Gradachiever presents:
Cyber Security Career & Education Workshop

~ Trupti Shiralkar

Agenda

Day 1
- Introduction
- Why Cyber Security is important?
- Overview of Cybersecurity Roles and Responsibilities
- Career Paths

Day 2
- Security Domains
- Education Paths
- Cybersecurity Internships
- Resources for continuous learning

About Me

"Life is either a daring adventure or nothing at all" ~ Helen Keller

WHO?
- Trupti Shiralkar
- India

EXPERTISE
- App Sec
- Secure SDLC
- Applied Crypto
- Privacy Engg

WORK
- Product security leader
- Founder, TrueNil

EDUCATION
- MS in Security Informatics
- Johns Hopkins University

INTERESTS
- Cognitive Psychology
- Hiking
- Meditation
- Travelling
- Painting

Trupti Shiralkar
Security Technologist | AML & Product
Security Leader | Trusted Advisor | Innova...

Introduction to Cyber Security

What is Cyber Security?
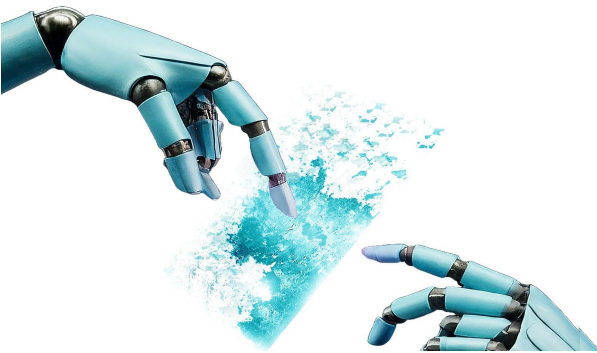
Word of software

Aviation industry

Critical Infrastructure

Cloud computing

Banking Industry

Artificial Intelligence

Data Breaches & Cyber Attacks

57,000 bank accounts

Genetic and ancestry data of 6.9 million users

January 2024 Nation State Attack

560 Million ticketmaster users

80,000 user's data exposed

500 Million+ FB user data leaked in 2021

Poll 1

What is your familiarity in cybersecurity?

1. None
2. Beginner
3. Intermediate
4. Advanced

Why Cyber Security workshop is important

- Career Exploration
- Informed Decision Making
- Early Preparation
- Diverse Opportunities
- High Demand and Job Growth

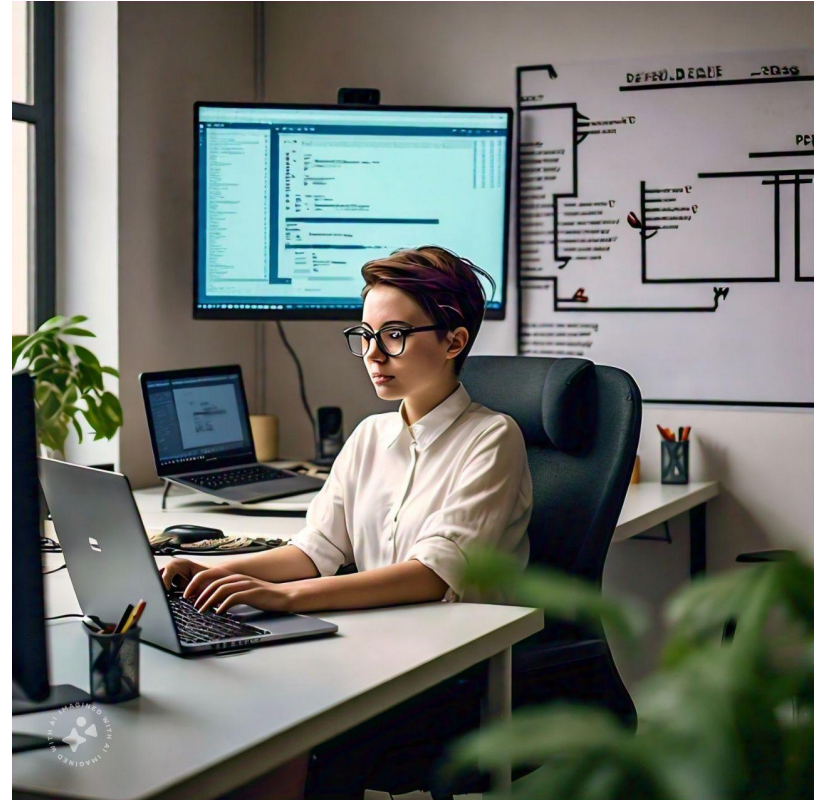Cyber Roles & Responsibilities

Security Analyst

Role & responsibilities

- Monitoring of threats
- Protecting systems and network
- Configure and maintain security solutions
- Participate security trainings and policy developments
- Conduct security Audit & compliance checks

