



# SOC and SIEM with Wazuh

สร้างระบบเฝ้าระวังและตอบสนองภัยคุกคามแบบ Blue Team ด้วย Wazuh

● 18 ชั่วโมง

● 3 วัน

● พื้นฐาน Linux, Windows และ Network

● ระดับ Intermediate



**ระยะเวลา: 3 วัน**

18 ชั่วโมง (3 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](http://www.itgenius.co.th)

องค์กรจำนวนมากมีไฟร์วอลล์และแอนตี้ไวรัสแล้ว แต่ยังไม่รู้ว่าเกิดอะไรขึ้นบนเครื่องและเซิร์ฟเวอร์ของตนเองในแต่ละวัน Log กระจายอยู่หลายที่ไม่มีใครดูจนกว่าระบบจะล่ม พอเกิดเหตุจริงก็ไม่ว่าผู้โจมตีเข้ามาทางไหนและทำอะไรไปแล้วบ้าง งานของทีม Blue Team และ SOC คือทำให้มองเห็นเหตุการณ์เหล่านี้ตั้งแต่ต้น และตอบสนองได้ทันก่อนความเสียหายจะลุกลาม

หลักสูตรนี้พาผู้เรียนสร้างระบบเฝ้าระวังความปลอดภัยของตนเองด้วย Wazuh แพลตฟอร์ม SIEM และ XDR แบบโอเพนซอร์ส เริ่มจากทำความเข้าใจบทบาทและขั้นตอนงานของ SOC ติดตั้ง Wazuh Indexer, Server และ Dashboard ด้วย Docker ติดตั้ง Agent บน Linux และ Windows แล้วรวบรวม Log จาก Syslog, Windows Event และ Sysmon จากนั้นจะทำการเขียน Decoder และ Rule เอง File Integrity Monitoring, Vulnerability Detection, Security Configuration Assessment และการจับคู่กับ MITRE ATT&CK ก่อนต่อยอดสู่ Active Response การแจ้งเตือน Threat Hunting และการจำลองการโจมตีเพื่อฝึกตอบสนองเหตุการณ์ตาม Playbook แล้วปิดท้ายด้วย Capstone ที่ผู้เรียนรับบทเป็นทีม SOC ตลอดทั้งเหตุการณ์ (อบรม 3 วัน วันละ 6 ชั่วโมง รวม 18 ชั่วโมง ระดับ Intermediate)

เครื่องมือ

Wz Wazuh

SI SIEM

SOC SOC

AT MITRE ATT&CK

IR Incident Response

ราคาค่าอบรม · PUBLIC / IN-HOUSE

**9,900** บาท / ท่าน

ราคายังไม่รวมภาษีมูลค่าเพิ่ม (VAT 7%) · รวมเอกสารประกอบการอบรม Lab Guide ไฟล์ docker-compose ชุด Rule และ Decoder ตัวอย่าง แม่แบบ Playbook และ Certificate · รับจัด In-house ขอใบเสนอราคาได้

สมัครผ่านเว็บไซต์ ลด 10%



เพิ่มเพื่อน  
LINE

## 01 วัตถุประสงค์ Objectives

- เข้าใจบทบาท ขั้นตอนงาน และตัวชี้วัดของ SOC รวมถึงแนวคิด SIEM และ XDR
- ติดตั้ง Wazuh ด้วย Docker และติดตั้ง Agent บน Linux และ Windows ได้
- รวบรวม Log จาก Syslog, Windows Event และ Sysmon เข้าสู่ Wazuh ได้ครบถ้วน
- อ่าน Decoder และ Rule ที่มีอยู่ และเขียน Custom Rule ให้ตรงกับระบบขององค์กร
- ใช้ FIM, Vulnerability Detection และ SCA ตรวจสอบความเสี่ยงของเครื่องในองค์กร
- จับคู่ Alert กับ MITRE ATT&CK และทำ Threat Hunting จากข้อมูลใน Wazuh
- ตั้ง Active Response และส่งการแจ้งเตือนไปยังอีเมล Slack หรือ Webhook
- ตอบสนองเหตุการณ์ตาม Incident Response Playbook ที่เขียนขึ้นเองได้

