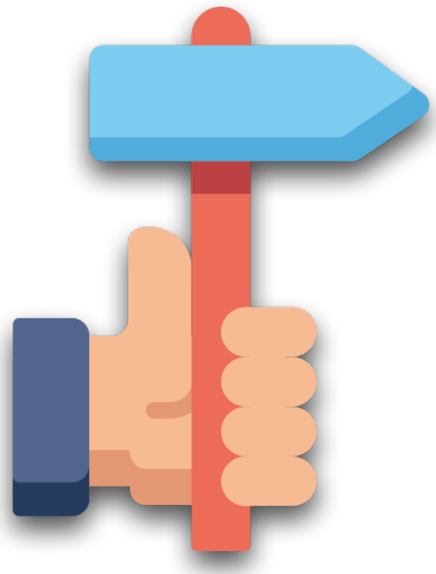
Cybersecurity Roadmap for Beginners



This way please

Sanjeev Jaiswal (Jassi)

Setting up the Context

Sanjeev Jaiswal (Jassi)

- 15+ years of Experience (5 in Dev, 10 in Sec)
- Security Architect, Tesco
  - ➤ Security Head in Lifesight for 2.5 years
  - ➤ India Lead, AppSec Team in Epam
- Application Security and
- Cloud Security (AWS, GCP)
- Programming: Perl, Python
- **Areas of Interest:** Shift Left Security, DevSecOps, Cloud Security & Security Automation

Key Audience

- College Students
- Freshers (0-2 years)
- Want to switch into Cybersecurity
- Interested in Cybersecurity
- Curious what's there in Cybersecurity

What we will cover

- For whom this session is (awareness session)
- What and Why of Cybersecurity
- Common Skill Sets
- Major domains in Cybersecurity
- Job profile categories
- Certifications
- Books
- Online Courses
- What's Next

What is Cybersecurity

Cybersecurity protects computers, networks, and data from unauthorised access, theft, or damage.

It ensures that sensitive information remains private, systems work reliably, and digital services are available when needed.

Cybersecurity is our shield, helping keep our online world safe and secure by defending against cyberattacks such as hacking, viruses, and data breaches.

In short, **Cybersecurity** is the practice of protecting(defensive) critical systems and sensitive information from digital attacks (offensive).

CYBERSECURITY AWARENESS MONTH 2024

663,434
cybersecurity job openings

1,129,659
employed in the cybersecurity workforce

Source: CyberSeek June 2023

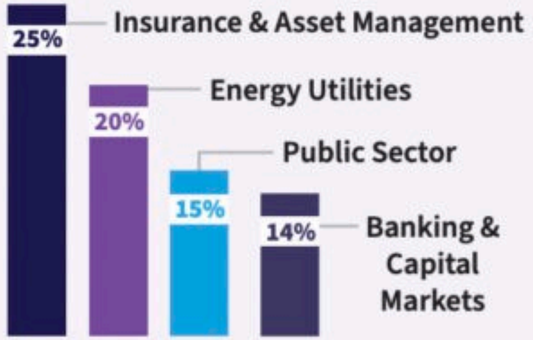
3.4 million
global shortage of cybersecurity professionals

Source: (ISC)2 2022 Cybersecurity Workforce Study

83%
of corporate boards recommend increasing IT security headcount

Source: Fortinet 2023 Cybersecurity Skills Gap

Few business leaders in critical sectors feel confident that they have the talent they need



Source: WEF Global Cybersecurity Outlook 2023

By 2025, **lack of talent or human failure** will be responsible for over half of significant cybersecurity incidents

Source: Gartner Predicts 2023

Every 39 seconds there is a new cyberattack

2,200 new cyberattacks every day

Frequency of ransomware attacks in 2021
Every 11 seconds

Frequency of ransomware attacks in 2031 (Estimated)
Every 2 Seconds

Sources:
https://exploidingtopics.com/blog/cybersecurity-stats
https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide
https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches
https://cybersecurityventures.com/ransomware-report-2021/
https://www.bluefin.com/bluefin-news/biggest-data-breach-es-year-2024/#:~:text=Verizon's%202024%20Data%20Breach%20Investigation,other%20Type%20of%20Extortion%20Technique

NOMADIX

Common Skill Sets

Hacker Mindset

- Attitude to deep dive
- **Never give up**
- Understanding of various security concepts
- Attention to detail
- Adaptive in nature
- Do your homework well
- Don’t hesitate to ask about doubts

