หลักสูตร

วิศวกรความมั่นคงปลอดภัย Security Engineer

ภายใต้โครงการเส้นทางสู่วิศวกรความมั่นคงปลอดภัย สำหรับนักศึกษาจบใหม่สู่การทำงานในภาคอุตสาหกรรม

NextGen Security Careers: Pathway for Fresh Graduates to Become Security Engineers in Industry

สารบัญ

เนื้อหา หน้า

เส้นทางสู่วิศวกรความมั่นคงปลอดภัยสำหรับนักศึกษาจบใหม่ สู่การทำงานในภาคอุตสาหกรรม
NextGen Security Careers: Pathway for Fresh Graduates to Become Security Engineers in Industry
หลักสูตรวิศวกรความมั่นคงปลอดภัย (Security Engineer)

รายละเอียดโครงการโดยย่อ

ในยุคดิจิทัลที่เทคโนโลยีสารสนเทศมีบทบาทสำคัญ ความมั่นคงปลอดภัยทางไซเบอร์เป็นสิ่งจำเป็นในการปกป้องระบบสารสนเทศและข้อมูลขององค์กรหรือบุคคลจากภัยคุกคามทางไซเบอร์ อย่างไรก็ตาม บุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ยังมีไม่เพียงพอต่อความต้องการในตลาดแรงงาน เพื่อพัฒนากำลังคนให้สอดคล้องกับความต้องการในภาคอุตสาหกรรม จึงมีความจำเป็นในการพัฒนาหลักสูตรวิศวกรความมั่นคงปลอดภัยทางไซเบอร์ (Security Engineer) ที่ครอบคลุมเนื้อหาตั้งแต่การเขียนโปรแกรมพื้นฐาน หลักการความมั่นคงปลอดภัย การรักษาความปลอดภัยระบบเครือข่าย การใช้งานเครื่องมือด้าน Security กรอบมาตรฐานด้านความปลอดภัย การไล่ล่าภัยคุกคาม การรักษาความปลอดภัยระบบคลาวด์ การเฝ้าระวังเหตุการณ์ด้วยระบบ SIEM การตอบสนองต่อเหตุการณ์ และการใช้งานระบบปฏิบัติการ Linux

หลักสูตรนี้มุ่งเน้นนักศึกษาที่เรียนในสาขาด้านเทคโนโลยีสารสนเทศและสาขาอื่น ๆ ที่เกี่ยวข้องกับไอที ให้มีความรู้เฉพาะด้าน Security และเมื่อจบการฝึกอบรมแล้ว จะเข้าสู่กระบวนการจับคู่กับนายจ้าง เพื่อส่งนักศึกษาที่ผ่านการอบรมให้สามารถเข้าสู่การทำงานในภาคอุตสาหกรรมได้ โดยกระบวนการจับคู่กับนายจ้างจะประกอบด้วยขั้นตอนต่าง ๆ ดังนี้

1. การประเมินทักษะและความสามารถ: นักศึกษาจะได้รับการประเมินทักษะและความสามารถที่ได้เรียนรู้จากหลักสูตร เพื่อให้แน่ใจว่ามีความพร้อมในการทำงานจริง
2. การให้คำปรึกษาและแนะแนวอาชีพ: นักศึกษาจะได้รับคำปรึกษาและแนะแนวอาชีพจากผู้เชี่ยวชาญ เพื่อช่วยในการเลือกเส้นทางอาชีพที่เหมาะสมกับความสามารถและความสนใจ
3. การจัดหางานและการจับคู่กับนายจ้าง: โครงการจะทำงานร่วมกับบริษัทและองค์กรต่างๆ ในภาคอุตสาหกรรม เพื่อจัดหางานและจับคู่นักศึกษากับนายจ้างที่ต้องการบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์
4. การติดตามผลและการสนับสนุนหลังการจ้างงาน: หลังจากที่นักศึกษาได้รับการจ้างงานแล้ว โครงการจะติดตามผลและให้การสนับสนุนเพิ่มเติม เพื่อให้นักศึกษาสามารถปรับตัวและทำงานได้อย่างมีประสิทธิภาพ

ผู้ที่ผ่านการอบรมจะสามารถประกอบอาชีพในตำแหน่งต่างๆ เช่น วิศวกรความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Engineer) นักวิเคราะห์ความปลอดภัย (Security Analyst) ผู้เชี่ยวชาญด้านการตอบสนองต่อเหตุการณ์ (Incident Response Specialist) และผู้เชี่ยวชาญด้านการไล่ล่าภัยคุกคาม (Threat Hunter) เป็นต้น

