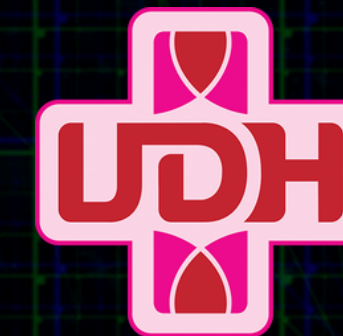




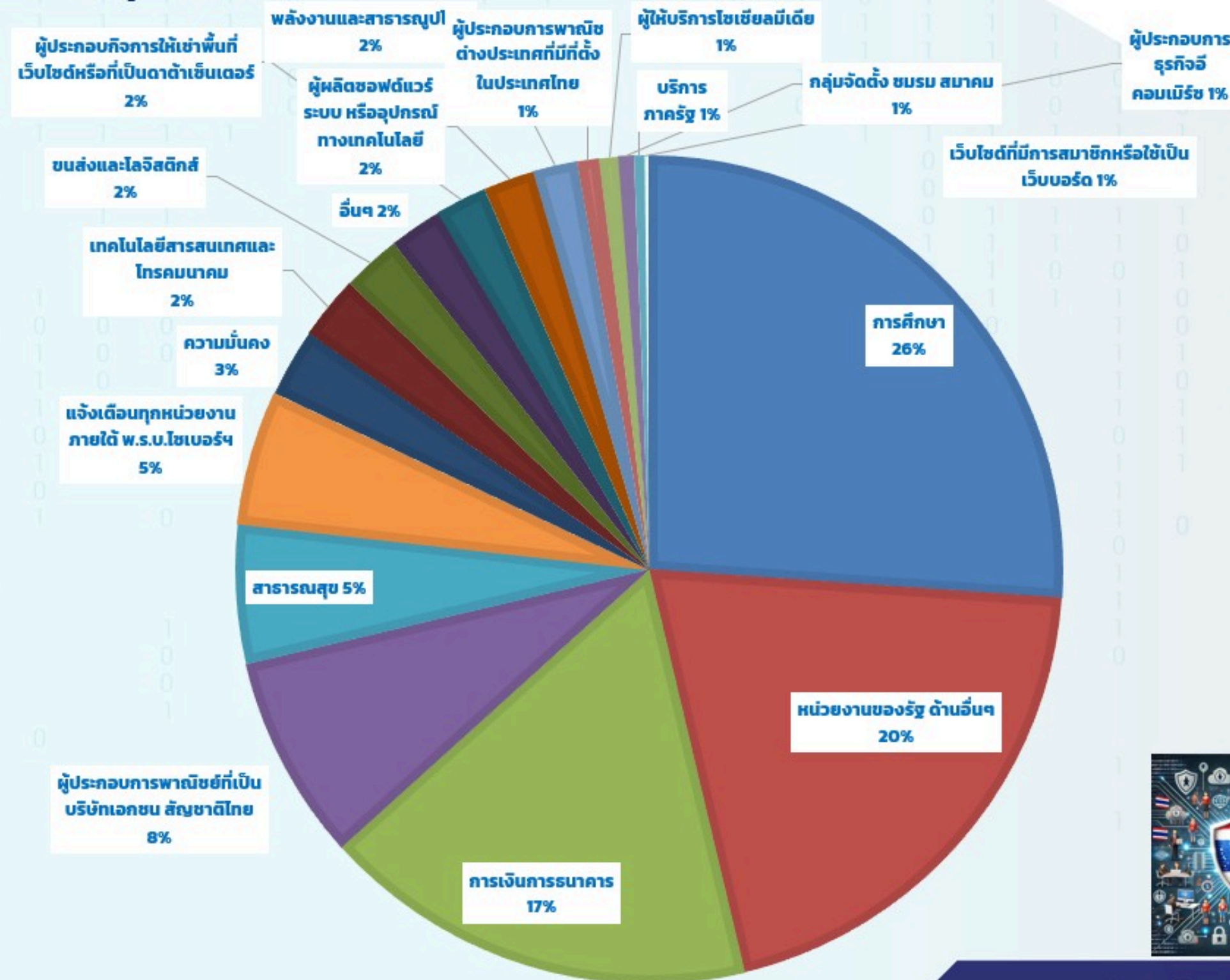
แนวทางดำเนินการ CSOC และ CERT ระดับจังหวัด

