หลักสูตร วิศวกรความปลอดภัย (Security Engineer)

ในยุคดิจิทัลที่เทคโนโลยีสารสนเทศมีบทบาทสำคัญ ความมั่นคงปลอดภัยทางไซเบอร์จึงมีความจำเป็นต่อการปกป้องข้อมูลและระบบสารสนเทศขององค์กรและบุคคล ทว่าตลาดแรงงานยังขาดแคลนบุคลากรด้านนี้ จึงต้องพัฒนาหลักสูตรวิศวกรความปลอดภัยทางไซเบอร์ (Security Engineer) เนื้อหาครอบคลุมตั้งแต่การเขียนโปรแกรมพื้นฐาน ความรู้ด้านความปลอดภัยเครือข่าย มาตรฐานความปลอดภัย การตรวจจับและตอบสนองภัยคุกคาม ไปจนถึงการรักษาความปลอดภัยระบบคลาวด์และการใช้ระบบ SIEM ผู้ที่ผ่านการอบรมจะมีทักษะพร้อมรับมือกับความท้าทายด้านไซเบอร์อย่างมืออาชีพ

วัตถุประสงค์

1. เพื่อให้ผู้เข้าอบรมสามารถเขียนโปรแกรมเบื้องต้นได้
2. เพื่อให้ผู้เข้าอบรมสามารถจัดการระบบสารสนเทศได้อย่างมีมาตรฐานด้านความปลอดภัยทางไซเบอร์
3. เพื่อให้ผู้เข้าอบรมสามารถใช้เครื่องมือด้านความมั่นคงปลอดภัยทางไซเบอร์ได้
4. เพื่อให้ผู้เข้าอบรมสามารถรักษาความปลอดภัยให้กับระบบคลาวด์ได้
5. เพื่อให้ผู้เข้าอบรมสามารถใช้งานระบบปฏิบัติการ Linux ได้

คุณสมบัติผู้เข้ารับการอบรม

1. นักศึกษาชั้นปีสุดท้าย
2. บัณฑิตจบใหม่ (ไม่เกิน 2 ปีหลังสำเร็จการศึกษา) ที่ยังไม่มีงานทำ
3. เกรดเฉลี่ยสะสม (GPA) ไม่น้อยกว่า 3.20
4. ศึกษาในสาขาวิชาที่เกี่ยวข้องกับคณิตศาสตร์ ตรรกศาสตร์ หรือสาขาใกล้เคียง
5. ผ่านเกณฑ์การทดสอบ Screen Test
6. สามารถเข้าร่วมโครงการได้ตั้งแต่แรก จนจบโครงการฯ

ระยะเวลา

10 วัน (60 ชั่วโมง)

รูปแบบการอบรม

ออนไลน์

ทักษะที่ได้รับ

☑ Programming/Coding
☑ Core Security Principles
☑ Network Security
☑ Security Tools
☑ Security Frameworks
☑ Linux Administration
☑ Threat Hunting
☑ Cloud Security
☑ Digital Forensics
☑ Incident Response
☑ Security Information and Event Management (SIEM)

☑ Vulnerability Assessment and Penetration Testing (VAPT)

เงื่อนไขการผ่านบทเรียน

- ต้องเข้าร่วมการเรียนไม่น้อยกว่า 80% ของระยะเวลาทั้งหมด
- ต้องผ่านการทดสอบหลังการอบรม โดยมีคะแนนไม่ต่ำกว่า 70%

สิ่งที่ผู้อบรมจะได้รับจากการอบรม

- สิทธิ์ในการสอบเพื่อรับ ประกาศนียบัตรมาตรฐานสากล IT Specialist: Cyber Security Certification

