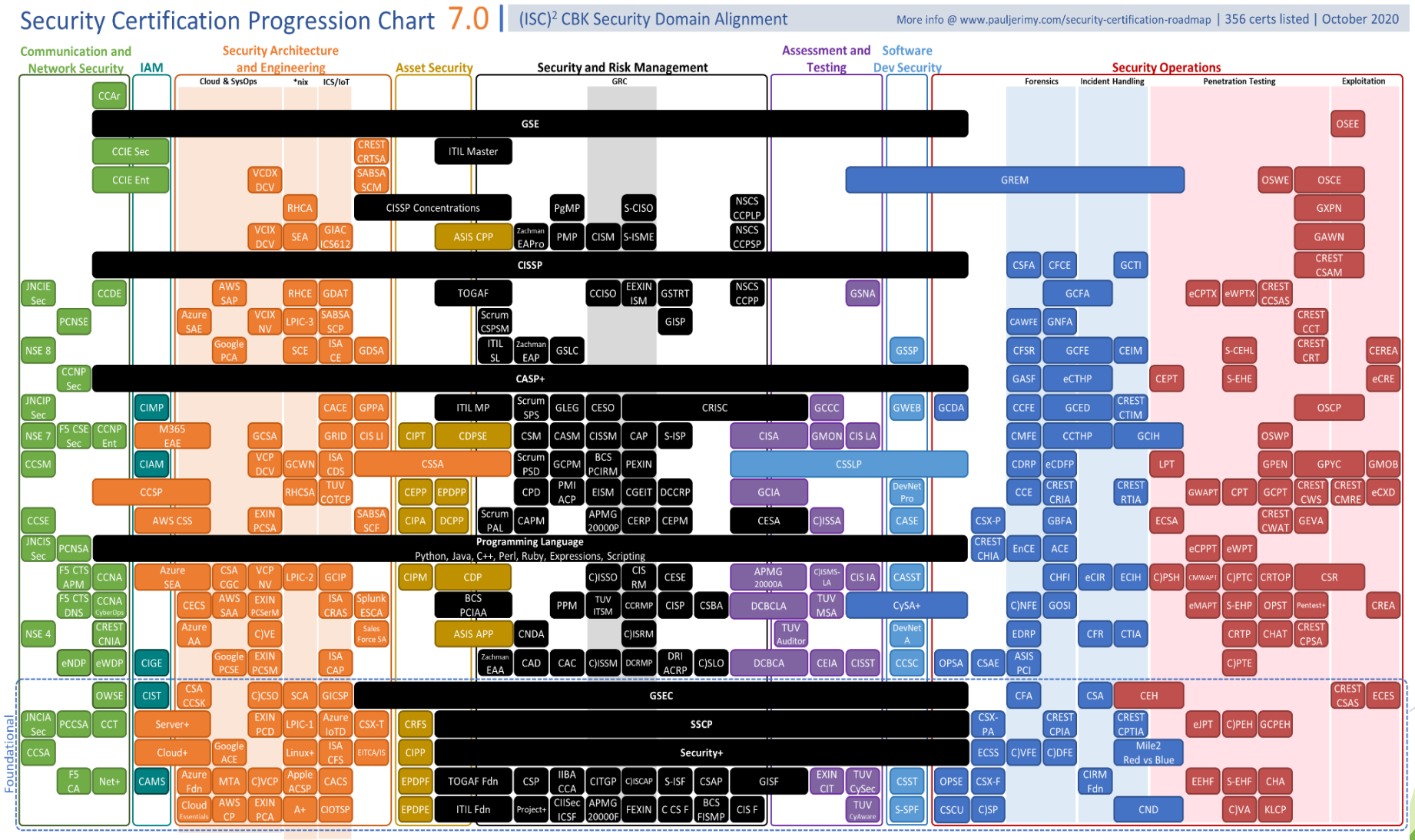
Cyber Security Architect/Project Manager (Professional Services)

Security Architects/Consultants provide business solutions for their organization or clients, and cyber security consultants do the same thing in the cyber security sphere. They assess all security measures, propose improvements and then oversee implementations of new measures. They can either work for one particular company or choose to work independently and help different organizations improve their cyber security measures. They also may get involved with training staff across an organization.

Digital Forensic Analyst

Post-hacking investigation, gathering digital evidence for the court. If you want to be directly involved in investigating cyber criminals, you might consider being a digital forensic analyst. They work closely with the police and other law enforcement agencies to investigate criminal activities and catch cyber criminals. They investigate a wide range of digital crimes from hacking, online scams and theft of sensitive information, to terrorist communications and illegal pornography. Often digital forensic analysts will be investigating data on a range of devices such as computers, tablets, phones and flash drives. If you're interested in this role, you'll need to have knowledge of the latest forensic computing techniques and software, have a great understanding of operating systems, and be comfortable with handling confidential or sensitive information.

Introducing known certifications and companies in the field



Resources

- Cybersecurity News(Twitter, reddit, security news websites[www.thehackernews.com
www.securityweek.com
www.bleepingcomputer.com
https://therecord.media
https://portswigger.net/daily-swig
]
- Read writeup for inspiration(Medium, Github)
- Watch online courses(Coursera, Security-tube, Udemy, YouTube, LinkedIn)
- Free resource, Hacking tools(Github[Awesome Hacking Repositories], hacking forums, Raid forums)
- Read eBooks(Basic RTFM, BTFM, The hacker Playbook2, Blackhat Go, Blackhat python)
- CTF(hackthebox, tryhackme, root-me)
- Good Blogs(OWASP wiki, portswigger free academy, NCCgroup, pentestmonkey, hackingarticle)