

Cybersecurity Roadmap for Beginners

Sanjeev Jaiswal (jassi)

This way please



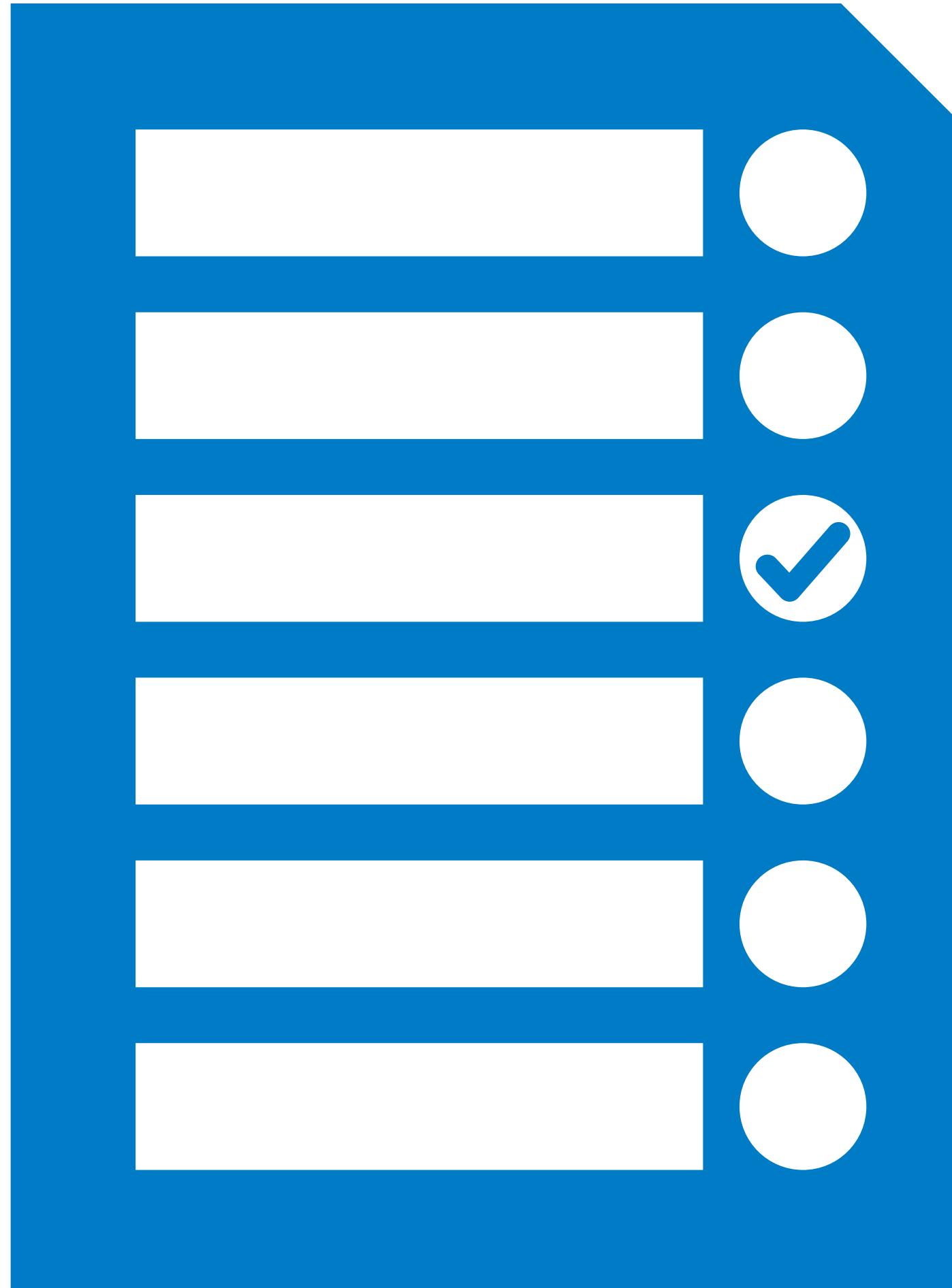
Sanjeev Jaiswal (jassi)

- 12+ years of Experience
- Application Security and
- Cloud Security
- Programming: Perl, Python
- Areas of Interest: Learning and teaching concepts on DevSecOps, Cloud Security Automation