เนื้อหาการอบรม วันที่ 1

- Introduction to Programming
  - What is Programming?
  - Overview of Programming Languages & Their Uses (Python, JavaScript, Java, C, etc.)
  - Understanding Syntax, Variables, Data Types
  - Setting Up the Development Environment (IDE, Code Editors, Terminals)
  - Hands-on: Writing & Executing Your First Program
- Control Structures & Logic Building
  - Conditional Statements (if-else, switch-case)
  - Loops (for, while)
  - Logical & Comparison Operators
  - Hands-on: Building a Simple Decision-Making Program
- Functions & Code Reusability
  - What Are Functions & Why Are They Important?
  - Defining & Calling Functions
  - Function Parameters & Return Values
  - Hands-on: Creating Functions for Code Modularity
- Data Structures & Working with Collections
  - Lists, Arrays, Tuples, and Dictionaries
  - Basic Operations on Data Structures (Adding, Removing, Modifying)
  - Hands-on: Implementing a Simple Data Processing Program
- File Handling & Basic Debugging
  - Reading & Writing to Files
  - Handling Errors & Debugging Techniques
  - Hands-on: Creating a Simple File-Based Data Storage Program
- Mini Project & Course Wrap-Up
  - Mini Project: Build a Basic CLI Tool or Simple Web Script

- Best Practices in Programming (Code Readability, Comments, DRY Principle)
- Next Steps: Learning Paths in Web Development, Data Science, Automation

เนื้อหาการอบรม วันที่ 2

- Introduction to Security Principles
  - Understanding Cybersecurity & Its Importance
  - The CIA Triad (Confidentiality, Integrity, Availability)
  - Common Cyber Threats (Malware, Phishing, Ransomware, Insider Threats)
  - Security Frameworks & Standards (NIST, ISO 27001, CIS Controls)
- Risk Management & Security Controls
  - Identifying & Assessing Security Risks
  - Security Control Types: Preventive, Detective, Corrective
  - Defense in Depth (Layered Security) & Zero Trust Model
- Identity & Access Management (IAM)
  - Authentication vs. Authorization
  - Role-Based Access Control (RBAC) & Least Privilege Principle
  - Multi-Factor Authentication (MFA) & Identity Federation
- Network & Endpoint Security
  - Secure Network Architecture (Firewalls, IDS/IPS, VPN)
  - Endpoint Security & Hardening (Antivirus, Patching, EDR)
  - Secure Configurations & Hardening Best Practices
- Security Awareness & Incident Response
  - Understanding Social Engineering Attacks (Phishing, Pretexting, Baiting)
  - Best Practices for Security Awareness Training
  - Incident Response Lifecycle (Detection, Containment, Eradication, Recovery)
- Security Best Practices
  - Implementing Security Policies & Governance
  - Cyber Hygiene & Secure Coding Practices
  - The Future of Cybersecurity: AI & Cloud Security Trends

เนื้อหาการอบรม วันที่ 3

- หลักการป้องกันภัยไซเบอร์แบบ Defense in Depth
  - ความมั่นคงปลอดภัยไซเบอร์ขั้นพื้นฐาน (Core security principles)

        - การรักษาความมั่นคงปลอดภัยทางกายภาพ (Physical security)
        - ประเภทของนโยบายด้านความมั่นคงปลอดภัย (Security policy types)
        - ประเภทของภัยคุกคามทางไซเบอร์ (Type of attack)
        - ประเภทของการสำรองและกู้คืนข้อมูล (Identify backup and restore types)
    - การรักษาความปลอดภัยให้กับระบบปฏิบัติการ (Operating System Security)
        - การป้องกันเครื่องลูกข่าย (Client) และเครื่องแม่ข่าย (Server)
        - การตั้งค่าการระบุ (Identification) และการยืนยันตัวตน (Authentication) ให้กับผู้ใช้งาน
        - การจัดการสิทธิ (Permission) บนระบบปฏิบัติการ Windows และ Linux
        - การใช้ Audit policies และ log files
        - เทคโนโลยีการเข้ารหัส (Encryption)
    - การรักษาความปลอดภัยให้กับอุปกรณ์ภายในระบบเครือข่าย (Network Device Security)
        - การรักษาความปลอดภัยให้กับเครือข่ายไร้สาย (Wireless security)
        - อุปกรณ์ป้องกันภัยคุกคามที่เกี่ยวข้องกับระบบเครือข่าย
        - หลักการแบ่งแยก (Isolation) ระบบเครือข่าย
        - การระบุและเลือกใช้โพรโทคอล (Protocol) ที่ปลอดภัย
    - การรักษาความปลอดภัยให้กับคอมพิวเตอร์ (Secure Computing)
        - การใช้งานอีเมลอย่างปลอดภัย
        - การใช้งานเว็บเบราวเซอร์อย่างปลอดภัย
        - การติดตั้งและการตั้งค่าโปรแกรมแอนตี้ไวรัส