Soft Skills

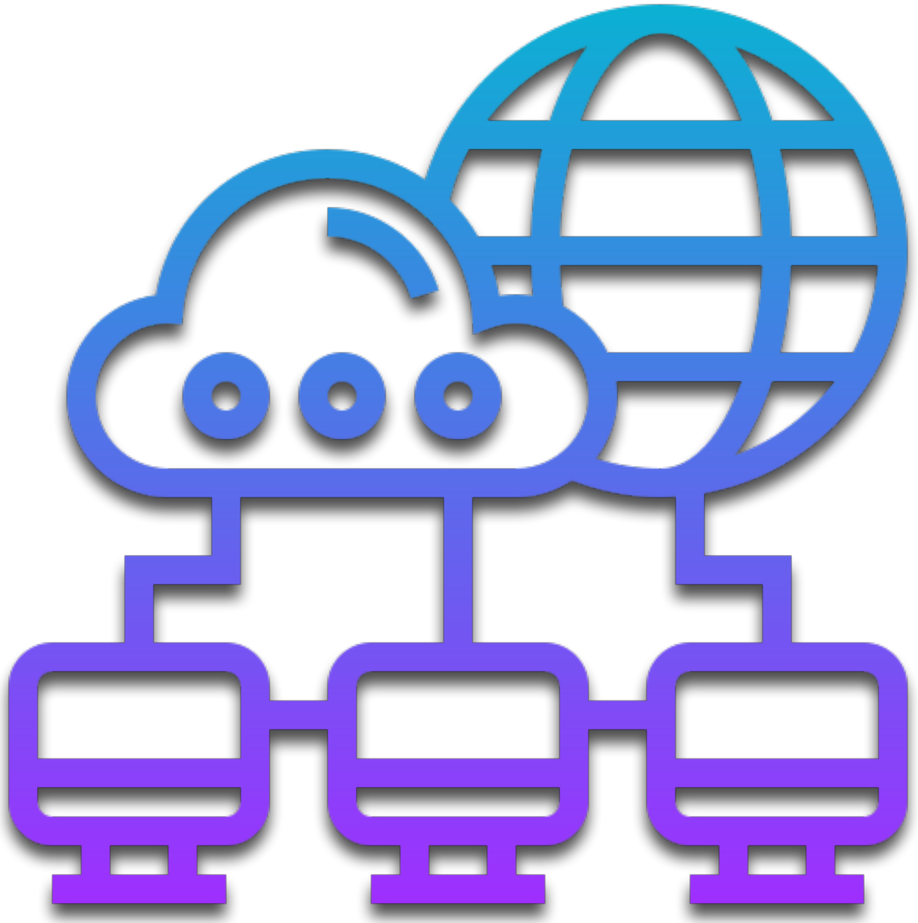
- Email
- Communication Skills
- Negotiation skills
- Public speaking
- Fill with the knowledge not ego

Linux Basics

- Linux OS Basics
- File structure and common places like /usr/bin /tmp /opt
- Linux Commands
  - ls, cp, mv, rm, chmod
  - grep, find, sed, awk
  - whois, curl, wget, openssl, host
- Basic admin commands

Computer Network Basics

- TCP/IP stack
- IPv4 and IPv6
- IP ranges
- Common ports
- SSL/TLS
- LAN/WAN
- Wireless networks
- How browser serves when you type flexmind.co



Programming Basics

- Any scripting language understandings
- Comfortable with command line
- Understand, debug and run
- Python or Go will give you wings to fly
- Understanding JavaScript is important for Pentest

Version Control (git)

- Save all your work at one place
- Easy to collaborate with others
- Keep track of your code, docs…
- Backup and lot more
- github, gitlab, bitbucket
- git pull, push, add, commit, fetch, clone …