วัตถุประสงค์โครงการ

1. พัฒนาทักษะนักศึกษาที่กำลังสำเร็จการศึกษา ที่อยู่ในสายการเรียนที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อยกระดับทักษะด้านความปลอดภัยทางไซเบอร์ให้สูงขึ้น เพื่อเตรียมความพร้อมสู่การประกอบอาชีพในอนาคต
2. สร้างโอกาสในการจ้างงาน เปิดโอกาสให้นักศึกษาได้พบกับบริษัทที่กำลังมองหาบุคลากรที่มีความสามารถ เพื่อเพิ่มโอกาสในการจ้างงานและสร้างเครือข่ายทางอาชีพ

กลุ่มเป้าหมาย จำนวน 70 คน/โครงการฯ

1. นักศึกษาชั้นปีสุดท้าย
2. บัณฑิตจบใหม่ (ไม่เกิน 2 ปีหลังสำเร็จการศึกษา) ที่ยังไม่มีงานทำ
3. ผู้สมัครต้องมี เกรดเฉลี่ยสะสม (GPA) ไม่น้อยกว่า 2.90 หากเกรดเฉลี่ยสะสม (GPA) ต่ำกว่า 2.90 ยังสามารถสมัครได้ หากได้เกรด B ขึ้นไปในรายวิชาใดวิชาหนึ่งที่เกี่ยวข้องกับหลักสูตร ดังนี้
    - ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)
    - โครงสร้างข้อมูลและอัลกอริทึม (Data Structures & Algorithms)
    - ระบบปฏิบัติการ (Operating Systems)
    - ระบบคอมพิวเตอร์และเครือข่าย (Computer Systems & Networks)
    - วิชาความปลอดภัยเครือข่าย (Network Security) หรือวิชาอื่นๆ ที่เกี่ยวข้อง
4. ศึกษาในสาขาวิชาที่เกี่ยวข้อง กับหลักสูตรอบรมและตำแหน่งงานที่ต้องการ

คุณสมบัติผู้เข้ารับการอบรม

1. นักศึกษาชั้นปีสุดท้าย (เกรดเฉลี่ยไม่ต่ำกว่า 2.90) หรือผู้สำเร็จการศึกษาไม่เกิน 2 ปี
2. มีพื้นฐานเขียนโปรแกรม + ความเข้าใจด้านระบบ/เครือข่าย + ความรู้เบื้องต้นเรื่อง Security เพื่อให้สามารถต่อยอดสู่หัวข้อเชิงลึกอย่าง Threat Hunting, Cloud Security, SIEM และ Incident Response ได้
3. ผ่านการทดสอบ Screen Test จากโครงการ
4. สามารถเข้าร่วมโครงการได้ครบทุกช่วง ตั้งแต่เริ่มต้นจนจบโครงการ

สิ่งที่ผู้เข้ารับการอบรมจะได้รับ

1. อบรมฟรี มูลค่า 50,000 บาท (ไม่มีค่าใช้จ่าย)
2. อัพสกิล Security Engineer ครบวงจร
3. อบรมออนไลน์ 10 วัน (60 ชั่วโมง) พร้อม Workshop ฝึกปฏิบัติจริง
4. รับ 2 ใบประกาศ
    - ใบรับรองสากล IT Specialist: Cyber Security Certification
    - ใบประกาศนียบัตรจาก depa
5. เตรียมพร้อมสู่การทำงานจริง → ทำ Resume, เข้าร่วม Job Matching, สัมภาษณ์กับบริษัทพันธมิตร

6. มีโอกาสได้งานทันที ในตำแหน่ง Security Engineer / Security Analyst / Threat Hunter

ขั้นตอนการเข้าร่วมโครงการ

1. ลงทะเบียนผ่านเว็บไซต์โครงการ
2. โครงการคัดเลือกผู้สมัคร และประกาศผล
3. อบรมออนไลน์
4. สอบใบรับรองมาตรฐานสากล IT Specialist: Cyber Security Certification
5. ผู้อบรมจัดทำและส่ง Resume
6. กิจกรรม Job Matching (ออนไลน์)
7. บริษัทพันธมิตรนัดสัมภาษณ์
8. บริษัทคัดเลือกและตกลงจ้างงาน
9. โครงการติดตามและรายงานผล
10. สิ้นสุดโครงการ

กำหนดการฝึกอบรม (ออนไลน์) เดือนพฤศจิกายน 2568

เวลา: 09.00 – 16.00 น.