เนื้อหาการอบรม วันที่ 4

- Introduction to Security Tools
    - Why Security Tools Are Essential in Cybersecurity
    - Categories of Security Tools:
    - Network Security (Firewalls, IDS/IPS)
    - Vulnerability Scanning (Nessus, OpenVAS)
    - Endpoint Protection (EDR, Antivirus)
    - Threat Detection & SIEM (Splunk, ELK, QRadar)
    - Forensics & Incident Response (Volatility, Wireshark)
- Network Security & Traffic Analysis Tools
    - Firewall & IDS/IPS Tools: pfSense, Snort, Suricata
    - Packet Capture & Network Monitoring: Wireshark, Zeek (Bro IDS)
- Vulnerability Scanning & Assessment Tools
    - Identifying Vulnerabilities in Networks & Applications
    - Popular Scanning Tools: Nessus, OpenVAS, Nmap, Nikto
- Threat Detection & SIEM Tools

- Introduction to SIEM & Log Analysis
- SIEM Platforms: Splunk, ELK Stack, IBM QRadar
- Digital Forensics & Incident Response (DFIR) Tools
- Memory Forensics: Volatility, Rekall
- File & Malware Analysis: Autopsy, VirusTotal, YARA

เนื้อหาการอบรม วันที่ 5

- Introduction to Security Frameworks
  - What is a Security Framework?
  - Importance of Security Frameworks in Risk Management
  - Overview of Common Frameworks
  - NIST Cybersecurity Framework (CSF)
  - ISO 27001 (Information Security Management System - ISMS)
  - CIS Critical Security Controls (CIS Controls)
  - PCI-DSS (Payment Card Industry Data Security Standard)
  - Selecting the Right Framework for Your Organization
- NIST Cybersecurity Framework (CSF)
  - The six Core Functions of NIST CSF:
  - Identify (Asset Management, Risk Assessment)
  - Protect (Access Control, Data Security, Awareness Training)
  - Detect (Anomalies, Continuous Monitoring)
  - Respond (Incident Response & Recovery)
  - Recover (Business Continuity Planning)
  - Govern (cybersecurity policies, processes, and governance)
- ISO 27001 – Information Security Management System (ISMS)
  - What is ISO 27001 & Why is it Important?
  - Understanding Annex, A Controls & ISMS Requirements
  - Risk Management & Continuous Improvement Approach
  - Compliance & Certification Process
- CIS Critical Security Controls
  - Overview of the Top 18 CIS Security Controls
  - Implementing CIS Controls in IT Infrastructure
  - Comparing CIS Controls with Other Frameworks

เนื้อหาการอบรม วันที่ 6

- Introduction to Linux
  - History & Evolution of Linux
  - Linux Distributions (Ubuntu, CentOS, RHEL, Debian)

        - Linux File System Hierarchy
        - User & Group Management
    - Linux Command Line & Shell Scripting
        - Basic Linux Commands (ls, cd, mv, cp, rm, cat, etc.)
        - File Permissions & Ownership (chmod, chown, chgrp)
        - Process Management (ps, top, kill, nice, nohup)
        - Introduction to Bash Scripting
        - Demo: Writing Basic Shell Scripts
    - Package Management & Software Installation
        - Package Managers (APT, YUM, DNF, Zypper)
        - Installing & Removing Software
        - Managing Repositories & Dependencies
        - Demo: Installing & Configuring Applications
    - User & Permission Management
        - Creating & Managing Users & Groups
        - Setting Password Policies
        - sudo & Privilege Escalation
        - Demo: Configuring User Access & Permissions

เนื้อหาการอบรม วันที่ 7

- Introduction to Threat Hunting
    - What is Threat Hunting?
    - Proactive vs. Reactive Security
    - Threat Hunting vs. Threat Intelligence vs. Incident Response
    - The Cyber Kill Chain & MITRE ATT&CK Framework
- Understanding Adversary Tactics & Techniques
    - Common Attack Vectors (Phishing, Ransomware, Insider Threats)
    - Advanced Persistent Threats (APTs) & Their Methodologies
    - Understanding Indicators of Compromise (IoCs) & Indicators of Attack (IoAs)
    - Demo: Mapping Attacks to MITRE ATT&CK Framework
- Threat Hunting Methodologies & Techniques
    - Hypothesis-Driven vs. Data-Driven Threat Hunting
    - TTP-Based Hunting (Tactics, Techniques, and Procedures)
    - Threat Hunting with Logs & Network Data
    - Demo: Building a Threat Hunting Hypothesis
- Tools & Data Sources for Threat Hunting
    - SIEM Solutions (Splunk, ELK, Graylog)

