เอกสารลับ

FILE : OMEGA-99

ภัยคุกคาม ความเสี่ยง และจุดอ่อน

วิเคราะห์ภูมิทัศน์ความมั่นคงปลอดภัยในโลกสมัยใหม่

SECURE LINE:
ACTIVE

DATA STREAM:

DATA STREAM:
ANALOG

YJING JI JILL REC

FILE: OMEGA-99
ACCESS LEVEL: RED

DECLASSIFIED/
สำหรับเผยแพร่เพื่อการศึกษา

ACCESS LEVEL: RED

เมื่อจุดอ่อนเพียงจุดเดียว เปลี่ยนแปลงทุกสิ่ง

SECRET

ทฤษฎีอุบัติเหตุแบบปกติ (Normal Accident Theory)

- **ภัยคุกคาม** (The Threat): เดนนิส เนดรี (Dennis Nedry) แสวงหาผลประโยชน์ทางการเงิน
- **อาวุธที่ใช้** (The Weapon): สิทธิ์ในการเข้าถึง (Authorized Access) และความรู้ลึกซึ้งในระบบ
- **จุดอ่อน** (The Vulnerability): การพึ่งพาคนเพียงคนเดียว (Single Point of Failure), ขาดระบบสำรอง, และขาดการแบ่งแยกหน้าที่

ภัยคุกคามไม่ได้กลายเป็นหายนะด้วยตัวมันเอง แต่มันต้องอาศัยการเจาะผ่านจุดอ่อน

สมการความเสี่ยง:
คัดแยกตัวแปรแห่งความสูญเสีย

SECRET

ภัยคุกคาม (Threat)
สิ่งที่อาจเกิดขึ้น (แฮกเกอร์, พายุ)
- ควบคุมไม่ได้

$$Risk = f(Threats, Vulnerability, Impacts)$$

จุดอ่อน (Vulnerability)
ช่องโหว่ของระบบ (ซอฟต์แวร์เก่า, รั้วเตี้ย)
- ควบคุมได้

มูลค่าสินทรัพย์ (Asset Value)
สิ่งที่ต้องปกป้อง

อุกกาบาตชนโลก คือภัยคุกคามร้ายแรง แต่มีความเสี่ยง (Risk) ต่ำเพราะโอกาสเกิดน้อย ตรงข้ามกับ สายไฟเก่าในโรงงาน ที่มีความเสี่ยงสูงกว่ามากและต้องจัดการทันที

SECRET

เมทริกซ์จำแนกภัยคุกคาม (Threat Matrix)

ภัยคุกคามภายนอก (External)	ภัยคุกคามภายใน (Internal)
- อาชญากรรมพื้นฐาน	- การก่อวินาศกรรม
- ภัยธรรมชาติ	- ความประมาท
- การก่อการร้าย	- การละเมิดนโยบาย
- โจมตีทางไซเบอร์จากแฮกเกอร์	- การขโมยข้อมูล

HYBRID THREATS (ภัยคุกคามแบบผสม)

เกลือเป็นหนอน: 60% ของการละเมิดข้อมูลเกิดจากภัยคุกคามภายใน

สถิติเตือนใจ: พนักงานที่กำลังจะลาออก 59% นำข้อมูลความลับของบริษัทติดตัวไปด้วย

TERMINAL GREEN

TOP SECRET

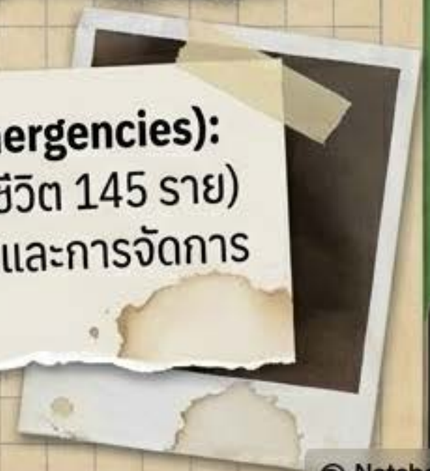
ภูมิทัศน์ภัยคุกคามฉบับท้องถิ่น (Local Intelligence)

CLASSIFIED

อาชญากรรมข้ามชาติ & Hybrid Scams:
แก๊งคอลเซ็นเตอร์, การใช้ AI/Deepfake
จากพื้นที่สีเทาชายแดน (เช่น KK Park)

ความไม่สงบ (Insurgency):
การลอบวางระเบิดแสวงเครื่อง (IEDs)
ที่มุ่งสร้างผลกระทบทางจิตวิทยา
ทับซ้อนกับเครือข่ายธุรกิจผิดกฎหมาย

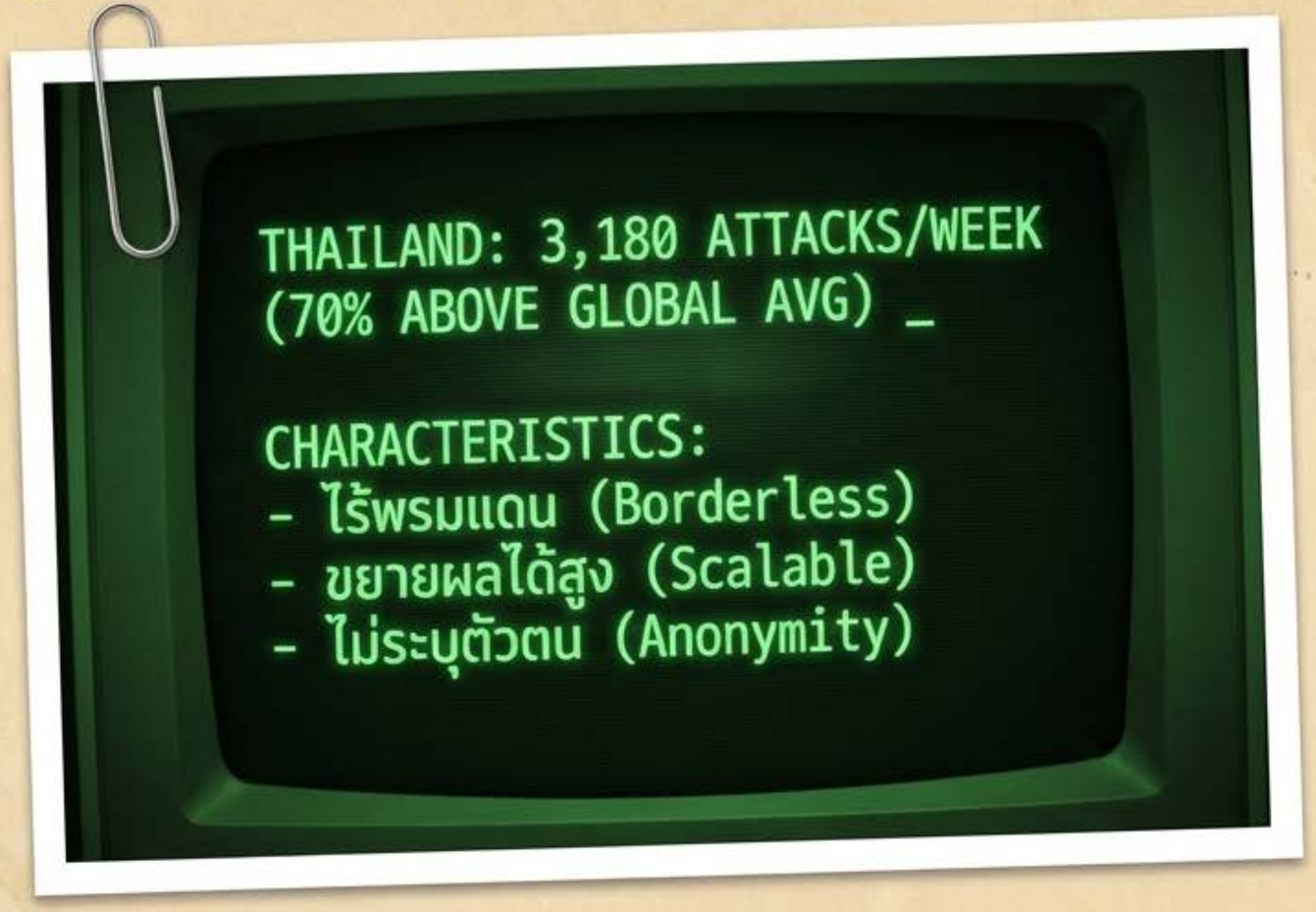
ภาวะฉุกเฉินซับซ้อน (Complex Emergencies):
มหาอุทกภัยหาดใหญ่ 2025 (ผู้เสียชีวิต 145 ราย)
วิกฤตซ้อนวิกฤตจากการสื่อสารล่มและการจัดการ
ที่แยกส่วน