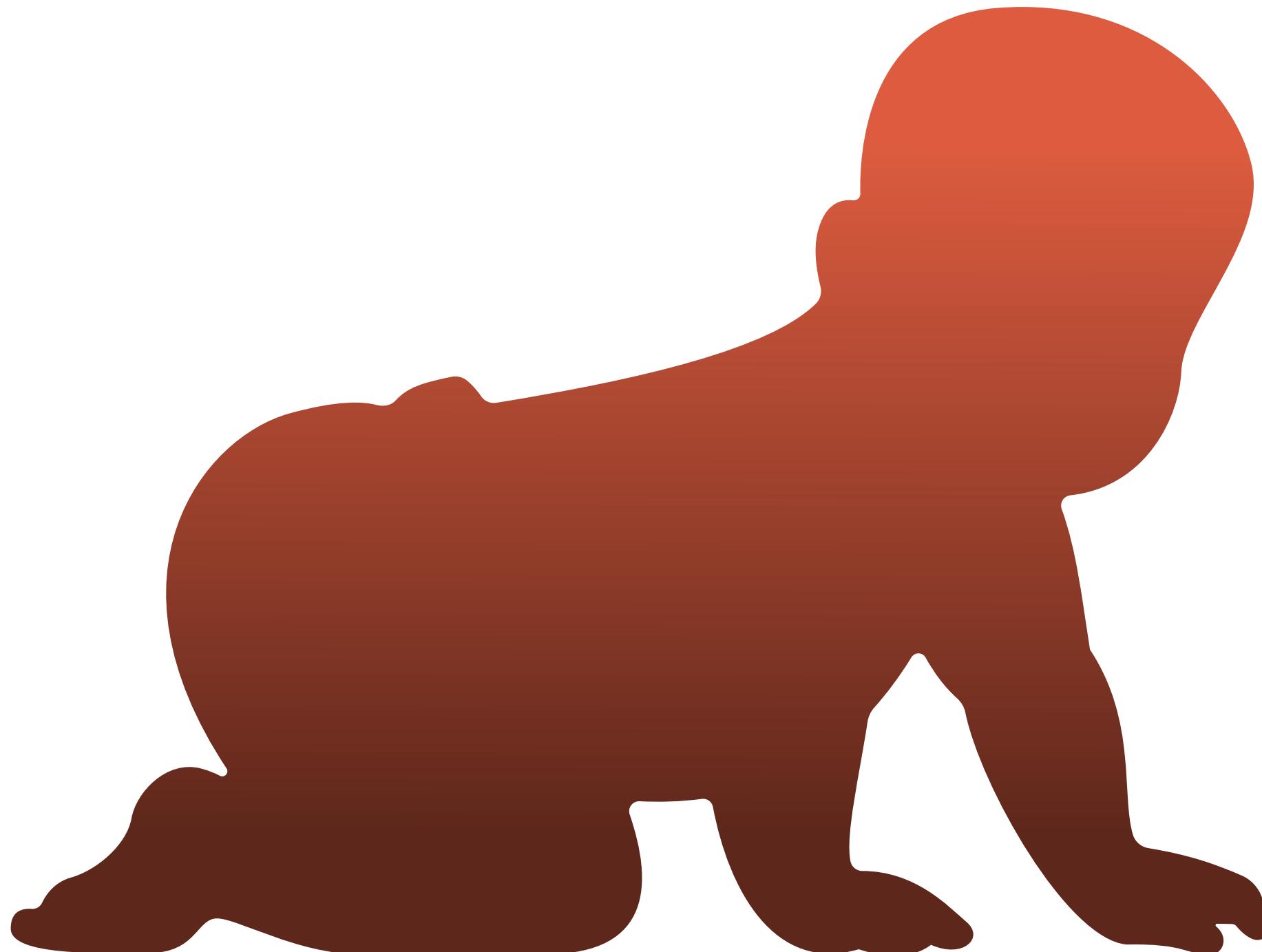
What we will cover

.....



- For whom this session is (awareness session)
- What is Cybersecurity
- Common Skill Sets
- What covers under cybersecurity umbrella
- Job profile categories
- Certifications
- Books
- Online Courses
- What's Next

