FREE COURSE

หลักสูตร ความมั่นคงปลอดภัยเชิงรุก Red Team ขั้นสูง

Advanced Offensive Security Red Team

ก้าวสู่สายงาน Red Team มืออาชีพ ฝึกโจมตีเชิงรุกแบบที่ใช้จริง
ในระดับองค์กร ตามกรอบมาตรฐานสากล MITRE ATT&CK

คำอธิบายหลักสูตร

หลักสูตรความมั่นคงปลอดภัยเชิงรุก Red Team ขั้นสูง (Advanced Offensive Security Red Team) เป็นหลักสูตรเชิงลึกที่มุ่งเน้นการพัฒนาทักษะการปฏิบัติงานด้าน Offensive Security และ Red Teaming ในระดับองค์กร ผู้เรียนจะได้เรียนรู้วิธีการโจมตีสมัยใหม่ เทคนิคการเข้าถึงระบบ การยกระดับสิทธิ์ การเคลื่อนย้ายภายในเครือข่าย (Lateral Movement) การตั้งค่า Persistence และการหลบเลี่ยงการตรวจจับ รวมถึงฝึกปฏิบัติผ่านสถานการณ์จำลองใกล้เคียงเหตุการณ์จริงในองค์กร (Enterprise Attack Simulation)

หลักสูตรนี้ครอบคลุมทั้ง Red Team Methodology (Recon – Weaponization – Delivery – Exploitation – Privilege Escalation – Pivoting – Exfiltration) พร้อมการประยุกต์ตามกรอบ MITRE ATT&CK Framework เหมาะสำหรับผู้ปฏิบัติงาน Cybersecurity ที่ต้องการยกระดับเป็นผู้เชี่ยวชาญด้าน Offensive Security

วัตถุประสงค์ของหลักสูตร

1.เพื่อพัฒนาทักษะ Red Team เชิงลึกให้สามารถปฏิบัติงานโจมตีจำลองแบบมืออาชีพ
2.เพื่อเสริมความเข้าใจเกี่ยวกับเทคนิคการโจมตีขั้นสูงที่ใช้ในโลกจริง
3.เพื่อให้ผู้เรียนสามารถวิเคราะห์ช่องโหว่และเส้นทางการโจมตีในระบบองค์กรได้ครบวงจร
4.เพื่อให้ผู้เข้ารับการฝึกสามารถจัดทำรายงาน Red Team Exercise พร้อมข้อเสนอแนะเชิงปฏิบัติได้
5.เพื่อเสริมสร้างกำลังคนด้าน Cybersecurity ให้ตรงกับความต้องการของประเทศ

ผลที่ได้รับจากการเข้าฝึกอบรม

- มีความสามารถในการดำเนินงาน Red Team Exercise ครบวงจร
- เข้าใจเทคนิคการโจมตีขั้นสูงในระดับองค์กร เช่น AD Attack, C2, Credential Harvesting
- สามารถวิเคราะห์และประเมินความเสี่ยง (Risk & Impact) ของช่องโหว่ได้อย่างแม่นยำ
- สามารถประยุกต์ความรู้เพื่อช่วยหน่วยงานรับมือภัยคุกคามได้จริง
- ได้รับประกาศนียบัตรและสิทธิ์สอบมาตรฐานสากล Cybersecurity พร้อมสอบซ่อม

รูปแบบการฝึกอบรม

- อบรมแบบ On-site
- การสอนแบบบรรยายรวมกับการฝึกปฏิบัติจริง (Hands-on Lab) ไม่น้อยกว่า 70%
- ใช้ระบบ Virtual Lab ที่จำลองโครงสร้างพื้นฐานขององค์กร
- ฝึกตามสถานการณ์จำลองจริง เช่น Initial Access, Lateral Movement, Privilege Escalation
- มีแบบทดสอบ Pre-Test และ Post-Test เพื่อประเมินผลพัฒนาการ

กลุ่มเป้าหมายผู้เข้ารับการฝึกอบรม

- Red Team / Blue Team / SOC Analyst
- Security Engineer / Network Engineer
- Penetration Tester
- System Administrator / DevSecOps
- บุคลากรที่มีหน้าที่ดูแลความมั่นคงปลอดภัยไซเบอร์ในองค์กร

คุณสมบัติของผู้เรียนและความรู้ขั้นพื้นฐานที่ผู้เข้ารับการฝึกต้องมี

- มีพื้นฐานด้าน IT Security หรือ Penetration Testing
- เข้าใจระบบเครือข่ายและโครงสร้าง Active Directory
- สามารถใช้งาน Linux และ Windows ได้ในระดับปฏิบัติการ
- เข้าใจเครื่องมือพื้นฐาน เช่น Nmap, Burp Suite, Metasploit
- เหมาะสำหรับผู้ทำงานสาย Cybersecurity อยู่แล้ว

จำนวนผู้เข้ารับการฝึกอบรม

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

เครื่องมือ อุปกรณ์ ซอฟต์แวร์หลักที่ใช้ในการฝึกอบรม

- Kali Linux / Parrot OS
- Metasploit Framework
- Cobalt Strike (หรือเทียบเท่า)
- BloodHound / Neo4j
- Empire / Covenant
- Burp Suite
- Wireshark
- SQLMap / OWASP ZAP
- Active Directory Attack Tools
- ระบบ Virtual Lab (Cyber Range)

ค่าลงทะเบียนและสิทธิประโยชน์

ผู้เข้าร่วมโครงการจะได้รับการอบรม โดยไม่เสียค่าใช้จ่ายในการลงทะเบียน โดยค่าใช้จ่ายดังกล่าวได้รับการสนับสนุนภายใต้มาตรการสร้างบุคลากรทักษะสูงสำหรับอุตสาหกรรมยุคใหม่ ทั้งนี้ ผู้เข้าร่วมโครงการจะได้รับสิทธิประโยชน์ตลอดระยะเวลาการอบรม ดังต่อไปนี้

- อาหารว่าง อาหารกลางวัน
- เอกสารฝึกอบรม
- ระบบปฏิบัติการ Workshop
- สิทธิ์สอบ IT Specialist: Cyber Security (พร้อมสอบซ่อม 1 ครั้ง)

รายละเอียดหลักสูตร

Module 1: Red Team Planning & Methodology
- แนวคิด Offensive Security
- Red Team vs PenTest
- MITRE ATT&CK / PTES / Kill Chain
- Rules of Engagement และ Scoping

Module 2: Reconnaissance & Initial Access
- OSINT / Passive Recon / Active Recon
- Exploit Web / Server / Application
- Credential Harvesting Techniques

Module 3: Privilege Escalation
- Windows Privilege Escalation
- Linux Privilege Escalation
- Token Manipulation / UAC Bypass

Module 4: Lateral Movement & Pivoting
- Pass-the-Hash / Pass-the-Ticket
- Kerberoasting / AS-REP Roasting
- VLAN Pivoting / Network Traversal

Module 5: Post-Exploitation & Persistence
- Command & Control (C2) Frameworks
- Data Exfiltration Techniques
- Persistence Mechanisms
- Anti-Forensics

Module 6: Advanced Web Application Hacking
- Authentication Bypass
- Server Misconfiguration Attack
- API Attack
- OWASP Top 10 (Advance Level)

Module 7: Reporting & Debriefing
- การเขียนรายงานแบบมืออาชีพ
- การจัดระดับความเสี่ยง
- Executive Summary
- การนำเสนอผล Red Team Exercise

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