Builder~ Software Security Developer

Role & responsibilities

- General understanding of threats, attacks, & mitigation strategies
- Design & development of security products or features or tools or services
- Secure coding practices
- Computer science background required

Breaker ~Penetration Tester

Role & responsibilities

- Gain unauthorized access
- Steal data
- Denial of Service

Types
- White hat (Ethical hackers)
- Blackhat (criminal) hackers
- Greyhat hackers
- Script Kiddies
- Nation State actors

Poll 2

If given choice what kind of hacker you would like to be?

1. Not decided
2. White hat hacker
3. Black hat hacker
4. Grey hat hacker

Security Architect

Role & responsibilities

- Design security systems
- Technology selection and Integration
- Selection of security frameworks and standards
- Overseeing implementation of layered security

Security Leader

Role & responsibilities

- Hiring of cyber security talent
- Leading projects and cyber initiatives
- Coaching & mentoring
- Organization-wide risk mitigation strategy

Security Researcher

Role & responsibilities

- Vulnerability research
- Exploit development
- Malware Analysis
- Bug bounty

Incident Responder

Role & responsibilities

- Incident investigation & analysis
- Incident communication
- Containment of incident
- Mitigation , recovery
- Reporting

Program manager

Role & responsibilities

- Cybersecurity education and awareness training
- Monthly security events
- Organize hackathon and capture the flag
- Security champion's program

Cryptographer

Role & responsibility

- Cryptographers build encryption algorithms/protocols
- Cryptanalyst break the code
- Background needed: Mathematics + Computer science
- Applied cryptography

World war 2- Enigma machine

Business roles in Cyber Security

Sales Engineer

- 7000+ cyber security vendors
- Sales of security products & services
- Technical & non-technical tracks

Recruiter

- Shortage of skilled cyber workers
- 4 million open positions across globe
  - 400,000 in USA

Product Marketer

- Market Research & competitive analysis
- Content marketing & lead generation
- Product messaging & promotion

Policy Maker

Role & responsibility

- National cybersecurity strategy development
- Crafting Policy Legislation
- Partnership between public & private sector
- Congressional Advocacy
- Public awareness campaigns

Security Executive

Role & responsibility

- Highest ranking officer in security organization
- Responsible for overall company's cyber security strategy
- Similar roles include
  - Data Privacy Officer
  - Chief AI Ethics Officer

Poll 3

What specific area of cybersecurity interests you the most?

- Security Analyst
- Penetration Tester
- Security Architect
- Incident Responder
- Other (non-technical)

Career Paths

Popular Team Structure

Technical Career Ladder

- Security Analyst
- Security Engineer
- Security Architect
- Software Security developer
- Ethical Hacker
- Security Researcher
- Computer Forensics expert
- Cryptographer
- Security Administrator

Photo by CJ Dayrit on Unsplash

Business Career Path in Cyber

- Program manager
- Security Trainer
- Sales Engineer
- Product Marketer
- Policy makers
- Managers
- Chief Security Officer
- Data Privacy Officer

Poll 4

What specific area of cybersecurity career path you would like to follow?

- Offensive Security
- Defensive Security
- Security Education & Training
- Product marketing & sales
- Management/leadership

Summary of Day 1

- Introduction to cyber security
- Why Cyber Security is important?
- Impact of Security Breaches
- Overview of Cybersecurity Roles and Responsibilities
- Career Paths

Welcome to Day 2
Cyber Security Workshop
By
Gradachiever

~ Trupti Shiralkar

Agenda

Day 1
- Introduction
- Why Cyber Security is important?
- Overview of Cybersecurity Roles and Responsibilities
- Career Paths

Day 2
- Security Domains
- Education Paths
- Cybersecurity Internships
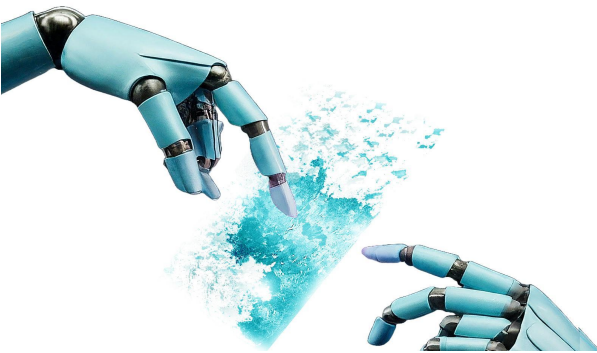- Resources for continuous learning

Recap of Day 1

What is Cyber Security?

