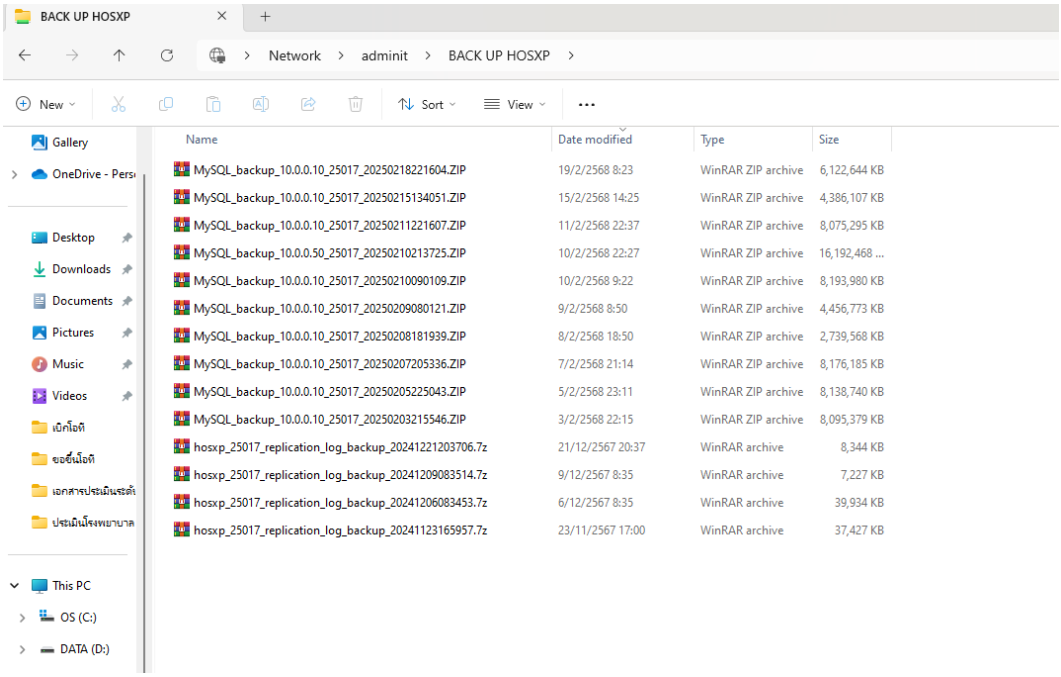
สำนักงานสาธารณสุขจังหวัดน่าน ปีงบประมาณ พ.ศ. ๒๕๖๙

