AetherFlow

CP42203 Introduction to Cybersecurity

อาจารย์ที่ปรึกษา ศ.ดร.จักรชัย โสอินทร์ อ.ดร.ชาติชาย ปุณริบูรณ์ และ ผศ.ดร.สาธิต กระเวนกิจ

หลักการและเหตุผล

ในปัจจุบันภัยคุกคามทางไซเบอร์ เช่น APTs และ Ransomware มักฝังตัวในระบบปฏิบัติการเพื่อควบคุมเครื่องในระยะยาว อีกทั้งผู้ใช้งานในองค์กรอาจดาวน์โหลดไฟล์หรือเข้าถึงเว็บไซต์ที่มีความเสี่ยง โครงการ AetherFlow จึงถูกพัฒนาขึ้นโดยใช้แนวคิด Moving Target Defense และ Zero Trust เพื่อสร้างสภาพแวดล้อมการทำงานแบบ Ephemeral ที่แยกการทำงานออกจากเครื่องหลัก หากเกิดการติดมัลแวร์ ระบบจะถูกทำลายและสร้างใหม่หลังใช้งาน ช่วยลดความเสี่ยงการแพร่กระจายของภัยคุกคามในเครือข่ายองค์กร

วัตถุประสงค์

- เพื่อสร้างพื้นที่ทำงานปลอดภัยด้วย Self-Destruct Container
- เพื่อพัฒนาระบบต่อเนื่องของงานด้วย Task-Based Snapshot
- เพื่อออกแบบการตรวจสอบข้อมูลด้วยตราประทับดิจิทัล
- เพื่อพัฒนาระบบเฝ้าระวังภัยคุกคามอัตโนมัติร่วมกับ Antivirus Engine

ขอบเขตการศึกษา

- สภาพแวดล้อมจำลอง พัฒนาบนระบบปฏิบัติการ Ubuntu Server ผ่านการจำลองด้วย VMware Workstation
- การจัดการ Container ใช้ Docker และ Kasm Workspaces ในการสร้างพื้นที่ทำงานเสมือน (Virtual Workspace)
- ระบบความปลอดภัย ครอบคลุมการสแกนไวรัสด้วย ClamAV, การตรวจสอบ Hash (SHA-256) และการแจ้งเตือนผ่าน Line Notify / Webhook
- การเข้าถึง รองรับการใช้งานผ่าน Web Browser ด้วยโปรโตคอล HTTPS ผ่าน Nginx Reverse Proxy
- การทดสอบ ทดลองใช้ไฟล์จำลองมาตรฐาน (EICAR Test File) เพื่อทดสอบประสิทธิภาพในการตรวจจับและกักกันไฟล์อันตราย

เครื่องมือและซอฟต์แวร์ที่ใช้

- Nginx / Kasm Web หน้าด่านการเชื่อมต่อ
- Docker, Python, ClamAV ประมวลผลและเฝ้าจับไวรัส
- PostgreSQL, Linux File System เก็บข้อมูลสำคัญและลายนิ้วมือ

ฟังก์ชันของระบบ

1.Ephemeral Workspace
สร้างพื้นที่ทำงานใหม่ที่สะอาด 100% จาก Image ต้นฉบับทุกครั้งที่เริ่มงาน และสั่งลบทิ้ง (Auto-Purge) ทันที

2.Task-Based Snapshot
ระบบ "จุดเซฟ" ตามภารกิจ ช่วยให้พนักงานสลับโหมดงาน (เช่น บัญชี, พัฒนาซอฟต์แวร์) ได้ทันที โดยไม่ต้องเปิดโปรแกรมใหม่

3.Snapshot Integrity Signing
ตรวจสอบ "ลายนิ้วมือดิจิทัล" ของจุดเซฟ ก่อนโหลดใช้งาน หากพบว่าไฟล์ถูกดัดแปลงแม้แต่ 1 บิต ระบบจะทำการกักกัน (Quarantine) ทันที

