



CompTIA Security+ for Developers

เข้าใจภัยคุกคาม เขียนโค้ดปลอดภัย และรับมือเหตุการณ์ตามกรอบ Security+

● 30 ชั่วโมง

● 5 วัน

● พื้นฐาน Web Application, เครือข่าย, Git และ Docker เบื้องต้น

● ระดับ Intermediate



ระยะเวลา: 5 วัน

30 ชั่วโมง (5 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

ช่องโหว่จำนวนมากเกิดขึ้นตั้งแต่ขั้นตอนการพัฒนา ไม่ว่าจะเป็นการตรวจสอบ Input ที่ไม่รัดกุม การฝัง Secret ไว้ในโค้ด การให้สิทธิ์เกินจำเป็น หรือการใช้ Library ที่มีช่องโหว่ ขณะเดียวกันภัยคุกคามที่เกี่ยวข้องกับ AI เช่น Prompt Injection และการรั่วไหลของข้อมูลผ่านโมเดล ก็เริ่มส่งผลกระทบต่อระบบที่นักพัฒนาสร้างโดยตรง องค์กรจึงต้องการนักพัฒนาที่เข้าใจความมั่นคงปลอดภัยในภาพรวม ไม่ใช่พึ่งทีม Security ปลายทางเพียงอย่างเดียว

หลักสูตรนี้ใช้ 5 Domain ของ CompTIA Security+ เป็นกรอบเนื้อหา อ้างอิง Exam Objectives ของ SY0-801 ซึ่งเป็นรุ่นใหม่ที่เพิ่มความเล็งด้าน AI และครอบคลุมเนื้อหาหลักของ SY0-701 โดยมองจากมุมมองนักพัฒนาและเน้นการนำไปใช้งานจริงมากกว่าการทวนสอบ ผู้เรียนลงมือกับ OWASP Juice Shop, ZAP, Nmap, Wireshark, Simgrep, Gitleaks, Trivy และ OpenSSL ในสภาพแวดล้อมจำลองที่แยกจากระบบจริง เพื่อค้นหา แก้ไข และป้องกันช่องโหว่ของระบบตัวอย่าง SecureLoan Portal ไปจนถึงรับมือเหตุการณ์และวางนโยบายความปลอดภัยของทีม ผู้ที่ต้องการสอบใบรับรองนำไปเป็นพื้นฐานได้ โดยสมัครสอบกับ CompTIA เอง (อบรม 5 วัน วันละ 6 ชั่วโมง รวม 30 ชั่วโมง ระดับ Intermediate)

เครื่องมือ

OWASP

Kali Linux

Nmap

Simgrep

Trivy

ราคาค่าอบรม · PUBLIC / IN-HOUSE

15,900 บาท / ท่าน

ราคายังไม่รวมภาษีมูลค่าเพิ่ม (VAT 7%) · ไม่รวมค่าสอบ CompTIA · รวมเอกสารประกอบการอบรม Lab Guide รายวัน ระบบตัวอย่างสำหรับ Lab และ Certificate · รับจัด In-house ขอใบเสนอราคาได้

สมัครผ่านเว็บไซต์ ลด 10%



เพิ่มเพื่อน
LINE



01 วัตถุประสงค์ Objectives

- เข้าใจแนวคิดพื้นฐานด้านความมั่นคงปลอดภัย เช่น CIA Triad, Security Control, Zero Trust และ Cryptography
- รู้จักผู้คุกคาม ช่องทางการโจมตี และช่องโหว่ที่พบบ่อยในแอปพลิเคชัน รวมถึงความเสี่ยงด้าน AI
- ค้นหาและแก้ไขช่องโหว่ตามแนวทาง OWASP ในโค้ดของตนเองได้
- ออกแบบสถาปัตยกรรมที่ปลอดภัยทั้งบน On-premise, Cloud และ Hybrid
- จัดการตัวตน สิทธิ์ และ Secret ของระบบได้อย่างถูกต้อง
- นำ Security Scanning เข้าสู่กระบวนการพัฒนาและ CI/CD แบบ DevSecOps
- เข้าใจการเฝ้าระวัง การตอบสนองต่อเหตุการณ์ และการเก็บหลักฐานเบื้องต้น
- เข้าใจการบริหารความเสี่ยง Governance และการปฏิบัติตามกฎหมาย เช่น PDPA