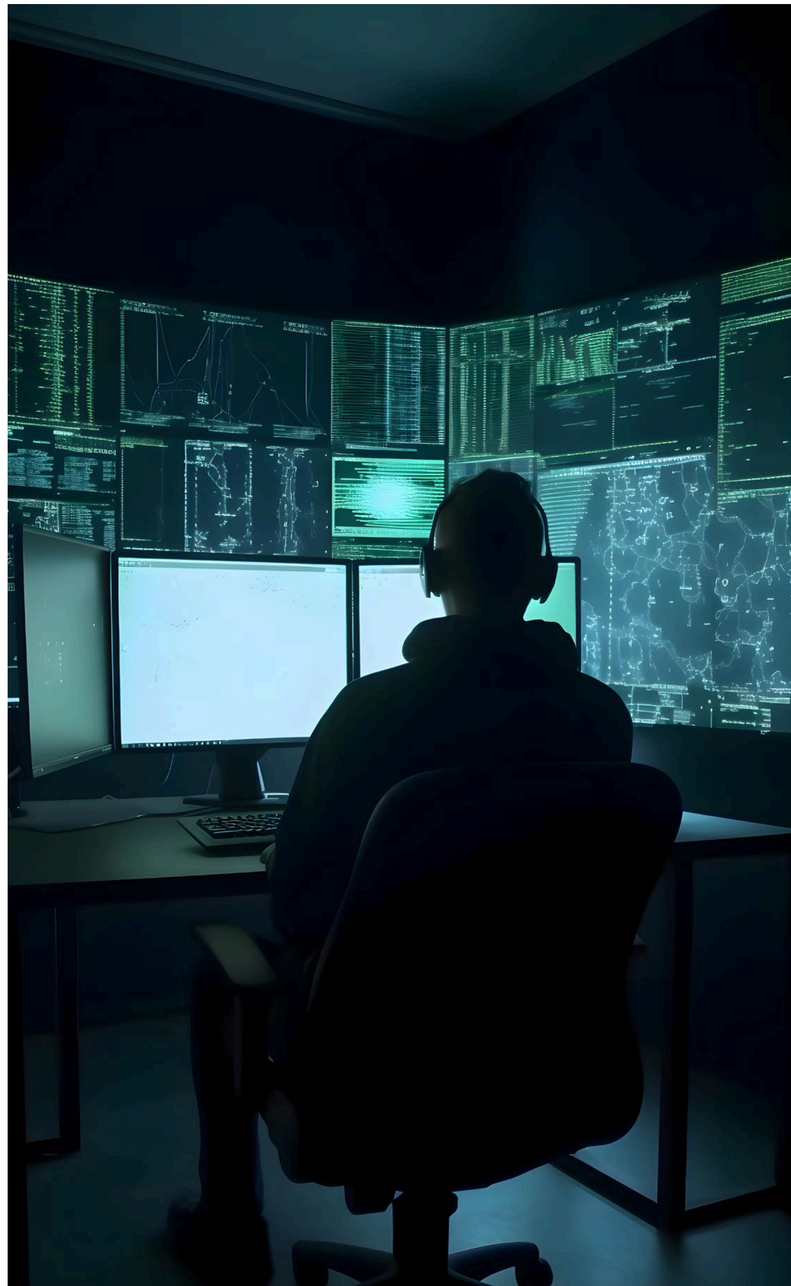
Major Cybersecurity Domains

Web Security/ Pentesting

- Understand how different web services work
- Understand request and response (security) headers
- Understand authentication and authorization
- Cookies, tokens, HSTS, httpOnly
- SOP, CORS, CSP
- OWASP Top 10 (Testing Guide, Code review guide)
- Understand various available encoding i.e. base64
- Comfortable with Burpsuite/OWASP Zap

Application Security

- Threat Modeling
- Secure Code design and principles
- Secure Code Review
- Secure-SDL
- Help developers through secure code training
- SAST/DAST/SCA
- API security
- git is your friend



Network Security

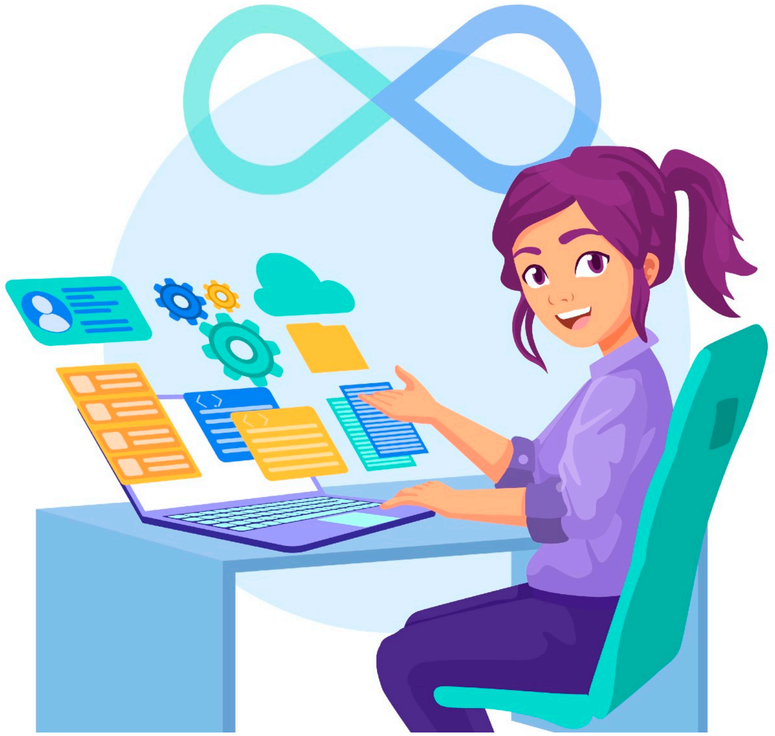
- Secure network architecture
- Firewalls
- Encryption solutions
- Networking commands
- Good with nmap and wireshark tools
- Know IDS/IPS
- DDos prevention
- Aware of CDN implementations

Cloud Security

- Cloud Computing fundamentals
- Security configuration
- Cloud Networking
- Serverless Architecture
- Secure API management
- Data Security
- Encryption at rest, in transit
- Logging and Monitoring

DevSecOps

- Think everything as a Code (Ansible, Terraform)
- You understand DevOps culture
- People, Process and Technology
- Embrace Security Automation
- Comfortable with VCS i.e. git
- Understand CI/CD well
- Well-versed with CI tools i.e. cirlceCI, Travis, Gitlab CI
- Know programming (Python, Ruby, Go)



SOC

- Alert and detect (IDS/IPS)
- IR (Incident Response)
- Proficiency with SIEM Tools (ArcSight, QRadar, Splunk…)
- Threat Intelligence
- Network security and EDR solutions
- Skills required for automation like Python, shell
- Malware Analysis
- Cross-functional working skills

Endpoint Security

- AV solutions or EPP (Sophos, McAfee…)
- EDR solutions (CrowdStrike, SentinelOne)
- MDM (Microsoft InTune)
- Encryption technologies, tools like Bitlocker
- bit of DLP
- Patch Management
- Incident Response

GRC

- IT Audit, Cloud Audit, System Audit, Application Audit
- Risk Analysis
- Data Governance
- DPO
- Data Privacy
- Security Policies and Standards
- Excellent soft skills and communication skills

