**รายงานสรุปผลการพัฒนาระบบความปลอดภัยทางไซเบอร์**

**กลุ่มที่ 4: ระบบ SIEM**

**1.ข้อมูลทีม**

**สมาชิกในทีม**

1.นายธีร์ภัทร ศรีสุวรรณ์ (ภูมิ) จ.เชียงใหม่

2.นายราเชษ สืบสันติกุล (เชษ) จ.นครสวรรค์

3.นายศาสตราวิท พิชัยหนัก (บลู) จ.เชียงใหม่

4.นายสมเกียรติ ชุ่มใจ (แมน) จ.แพร่

5.นายธนพล นางาม (บูม) จ.ขอนแก่น

6.นายธนวัฒน์ รุกขพันธ์ (น๊อต) จ.นราธิวาส

7.นายอิศราพงษ์ สุยะ (ท๊อป) จ.ลำปาง

8.นายสาธิต รินคำ (ธิต) จ.ลำปาง

9.นายวศินภัทร์ ไพศาลยศกุล (ไทด์) จ.เชียงราย

10.นายมานพ บุญจำเนียร (นพ) จ.เชียงใหม่

11.นายอดิเรก จำปาทอง (เอก) จ.ราชบุรี

12.นายสิริวัชร ภวะภูตานนท์ (ล็อตโต้) จ.อุดรธานี

**2.การวิเคราะห์ปัญหาและความต้องการ**

2.1 ปัญหาที่พบในปัจจุบัน

* มีการโจมตีในระบบ Network ของทางโรงพยาบาล ทั้งโดยภายในและภายนอกตลอดเวลา และหลากหลายรูปแบบ
* เจ้าหน้าที่ IT ไม่ทราบถึงการถูกโจมตี ส่งผลให้ไม่สามารถควบคุมหรือยับยั้งปัญหาที่ลุกลามได้ทันเวลา
* ผู้บริหารและผู้ใช้งานไม่ได้รับข้อมูลถึงการถูกโจมตี ทำให้ไม่มีความตระหนักในการป้องกันตนเองเบื้องต้น
* การโจมตีระบบมีการพัฒนาอย่างต่อเนื่อง
* โรงพยาบาลขนาดเล็กขาดงบประมาณ เครื่องมือ และอุปกรณ์ในการตรวจสอบ และป้องกัน การโจมตี

2.2 แนวทางแก้ไขปัญหา

* ระบบ SIEM แบบ Open Source ค้นหาระบบ SIEM ที่เป็น Open source (ฟรี) ที่สามารถมาลงอุปกรณ์เดิมของโรงพยาบาลได้
* เพิ่มความสามารถให้เจ้าหน้าที่ IT ส่งเจ้าหน้าที่ IT อบรมในหลักสูตร Cyber ต่างๆ เพื่อเพิ่มความสามารถ และทันสมัย
* เครื่องมือ และอุปกรณ์ ผู้บริหารเข้าใจในความสำคัญของการป้องกันระบบ มีการจัดซื้อเครื่องมือ อุปกรณ์ให้เหมาะสมในการป้องกันระบบ
* ตรวจสอบการถูกโจมตีได้ สามารถแจ้งข้อมูลและผู้บริหารและผู้ใช้งาน จัดอบรมให้ผู้ใช้งานตระหนักถึงความสำคัญของการป้องกันระบบ