4.Python Sentinel (The Brain)
สมองกลที่คอยดักจับ Event การปิด Workspace เพื่อสั่งให้ ClamAV เข้าไปสแกนไฟล์ใน Persistent Volume โดยอัตโนมัติ

5.Automated Incident Response
เมื่อพบไฟล์อันตราย ระบบจะย้ายไฟล์ไปที่ "Isolated Vault" และแจ้งเตือนแอดมินผ่าน Line/Telegram ทันที

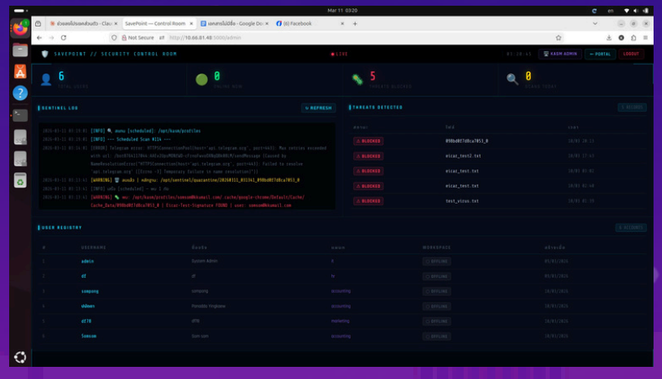
6.Dashboard Real-time log
แอดมินสามารถดูพฤติกรรมของผู้ใช้ได้ และระบบแสดงผลการทำงานแบบ
เรียลทามว่าตรวจพบไวรัสไหม และหากพบจะลบให้ทันที

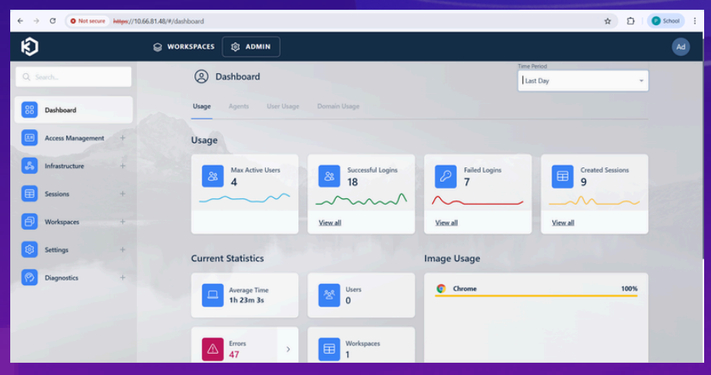
วิธีการเข้าใช้งาน

1. เปิดลิงก์ URL
2. สมัครบัญชี/เข้าสู่ระบบใช้งาน
3. พบหน้าต่าง workspaces จากนั้นเข้าสู่ระบบโดยเป็นบัญชีเดิมที่เข้าในขั้นตอนที่ 2
4. กด Lunch session
5. เริ่มการทำงาน