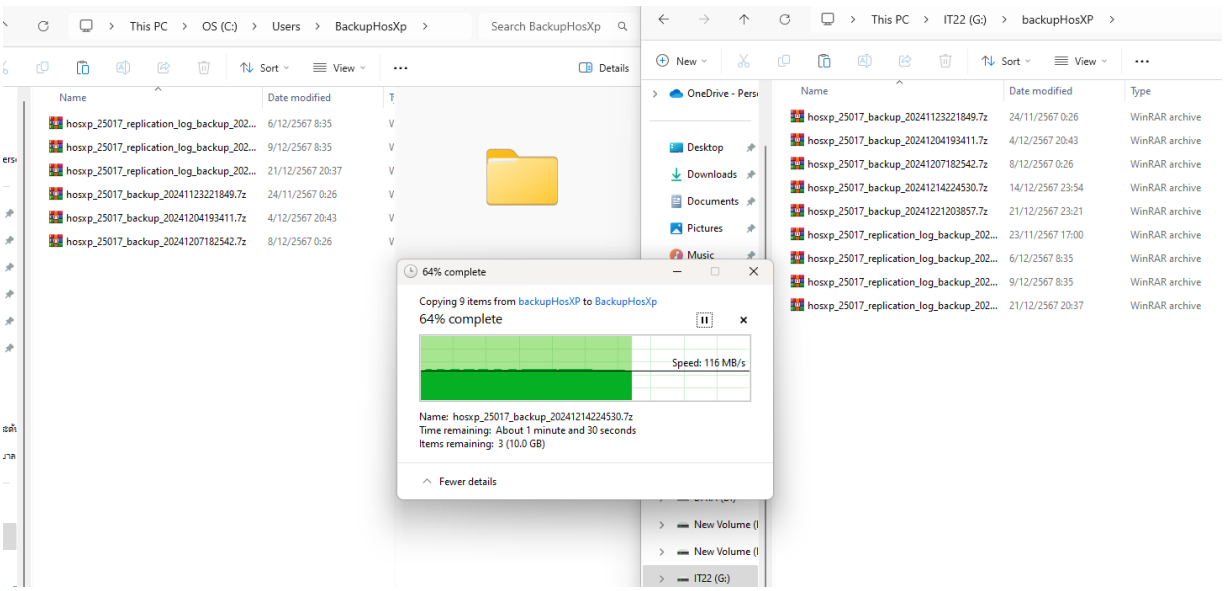
๑. backup

- รายงานผลการดำเนินงาน และมีการสำรองข้อมูล (backup) แบบ ๓-๒-๑ ครบ ๗ วัน ดังภาพ

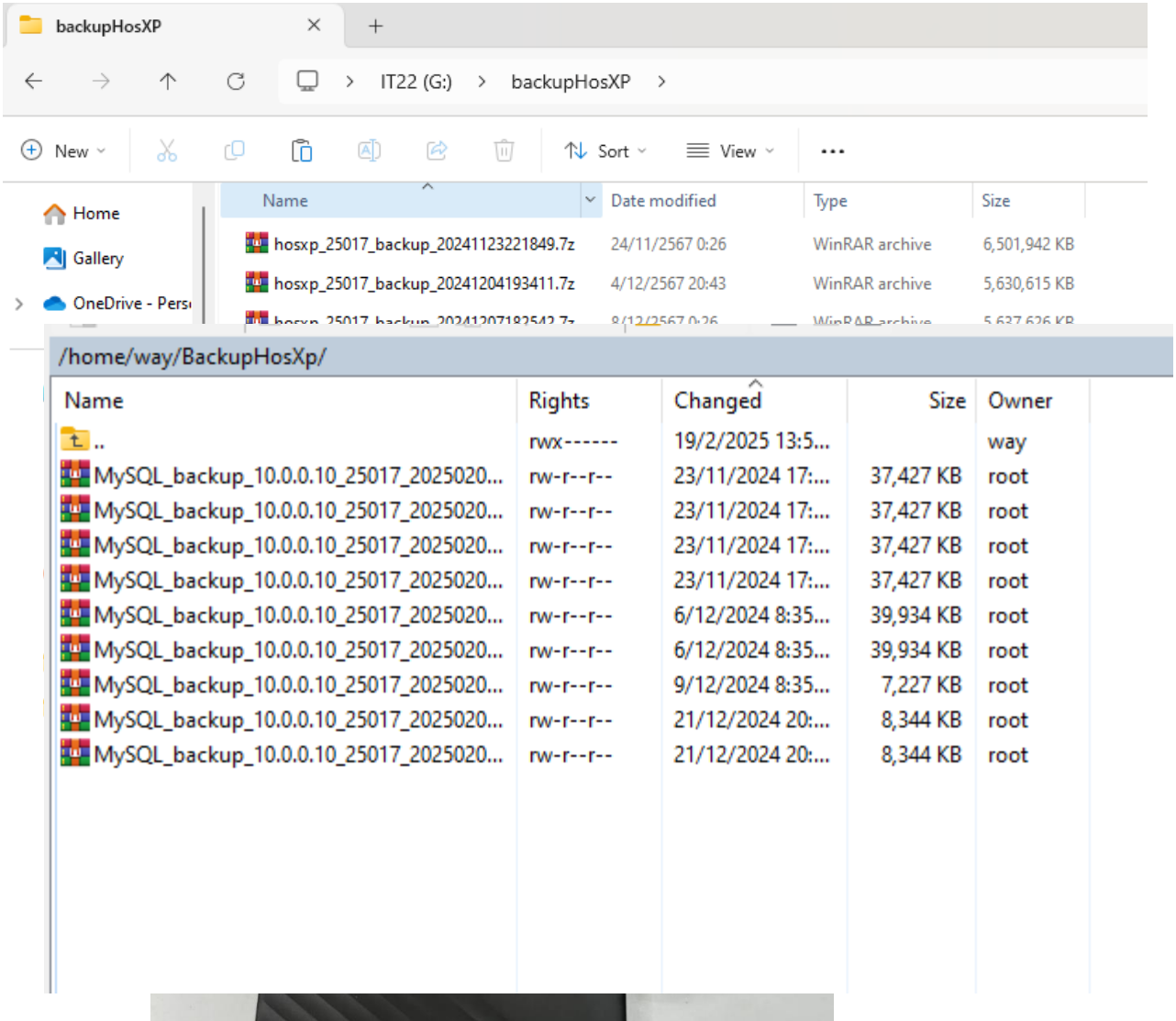