02 กลุ่มเป้าหมาย Target Audience

- นักพัฒนาซอฟต์แวร์ (Frontend, Backend, Full Stack และ Mobile) ที่ต้องการเขียนระบบให้ปลอดภัยตั้งแต่ต้น
- DevOps Engineer ที่ต้องการนำ Security เข้าสู่ Pipeline
- Tech Lead และ Software Architect ที่รับผิดชอบด้านความปลอดภัยของระบบ
- เจ้าหน้าที่ IT ที่ต้องการปูพื้นฐาน Cybersecurity อย่างเป็นระบบ
- ผู้ที่ต้องการพื้นฐานก่อนเตรียมสอบ CompTIA Security+ หรือใบรับรองด้านความปลอดภัยอื่น

03 จุดเด่นของหลักสูตร Highlights

- **ครบ 5 Domain ของ Security+** อ้างอิง SY0-801 และครอบคลุม SY0-701
- **มุมมองของนักพัฒนา** Secure Coding, OWASP, Secret และ IAM
- **เน้นใช้งานจริง ไม่ใช่ตัวสอบ** ทุกหัวข้อมีกรณีศึกษาและ Lab
- **Lab ในสภาพแวดล้อมจำลอง** VM และ Container ที่แยกจากระบบจริง
- **ปิดท้ายด้วย Incident Response** รับมือเหตุข้อมูลรั่วไหลจำลอง

04 ความรู้พื้นฐาน Prerequisites

- เขียนโปรแกรมได้อย่างน้อย 1 ภาษา และเข้าใจการทำงานของ Web Application และ REST API
- ใช้ Command Line (Linux Shell หรือ PowerShell) ได้ในระดับพื้นฐาน
- เข้าใจพื้นฐานเครือข่าย เช่น IP Address, Port, DNS และ HTTP/HTTPS และใช้ Git กับ Docker เบื้องต้นได้
- ไม่จำเป็นต้องมีประสบการณ์ด้าน Security หรือ Penetration Testing มาก่อน

05 สิ่งที่ต้องเตรียมและเครื่องมือ Setup & Tools

รายการ	รายละเอียด
สภาพแวดล้อม Lab	VirtualBox หรือ VMware, Kali Linux และ Docker บนเครื่องผู้เรียน แยกจากเครือข่ายจริง
เป้าหมายจำลอง	OWASP Juice Shop และระบบตัวอย่าง SecureLoan Portal ที่งัดใจมีช่องโหว่
Web และ Network	ZAP, Burp Suite Community Edition, Nmap, Wireshark และ tcpdump
Code และ Container	OpenSSL, Semgrep (SAST), Gitleaks (Secret Scanning) และ Trivy (Dependency และ Image)
อุปกรณ์ผู้เรียน	Notebook RAM 16 GB ขึ้นไป พื้นที่ว่าง 60 GB เปิด Virtualization แล้ว พร้อม VS Code, Git และ Docker

หมายเหตุ: หลักสูตรนี้เป็นการอบรมเชิงปฏิบัติการที่อ้างอิง Exam Objectives ของ CompTIA Security+ ไม่ใช่หลักสูตรทางการของ CompTIA และไม่รวม Exam Voucher ผู้เรียนสมัครสอบเอง ต่างจาก Ethical Hacking และ Penetration Testing เบื้องต้นที่เน้นการทดสอบเจาะระบบ และ DevSecOps in Practice ที่เน้น Pipeline โดยผู้ฝึกสอนจะคอยประกบทุกด้านจากมุมมองนักพัฒนา การทดสอบทั้งหมดทำใน Lab จำลองบนเครื่องผู้เรียนเท่านั้น

06 ภาพรวมการเรียนรู้ 5 วัน Big Picture

วัน	หัวข้อหลัก
Day 1 Section 1-5	CIA Triad และ Security Control, Zero Trust, Change Management และ Secure SDLC, Cryptography และ PKI ด้วย OpenSSL, Threat Modeling ด้วย STRIDE
Day 2 Section 6-10	Threat Actor และ Attack Vector, ช่องโหว่ตาม OWASP Top 10, ความเสี่ยงด้าน AI และ Prompt Injection, Network และ Supply Chain Attack, Vulnerability Assessment ใน Lab
Day 3 Section 11-15	Secure Architecture และ Segmentation, Data Protection, Secure Coding แก่ Injection, XSS และ Access Control, Secrets Management ด้วย Gitleaks และ Resilience
Day 4 Section 16-20	IAM, MFA, OAuth 2.0 และ OpenID Connect, Hardening ของ Container, Vulnerability Management, Security Monitoring และ DevSecOps ด้วย Semgrep และ Trivy
Day 5 Section 21-25	Incident Response, Digital Forensics เบื้องต้น, Governance และ Risk Management, Compliance และ PDPA และ Master Workshop รับมือเหตุข้อมูลรั่วไหล