2.3 ความต้องการของระบบ

**OS**

Ubuntu 22.0.4

**System Requirements**

**CPU:** Dual-core หรือมากกว่า

**RAM:** อย่างน้อย 4GB

**Storage:** ขึ้นอยู่กับปริมาณข้อมูล (ขั้นต่ำ 20GB)

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, จำนวน, ตัวอักษร

คำอธิบายที่สร้างโดยอัตโนมัติ

**3.การออกแบบระบบ**

3.1 สถาปัตยกรรมระบบ เช่น

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ตัวอักษร, จำนวน

คำอธิบายที่สร้างโดยอัตโนมัติ

3.2 การออกแบบความปลอดภัย

* วิเคราะห์ภัยคุกคามทางไซเบอร์
* ครอบคลุมการตรวจจับพื้นฐาน
* ตรวจจับและแจ้งเตือนการบุกรุกที่เข้าถึงระบบเครือข่าย การพยายาม Brute force Login เข้าระบบ / การ Scan port
* Malware-Virus Detection ตรวจจับและแจ้งเตือน Malware หรือ Virus จากพฤติกรรมต่างที่เกิดขี้น หรือจาก signature
* Blacklist IP การตรวจจับและแจ้งเตือนการเข้าถึง IP Address ที่เป็น Blacklist และระบุการเปิด connection ได้
* Unauthorized Access การตรวจจับการเข้าถึงข้อมูลหรือระบบที่ไม่ได้รับอนุญาต หรือไม่มีสิทธิ์เข้าถึงระบบ
* DDoS Attack การตรวจจับพฤติกรรมการโจมตีในรูปแบบของ DDosS ได้ ทั้งภายในและภายนอก
* Data Breaches การตรวจจับและแจ้งเตือนการละเมิดการเข้าถึงข้อมูลที่สำคัญของระบบ ที่ไม่อนุญาตให้เข้าถึง
* การแจ้งเตือนทาง E-mail
* Dashboard ดูระบบการทำงานทั้งหมดของ SIEM

3.3 แผนการทดสอบ

• Test Cases

รูปภาพประกอบด้วย คน, ในร่ม, เสื้อผ้า, ข้อความ

คำอธิบายที่สร้างโดยอัตโนมัติ

• Results

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, จำนวน, แผนภาพ

คำอธิบายที่สร้างโดยอัตโนมัติ

4. การพัฒนาและติดตั้ง

4.1 เครื่องมือและเทคโนโลยี

* Wazuh: Open-source Security Information and Event Management

(SIEM) platform.

4.2 ขั้นตอนการติดตั้ง

เตรียมระบบ Ubuntu 22.04

1.ติดตั้ง Ubuntu 22.0.4

2.#sudo apt update && sudo apt upgrade -y

3.ติดตั้ง Wazuh

#sudo curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh && sudo bash ./wazuh-install.sh -a

รอจนกว่า จะติดตั้งเสร็จ

07/12/2024 04:08:33 INFO: --- Summary ---

07/12/2024 04:08:33 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443

User: admin

Password: fYdhJ2ngVKD0g4a.W9+Jel3mbBxxxxxx

จากนั้นให้ Copy User / Password ไว้

4.Login เข้าเว็บ https://192.168.30.128/app/login?

5.Server Magement -> endpoints-summary->agents-preview ->Deploy new agent

6.Assign a server address ใส่ IP Server

7..Assign an agent name ระบุ ชื่อ Agent

8. คัดลอก Run the following commands to download and install the agent:

มาวางใน Powershell ของเครื่อง Serevr ที่ต้องการ โดย Run As Administrator

9. 9. Start the agent: ใน Powershell

NET START WazuhSvc

ก็จะได้ Dashboard ตามต้องการ

5. ผลการทดสอบ

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, จำนวน, แผนภาพ

คำอธิบายที่สร้างโดยอัตโนมัติ

6. แผนการบำรุงรักษา

* อัพเดท Wazuh
  + sudo apt update
  + sudo apt upgrade wazuh-manager
  + sudo systemctl restart wazuh-manager
* อัพเดท Ubantu
  + sudo apt update
* เช็ค Hardware
* สรุปผล แจ้งผู้บริหาร
* ทำแผนจัดซื้ออุปกรณ์ เครื่องมือ

7. ข้อเสนอแนะและแนวทางพัฒนาต่อ

* MISP เชื่อมต่อกับ Wazuh กับทาง สกมช. (IOC Sharing)ทำให้ได้รับการอัพเดทภัยคุกคามจากทาง สกมช ที่ได้รับการอัพเดทภัยคุกคามจากในประเทศและต่างประเทศ

รูปภาพประกอบด้วย ข้อความ, ซอฟต์แวร์, จำนวน, ไอคอนคอมพิวเตอร์

คำอธิบายที่สร้างโดยอัตโนมัติ

* Cross-Cluster Search (CCS)

