กำหนดการ

จัดฝึกอบรมเชิงปฏิบัติการหัวข้อ “การพัฒนาระบบตรวจจับและแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ด้วย Wazuh”

วันจันทร์ที่ 25 พฤษภาคม 2569 เวลา 08.30-16.00 น.

ณ ห้องประชุม Main Conference ชั้น 1 อาคารศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยนเรศวร

วันจันทร์ที่ 25 พฤษภาคม 2569

เวลา 08.30 – 09.00 น.	ลงทะเบียน ณ ห้องประชุม Main Conference ชั้น 1 อาคารศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยนเรศวร
เวลา 09.00 – 10.30 น.	***ภาพรวมของระบบ Wazuh*** โดยวิทยากร นายณัฏฐชัย อัจฉริยากุล ตำแหน่งเจ้าหน้าที่ด้านความมั่นคงปลอดภัยไซเบอร์ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) **หัวข้อ** สถาปัตยกรรมของ Wazuh (Indexer, Server, Dashboard, Agent) **หัวข้อ** หลักการท างานของ SIEM และ XDR **หัวข้อ** การไหลของข้อมูล (Data Flow) จาก Agent สู่ Dashboard
เวลา 10.30 - 10.45 น.	พักรับประทานอาหารว่าง
เวลา 10.45 - 12.00 น.	***การติดตั้งระบบ Wazuh Server*** โดยวิทยากร นายณัฏฐชัย อัจฉริยากุล ตำแหน่งเจ้าหน้าที่ด้านความมั่นคงปลอดภัยไซเบอร์ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) **หัวข้อ** การติดตั้งแบบ All-in-one กับ Distributed **หัวข้อ** Workshop: การติดตั้ง Wazuh Manager, Indexer และ Dashboard **หัวข้อ** การเข้าใช้งาน Web Interface
เวลา 12.00 – 13.00 น.	พักรับประทานอาหารกลางวัน
เวลา 13.00 – 14.30 น.	***Wazuh Server Dashboard*** โดยวิทยากร นายณัฏฐชัย อัจฉริยากุล ตำแหน่งเจ้าหน้าที่ด้านความมั่นคงปลอดภัยไซเบอร์ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) **หัวข้อ** แนะน าเมนูต่างๆ บน Wazuh Dashboard **หัวข้อ** การดู Security Events และ Alerts **หัวข้อ** การตรวจสอบสถานะ Health Check ของระบบ
เวลา 14.30 – 14.45 น.	พักรับประทานอาหารว่าง

*** กำหนดการอาจมีการเปลี่ยนแปลงได้ตามความเหมาะสม***

กำหนดการ

จัดฝึกอบรมเชิงปฏิบัติการหัวข้อ “การพัฒนาระบบตรวจจับและแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ด้วย Wazuh”

วันจันทร์ที่ 25 พฤษภาคม 2569 เวลา 08.30-16.00 น.

ณ ห้องประชุม Main Conference ชั้น 1 อาคารศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยนเรศวร

วันจันทร์ที่ 25 พฤษภาคม 2569

เวลา 14.45 – 16.00 น. ***Wazuh Agent Deployment*** โดยวิทยากร นายณัฏฐชัย อัจฉริยากุล
ตำแหน่งเจ้าหน้าที่ด้านความมั่นคงปลอดภัยไซเบอร์
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)
หัวข้อ วิธีการลงทะเบียน Agent (Registration Process)
หัวข้อ ติดตั้งAgent บน Windows
(ผ่าน GUI และ CLI)
หัวข้อ ติดตั้ง Agent บน Linux (ผ่าน Package Manager) การตรวจสอบสถานะการเชื่อมต่อ (Active/Disconnected)

*** กำหนดการอาจมีการเปลี่ยนแปลงได้ตามความเหมาะสม***

กำหนดการ

จัดฝึกอบรมเชิงปฏิบัติการหัวข้อ “การพัฒนาระบบตรวจจับและแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ด้วย Wazuh”

วันอังคารที่ 26 พฤษภาคม 2569 เวลา 08.30-16.00 น.

