ENDPOINT RISK ANALYSIS AI-POWERED SYSTEM

ระบบตรวจสอบความเสี่ยงเครื่องปลายทางด้วย *AI* — *CP422031: INTRODUCTION TO CYBERSECURITY*

เสนอ อาจารย์ประจำวิชา ศ.ดร.จักรชัย โสอินทร์, ผศ.ดร.สาธิต กระเวนกิจ และ อ. ดร.ชาติชาย ปุณริบูรณ์

งานของเราคืออะไร?

โครงงานนี้คือการพัฒนาระบบรักษาความปลอดภัยและการจัดการเครื่องปลายทาง (Endpoint Detection and Response - EDR) แบบรวมศูนย์ โดยทำงานในรูปแบบ Client-Server ระบบประกอบด้วย "Agent" ที่ติดตั้งในเครื่องของผู้ใช้งานเพื่อคอยเฝ้าระวังพฤติกรรมต่างๆ และ "Server" ที่ทำหน้าที่แสดงผลผ่าน Dashboard แบบ Real-time จุดเด่นของระบบคือการนำปัญญาประดิษฐ์ (Artificial Intelligence/Machine Learning) มาใช้วิเคราะห์โครงสร้างไฟล์ปฏิบัติการ (PE Header) เพื่อตรวจจับมัลแวร์โดยอัตโนมัติ

หลักการและเหตุผล

ในปัจจุบัน ภัยคุกคามทางไซเบอร์มีความซับซ้อนมากขึ้น โดยเฉพาะการโจมตีผ่านเครื่องปลายทาง (Endpoint) ของพนักงานในองค์กร ไม่ว่าจะเป็นการนำอุปกรณ์ USB ที่ไม่ได้อนุญาตมาเชื่อมต่อ การลักลอบใช้งานโปรแกรมควบคุมระยะไกล (Remote Desktop) หรือการดาวน์โหลดไฟล์มัลแวร์ที่โปรแกรม Antivirus แบบดั้งเดิม (Signature-based) อาจตรวจไม่พบ

ในฐานะผู้ดูแลระบบ (System Engineer) การตรวจสอบความผิดปกติเหล่านี้ทีละเครื่องเป็นเรื่องที่ทำได้ยากและใช้เวลานาน ดังนั้นจึงมีความจำเป็นต้องพัฒนาระบบมอนิเตอร์แบบ Real-time ที่สามารถรวบรวมข้อมูลสถานะของเครื่อง (CPU, Port, Application, USB) และนำเทคโนโลยี Machine Learning มาช่วยวิเคราะห์ความเสี่ยงของไฟล์ที่ถูกดาวน์โหลด เพื่อให้ผู้ดูแลระบบสามารถรับมือกับภัยคุกคามได้อย่างทันท่วงที (AIOps)

วัตถุประสงค์

1. เพื่อพัฒนาระบบตรวจสอบทรัพยากรและพฤติกรรมเสี่ยงของเครื่องปลายทาง (Endpoint Monitoring) แบบ Real-time
2. เพื่อประยุกต์ใช้เทคโนโลยี Machine Learning (AI) ในการวิเคราะห์และจำแนกไฟล์ปฏิบัติการ (.exe) ว่าเป็นมัลแวร์หรือไม่จากโครงสร้างของไฟล์ (PE Features)
3. เพื่อสร้างหน้ากระดานแสดงผล (Dashboard) แบบรวมศูนย์ที่ช่วยให้ผู้ดูแลระบบประเมินความเสี่ยงและสถานะความปลอดภัยของระบบเครือข่ายได้อย่างรวดเร็ว

เครื่องมือที่ใช้

Flask (web development, one drop at a time) · scikit learn · pandas · Joblib · Python

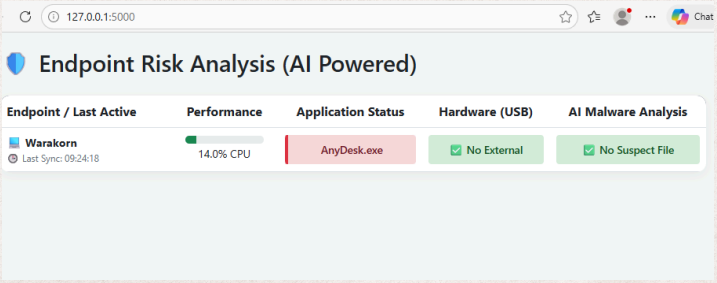
ขอบเขตของระบบ

สิ่งที่ระบบทำได้

1. Performance Monitoring: ตรวจสอบและแจ้งเตือนการใช้งาน CPU ของเครื่องปลายทาง
2. Network & Port Detection: ตรวจจับการเปิดพอร์ตเครือข่ายที่มีความเสี่ยง (เช่น พอร์ตที่มักใช้โดย Hacker หรือ Ransomware)
3. Application Control: ตรวจสอบและแจ้งเตือนเมื่อมีการเรียกใช้งานโปรแกรมที่อยู่ใน Blacklist (เช่น AnyDesk, โปรแกรม Remote อื่นๆ)
4. Hardware Device Detection: ตรวจจับการเชื่อมต่ออุปกรณ์จัดเก็บข้อมูลภายนอก (USB Drive / Removable Media)
5. AI Malware Analysis: สแกนไฟล์นามสกุล .exe ที่เข้ามาใหม่ในโฟลเดอร์ Downloads โดยใช้ AI วิเคราะห์ PE Header เพื่อทำนายว่าเป็นมัลแวร์ (Malware) หรือไฟล์ปกติ (Legitimate)
6. Centralized Dashboard: แสดงผลข้อมูลความเสี่ยงทั้งหมดของทุกเครื่องในเครือข่ายผ่าน Web Application

สิ่งที่ระบบทำไม่ได้

1. ระบบไม่สามารถ "ลบ" หรือ "กักกัน" (Quarantine) ไฟล์มัลแวร์ได้โดยอัตโนมัติ ทำได้เพียง "แจ้งเตือน" ให้ผู้ดูแลระบบทราบเท่านั้น
2. ระบบ AI ไม่สามารถวิเคราะห์ไฟล์ประเภทอื่นได้ (เช่น .pdf, .docx, .xlsx) รองรับเฉพาะไฟล์ปฏิบัติการ (.exe) ที่มีโครงสร้างแบบ PE (Portable Executable) เท่านั้น
3. ระบบไม่สามารถบล็อกการเชื่อมต่อ USB หรือสั่งปิดโปรแกรมข้ามเครื่องได้โดยตรง (ทำงานในโหมด Monitoring & Alerting)



สมาชิก เซค 1 กลุ่ม 11

673380004-6 กฤษฎิพัชญ์ แก้วสง่า
673380179-1 ภานุกร แก้วการ
673380185-6 วรากร แก้วมาคูณ
673380189-8 ศุภวงศ์ สายประเสริฐ
673380494-3 เบนจามิน เคิก