Key Audience



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

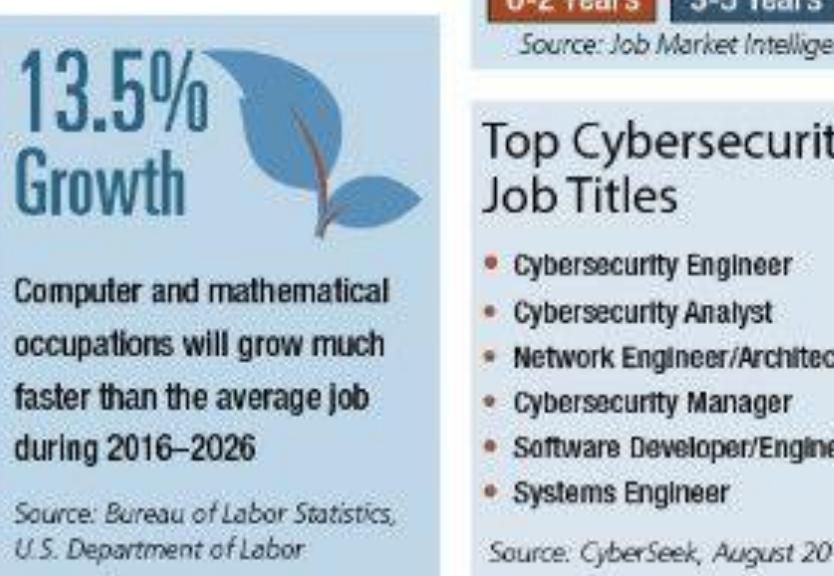
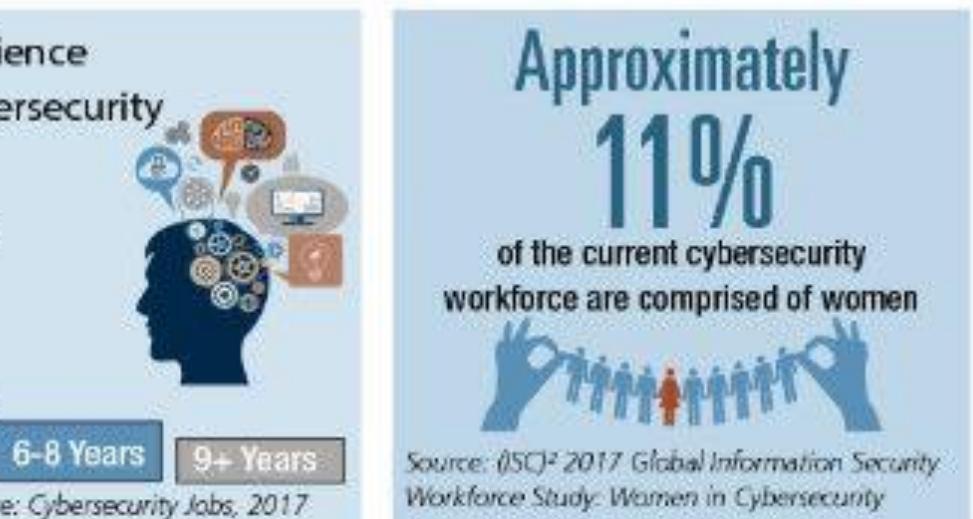
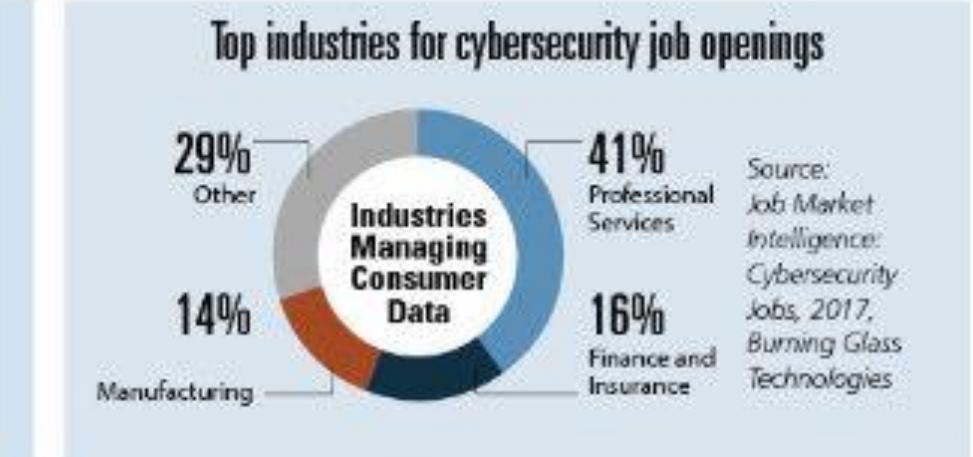
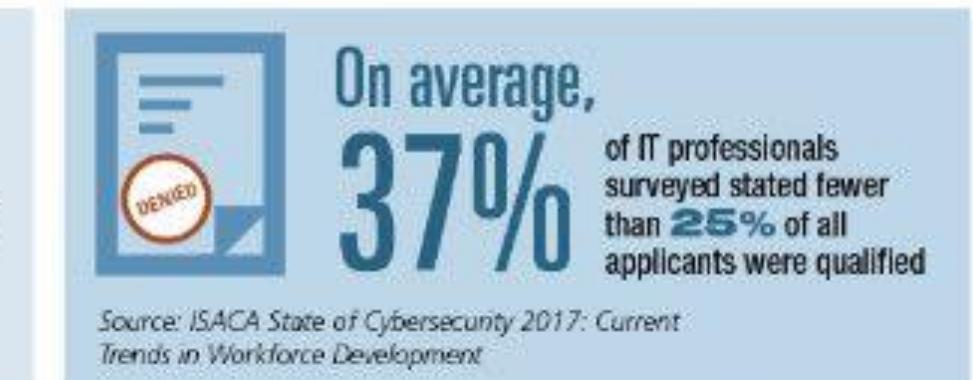
What is Cybersecurity

Computer security, cybersecurity, or information technology security is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

- Wikipedia

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

Cybersecurity Workforce Demand



Common Skill Sets

Hacker Mindset

- Attitude to deep dive
- Never give up
- Understanding of various security concepts
- Attention to detail
- Adaptive in nature



