

Shift Up People : ปั่นกำลังคนไซเบอร์ให้พร้อมรับมือสิ่งที่ยังไม่รู้

จุดเริ่มต้น: Cybersecurity ในยุค OT + IT + IoT

- โลกอุตสาหกรรมกำลัง “หลอมรวม” ระบบ IT (ข้อมูล) กับ OT (เครื่องจักร/การผลิต)
- เกิดแนวคิด Smart Factory / Industry 4.0 ที่ต้องอาศัยความมั่นคงปลอดภัยไซเบอร์ขั้นสูง
- แนวคิดสำคัญ: “Data-Driven Manufacturing”

แนวปฏิบัติที่ถูกต้องในการทดสอบเจาะระบบ OT

การทำ VA/Pentest ในระบบ OT มีความสำคัญอย่างยิ่ง ในเบื้องต้นมีอะไรเป็นสิ่งที่ควรทำไม่ควรทำบ้าง

- ✓ Do: มีแผน Backup, แจ้งล่วงหน้า, ใช้ Simulation, เริ่มแบบ Safe
- ✗ Don't: ทดสอบ Production จริง, ปลอ่ย payload อันตราย, ไม่มี fallback



อ.ดร.กัณท์เทพพร ทาโรจน์

อาจารย์ประจำกลุ่มวิชาการคอมพิวเตอร์ มหาวิทยาลัยมหิดล

ปัญหาใหญ่ทั่วโลก: ขาดคนไซเบอร์ (Cyber Skills Gap)

- ขาดบุคลากรทั่วโลกกว่า 4.8 ล้านคน (ปี 2024) โดยเฉพาะเอเชียแปซิฟิกขาดแคลนมากที่สุด
- ความซับซ้อนของภัยไซเบอร์เพิ่มขึ้น เช่น AI phishing, ransomware, supply chain attack



กลยุทธ์สร้าง “ขุนพลไซเบอร์รุ่นใหม่”

- Upskill / Reskill: ฝึกอบรมเดิมให้เก่งขึ้น (76%)
- Recruit: หาผู้เชี่ยวชาญจากภายนอก (54%)
- Apprentice / Bootcamp: สร้างคนใหม่จากมหาวิทยาลัย (24%)
- Soft Skills สำคัญ: สื่อสารระหว่าง IT-OT, แก้ปัญหา, ทำงานร่วมกัน



บทบาทของสถาบันการศึกษา

- ต้อง “เปลี่ยนจากการสอน → การสร้างคน”
- สร้าง ecosystem ร่วมกับภาคอุตสาหกรรม
- ใช้ Active Learning / Lab / CTF / Hackathon
- บูรณาการกับทุกสาขา ไม่เฉพาะคอมพิวเตอร์

วิสัยทัศน์: “Proactive Cyber Hunter”

- บุคลากรไม่ใช่แค่ตามกฎ แต่ต้อง “ล่าภัยคุกคามเชิงรุก”
- เปลี่ยนจาก Rule Follower → Threat Hunter
- สร้างวัฒนธรรม “Living Sensor” — ทุกคนในองค์กรช่วยเฝ้าระวังภัย



สรุปและข้อคิด

- ขาดแคลนบุคลากรไซเบอร์
- สถาบันการศึกษามีบทบาทสำคัญ
- ผัง OT / IIoT มีความท้าทายเฉพาะ
- การศึกษา & พัฒนากำลังคนต้องตั้งใจ



ข้อคิดก้าวต่อไปสำหรับผู้ฟัง (สถาบัน / คณะ)

- สำรวจ gap
- เริ่มทดลองโครงการเล็ก ๆ
- เสาะหาความร่วมมือ
- ติดตามแนวโน้มใหม่

CYBER SKILLS GAP



ผศ.ดร.ฐิติพันธ์ ตันติธรรม

คณะเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยมหิดล