



สถาบันไอทีจีเนียส
IT GENIUS INSTITUTE

COURSE ID
CYC-06

COURSE OUTLINE · รายละเอียดหลักสูตรอบรม

CYBERSECURITY / BLUE TEAM

AI for Cybersecurity Operations

ใช้ AI ช่วยทีม SOC คัดกรองแจ้งเตือน วิเคราะห์ Log และล่าภัยคุกคาม

● 12 ชั่วโมง

● 2 วัน

● พื้นฐาน ใช้งาน Wazuh และ SOC

● ระดับ Intermediate



ระยะเวลา: 2 วัน

12 ชั่วโมง (2 วัน วันละ 6 ชม.) · 09:00-16:00 น.



รูปแบบ: Classroom / Hybrid

Onsite หรือ Online ผ่าน Microsoft Teams · Public / In-house



รายละเอียดหลักสูตร

www.itgenius.co.th

ทีม SOC ส่วนใหญ่ไม่ได้ขาดข้อมูล แต่จมอยู่กับ Alert จำนวนมากที่ต้องเปิดดูทีละรายการ ต้องสลับหน้าจอไปค้นข้อมูล IP หรือ Hash เขียน Query ใหม่ทุกครั้งที่ต้องล่าภัยคุกคาม และใช้เวลานานกับการสรุปเหตุการณ์เป็นรายงาน AI และ LLM ช่วยงานเหล่านี้ได้มาก แต่ถ้านำมาใช้โดยไม่ครอบ ก็เสี่ยงทั้งคำตอบที่ฟังดูถูกแต่ผิด ข้อมูล Log ที่มีข้อมูลส่วนบุคคลหลุดออกไปยังบริการภายนอก และผู้โจมตีที่ฝังคำสั่งไว้ใน Log เพื่อหลอก AI

หลักสูตรนี้ต่อยอดจาก SOC and SIEM with Wazuh โดยไม่ทวนการติดตั้งและพื้นฐานของ Wazuh แต่พาผู้เรียนนำ AI เข้าไปช่วยทุกขั้นของงาน SOC เริ่มจากต่อ Wazuh เข้ากับ LLM ที่รันบนเครื่อง ออกแบบ Prompt คัดกรอง Alert ที่ให้ผลเป็นโครงสร้างและวัดความแม่นยำได้ เติมข้อมูล Threat Intelligence สร้าง Pipeline คัดกรองอัตโนมัติด้วย n8n จากนั้นใช้ AI ช่วยล่าภัยคุกคาม เชื่อม Wazuh กับ AI Agent ผ่าน MCP ร่าง Timeline และรายงานเหตุการณ์ และหาช่องว่างของการตรวจจับตาม MITRE ATT&CK ทุกขั้นมีมนุษย์ตรวจทานก่อนตัดสินใจ และปิดท้ายด้วย Capstone ศูนย์ SOC จำลองที่มี AI ช่วยงาน (อบรม 2 วัน วันละ 6 ชั่วโมง รวม 12 ชั่วโมง ระดับ Intermediate)

เครื่องมือ

Wz Wazuh

GPT LLM

MT MITRE ATT&CK

n8n n8n

Py Python

ราคาค่าอบรม · PUBLIC / IN-HOUSE

8,900 บาท / ท่าน

ราคายังไม่รวมภาษีมูลค่าเพิ่ม (VAT 7%) · รวมเอกสารประกอบการอบรม Lab Guide ชุด Prompt สำหรับงาน SOC ไฟล์ Workflow ของ n8n สคริปต์ Python และ Certificate · รับจัด In-house ขอใบเสนอราคาได้