AI Security

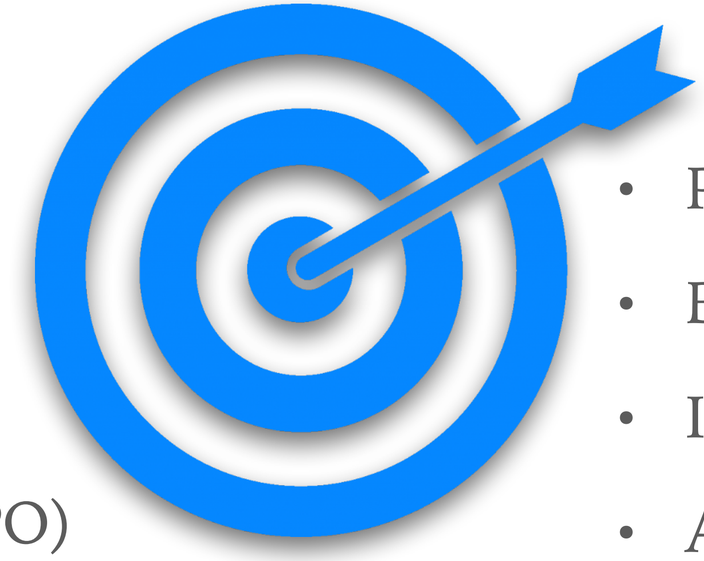
- Security for AI Applications
- AI security policies
- AI Tools knowledge (SIEM systems with AI features)
- Threat Detection/ Anamoly Detection
- Automation: AI helps automate repetitive security tasks, like monitoring and responding to alerts.
- **Security Data Scientist**: Works with AI models to improve threat detection systems.
- **AI Security Engineer**: Builds and maintains AI systems focused on cybersecurity.

Many more

- Bug Bounty
- Red Team/ Blue Team / Purple Team
- Hardware Security
- Container Security
- System Security
- OT/IoT Security/ Industrial Cybersecurity
- Digital Forensics
- Data Privacy
- Mobile Security
- Malware Analyst

Job Profiles & Current Stats

Job Profile Categories

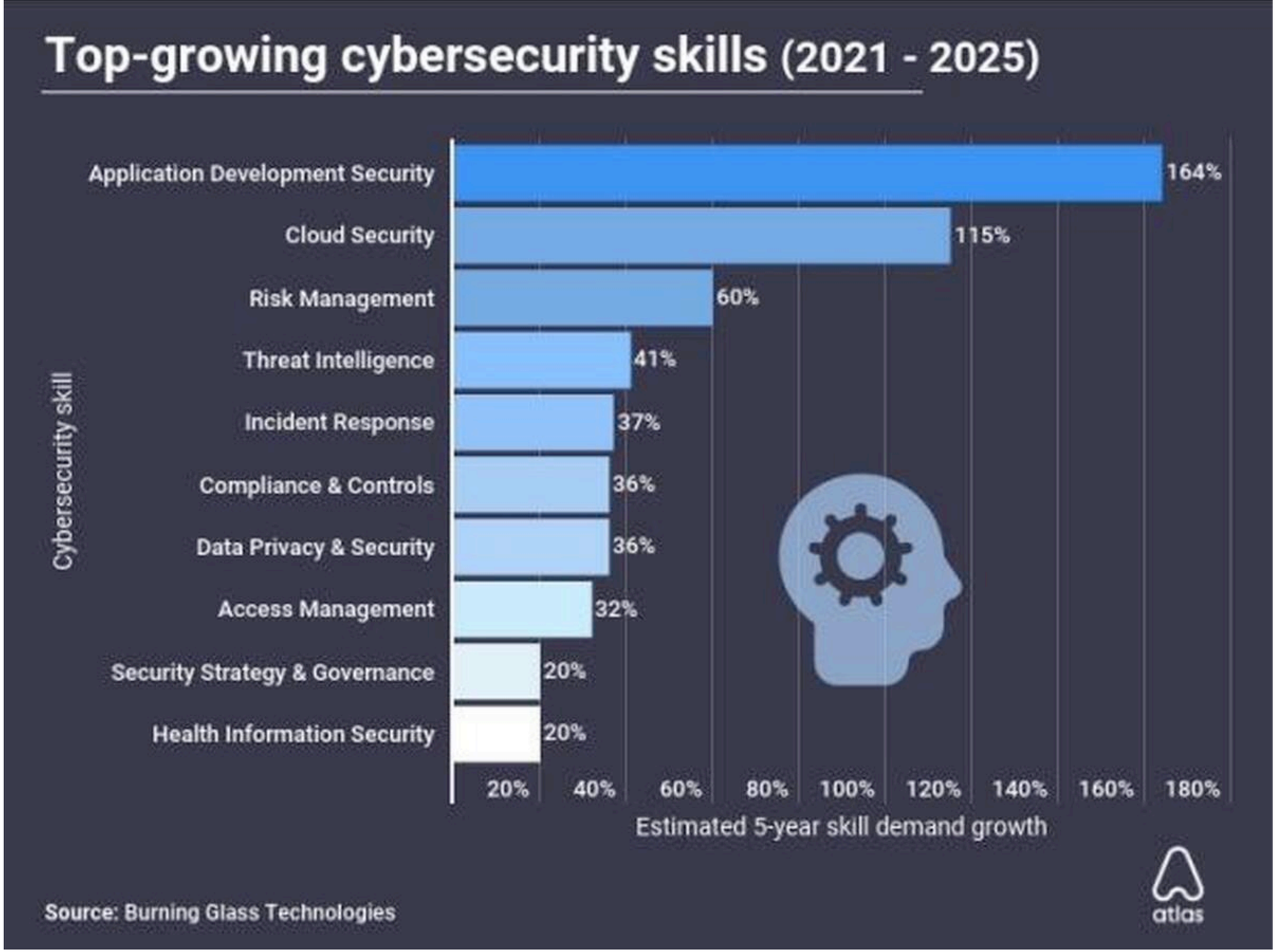


- AI Security Engineer
- Cyber Risk Analyst
- Malware Analyst
- Data Privacy Officer (DPO)
- Compliance Officer/Manager
- Security Program/Project Manager
- TPRM
- Security Architect

What not?