## 02 กลุ่มเป้าหมาย Target Audience

- ผู้ดูแลระบบและผู้ดูแลเครือข่ายที่ต้องรับผิดชอบงานความปลอดภัยขององค์กร
- SOC Analyst ระดับเริ่มต้นและผู้ที่ต้องการเข้าสู่สาย Blue Team
- ทีม IT Security ที่ต้องการระบบ SIEM แบบโอเพนซอร์สสำหรับองค์กร
- DevOps และ Cloud Engineer ที่ต้องเฝ้าระวังเซิร์ฟเวอร์และ Container
- ผู้ที่เรียนด้าน Ethical Hacking แล้วอยากเข้าใจมุมมองการป้องกันและตรวจจับ

## 03 จุดเด่นของหลักสูตร Highlights

- มุมมอง **Blue Team เต็มรูปแบบ** ตรวจจับ วิเคราะห์ และตอบสนองเหตุการณ์
- สร้าง **SOC Lab ของตัวเอง** Wazuh บน Docker พร้อม Agent หลายระบบ
- เขียน **Rule ได้เอง** Decoder และ Custom Rule ตามระบบจริง
- เชื่อมกับ **MITRE ATT&CK** เข้าใจ Alert ในมุมมองเทคนิคของผู้โจมตี
- ฝึกรับมือเหตุการณ์จริง จำลองการโจมตีและใช้ Playbook ตอบสนอง

#### 04 ความรู้พื้นฐาน Prerequisites

- ใช้งาน Linux Command Line และ Windows ในระดับผู้ดูแลระบบเบื้องต้นได้
- เข้าใจพื้นฐาน Network เช่น IP, Port, Protocol และ DNS
- มีความรู้พื้นฐานด้านความปลอดภัย เช่น Malware, Brute Force และ Firewall
- โน้ตบุ๊ก RAM อย่างน้อย 16 GB ที่ติดตั้ง Docker Desktop หรือ VirtualBox ได้ พร้อมสิทธิ์ Admin

#### 05 สิ่งที่ต้องเตรียมและเครื่องมือ Setup & Tools

| รายการ          | รายละเอียด                                                                 |
|-----------------|----------------------------------------------------------------------------|
| อุปกรณ์         | Notebook RAM 16 GB ขึ้นไป เชื่อมต่ออินเทอร์เน็ต ติดตั้ง Docker Desktop ได้ |
| แพลตฟอร์มหลัก   | Wazuh Indexer, Wazuh Server และ Wazuh Dashboard แบบ Single-node บน Docker  |
| เครื่องใน Lab   | Linux VM หรือ Container และ Windows VM สำหรับติดตั้ง Wazuh Agent           |
| เครื่องมือเสริม | Sysmon, ไฟล์ทดสอบ EICAR, Hydra สำหรับจำลอง Brute Force และ Slack Webhook   |
| เอกสารอ้างอิง   | MITRE ATT&CK Matrix และแม่แบบ Incident Response Playbook                   |

**หมายเหตุ:** เครื่องมือทั้งหมดเป็นโอเพนซอร์สหรือมีแบบใช้ฟรี ทุก Lab ทำงานในสภาพแวดล้อมจำลองบนเครื่องของผู้เรียน การจำลองการโจมตีทำเฉพาะกับเครื่องใน Lab ที่ได้รับอนุญาตเท่านั้น หลักสูตรนี้เน้นมุมมองการป้องกันและตรวจจับ จึงเสริมกับหลักสูตรด้าน Ethical Hacking ที่เน้นมุมมองการโจมตีได้ดี และไม่ครอบคลุมการติดตั้ง Wazuh แบบ Cluster ขนาดใหญ่สำหรับ Production