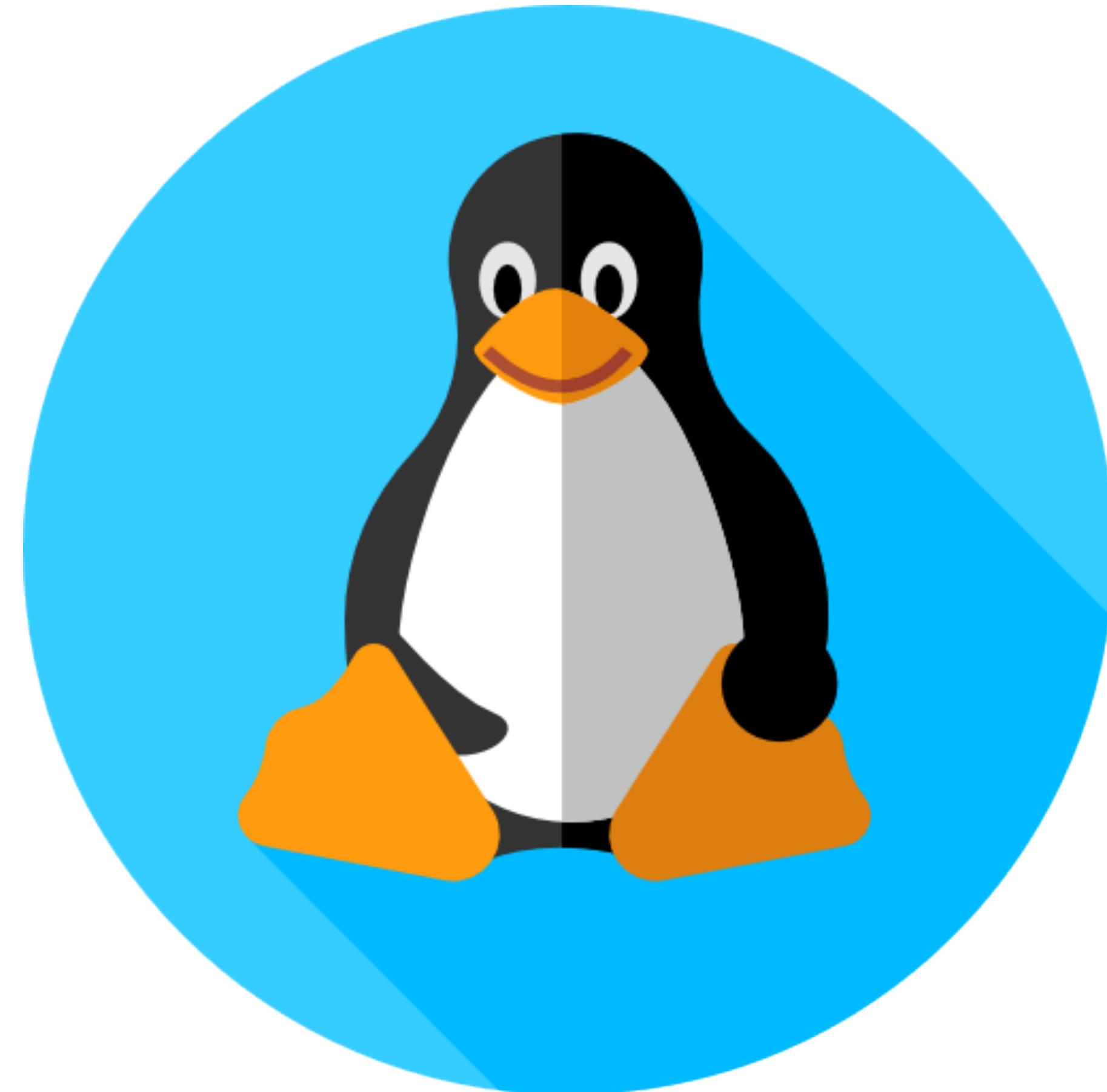
Soft Skills

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



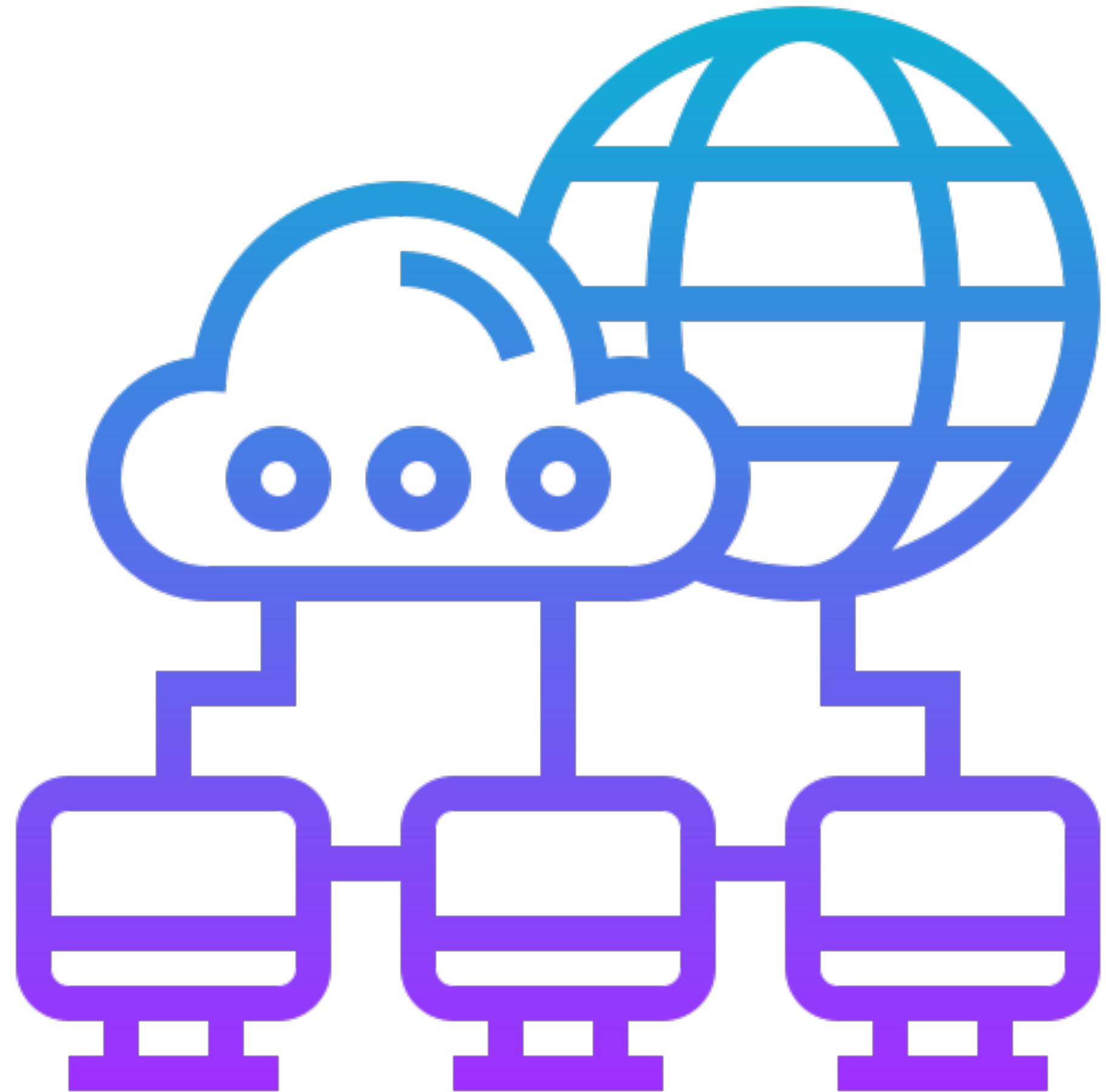
Linux Basics

- Linux OS Basics
- File structure and common places like /usr/bin /tmp /opt
- Linux Commands
- 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