- Penetration Testers
- Bug Bounty Hunters
- Information Security Analyst
- Application Security Engineer
- Cloud Security Engineer
- DevSecOps Engineer
- IAM Architect
- CISO

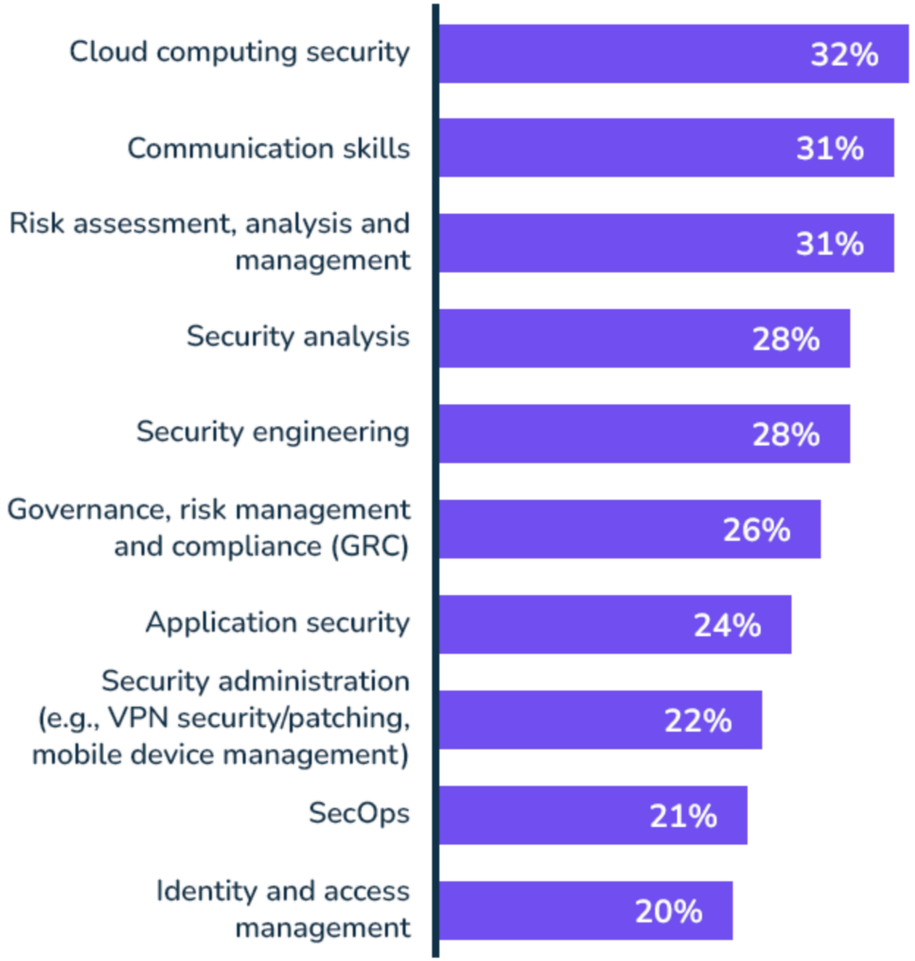
Top-growing cybersecurity skills (2021 - 2025)



Most In-Demand Skills and Specialisms for 2024

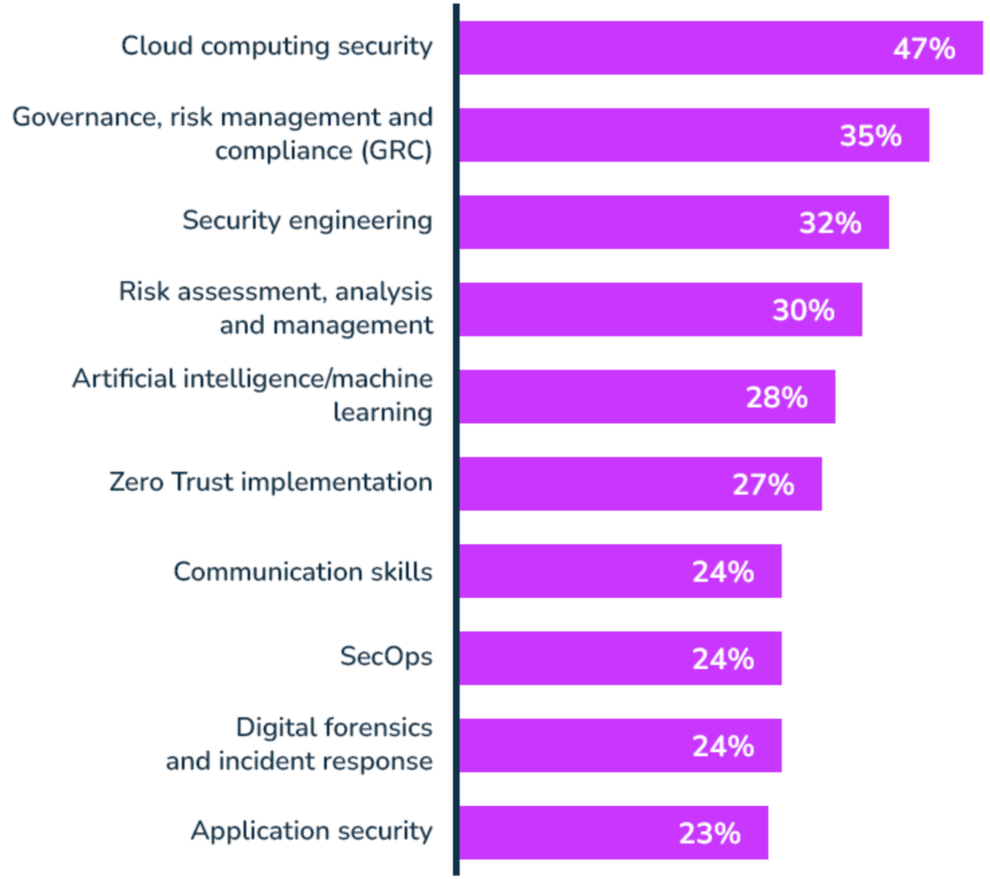
What skills are you most looking for right now when hiring?

