



1

การประเมินความเสี่ยงด้านการรักษา ความมั่นคงปลอดภัยทางไซเบอร์ Risk Assessment



กระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO ERM



2

ความสามารถในการเตรียมตัว และตอบสนองต่อภัยคุกคามทางไซเบอร์ Cyber Resilience

หลัก CIA Security Model



3

กรอบมาตรฐานด้านการรักษา ความมั่นคงปลอดภัยทางไซเบอร์ Cybersecurity Framework

NIST Cybersecurity Framework ประกอบด้วย 5 ส่วน



4

การประเมินช่องโหว่ Vulnerability Assessment

ประโยชน์

- 4.1 ช่วยประเมินความเสี่ยงที่เกิดจากช่องโหว่
- 4.2 ช่วยการสร้างรายงานที่รวบรวมข้อมูลเกี่ยวกับช่องโหว่
- 4.3 ช่วยตรวจสอบว่าระบบสอดคล้องกับมาตรฐาน
- 4.4 ช่วยค้นพบและแก้ไขช่องโหว่และปัญหาความปลอดภัย



5

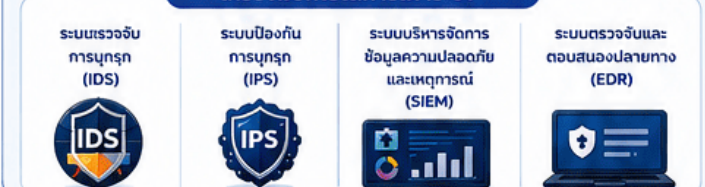
การตรวจสอบและเฝ้าระวัง ภัยคุกคามทางไซเบอร์ Detect

วัตถุประสงค์

- ✓ ลดความเสียหาย
- ✓ ลดโอกาสและระยะเวลาโจมตี
- ✓ สามารถให้ข้อมูลที่เป็นประโยชน์กระบวนการตอบสนองต่อเหตุการณ์



เครื่องมือที่ใช้ในการเฝ้าระวัง



6

การเผชิญเหตุภัยคุกคามทางไซเบอร์ Respond และการฟื้นฟูความเสียหาย จากภัยคุกคามทางไซเบอร์ Recover

ขั้นตอนการรับมือภัยคุกคามทางไซเบอร์