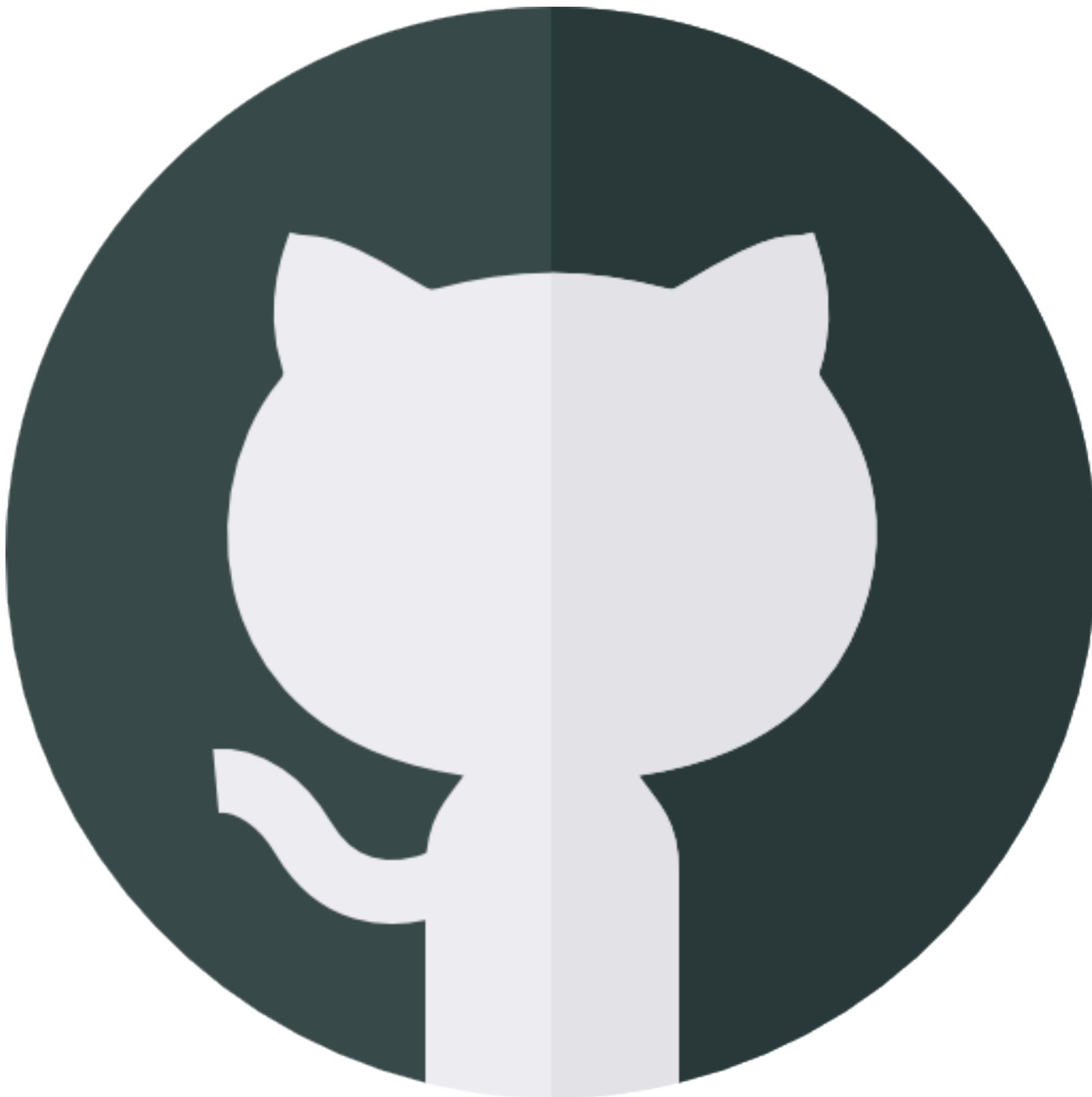
Programming Basics

- 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



Cybersecurity Umbrella

Web Security/ Penetration Testing

- 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
- 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)

Many more

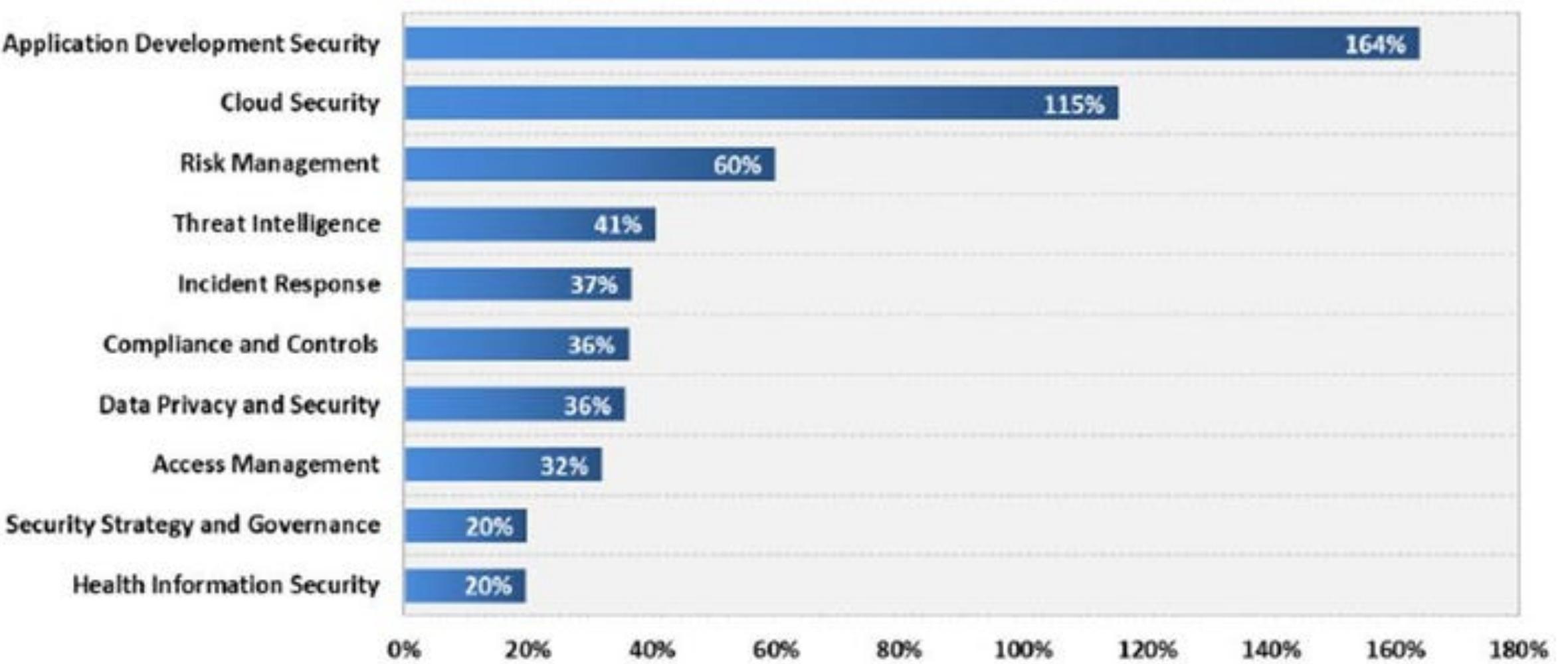
- AI/ML Security
- Hardware Security
- System Security
- IoT Security
- Compliance, Risk and Audit
- Data Privacy

Job Profile Categories



- Penetration Testers
- Bug Bounty Hunters
- Information Security Analyst
- Application Security Engineer
- Cloud Security Engineer
- DevSecOps
- Data Privacy Officer (DPO)
- Risk Analyst
- Malware Analyst
- Security Program Manager
- What not?

