Cyber Security course contents

1. **Course 1**: Information Security Fundamentals
2. **Course 2**: Cyber Security Introduction
3. **Course 3**: Technologies in Cybersecurity eco-system
4. **Course 4**: Core Threat Intelligence Engineering
5. **Course 5**: Core Vulnerability Management Engineering
6. **Course 6**: Core Penetration Management Techniques
7. **Course 7**: Core Cyber Exploitations
8. **Course 8**: Global Cyber Attack Trends
9. **Course 9**: Security Operations Management
10. **Course 10**: Incident Management
11. **Course 11**: Web and Mobile security Techniques
12. **Course 12**: Privacy and Online Rights
13. **Course 13**: Best Practices for keeping Systems and Data safe
14. **Course 14**: Cloud Security Engineering
15. **Course 15**: Industry Infosec Governance

Course 1 - Information Security Fundamentals : Broad Overview of Information Security will cover the following topics:

- 1.1 Information Security, 1.2 Computer Security, 1.3 CIA Triad/Principles, 1.4 Non-repudiation, 1.5 Risk Management
- 1.6 Cryptography Basics, 1.7 Authentication, 1.8 Authorization, 1.9 Access Control, 1.10 Security Policies
- 1.11 Security Auditing, 1.12 Security Laws and Regulations, 1.13 Defense, 1.14 Security Monitoring, 1.15 ISO 27000 framework
- 1.16 Information Security use case demonstration as per industry verticals, 1.17 Policy, Process, Procedures, Standards, Guidelines, Baselines

Case Study / Demo / Role Play / Discussion / Quiz will cover the following topics:

- Case structure – Objectives, Target audience, Executive summary, Background, Your evaluation, Proposed solution, Conclusion
- **Case Study #1:** List Foundations of HealthCare Industries
  - Patient medical records contain sensitive information that must be protected from unauthorized access.
- **Case Study #2:** List Strong Foundations of Fintech Industries
  - Financial institutions handle large amounts of sensitive financial data, such as account numbers and transaction history, which must be protected from cyber threats

- Demo
- Scenario based role play (Cybersecurity strategy development, Incident response plan)
- Group discussion
- Quiz

Course 2 - Cyber Security Introduction : Broad Overview of Cyber Security will cover the following topics:

- 2.1 Cybersecurity, 2.2 Cybers attacks, 2.3 Social Engineering, 2.4 Cybersecurity Defences (Firewall, AV, SIEM, Patch, Password etc), 2.5 Cloud security, 2.6 Endpoint security, 2.7 Mobile security, 2.8 Zero trust, 2.9 IOT, 2.10 Layers of cybersecurity, 2.11 Hacking, 2.12 Incident management, 2.13 Security operations

Case Study / Demo / Role Play / Discussion / Quiz will cover the following topics:

- **Case Study #3: Define cyber security governance structure for CISO in bank**
- **Case Study #4: Define cyber security structure for CISO in Auto manufacturing**
- Scenario based role play (Cybersecurity strategy development, Incident response plan)
- Group discussion
- Quiz

Course 3 - Technologies in Cybersecurity eco-system: Broad Overview of Technologies will cover the following topics:

- 3.1 Network security – Architecture and Standards, Wireless security, Network Vulnerabilities, Threats – Password cracking, Spoofing, Packet sniffing, Port scanning, Poisoning
- 3.2 System security - Asset classification, Asset accountability, Configuration management, Privilege access control, Virtualization security, System hardening, End-point security, System upgrades and patches, Backup and recovery, Systems Auditing, Threats – Denial of Service (DOS), DHCP spoofing, Dictionary attack, Email spoofing
- 3.3 Software security – Secure Design, Secure Coding, Static Security, Dynamic Security, Open source governance, Software composition analysis, Log and audit trail ,OWASP Top10 Threats - SQL Injection, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF)
- 3.4 Cryptography Basics – Security by Obscurity, Cryptographic Keys, Asymmetric, Symmetric, Hashing, Public Key Infrastructure (PKI), Challenges in cryptography
- 3.5 Application of Cryptography – Virtual Private Network (VPN), Secure Socket Layer (SSL), Digital Signature
- 3.6 Cloud security – Identity and Access management (IAM), Key management, Governance, Risk and Compliance (GRC), Legal, Data sovereignty, Business continuity, Disaster recovery, Cloud security models

- 3.7 Block chain security, 3.8 Zero Trust, 3.9 XDR, 3.10 AI, 3.11 MUD, 3.12 Context aware

Case Study / Demo / Role Play / Discussion / Quiz will cover the following topics:

- **Case Study #5:** What are the Fundamental Network protections used in Any Industry
  - Firewalls, IDS, IPS, VPN, Antivirus, SIEM
- **Case Study #6:** List methods to Secure Data in transit and Data at rest
  - Encryption, Hashing,
- **Case Study #7:** How many ways can you protect any user account in applications
  - 2FA, MFA, Password Management
- Demo
- Scenario based role play (Cybersecurity strategy development, Incident response plan)
- Group discussion
- Quiz

Course 4 - Core Threat Intelligence Engineering: Broad Overview of threat intelligence will cover the following topics:

