BERITECK CURRICULUM

- **Computer fundamentals**
    1. Windows
    2. Linux

- **Networking fundamentals**
    1. Computer Networks
    2. Network devices (Firewalls, switches, routers, IPS/IDS, VPN)
    3. The OSI model
    4. Network Protocols (HTTP(S), SSH, SMTP
    5. HTTP status code
    6. Ports and services
    7. Port scanning with **Nmap**

- **Threat intelligence**
    1. Threats
    2. Threat actors
    3. Threats, vulnerability, risk
    4. IOC’s
    5. Zero day

- **Open-source intelligence**
    1. Reconnaissance
    2. Mitre Attack Matrix

- **Malware**
    1. Types of malwares
    2. What is malware?
    3. Types of cyber attack

- **Social Engineering**
    1. Phishing
    2. What is phishing?
    3. Types of phishing

- **Email Header Analysis**
    1. Email header
    2. Email header analysis
    3. Email filtering tool (**Proofpoint**)

BERITECK CURRICULUM

- **Cryptography/Encryption**
  1. Types of cryptography
  2. Encryption
  3. Hashing
  4. Steganography
  5. CIA Triad

- **Endpoint Security**
  1. SentinelOne
  2. Crowdstrike

- **Blue Team Operations Architecture**
  1. Why do we need SOC
  2. Functions of SOC
  3. Incident vs events
  4. True vs false positive
  5. Concept of logs

- **SIEM – security information and event management**
  1. What is a SIEM?
  2. Types of SIEM’s
  3. Splunk
  4. QRadar

- **Vulnerability scanning tools.**
  1. Nessus
  2. ZAP
  3. Qualys