๑.๑ สำเนาข้อมูลไว้บนระบบ ๓ ชุด



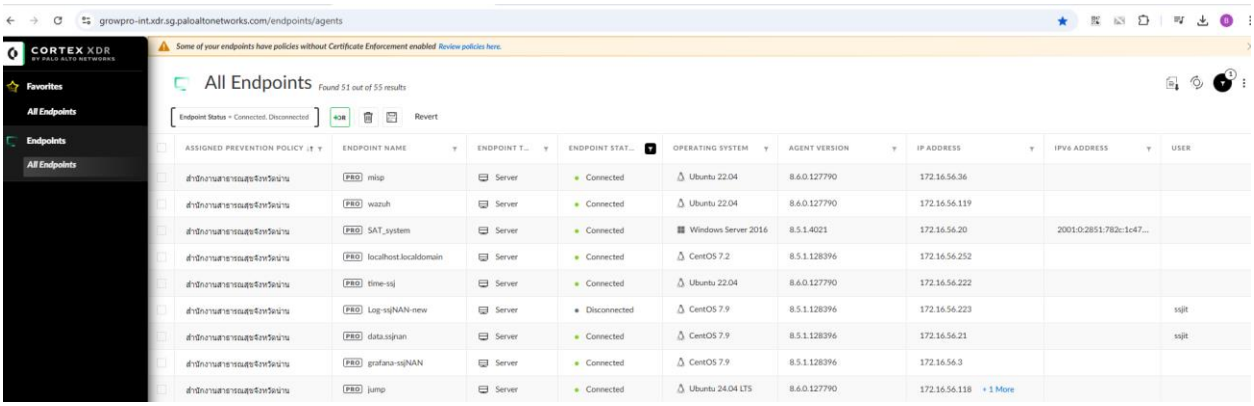
๑.๒ สำเนาข้อมูลไว้บนเทคโนโลยีต่างกัน ๒ ชุด ซึ่ง ชุดแรกจะอยู่ที่เครื่อง linux ชุดที่ ๒ จะอยู่ที่ windows