Word of software

Aviation industry

Critical Infrastructure

Artificial Intelligence

Cloud computing

Banking Industry

Data Breaches & Cyber Attacks

57,000 bank accounts

Genetic and ancestry data of 6.9 million users

January 2024 Nation State Attack

560 Million ticketmaster users

80,000 user's data exposed

500 Million+ FB user data leaked in 2021

Popular Team Structure

Yellow Team
Software coders and Architects

Orange Team
Facilitates Interaction and Education

Green Team
Enhances security automation with code and design

White Team
Management, Compliance, Analysts, Logistics

Red Team
Offensive Security

Blue Team
Defensive Security

Purple Team
Integrates defensive tactics with offensive results

Cyber Career Paths

- Security Analyst
- Security Engineer
- Security Architect
- Software Security developer
- Ethical Hacker
- Security Researcher
- Computer Forensics expert
- Cryptographer
- Security Administrator

- Program manager
- Security Trainer
- Sales Engineer
- Product Marketer
- Policy makers
- Managers
- Chief Security Officer
- Data Privacy Officer

Security Domains

Network Security

- Focuses on securing network infrastructure (routers, switches, firewalls, etc.)
- Aims to prevent unauthorized access and disruption
- Protects against data breaches and other cyber threats

Cloud Security

- Cloud security is about protecting data, applications, and workloads in public and private clouds
- Enforces security controls and policies through shared mechanisms between customers and providers
- Secures cloud computing environments and infrastructure (servers, storage, services)

Identity & Access management

- Secured Access: Right People, Right Data
- Layered Defenses: Auth, Authz, & Access Control
- Breach prevention

Applied cryptography

- Essential for implementing confidentiality, authentication, and integrity
- Includes secure usage of cryptographic protocols and algorithms
- Involves public key infrastructure (PKI)

Endpoint Security

- Secures end-user devices (laptops, mobile devices)
- Protects against malware and ransomware
- Guards against phishing and other cyber attacks

Data Security

- Utilizes technologies like encryption, access control, DSPM, and DLPs
- Prevents loss of sensitive data (personal, financial, health, business)
- Protects against unauthorized access, theft, and disclosure
- Defends against various security threats

Product Security

- Secures architecture, design, and code from vulnerabilities and threats
- Focuses on security throughout the software development life cycle (SDLC)
- Includes security of CI/CD processes
- Protects software supply chains

Privacy Engineering

- Ensures privacy and data protection as required by regulations and compliance
- Applies throughout the engineering lifecycle
- Involves user consent management
- Manages data access rights

E-discovery & forensics
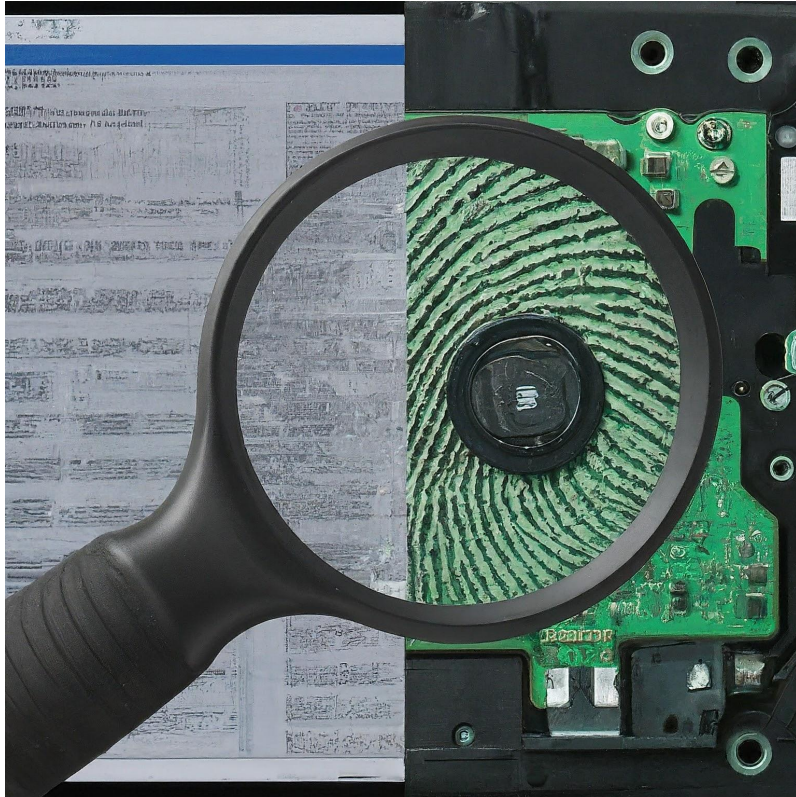
- Investigates security events, incidents, breaches, and attacks
- Collects and analyzes evidence for root cause analysis
- Mitigates or reduces the impact of security breaches
- Uses incident response and digital forensics techniques