สมัครผ่านเว็บไซต์ ลด 10%



เพิ่มเพื่อน
LINE

☎ 02-570-8449

☎ 088-807-9770

LINE @itgenius

🌐 www.itgenius.co.th

01 วัตถุประสงค์ Objectives

- ประเมินว่างาน SOC ส่วนใดควรใช้ AI ช่วย ส่วนใดต้องให้มนุษย์ตัดสินใจ
- เชื่อม Wazuh เข้ากับ LLM บนเครื่องหรือผ่าน API โดยคำนึงถึงข้อมูลส่วนบุคคลใน Log
- ออกแบบ Prompt คัดกรอง Alert ที่ให้ผลเป็นโครงสร้างและวัดความแม่นยำได้
- สร้าง Pipeline คัดกรองและเติมข้อมูล Alert อัตโนมัติด้วย n8n พร้อมขั้นตอนุมัติ
- ใช้ AI ช่วยเขียน Query ล่าภัยคุกคาม พร้อมตรวจสอบผลก่อนนำไปใช้
- เชื่อม Wazuh กับ AI Agent ผ่าน MCP โดยกำหนดสิทธิ์อย่างปลอดภัย
- ใช้ AI ช่วยร่าง Timeline รายงานเหตุการณ์ และ Rule ตรวจจับใหม่
- รู้จักความเสี่ยงของ AI ใน SOC เช่น Prompt Injection จาก Log และวางมาตรการควบคุม

02 กลุ่มเป้าหมาย Target Audience

- SOC Analyst ระดับ Tier 1 และ Tier 2 ที่ต้องการลดเวลาคัดกรองและสืบสวน Alert
- ผู้ดูแล Wazuh หรือ SIEM ที่ต้องการนำ LLM มาช่วยงานตรวจจับและวิเคราะห์ Log
- Incident Responder และ Threat Hunter ที่อยากใช้ AI ช่วยวิเคราะห์และเขียนรายงาน
- หัวหน้าทีม SOC ที่ต้องวางแผนทางการใช้ AI ในทีมอย่างปลอดภัย
- ผู้ที่ผ่านหลักสูตร SOC and SIEM with Wazuh หรือมีประสบการณ์ใกล้เคียง

03 จุดเด่นของหลักสูตร Highlights

- **ต่อยอดจาก Wazuh** ไม่ทวนพื้นฐาน เริ่มที่การใช้ AI กันที่
- **LLM บนเครื่อง** Log ไม่ต้องออกนอกองค์กร
- **คัดกรองอัตโนมัติ** n8n, Threat Intel และขั้นตอนุมัติ
- **AI Agent ผ่าน MCP** ตาม Wazuh ด้วยภาษาธรรมชาติ
- **มีมนุษย์ตรวจทาน** วัดความแม่นยำและกันการหลอก AI

04 ความรู้พื้นฐาน Prerequisites

- ใช้งาน Wazuh ได้ เข้าใจ Agent, Decoder, Rule และ Dashboard หรือผ่านหลักสูตร SOC and SIEM with Wazuh
- เข้าใจขั้นตอนงาน SOC และ MITRE ATT&CK เบื้องต้น
- เขียน Python ขั้นพื้นฐานและใช้ Command Line บน Linux ได้
- โน้ตบุ๊ก RAM อย่างน้อย 16 GB ที่ติดตั้ง Docker Desktop ได้ พร้อมสิทธิ์ติดตั้งโปรแกรม

05 สิ่งที่ต้องเตรียมและเครื่องมือ Setup & Tools

รายการ	รายละเอียด
อุปกรณ์	Notebook RAM 16 GB ขึ้นไป ติดตั้ง Docker Desktop และ Docker Compose ได้
SIEM	Wazuh 4.14 แบบ Single-node บน Docker พร้อมข้อมูล Alert ตัวอย่าง
LLM	โมเดลขนาดเล็กผ่าน Ollama บนเครื่อง หรือ LLM API Key ของผู้เรียน
Automation	n8n แบบ Self-host, Python และ MCP Server ของ Wazuh จากชุมชนโอเพนซอร์ส
Threat Intel	บริการ Threat Intelligence แบบใช้ฟรี เช่น VirusTotal และ AbuseIPDB