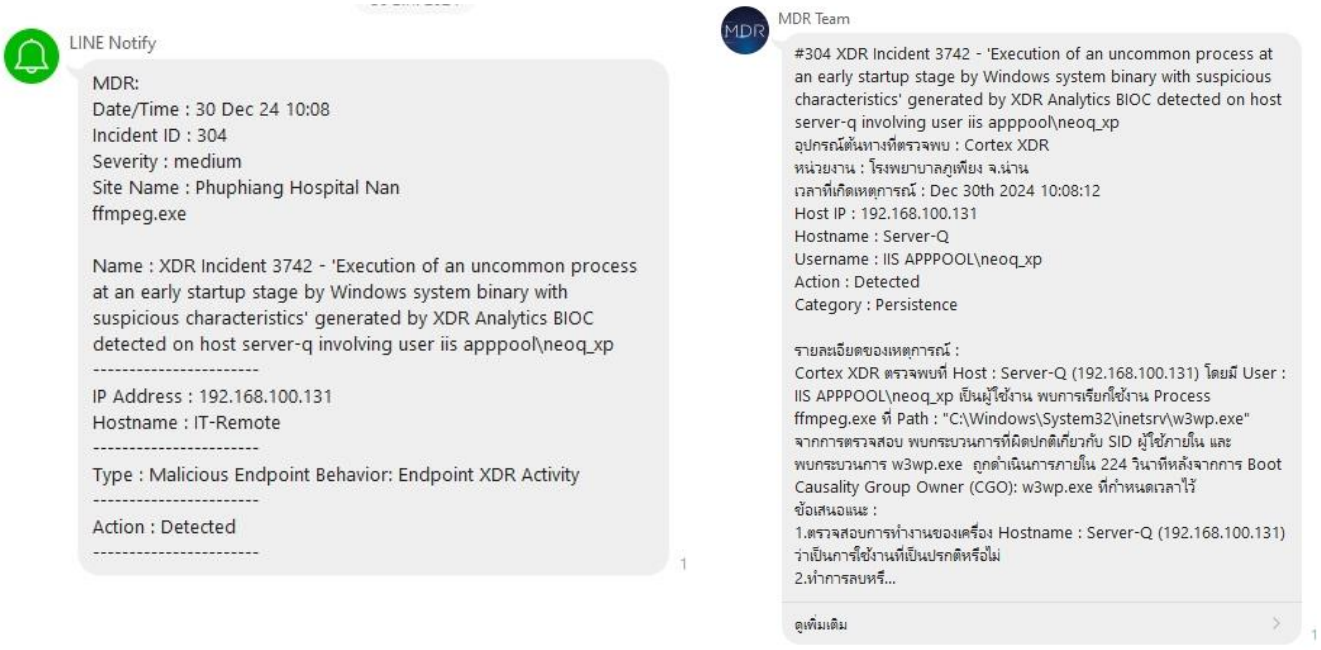
๑.๓ สำเนาข้อมูลไว้แบบ Offline ชนิด external-HDD



๒. Antivirus Software – coretex XDR by PALO



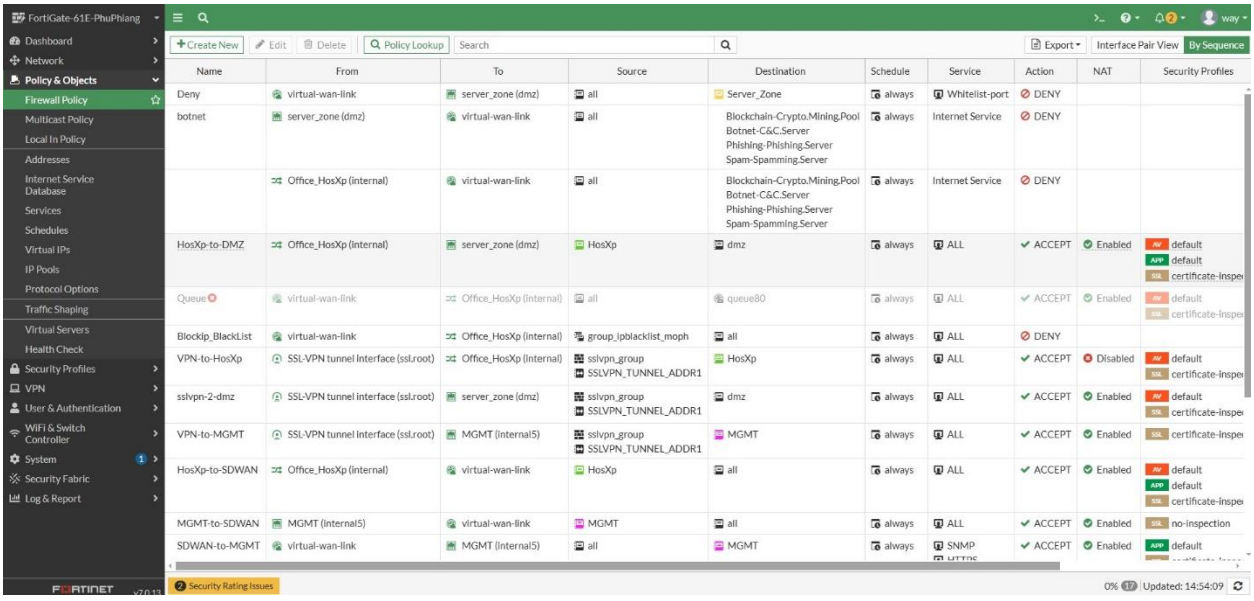
- และมีทีม soc จาก vendor coretex ทำการแจ้งเตือน อุบัติการ ให้ทราบเมื่อมีเหตุการณ์น่าสงสัย