อาทิตย์	จันทร์	อังคาร	พุธ	พฤหัสบดี	ศุกร์	เสาร์
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

สรุปวันอบรม เดือนพฤศจิกายน 2568 รวม 10 วัน ดังนี้

สัปดาห์ที่ 1 → 3, 4, 5, 6, 7

สัปดาห์ที่ 2 → 10, 11, 12, 13, 14

ตารางแผนงานและช่วงเวลาดำเนินโครงการ

ลำดับ	ขอบเขตและแผนการดำเนินงาน	พ.ศ. 2568				พ.ศ. 2569			
		ก.ย.	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.
1	เปิดรับสมัคร	→							
2	คัดเลือกผู้สมัคร	→							
3	กิจกรรมอบรม		→	→	→				

4	สอบมาตรฐานสากล				→				
5	จัดทำและส่ง Resume				→	→			
6	กิจกรรม Job Matching (ออนไลน์)					→	→		
7	บริษัทพันธมิตรนัดสัมภาษณ์						→	→	
8	บริษัทคัดเลือกและตกลงจ้างงาน						→	→	
9	ติดตามผลและรายงาน							→	→
10	สิ้นสุดโครงการ								→

รูปแบบและระยะเวลาการอบรม

1. อบรมรูปแบบออนไลน์ 2. ระยะเวลา 10 วัน (60 ชั่วโมง)

หลักสูตรวิศวกรความมั่นคงปลอดภัย (Security Engineer)

ครอบคลุมเนื้อหา ดังนี้

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

ช่องทางการรับสมัคร

สมัครผ่านเว็บไซต์โครงการ www.arit.co.th/secareer
ภายในวันที่ 17 ตุลาคม 2568
ประกาศผลผู้ผ่านการคัดเลือกเข้ารับอบรม วันที่ 24 ตุลาคม 2568

ผู้บริหารโครงการ

บริษัท เออาร์ไอที จำกัด
1023 อาคารเอ็มเอสสยาม ชั้น 8 ถ.พระราม 3 ช่องนนทรี ยานนาวา กรุงเทพฯ 10120

ฝ่ายประสานงานโครงการ

คุณศาสตรา นะรารัมย์ 087-444-5526 sastran@ar.co.th

รายละเอียดหลักสูตรและกำหนดการอบรม
หลักสูตรวิศวกรความมั่นคงปลอดภัย (Security Engineer)

ในยุคดิจิทัลที่เทคโนโลยีสารสนเทศมีบทบาทสำคัญ ความมั่นคงปลอดภัยทางไซเบอร์เป็นเรื่องจำเป็นในการปกป้องระบบสารสนเทศและข้อมูลขององค์กรหรือของบุคคลให้ปลอดภัยจากภัยคุกคามทางไซเบอร์ ในขณะที่บุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์มีไม่เพียงพอต่อความต้องการในตลาดแรงงาน ดังนั้นเพื่อเป็นการพัฒนากำลังคนให้สอดคล้องกับความต้องการในภาคอุตสาหกรรม จึงมีความจำเป็นในการพัฒนาหลักสูตรวิศวกรความมั่นคงปลอดภัยทางไซเบอร์ (Security Engineer) โดยมีเนื้อหาครอบคลุมตั้งแต่การเขียนโปรแกรมพื้นฐาน (Introduction to Programming) หลักการความมั่นคงปลอดภัย (Security Principles) การรักษาความปลอดภัยระบบเครือข่าย (Network Security) การใช้งานเครื่องมือด้าน Security กรอบมาตรฐานด้านความปลอดภัย (Security Framework) การไล่ล่าภัยคุกคาม (Threat Hunting) การรักษาความปลอดภัยให้กับระบบคลาวด์ (Cloud Security) การเฝ้าระวังเหตุการณ์ด้วยระบบ SIEM การตอบสนองต่อเหตุการณ์ (Incident Response) ตลอดจนการใช้งานระบบปฏิบัติการ Linux เมื่อผู้เข้าอบรมผ่านการฝึกอบรมในหลักสูตรนี้แล้วจะสามารถรับมือกับความท้าทายด้านความปลอดภัยทางไซเบอร์ได้อย่างมืออาชีพ

วัตถุประสงค์

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

รูปแบบการฝึกอบรม

บรรยาย และสาธิตพร้อมให้ผู้เรียนฝึกปฏิบัติกับไฟล์ตัวอย่าง (Workshop)

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 Compromised Machine