

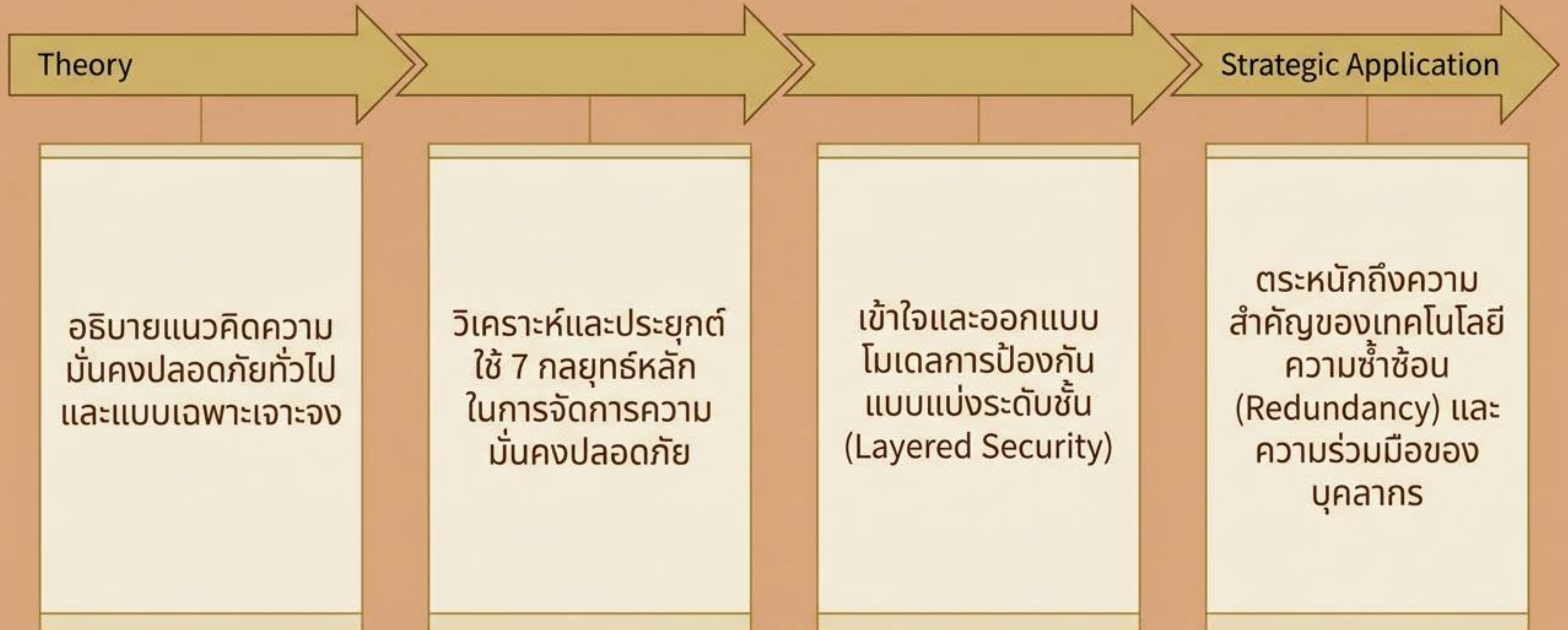


บทที่ 4 กลยุทธ์การรักษาความมั่นคงปลอดภัย (Security Strategies)

รายวิชา: SEM1201 การบริหารและการจัดการความมั่นคง (Introduction to Security Management)
ผู้บรรยาย: ผศ.ดร.หทัยพันธุ์ สุนทรพิพิธ

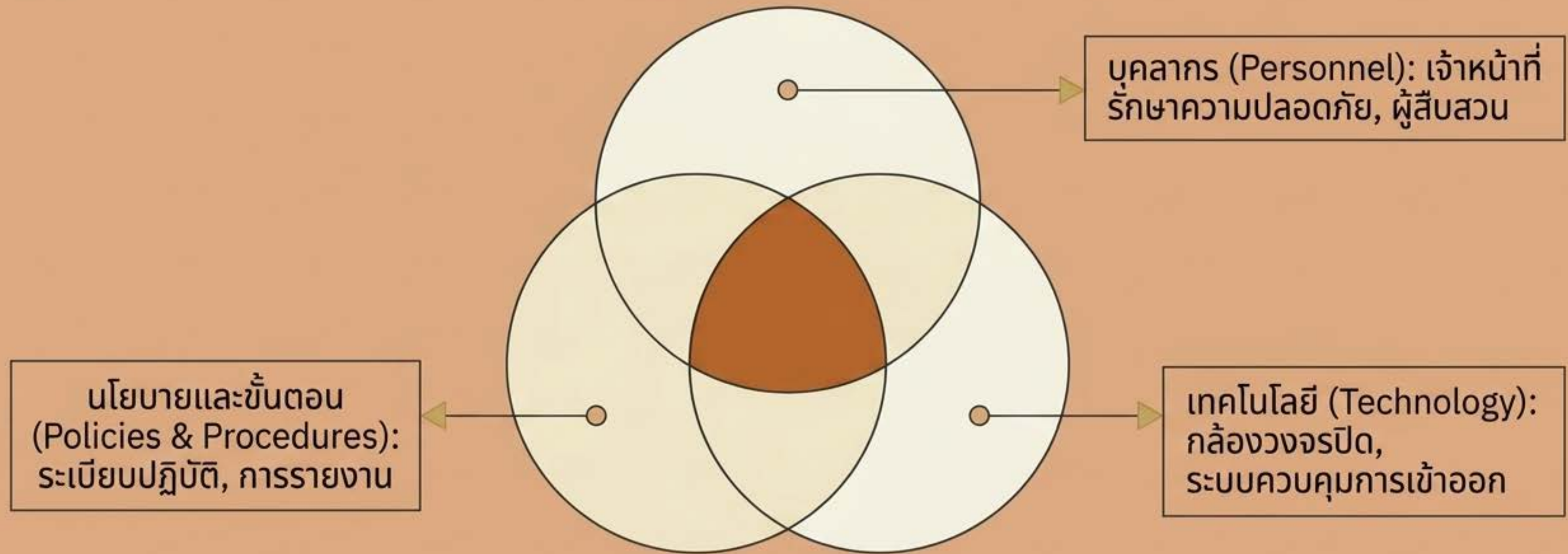
สร้างรากฐานความมั่นคงปลอดภัยผ่านกลยุทธ์ที่เชื่อมโยงกันอย่างเป็นระบบ

วัตถุประสงค์การเรียนรู้ (Learning Objectives)



ความหมายและองค์ประกอบของกลยุทธ์ความมั่นคงปลอดภัย

การประยุกต์ใช้ทรัพยากรบุคคล เทคโนโลยี และนโยบายเข้าด้วยกัน



ความมั่นคงปลอดภัยที่มีประสิทธิภาพเกิดจากการบูรณาการคน นโยบาย และเทคโนโลยี

การรักษาความมั่นคงปลอดภัยทั่วไป (Generic Security)

แนวทางการป้องกันขั้นพื้นฐานที่ใช้กัน
อย่างแพร่หลายในทุกอุตสาหกรรม

ครอบคลุมการปฏิบัติงานประจำวัน
ของบุคลากรตามนโยบายองค์กร

กำหนดมาตรฐาน เช่น การแลกบัตร
ผู้มาติดต่อ และการติดป้ายชื่อ

ใช้เทคโนโลยีพื้นฐาน เช่น CCTV และ
ระบบเตือนภัย



รากฐานมาตรฐานที่ทุกองค์กรต้องมีเพื่อความปลอดภัยขั้นต้น

การรักษาความมั่นคงปลอดภัยเฉพาะ (Specific Security)

