So You Want a Career In Cybersecurity?

Cybersecurity Awareness Day

January 26, 2023

Jessica Hoffman, CISSP
JessicaPHoffman@gmail.com

WHAT CAREERS COME TO MIND WHEN YOU THINK OF CYBERSECURITY?

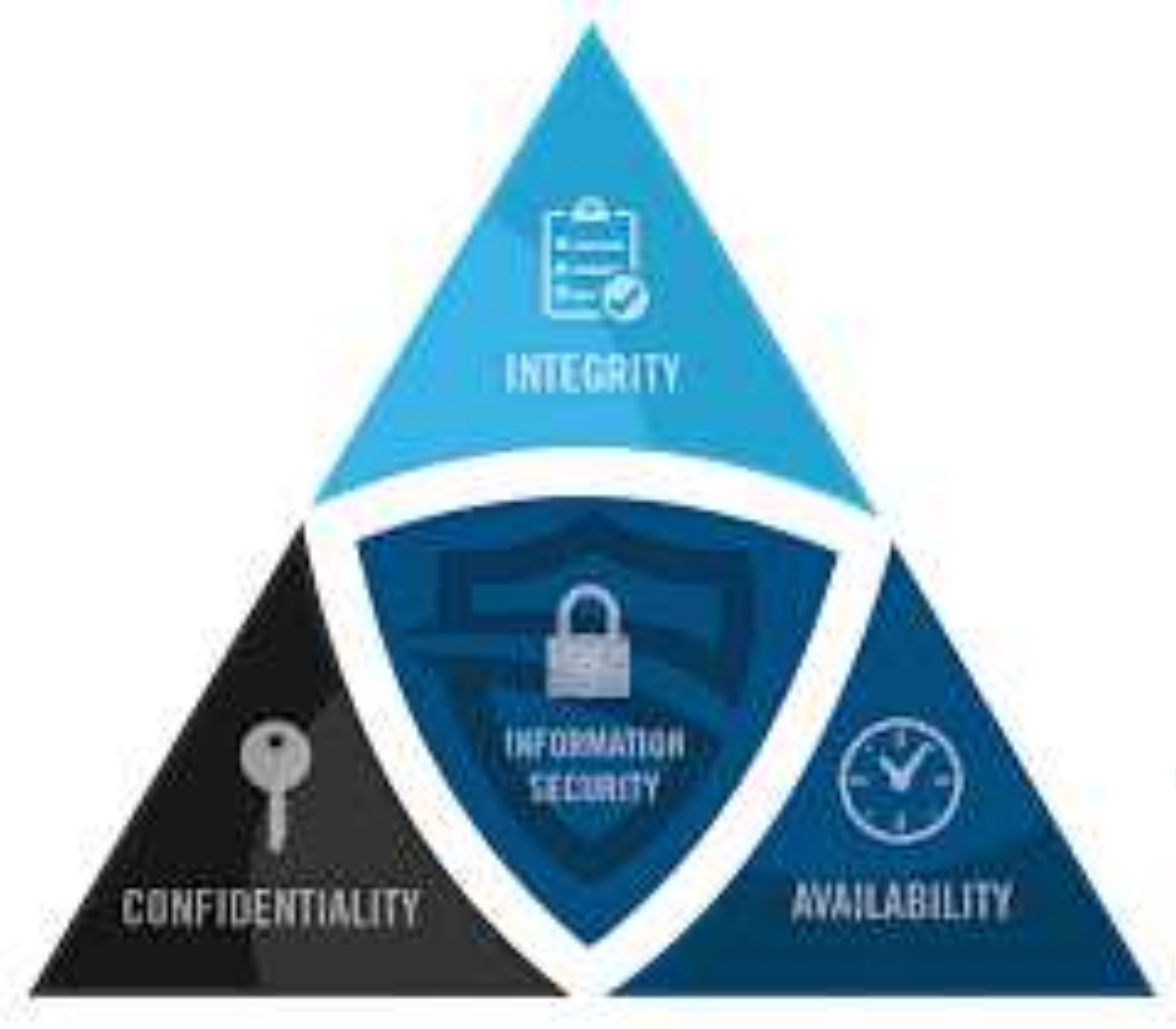
WHAT IS CYBERSECURITY?