หมายเหตุ: หลักสูตรนี้ต่อยอดจาก SOC and SIEM with Wazuh และไม่ทวนการติดตั้งหรือการเขียน Rule พื้นฐาน เครื่องมือหลักเป็นโอเพนซอร์ส ทุก Lab รันบนเครื่องของผู้เรียน บริการ Threat Intelligence ใช้บัญชีแบบฟรีของผู้เรียนเอง และหากใช้ LLM เชิงพาณิชย์ ผู้เรียนใช้ API Key ของตนเองหรือของบริษัท ค่าใช้ API เป็นไปตามการใช้งานจริง ข้อมูล Log ใน Lab เป็นข้อมูลจำลอง ชื่อเครื่องมือและฟีเจอร์ด้าน AI เปลี่ยนเร็ว เนื้อหาจะอัปเดตตามเวอร์ชันล่าสุด ณ วันอบรม

06 ภาพรวมการเรียนรู้ 2 วัน Big Picture

วัน	หัวข้อหลัก
Day 1 Section 1-6	วางแผนเขตการใช้ AI ใน SOC อย่างปลอดภัย, ต่อ Wazuh เข้ากับ LLM บนเครื่อง, ออกแบบ Prompt คัดกรอง Alert แบบมีโครงสร้าง, เพิ่มข้อมูล Threat Intelligence, สร้าง Pipeline คัดกรองอัตโนมัติด้วย n8n และให้ AI ช่วยร่าง Decoder กับ Rule
Day 2 Section 7-12	ล่าภัยคุกคามด้วยภาษาธรรมชาติ, เชื่อม Wazuh กับ AI Agent ผ่าน MCP, ใช้ AI ช่วย Incident Response และ Detection Engineering, กำกับความเสี่ยงของ AI ใน SOC และ Capstone ศูนย์ SOC ที่มี AI ช่วยงาน

DAY
1

AI ช่วยคัดกรองและวิเคราะห์ Alert

เนื้อหาการอบรม · Section 1-6

รวม
6 ชั่วโมง

1 AI ในงาน SOC: ช่วยได้แค่ไหน เสี่ยงตรงไหน

- งาน SOC ที่ AI ช่วยได้ดี: สรุป Alert, เต็มบริบท, เขียน Query และร่างรายงาน
- งานที่ต้องให้มนุษย์ตัดสินใจ และเหตุผลที่ไม่ควรให้ AI สั่ง Active Response เอง
- ปัญหาคำตอบที่ฟังดูถูกแต่ผิด และวิธีบังคับให้ AI อ้างหลักฐานจาก Log
- Log มีข้อมูลส่วนบุคคล: เลือก LLM บนเครื่องหรือบริการภายนอกตามระดับชั้นข้อมูลและ PDPA

2 Lab: เชื่อม Wazuh กับ LLM บนเครื่อง

- นำ Wazuh 4.14 บน Docker จาก Lab เดิมกลับมาใช้ พร้อมชุด Alert จำลอง
- ติดตั้ง Ollama และเลือกโมเดลขนาดเล็กให้เหมาะกับงานวิเคราะห์ Log
- ดึง Alert ผ่าน Wazuh Server API และค้นข้อมูลจาก Wazuh Indexer ด้วย Python
- Lab: ให้ LLM สรุป Alert ระดับสูงล่าสุดเป็นภาษาไทยที่ทีมอ่านเข้าใจ

3 Lab: Prompt สำหรับคัดกรอง Alert

- ออกแบบ Prompt ที่ให้ผลเป็น JSON: ความรุนแรง, Technique ของ ATT&CK และเหตุผล
- ให้ AI แยก False Positive พร้อมหลักฐานที่ตรวจสอบย้อนกลับได้
- วัดความแม่นยำเทียบกับชุด Alert ที่มีคำตอบ แล้วปรับ Prompt ตามผล
- Lab: สร้างชุดทดสอบ Alert 30 รายการ แล้วเปรียบเทียบ Prompt สองแบบ

4 Lab: เต็มบริบทด้วย Threat Intelligence

- ตรวจสอบ IP, Domain และ Hash จาก Alert กับบริการ Threat Intelligence แบบใช้ฟรี
- รวมข้อมูล Asset, เจ้าของเครื่อง และประวัติ Alert เดิมเข้ากับผลวิเคราะห์
- ให้ AI สรุปผลจากหลายแหล่งเป็นข้อแนะนำเดียว โดยระบุแหล่งที่มาทุกข้อ
- Lab: เพิ่มข้อมูลให้ Alert การเชื่อมต่อออกไปยัง IP ต้องสงสัยแล้วสรุปความเสี่ยง

5 Lab: Pipeline คัดกรองอัตโนมัติด้วย n8n

- ส่ง Alert จาก Wazuh เข้า n8n ผ่าน Custom Integration แบบ Webhook
- ต่อขั้นตอนเพิ่มข้อมูล วิเคราะห์ด้วย LLM และจัดระดับความเร่งด่วน
- เพิ่มขั้นตอนอนุมัติจากมนุษย์ก่อนทำงานที่มีผลต่อระบบ
- Lab: Workflow ที่คัดกรอง Alert SSH Brute Force และขออนุมัติก่อนบล็อก IP

6 Lab: AI ช่วยวิเคราะห์ Log และเขียน Rule

- ร่าง Custom Decoder และ Rule ของ Wazuh จากตัวอย่าง Log
- ทดสอบทุก Rule ที่ AI ร่างด้วย wazuh-logtest ก่อนใช้งานจริง
- แปลงแนวคิดจาก Sigma Rule เป็น Rule ของ Wazuh แล้วตรวจสอบผลด้วยตนเอง
- Lab: สร้าง Rule ตรวจสอบการใช้ API ผิดปกติจาก Log ของแอปตัวอย่าง

DAY
2

Threat Hunting, Incident Response และ SOC Agent

เนื้อหาการอบรม · Section 7-12

รวม
6 ชั่วโมง

7 Lab: Threat Hunting ด้วยภาษาธรรมชาติ

- ตั้งสมมติฐานการล่าจาก Technique ของ MITRE ATT&CK ด้วยความช่วยเหลือของ AI
- แปลงคำถามภาษาธรรมชาติเป็น Query สำหรับค้นข้อมูลใน Wazuh Indexer
- ตรวจสอบ Query ที่ AI เขียนก่อนรัน และเทียบผลกับการค้นด้วยมือ
- Lab: ล่าร่องรอย Persistence บน Windows จากข้อมูล Sysmon

8 Lab: เชื่อม Wazuh กับ AI Agent ผ่าน MCP

- แนวคิด Model Context Protocol และ MCP Server ของ Wazuh จากชุมชนโอเพนซอร์ส
- ตั้งค่า MCP Server ให้ AI Agent ค้น Alert, สถานะ Agent และช่องโหว่ได้
- เริ่มจากสิทธิ์อ่านอย่างเดียว ใช้บัญชี API แยก และบันทึกทุกคำสั่งที่ Agent เรียก
- Lab: ให้ Agent ตอบคำถามเช่น เครื่องใดมี Alert ระดับสูงในหนึ่งวันที่ผ่านมา

9 Lab: AI ช่วย Incident Response

- รวบรวม Alert และ Log ที่เกี่ยวข้องให้ AI เรียงเป็น Timeline ของเหตุการณ์
- ร่างรายงานเหตุการณ์สองระดับ: รายละเอียดเชิงเทคนิค และสรุปสำหรับผู้บริหาร
- ตรวจสอบความถูกต้องของทุกข้อสรุปเทียบกับหลักฐานก่อนส่งต่อ
- Lab: สร้าง Timeline และรายงานจากชุดเหตุการณ์ Brute Force ถึงการสร้างบัญชีปลอม

10 Lab: Detection Engineering ด้วย AI

- หาช่องว่างของการตรวจจับโดยเทียบ Rule ที่มีอยู่กับ MITRE ATT&CK
- ให้ AI เสนอ Rule ใหม่พร้อมตัวอย่าง Log ที่ควรจับได้และไม่ควรจับ
- สร้างชุดทดสอบ Rule เพื่อป้องกันการแก้ไข Rule แล้วการตรวจจับเดิมหาย
- Lab: ปิดช่องว่างการตรวจจับหนึ่ง Technique ตั้งแต่ร่าง Rule จนผ่านการทดสอบ