โดย นายธนโชติ กมลรัตน
นักวิชาการคอมพิวเตอร์ปฏิบัติการ โรงพยาบาลอุดรธานี
วันที่ 30 กรกฎาคม 2568

มกราคม – มิถุนายน 2568

รวมทั้งสิ้น 1,050 เหตุการณ์

การศึกษา	274
หน่วยงานของรัฐ ด้านอื่นๆ	212
การเงินการธนาคาร	179
ผู้ประกอบการพาณิชย์ที่เป็นบริษัทเอกชน สัญชาติไทย	84
สาธารณสุข	57
แจ้งเตือนทุกหน่วยงานภายใต้ พ.ร.บ.ไซเบอร์ฯ	55
ความมั่นคง	28
เทคโนโลยีสารสนเทศและโทรคมนาคม	26
ขนส่งและโลจิสติกส์	24
อื่นๆ	22
ผู้ประกอบการให้เข้าพื้นที่เว็บไซต์หรือที่เป็นดาต้าเซ็นเตอร์	21
ผู้ผลิตซอฟต์แวร์ ระบบ หรืออุปกรณ์ทางเทคโนโลยี	21
พลังงานและสาธารณูปโภค	18
ผู้ประกอบการพาณิชย์ต่างประเทศที่มีที่ตั้งในประเทศไทย	9
ผู้ให้บริการโฮสติ้ง	8
กลุ่มจัดตั้ง ชมรม สมาคม	6
บริการภาครัฐ	4
ผู้ประกอบการธุรกิจอีคอมเมิร์ซ	1
เว็บไซต์ที่มีการสมาชิกหรือใช้เป็นเว็บบอร์ด	1



เกณฑ์การประเมินการรักษาความมั่นคงปลอดภัยไซเบอร์ และตัวชี้วัด ปี 2568 (Technology Cybersecurity Assessment Matrix : TAM)

เกณฑ์การประเมิน

1. Backup *
2. Antivirus Software *
3. Access Control (Public และ Private) *
4. Privileged Access Management (PAM) *

5. Business Continuity Plan (BCP) และ Disaster Recovery Plan (DRP)
6. OS Patching
7. Multi-Factor Authentication (2FA) *
8. Web Application Firewall (WAF) *
9. Log Management *
10. Security Information & Event Management (SIEM)
11. Vulnerability Assessment (VA Scan)

12. Software Update -> Optional
13. Penetration Testing -> Optional
14. Disaster Recovery site (DR) -> Optional

- CSOC/SOC ?
- ทำเอง หรือ จ้าง ?
- ป้องกันได้ 100% ?