Security Operations

- Includes threat intelligence and threat hunting
- Focuses on monitoring and detection
- Manages vulnerabilities
- Utilizes incident response technologies

AI/ML Security

- Secures AI/ML models and their data
- Addresses security, privacy, ethics, and safety
- Applies throughout the MLOps life cycle
- Subdomain of software security

Governance Risk Compliance

- Assessing and managing cybersecurity risks
- Ensuring compliance with regulations and standards
- Implementing frameworks, processes, and standards
- Measuring effectiveness of security controls

Poll 1

What specific domain of cybersecurity you would like to follow?

- Data Security
- Cloud security
- Product Security
- Identity & Access
- Security Operations
- Endpoint Security
- Other

Education Paths

Types of Education

- Bachelor's degree in computer science, networking, information technology, information systems with focus on cyber security:
  - Network security
  - Cryptography
  - Operating systems
  - Computer forensics
  - Security analysis
  - Risk management
- Master's degree in Information Security
- Doctorate in Cryptography, Security & privacy

Other options

- Community colleges
  - Associate degrees in cybersecurity or related fields like information technology with a cybersecurity focus.
  - https://cybersecurityguide.org/ contains searchable database of cybersecurity programs, including associate degrees.
- MOOC
  - Coursera offers 1000+ online courses (JHU, IBM)
 - EdX (Microsoft, MIT, Harvard)
  - Udemy

Certifications

- Security+
- Systems Security Certified Practitioner (SSCP) by (ISC)²
- Certified Information Systems Security Professional (CISSP) by (ISC)²
- Certified Information Systems Auditor (CISA)by ISACA
- Certified Ethical Hacker (CEH) by EC-Council, OSCP
- CompTIA Security+
- GIAC Security Essentials (GSEC) by SANS
- CompTIA Advanced Security Practitioner (CASP+):
- Certified in Risk and Information Systems Control (CRISC) by ISACA
- (ISC)² Certified Authorization Professional (CAP)
- Cloud Security Alliance (CSA)
- Vendor specific security certification(AWS, Google, CISCO)

Security conferences & meet up groups

- 300 + cyber security conferences
- 2 days long hands on training workshops
- Popular conferences (Bsides, OWASP, DefCon)
- Monthly meetup groups
  - OWASP
  - ISC2
  - ISACA
  - Women's cyber security forums
- Slack channels, WhatsApp Groups
- Security open Source projects
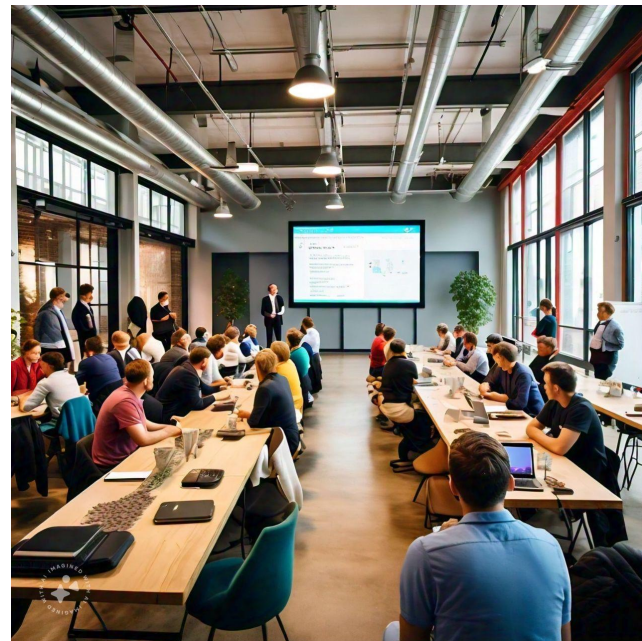
Poll 2

What specific education path cybersecurity you would like to follow?