ออกแบบพิเศษเพื่อตอบสนองความท้าทายและภัยคุกคามเฉพาะของหน่วยงาน



โรงพยาบาล: เน้นการจัดการผู้ป่วยจิตเวชหรือการควบคุมโรคติดต่อ



ร้านค้าปลีก: ใช้ระบบป้องกันการขโมยสินค้า (EAS)



การทหาร: ปรับเปลี่ยนมาตรการหลังวิกฤต เช่น เหตุการณ์โจมตีเรือรบ USS Cole

ภัยคุกคามเฉพาะรูปแบบ ต้องการกลยุทธ์ที่ปรับแต่งมาอย่างเจาะจง

เปรียบเทียบกลยุทธ์: ทัวไป vs. เฉพาะเจาะจง

- นักวางแผนที่ดีมักเริ่มจาก Generic แล้วจึงปรับปรุงเป็น Specific
- กลยุทธ์ทั้งสองต้องทำงานประสานกัน ไม่สามารถแยกขาดจากกันได้
- ความเสี่ยงและประวัติดูเหตุการณ์จะเป็นตัวกำหนดระดับการปรับแต่ง

ลักษณะ (Aspect)	ทัวไป (Generic)	เฉพาะเจาะจง (Specific)
เป้าหมาย (Goal)	มาตรฐานความปลอดภัยพื้นฐาน	ตอบสนองความเสี่ยงเฉพาะอุตสาหกรรม
เทคโนโลยี (Tech)	CCTV, รั้ว, บัตรประจำตัว	EAS, เซ็นเซอร์วัตถุระเบิด, Honeypots
ตัวอย่าง (Example)	อาคารสำนักงานทัวไป	โรงพยาบาลจิตเวช, ฐานทัพทหาร

การออกแบบความปลอดภัยที่ดี เริ่มต้นที่มาตรฐานและจบลงที่ความเหมาะสมเฉพาะตัว

กลยุทธ์ที่ 1: การป้องปราม (Deterrence)

เป้าหมาย: ป้องกันและยับยั้งไม่ให้เกิดอาชญากรรมตั้งแต่ต้น

วิธีการ: การลาดตระเวน, การแสดงตนของเจ้าหน้าที่, บทลงโทษที่รุนแรง

พื้นฐานทฤษฎี: อาศัย 'การเลือกอย่างมีเหตุผล' (Rational Choice Theory)

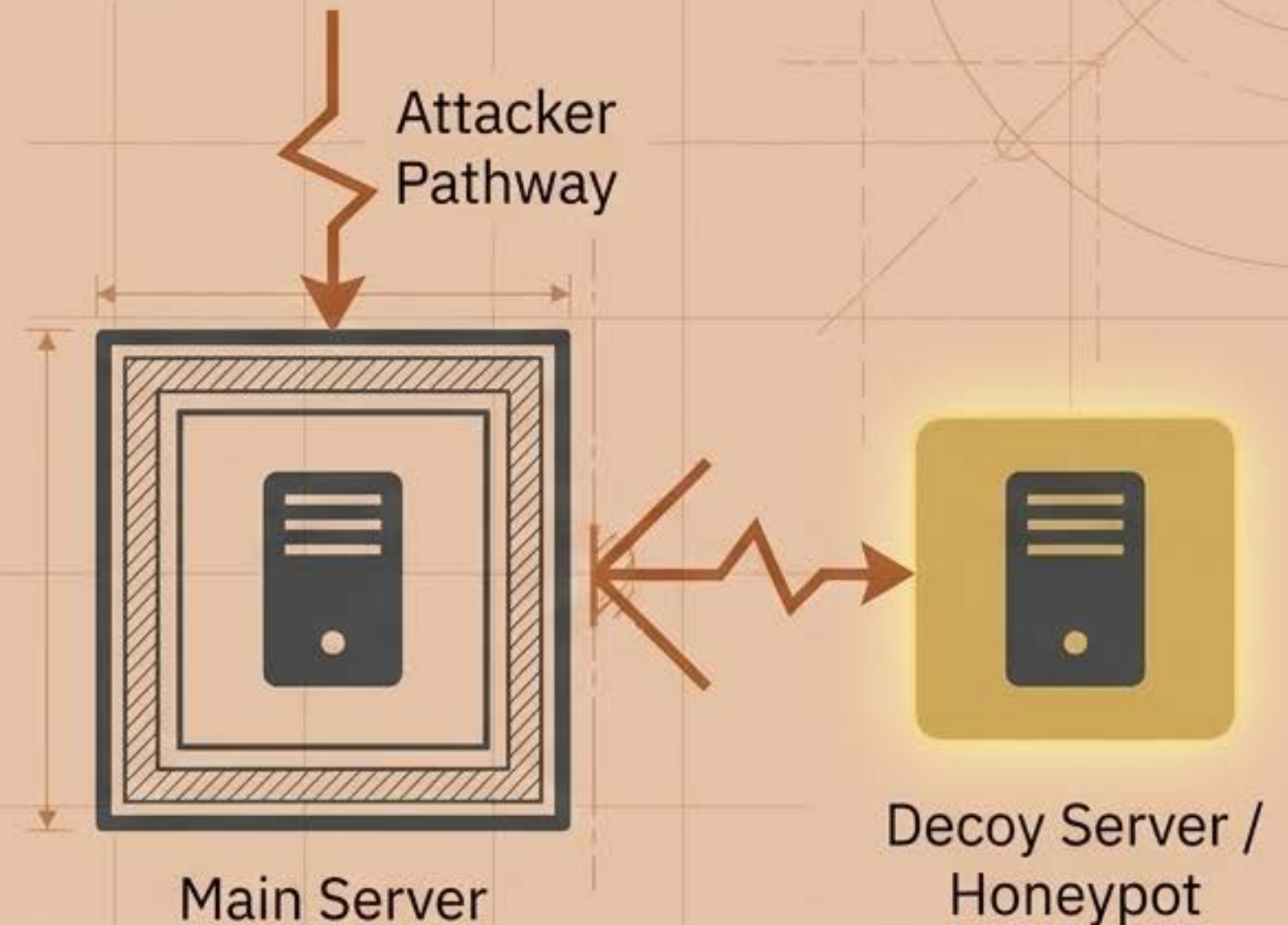
หลักการ: ทำให้ผู้ก่อเหตุรับรู้ว่ 'ความเสี่ยงและต้นทุน' สูงกว่า 'ผลประโยชน์'



เปลี่ยนความคิดผู้ก่อเหตุ โดยทำให้ความเสี่ยงมีมากกว่าผลตอบแทน

กลยุทธ์ที่ 2: การลวง (Deception)

- **เป้าหมาย:** สร้างความสับสนและเปลี่ยนเส้นทางภัยคุกคาม
- **ทางกายภาพ:** พรางตาสถานที่สำคัญให้ดูเป็นพื้นที่เป้าหมายรอง
- **ทางไซเบอร์ (Honeypots/Honeynets):** สร้างระบบเครือข่ายล่อลวงแฮกเกอร์
- **ประโยชน์:** สังเกตพฤติกรรมผู้โจมตีโดยไม่กระทบระบบจริง

