FREE COURSE

หลักสูตร
ความมั่นคงปลอดภัยเชิงรับ
Blue Team ขั้นสูง
Advanced Defensive Security Blue Team

หลักสูตรภายใต้มาตรการสร้างบุคลากรทักษะสูงสำหรับอุตสาหกรรมยุคใหม่ ความร่วมมือระหว่าง BOI และกระทรวง อว.

คำอธิบายหลักสูตร

หลักสูตรความมั่นคงปลอดภัยเชิงรับ Blue Team ขั้นสูง (Advanced Defensive Security Blue Team) เป็นหลักสูตรเชิงลึกด้านการป้องกัน ตรวจจับ วิเคราะห์ และตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ในระดับองค์กร โดยมุ่งเน้นให้ผู้เข้ารับการฝึกอบรมสามารถทำหน้าที่เป็นทีมป้องกัน (Blue Team) และศูนย์ปฏิบัติการความมั่นคงปลอดภัย (Security Operation Center: SOC) ได้อย่างมืออาชีพ

เนื้อหาหลักสูตรครอบคลุมกรอบการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Incident Management) ตามมาตรฐานสากล เช่น NIST SP 800-61, ISO/IEC 27035 และแนวทาง SANS PICERL รวมถึงการปฏิบัติงานจริงใน SOC ตั้งแต่การเฝ้าระวังภัยคุกคาม การวิเคราะห์ Log จากแหล่งข้อมูลหลากหลาย การใช้เครื่องมือ SIEM/EDR/NDR/XDR การทำ Threat Hunting และการทำ Digital Forensics ในระดับพื้นฐานถึงระดับปฏิบัติการจริง

ผู้เข้ารับการฝึกอบรมจะได้เรียนรู้จากกรณีศึกษา (Case Study) และฝึกปฏิบัติจริง (Hands-on Lab) ผ่านสถานการณ์จำลอง (Scenario-based Exercise) เช่น Ransomware Incident, Phishing Campaign, Brute-force Attack, Insider Threat และ Advanced Persistent Threat (APT) เพื่อให้พร้อมนำความรู้ไปใช้ในองค์กรจริงได้ทันที

วัตถุประสงค์ของหลักสูตร

1.เพื่อพัฒนาทักษะของบุคลากรด้านการเฝ้าระวัง ตรวจจับ วิเคราะห์ และตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ในระดับองค์กร
2.เพื่อให้ผู้เข้ารับการฝึกอบรมสามารถดำเนินงานตามวงจร Incident Response Lifecycle ได้อย่างเป็นระบบ ตั้งแต่ Preparation, Detection, Containment, Eradication, Recovery และ Post-Incident Activity
3.เพื่อเสริมความสามารถในการปฏิบัติงานในศูนย์ปฏิบัติการความมั่นคงปลอดภัย (SOC) ทั้งในบทบาท Tier 1, Tier 2, Tier 3 และ Incident Responder
4.เพื่อให้ผู้เรียนสามารถออกแบบ ใช้งาน และปรับปรุง Use Case, Detection Rules, Playbooks และมาตรการตอบสนองเหตุการณ์ให้สอดคล้องกับภัยคุกคามสมัยใหม่
5.เพื่อยกระดับกำลังคนด้านความมั่นคงปลอดภัยไซเบอร์เชิงรับ (Blue Team) ให้สอดคล้องกับความต้องการของหน่วยงานภาครัฐและภาคเอกชน

ผลที่ได้รับจากการเข้าฝึกอบรม

- ผู้เข้ารับการฝึกอบรมสามารถบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างเป็นระบบ ตั้งแต่การตรวจจับ การยืนยันเหตุการณ์ การควบคุมความเสียหาย การกำจัดภัยคุกคาม จนถึงการฟื้นฟูระบบ
- สามารถใช้งานเครื่องมือสำคัญใน SOC เช่น SIEM, EDR, NDR/XDR, Threat Intelligence Platform และเครื่องมือวิเคราะห์ Log ต่าง ๆ ได้อย่างมีประสิทธิภาพ
- มีทักษะการทำ Threat Hunting เชิงรุก สามารถค้นหาเบาะแสการบุกรุก (Indicators of Compromise / Indicators of Attack) และพฤติกรรมผิดปกติในระบบได้
- สามารถวิเคราะห์เหตุการณ์และจัดทำรายงานด้านความมั่นคงปลอดภัยทั้งเชิงเทคนิค (Technical Report) และเชิงผู้บริหาร (Executive Summary) ได้อย่างมีมาตรฐาน

