



NSTDA

Career for the Future Academy
สถาบันพัฒนาบุคลากรแห่งอนาคต

กำหนดการ

หลักสูตร "ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ" **รุ่นที่ 4** (Security Operations Center: SOC)

ระหว่างวันที่ 4 - 7 กรกฎาคม 2566 เวลา 09.00 - 16.00 น.
ณ โรงแรม ไอบีเอส สไตล์ กรุงเทพฯ รัชดา

กำหนดการอบรม (ระยะเวลา 4 วัน)

เวลา	หัวข้อ
วันอังคารที่ 4 กรกฎาคม 2566	
09.00 - 12.00 น.	- Some Useful Attack Statistics - What is SOC? - Why do You Need a SOC? - Key Objectives for SOC - SOC Benefits - SOC Standards and Process - SOC Components (Core Components)
13.00 - 16.00 น.	- SOC Technologies - SOC People - SOC Management - Types of SOC - Planning for SOC - SOC Structure, Roles and Responsibilities and Processes - Workshop 1 : กระบวนการ บทบาท และหน้าที่ความรับผิดชอบของ ผู้ปฏิบัติงานเฝ้าระวังด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
วันพุธที่ 5 กรกฎาคม 2566	
09.00 - 12.00 น.	- Procedure for Daily and Monthly Incident Handling Operations - Incident management and systems - Types of incidents - Dashboard and reporting - Shift handover - การจำลองสถานการณ์การโจมตีในรูปแบบต่างๆ เช่น SQL Injection, Cross-site Scripting (XSS), Brute Force เป็นต้น - Workshop 2 : การจำลองสถานการณ์การโจมตีในรูปแบบต่างๆ - Demo ทดสอบการโจมตีระบบเพื่อให้เห็นถึงความสำคัญของการโจมตีและการใช้ SIEM เพื่อป้องกันการบุกรุกระบบ
13.00 - 16.00 น.	- SIEM (Security Information and Event Management) - Introduction to SIEM - New Rule Determination - Application Log Monitoring - System and Device Log Monitoring - Object Access Auditing - User Activity Monitoring - Real-time Alerting - Log Analysis - Event Correlation - Log Retention - การติดตั้ง Agent สำหรับการบันทึกข้อมูลล็อก

เวลา	หัวข้อ
	- Workshop 3 : การติดตั้ง Agent - การติดตั้ง Agent Log บน Windows - การติดตั้ง Agent Log บน Linux - การติดตั้ง Agent Log บน Apache Server - การติดตั้ง Agent Log บน IIS Server - การกำหนดกฎเกณฑ์ (Correlation Rules) ที่ใช้ในการ วิเคราะห์ข้อมูลล็อก - Workshop 4 : การกำหนดกฎเกณฑ์ต่างๆ
วันพฤหัสบดีที่ 6 กรกฎาคม 2566	
09.00 - 12.00 น.	- การจัดทำรายงานประเภทต่างๆ ที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัย ได้แก่ การแจ้งเตือนประเภทต่างๆ (Alert) และรายงานประเภท สถิติต่างๆ (Dashboard) ที่จำเป็นต่อการใช้งาน - Workshop 5 : การจัดทำรายงานประเภทต่างๆ - การสร้างการแจ้งเตือน (Alert) บน SIEM - การสร้างหน้ารายงาน (Dashboard) บน SIEM
13.00 - 16.00 น.	- Related Laws and Compliance - การใช้ SIEM เพื่อวิเคราะห์ความสอดคล้องกับนโยบายและขั้นตอนปฏิบัติที่กำหนดไว้ - Workshop 6 : การใช้ SIEM เพื่อวิเคราะห์ความสอดคล้องกับนโยบายและขั้นตอนปฏิบัติที่กำหนดไว้ - Log Forensics - Forensic Tools - Workshop 7 : การจัดเก็บข้อมูลหลักฐานด้านคอมพิวเตอร์
วันศุกร์ที่ 7 กรกฎาคม 2566	
09.00 - 12.00 น.	- VA Techniques - Vulnerability Assessment - Workshop 8 : การใช้เครื่องมือในการวิเคราะห์หาช่องโหว่ในระบบ
13.00 - 16.00 น.	- ซอฟต์แวร์หรือระบบสำหรับตรวจสอบการเปลี่ยนแปลงแก้ไขไฟล์ข้อมูลต่างๆ ในระบบโดยไม่ได้รับอนุญาต (File Integrity Checkers) - Workshop 9 : การใช้เครื่องมือในการวิเคราะห์และตรวจสอบการเปลี่ยนแปลงแก้ไขไฟล์ข้อมูลต่างๆ ในระบบโดยไม่ได้รับอนุญาต - Network and System Monitoring - Workshop 10 : การใช้เครื่องมือในการเฝ้าระวังและติดตามการทำงานของ ระบบและ อุปกรณ์ต่างๆ

****หมายเหตุ สถาบันพัฒนานาบุคลากรแห่งอนาคต
ขอสงวนสิทธิ์ในการเปลี่ยนแปลงกำหนดการอบรม และวิทยากรตามความเหมาะสม**