ASKED TO HIRING MANAGERS

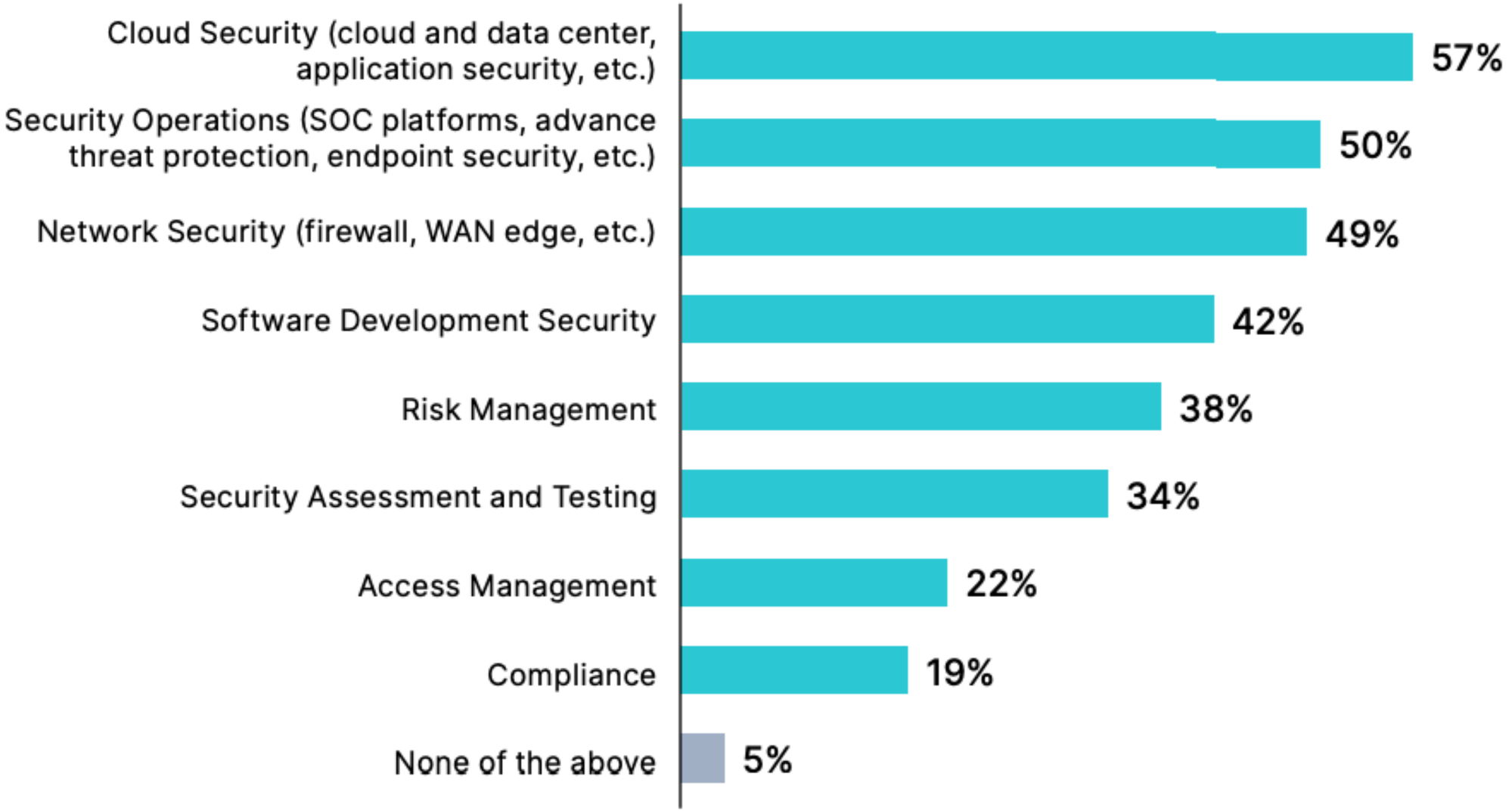


Which of these skills do you think are most in demand for security professionals looking to advance their careers (via new jobs and promotions)?

ASKED TO NON-HIRING MANAGERS



Which are the hardest roles to fill?



Learning Resources

Books

- The Web Application Hackers Handbook
- Hacking: The art of exploitation
- Schneier on Security
- Cybersecurity for Dummies
- Secure By Design
- Security Engineering
- Thinking Security
- Black Hat Python
- Agile Application Security
- API Security in Action


TCP/IP Illustrated, Volume 1
Second Edition
PEARSON
Security Engineering
SECOND EDITION
WILEY
MALWARE, ROOTKITS & BOTNETS A BEGINNER'S GUIDE
COMPUTER FORENSICS INFOSEC PRO GUIDE
NETWORK SECURITY A BEGINNER'S GUIDE THIRD EDITION
WIRELESS NETWORK SECURITY A BEGINNER'S GUIDE
WEB APPLICATION SECURITY A BEGINNER'S GUIDE
threat modeling designing for security
The Mobile Application Hacker's Handbook
The Web Application Hacker's Handbook
Second Edition
The Browser Hacker's Handbook
Cryptography and Network Security
2nd EDITION
Forouzan Mukhopadhyay
Microsoft Azure Security Infrastructure
Microsoft
Security What Every Programmer Needs to Know
Daswani, Kern, Kesavan
apress
CRYPTOGRAPHY ENGINEERING
Modern Authentication with Azure Active Directory for Web Applications
Microsoft
Thinking Security
Bellovin
APPLIED CRYPTOGRAPHY
20TH ANNIVERSARY EDITION
WILEY
CISSP
(ISC) Certified Information Systems Security Professional
CISSP
EXAM GUIDE
CISSP OFFICIAL (ISC) PRACTICE TESTS
Cisco Certified Network Associate
Todd Lammle
CompTIA Security+
CEH Certified Ethical Hacker Practice Exams
CEH Certified Ethical Hacker
Python Penetration Testing Cookbook
Effective DevOps with AWS
Learning Django Web Development
Sanjeev Jaiswal
Ratan Kumar
Industrial Cybersecurity
Pascal Ackerman
Building Serverless Applications with Python
Applied Network Security
Arthur Salmon, Warun Levesque, Michael McLafferty
Cloud Native Python
Manish Sethi
Mastering Data Mining with Python – Find patterns hidden in your data
Python Unlocked
Python for Secret Agents
Arun Tigeraniya
Steven F. Lott
Modern Python Cookbook
Steven F. Lott
Security Automation with Ansible 2
Madhu Akula, Akash Mahajan
Pro Git
Mastering AWS Security
Chacon
Building Microservices
Newman
The Phoenix Project
Gene Kim, Kevin Behr, and George Spafford
DATA AND GOLIATH
BRUCE SCHNEIER
Secrets & Lies
Digital Security in a Networked World
SCHNEIER ON SECURITY
LIARS & OUTLIERS
Gamma | Helm Johnson | Vlissides
Design Patterns
PEARSON
Serverless Architectures on AWS
amazon
AWS Certified Solutions Architect
STUDY GUIDE
Learning Python
Lutz
O'REILLY
Programming Perl
Christiansen, foy & Wall
Intermediate Perl
Learning Perl
Mastering Perl
Perl Best Practices

Certifications

- CompTIA
- EC-council
- ISC2
- CSA
- ISACA
- SANS
- Offensive Security
- Cisco/Checkpoint/Juniper
- Practical-DevSecOps
- Elearn Security

THE MOST DESIRED PROFESSIONAL CERTIFICATIONS FOR CYBER SECURITY JOBS

RANK	PROFESSIONAL CERTIFICATION	OUT OF 843 JOBS LISTINGS ANALYSED PROFESSIONAL CERTIFICATION APPEARED IN...	HOW DESIRED?	AVERAGE PAY SCALE (£)
1	Information Systems Security Professional (CISSP)	279	33%	£58,675
2	Certified Information Security Manager (CISM)	174	21%	£59,689
3	Certified Information Systems Auditor (CISA)	116	14%	£57,936
4	Certified Ethical Hacker (CEH)	41	5%	£46,500
5	Certified Cloud Security Professional (CCSP)	30	4%	£60,000
6	Cisco Certified Network Associate (CCNA) Security	28	3%	£31,738
7	CompTIA Security+	25	3%	£34,153
8	Computer Hacking Forensic Investigator (CHFI)	5	1%	£45,000

Online Courses

- Coursera/Udacity/EdX
- Acloud.guru -> Pluralight
- Cybrary
- OpensecurityTraining
- APISec University
- Portswigger Academy
- YouTube
- **Flexmind**
- AppSecEngineer
- AttackDefense Labs

