



สถาบันไอจีเนียส
IT GENIUS INSTITUTE

COURSE ID
DOP-05

COURSE OUTLINE · รายละเอียดหลักสูตรอบรม

DEVOPS / SECURITY

DevSecOps in Practice

ใส่ความปลอดภัยลงในทุกชั้นของ CI/CD Pipeline ตั้งแต่โค้ดถึง Kubernetes

● 18 ชั่วโมง

● 3 วัน

● พื้นฐาน Git, Docker และ CI/CD

● 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

ทีมพัฒนาปัจจุบันส่งโค้ดขึ้น Production ได้หลายครั้งต่อวันด้วย CI/CD แต่งานความปลอดภัยจำนวนมากยังรอตรวจสอบก่อนขึ้นระบบจริง ผลคือช่องโหว่ถูกพบช้า แก่ยากและแพง หรือหลุดขึ้น Production ไปเลย ทั้ง Password ที่ติดไปกับโค้ด Library ที่มีช่องโหว่ Container Image ที่ไม่เคสแกน และ Cluster ที่ให้สิทธิ์กว้างเกินจำเป็น DevSecOps คือการย้ายการตรวจเหล่านี้มาไว้ในทุกชั้นของ Pipeline ให้ทีมรู้ปัญหาตั้งแต่ตอนเขียนโค้ด

หลักสูตรนี้พาผู้เรียนสร้าง Secure Pipeline ด้วย GitLab CI ทีละชั้นบนแอปตัวอย่างชุดเดียว เริ่มจากแนวคิด Shift-left และ Threat Modeling เบื้องต้น ตรวจสอบ Secret ที่หลุดด้วย Gitleaks ทำ SAST ด้วย SonarQube สแกน Dependency และ Container Image ด้วย Trivy ตรวจสอบ Infrastructure as Code สร้าง SBOM และเซ็น Image ด้วย Syft และ cosign แล้วทดสอบแอปที่รันจริงด้วย OWASP ZAP จากนั้นรวมผลทั้งหมดเป็น Security Gate ที่หยุด Pipeline เมื่อพบปัญหาร้ายแรง ก่อนทยอยลดสู่ความปลอดภัยบน Kubernetes ทั้ง RBAC, Pod Security Standards, Network Policy, Admission Control และ Runtime Monitoring แล้วปิดท้ายด้วย Capstone สร้าง Secure Pipeline ตั้งแต่โค้ดจนถึง Cluster (อบรม 3 วัน วันละ 6 ชั่วโมง รวม 18 ชั่วโมง ระดับ Intermediate)

เครื่องมือ

GL

GitLab CI

SQ

SonarQube

ZAP

OWASP ZAP

Tv

Trivy

K8s

Kubernetes

ราคาค่าอบรม · PUBLIC / IN-HOUSE

9,900 บาท / ท่าน

สมัครผ่านเว็บไซต์ ลด 10%

ราคายังไม่รวมภาษีมูลค่าเพิ่ม (VAT 7%) · รวมเอกสารประกอบการอบรม Lab Guide แอปตัวอย่าง ไฟล์ Pipeline และ Kubernetes Manifest คนทุก Lab และ Certificate · รับจัด In-house ขอใบเสนอราคาได้



เพิ่มเพื่อน
LINE

☎ 02-570-8449

☎ 088-807-9770

LINE @itgenius

🌐 www.itgenius.co.th

01 วัตถุประสงค์ Objectives

- เข้าใจแนวคิด Shift-left และบทบาทของทีม Dev, Ops และ Security ใน DevSecOps
- ทำ Threat Modeling เบื้องต้นเพื่อเลือกการตรวจที่เหมาะสมกับความเสี่ยงของระบบ
- ตรวจสอบ Secret ที่หลุด และทำ SAST กับ SCA ใน GitLab CI ได้
- สแกน Container Image และ Infrastructure as Code ด้วย Trivy ได้
- สร้าง SBOM และเซ็น Container Image เพื่อดูแล Software Supply Chain
- ทดสอบแอปที่รันจริงด้วย DAST จาก OWASP ZAP ใน Pipeline
- ตั้ง Security Gate และจัดการผลการสแกนโดยไม่ทำให้ทีมทำงานช้าลง
- ป้องกัน Workload บน Kubernetes ด้วย RBAC, Pod Security Standards และ Network Policy