องค์กรที่ส่งบุคลากรเข้ารับการฝึกอบรมจะมีขีดความสามารถในการเฝ้าระวังและตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ดีขึ้น ลดความเสี่ยงและผลกระทบจากภัยคุกคามได้อย่างเป็นรูปธรรม

รูปแบบการฝึกอบรม

1) **รูปแบบการฝึกอบรม:** ฝึกอบรมแบบ On-site
2) **ระยะเวลา:** รวม 5 วัน วันละประมาณ 6 ชั่วโมง (รวม 30 ชั่วโมง)
3) **รูปแบบการเรียนรู้**
   - บรรยายเชิงทฤษฎีผสมผสานตัวอย่างจริง (Case Study)
   - ฝึกปฏิบัติจริงในห้องปฏิบัติการ (Hands-on Lab) ผ่านระบบจำลอง SOC / Incident Response Lab
   - การทำ Workshop แบบกลุ่มจากสถานการณ์จำลอง (Scenario-based Exercise)
   - การแลกเปลี่ยนประสบการณ์ระหว่างผู้เข้าร่วมและวิทยากรผู้เชี่ยวชาญ

กลุ่มเป้าหมายผู้เข้ารับการฝึกอบรม

- เจ้าหน้าที่ในศูนย์ปฏิบัติการความมั่นคงปลอดภัย (Security Operation Center: SOC) เช่น SOC Analyst Tier 1–3, Incident Responder, Threat Hunter
- ผู้ปฏิบัติงานด้านการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Incident Management / CERT / CSIRT)
- ผู้ดูแลระบบคอมพิวเตอร์และเครือข่าย (System Administrator, Network Administrator)
- บุคลากรด้าน Security Engineer / Security Analyst / IT Risk / IT Audit ที่ต้องเกี่ยวข้องกับการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
- บุคลากรของหน่วยงานภาครัฐ รัฐวิสาหกิจ และเอกชน ที่มีหน้าที่รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

คุณสมบัติของผู้เรียนและความรู้ขั้นพื้นฐานที่ผู้เข้ารับการฝึกต้องมี

- มีพื้นฐานความรู้ด้านระบบปฏิบัติการ Windows และ/หรือ Linux ในระดับปฏิบัติงาน
- มีความเข้าใจพื้นฐานเกี่ยวกับโครงสร้างระบบเครือข่าย (TCP/IP, Routing, Firewall, DNS ฯลฯ)
- มีประสบการณ์ทำงานด้าน IT Infrastructure / Cybersecurity / SOC / Incident Response หรือเกี่ยวข้อง
- สามารถอ่านและทำความเข้าใจ Log เบื้องต้น เช่น Windows Event Log, Firewall Log, Web/Proxy/DNS Log ได้

จำนวนผู้เข้ารับการฝึกอบรม

- จำนวนผู้เข้ารับการอบรม 30 คน/รุ่น
- ดำเนินการทั้งหมด 6 รุ่น
- รวมผู้เข้าร่วมทั้งหมด 180 คน

เครื่องมือ อุปกรณ์ ซอฟต์แวร์หลักที่ใช้ในการฝึกอบรม

- ระบบจำลองศูนย์ปฏิบัติการความมั่นคงปลอดภัย (SOC Lab / Cyber Range)
- ระบบบริหารจัดการเหตุการณ์และวิเคราะห์ Log (Security Information and Event Management: SIEM)
- ระบบตรวจจับและตอบสนองปลายทาง (Endpoint Detection and Response: EDR) และ/หรือ NDR / XDR
- เครื่องมือวิเคราะห์ทราฟฟิกเครือข่าย เช่น Wireshark, Packet Capture Tools
- เครื่องมือด้าน Digital Forensics พื้นฐาน เช่น Volatility, Autopsy (หรือเทียบเท่า) สำหรับ Memory / Disk / Network Forensics
- ระบบ Threat Intelligence Feed / Dashboards สำหรับประกอบการวิเคราะห์ภัยคุกคาม
- ระบบแบบฝึกหัดและโจทย์ปฏิบัติ (Hands-on Lab Platform)
- ระบบสนับสนุนการเรียน เช่น ระบบลงทะเบียน ระบบประเมินผล และระบบจัดเก็บ Log ตัวอย่าง