Lab Practice

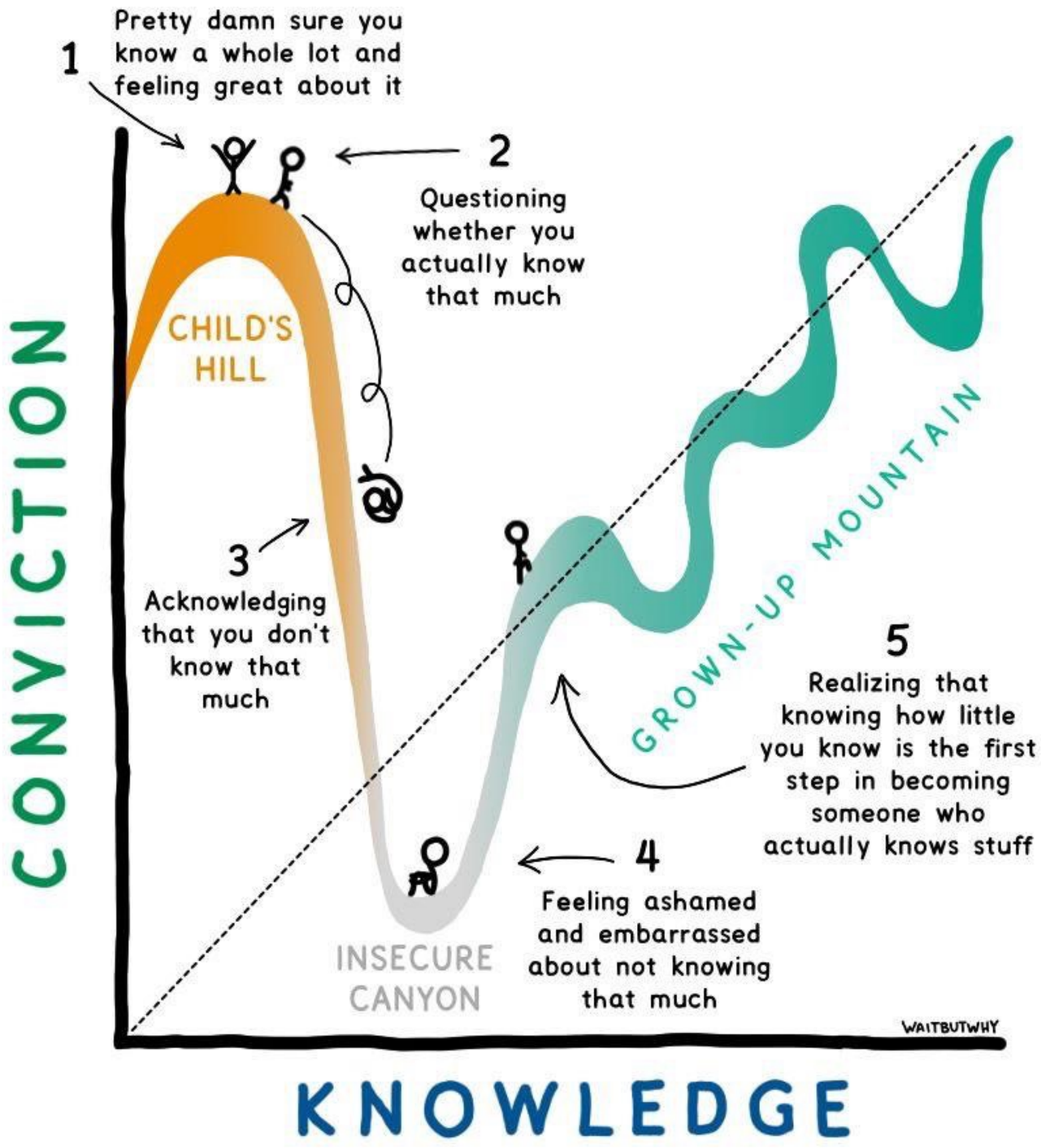
- Set up your machine as you like
- DVWA
- OWASP Juice Shop
- CloudGoat2/GCP Goat/ Kubernetes Goat
- Hack The Box (HTB)
- Try Hack Me
- Hack this site
- Pentester Academy
- Flaws.cloud, Flaws2.cloud

Security Tools

- Kali Linux
- Burp Suite
- nmap
- sqlmap
- nikto, fierce
- arachni
- dirbuster
- dnsenum
- Hydra, John The Ripper
- Metasploit
- Wireshark
- OpenVAS, Nessus
- Shodan
- Maltego
- scapy
- mitmproxy
- kismet
- OWASP ZAP
- Nosqlmap
- wappalyzer

Networking is the key

- Null chapter /OWASP Chapter /Bsides Chapter / ISC2 Chapter
- join mailing list, i.e. null Google Group
- Attend International events i.e. Defcon, Blackhat, Nullcon, OWASP Seasides, Bsides
- jobs.null.co.in for job search
- Meet like-minded people, i.e. local meetups
- LinkedIn contacts, groups
- Follow people on Twitter
- Bookmark a few security websites



Never Give Up

My Social Channels

linkedin.com/in/jassics

github.com/jassics

twitter.com/jassics

youtube.com/jassics

NEWSLETTER

Cybersecurity Learnings

Monthly newsletter for topics covering AppSec, DevSecOps, Cloud Security, Container Security, Secure Code etc.

By **Sanjeev Kumar Jaiswal**
+9k | Security Architecture | Application Security | ...

Published monthly
3,812 subscribers

Sanjeev Jaiswal
jassics · he/him

A Seasoned security professional with 15+ years of experience.
#ApplicationSecurity #CloudSecurity #Python #DevSecOps #ContainerSecurity #Pentest

Edit profile

655 followers · **50** following

jassics / READ

Hi 👋, I am Sanjeev Jaiswal

FOLLOW @JASSICS | SUBSCRIBERS 1.6K

- 🔭 I'm an Application Security professional having 15+ year
- 🌱 I'm currently experimenting with Container Security, IaC
- Something which I was working till 2021: AWS Security and
- 💬 Ask me about *AWS Security, GCP Security, Application S DevSecOps and Career Guidance*
- 📫 You can contact me through: Twitter | Linkedin | Youtube
- ⚡ Fun fact: I like Punjabi songs and Bengali Cuisines 😉

📊 Jassics Git hub stats

Sanjeev Jaiswal's GitHub Stats

Total Stars Earned:	6.6k
Total Commits (2024):	133
Total PRs:	9
Total Issues:	8
Contributed to (last year):	0

B+

SUBSCRIBE FOR:

- Cloud Security
- DevSecOps
- Python
- API Security
- Application Security
- Career Guidance

Sanjeev Jaiswal (Jassi)

@jassics · 270 subscribers · 28 videos

Welcome to my channel. I am a seasoned security professional and am here to share con ...more

linkedin.com/in/jassics and 4 more links

Customise channel | Manage videos | View channel stats