**Cybersecurity SOC ANALYST**

**ทีมงาน**

1. นายนคร ธรรมโท๊ะ , (ยุ้ย), สสจ.เชียงใหม่, เขต 1

2. นายสาโรช กล่องชู , (บอย), โรงพยาบาลพุทธชินราช พิษณุโลก, เขต 2

3. นายอภิวัฒน์ มะโนชัย , (โต้ง), โรงพยาบาลปง, เขต 1

4. นายวัชรพงษ์ วัชรินทร์ , (บอย), สสจ.แพร่, เขต 1

5. นายพิพัฒน์ เลาหลื่อ , (พัฒน์), รพ.แม่สะเรียง, เขต 1

6. นายราเชน กันใจมา , (เชน), รพ.แม่จริน, เขต 1

7. น.ส.นิรัชชา สุขอยู่ , (นุ้ย), โรงพยาบาลพิจิตร, เขต 3

8. นายสิทธิโชค สุภา , (ตู่), โรงพยาบาลน่าน, เขต 1

9. นายพงษ์ศักดิ์ พันธวงค์ , (ศักดิ์), โรงพยาบาลสันติสุข, เขต 1

10. นายอภิวัฒน์ นิพิฐวัธนะผล , (อภิวัฒน์), โรงพยาบาลสันทราย, เขต 1

11. นายทรงวุฒิ กาญจนโกศัย , (อั๋น), โรงพยาบาลแพร่, เขต 1

12. นายณัฐวัฒน์ นันทโกวัฒน์ , (นัท), โรงพยาบาลบ้านนา, เขต 4

**1. บทนำ**

การรักษาความปลอดภัยระบบสารสนเทศในโรงพยาบาลเป็นเรื่องสำคัญอย่างยิ่ง ตาม พรบ.คุ้มครองข้อมูลส่วนบุคคลและพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ต้องปกป้องข้อมูลส่วนตัวของผู้ป่วยซึ่งเป็นข้อมูลอ่อนไหว และรักษาความต่อเนื่องของการให้บริการทางการแพทย์ งานวิจัยนี้มุ่งเน้นการนำเทคโนโลยี Wazuh และ Graylog มาใช้ในการตรวจสอบและรักษาความปลอดภัยระบบเซิร์ฟเวอร์

**2. การวิเคราะห์ปัญหาและความต้องการ**

2.1 ปัญหาที่พบในปัจจุบัน

- ขาดแคลนบุคลากรที่มีความสามารถ และความรับผิดชอบตามภาระงานที่เกินกำลัง

- ขาดระบบการตรวจสอบและแจ้งเตือนการโจมตีทางไซเบอร์แบบเรียลไทม์

- การตรวจจับช่องโหว่และภัยคุกคามล่าช้า

- ไม่มีการรวบรวมและวิเคราะห์ log จากหลายแหล่งอย่างเป็นระบบ ไม่สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

- การบริหารจัดการความปลอดภัยกระจัดกระจาย

2.2 ความต้องการของระบบ

- ระบบตรวจสอบและแจ้งเตือนภัยคุกคามแบบเรียลไทม์

- การรวบรวม log จากทุกระบบอย่างมีประสิทธิภาพ

- ความสามารถในการตรวจหาและตอบสนองต่อเหตุการณ์ด้านความปลอดภัย

- การปกป้องข้อมูลส่วนตัวของผู้ป่วย

- ระบบที่สามารถขยายและปรับขนาดได้

**3. การออกแบบระบบ**

3.1 สถาปัตยกรรมระบบ

System Architecture Diagram

รพ.ศูนย์/รพท.

[External Network] --> [Firewall] --> [Wazuh Manager] <--> [Graylog Server]

^ |

| |

[Servers รพ.ชุมชน] <--- [Wazuh Agents]

**Network Diagram**

- เครือข่ายแบ่งเป็นโซน (Network Segmentation)

- DMZ สำหรับเซิร์ฟเวอร์สาธารณะ

- Internal Network สำหรับระบบภายใน

- Monitoring Network แยกออกมาต่างหาก

**Security Components**

- Wazuh: ระบบตรวจจับและป้องกันการบุกรุก (HIDS/HIPS)

- Graylog: ระบบรวบรวมและวิเคราะห์ log ตามกฎหมาย

- Firewall

- Intrusion Prevention System (IPS)

**3.2 การออกแบบความปลอดภัย**

- การเข้ารหัสการสื่อสารระหว่าง Agent และ Server

- การควบคุมการเข้าถึง (Access Control)

- การเก็บ log แบบปลอดภัยและเข้ารหัส

- การแบ่งแยกสิทธิ์การเข้าถึงข้อมูล

**3.3 แผนการทดสอบ**

Test Cases

1. การตรวจจับการโจมตีแบบต่างๆ

2. ประสิทธิภาพการแจ้งเตือน

3. ความถูกต้องของการเก็บ log

4. ประสิทธิภาพระบบ

ผลการทดสอบ

- รายงานผลการทดสอบแต่ละ Test Case

- การวิเคราะห์ช่องโหว่และข้อเสนอแนะ

**4. การพัฒนาและติดตั้ง**

4.1 เครื่องมือและเทคโนโลยี

Tools & Technologies

- Wazuh

- Graylog

( Ubuntu Server )

**Configurations**

- ค่าคอนฟิกพื้นฐานของ Wazuh

- การตั้งค่า Graylog Input

- Rules และ Dashboards

4.2 ขั้นตอนการติดตั้ง

1. เตรียมเซิร์ฟเวอร์และเครือข่าย (Ubuntu)

2. ติดตั้ง Wazuh Manager

3. ติดตั้ง Graylog

4. ติดตั้ง Wazuh Agent บนเซิร์ฟเวอร์ต่างๆ

5. กำหนดค่าการเชื่อมต่อและการส่ง log

6. ทดสอบและปรับแต่งระบบ

**5. ผลการทดสอบ**

- สามารถตรวจจับภัยคุกคามได้รวดเร็ว

- ลดระยะเวลาในการตอบสนองต่อเหตุการณ์

- เพิ่มประสิทธิภาพการบริหารจัดการความปลอดภัย

**6. แผนการบำรุงรักษา**

- อัพเดตซอฟต์แวร์และ Signature อย่างสม่ำเสมอ

- ตรวจสอบระบบประจำเดือน

- ฝึกอบรมบุคลากร

- ทบทวนและปรับปรุงนโยบายความปลอดภัย

**7. ข้อเสนอแนะและแนวทางพัฒนาต่อ**

- พัฒนาบุคลากรในการปรับจูนกรอง Event ที่จะแจ้งเตือน

- แลกเปลี่ยนข้อมูลรูปแบบการโจมตีทางไซเบอร์ระหว่างหน่วยงาน

- เพิ่มความสามารถบุคลากรในการวิเคราะห์ข้อมูลขั้นสูง

- บูรณาการกับระบบ Machine Learning

- พัฒนาระบบ Threat Intelligence

- ขยายขอบเขตการตรวจสอบไปยังอุปกรณ์เครือข่ายอื่นๆ