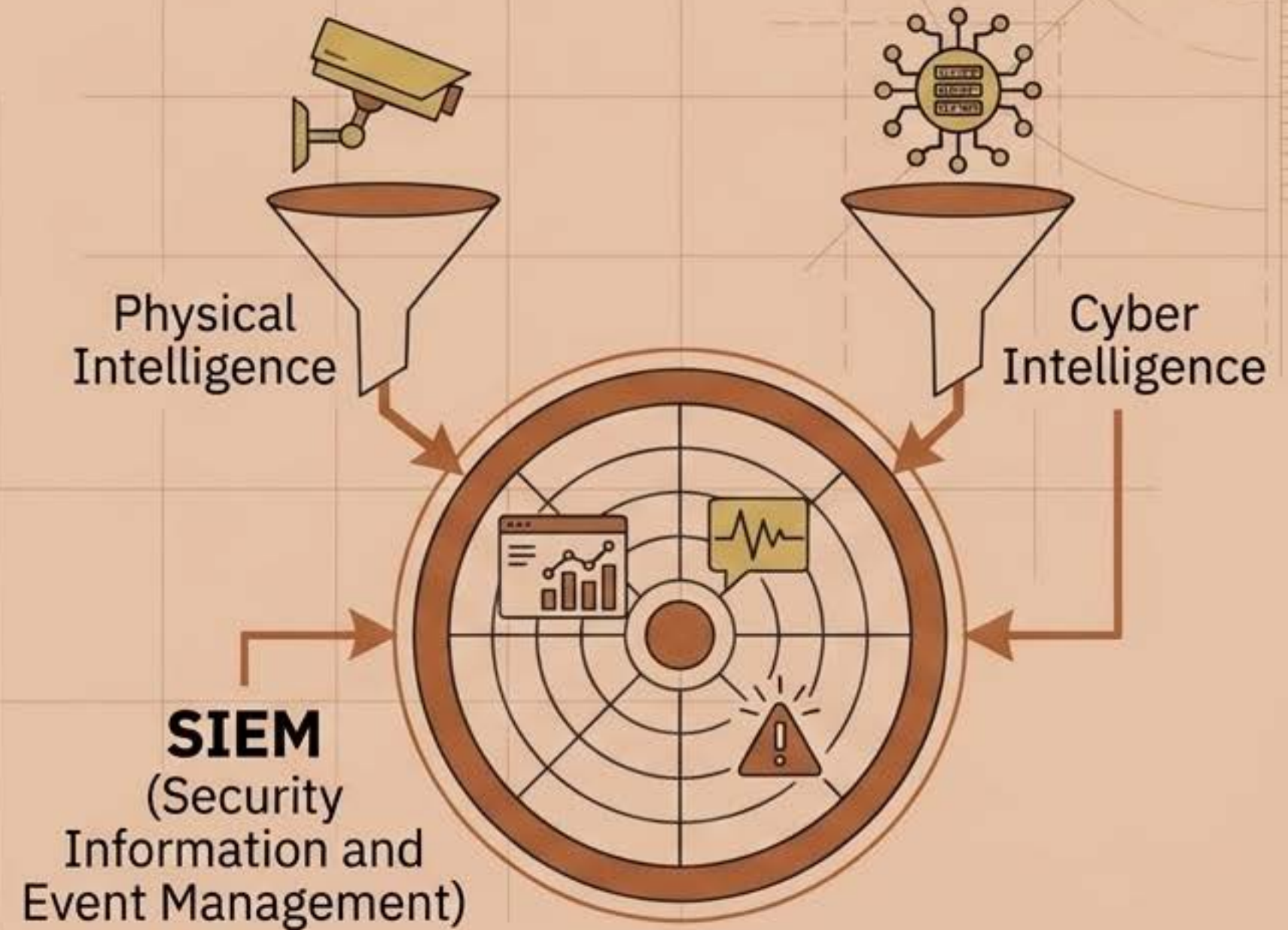


FEMA, 2003; Peter & Schiller, 2008

การลวงคือการรุกเชิงรับ ควบคุมทิศทางของผู้บุกรุกเพื่อปกป้องระบบหลัก

กลยุทธ์ที่ 3: การตรวจจับ (Detection)

- **เป้าหมาย:** ระบุภัยคุกคามเชิงรุกและต่อเนื่องเมื่อการป้องกันล้มเหลว
- **ทางกายภาพ:** กล้องวงจรปิด (CCTV), เครื่องข่ายเพื่อนบ้านเตือนภัย, ข่าวกอง
- **ทางไซเบอร์:** ระบบตรวจจับการบุกรุก (IDS), โปรแกรม SIEM
- รวบรวมและวิเคราะห์ข้อมูลจากหลายแหล่งแบบอัตโนมัติ



ยิ่งตรวจพบได้เร็วเท่าใด ความสูญเสียก็จะยิ่งน้อยลงเท่านั้น

กลยุทธ์ที่ 4: การหน่วง (Delay)

- **เป้าหมาย:** ชื้อเวลาให้ทีมรักษาความปลอดภัยเพื่อตรวจจับและตอบสนอง
- **ทางกายภาพ:** ประตุนิรภัยลิคคแน่นหนา, การออกแบบเส้นทางคดเคี้ยว
- **ทางไซเบอร์:** การยืนยันตัวตนหลายปัจจัย (MFA), เครื่องมือ EDR
- ยิงหน่วงเวลาได้นาน ความเครียดของผู้ก่อเหตุยิ่งเพิ่มขึ้น

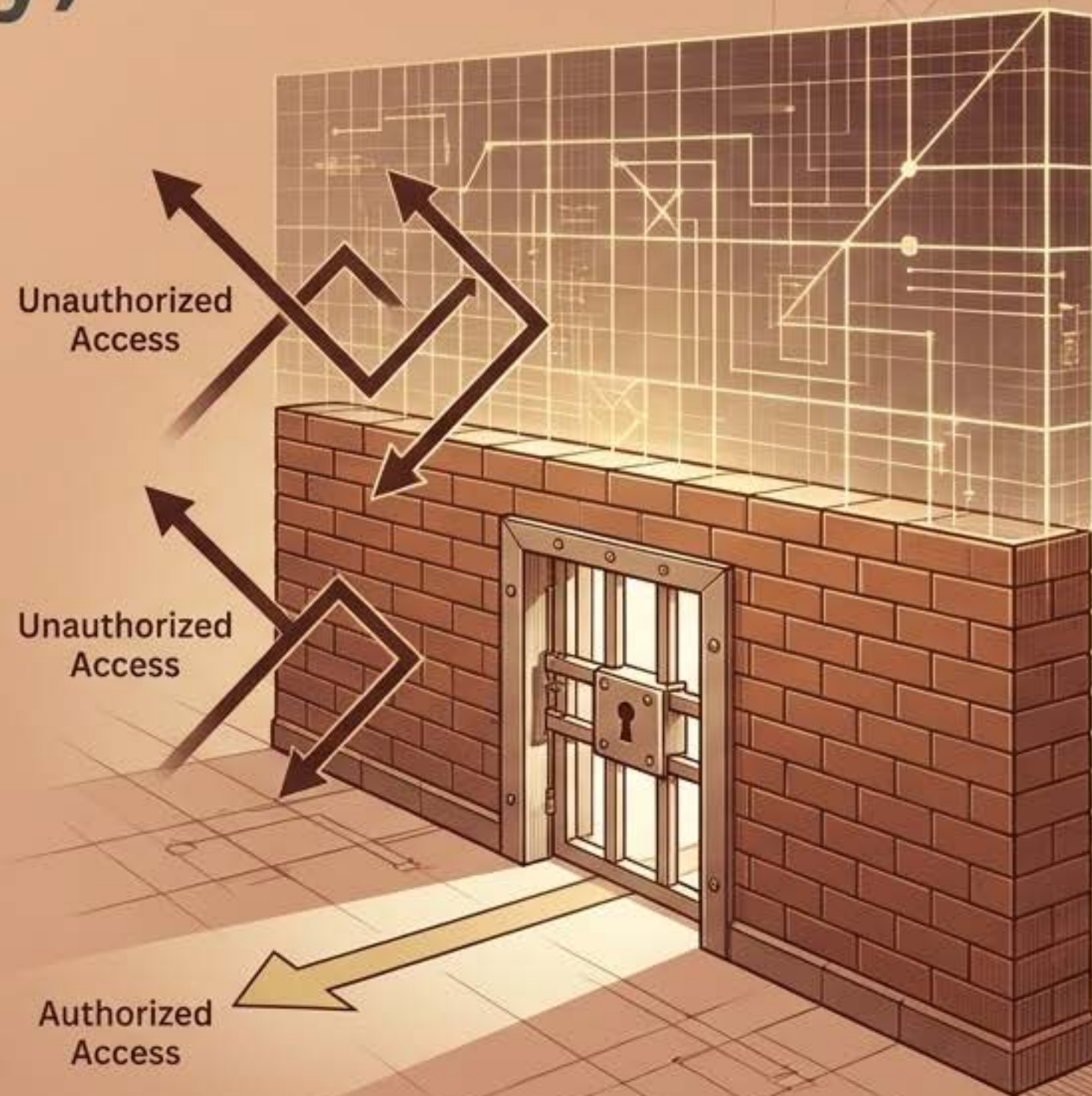


Secret Double Octopus, 2023

เวลาคือเกราะป้องกัน การสร้างความล่าช้าคือการเพิ่มโอกาสจับกุม

กลยุทธ์ที่ 5: การยับยั้ง (Deny)