#### 06 ภาพรวมการเรียนรู้ 3 วัน Big Picture

| วัน                           | หัวข้อหลัก                                                                                                                                                                       |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Day 1</b><br>Section 1-5   | เข้าใจบทบาทและขั้นตอนงานของ SOC, แนวคิด SIEM และ XDR, สถาปัตยกรรม Wazuh, ติดตั้งด้วย Docker, ติดตั้ง Agent บน Linux และ Windows และเก็บ Log จาก Syslog, Windows Event และ Sysmon |
| <b>Day 2</b><br>Section 6-10  | อ่านและเขียน Decoder กับ Rule เอง, File Integrity Monitoring, Vulnerability Detection, Security Configuration Assessment และจับคู่ Alert กับ MITRE ATT&CK                        |
| <b>Day 3</b><br>Section 11-15 | ตั้ง Active Response, ส่ง Alert ไปอีเมล Slack และ Webhook, Threat Hunting เบื้องต้น, จำลองการโจมตีใน Lab, เขียน Incident Response Playbook และปิดท้ายด้วย Capstone SOC จำลอง     |

DAY  
1

## พื้นฐาน SOC และติดตั้ง Wazuh

เนื้อหาการอบรม · Section 1-5

รวม  
6 ชั่วโมง

### 1 SOC และบทบาทของ Blue Team

- SOC คืออะไร และบทบาทของ Analyst ระดับ Tier 1 ถึง Tier 3
- ขั้นตอนงานของ SOC ตั้งแต่ตรวจจับ คัดกรอง วิเคราะห์ จนถึงตอบสนอง
- ตัวชี้วัดที่ใช้วัดงาน SOC เช่น MTTD และ MTTR
- ปัญหา Alert Fatigue และแนวทางลด False Positive
- ภาพรวมภัยคุกคามที่องค์กรไทยพบบ่อย และสิ่งที่ SOC ต้องมองเห็น

### 2 แนวคิด SIEM, XDR และสถาปัตยกรรม Wazuh

- SIEM, EDR และ XDR ต่างกันอย่างไร และทำงานร่วมกันแบบไหน
- องค์ประกอบของ Wazuh: Indexer, Server, Dashboard และ Agent
- เส้นทางของข้อมูลจาก Agent ผ่าน Decoder และ Rule จนกลายเป็น Alert
- รูปแบบการติดตั้งแบบ All-in-one, Distributed และบน Docker
- การวางแผนขนาดเครื่องและการเก็บข้อมูลย้อนหลัง

### 3 Lab: ติดตั้ง Wazuh ด้วย Docker

- เตรียมเครื่องและค่าระบบที่ Wazuh Indexer ต้องการ
- ติดตั้ง Wazuh แบบ Single-node ด้วย Docker Compose
- สร้าง Certificate และเปลี่ยนรหัสผ่านเริ่มต้นให้ปลอดภัย
- สำรวจ Wazuh Dashboard: Overview, Endpoint และ Module ต่าง ๆ
- Lab: ตรวจสอบสถานะ Service และแก้ปัญหาการติดตั้งที่พบบ่อย

### 4 Lab: ติดตั้ง Agent บน Linux และ Windows

- ลงทะเบียน Agent และการสื่อสารระหว่าง Agent กับ Server
- ติดตั้ง Agent บน Linux และ Windows ผ่านคำสั่งที่ Dashboard สร้างให้
- จัดกลุ่ม Agent และใช้ Centralized Configuration ผ่าน agent.conf
- ตรวจสอบสถานะ Agent และแก้ปัญหา Agent ที่ไม่เชื่อมต่อ
- Lab: นำเครื่อง Linux และ Windows เข้าระบบและดูเหตุการณ์แรก

### 5 Lab: เก็บ Log จาก Syslog, Windows Event และ Sysmon

- เก็บ Log จากไฟล์บน Linux และรับ Syslog จากอุปกรณ์เครือข่าย
- เลือก Windows Event Channel ที่สำคัญต่องานความปลอดภัย
- ติดตั้ง Sysmon พร้อม Configuration ที่เหมาะสม และส่ง Event เข้า Wazuh
- ค้นหาและกรองเหตุการณ์ใน Dashboard ด้วย Query และ Filter
- Lab: ติดตาม Process และการเชื่อมต่อเครือข่ายบน Windows ผ่าน Sysmon