- Bachelor's degree with specialization in cyber security
- MS/MBA in cyber security
- Online courses
- Associate degree in cyber security by community college
- Certification
- Attending workshops at cyber conference

Cyber Security Internship

Internships

- Most organization's security teams have cyber internships
  - Check their website, network with security professionals
  - Startups
  - Non-profit organizations & universities
- Internships with USA government agencies
  - Department of Homeland Security ([DHS](#))
  - The NSA's Cybersecurity Directorate Summer Intern Program (CSDIP)
  - Defense Intelligence Agency (DIA)
  - Federal Bureau of Investigation (FBI)
  - National Institute of Standards and Technology (NIST)
- (ISC)² and ISACA
- Open source security project contribution to stand out
- Local meetup groups

Cyber Security Job Search

IKIGAI Framework
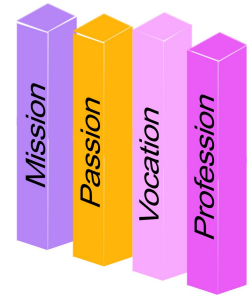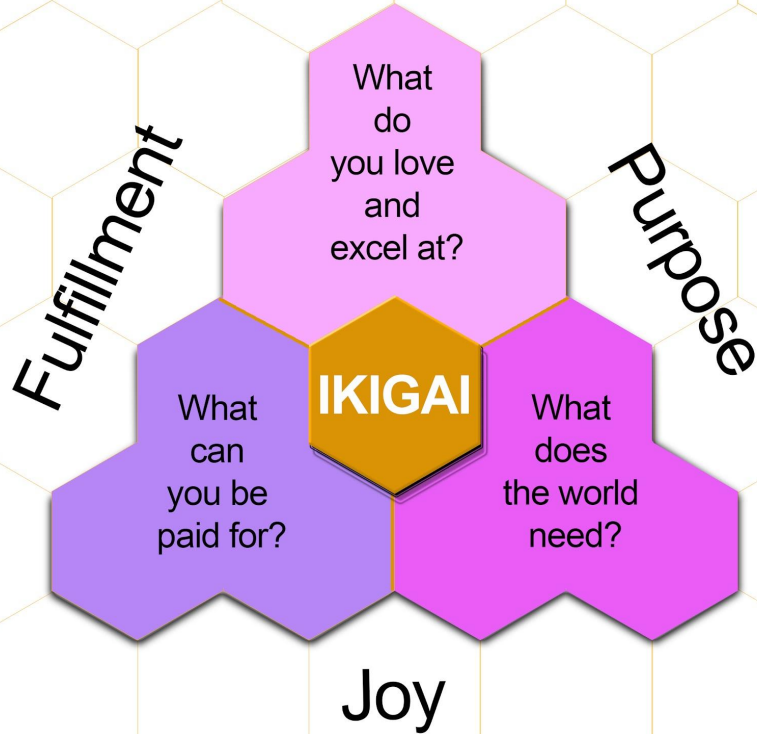
Cyber security job search

- Identify your strengths, interests and career track
- Apply IKIGAI framework to get even more clarity
- Start relentless networking at university, local meetup groups, conferences, company events
- Participate in career fairs and CTF tournaments
- Contribute to open source security projects
- Share your learning through publications & public speaking
- Volunteer
- Every experience counts
- Approach experts and seasoned professionals on Linkedin for mentorship & coaching
- Explore cyber startups
- Join job boards (Linkedin, indeed, CyberSN, Code Red partners)

Poll 3

Where are you in your cyber security journey?

- About to start
- Studying cyber security
- Looking for internships
- Looking for job opportunities

Resources for continuous learning

STANDARD Bodies
- National Institute of Technology (NIST) ~ (https://www.nist.gov/cyberframework)
- MITRE ATT&CK (https://attack.mitre.org/)
- OWASP Foundation (https://owasp.org/)
- Cybersecurity & Infrastructure Security Agency ~ (https://www.cisa.gov/)

Blogs (100+)
- Industry leaders
- Vendors
- Domain specific blogs

Conferences & meetup groups (300+)
- Hands on workshops
- Certifications

Summary of Day 2

- Introduction to cyber security
- Why Cyber Security is important?
- Impact of Security Breaches
- Overview of Cybersecurity Roles and Responsibilities
- Career Paths
- Education Paths
- Cyber security internships
- IKIGAI framework
- Cyber security Job Search

Poll 4

Was this cyber security career workshop useful ?

- Good Overview
- Somewhat useful, could be better
- More detailed information needed
- Very useful

Thank You!

Trupti Shiralkar
Security Technologist | AML & Product
Security Leader | Trusted Advisor | Innova...