

กำหนดการอบรมเชิงปฏิบัติการออนไลน์ ผ่านระบบ Google Meet
หลักสูตร “การใช้งาน SonarQube เพื่อยกระดับมาตรฐานความปลอดภัยด้านการพัฒนาระบบ”
สำหรับนักพัฒนาระบบของส่วนงาน
วันที่ 19 - 20 ตุลาคม 2569 เวลา 09.00 – 16.00 น.

วิทยากร : คุณธนสิทธิ์ ปาณิวรรณ จาก SOFTWAREONE CO., LTD

** ห้องอบรม Google Meet เปิดในเวลา 08.45 น. **

วันจันทร์ที่ 19 ตุลาคม 2569 เวลา 09.00 – 16.00 น.		
เวลา	หัวข้อ	รายละเอียด
09.00 – 09.10 น.	พิธีเปิดการอบรม	
09.10 – 10.30 น.	Introduction to Security Mindset	○ แนวคิดการพัฒนาซอฟต์แวร์โดยคำนึงถึงความปลอดภัยตั้งแต่ต้น ○ บทบาทของ Developer ใน Secure SDLC ○ การระบุความเสี่ยง ภัยคุกคามและจุดอ่อนของระบบเบื้องต้น
	Basic Security - Encoding, Encryption, Hash - Public / Private Key - Basic HTTP Protocol - Cookies, Session, CORS - Web Application Common Vulnerabilities and Mitigations	หัวข้อความปลอดภัยพื้นฐานสำหรับนักพัฒนาซอฟต์แวร์
10.30 – 10.40 น.	พัก 10 นาที	
10.40 – 12.00 น.	OWASP Top 10	○ ภาพรวมความเสี่ยงด้านความปลอดภัยของ Web Application ตาม OWASP Top 10 ○ ตัวอย่างช่องโหว่ สาเหตุ ผลกระทบ และแนวทางลดความเสี่ยงในขั้นตอนพัฒนา
	Modern Auth & Data Protection	○ กลไก Hashing สำหรับรหัสผ่าน ○ โครงสร้างและการใช้งาน JWT อย่างปลอดภัย และแนวคิด OAuth 2
12.00 – 13.00 น.	พักรับประทานอาหารกลางวัน	
13.00 – 14.30 น.	SonarQube Enterprise Edition Overview	ภาพรวมความสามารถระดับ Enterprise เช่น การรายงาน Security-issue ภายใน GitHub และ GitLab
	Taint Analysis & Custom Secret Detection	การใช้ Taint analysis วิเคราะห์ช่องโหว่ Injection และกำหนด Custom secret-detection rules เพื่อจับรหัสลับขององค์กร
	Pipeline Integration & Merge Prevention	วิธีเชื่อมต่อกับ Pipeline, การตั้ง Quality-gate และบล็อก PR ที่ไม่ผ่านเกณฑ์ (Merge prevention)
14.30 – 14.40 น.	พัก 10 นาที	
14.40 – 15.45 น.	Security & Regulatory Reports	การเรียกรายงานความปลอดภัยตามมาตรฐาน PCI DSS, OWASP ASVS, OWASP Top 10, CWE Top 25, STIG และ CASA พร้อม Audit logs
	Hands-on Workshop: Source Code Remediation	ทดลองนำผลการสแกนมาวิเคราะห์หาสาเหตุ และแก้ไขซอร์สโค้ดจริง (Code Remediation) ให้ผ่านเงื่อนไข Quality Gate
15.45 – 16.00 น.	Q & A	

**** ห้องอบรม Google Meet เปิดในเวลา 08.45 น. ****

วันอังคารที่ 20 ตุลาคม 2569 เวลา 09.00 – 16.00 น.		
เวลา	หัวข้อ	รายละเอียด
09.00 – 10.30 น.	Secure Architecture & API Design (Standalone)	ทฤษฎีการออกแบบสถาปัตยกรรมและ API ที่ปลอดภัย โดยมุ่งเน้นที่ Logic การทำงาน มากกว่าการพึ่งพาเครื่องมือ
	Threat Modeling Fundamentals	เรียนรู้กระบวนการจำลองสถานการณ์และค้นหาความเสี่ยง (Threat Modeling) ก่อนเริ่มเขียนโค้ด
10.30 – 10.40 น.	พัก 10 นาที	
10.40 – 12.00 น.	Manual Code Review & Secure Checklist	เทคนิคการตรวจสอบโค้ดด้วยสายตา (Manual Review) การค้นหาจุดอ่อนที่เครื่องมืออัตโนมัติอาจมองข้าม และการสร้าง Checklist
	Password Hashing	หลักการจัดเก็บรหัสผ่านด้วย Hash และ Salt; การเลือก Algorithm ที่เหมาะสม เช่น bcrypt, scrypt หรือ Argon2; แนวทางตรวจสอบรหัสผ่านและการหลีกเลี่ยงวิธีที่ไม่ปลอดภัย
12.00 – 13.00 น.	พักรับประทานอาหารกลางวัน	
13.00 – 14.30 น.	Workshop: Manual Code Audit	กิจกรรมกลุ่มฝึกวิเคราะห์ช่องโหว่จาก Use Cases เชิงแนวคิด
	Code Secure with AI Agent	บทบาทของปัญญาประดิษฐ์ (AI-assisted coding) ในวงจรการพัฒนาซอฟต์แวร์สมัยใหม่ และแนวทางรับมือกับความเสี่ยงใหม่ๆ ที่มาพร้อม AI
	SonarQube Advanced Security Overview	แนะนำฟีเจอร์ส่วนเสริมแบบเสียค่าใช้จ่าย (Paid add-on) ที่ต่อยอดความปลอดภัยให้ล้ำหน้ายิ่งกว่า Enterprise Edition
14.30 – 14.40 น.	พัก 10 นาที	
14.40 – 15.45 น.	Advanced SAST Capabilities	เจาะลึกความสามารถของ Advanced SAST ในการค้นหาและวิเคราะห์ช่องโหว่ที่มีความซับซ้อนสูงในระดับ Source Code
	Software Composition Analysis (SCA) & Use Cases	การใช้ SCA วิเคราะห์ส่วนประกอบซอฟต์แวร์ เพื่อบริหารจัดการความเสี่ยงจาก Open-source libraries พร้อมยกตัวอย่าง Use cases จริงในระดับองค์กร
15.45 – 16.00 น.	Q & A	

**** กำหนดการอาจมีการเปลี่ยนแปลงได้ตามความเหมาะสม ****

รายละเอียดการอบรม : <https://muit.mahidol.ac.th/sonarqube-2569/>