Fastest-Growing Cybersecurity Skills
5-Year Projected Growth



Based on the Burning Glass analysis of employer demand in postings, the skills projected to grow fastest in the next five years are:

| Skill | 5-Year Projected Growth | Postings Oct. 2019-Sept. 2020 | Salary Premium |
|----------------------------------|-------------------------|-------------------------------|----------------|
| Application Development Security | 164% | 29,635 | \$12,266 |
| Cloud Security | 115% | 19,477 | \$15,025 |
| Risk Management | 60% | 57,967 | \$13,379 |
| Threat Intelligence | 41% | 60,039 | \$9,609 |
| Incident Response | 37% | 23,497 | \$5,683 |
| Compliance and Controls | 36% | 54,770 | \$12,423 |
| Data Privacy and Security | 36% | 88,527 | \$5,256 |
| Access Management | 32% | 118,096 | \$6,451 |
| Security Strategy and Governance | 20% | 82,952 | \$7,735 |
| Health Information Security | 20% | 413,687 | \$738 |

Books

.....



- * The Cyber Effect
- * Schneier on Security
- * Cybersecurity for Dummies
- * Secure By Design
- * Security Engineering
- * Thinking Security
- * The art of invisibility by Kevin Mitnick
- * Ghost in the wires by Kevin Mitnick



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

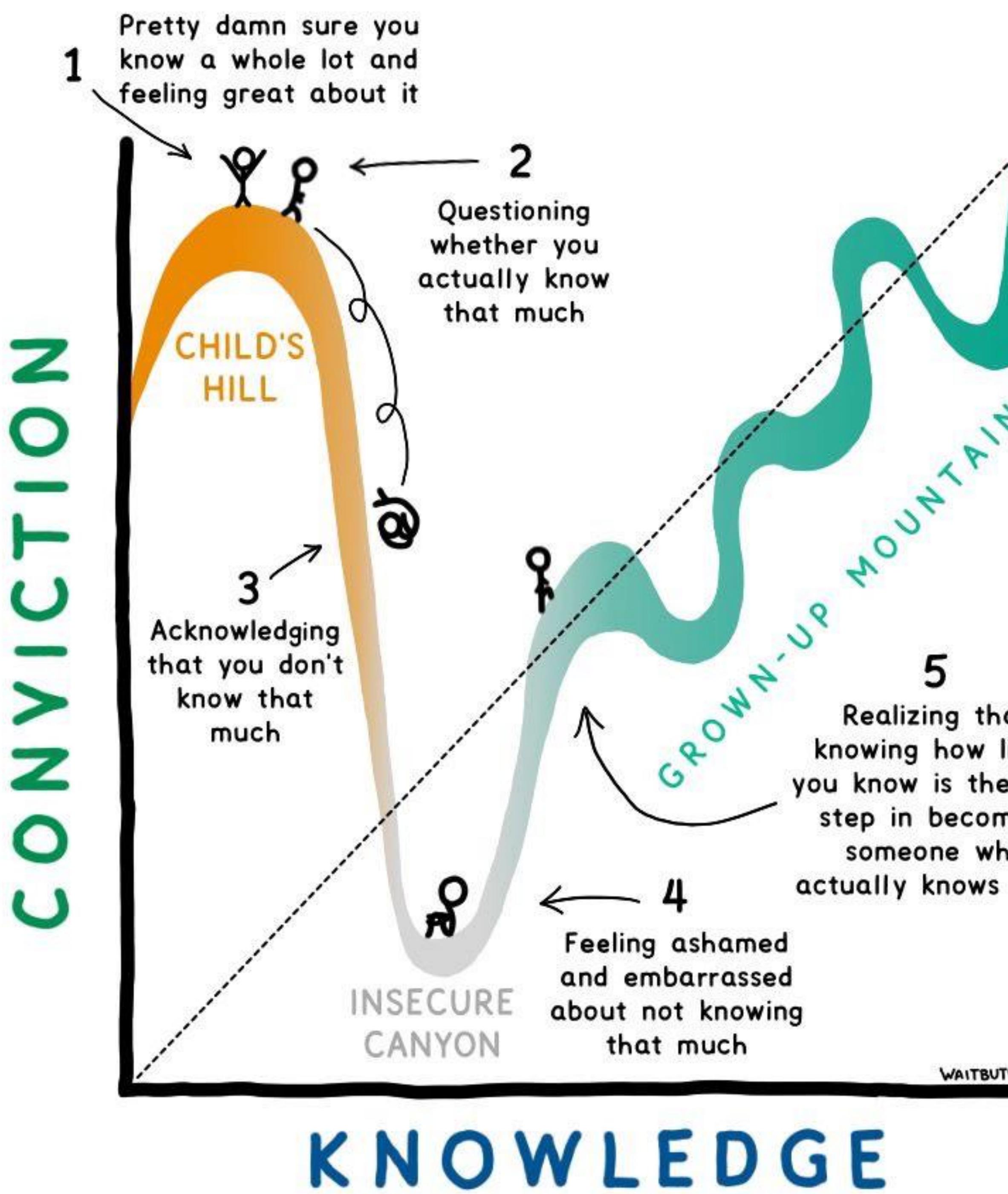


- Coursera
- Udacity
- EdX
- Acloud.guru
- Cybrary
- OpensecurityTraining
- Securitytube
- YouTube
- Flexmind