DAY  
2

## ตรวจจับภัยคุกคามและประเมินความเสี่ยง

เนื้อหาการอบรม · Section 6-10

รวม  
6 ชั่วโมง

### 6 Decoder และ Rule ของ Wazuh

- โครงสร้าง Decoder และวิธีแยก Field ออกจาก Log
- โครงสร้าง Rule: Level, Group, If\_sid และ Frequency
- ทดสอบ Log กับ Decoder และ Rule ด้วยเครื่องมือ wazuh-logtest
- ลำดับการทำงานของ Rule และการปรับ Level ให้เหมาะกับองค์กร
- Lab: ไล่ดู Rule ของเหตุการณ์ SSH Login ล้มเหลวทีละขั้น

### 7 Lab: เขียน Custom Decoder และ Custom Rule

- เขียน Decoder สำหรับ Log ของแอปพลิเคชันภายในองค์กร
- เขียน Rule ตรวจจับพฤติกรรมผิดปกติที่ต่อยอดจาก Rule เดิม
- Rule แบบนับความถี่ตามช่วงเวลาสำหรับเหตุการณ์ซ้ำ
- ลด False Positive ด้วยการยกเว้นและปรับเงื่อนไข Rule
- Lab: ตรวจจับการเข้าสู่ระบบผิดปกติจาก Log ของเว็บแอปตัวอย่าง

### 8 Lab: File Integrity Monitoring

- หลักการของ FIM และไฟล์หรือโฟลเดอร์ที่ควรเฝ้าระวัง
- ตั้งค่า syscheck แบบ Scheduled และ Real-time
- ติดตามว่าใครแก้ไขไฟล์ด้วยโหมด Who-data บน Linux และ Windows
- เฝ้าระวัง Windows Registry ที่ผู้โจมตีมักใช้ฝังตัว
- Lab: จับการแก้ไขไฟล์เว็บและไฟล์ตั้งค่าที่สำคัญ

### 9 Lab: Vulnerability Detection และ SCA

- Vulnerability Detection ตรวจช่องโหว่จากรายการซอฟต์แวร์บนเครื่องอย่างไร
- อ่านรายงานช่องโหว่ จัดลำดับความสำคัญตามความรุนแรง และวางแผนแพตช์
- Security Configuration Assessment กับ Policy ตามแนวทาง CIS Benchmark
- ปรับแต่งหรือเขียน SCA Policy ให้ตรงมาตรฐานขององค์กร
- Lab: ประเมินและแก้ไขค่าความปลอดภัยของเครื่อง Linux ตามผล SCA

### 10 MITRE ATT&CK กับ Wazuh

- โครงสร้าง MITRE ATT&CK: Tactic, Technique และ Sub-technique
- วิธีที่ Wazuh จับคู่ Rule กับ Technique ของ ATT&CK
- ใช้ ATT&CK Dashboard ดูภาพรวมเทคนิคที่เกิดขึ้นในองค์กร
- เพิ่ม MITRE ID ให้กับ Custom Rule ที่เขียนเอง
- Lab: หาช่องว่างของการตรวจจับจาก ATT&CK Matrix



DAY  
3

## ตอบสนองเหตุการณ์และ SOC ในงานจริง

เนื้อหาการอบรม · Section 11-15

รวม  
6 ชั่วโมง

### 11 Lab: Active Response

- แนวคิด Active Response และความเสี่ยงของการตอบสนองอัตโนมัติ
- ใช้ Script สำเร็จรูป เช่น บล็อก IP ด้วย Firewall
- กำหนดเงื่อนไข ระยะเวลา และเครื่องที่ Active Response จะทำงาน
- เขียน Custom Active Response Script อย่างง่าย
- Lab: บล็อก IP ที่ Brute Force SSH โดยอัตโนมัติ

### 12 Lab: การแจ้งเตือนและ Integration

- ตั้งค่าการส่ง Alert ทางอีเมลตาม Level และ Group ของ Rule
- เชื่อม Wazuh กับ Slack ผ่าน Integration ที่มีมาในตัว
- เขียน Custom Integration ส่ง Alert ไปยัง Webhook ของระบบแชตหรือระบบ Ticket
- ออกแบบระดับการแจ้งเตือนเพื่อลด Alert Fatigue ของทีม
- Lab: ส่ง Alert สำคัญเข้าช่องแชตของทีม SOC