การเชื่อมต่อ Wazuh ระหว่างองค์กร

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, แผนภาพ, ไลน์

คำอธิบายที่สร้างโดยอัตโนมัติ

* Leveraging LLMs for alert enrichment

Detects Malware

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, แผนภาพ, ตัวอักษร

คำอธิบายที่สร้างโดยอัตโนมัติ

**คู่มือ**

**การติดตั้ง Wazuh**

**ติดตั้ง Ubantu**

(ตัวอย่างติดตั้งบน VMware Workstation)

1. ติดตั้ง VMware Workstation

2.ติดตั้ง Ubantu > เลือก “New Virtual Machine”

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ซอฟต์แวร์, ซอฟต์แวร์มัลติมีเดีย

คำอธิบายที่สร้างโดยอัตโนมัติ

เลือก “Typical (recommended)”



เลือก “Browse…” เพื่อเลือก .iso ของ Ubantu

รูปภาพประกอบด้วย ข้อความ, อิเล็กทรอนิกส์, ภาพหน้าจอ, แสดง

คำอธิบายที่สร้างโดยอัตโนมัติ

รูปภาพประกอบด้วย ข้อความ, ซอฟต์แวร์, ไอคอนคอมพิวเตอร์, แสดง

คำอธิบายที่สร้างโดยอัตโนมัติ

เลือก “NEXT”

รูปภาพประกอบด้วย ข้อความ, อิเล็กทรอนิกส์, ภาพหน้าจอ, ซอฟต์แวร์

คำอธิบายที่สร้างโดยอัตโนมัติ

ตั้งชื่อ VM ที่ “Virtual machine name:”

เลือกที่อยู่การติดตั้งที่ “Browse” > เลือก “OK” > เลือก “Next>”

รูปภาพประกอบด้วย ข้อความ, ซอฟต์แวร์, ไอคอนคอมพิวเตอร์, หน้าเว็บ

คำอธิบายที่สร้างโดยอัตโนมัติ

เลือกขนาดพื้นที่ที่ต้องการที่ “Maximum disk size (GB)”

รูปภาพประกอบด้วย ข้อความ, อิเล็กทรอนิกส์, ภาพหน้าจอ, แสดง

คำอธิบายที่สร้างโดยอัตโนมัติ

เลือก “Finish”

รูปภาพประกอบด้วย ข้อความ, อิเล็กทรอนิกส์, ภาพหน้าจอ, แสดง

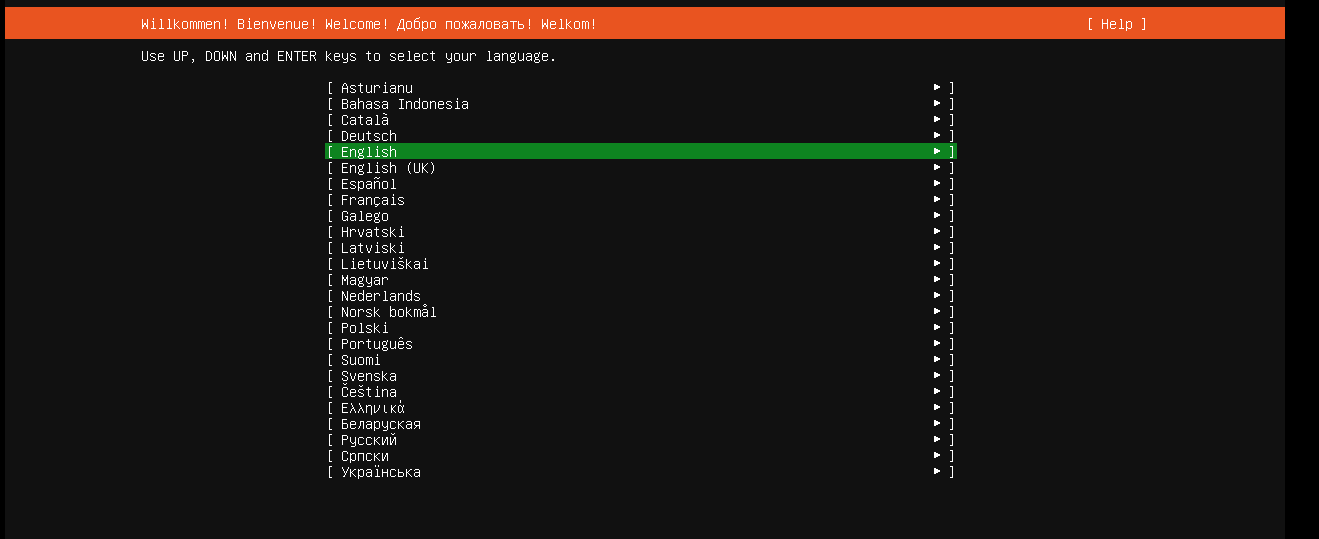
คำอธิบายที่สร้างโดยอัตโนมัติ

กด เลือก “Try or Install Ubuntu Server” > กด “Enter”