02 กลุ่มเป้าหมาย Target Audience

- DevOps Engineer และ Platform Engineer ที่ดูแล CI/CD Pipeline ขององค์กร
- นักพัฒนาซอฟต์แวร์ที่ต้องการเขียนและส่งโค้ดให้ปลอดภัยตั้งแต่ต้น
- ทีม Application Security ที่ต้องการนำการตรวจความปลอดภัยเข้าสู่ Pipeline
- Cloud Engineer และ SRE ที่ดูแลระบบบน Container และ Kubernetes
- Tech Lead ที่ต้องวางมาตรฐานความปลอดภัยของทีมพัฒนา

03 จุดเด่นของหลักสูตร Highlights

- **สร้าง Secure Pipeline ที่ละขั้น** บนแอปตัวอย่างชุดเดียวตลอดหลักสูตร
- **ครบทุกชั้นของการตรวจ** Secret, SAST, SCA, Image, IaC และ DAST
- **ดูแล Supply Chain SBOM** ด้วย Syft และเซ็น Image ด้วย cosign
- **Security Gate ที่ใช้ได้จริง** หยุดสิ่งร้ายแรงโดยไม่ถ่วงทีม
- **ต่อยอด Kubernetes** RBAC, Pod Security และ Network Policy

04 ความรู้พื้นฐาน Prerequisites

- ใช้งาน Git และเข้าใจขั้นตอน Merge Request หรือ Pull Request
- สร้างและรัน Container ด้วย Docker ได้ และเข้าใจ Dockerfile
- เคยใช้หรือเข้าใจหลักการ CI/CD Pipeline และมีพื้นฐาน Kubernetes เบื้องต้น
- โน้ตบุ๊ก RAM อย่างน้อย 16 GB ที่ติดตั้ง Docker Desktop และ VS Code ได้ พร้อมบัญชี GitLab

05 สิ่งที่ต้องเตรียมและเครื่องมือ Setup & Tools

รายการ	รายละเอียด
อุปกรณ์	Notebook RAM 16 GB ขึ้นไป เชื่อมต่ออินเทอร์เน็ต ติดตั้ง Docker Desktop ได้
CI/CD	GitLab และ GitLab Runner พร้อมแอปตัวอย่างที่มีช่องโหว่ให้ฝึกแก้
เครื่องมือสแกน	Gitleaks, SonarQube, Trivy, OWASP ZAP, Syft และ cosign
Kubernetes	Cluster สำหรับ Lab เช่น kind หรือ k3d พร้อม kubectl และ Helm
Policy และ Runtime	Pod Security Admission, Kyverno และ Falco สำหรับทดลอง

หมายเหตุ: เครื่องมือทั้งหมดเป็นโอเพนซอร์สหรือมีแบบใช้ฟรี ทุก Lab ทำงานบนแอปตัวอย่างชุดเดียวที่ตั้งใจใส่ช่องโหว่ไว้ให้ฝึกค้นหาและแก้ไข ตัวอย่าง Pipeline ใช้ GitLab CI เป็นหลัก และมีแนวทางปรับใช้กับ Jenkins หรือระบบ CI/CD อื่น หลักสูตรนี้เน้นการนำการตรวจความปลอดภัยเข้าสู่กระบวนการพัฒนา ไม่ครอบคลุมการทดสอบเจาะระบบเชิงลึกหรือการดูแล SOC