CONFIDENTIAL

TERMINAL GREEN

สมรภูมิดิจิทัล: ภัยคุกคามทางไซเบอร์ที่ไร้พรมแดน



CRITICAL ALERT: OT/ICS ATTACKS

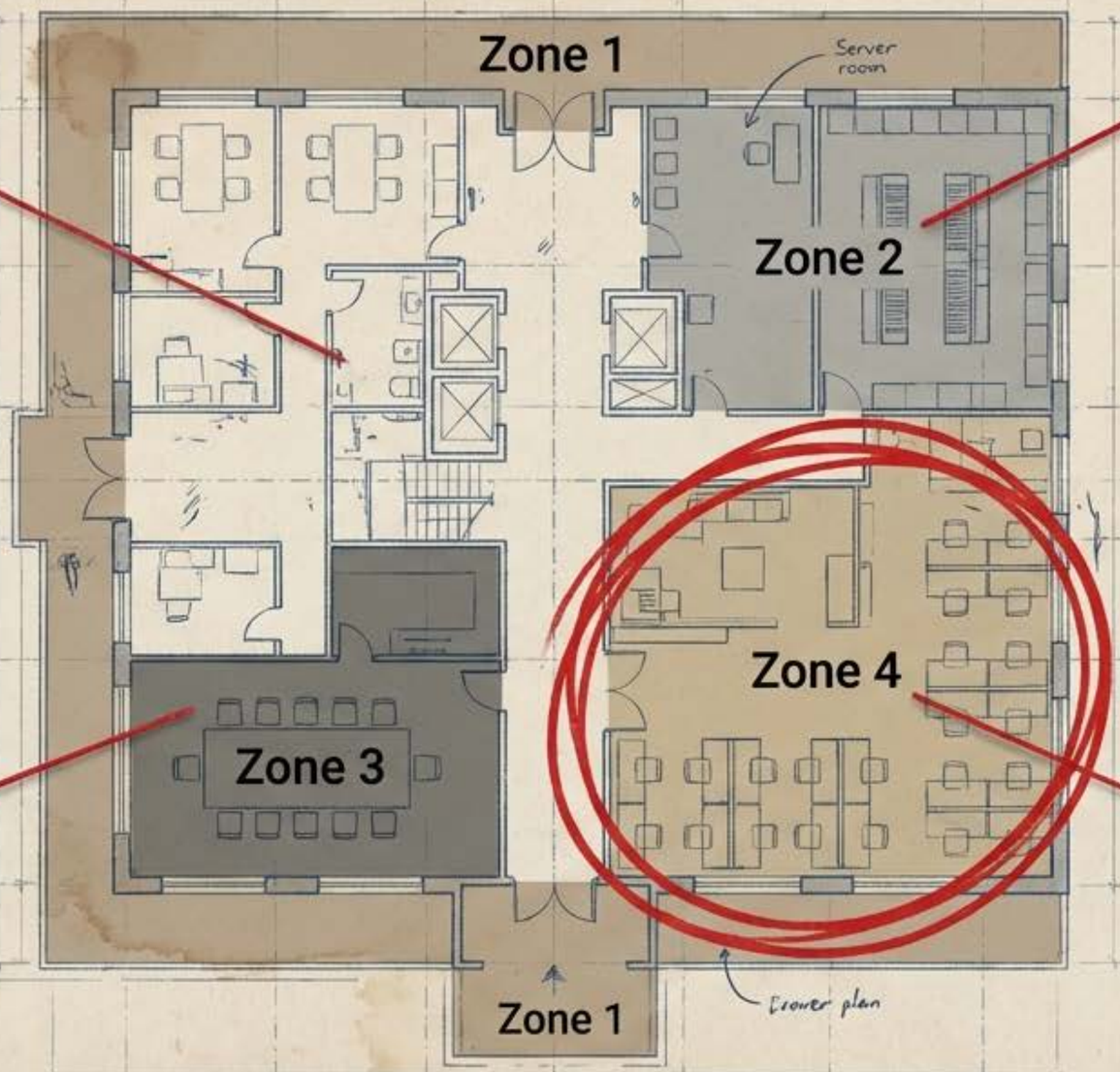
เป้าหมายเปลี่ยนไป: ไม่ใช่แค่ขโมยข้อมูล แต่คือ Ransomware ที่มุ่งโจมตีโครงสร้างพื้นฐาน (โรงพยาบาล, ระบบควบคุมไฟฟ้า, ระบบประปา) การโจมตีทางไซเบอร์ในปัจจุบันสร้างความเสียหายทางกายภาพได้โดยตรง

โครงสร้างความเปราะบาง 4 มิติ

TOP SECRET

โซน 1: กายภาพ (Physical)

รั้วเตี้ย, กล้องวงจรปิดมีจุดบอด, ทางหนีไฟถูกปิดตาย (กรณีศึกษา: ชานติก้าผับ)



โซน 2: เทคโนโลยี (Technical)

ระบบปฏิบัติการล้าสมัย (Legacy Systems), การใช้ Shadow IT (เช่น ส่งไฟล์งานลับผ่าน LINE ส่วนตัว)

โซน 3: องค์กร (Organizational)

ขาดการสื่อสารข้ามแผนก, งบประมาณความปลอดภัยไม่เพียงพอ, โครงสร้างบัญชาการที่ซับซ้อน

โซน 4: มนุษย์ (Human)

CRITICAL ALERT

ห่วงโซ่ที่อ่อนแอที่สุด! มากกว่า 90% ของการละเมิดไซเบอร์เกิดจากความผิดพลาดของมนุษย์ (Phishing, อ่อนล้า, รหัสผ่านง่าย)

จุดอ่อนเชิงสังคมและวัฒนธรรมไทย (Socio-Cultural Intel)

ความ เกรงใจ - เพชฌฆาตเงียบในงานความปลอดภัย
ผู้น้อยไม่กล้าทักท้วงผู้ใหญ่เมื่อเห็นความไม่ปลอดภัย
หรือยอมเปิดประตูให้เพราะความเห็นใจ

Silent killer in security!

"ไม่เป็นไร" วัฒนธรรม ไม่เป็นไร (Sabai Sabai) -
ทัศนคติที่ยอมรับความเสี่ยงเล็กๆ น้อยๆ นำไปสู่การละเลย
กฎระเบียบอย่างเป็นระบบ (Weak Safety Culture)

Systemic neglect!

ระบบอุปถัมภ์ (ระบบอุปถัมภ์ (Patronage System) -
การแต่งตั้งบุคลากรดูแลความปลอดภัยตามความใกล้ชิด
มากกว่าความสามารถ (Competency)

Competency over connection!

ช่องว่างแห่งความกลัว (Actual vs. Perceived Risk)

มนุษย์ตัดสินความเสี่ยงจาก ความรู้สึก มากกว่าสถิติ

การรับรู้ความเสี่ยงที่สูงเกินจริง

การก่อการร้าย, การกราดยิง (Dread Risks).
ขยายตัวด้วย Mean World Syndrome
จากสื่อโซเชียล

DREAD RISKS

ภัยเงียบที่ถูกมองข้าม

- อุบัติเหตุทางถนน (เสียชีวิต 50-60 ศพ/วัน)

- ฝุ่น PM 2.5: ภัยคุกคามแบบช้า ๆ (Slow-onset Hazard) บั่นทอนทรัพยากรมนุษย์ สร้างภาระสาธารณสุข และลดผลิตภาพทางเศรษฐกิจอย่างมหาศาล

SILENT KILLER

การวิเคราะห์อาชญากรรม (Crime Analysis)

การวิเคราะห์เชิงยุทธวิธี (Tactical)

ระยะสั้น (วัน-สัปดาห์).
ระบุรูปแบบ (MO) และจุดเกิดเหตุ (Hot spots)
เพื่อหยุดยั้งเหตุการณ์เฉพาะหน้า

การวิเคราะห์เชิงกลยุทธ์ (Strategic)

ระยะยาว (เดือน-ปี).
ค้นหาสาเหตุรากเหง้า (Root Causes)
เพื่อวางแผนนโยบายและจัดสรร
งบประมาณล่วงหน้า

การวิเคราะห์บริหารงาน (Administrative)

การรายงานสรุปสถิติเพื่อความโปร่งใส
ยืนยันการปฏิบัติตามกฎหมาย (เช่น PDPA)
และชี้แจงผู้มีส่วนได้ส่วนเสีย

การป้องกันอาชญากรรมผ่านการออกแบบ (CPTED)

BEFORE: สภาพแวดล้อมที่เอื้อต่ออาชญากรรม

AFTER: สถาปัตยกรรมป้องกันภัย

1 แสงสว่าง (Lighting): ลบจุดอับแสง เพิ่มโอกาสการตรวจจับ

2 แนวสายตา (Visibility): การเฝ้าระวังตามธรรมชาติ (Natural Surveillance)

3 ความเป็นระเบียบ: ทฤษฎีหน้าต่างแตก (Broken Windows Theory)