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ตัวอักษร, ออกแบบ

คำอธิบายที่สร้างโดยอัตโนมัติ

เลือก “English” > กด “Enter”



เลือก “Continue without updating” > กด “Enter”

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ซอฟต์แวร์, ซอฟต์แวร์มัลติมีเดีย

คำอธิบายที่สร้างโดยอัตโนมัติ

เลือก “Done” > “กด Enter”

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ซอฟต์แวร์, ซอฟต์แวร์มัลติมีเดีย

คำอธิบายที่สร้างโดยอัตโนมัติ

เลือก “Done” > “กด Enter”

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ซอฟต์แวร์, ซอฟต์แวร์มัลติมีเดีย

คำอธิบายที่สร้างโดยอัตโนมัติ

เลือก “Done” > “กด Enter”

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ซอฟต์แวร์, ซอฟต์แวร์มัลติมีเดีย

คำอธิบายที่สร้างโดยอัตโนมัติ

เลือก “Done” > “กด Enter”

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ซอฟต์แวร์, ซอฟต์แวร์มัลติมีเดีย

คำอธิบายที่สร้างโดยอัตโนมัติ

เลือก “Done” > “กด Enter”

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ซอฟต์แวร์, ซอฟต์แวร์มัลติมีเดีย

คำอธิบายที่สร้างโดยอัตโนมัติ

กด “Tabs” > เลือก “Done” > “กด Enter”

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ซอฟต์แวร์

คำอธิบายที่สร้างโดยอัตโนมัติ

เลือก “ubantu-lv…” > “กด Enter” > เลือก “Edit” > “กด Enter”

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ซอฟต์แวร์, แสดง

คำอธิบายที่สร้างโดยอัตโนมัติ

กด “Tab” มาที่ “Size (max ….)” เลือก พื้นที่เต็มพื้นที่ > กด “Tab” มาที่ “Save” > กด “Enter”

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, แสดง, ซอฟต์แวร์

คำอธิบายที่สร้างโดยอัตโนมัติ

กด “Tab” มาที่ “Done” > กด “Enter”

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ซอฟต์แวร์, ซอฟต์แวร์มัลติมีเดีย

คำอธิบายที่สร้างโดยอัตโนมัติ

เลือก “Continue” > กด “Enter”

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ตัวอักษร, จำนวน

คำอธิบายที่สร้างโดยอัตโนมัติ

กรอกข้อมูลให้ครบถ้วน

Yure name : ชื่อเครื่อง

Your server’s name : ชื่อเครื่อง(ตั้งเหมือนกับบรรทัดก่อนหน้า)

Pick a username : ชื่อเข้าระบบ ubantu

Choose a password : รหัสผ่าน เข้า ubantu

Confirm Your password : รหัสผ่าน เข้า ubantu

> เลือก “Done” > กด “Enter”

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ซอฟต์แวร์, ซอฟต์แวร์มัลติมีเดีย

คำอธิบายที่สร้างโดยอัตโนมัติ

เลือก “Install OpenSSH server” โดยการกด Spacbar > กด “Tab” เลือก “Done” > กด “Enter”

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ซอฟต์แวร์, ซอฟต์แวร์มัลติมีเดีย

คำอธิบายที่สร้างโดยอัตโนมัติ

กด “Tab” มาที่ “Done” > กด “Enter”

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, แสดง, ซอฟต์แวร์

คำอธิบายที่สร้างโดยอัตโนมัติ

รอการติดตั้ง Ubantu จนกว่าจะเสร็จ

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ออกแบบ

คำอธิบายที่สร้างโดยอัตโนมัติ

**การติดตั้ง Wazuh**

1.ติดตั้งโปรแกรม SSH ที่เครื่องคอมพิวเตอร์ เช่น Putty

ดาวโหลด Putty จาก google.co.th > กด “Enter”