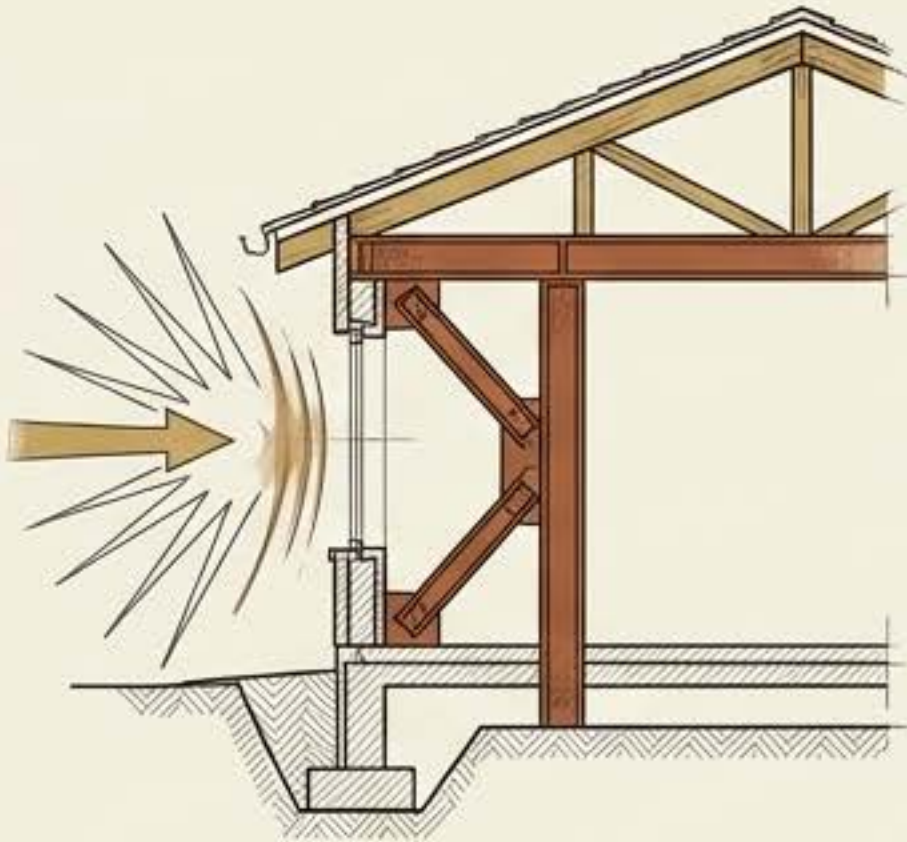
- **เป้าหมาย:** ป้องกันการเข้าถึงบุคคล ข้อมูล หรือทรัพย์สินโดยเด็ดขาด
- **กลไกการควบคุม:** การให้สิทธิ์ขั้นต่ำ (Least Privilege), การตรวจสอบสิทธิ์
- **ทางไซเบอร์:** ไฟร์วอลล์ (Firewalls), การแบ่งส่วนเครือข่าย, ระบบ IDS/IPS
- **ทางกายภาพ:** ตู้เซฟ, สิ่งกีดขวางที่แข็งแกร่งทนทาน



ตัดโอกาสการเข้าถึงโดยเด็ดขาด สร้างปราการที่ยากต่อการเจาะทะลุ

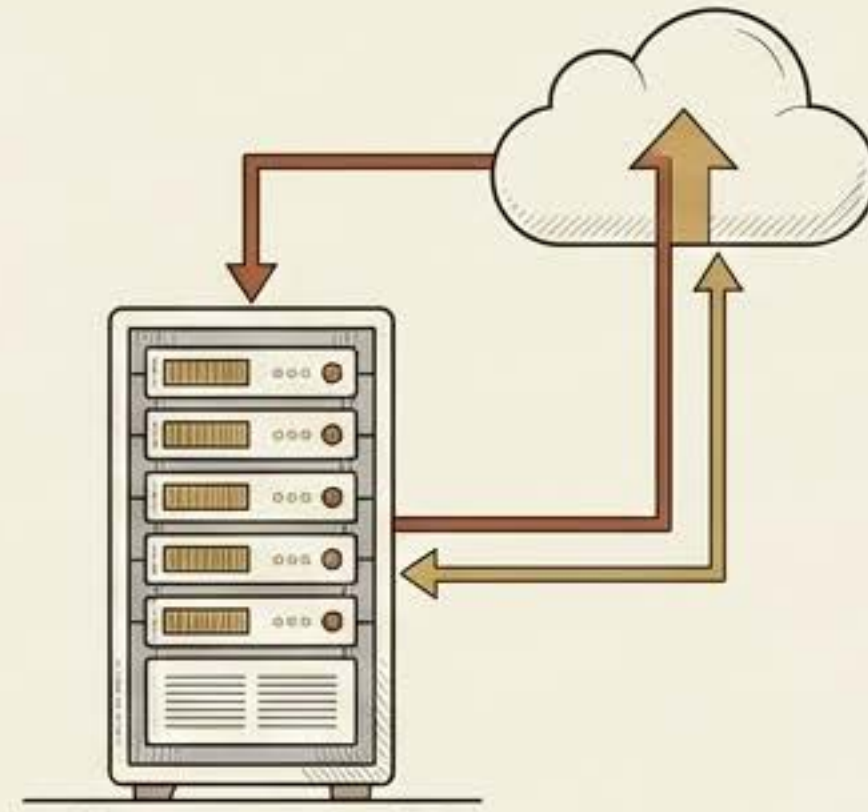
กลยุทธ์ที่ 6: การบรรเทา (Mitigate)

เป้าหมาย: ลดขนาดผลกระทบและจำกัดความเสียหายหลังเกิดเหตุ
ปกป้องชีวิตและจำกัดการลุกลามของเหตุการณ์



ทางกายภาพ: การเสริมความแข็งแรงของ
อาคารเพื่อต้านทานแรงระเบิด

FEMA, 2003

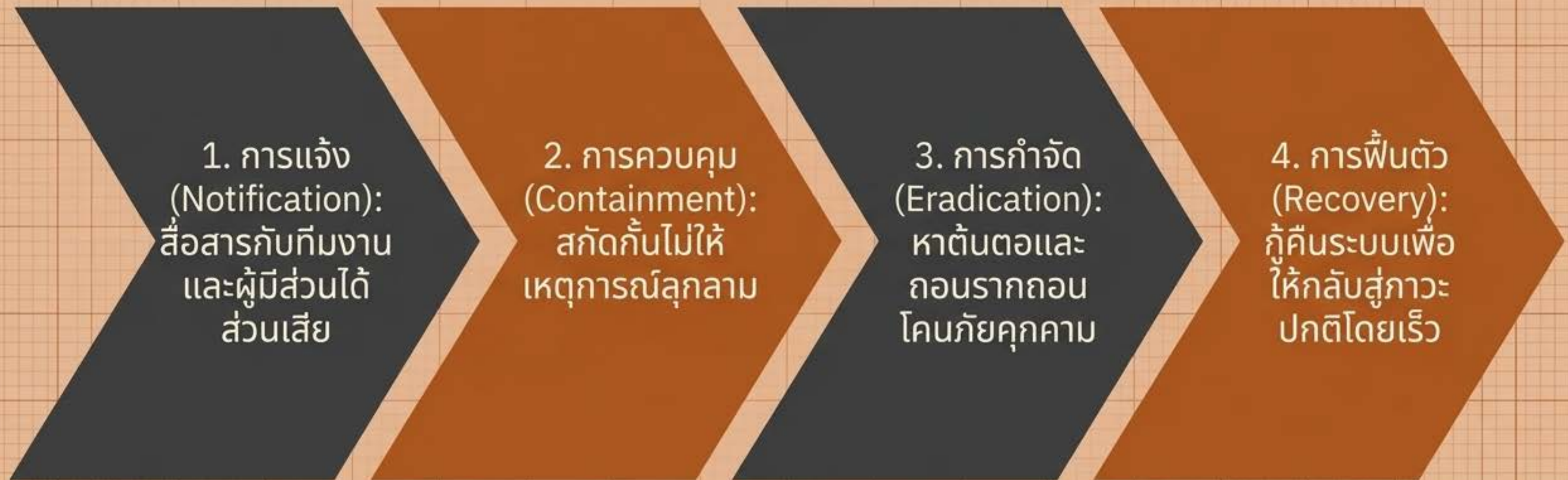


ทางไซเบอร์: การแยกส่วนระบบที่ติดมัลแวร์,
การอัปเดตแพตช์, การสำรองข้อมูล

เมื่อหลีกเลี่ยงความเสียหายไม่ได้ ต้องจำกัดวงและควบคุมให้ไวที่สุด

กลยุทธ์ที่ 7: การตอบสนอง (Respond)

เป้าหมาย: จัดการแก้ไขและฟื้นฟูอย่างเป็นระบบ



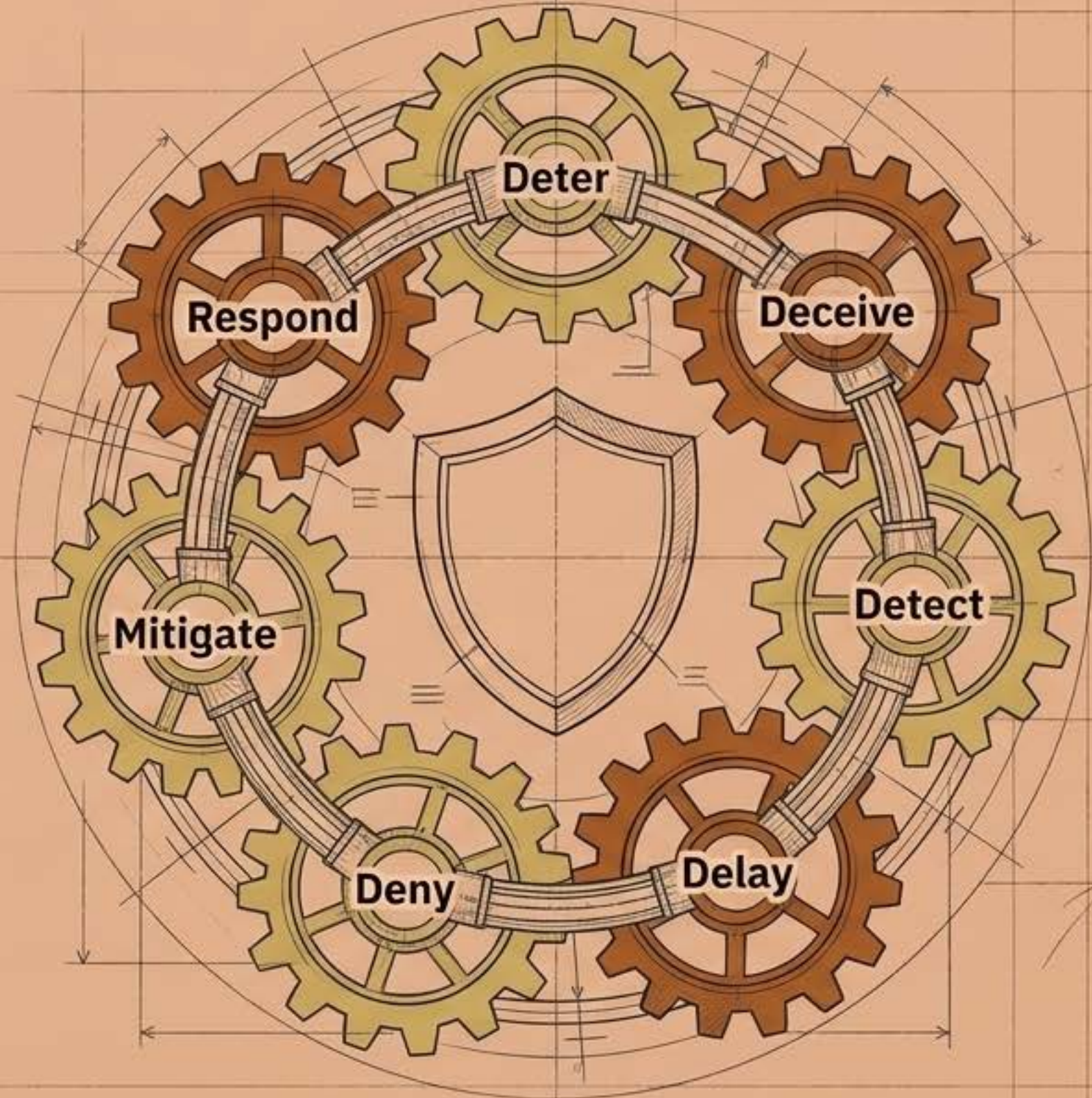
การเผชิญเหตุที่มีประสิทธิภาพ ต้องดำเนินการตามขั้นตอนที่วางแผนไว้อย่างเคร่งครัด

บูรณาการ 7 กลยุทธ์: วงจรความมั่นคงปลอดภัย

กลยุทธ์ทั้ง 7 ทำงานเชื่อมโยงกัน
ในลักษณะวงจรที่ไม่มีจุดสิ้นสุด

เป็นกระบวนการที่ต่อเนื่องและ
สนับสนุนซึ่งกันและกัน

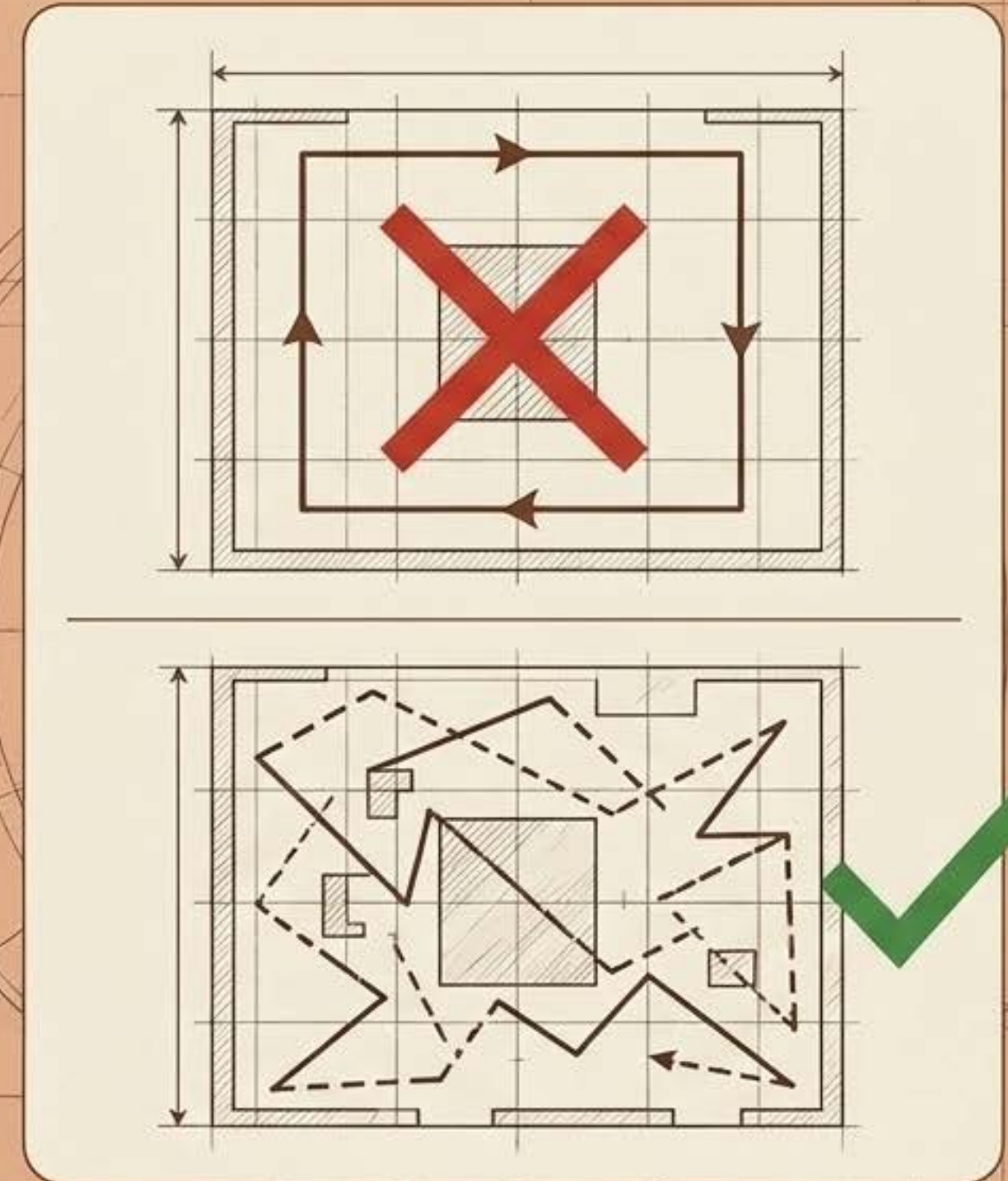
หากชิ้นใดล้มเหลว กลยุทธ์ถัดไป
จะทำหน้าที่รับช่วงต่อทันที



กลยุทธ์ความมั่นคงปลอดภัยไม่ใช่ทางเลือกเดียว แต่คือฟันเฟืองที่ต้องหมุนร่วมกัน

ความไม่แน่นอน: หัวใจของ การป้องกันที่คาดเดาไม่ได้

- หลีกเลียงรูปแบบการทำงานที่ซ้ำซากจำเจ (Creatures of habit)
- การลาดตระเวน: เปลี่ยนแปลงเวลาและเส้นทางอย่างสม่ำเสมอ
- ทางกายภาพ: สุ่มตรวจสอบยานพาหนะหรือย้ายจุดตั้งกล้องวงจรปิด
- ป้องกันไม่ให้ฝ่ายตรงข้ามคาดเดาช่องโหว่ได้

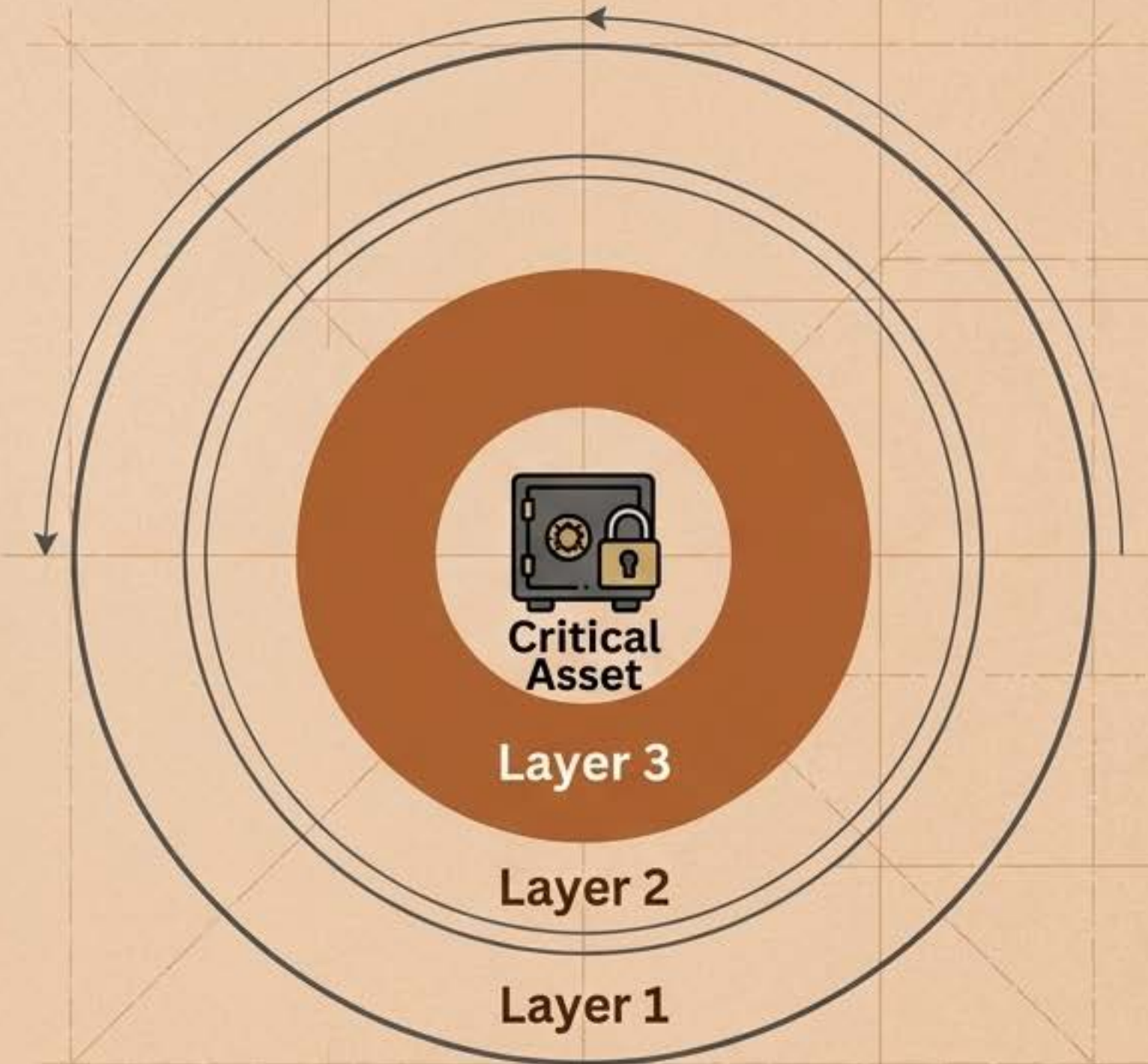


Purpura, 2018

ความสามารถในการคาดเดาไม่ได้ คืออาวุธที่ทรงพลังที่สุดของผู้ป้องกัน

แนวคิดระดับชั้นความมั่นคงปลอดภัย (Security Layers)

- การแบ่งเขตป้องกันแบบวงกลมที่มีจุดศูนย์กลางเดียวกัน (Concentric circles)
- ชั้นที่ 1 (Outer): ภายนอกขอบเขตพื้นที่เน้นการป้องกัน
- ชั้นที่ 2 (Intermediate): ระหว่างขอบเขตและตัวอาคาร เน้นการควบคุม
- ชั้นที่ 3 (Inner): ทรัพย์สินหรือตัวอาคาร เน้นการปกป้องขั้นสูงสุด