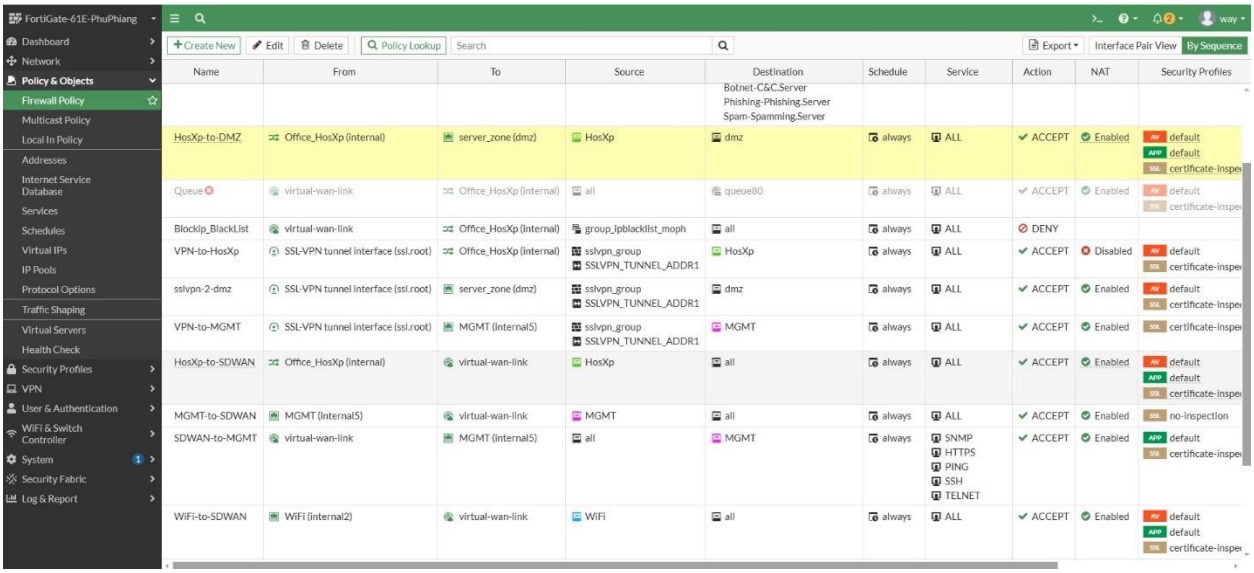
๓. Access Control (Public และ Private)

- มีการกำหนด ขาเข้าจากภายนอกไปยัง server zone และมีการกำหนดจากภายในเข้าไปยัง server zone เช่น ๔๔๓ , ๕๕๐๕,

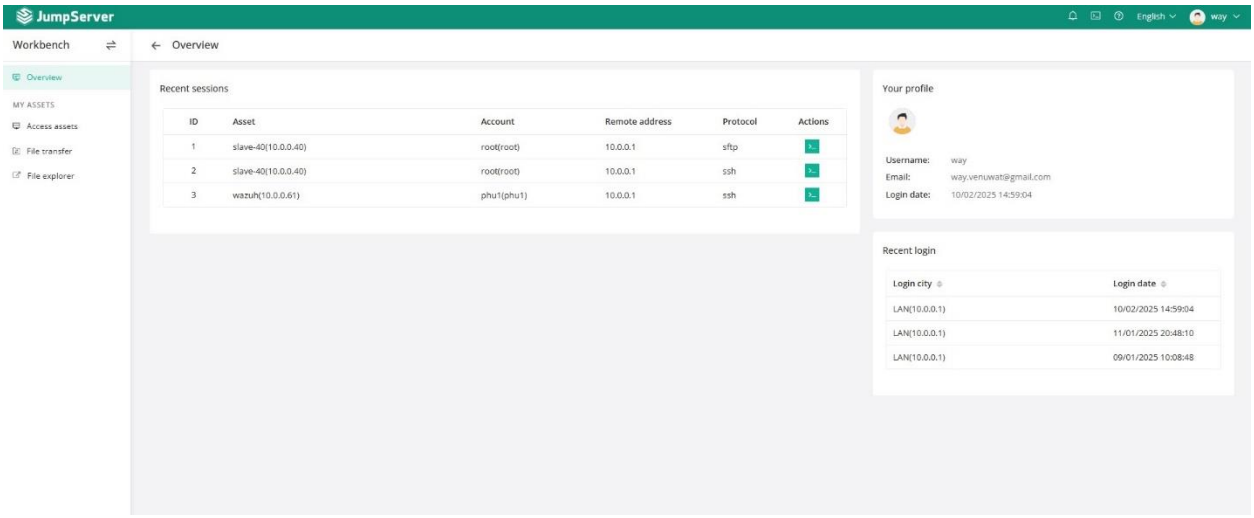
๓.๑ ขาเข้าจากภายนอกไปยัง server zone มีการเปิดใช้งานเฉพาะ port ที่จำเป็นเท่านั้น ดังภาพ