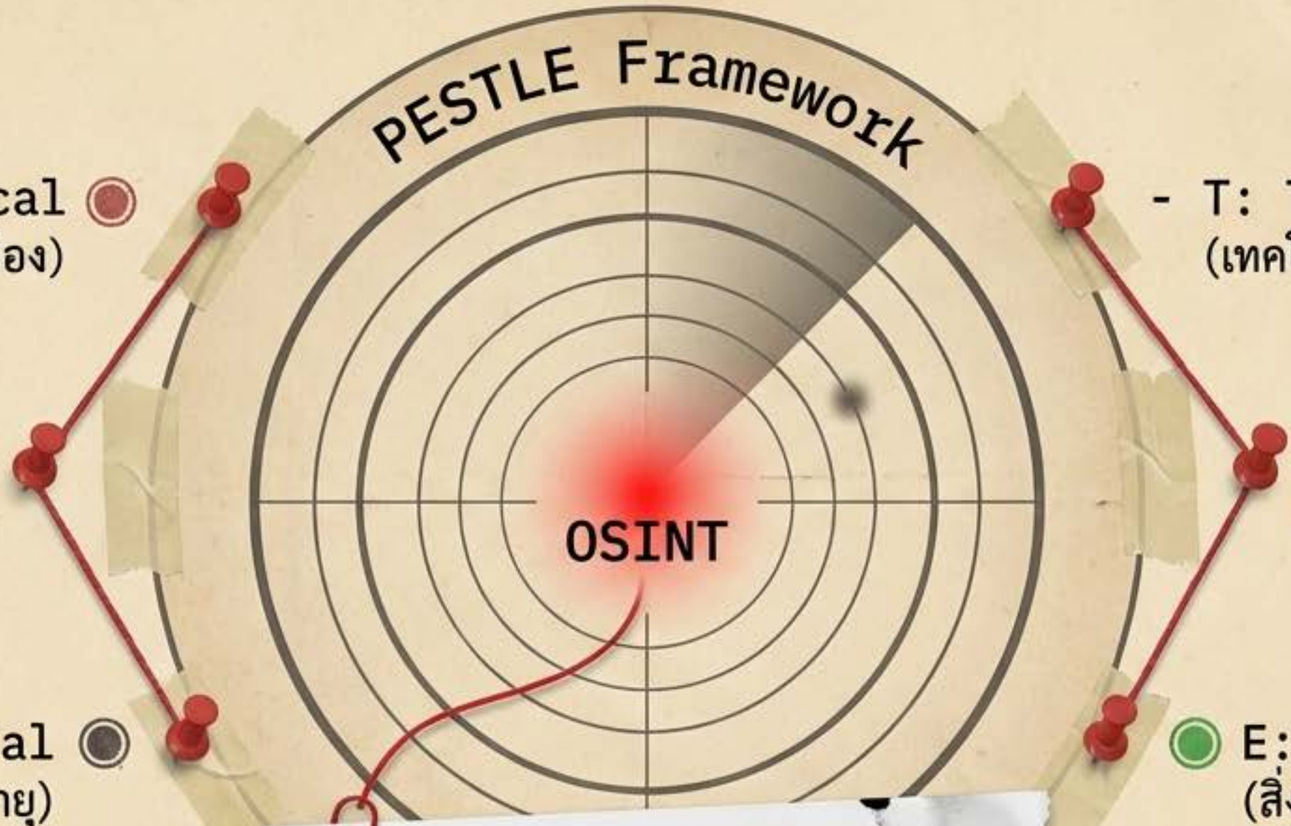
- พื้นที่รกร้างดึงดูดอาชญากรรม

CLASSIFIED

4 เส้นทางหลบหนี (Escape Routes): การสร้างทางดันหรือจำกัดทางออก ช่วยป้องปรามผู้กระทำผิดที่ต้องการหนีอย่างรวดเร็ว (เช่น สถานี MRT)

การข่าวกรองและการสแกนขอบฟ้า (Strategic Foresight)

CLASSIFIED



- P: Political
(การเมือง)

- E: Economic
(เศรษฐกิจ)

- S: Social
(สังคม เช่น สังคมผู้สูงอายุ)

- T: Technological
(เทคโนโลยี เช่น AI/Deepfake)

L: Legal
(กฎหมาย เช่น PDPA)

E: Environmental
(สิ่งแวดล้อม เช่น
อุทกภัยรุนแรง)

ข่าวกรองจากแหล่งข้อมูลสาธารณะ
(โซเชียลมีเดีย, ข่าว, ประกาศราชการ)
เพื่อระบุสัญญาณบ่งชี้ความเสี่ยงตั้งแต่เนิ่น ๆ

INTELLIGENCE BRIEFING

บทสรุปปฏิบัติการ: สถาปัตยกรรมความปลอดภัยที่ยืดหยุ่น

CLASSIFIED

- **ความจริงแห่งการป้องกัน:** องค์กรไม่สามารถกำจัดภัยคุกคามได้ทั้งหมด แต่สามารถลดจุดอ่อน ได้
- **บูรณาการข้อมูล:** เปลี่ยนจากการตั้งรับแบบเดิม เป็นการใช้ข่าวกรอง (OSINT) และการวิเคราะห์สภาพแวดล้อมเชิงรุก
- **บริบทคือหัวใจ:** การคัดลอกระบบสากลมาใช้จะล้มเหลว หากไม่ปรับเทียบให้เข้ากับวัฒนธรรม ภูมิศาสตร์ และวิถีชีวิตของสังคมไทย

> ความปลอดภัยมิได้อยู่แค่การสร้างกำแพงสูง
> แต่อยู่ที่การเข้าใจธรรมชาติของความเสี่ยง
> ที่อยู่ทั้งนอกและในกำแพงนั้น

APPROVED / อนุมัติ