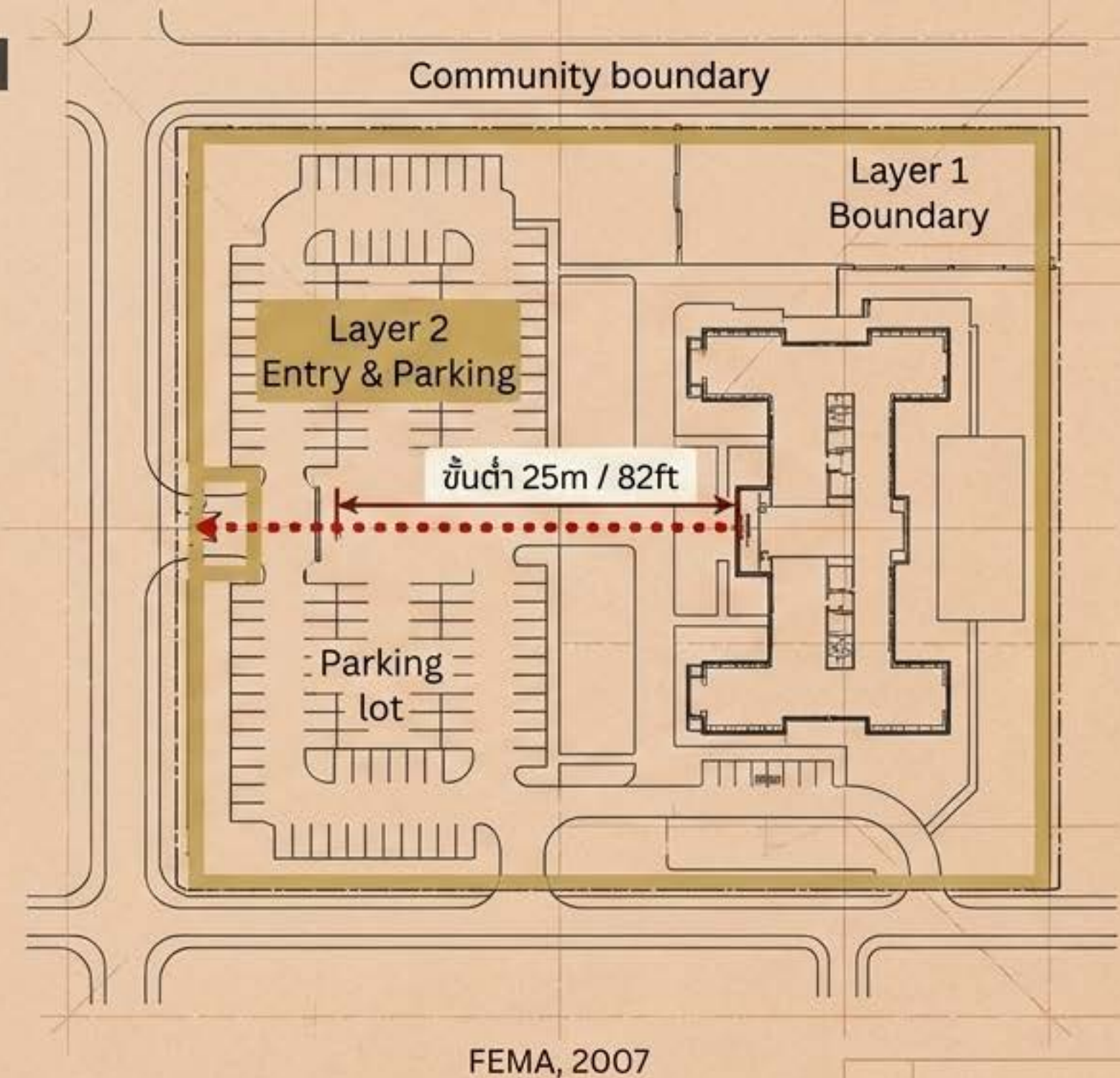


FEMA, 2005

การป้องกันแบบหลายชั้น บังคับให้ผู้บุกรุกต้องฝ่าฟันอุปสรรคที่เพิ่มขึ้นเรื่อยๆ

การป้องกันชั้นที่ 1 และ 2: สภาพแวดล้อมและอาณาบริเวณ

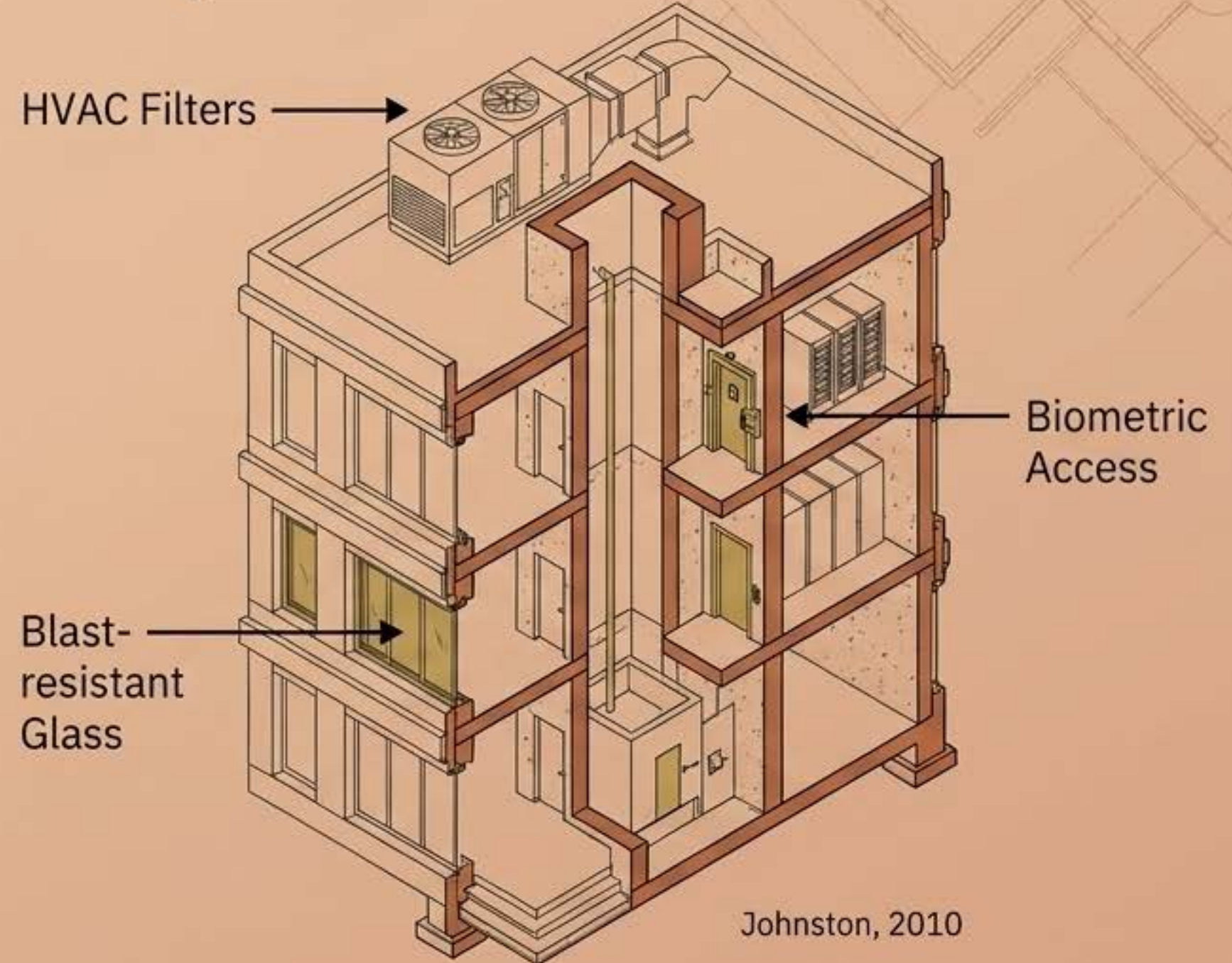
- ชั้นที่ 1: การใช้ GIS ประเมินบริบทชุมชนรอบนอกและสิ่งแวดล้อม
- ชั้นที่ 2: ควบคุมทางเข้า-ออก ที่จอดรถ และแสงสว่าง
- ระยะห่างในการเผชิญหน้า (Stand-off distance): สำคัญต่อการลดแรงระเบิด
- ใช้การออกแบบสภาพแวดล้อม (CPTED) เพื่อป้องกันอาชญากรรม