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

ITS ALL ABOUT THE DATA!!!

Cybersecurity protects the Confidentiality, Integrity, and Availability (CIA) of data.

WHY DO WE NEED CYBER PROFESSIONALS?



1.Confidentiality – Keeping sensitive information private. Encryption services can protect your data at rest or in transit and prevent unauthorized access to protected data.

2.Integrity – is the consistency of data, networks, and systems. This includes mitigation and proactive measures to restrict unapproved changes, while also having the ability to recover data that has been lost or compromised.

3.Availability – refers to authorized users that can freely access the systems, networks, and data needed to perform their daily tasks. Resolving hardware and software conflicts, along with regular maintenance is crucial to keep systems up and available.

YOU ARE A CYBERSECURITY PROFESSIONAL AT…???

YOU’RE AN APPLICATION SECURITY DEVELOPER FOR TIK TOK…

Tik Tok, as web application, should be programmed, or coded, with security in mind. The following activities are related to application security:

- Restrict Text Input (i.e. text boxes) and Uploads
- Application Session and data encryption
- Data at rest encryption (i.e. user activities, login credentials)
- Audit logs (i.e. code changes, user activities and account information)
- Documentation and Training
- Access Control for Developers and Users: Separation of duties, Least Privilege, Multi-Factor Authentication (MFA)

YOU’RE A PENETRATION TESTER FOR TIK TOK….

The Tik Tok web application and supporting network infrastructure should undergo penetration testing (technical) both internally and externally. The following activities are related to penetration testing:

- Simulate the bad actor, or adversary
- Access Control: Unauthorized Access, Privilege Escalation
- Password Cracking
- Social engineering
- Identify and exploit known weakness (i.e. weak encryption, outdated SW/HW, weak configurations, open network ports

YOU’RE ON THE RISK & COMPLIANCE TEAM AT TIK TOK…

What is risk?

Tik Tok as a program (application & infrastructure) should be accessed for risk to the program and the company. The following activities are related to risk and compliance:

- Identify and Review the Legal Compliance Requirements
- Review Penetration Testing Results
- Review security documentation
- Examine Evidence (i.e. server configurations, audit logs, source code, inventory lists)
- Account management (i.e. privilege vs non-privilege)
- Review Firewall Rules: determines the traffic that flows in the application and infrastructure
- Supply Chain Management Review

YOU'RE ON THE SECURITY OPERATIONS CENTER TEAM AT TIK TOK…

Tik Tok, as a program, should be monitored by Security Operations Center (SOC) analysts, for the following:

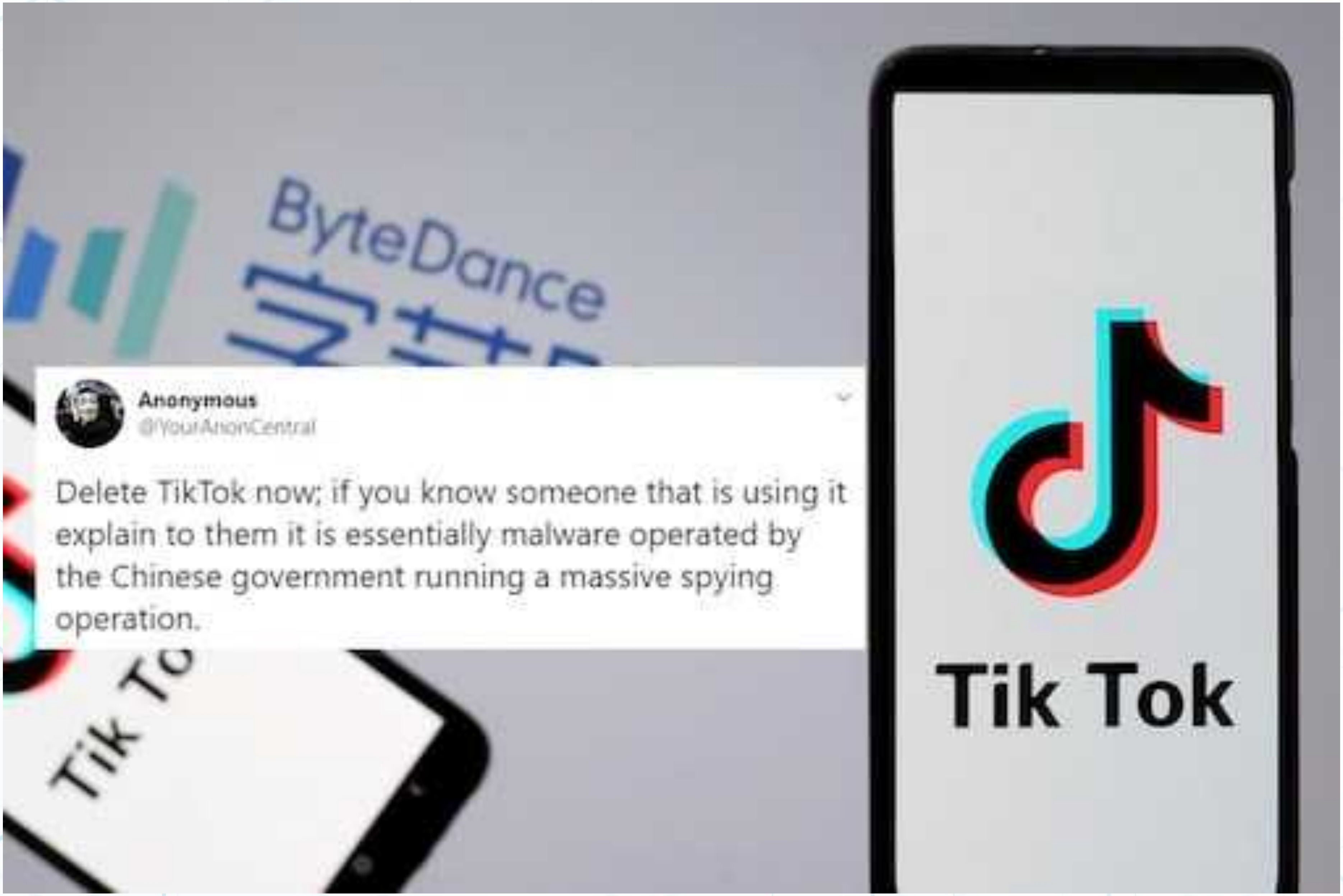
- Identify and monitor for deep fake, inappropriate, unauthorized content (may be a separate group)
- Scan servers for vulnerabilities (i.e. viruses, malware, weak encryption, security misconfigurations)
- Scan network for abnormal, or unusual traffic (i.e. increase in traffic, activity during "off" hours, access attempts from nation states)
- Identify and/or handle incident response
- Identify outdated patches and software/hardware
- Monitor application/network access and activities
- Threat hunting and intelligence

YOU’RE ON THE PHYSICAL SECURITY TEAM AT TIK TOK…

Physically, the Tik Tok program must be protected from unauthorized physical access. The company has many locations where the application and supporting infrastructure (i.e. servers, databases, network devices) are housed; as well as corporate offices for employees (i.e. laptops, hard copies, printers, VoIP). The following activities are related to physical security:

- Employee badges and readers
- Metal detectors and screening machines
- Guards, dogs, censors
- Visitor sponsorship, sign in, and/or escort
- Cable locks on workstations
- Closed caption TV (CCTV)
- Fences, bollards, spikes in roadways
- No windows
- Back up Power generators
- Water sprinklers, fire extinguishers, heating/cooling
- Biometrics (i.e. retina scanning, fingerprints)
- Disguised buildings and discrete entrances

DID YOU KNOW…..?



Anonymous
@YourAnonCentral

Delete TikTok now; if you know someone that is using it explain to them it is essentially malware operated by the Chinese government running a massive spying operation.