06 ภาพรวมการเรียนรู้ 3 วัน Big Picture

วัน	หัวข้อหลัก
Day 1 Section 1-5	แนวคิด Shift-left และ DevSecOps, Threat Modeling เบื้องต้น, วาง GitLab CI Pipeline ต้นแบบ, ตรวจสอบ Secret ที่หลุดด้วย Gitleaks และทำ SAST ด้วย SonarQube
Day 2 Section 6-10	สแกน Dependency และทำ SCA, สแกน Container Image ด้วย Trivy, ตรวจสอบ IaC, สร้าง SBOM และเซ็น Image ด้วย Syft และ cosign แล้วทำ DAST ด้วย OWASP ZAP
Day 3 Section 11-15	ตั้ง Security Gate ใน Pipeline, ความปลอดภัยของ Kubernetes ทั้ง RBAC, Pod Security Standards, Network Policy และ Admission Control, Runtime Monitoring และ Capstone Secure Pipeline



DAY
1

แนวคิด DevSecOps และตรวจตั้งแต่โค้ด

เนื้อหาการอบรม · Section 1-5

รวม
6 ชั่วโมง

1 DevSecOps และแนวคิด Shift-left

- ทำไมการตรวจความปลอดภัยตอนท้ายโปรเจกต์จึงไม่ทันการส่งงานแบบ CI/CD
- แนวคิด Shift-left และความรับผิดชอบร่วมของทีม Dev, Ops และ Security
- ภาพรวมการตรวจแต่ละแบบ: Secret, SAST, SCA, Image, IaC และ DAST
- OWASP Top 10 และความเสี่ยงของ Software Supply Chain ที่ต้องรู้
- วัดความพร้อมของทีมและวางแผนนำ DevSecOps เข้าไปที่ละขั้น

2 Workshop: Threat Modeling เบื้องต้น

- Threat Modeling คืออะไร และควรทำเมื่อไรในวงจรการพัฒนา
- วาด Data Flow Diagram ของระบบและหาขอบเขตความเชื่อถือ
- ระบุภัยคุกคามด้วยกรอบ STRIDE
- จัดลำดับความเสี่ยงและเลือกการตรวจที่ตอบโจทย์แต่ละความเสี่ยง
- Workshop: ทำ Threat Model ของแอปตัวอย่างที่ใช้ตลอดหลักสูตร

3 Lab: วาง GitLab CI Pipeline ดันแบบ

- โครงสร้าง .gitlab-ci.yml: Stage, Job, Rule และ Artifact
- ติดตั้ง GitLab Runner และรัน Pipeline สำหรับ Build และ Test
- ออกแบบลำดับ Stage ให้มีที่วางการตรวจความปลอดภัยแต่ละแบบ
- จัดการ Variable และ Secret ของ Pipeline ให้ปลอดภัย
- แนวทางปรับใช้แนวคิดเดียวกันกับ Jenkins

4 Lab: ตรวจหา Secret ที่หลุดด้วย Gitleaks

- Secret ที่มักหลุดไปกับโค้ด เช่น API Key, Token และ Password
- สแกนประวัติ Git ทั้งหมดด้วย Gitleaks และอ่านผลลัพธ์
- ติดตั้ง Pre-commit Hook เพื่อกันตั้งแต่ก่อน Commit
- เพิ่ม Job ตรวจ Secret ใน Pipeline และจัดการ False Positive
- ขั้นตอนรับมือเมื่อ Secret หลุด: เพิกถอน เปลี่ยนใหม่ และล้างประวัติ

5 Lab: SAST ด้วย SonarQube

- SAST ทำงานอย่างไร จุดแข็ง และข้อจำกัด
- ติดตั้ง SonarQube ด้วย Docker และเชื่อมกับโปรเจกต์
- อ่านผล Vulnerability, Security Hotspot และ Code Smell
- ตั้ง Quality Gate และแสดงผลใน Merge Request
- Lab: แก้ช่องโหว่ SQL Injection และ XSS ที่ SonarQube พบ