- 4.1 Threat model, 4.2 Tactical, operations and strategic threat intelligence, 4.3 How to detect, respond and defeat threats, 4.4 Adversary data, 4.5 Reactive and proactive threat approach , 4.6 IOC, 4.7 Cyber kill chain,. 4.8 MITRE ATT@ACK

Case Study / Demo / Role Play / Discussion / Quiz will cover the following topics:

- **Case Study #8: How many Levels of User expertise are involved to form an Threat Intel team**
- **Case Study #9: What are the roles included in Threat Intelligence at Industry level**
- Demo
- Scenario based role play (Cybersecurity strategy development, Incident response plan)
- Group discussion
- Quiz

Course 5 - Core Vulnerability Management Engineering: Broad Overview of Vulnerability management will cover the following topics:

- 5.1 what is vulnerability, Threats, Risks, Exploitation, 5.2 Computer ports / protocols, 5.3 Ethical hack, Recon, Enumeration, Port Scanning, 5.4 Tools, 5.5 Attack Toolset – Metasploit, Nessus, nmap, Burpsuite, 5.6 Basic defence measures - Antivirus, Intrusion Detection / Prevention systems

Case Study / Demo / Role Play / Discussion / Quiz will cover the following topics:

- **Case Study #10: What are few examples of an Vulnerability as per Industry oriented applications**
- **Case Study #11: Explain RACI Matrix in banking environment**
- Demo
- Scenario based role play (Cybersecurity strategy development, Incident response plan)
- Group discussion
- Quiz

Course 6 - Core Penetration test techniques: Broad Overview of penetration test techniques will cover the following topics:

- 6.1 what is penetration testing, vulnerability, Threats, Risks, Exploitation, 6.2 Computer ports / protocols, 6.3 Port Scanning, 6.4 Tools, 6.5 Attack Toolset – Metasploit, Nessus, nmap, Burpsuite, 6.6 Basic defence measures - Antivirus, Intrusion Detection / Prevention systems, 6.7 Penetration test approach, tools, 6.8 Pen test reporting, 6.9 Pen test rules, 6.10 Gray box, White box, Black box , 6.11 Sniffing, 6.12 DOS, 6.12 Social engineering, 6.13 Session hijacking, SQL Injection

Case Study / Demo / Role Play / Discussion / Quiz will cover the following topics:

- **Case Study #12: How to do network scanning in banking industry**
- **Case Study #13: How to do social engineering (email phishing) in auto manufacturing**
- Demo
- Scenario based role play (Cybersecurity strategy development, Incident response plan)
- Group discussion
- Quiz

Course 7 - Core Cyber Exploitations: Broad Overview of cyber exploitation will cover the following topics:

- 7.1 Exploitation, 7.2 Types of exploits, 7.3 Identify, Protect, Detect, Respond, Recover, 7.3 Honey pot, 7.4 Data collection, analytics 7.5 Proactive and reactive exploitation, 7.6 Red , blue team, and purple team, 7.7 Incident management, 7.8 Data breach, 7.9 Ransomware, 7.10 Zero day attack, 7.11 Man in the middle

Case Study / Demo / Role Play / Discussion / Quiz will cover the following topics:

- **Case Study #14: Difference between Vulnerability and Exploitations. How to identify exploitation in banking industry**
- **Case Study #15: What Network vectors are considered for exploitation. How to implement in healthcare**

- Demo
- Scenario based role play (Cybersecurity strategy development, Incident response plan)
- Group discussion
- Quiz

Course 8 - Global attack trends: Broad Overview of cyber-attack trends will cover the following topics:

- 8.1 Past, present & future trends of cyber threat landscape (Worldwide)
- 8.2 Cybercrime landscape in Asia Pacific
- 8.3 Organizational processes, Security roles and responsibilities, Due care and Due diligence
- 8.4 Cybersecurity threats – Malware, Viruses and Worms, Trojan horses, Botnets, Zero-day exploits, Phishing, Spear phishing, Whaling, Social engineering, etc.
- 8.5 Risk management concepts, Personnel security policies, Information security training and awareness
- 8.6 Critical infrastructure protection, Privacy by design

Case Study / Demo / Role Play / Discussion / Quiz will cover the following topics:

- **Case Study #16: Explain Ransomware behaviour and impact within the industries.**
- **Case Study #17: What is a Malware and how to setup malware protection in hospital**
- **Case Study #18: Will Linux and Mac have any Attacks and Malware. Consider ecommerce services**
- Demo
- Scenario based role play (Cybersecurity strategy development, Incident response plan)
- Group discussion
- Quiz

Course 9 - Security Operations Management : Broad Overview of SOC will cover the following topics:

- 9.1 SOC security operations centre concept, 9.2 Logging, Attack methodology and monitoring, 9.3 Incident detection and Reporting, 9.4 SIEM, 9.5 Threat intelligence feed , 9.6 24x7 monitoring

Case Study / Demo / Role Play / Discussion / Quiz will cover the following topics:

- Case Study #19: **What is Security posture for any healthcare industry**
- **Case Study #20: What is SOC in food chain industry**
- Demo
- Scenario based role play (Cybersecurity strategy development, Incident response plan)
- Group discussion