11 กำกับความเสี่ยงของ AI ใน SOC

- Prompt Injection ผ่าน Field ใน Log เช่น User-Agent หรือชื่อไฟล์ และวิธีลดผลกระทบ
- นโยบายข้อมูล: ข้อมูลใดส่งให้ LLM ภายนอกได้ และข้อมูลใดต้องอยู่ในองค์กร
- วัดผลการใช้ AI: เวลาคิดกรอง, MTTR, ความแม่นยำ และค่าใช้จ่าย
- Workshop: เขียนแนวทางการใช้ AI สำหรับทีม SOC ขององค์กร

12 Workshop: Capstone SOC ที่มี AI ช่วยงาน

- รับชุดเหตุการณ์จำลองหลายขั้นตอนจากวิทยากร
- คิดกรองผ่าน Pipeline อัตโนมัติ และสืบสวนต่อด้วย AI Agent
- ล่าร่องรอยเพิ่มเติม ควบคุมเหตุการณ์ตาม Playbook และเสนอ Rule ใหม่
- นำเสนอรายงานเหตุการณ์ พร้อมชี้จุดที่ AI ช่วยได้และจุดที่ AI พลาด

07 เรียนจบแล้วได้อะไร Outcomes

- ใช้ AI คัดกรอง Alert ผลแบบมีโครงสร้างและวัดความแม่นยำได้
- สร้าง Pipeline อัตโนมัติ Wazuh, n8n, Threat Intel และ LLM
- ลำกัยคุกคามได้เร็วขึ้น แปลงคำถามเป็น Query อย่างตรวจสอบได้
- ต่อ AI Agent กับ SIEM MCP พร้อมสิทธิ์ที่ปลอดภัย
- เขียนรายงานเร็วขึ้น Timeline และสรุปสำหรับผู้บริหาร
- กำกับการใช้ AI ข้อมูล, Prompt Injection และการวัดผล

08 สิ่งที่คุณเรียนจะได้รับ Deliverables

- เอกสารประกอบการอบรมฉบับสมบูรณ์ครบทั้ง 2 วัน และ Lab Guide ที่ละขั้นตอน
- ชุด Prompt สำหรับคัดกรอง Alert ลำกัยคุกคาม และเขียนรายงานเหตุการณ์
- ไฟล์ Workflow ของ n8n และสคริปต์ Python สำหรับเชื่อม Wazuh กับ LLM
- แม่แบบแนวทางการใช้ AI ในทีม SOC และ Checklist ก่อนใช้งานจริง
- ประกาศนียบัตรจบหลักสูตร (Certificate of Completion) และช่องทางสอบถามวิทยากรหลังจบหลักสูตร

09 ข้อมูลผู้สอน Instructor

อ.สามิตร โกยม ผู้สอนและผู้ปฏิบัติงานด้าน Security Operations ที่ใช้ SIEM ร่วมกับเครื่องมืออัตโนมัติและ AI ในงานตรวจจับและตอบสนองเหตุการณ์ จุดเด่นคือการสอนจากขั้นตอนงานจริงของทีม SOC ให้ผู้เรียนเห็นว่า AI ช่วยลดงานซ้ำได้ตรงไหน และต้องตรวจสอบตรงไหน ทุก Lab ให้วัดผลเทียบกับการทำงานแบบเดิม เพื่อให้กลับไปนำ AI เข้าทีมได้อย่างมีประสิทธิภาพและปลอดภัย

ราคาค่าอบรม 8,900 บาท/ท่าน · สนใจ IN-HOUSE ขอใบเสนอราคา

8,900 บาท / ท่าน (ยังไม่รวม VAT 7%)

สมัครผ่านเว็บไซต์ ลด 10%

☎ 02-570-8449

☎ 088-807-9770

📞 @itgenius

✉ contact@itgenius.co.th



เพิ่มเพื่อน
LINE