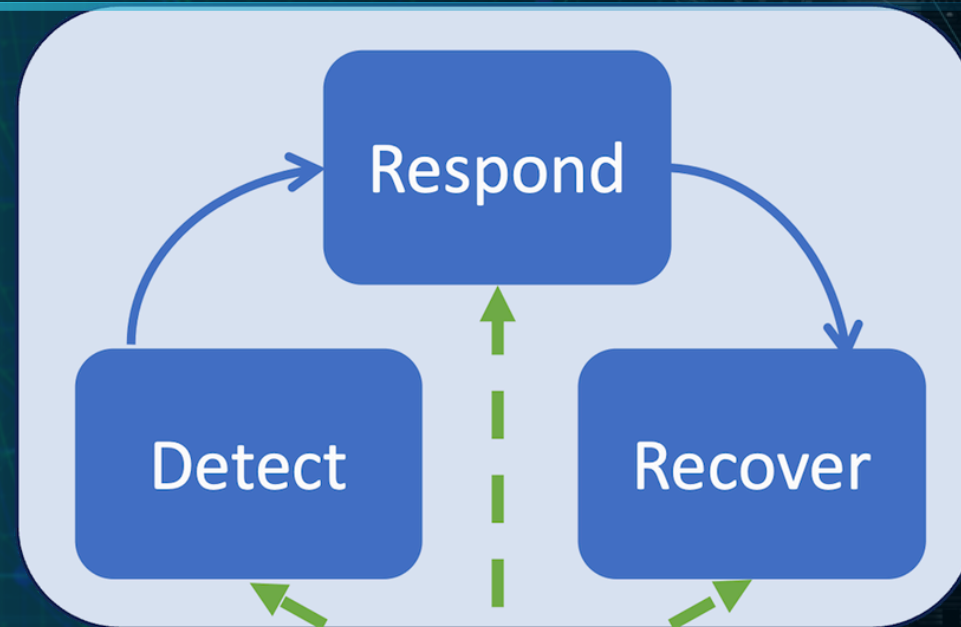
CSOC คืออะไร ?



- Cyber Security Operation Center (CSOC) คือ ศูนย์เฝ้าระวัง วิเคราะห์ และตอบสนองต่อภัยคุกคามไซเบอร์แบบรวมศูนย์
- ทำหน้าที่ตรวจจับ วิเคราะห์ และแจ้งเตือนเมื่อเกิดความผิดปกติหรือการโจมตีระบบสารสนเทศ
- ช่วยให้องค์กรสามารถป้องกันและตอบโต้ภัยคุกคามได้อย่างมีประสิทธิภาพ รวดเร็ว และเป็นระบบ

NIST INCIDENT RESPONSE

Incident Response



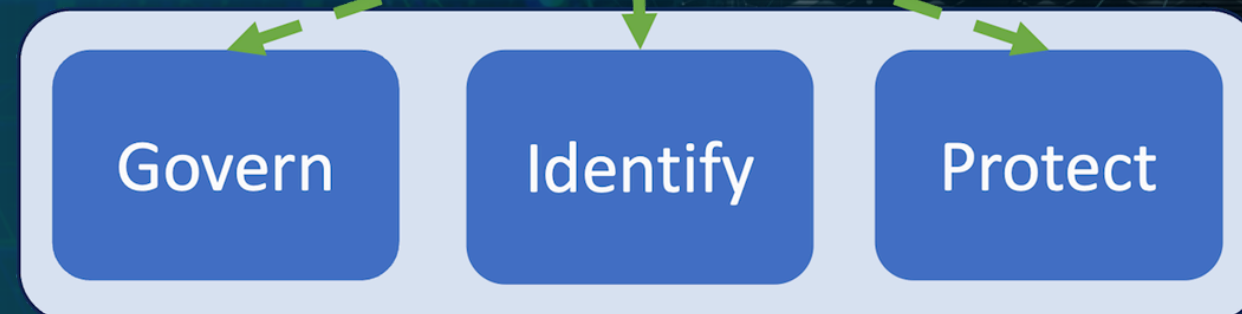
เป้าหมาย: ตรวจสอบ – ตอบสนอง – ฟื้นฟูระบบจากเหตุการณ์ที่เกิดขึ้น

Lessons Learned

(Identify) Improvement

เป้าหมาย: ปรับปรุงกระบวนการให้ดีขึ้นจากประสบการณ์จริง

Preparation



เป้าหมาย: เตรียมองค์กรให้พร้อมรับมือก่อนเกิดเหตุการณ์

CERT คืออะไร ?