ค่าลงทะเบียนและสิทธิประโยชน์

ผู้เข้าร่วมโครงการจะได้รับการอบรม โดยไม่เสียค่าใช้จ่ายในการลงทะเบียน โดยค่าใช้จ่ายดังกล่าวได้รับการสนับสนุนภายใต้มาตรการสร้างบุคลากรทักษะสูงสำหรับอุตสาหกรรมยุคใหม่ ทั้งนี้ ผู้เข้าร่วมโครงการจะได้รับสิทธิประโยชน์ตลอดระยะเวลาการอบรม ดังต่อไปนี้

- อาหารกลางวัน
- อาหารว่าง 2 มื้อ
- เอกสารประกอบการฝึกอบรม
- ระบบ Lab ออนไลน์สำหรับฝึก
- สิทธิ์สอบมาตรฐานสากล IT Specialist Cybersecurity
- สิทธิ์สอบซ่อม 1 ครั้ง

รายละเอียดหลักสูตร

Day 1: SOC Foundation & Threat Landscape

- บทนำเกี่ยวกับ Security Operation Center (SOC): บทบาท หน้าที่ โครงสร้างทีม (Tier 1–3, Incident Responder, Threat Hunter, DFIR)
- รูปแบบการจัดตั้ง SOC: In-house SOC, MSSP, Hybrid SOC
- แนวโน้มภัยคุกคามไซเบอร์ (Threat Landscape) เช่น Malware, Ransomware, Insider Threats, APT
- กรอบแนวคิด Cyber Kill Chain และ MITRE ATT&CK Framework เพื่อใช้วิเคราะห์ Tactics, Techniques & Procedures (TTPs)
- แนะนำพื้นฐาน Incident Response Lifecycle และความเชื่อมโยงกับการทำงานของ SOC

Day 2: Incident Response Lifecycle & Log Analysis

- กรอบมาตรฐานการรับมือเหตุการณ์ NIST SP 800-61, ISO/IEC 27035, SANS PICERL
- ขั้นตอน Preparation, Detection & Analysis, Containment, Eradication, Recovery, Post-Incident Activity
- แหล่งที่มาของการตรวจจับเหตุการณ์ (Sources of Detection): EDR, SIEM, SOAR, Network Sensors, Firewall, IDS/IPS Logs
- การวิเคราะห์ Log พื้นฐาน: Windows Event Logs, Linux Audit Logs, Firewall/Proxy/DNS Logs
- การคัดกรองเหตุการณ์ (Triage) การจัดลำดับความสำคัญ (Severity Classification & Prioritization)
- Workshop: วิเคราะห์เหตุการณ์จาก Log จริง / กึ่งจำลอง เช่น Suspicious Login, Malware Activity, Brute Force Scenario

Day 3: SOC Operations & SIEM Use Cases

- ภาพรวมสถาปัตยกรรม SOC และเทคโนโลยีหลัก: SIEM, SOAR, EDR, NDR/XDR, Case Management
- การออกแบบและใช้งาน Use Case/Detection Rule บน SIEM
- การเขียน Query (เช่น KQL / SPL หรือเทียบเท่า) เพื่อค้นหาเหตุการณ์ผิดปกติ
- การจัดการ Alert: Alert Triage Workflow, False Positive Handling, Escalation Process
- Workshop:
  - วิเคราะห์ Alert จริงจาก SOC (Lab)
  - สร้าง Dashboard และ Detection Rule พื้นฐาน
  - ออกแบบ Playbook สำหรับกรณี Phishing, Malware Infection, Unauthorized Access, Ransomware