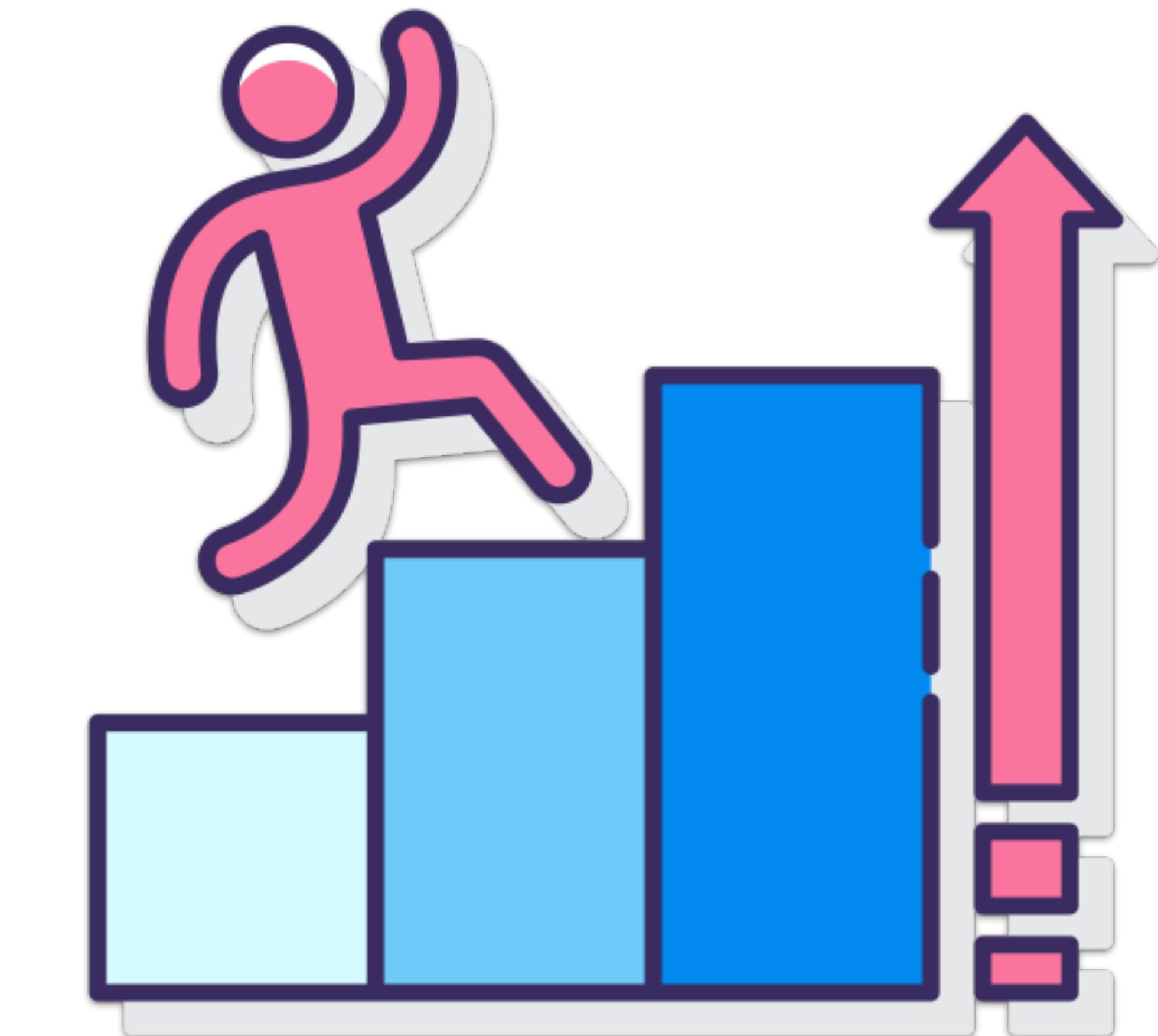
Networking is the key

- Null chapter
- OWASP Chapter
- Bsides Chapter
- join mailing list i.e. null google group
- Attend International events i.e. Defcon, Blackhat, Nullcon, OWASP Seasides
- jobs.null.co.in for job search
- Meet like minded people i.e. local meetup
- Linkedin contacts, groups
- Follow people in twitter
- Bookmark few security websites





Never Give Up



My Social Channels



sanjeevjaiswal.com



github.com/jassics



twitter.com/jassics



linkedin.com/in/jassics

For further queries, please feel free to contact us at learning@flexmind.co