ณ ห้องประชุม Main Conference ชั้น 1 อาคารศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยนเรศวร

วันอังคารที่ 26 พฤษภาคม 2569

เวลา 08.30 – 09.00 น.	ลงทะเบียน ณ ห้องประชุม Main Conference ชั้น 1 อาคารศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยนเรศวร
เวลา 09.00 – 10.30 น.	***Wazuh Configuration*** โดยวิทยากร นายวันเฉลิม นิธิมณีรัตน์ ตำแหน่งเจ้าหน้าที่ด้านความมั่นคงปลอดภัยไซเบอร์ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) **หัวข้อ** โครงสร้างไฟล์ Config หลัก **หัวข้อ** การเปิด/ปิด Module ต่างๆ (FIM, Vulnerability Detector) ***Wazuh Agent Group*** **หัวข้อ** การจัดกลุ่ม Agent (Centralized Configuration) **หัวข้อ** การส่ง Config จาก Server ไปยังกลุ่ม Agent โดยอัตโนมัติ
เวลา 10.30 - 10.45 น.	พักรับประทานอาหารว่าง
เวลา 10.45 - 12.00 น.	***Wazuh Custom Rule & Decoder*** โดยวิทยากร นายวันเฉลิม นิธิมณีรัตน์ ตำแหน่งเจ้าหน้าที่ด้านความมั่นคงปลอดภัยไซเบอร์ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) **หัวข้อ** ความเข้าใจเรื่อง Log Analysis (Decoder vs Rule) **หัวข้อ** Lab: การเขียน Rule XML ขึ้นเองเพื่อจับ Log เฉพาะทาง ***Wazuh CDB List*** **หัวข้อ** การทำ White/Blacklist ด้วย CDB (Constant Database) **หัวข้อ** การนำ CDB มาใช้ร่วมกับ Rule เพื่อลด False Positive
เวลา 12.00 – 13.00 น.	พักรับประทานอาหารกลางวัน

*** กำหนดการอาจมีการเปลี่ยนแปลงได้ตามความเหมาะสม***

กำหนดการ

จัดฝึกอบรมเชิงปฏิบัติการหัวข้อ “การพัฒนาระบบตรวจจับและแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ด้วย Wazuh”

วันอังคารที่ 26 พฤษภาคม 2569 เวลา 08.30-16.00 น.

ณ ห้องประชุม Main Conference ชั้น 1 อาคารศูนย์บริการเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยนเรศวร

วันอังคารที่ 26 พฤษภาคม 2569

เวลา 13.00 – 14.30 น. ***Windows Sysmon Integration*** โดยวิทยากร นายวันเฉลิม นิธิมณีรัตน์
ตำแหน่งเจ้าหน้าที่ด้านความมั่นคงปลอดภัยไซเบอร์
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)
หัวข้อ ประโยชน์ของ Sysmon ในการดู Process เชิงลึก
หัวข้อ การติดตั้งและ Config Sysmon บน Windows
หัวข้อ การตั้งค่า Wazuh ให้ดึง Log จาก Sysmon
Linux AuditD Integration
หัวข้อ การใช้งาน Audit Framework บน Linux เพื่อตรวจสอบ System Call
หัวข้อ การเขียน Rule audit.rules และเชื่อมต่อกับ Wazuh

เวลา 14.30 – 14.45 น. พักรับประทานอาหารว่าง

เวลา 14.45 – 16.00 น. ***Zeek (Network Monitor)*** โดยวิทยากร นายวันเฉลิม นิธิมณีรัตน์
ตำแหน่งเจ้าหน้าที่ด้านความมั่นคงปลอดภัยไซเบอร์
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)
หัวข้อ การติดตั้ง Zeek เพื่อดึง Network Logs
หัวข้อ การตั้งค่า Wazuh ให้วิเคราะห์ไฟล์ Log ของ Zeek

*** กำหนดการอาจมีการเปลี่ยนแปลงได้ตามความเหมาะสม***