Day 4: Threat Hunting & Digital Forensics Essentials

- แนวคิด Threat Hunting: Proactive Security, Hypothesis-driven Hunting, การใช้ MITRE ATT&CK ในการออกแบบ Hunt
- การตั้งสมมติฐานเพื่อค้นหา Lateral Movement, Persistence, Privilege Escalation
- Workshop: Threat Hunt บนสภาพแวดล้อม Lab – วิเคราะห์ Log และพฤติกรรมเพื่อค้นหา IOC/IOA
- พื้นฐาน Digital Forensics: Memory Forensics, Disk Forensics, Network Forensics
- เครื่องมือ Forensics เบื้องต้น เช่น Volatility, Autopsy, Wireshark และการใช้งานใน Incident Response
- Workshop: วิเคราะห์ PCAP File, แยกแยะพฤติกรรมผิดปกติ, ดึง IOCs ไปใช้ใน SIEM/Detection Rules

Day 5: Containment, Eradication, Recovery & Reporting

- กลยุทธ์การควบคุมเหตุการณ์ (Containment Strategies): Short-term vs Long-term Containment, Isolation Techniques, ป้องกัน Lateral Movement
- การกำจัดภัยคุกคาม (Eradication): Malware Removal Techniques, Cleaning System, Removing Persistence Mechanism, Patch & Configuration Update
- การฟื้นฟูระบบ (Recovery): System Rebuild, Validating System Integrity, Service Restoration
- การจัดทำเอกสารและรายงาน (Documentation & Reporting):
  - Technical Incident Report
  - Executive Summary
  - Evidence Handling & Chain of Custody
- กิจกรรม Lessons Learned & Continuous Improvement: Root Cause Analysis, ปรับปรุง Detection Rules, SIEM Correlation, สร้าง KPI/Metrics สำหรับวัดประสิทธิภาพ Incident Response
- Final Exercise: จำลองเหตุการณ์แบบครบวงจร (End-to-end IR/SOC Scenario) แล้วให้ผู้เข้าอบรมวิเคราะห์ แก้ไข และจัดทำรายงานสรุปเสนอผู้บริหาร

เกณฑ์การวัดผลและเกณฑ์การสำเร็จการศึกษา

1) การทดสอบก่อนและหลังการฝึกอบรม (Pre-Test / Post-Test) เพื่อวัดการพัฒนาความรู้
2) การประเมินผลจากการทำแบบฝึกหัดเชิงปฏิบัติ (Hands-on Lab / Workshop / Scenario Exercise)
3) การประเมินผลงาน Mini Project หรือ Final Exercise ด้าน Incident Response / SOC Operation
4) เกณฑ์การผ่านอบรม:

- ได้คะแนนรวม (ทฤษฎี + ปฏิบัติ) ไม่น้อยกว่า 70%
- เข้าร่วมการฝึกอบรมไม่น้อยกว่าร้อยละ 80 ของเวลาอบรมทั้งหมด
- ส่งผลงาน/แบบฝึกหัดครบถ้วนตามที่กำหนด

สิ่งที่ผู้เข้ารับการอบรมจะได้รับเพิ่มเติม

- ประกาศนียบัตรการผ่านการฝึกอบรมหลักสูตรความมั่นคงปลอดภัยเชิงรับ Blue Team ขั้นสูง
- สิทธิ์สอบมาตรฐานสากลด้าน Cybersecurity (ตามที่โครงการกำหนด) พร้อมสิทธิ์สอบซ่อม 1 ครั้ง
- เอกสารประกอบการฝึกอบรม ทั้งในรูปแบบเล่มและไฟล์ดิจิทัล รวมถึงตัวอย่าง Playbook, Use Case, Detection Rules และ Template รายงาน
- สิทธิ์เข้าร่วมกลุ่มเครือข่ายผู้ปฏิบัติงาน Blue Team / SOC (Community) เพื่อแลกเปลี่ยนข้อมูลข่าวสารและ Threat Intelligence ในระยะยาว

การบริหารโครงการ
บริษัท เออาร์ไอที จำกัด
1023 อาคารเอ็มเอสสยาม ชั้น 8 ถ.พระรามสาม
แขวงช่องนนทรี เขตยานนาวา กรุงเทพมหานคร
โทร 02 610 3099 | www.arit.co.th

ฝ่ายประสานงานโครงการ
นายศาสตรา นะรารัมย์
โทรศัพท์: 087-444-5526
อีเมล: sastran@ar.co.th