- CERT (Computer Emergency Response Team) หรือ CSIRT คือทีมเฉพาะกิจด้านความมั่นคงปลอดภัยไซเบอร์
- มีหน้าที่หลักในการประสานงาน รับแจ้งเหตุ วิเคราะห์ และตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ของระบบคอมพิวเตอร์
- ทำงานหรือระดับองค์กร เพื่อช่วยลดผลกระทบจากภัยคุกคามไซเบอร์

แนวทางดำเนินการติดตั้ง CSOC ระดับจังหวัด

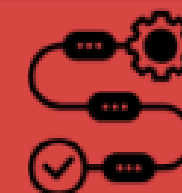
ประกอบด้วย

Cyber Security
Operations Center

People



Process



Technology



แนวทางดำเนินการติดตั้ง CSOC ระดับจังหวัด

PROCESS



แนวทางดำเนินการติดตั้ง CSOC ระดับจังหวัด

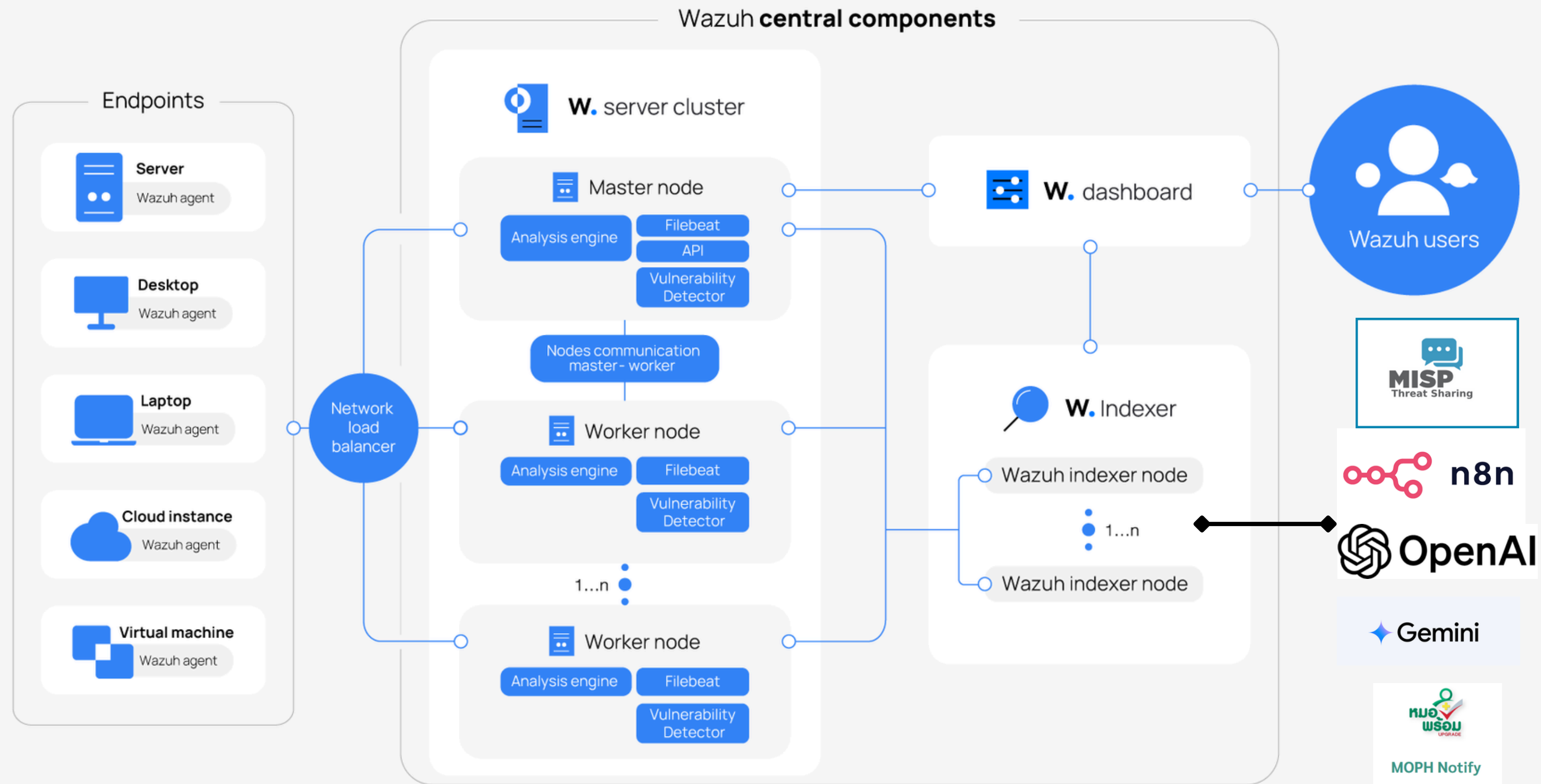
Technology / Tools



- เทคโนโลยีหลักที่ใช้: Wazuh SIEM
- ฟรี / Open Source
- รวมความสามารถ SIEM + Vulnerability Detection + Alerting
- รองรับการจัดกลุ่ม sw. และสามารถแยก dashboard ตามหน่วยงาน

Agents	CPU	RAM	Storage (90 days)
1-25	4 vCPU	8 GiB	50 GB
25-50	8 vCPU	8 GiB	100 GB
50-100	8 vCPU	8 GiB	200 GB

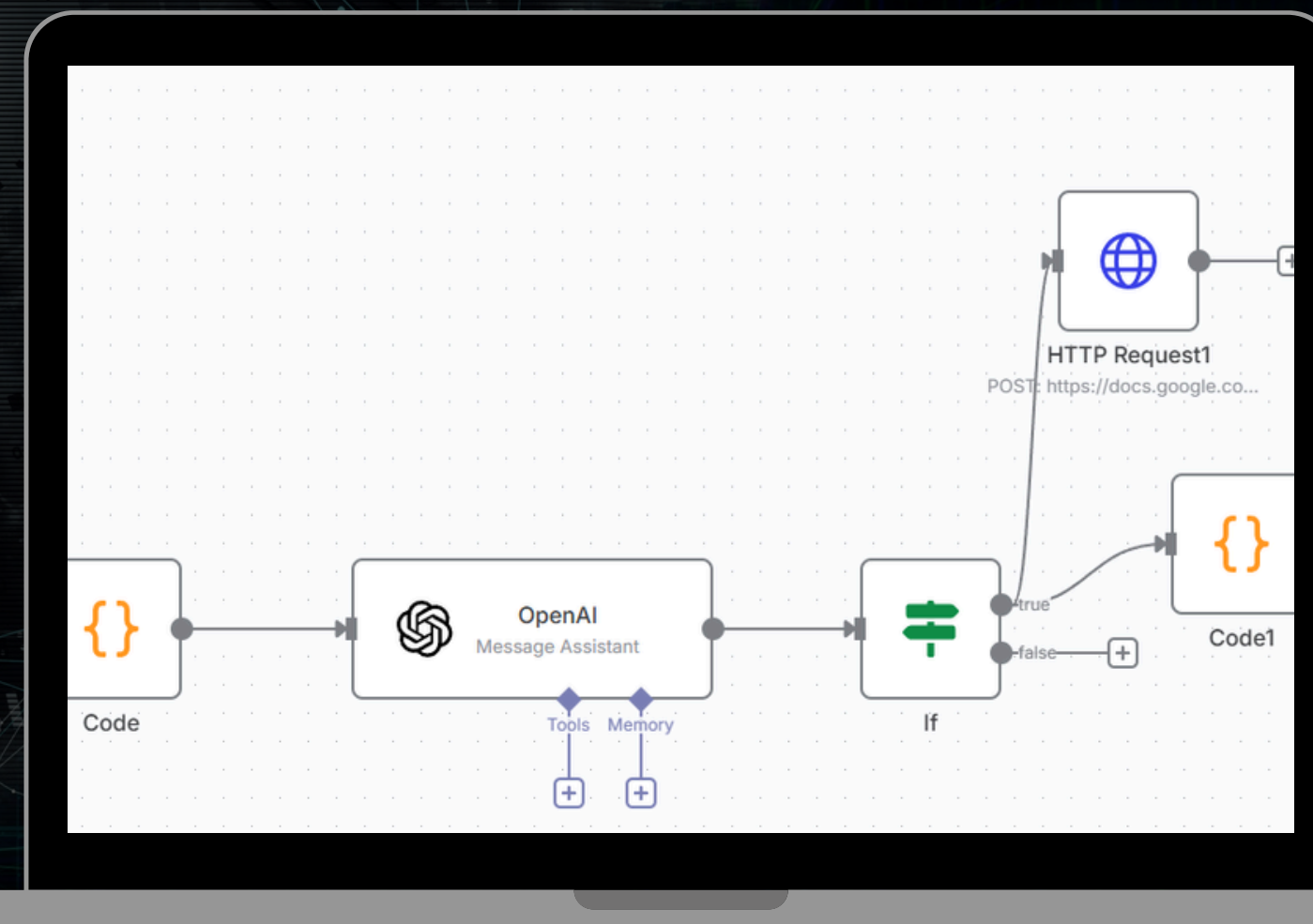
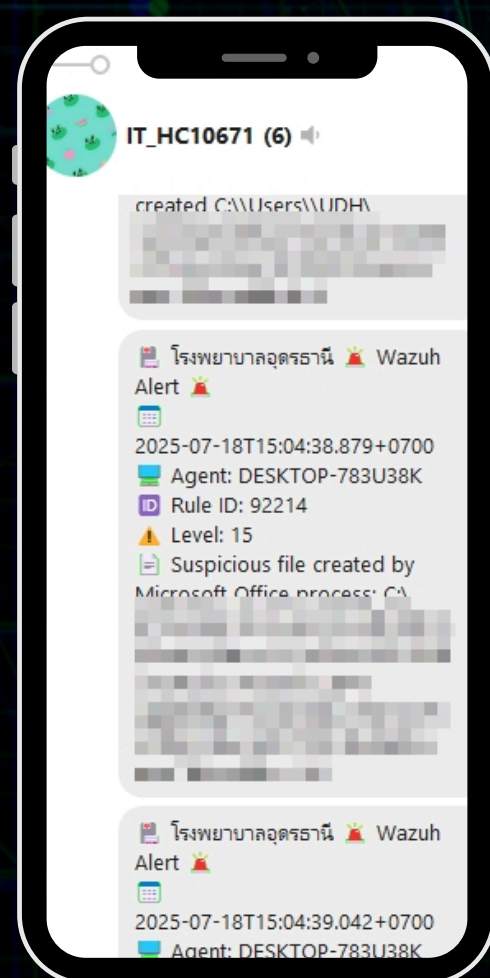
แนวทางดำเนินการติดตั้ง CSOC ระดับจังหวัด