### 13 Threat Hunting เบื้องต้น

- ความต่างระหว่าง Alert กับการออกล่าภัยคุกคามเชิงรุก
- ตั้งสมมติฐานการล่าจากเทคนิคใน MITRE ATT&CK
- ค้นหาร่องรอยใน Wazuh Dashboard ด้วย Query และ Visualization
- ใช้ IOC เช่น Hash, IP และ Domain ในการค้นหา
- Lab: ล่าร่องรอย PowerShell ที่น่าสงสัยจากข้อมูล Sysmon

### 14 Lab: จำลองการโจมตีและ Incident Response

- วงจร Incident Response: เตรียมพร้อม ตรวจสอบ ควบคุม กำจัด และฟื้นฟู
- จำลอง Brute Force และสร้างบัญชีผู้ใช้แปลกปลอมบนเครื่องใน Lab
- จำลองการวางไฟล์ Malware ทดสอบ (EICAR) และติดตามการตรวจจับ
- สืบสวนเหตุการณ์จาก Alert และสร้าง Timeline ของการโจมตี
- เขียน Incident Response Playbook สำหรับเหตุการณ์ที่พบบ่อย

### 15 Workshop: Capstone SOC จำลอง

- รับบทเป็นทีม SOC ตรวจสอบและวิเคราะห์ชุดการโจมตีที่วิทยากรจำลองขึ้น
- คัดกรอง Alert แยก False Positive และประเมินความรุนแรง
- ควบคุมเหตุการณ์ด้วย Active Response และมาตรการตาม Playbook
- เขียนรายงานเหตุการณ์และข้อเสนอปรับปรุงการตรวจจับ
- Checklist ก่อนนำ Wazuh ไปใช้งานจริงในองค์กร

## 07 เรียนจบแล้วได้อะไร Outcomes

- เข้าใจงาน **SOC** บทบาท ขั้นตอน และตัวชี้วัด
- ติดตั้งและดูแล **Wazuh** Docker, Agent และการเก็บ Log
- เขียน **Rule** ตรวจสอบตัวเอง Decoder, Custom Rule และลด False Positive
- ประเมินความเสี่ยงของเครื่อง FIM, Vulnerability Detection และ SCA
- ตอบสนองได้รวดเร็ว Active Response และการแจ้งเตือน
- รับมือเหตุการณ์เป็นระบบ Threat Hunting และ Playbook

## 08 สิ่งที่คุณเรียนจะได้รับ Deliverables

- เอกสารประกอบการอบรมฉบับสมบูรณ์ครบทั้ง 3 วัน และ Lab Guide ทีละขั้นตอน
- ไฟล์ docker-compose สำหรับ Wazuh และ Configuration ของ Agent และ Sysmon
- ชุด Custom Decoder, Custom Rule และสคริปต์ Active Response ตัวอย่าง
- แม่แบบ Incident Response Playbook และรายงานเหตุการณ์
- ประกาศนียบัตรจบหลักสูตร (Certificate of Completion) และช่องทางสอบถามวิทยากรหลังจบหลักสูตร

## 09 ข้อมูลผู้สอน Instructor

**อ.สามิตร โกยม** ผู้สอนและผู้ปฏิบัติงานด้านความปลอดภัยที่ออกแบบและดูแลระบบเฝ้าระวังด้วย Wazuh ให้กับองค์กรจริง ทั้งการเก็บ Log การเขียน Rule และการตอบสนองเหตุการณ์ จุดเด่นคือการสอนผ่าน Lab ที่จำลองการโจมตีให้ผู้เรียนเห็นร่องรอยจริงบนหน้าจอ แล้วพาคิดแบบ Analyst ว่า Alert ใดสำคัญ ต้องสืบต่ออย่างไร และควรตอบสนองแค่ไหน เพื่อให้กลับไปวางระบบเฝ้าระวังในองค์กรของตนเองได้ทันที

ราคาค่าอบรม 9,900 บาท/ท่าน · สนใจ IN-HOUSE ขอใบเสนอราคา

**9,900 บาท** / ท่าน (ยังไม่รวม VAT 7%)

สมัครผ่านเว็บไซต์ ลด 10%

☎ 02-570-8449

LINE @itgenius

☎ 088-807-9770

✉ contact@itgenius.co.th



เพิ่มเพื่อน  
LINE