AI for Security: Practical Protection with AI Tools

ระยะเวลา 1 วัน

หลักการและเหตุผล

ในยุคที่ภัยคุกคามไซเบอร์เพิ่มขึ้นอย่างต่อเนื่อง การเฝ้าระวังและตอบสนองเหตุการณ์ด้านความปลอดภัยด้วยวิธีการเดิม ๆ เช่น การตรวจ Log ด้วยมือ หรือการใช้ระบบขนาดใหญ่ที่ซับซ้อน มักไม่ทันต่อสถานการณ์จริง หลายองค์กรจึงเริ่มมองหาแนวทางใหม่ที่ "ฉลาดกว่าและเร็วกว่า" โดยใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) เข้ามาช่วย

หลักสูตรนี้ออกแบบมาเพื่อให้ผู้เรียนเข้าใจ แนวคิดการประยุกต์ AI กับงาน Security จริงในองค์กร ตั้งแต่การวิเคราะห์ Log เบื้องต้น การตรวจจับพฤติกรรมผิดปกติ การวิเคราะห์ข้อความเพื่อค้นหา Phishing รวมถึงการสร้าง Workflow อัตโนมัติด้วยเครื่องมือ Open Source เช่น N8N และ ChatGPT โดยไม่ต้องพึ่งระบบราคาแพงอย่าง SIEM หรือ SOC เต็มรูปแบบ ผู้เข้าอบรมจะได้เห็นภาพชัดว่า AI สามารถช่วยให้ทีมมองเห็นความเสี่ยงที่มองข้ามได้อย่างไร และสามารถนำกลับไปปรับใช้ภายในองค์กรเพื่อเพิ่มประสิทธิภาพการตรวจจับ การแจ้งเตือน และการสร้างระบบป้องกันแบบต่อเนื่องได้ทันที

วัตถุประสงค์

- เข้าใจแนวทางใช้ AI เพื่อช่วย "เฝ้าระวัง – แจ้งเตือน – ป้องกัน" ในระบบ IT ได้ทันที
- เห็นภาพการใช้ N8N และ ChatGPT เพื่อสร้าง Security Automation เบื้องต้น
- ไม่ต้องใช้ระบบใหญ่ เช่น SIEM/IPS ก็สามารถเริ่มต้น AI Security ได้
- พร้อมต่อยอดเป็นระบบ Security Dashboard หรือ Awareness System ภายในองค์กร

รายละเอียดหลักสูตร

Introduction & Overview

- ภาพรวมภัยคุกคามไซเบอร์ยุคใหม่ และบทบาทของ AI ในการตรวจจับและป้องกัน
- แนวคิด Threat Intelligence, Behavior Monitoring และ Automation ด้วย AI
- ตัวอย่างกรณีจริง: AI ตรวจจับการโจมตีในระบบอีเมล, login ผิดปกติ, และข้อมูลรั่วไหล
- ภาพรวมเครื่องมือ AI ที่องค์กรสามารถเริ่มต้นได้ทันที (ChatGPT, Copilot, N8N, Open-Source Tools)

Core Applications in IT Security

- การใช้ AI วิเคราะห์พฤติกรรมที่ผิดปกติจากข้อมูล Log
- การใช้ ChatGPT หรือ Copilot ช่วยอ่าน Log และสรุปเป็น Human-readable Summary
- การผสาน N8N กับ Open API เพื่อส่งข้อมูลแจ้งเตือนอัตโนมัติ
- ตัวอย่าง Workflow ที่ใช้ใน Incident Monitoring & Response ระดับพื้นฐาน

Lab 1 – "AI Reads Security Log" (Simple & Practical)

- เครื่องมือ: N8N + ChatGPT
- วัตถุประสงค์: เห็นกระบวนการที่ AI วิเคราะห์ Log เพื่อค้นหาความผิดปกติ
- กิจกรรม:
- นำ Log ตัวอย่าง (เช่น Login Failures หรือ Access Attempt จาก CSV) เข้าสู่ N8N
- ใช้ Node "AI Text Analysis" หรือ ChatGPT Node ช่วยสรุป Log ที่น่าสงสัย

- ให้ระบบส่งข้อความแจ้งเตือน (ผ่าน Email หรือ Line Notify) เมื่อพบ Keyword เช่น "failed", "denied", "unauthorized"
- อภิปรายผลและวิธีขยาย workflow ให้เหมาะกับองค์กร

ผลลัพธ์: ผู้เรียนเข้าใจการใช้ AI เพื่อช่วย "มองเห็น" พฤติกรรมที่น่าสงสัย โดยไม่ต้องใช้ SIEM จริง

Lab 2 – "AI Detects Suspicious Message"

- เครื่องมือ: ChatGPT (Web หรือ API ผ่าน N8N)
- วัตถุประสงค์: เรียนรู้วิธีให้ AI วิเคราะห์ข้อความอีเมลเพื่อหาความเสี่ยง Phishing
- กิจกรรม:
- ให้ผู้เรียนลองป้อนข้อความอีเมลจำลอง 2–3 ฉบับ (จริง/ปลอม)
- ใช้ Prompt เพื่อให้ AI ระบุว่าอีเมลนั้น "ปลอดภัย / น่าสงสัย / อันตราย" พร้อมเหตุผล
- สรุปรูปแบบของข้อความ Phishing ที่ AI มักจับได้ เช่น คำเร่งเร้า / ลิงก์ปลอม / ข้อความคลุมเครือ
- แชร์ผลและอภิปรายว่าควรปรับนโยบาย Awareness อย่างไร

ผลลัพธ์: ผู้เรียนเข้าใจการประยุกต์ AI ด้าน NLP กับ Security Awareness ได้ทันที

Risk Management & Continuous Protection

- ระบุความเสี่ยงจากการใช้ AI ในระบบความปลอดภัย (เช่น False Alarm, Data Exposure)
- หลักการ Human Oversight: ให้คนตรวจสอบผลลัพธ์ AI ก่อนแจ้งเตือนจริง
- ใช้ PDCA เพื่อพัฒนา Workflow ให้แม่นยำขึ้นเรื่อย ๆ
- แนวทางการเชื่อมโยงกับ ISO/IEC 27001 และ NIST AI RMF

Discussion & Wrap-up

- สรุปแนวทางการนำ AI Security Automation มาใช้ในองค์กร
- แชร์กรณีศึกษา AI ใช้จริงใน Cyber Defense
- Q&A / Reflection: "AI ไม่ได้แทนคน แต่ช่วยคนให้เห็นสิ่งที่มองไม่ทัน"

กลุ่มเป้าหมาย

- เจ้าหน้าที่ IT / Security Analyst / System Admin ที่ต้องการเรียนรู้วิธีใช้ AI มาช่วยตรวจจับภัยคุกคาม
- ผู้จัดการด้านความปลอดภัยสารสนเทศ (Information Security / Risk Manager) ที่ต้องการแนวทางเริ่มต้นด้าน AI Security Automation
- ทีม SOC / Incident Response / IT Operation ที่อยากลดภาระการตรวจ Log และเพิ่มความเร็วในการตอบสนองเหตุการณ์
- บุคลากรสาย Data / Developer / AI Enthusiast ที่สนใจทดลองใช้เครื่องมืออย่าง ChatGPT, Copilot, N8N เพื่อสร้างระบบป้องกันภัยไซเบอร์แบบง่าย ๆ

มาตรฐานอ้างอิง

- NIST AI Risk Management Framework (RMF)
- ISO/IEC 27001: Information Security Management System
- ISO/IEC 42001: Artificial Intelligence Management System
- NIST SP 800-177 & MITRE ATT&CK

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th