- EDR & XDR Platforms (CrowdStrike, SentinelOne, Microsoft Defender)
- Network Traffic Analysis (Wireshark, Zeek, Suricata)
- Demo: Collecting & Analyzing Threat Intelligence

เนื้อหาการอบรม วันที่ 8

- Introduction to Cloud Security
  - Understanding Cloud Computing Models (IaaS, PaaS, SaaS)
  - Shared Responsibility Model in Cloud Security
  - Common Cloud Security Threats (Misconfigurations, Data Breaches, API Exploits)
  - Compliance & Regulatory Standards (ISO 27017, NIST, CSA, GDPR, PCI-DSS)
  - Cloud Security vs. Traditional Security
- Cloud Identity & Access Management (IAM)
  - Identity & Access Control Models
  - Role-Based Access Control (RBAC) vs. Attribute-Based Access Control (ABAC)
  - Multi-Factor Authentication (MFA) & Single Sign-On (SSO)
  - Least Privilege Access Best Practices
- Securing Cloud Workloads & Data
  - Data Encryption (At Rest & In Transit)
  - Secure Storage (AWS S3, Azure Blob, GCP Storage Security)
  - Cloud Network Security: VPC, Security Groups, Firewalls
  - Logging & Monitoring: CloudTrail, Azure Monitor, GCP Audit Logs
- Cloud Threat Detection & Incident Response
  - Cloud Security Tools: AWS GuardDuty, Azure Security Center, GCP Security Command Center
  - Cloud Incident Response Process (Containment, Eradication, Recovery)
  - Case Study: Real-World Cloud Security Breaches

เนื้อหาการอบรม วันที่ 9

- Introduction to SIEM
  - What is SIEM?
  - Importance of SIEM in Cybersecurity
  - Key Components of a SIEM Solution
  - SIEM vs. Log Management vs. Security Analytics

        - Overview of Popular SIEM Tools (Splunk, ELK, QRadar, ArcSight, Microsoft Sentinel)
    - Log Sources & Data Collection
        - Understanding Logs & Log Collection Methods
        - Common Log Sources
        - Network Devices (Firewalls, Routers, IDS/IPS)
        - Servers & Endpoints (Windows, Linux, Cloud)
        - Applications & Databases
        - Demo: Configuring Log Collection & Forwarding
    - SIEM Architecture & Deployment
        - SIEM Deployment Models (On-Prem, Cloud, Hybrid)
        - Event Forwarding & Data Ingestion
        - Correlation Rules & Use Case Development
        - Demo: Setting Up a Basic SIEM Instance
    - Log Parsing & Normalization
        - Understanding Raw Logs vs. Structured Logs
        - Log Parsing Techniques & Regular Expressions
        - Normalization & Enrichment for Better Analysis
        - Demo: Parsing & Normalizing Logs in a SIEM

เนื้อหาการอบรม วันที่ 10

Introduction to Incident Response (IR)

- What is Incident Response?
- Importance of IR in Cybersecurity
- Incident Response Lifecycle (NIST, SANS, ISO 27035)
- Role of an IR Team (CSIRT, SOC, Threat Hunters)
- Demo: Understanding the IR Process with a Real-World Case Study Incident Detection & Triage
- Identifying Security Incidents vs. False Positives
- Common Attack Vectors & Threat Intelligence Sources
- Indicators of Compromise (IoCs) & Indicators of Attack (IoAs)
- Demo: Detecting Suspicious Events in SIEM Logs

- Containment & Eradication Strategies
    - Network Segmentation & Isolation Techniques
    - Host-Based vs. Network-Based Containment
    - Root Cause Analysis & Threat Removal
    - Demo: Containing & Mitigating a Ransomware Attack
- Digital Forensics & Evidence Collection

- Digital Forensics Basics (Memory, Disk, Network)
- Chain of Custody & Legal Considerations
- Tools for Forensic Investigation (Autopsy, Volatility, FTK, Wireshark)

Demo: Acquiring & Analyzing Evidence from a Com