NATIONAL INSTITUTE OF ELECTRONICS AND INFORMATION TECHNOLOGY, PATNA

SUVIKSAN TECHNOLOGIES PRIVATE LIMITED

Syllabus

Course : Infrastructure Security Expert,

Duration: 3 months

Module 1: Basics of Networking

- Networking Fundamentals
  - OSI & TCP/IP Models
  - IP Addressing, Subnetting, CIDR
  - Routing vs Switching
  - Common Protocols (HTTP/S, DNS, DHCP, FTP, SSH, RDP, SNMP)

- Network Devices & Security Functions
  - Routers, Switches, Firewalls
  - IDS/IPS, Load Balancers, Proxies

- Hands-on Labs
  - Configure basic networking on Linux/Windows
  - Packet capture with Wireshark

Module 2: Introduction to Infrastructure Security

- What is Infrastructure Security?
- CIA Triad in Infra Context
- Threats to IT Infrastructure
- Security Frameworks: NIST CSF, CIS Controls, ISO 27001

Module 3: Network Security & Monitoring

- Secure Network Design
  - Network Segmentation, VLANs
  - DMZ & Bastion Hosts

- Perimeter Security
  - Firewalls, IDS/IPS, Web Application Firewall (WAF)
  - DDoS Protection

- Network Monitoring & Traffic Analysis
  - Tools: Wireshark, Zeek, Snort, Suricata

- Hands-on Labs
  - Configure firewall rules & packet filtering
  - IDS/IPS deployment and log analysis

Module 4: Endpoint & Server Security

- System Hardening
  - Windows Hardening: GPO, Sysmon, Event Logs
  - Linux Hardening: iptables, auditd, fail2ban

- Patch & Vulnerability Management
- Endpoint Detection & Response (EDR)
  - Tools: CrowdStrike, MS Defender ATP, OSSEC

- Hands-on Labs
  - Harden a Windows & Linux Server
  - Deploy EDR/AV solution

Module 5: Cloud & Virtual Infrastructure Security

- Virtualization Security
  - Securing Hypervisors (VMware, VirtualBox, Hyper-V)

- Cloud Infrastructure Security
  - AWS, Azure, GCP Basics
  - Shared Responsibility Model
  - Securing VMs, Storage, and Networking in Cloud

- Cloud Security Posture Management (CSPM)
- Hands-on Labs
  - Deploy secure VM in AWS/Azure
  - Enable & analyze cloud logs

Module 6: Identity & Access Management

- IAM Fundamentals: AAA (Authentication, Authorization, Accounting)
- Active Directory Security & Hardening
- Privileged Access Management (PAM)
- MFA, SSO, Zero Trust
- Hands-on Lab: Secure an AD Domain & enforce MFA

Module 7: Infrastructure Threats, Vulnerabilities & Pentesting

- Common Infra Weaknesses: Misconfigurations, Open Ports, Weak Passwords
- Vulnerability Scanning Tools: Nessus, OpenVAS
- Infra Pentesting Basics (SMB, RDP, SSH Exploits)
- Hands-on Labs
  - Perform vulnerability scan
  - Exploit & patch misconfigurations

Module 8: Incident Detection & Response

- Infra Security Monitoring (SIEM, SOC workflows)
- Log Analysis & Threat Hunting
- Incident Response Life Cycle (NIST 800-61)
- Case Studies: WannaCry, Colonial Pipeline
- Hands-on Lab: Investigate security logs, create IR playbook

Module 9: Compliance, Governance & Capstone Project

- Regulatory Frameworks: PCI DSS, HIPAA, GDPR, SOX
- Business Continuity & Disaster Recovery in Infra Security
- Capstone Project Options
  - Secure Network & Server Setup with Monitoring
  - Cloud Infra Deployment with Security Controls
  - Incident Simulation & IR Plan Execution

(Note: Points mentioned are just short summary, but they consist of a lot of subtopics and detailed structu re with practical scenarios)