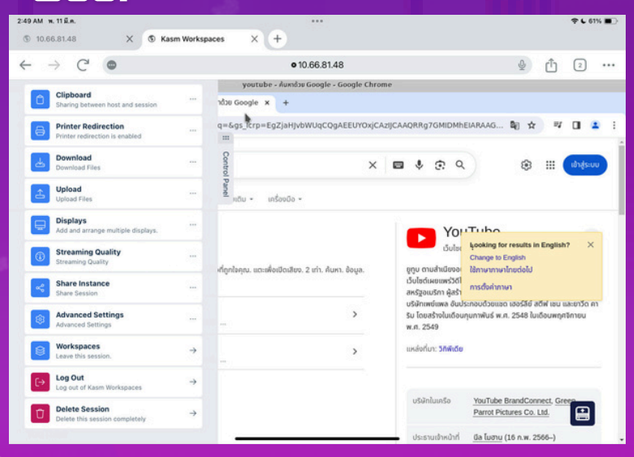
ตัวอย่าง

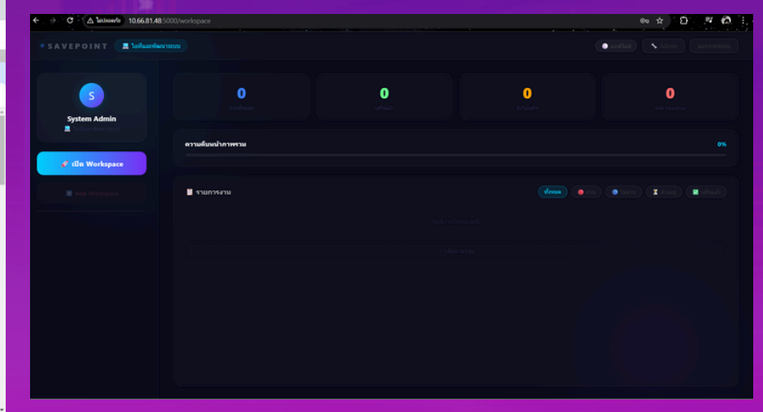
Admin





User





สรุปผลการดำเนินงาน

โครงการ AetherFlow ประสบความสำเร็จในการสร้างระบบพื้นที่ทำงานความปลอดภัยสูงที่ผสานแนวคิด Moving Target Defense และ Zero Trust เข้าด้วยกันอย่างมีประสิทธิภาพ ผลการทดสอบยืนยันว่าระบบสามารถขจัดปัญหาการฝังตัวของมัลแวร์ (Persistence) ได้โดยสมบูรณ์ผ่านกลไกการทำลายและสร้าง Container ใหม่ทุกครั้งหลังใช้งาน (Ephemeral Workspace)
ในด้านการใช้งานจริง ระบบ Task-Based Snapshot ช่วยรักษาความต่อเนื่องของงานได้แม่นยำและลดเวลาการเตรียมระบบได้มากกว่า 80% โดยมีการควบคุมความถูกต้องของข้อมูลด้วยรหัสลับ SHA-256 เพื่อป้องกันการดัดแปลงจุดเซฟ นอกจากนี้ การทำงานร่วมกันระหว่าง Python Sentinel และ ClamAV ยังช่วยให้การตรวจจับและกักกันไฟล์อันตราย (Incident Response) เป็นไปอย่างอัตโนมัติพร้อมการแจ้งเตือนแบบ Real-time สถาปัตยกรรมที่แยกโซนการประมวลผลออกจากโซนจัดเก็บข้อมูล (Isolation) จึงทำให้ระบบมีความมั่นคงปลอดภัยสูง เหมาะสำหรับการนำไปประยุกต์ใช้เป็นมาตรฐานพื้นที่ทำงานยุคใหม่ที่ปลอดภัยจากภัยคุกคามไซเบอร์ในระดับองค์กร

อ้างอิง

[1] Kasm Technologies. (2023). Kasm Workspaces Documentation.
[2] เจือตี๋ อ. (2568). การวิเคราะห์แนวโน้มการโจมตีทางไซเบอร์และแนวทางการป้องกันเชิงรุก. วารสารการประยุกต์ใช้เทคโนโลยีสารสนเทศ.

สมาชิก GROUP 14 SECTION 1

นางสาวกฤตยา คุขวัฒน์	รหัสนักศึกษา 673380143-2
นางสาวกัลยารัตน์ รอดพันดุง	รหัสนักศึกษา 673380146-6
นางสาวปนัดดา ยิงแก้ว	รหัสนักศึกษา 673380168-6
นางสาวอธิชนันท์ ปัญญาชนวัฒน์	รหัสนักศึกษา 673380195-3
นางสาวธีรนาฏ บางผึ้ง	รหัสนักศึกษา 673380482-0
นางสาวภัทราพร โกศล	รหัสนักศึกษา 673380485-4