SOME CERTIFICATION REQUIREMENTS

ISC2 CERTIFIED INFORMATION SYSTEM SECURITY PROFESSIONAL (CISSP)

Industry standard certification especially for any of the following positions: management/executive leadership, ISSO/SSO, consultant. Years of experience required.

ISC2 Certified Cloud Security Professional (CCSP), Certified Secure Software Lifecycle Professional (CSSLP), Healthcare Information Security and Privacy Practitioner (HCISPP), System Security Certified Practitioner (SSCP), Certified Authorization Professional (CAP)

ISACA CERTIFIED INFORMATION SYSTEMS MANAGER, ISACA CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA)

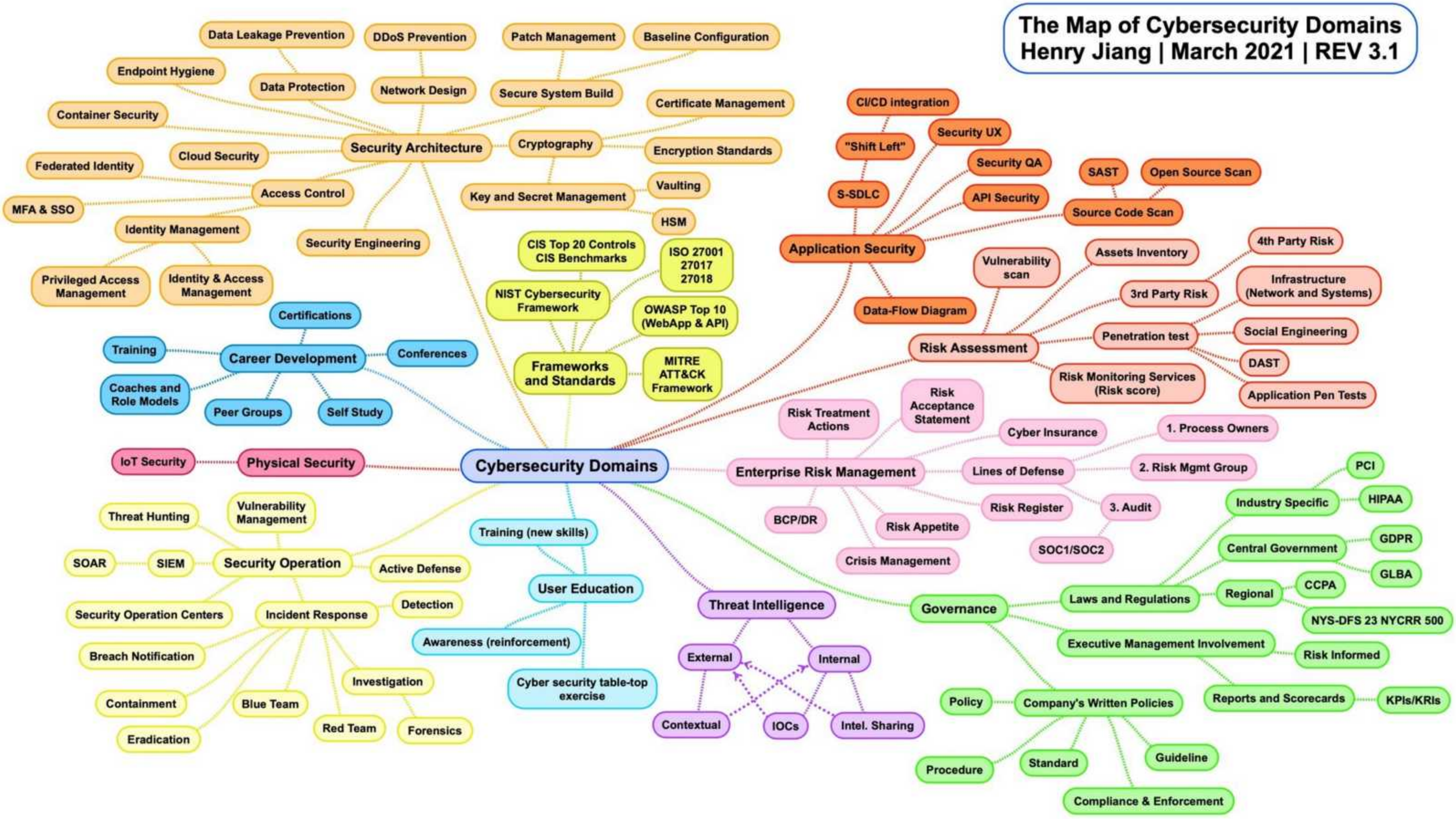
COMPTIA SECURITY+ (ENTRY), NETWORK+ (ENTRY), CYBERSECURITY ANALYSIS (CySA+), PENTEST+, ADVANCED SECURITY PRACTITIONER (CASP+)