DAY
2

ทบทวน Dependency, Container, IaC และแอปที่รันจริง

เนื้อหาการอบรม · Section 6-10

รวม
6 ชั่วโมง

6 Lab: Dependency และ SCA

- ความเสี่ยงจาก Open Source Library และ Transitive Dependency
- สแกน Dependency ของโปรเจกต์ด้วย Trivy แบบ Filesystem
- อ่านค่า CVE, CVSS และจัดลำดับการแก้ตามความเสี่ยงจริง
- ตรวจสอบ License ของ Library ที่อาจขัดกับนโยบายองค์กร
- ใช้ Lock File และระบบอัปเดต Dependency อัตโนมัติ

7 Lab: สแกน Container Image ด้วย Trivy

- ช่องโหว่ที่มากับ Base Image และแพ็คเกจในระบบปฏิบัติการ
- สแกน Image ใน Pipeline ก่อน Push ขึ้น Registry
- เขียน Dockerfile ให้ปลอดภัย: Minimal Base Image, Non-root User และ Multi-stage Build
- จัดการช่องโหว่ที่ยังไม่มีแพตช์ด้วยไฟล์ Ignore อย่างมีประสิทธิภาพ
- Lab: ลดช่องโหว่ของ Image แอปตัวอย่างแล้วเทียบผลก่อนและหลัง

8 Lab: IaC Scanning

- ความผิดพลาดที่พบบ่อยใน Terraform, Kubernetes Manifest และ Dockerfile
- สแกน Misconfiguration ด้วย Trivy แบบ Config
- อ่านผลลัพธ์และแก้ไขตามแนวทางของแต่ละกฎ
- เพิ่ม Job ตรวจสอบ IaC ใน Merge Request ก่อน Deploy
- Lab: แก้ Kubernetes Manifest ที่รันด้วยสิทธิ์สูงเกินจำเป็น

9 Lab: SBOM และการเซ็น Container Image

- SBOM คืออะไร และรูปแบบ SPDX กับ CycloneDX
- สร้าง SBOM ของ Image ด้วย Syft และใช้ตรวจสอบช่องโหว่ย้อนหลัง
- เซ็น Image ด้วย cosign และแนบ SBOM เป็น Attestation
- ตรวจสอบลายเซ็นก่อน Deploy เพื่อยืนยันที่มาของ Image
- ภาพรวมแนวคิด SLSA สำหรับยกระดับความน่าเชื่อถือของ Build

10 Lab: DAST ด้วย OWASP ZAP

- DAST ต่างจาก SAST อย่างไร และควรรันที่ขั้นตอนไหนของ Pipeline
- รัน ZAP Baseline Scan กับแอปที่ Deploy ใน Environment ทดสอบ
- สแกน API จาก OpenAPI Specification
- ปรับ Rule ของ ZAP และจัดการ False Positive
- Lab: ตรวจสอบและแก้ Security Header และ Cookie ที่ตั้งค่าไม่ปลอดภัย

DAY
3

Security Gate, Kubernetes และ Capstone

เนื้อหาการอบรม · Section 11-15

รวม
6 ชั่วโมง

11 Lab: Security Gate และการจัดการผลการสแกน

- กำหนดเกณฑ์ว่าเมื่อไร Pipeline ควรหยุด และเมื่อไรแค่แจ้งเตือน
- รวมผลการสแกนหลายเครื่องมือไว้ที่เดียวและลดผลซ้ำซ้อน
- จัดการข้อยกเว้นอย่างมีเจ้าของและวันหมดอายุ
- ให้ Feedback กับนักพัฒนาใน Merge Request โดยไม่ถ่วงความเร็วทีม
- Lab: ตั้ง Security Gate ของ Pipeline แอปตัวอย่าง

12 Lab: Kubernetes RBAC และ Pod Security

- พื้นผิวการโจมตีของ Kubernetes และสิ่งที่ต้องป้องกันก่อน
- RBAC: Role, ClusterRole, ServiceAccount และหลัก Least Privilege
- Pod Security Standards ระดับ Privileged, Baseline และ Restricted
- บังคับใช้ด้วย Pod Security Admission ระดับ Namespace
- Lab: ปรับ Deployment ให้ผ่านระดับ Restricted