- Quiz

Course 10 - Security Incident Management **:** Broad Overview of incident management will cover the following topics:

- 10.1 Incident handling and response, 10.2 Incident RACI, 10.3 Forensic package , critical incident package, 10.4 Malware incidents, 10.5 Email security and phishing incidents , 10.6 Threat reporting, 10.7 Third party incidents, 10.8 Feedback process, 10.9 TTX

Case Study / Demo / Role Play / Discussion / Quiz will cover the following topics:

- **Case Study #21: What is Zero Day? Does it have any impact on any industry applications. Define process framework**
- **Case Study #22: How are Incidents managed for HealthCare , FinTech, SCADA and Automotive industries**
- Demo
- Scenario based role play (Cybersecurity strategy development, Incident response plan)
- Group discussion
- Quiz

Course 11 - Web and Mobile security Techniques: Broad Overview of web and mobile security techniques will cover the following topics:

- 11.1 Web environment setup for scan and tools, 11.2 Scan web application, 11.3 Exploit vulnerabilities, 11.4 Deep analysis, 11.5 Reporting
- 11.6 Mobile environment setup for scan and tools, 11.7 Scan mobile application, 11.8 Exploit vulnerabilities, 11.9 Deep analysis, 11.10 Reporting

Case Study / Demo / Role Play / Discussion / Quiz will cover the following topics:

- Cyber breach case study (Equifax, Uber, Target, Stuxnet, SWIFT)
- **Case Study #23: What's the Top standard followed in Web Applications**
- **Case Study #24: What the Top standard followed in Mobile Applications**
- **Case Study #25: List secure frameworks used in Mobile App Development**
- Demo
- Scenario based role play (Cybersecurity strategy development, Incident response plan)
- Group discussion
- Quiz

Course 12 – Privacy and online rights: Broad Overview of privacy techniques will cover the following topics:

- 12.1 Privacy concept, 12.2 Privacy regulations, 12.3 GDPR, 12.4 Online privacy challenges 12.5 Online marketing/ sales privacy challenges, 12.6 Privacy protection and penalties

Case Study / Demo / Role Play / Discussion / Quiz will cover the following topics:

- Cyber breach case study (Equifax, Uber, Target, Stuxnet, SWIFT)
- **Case Study #26: What data is considered as Privacy issue in online ecommerce**
- **Case Study #27: Whats the impact if your company related data is available online?**
- Demo
- Scenario based role play (Cybersecurity strategy development, Incident response plan)
- Group discussion
- Quiz

Course 13 – Best Practices for keeping Systems and Data safe: Broad overview of Security best practices will cover the following topics:

- 13.1 Understand your data and risk, 13.2 Protect your systems, 13.3 Cyber Insurance, 13.4 AV, 13.5 Data leakage , 13.6 Security guidelines – NIST, ISO 27001, GDPR, 13.7 Risk Management Frameworks and Security Standards
  - NIST SP800-30: Evaluating security risks
  - ISO 27000 - Information Security Management Standards (ISMS)
  - DO-178C - Software Considerations in Airborne Systems and Equipment Certification
  - ISO/IEC 27034 – Application security guidelines
  - SS 584 : Singapore Standard for Multi Tier Cloud Security

Case Study / Demo / Role Play / Discussion / Quiz will cover the following topics:

- **Case Study #28: How can you assure your data is safe in Public network and corporate network**
- **Case Study #29: List 3 simple methods to keep your system safe from malware**
- Demo
- Scenario based role play (Cybersecurity strategy development, Incident response plan)
- Group discussion
- Quiz

Course 14 – Cloud security engineering: Broad Overview of cloud security will cover the following topics:

- 14.1 Cloud security fundamentals, 14.2 Cloud providers, 14.3 Tools for cloud security, 14.4 Cloud recovery, 14.5 Cloud Monitoring, 14.6 Cloud compliance, certification, audit and compliance, Pen test

Case Study / Demo / Role Play / Discussion / Quiz will cover the following topics:

- **Case Study #30: How the Cloud services or applications can be targeted to hackers**
- **Case Study #31: What are the Different methods to store data safe**
- Demo
- Scenario based role play (Cybersecurity strategy development, Incident response plan)
- Group discussion
- Quiz

Course 15 – Industry Infosec Governance: Broad Overview of Industry security governance will cover the following topics:

- 15.1 Industry roles and student skill identification, 15.2 Industry training, certification, 15.3 Industry career path, 15.4 How to become industry cybersecurity expert, 15.5 Job application process, 15.6 Salary / perks, 15.7 Working in healthcare industry

Case Study / Demo / Role Play / Discussion / Quiz will cover the following topics:

- Cyber breach case study (Equifax, Uber, Target, Stuxnet, SWIFT)
- **Case Study #32: Abbreviated CIA and give one example for Healthcare industry**
- **Case Study #33: Are Policies, procedures and standards important to protect CIA for an Industry**
- Demo
- Scenario based role play (Cybersecurity strategy development, Incident response plan)
- Group discussion
- Quiz