DAY
1

General Security Concepts

เนื้อหาการอบรม · Section 1-5

รวม
6 ชั่วโมง

1 หลักการพื้นฐานด้านความมั่นคงปลอดภัย

- CIA Triad, Non-repudiation และ AAA (Authentication, Authorization, Accounting)
- ประเภทของ Security Control: Technical, Managerial, Operational และ Physical
- หน้าที่ของ Control: Preventive, Detective, Corrective, Deterrent และ Compensating
- ภาพรวมโปรเจกต์ SecureLoan Portal และ 5 Domain ของ Security+

2 Zero Trust และ Defense in Depth

- แนวคิด Never Trust, Always Verify
- Policy Decision Point และ Policy Enforcement Point
- ประยุกต์ Zero Trust กับ API และ Microservices
- Lab: วาดชั้นการป้องกันของ SecureLoan Portal และหาจุดที่ยังเชื่อใจกันโดยไม่ตรวจ

3 Change Management และ Secure Development Lifecycle

- ผลของ Change Management ต่อความปลอดภัย
- Approval, Impact Analysis, Rollback Plan และ Version Control
- ผนวก Security เข้ากับทุกชั้นของ SDLC
- กรณีศึกษา: การเปลี่ยนแปลงระบบที่ไม่ผ่านการทบทวนแล้วกลายเป็นช่องโหว่

4 Lab: Cryptography และ PKI

- Symmetric เทียบกับ Asymmetric Encryption และการเลือกใช้
- Hashing, Salting และ Key Stretching สำหรับเก็บรหัสผ่าน
- Digital Signature, Certificate, Certificate Authority, TLS และการจัดการ Key
- Lab: ใช้ OpenSSL สร้าง Key และ Certificate สำหรับ HTTPS ใน Lab และตรวจ TLS ของระบบ

5 Workshop Day 1: Threat Modeling

- ระบุทรัพย์สินข้อมูลและขอบเขตความเชื่อถือ (Trust Boundary)
- STRIDE Model สำหรับนักพัฒนา และการจัดลำดับภัยคุกคามตามผลกระทบและโอกาสเกิด
- Workshop: จัดทำ Data Flow Diagram และ Threat Model ของ SecureLoan Portal
- Workshop: ปรับการเก็บรหัสผ่านจาก Plain Text เป็น Hash ที่ปลอดภัย



DAY
2

Threats, Vulnerabilities and Attacks

เนื้อหาการอบรม · Section 6-10

รวม
6 ชั่วโมง

6 Threat Actors และ Attack Vectors

- ประเภทของผู้คุกคาม แรงจูงใจ และขีดความสามารถ
- ช่องทางการโจมตี: Email, Social Engineering, Supply Chain, Removable Media และ Unsecured Network
- Phishing, Pretexting และ Business Email Compromise
- กรณีศึกษา: วิเคราะห์อีเมล Phishing ตัวอย่างและสัญญาณเตือน

7 Lab: Application Vulnerabilities ตาม OWASP

- Injection, Cross-site Scripting และ Broken Access Control
- Authentication Failure, Security Misconfiguration และ Vulnerable Components
- Race Condition, Memory Issue และ Insecure Deserialization ในระดับแนวคิด
- Lab: ค้นหาช่องโหว่ตาม OWASP Top 10 ฉบับล่าสุดบน OWASP Juice Shop

8 Lab: ความเสี่ยงที่เกี่ยวข้องกับ AI

- Prompt Injection และการโจมตีผ่านข้อมูลนำเข้าของโมเดล
- การรั่วไหลของข้อมูลส่วนบุคคลและข้อมูลภายในผ่าน AI
- การใช้ AI ของฝั่งผู้โจมตี เช่น Phishing อัตโนมัติและ Deepfake
- Lab: ทดลอง Prompt Injection กับ Chatbot จำลองของระบบและหาแนวทางป้องกัน

9 Network, Cloud และ Supply Chain Attacks

- DDoS, On-path Attack, DNS Attack และ Credential Replay
- Misconfiguration บน Cloud และความเสี่ยงของ Third-party Dependency
- Indicator of Compromise และสัญญาณบ่งชี้การโจมตี
- Lab: ดู Traffic ที่ไม่เข้ารหัสด้วย Wireshark เพื่อเห็นความเสี่ยงของ Credential

