CYBER SECURITY ANALYST SYLLABUS

Introduction:

- Introduction to Cyber Security
- Cyber Security Roles & Responsibilities

Frameworks:

- Framework & Security Controls
- Penetration Testing Processes
- Reconnaissance Techniques
- Open Source Intelligence
- Social Engineering

Discovery Techniques & Tools:

- Topology Discovery
- Port Scanning
- Service Discovery Techniques & Tools

OS Fingerprinting:

- Security Appliances
- Configuring Firewalls

Intrusion Detection & Prevention

Configuring IDS

Malware Threats

Configuring Anti-virus Software

Sysinternals Tools:

- Enhanced Mitigation Experience Toolkit
- Logging & Analysis
- Packet Capture Tools
- Monitoring Tools

Log Review & SIEM:

- SIEM Data Outputs

- SIEM Data Analysis
- Point-in-time Data Analysis

Vulnerabilities:

- Managing Vulnerabilities
- Vulnerability Management Requirements
- Asset Inventory
- Data Classification
- Vulnerability Management Processes
- Vulnerability Scanner
- Microsoft baseline security analyser
- SCAP
- Configuring Vulnerability Scans
- Vulnerability Scanning Criteria
- Exploit Frameworks

Remediating Vulnerabilities:

- Analyzing Vulnerability Scans
- Remediation & Change Control
- Remediating Host Vulnerabilities
- Remediating Virtual Infrastructure Vulnerabilities

Software Developments:

- Secure Software Development
- Software Development Life Cycle
- Software Vulnerabilities
- Software Security Testing

Interception Proxies:

- Web Application Firewalls
- Source Authenticity
- Reverse Engineering

Incident Response:

- Incident Response Processes
- Threat Classification
- Incident Severity & Prioritization
- Types of Data

Forensics Tools:

- Digital Forensics Investigations
- Documentation & Forms
- Digital Forensics Crime Scenes
- Digital Forensics Kits
- Image acquisition
- Password Cracking
- Analysis Utilities
- Incident Analysis & Recovery

Analyzing& Recovery Frameworks:

- Analyzing Network Symptoms
- Analyzing Host Symptoms
- Analyzing Data Exfiltration
- Analyzing application Symptoms

Using Sysinternals:

- Containment Techniques
- Eradication Techniques
- Validation Techniques
- Corrective Actions

Network Design:

- Secure Network Design
- Network Segmentation
- Blackholes
- Sinkholes & Honeypots
- System Hardening

Group Policies & MAC:

- Endpoint Security
- Managing Identities & Access
- Network Access Control

Identity Management:

- Identity Security Issue
- Identity Repositories
- Context Based Authentication

Single Sign on & Federation:

- Exploiting identities
- Exploiting Web Browsers & Applications
- Security Frameworks & Policies
- Frameworks & Compliance

Security Architecture:

- Reviewing Security Architecture
- Procedures & Compensating Controls
- Verification & Quality Control
- Security Policies & Procedures
- Personnel Policies & Training