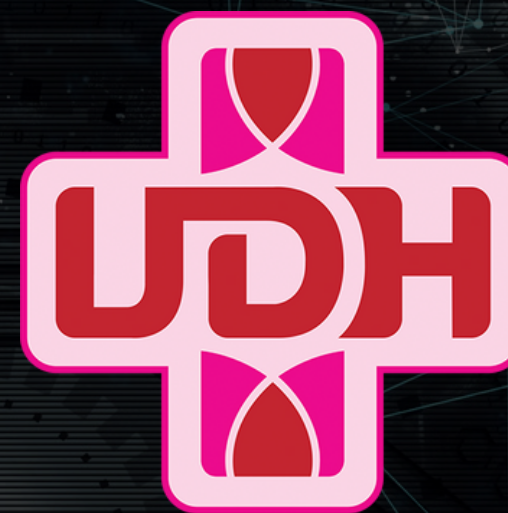


แนวทางดำเนินการติดตั้ง CSOC ระดับจังหวัด

ตัวอย่าง

Wazuh ตรวจพบเหตุการณ์ → เปรียบเทียบกับ IOC จาก MISIP → หากตรงหรือมีความเสี่ยงสูง → ส่ง log ไปให้ GPT-4 วิเคราะห์ → แจ้งเตือนผ่าน LINE OA → ส่งต่อเข้า n8n บล็อก IP API ของ Firewall → แจ้งผลผ่าน LINE OA





THANK YOU