10 Workshop Day 2: Vulnerability Assessment ใน Lab

- ขอบเขต จริยธรรม และการขออนุญาตก่อนทดสอบทุกครั้ง
- สแกนบริการด้วย Nmap และทดสอบ Web Application ด้วย ZAP พร้อมอ่านผลอย่างถูกต้อง
- Workshop: ทดสอบ SecureLoan Portal ใน Lab จำลองตามขอบเขตที่กำหนด
- จัดทำรายงานช่องโหว่พร้อมจัดลำดับความเสี่ยง



DAY
3

Security Architecture และ Secure Development

เนื้อหาการอบรม · Section 11-15

รวม
6 ชั่วโมง

11 Secure Architecture Models

- ความปลอดภัยของ On-premise, Cloud, Hybrid และ Operational Technology (OT)
- Network Segmentation, DMZ และ Microsegmentation
- ความปลอดภัยของ Container, Serverless และ Infrastructure as Code
- Lab: แยก Network ของฐานข้อมูลออกจากส่วน Public ด้วย Docker Network

12 Data Protection

- Data Classification และ Data State (at Rest, in Transit, in Use)
- Encryption, Tokenization, Masking และ Data Minimization
- Data Sovereignty และข้อกำหนดด้านการจัดเก็บข้อมูล
- Lab: จัดระดับข้อมูลลูกค้าของ SecureLoan และ Mask ข้อมูลที่แสดงผล

13 Lab: Secure Coding Practices

- Input Validation, Output Encoding และ Parameterized Query
- จัดการ Session, Cookie และ JSON Web Token อย่างปลอดภัย
- Error Handling และ Logging ที่ไม่เปิดเผยข้อมูลสำคัญ
- Lab: แก้ช่องโหว่ Injection, XSS และ Broken Access Control ในโค้ดของระบบ

14 Lab: Secrets Management

- ความเสี่ยงของการฝัง Secret ไว้ในโค้ด ไฟล์ .env และ Git History
- เก็บ Secret ด้วย Vault หรือ Cloud Secret Manager (สาธิต)
- Secret Rotation และการตอบสนองเมื่อ Secret หลุด
- Lab: ใช้ Gitleaks ค้นหา Secret ที่หลุดใน Repository แล้วย้ายออกจากโค้ด

15 Workshop Day 3: Resilience และทดสอบซ้ำ

- High Availability, Redundancy และ Backup
- วางแผน Disaster Recovery และ Business Continuity และการทดสอบการกู้คืน
- Workshop: ทดสอบ SecureLoan Portal ซ้ำเพื่อยืนยันว่าช่องโหว่ที่พบเมื่อวานถูกปิดแล้ว
- บันทึกผลก่อนและหลังแก้ไขงานช่องโหว่



DAY
4

Security Operations

เนื้อหาการอบรม · Section 16-20

รวม
6 ชั่วโมง

16 Lab: Identity and Access Management

- Authentication Factor, MFA และ Passwordless
- OAuth 2.0, OpenID Connect, SAML และ Single Sign-On
- Role-based และ Attribute-based Access Control, Least Privilege และ Privileged Access Management
- Lab: เพิ่ม MFA ให้ระบบ Login และควบคุมสิทธิ์แบบ Role-based

17 Lab: Hardening และ Secure Baseline

- Hardening ของ Server, Container และ Endpoint
- รับ Container แบบ Non-root, Read-only Filesystem และลด Attack Surface
- Secure Configuration Baseline และการตรวจความสอดคล้อง
- Lab: Harden Container ของ SecureLoan ให้รับแบบ Non-root

18 Vulnerability Management

- วงจร Identify, Analyze, Prioritize, Remediate และ Verify
- CVE, CVSS และการจัดลำดับการแก้ไขตามความเสี่ยงจริง
- SAST, DAST, SCA และ Container Image Scanning
- Lab: สแกน Dependency และ Image ด้วย Trivy แล้วจัดลำดับการแก้ไข

19 Lab: Security Monitoring

- เก็บและวิเคราะห์ Log จาก Application, System และ Network
- SIEM (สาริต), Alerting และการลด False Positive
- ตรวจจับพฤติกรรมผิดปกติจาก Log ของระบบ
- Lab: ตั้งการเก็บ Log และตรวจจับการ Login ที่ผิดปกติ

20 Workshop Day 4: Automation และ DevSecOps

- นำ Security Scanning เข้าสู่ CI/CD Pipeline (Shift Left)
- Security Gate และเกณฑ์การ Block Pipeline
- ใช้ AI ช่วยวิเคราะห์ผลสแกนและ Log อย่างรู้เท่าทัน
- Workshop: เพิ่ม Semgrep, Gitleaks และ Trivy ใน Pipeline พร้อมกำหนด Security Gate