จัดการความเสี่ยงตั้งแต่ภายนอก และรักษาระยะห่างเพื่อลดความเสียหาย

การป้องกันขั้นที่ 3: ปราการด่านสุดท้าย

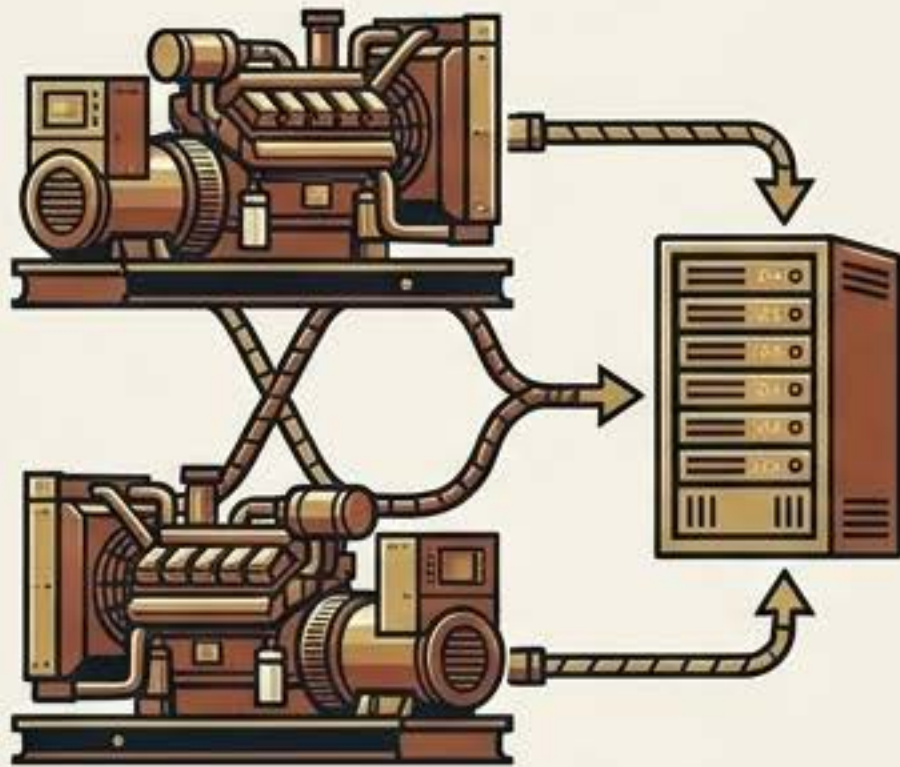
- **เป้าหมายหลัก:** ปกป้องบุคคล อาคาร และทรัพย์สินดิจิทัลที่สำคัญที่สุด
- **การป้องกันกายภาพ:** กระสุนเกราะระเบิด, ล็อคประตูนิรภัย
- **ระบบสนับสนุน:** แผนอพยพฉุกเฉิน, ระบบ HVAC ป้องกันสารพิษ
- **การประสานกลยุทธ์บุคลากรและเทคโนโลยีขั้นสูงสุด**



เมื่อปราการภายนอกถูกเจาะ ชั้นที่ 3 ต้องเป็นเส้นเลือดใหญ่ที่ไม่มีวันพังทลาย

ความซ้ำซ้อน (Redundancy) และตัวคูณกำลัง (Force Multipliers)

ความซ้ำซ้อน: การมีระบบสำรอง (เช่น กล้องคู่, รั้ว 2 ชั้น) เพื่อป้องกันจุดล้มเหลวเดียว



ตัวคูณกำลัง: ใช้เทคโนโลยีขยายขีดความสามารถของบุคลากรที่จำกัด

การสร้างวัฒนธรรมความปลอดภัย: ฝึกอบรมพนักงานให้เป็นหูเป็นตา

ความร่วมมือ: สร้างเครือข่ายกับหน่วยงานรัฐ (ตำรวจ, ดับเพลิง) ล่วงหน้า



ASIS, 2018; Kotwica, 2007; Mallery, 2007

ความซ้ำซ้อนสร้างความยืดหยุ่น ตัวคูณกำลังสร้างประสิทธิภาพสูงสุด

บทสรุปและการประยุกต์ใช้ (Summary & Activity)



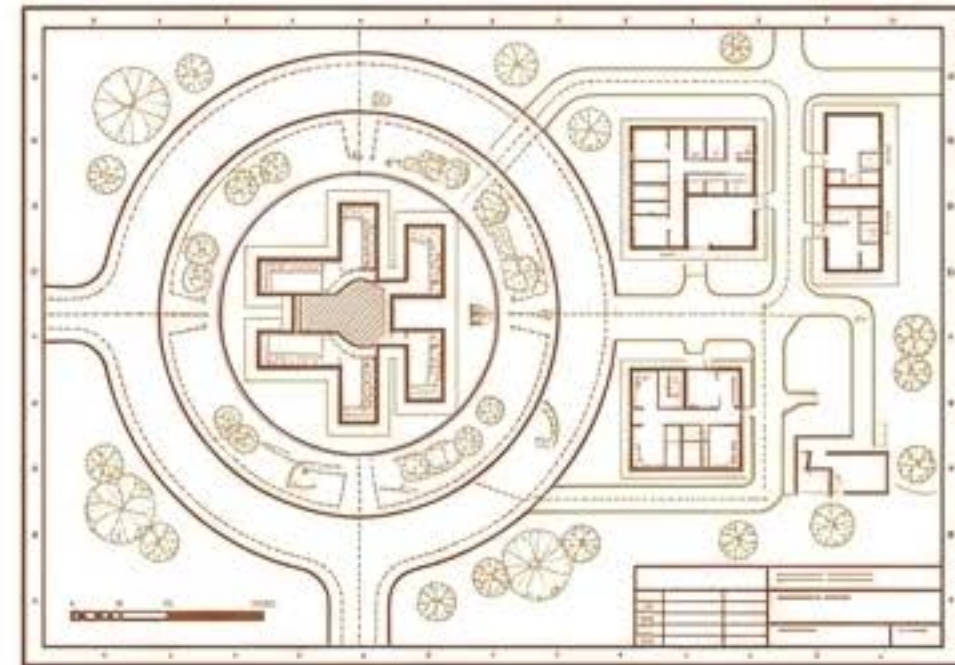
สรุป: ความมั่นคงคือการบูรณาการ 7 กลยุทธ์, การแบ่งระดับชั้น และเทคโนโลยี

Q1: กลยุทธ์ใดสำคัญที่สุดสำหรับองค์กรของคุณ และเพราะเหตุใด?

Q2: ความซ้ำซ้อน (Redundancy) ช่วยลดความเสี่ยงได้อย่างไร?

Q3: การป้องกันความปลอดภัยทั่วไปและเฉพาะเจาะจงต่างกันอย่างไร?

Activity: ให้ออกแบบแผนที่รักษาความปลอดภัยวิทยาเขต 3 ระดับชั้น (Campus-Security Design)



ความปลอดภัยที่ยั่งยืนคือระบบที่มีพลวัต ปรับตัวได้ และผสานคนเข้ากับเทคโนโลยี