13 Lab: Network Policy และ Admission Control

- Network Policy แบบ Default Deny และเปิดเฉพาะการเชื่อมต่อที่จำเป็น
- จัดการ Secret บน Kubernetes และแนวทางใช้ External Secret Store
- Admission Control คืออะไร และการเขียน Policy ด้วย Kyverno
- บังคับให้ Deploy ได้เฉพาะ Image ที่เซ็นแล้วและมาจาก Registry ที่อนุญาต
- Lab: บล็อก Pod ที่จะเปิด Policy ขององค์กร

14 Runtime Security และ Monitoring

- ทำไมการสแกนก่อน Deploy จึงยังไม่พอ
- ภาพรวม Runtime Detection ด้วย Falco และตัวอย่าง Rule
- เก็บ Audit Log ของ Kubernetes และส่งเข้าระบบ Monitoring
- ตัวชี้วัดของโปรแกรม DevSecOps และการรายงานต่อผู้บริหาร
- Lab: ตรวจจับการเปิด Shell เข้า Container ที่กำลังทำงาน

15 Workshop: Capstone Secure Pipeline

- ออกแบบ Secure Pipeline ของแอปตัวอย่างจาก Threat Model ที่ทำได้
- รวม Secret Detection, SAST, SCA, Image Scan, IaC Scan, SBOM และ DAST
- Deploy ขึ้น Kubernetes ที่บังคับใช้ Pod Security และ Admission Policy
- นำเสนอผล ริ้วร่วมกัน และวาง Roadmap สำหรับทีมของตนเอง
- สรุป Checklist DevSecOps สำหรับนำไปใช้ในองค์กร

07 เรียนจบแล้วได้อะไร Outcomes

- เข้าใจ DevSecOps Shift-left และ Threat Modeling
- ตรวจตั้งแต่โค้ด Secret Detection, SAST และ SCA
- ปกป้อง Container และ IaC Trivy และ Dockerfile ที่ปลอดภัย
- ดูแล Supply Chain SBOM และการเซ็น Image
- ตั้ง Security Gate ได้ DAST และเกณฑ์หยุด Pipeline
- ป้องกัน Kubernetes RBAC, Pod Security และ Policy

08 สิ่งที่คุณเรียนจะได้รับ Deliverables

- เอกสารประกอบการอบรมฉบับสมบูรณ์ครบทั้ง 3 วัน และ Lab Guide ที่ละขั้นตอน
- แอปตัวอย่างพร้อมไฟล์ .gitlab-ci.yml ของ Secure Pipeline ฉบับสมบูรณ์
- Dockerfile, Kubernetes Manifest และ Kyverno Policy ตัวอย่างที่ผ่านการตรวจแล้ว
- แม่แบบ Threat Model และ Checklist DevSecOps สำหรับทีม
- ประกาศนียบัตรจบหลักสูตร (Certificate of Completion) และช่องทางสอบถามวิทยากรหลังจบหลักสูตร

09 ข้อมูลผู้สอน Instructor

อ.สามิตร โกยม ผู้สอนและผู้ปฏิบัติงานด้าน DevOps และความปลอดภัยของแอปพลิเคชัน ที่วาง CI/CD Pipeline และระบบบน Kubernetes ให้กับทีมพัฒนาในงานจริง จุดเด่นคือการสอนบนแอปตัวอย่างชุดเดียวที่มีช่องโหว่จริง ให้ผู้เรียนเห็นว่าแต่ละเครื่องมือจะอะไรได้และพลาดอะไร แล้วพาตัดสินใจว่าควรตั้งเกณฑ์อย่างไรให้ปลอดภัยโดยไม่ทำให้ทีมส่งงานช้าลง เพื่อให้กลับไปวาง Secure Pipeline ในองค์กรของตนเองได้ทันที

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