DAY
5

Incident Response, Governance และ Master Workshop

เนื้อหาการอบรม · Section 21-25

รวม
6 ชั่วโมง

21 Incident Response

- ขั้นตอน Preparation, Detection, Analysis, Containment, Eradication, Recovery และ Lessons Learned
- จัดทำ Playbook และ Runbook สำหรับเหตุการณ์ที่พบบ่อย
- การสื่อสารระหว่างเกิดเหตุและการรายงานผู้เกี่ยวข้อง
- Lab: เขียน Playbook สำหรับเหตุ Secret หลุด

22 Lab: Digital Forensics เบื้องต้น

- Chain of Custody และการรักษาหลักฐาน
- วิเคราะห์ Log และสร้าง Timeline ของเหตุการณ์
- Root Cause Analysis
- Lab: สร้าง Timeline จาก Log ชุดตัวอย่างของการโจมตีจำลอง

23 Governance และ Risk Management

- Security Policy, Standard, Procedure และ Guideline
- Risk Identification, Risk Assessment และ Risk Treatment
- Third-party และ Vendor Risk Management
- จัดทำ Risk Register ของ SecureLoan Portal

24 Compliance และ Security Awareness

- กฎหมายและมาตรฐานที่เกี่ยวข้อง เช่น PDPA และ ISO/IEC 27001
- Audit และ Assessment
- Security Awareness Training สำหรับทีมพัฒนาและผู้ใช้งาน
- ทบทวนความเชื่อมโยงของงานทั้ง 5 วันกับ 5 Domain ของ Security+

25 Master Workshop: ข้อมูลลูกค้ารั่วไหล

- แบ่งกลุ่มรับมือเหตุข้อมูลรั่วไหลจำลองจาก Secret ที่หลุดและช่องโหว่ที่ยังไม่ถูกแก้
- วิเคราะห์ Log สร้าง Timeline ระบุ Root Cause จำกัดความเสียหาย และกู้คืนระบบ
- จัดทำ Incident Report โดยคำนึงถึงหน้าที่ตาม PDPA
- จัดทำ Security Policy และ Secure Development Checklist ของทีม พร้อมนำเสนอแนวทางป้องกัน

07 เรียนจบแล้วได้อะไร Outcomes

- พื้นฐาน Security ที่เป็นมาตรฐาน คsu 5 Domain ของ Security+
- มองเห็นภัยคุกคามแบบผู้โจมตี OWASP Top 10 และความเสี่ยงด้าน AI
- เขียนโค้ดที่ปลอดภัย Secure Coding และ Secrets Management
- จัดการ IAM ได้ถูกต้อง MFA, RBAC และ Least Privilege
- นำ Security เข้าสู่ Pipeline Semgrep, Gitleaks และ Trivy
- รับมือเหตุการณ์อย่างเป็นขั้นตอน Incident Response, Forensics และ PDPA

08 สิ่งที่คุณเรียนจะได้รับ Deliverables

- เอกสารประกอบการอบรมครบทั้ง 5 วัน และ Lab Guide รายวัน
- ระบบตัวอย่าง SecureLoan Portal และไฟล์ตั้งค่า Pipeline สำหรับ Security Scan
- Template ของ Threat Model, รายงานช่องโหว่, Incident Playbook และ Secure Development Checklist
- ประกาศนียบัตรจบหลักสูตร (Certificate of Completion) ของสถาบันไอทิจิเนียส

09 ข้อมูลผู้สอน Instructor

อ.สามิตร โทยม วิทยากรผู้มีประสบการณ์ด้านการพัฒนาซอฟต์แวร์และ DevSecOps สอนความมั่นคงปลอดภัยจากมุมมองของคนเขียนโค้ด เริ่มจากให้ผู้เรียนเห็นช่องโหว่ด้วยตาตนเองใน Lab จำลอง แล้วลงมือแก้ไขในโค้ดจริงและป้องกันไม่ให้เกิดซ้ำด้วย Pipeline เน้นจริยธรรมและขอบเขตการทดสอบ เพื่อให้ผู้เรียนนำแนวทางกลับไปใช้กับทีมได้อย่างถูกต้อง

ราคาค่าอบรม 15,900 บาท/ท่าน · สนใจ IN-HOUSE ขอใบเสนอราคา

15,900 บาท / ท่าน (ยังไม่รวม VAT 7%)

สมัครผ่านเว็บไซต์ ลด 10%

☎ 02-570-8449

LINE @itgenius

☎ 088-807-9770

✉ contact@itgenius.co.th



เพิ่มเพื่อน
LINE