IAPP CERTIFIED INFORMATION PRIVACY PROFESSIONAL, ISACA CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER, EU GENERAL DATA PROTECTION REGULATION (GDPR)

Conclusion

Certifications are increasingly important when applying for cybersecurity positions. Employers measure your knowledge based on the certifications obtained and experience & NOT always based on traditional college degrees.

CAREER PATHWAYS



The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.1

- Cybersecurity Domains
  - Security Architecture
    - Data Protection
      - Data Leakage Prevention
    - Endpoint Hygiene
    - Network Design
      - DDoS Prevention
    - Secure System Build
      - Patch Management
      - Baseline Configuration
    - Container Security
    - Cloud Security
    - Cryptography
      - Certificate Management
      - Encryption Standards
      - Key and Secret Management
        - Vaulting
        - HSM
    - Access Control
      - Federated Identity
      - MFA & SSO
      - Identity Management
        - Privileged Access Management
        - Identity & Access Management
    - Security Engineering
  - Frameworks and Standards
    - CIS Top 20 Controls CIS Benchmarks
    - NIST Cybersecurity Framework
    - ISO 27001 27017 27018
    - OWASP Top 10 (WebApp & API)
    - MITRE ATT&CK Framework
  - Application Security
    - S-SDLC
      - "Shift Left"
        - CI/CD integration
    - Security UX
    - Security QA
    - API Security
    - Source Code Scan
      - SAST
      - Open Source Scan
    - Data-Flow Diagram
  - Risk Assessment
    - Vulnerability scan
    - Assets Inventory
    - 3rd Party Risk
      - 4th Party Risk
    - Penetration test
      - Infrastructure (Network and Systems)
      - Social Engineering
      - DAST
      - Application Pen Tests
    - Risk Monitoring Services (Risk score)
  - Enterprise Risk Management
    - Risk Treatment Actions
    - Risk Acceptance Statement
    - Cyber Insurance
    - Lines of Defense
      - 1. Process Owners
      - 2. Risk Mgmt Group
      - 3. Audit
        - SOC1/SOC2
    - Risk Register
    - BCP/DR
    - Risk Appetite
    - Crisis Management
  - Governance
    - Laws and Regulations
      - Industry Specific
        - PCI
        - HIPAA
      - Central Government
        - GDPR
        - GLBA
      - Regional
        - CCPA
        - NYS-DFS 23 NYCRR 500
    - Executive Management Involvement
      - Risk Informed
    - Reports and Scorecards
      - KPIs/KRIs
    - Company's Written Policies
      - Policy
      - Procedure
      - Standard
      - Guideline
      - Compliance & Enforcement
  - Threat Intelligence
    - External
    - Internal
    - Contextual
    - IOCs
    - Intel. Sharing
  - User Education
    - Training (new skills)
    - Awareness (reinforcement)
    - Cyber security table-top exercise
  - Security Operation
    - Threat Hunting
    - Vulnerability Management
    - SIEM
      - SOAR
    - Active Defense
    - Security Operation Centers
    - Incident Response
      - Detection
      - Breach Notification
      - Containment
      - Eradication
      - Blue Team
      - Red Team
      - Investigation
        - Forensics
  - Physical Security
    - IoT Security
  - Career Development
    - Certifications
    - Training
    - Conferences
    - Coaches and Role Models
    - Peer Groups
    - Self Study

QUESTIONS??