รูปภาพประกอบด้วย ภาพหน้าจอ, ข้อความ, ตัวอักษร, ไลน์

คำอธิบายที่สร้างโดยอัตโนมัติ

เลือก “https://www.putty.org”

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, คอมพิวเตอร์, เว็บไซต์

คำอธิบายที่สร้างโดยอัตโนมัติ

เลือก “Download PuTTY”

รูปภาพประกอบด้วย ข้อความ, ซอฟต์แวร์, ตัวอักษร, ซอฟต์แวร์มัลติมีเดีย

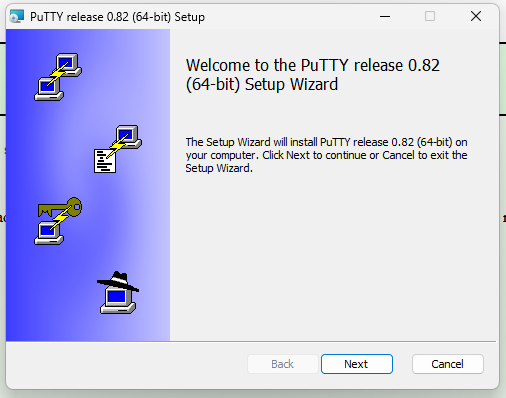
คำอธิบายที่สร้างโดยอัตโนมัติ

เลือกติดตั้งตามรุ่นระบบปฏิบัติการตนเอง

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, ตัวอักษร, จำนวน

คำอธิบายที่สร้างโดยอัตโนมัติ

ติดตั้ง PuTTY > “Next”



เลือก “Next”

รูปภาพประกอบด้วย ข้อความ, อิเล็กทรอนิกส์, ภาพหน้าจอ, แสดง

คำอธิบายที่สร้างโดยอัตโนมัติ

เลือก “Install”

รูปภาพประกอบด้วย ข้อความ, อิเล็กทรอนิกส์, ภาพหน้าจอ, แสดง

คำอธิบายที่สร้างโดยอัตโนมัติ

เลือก “Finish”

รูปภาพประกอบด้วย ข้อความ, อิเล็กทรอนิกส์, ภาพหน้าจอ, แสดง

คำอธิบายที่สร้างโดยอัตโนมัติ

2. การติดตั้ง Wazuh

- เปิดการใช้งาน PuTTY

รูปภาพประกอบด้วย ข้อความ, ซอฟต์แวร์, ไอคอนคอมพิวเตอร์, ระบบปฏิบัติการ

คำอธิบายที่สร้างโดยอัตโนมัติ

- กรอกไอพีของ Ubantu > เลือก “Open” > กรอก User และ Password > กด “Enter”

รูปภาพประกอบด้วย ข้อความ, ภาพหน้าจอ, แสดง, ซอฟต์แวร์

คำอธิบายที่สร้างโดยอัตโนมัติ

- กรอกโค้ด ติดตั้ง Wazuh

#sudo curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh && sudo bash ./wazuh-install.sh -a

รอจนกว่า จะติดตั้งเสร็จ

07/12/2024 04:08:33 INFO: --- Summary ---

07/12/2024 04:08:33 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443

User: admin

Password: fYdhJ2ngVKD0g4a.W9+Jel3mbBxxxxxx

- จากนั้นให้ Copy User / Password ไว้

- Login เข้าเว็บ https://(ไอพี)/app/login?

- Server Magement -> endpoints-summary->agents-preview ->Deploy new agent

- Assign a server address ใส่ IP Server

- Assign an agent name ระบุ ชื่อ Agent

- คัดลอก Run the following commands to download and install the agent:

มาวางใน Powershell โดย Run As Administrator

- Start the agent: ใน Powershell

NET START WazuhSvc ก็จะได้ Dashboard ตามต้องการ

รูปภาพประกอบด้วย ข้อความ, ตัวอักษร, จำนวน, ซอฟต์แวร์

คำอธิบายที่สร้างโดยอัตโนมัติ