๓.๒ ขาเข้าจากภายในไปยัง server zone มีการเปิดใช้งานเฉพาะ port ที่จำเป็นเท่านั้น ดังภาพ



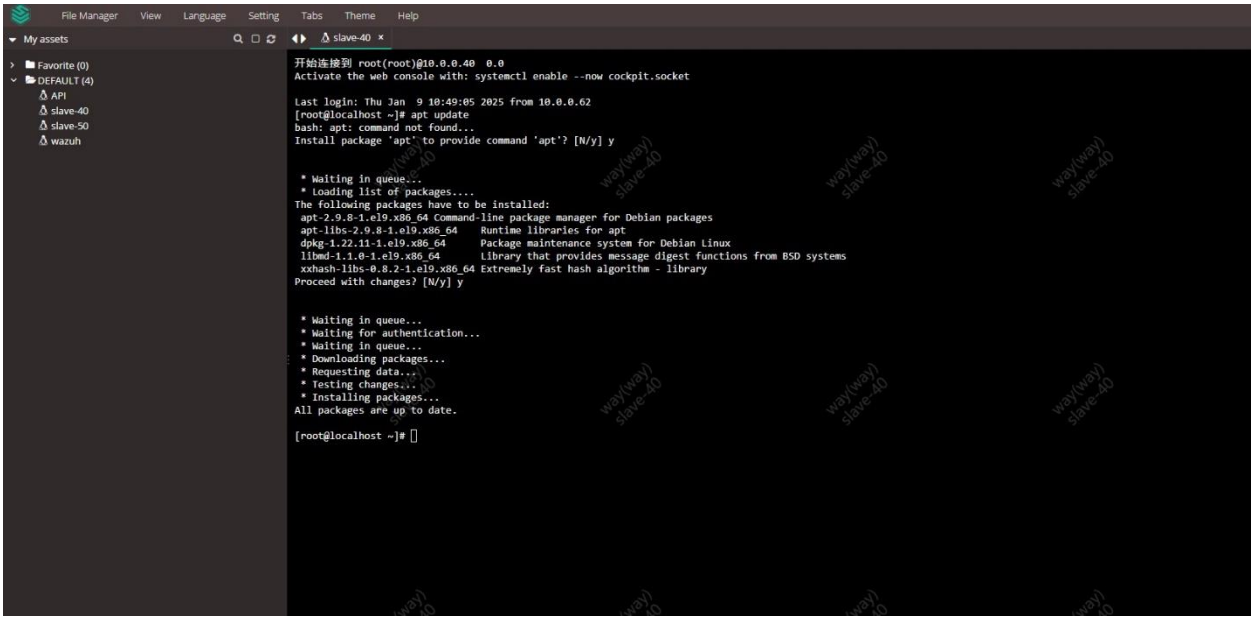
๔. Privileged Access Management (PAM) ใช้ jump ในการเข้าถึงการใช้งาน server โดยตรง เพราะจะมีการเก็บ log ของผู้ที่เข้าใช้งาน ว่าใช้คำสั่งอะไรไปบ้าง ดังภาพ



๕. Business Continuity Plan (BCP) Disaster Recovery Plan (DRP)

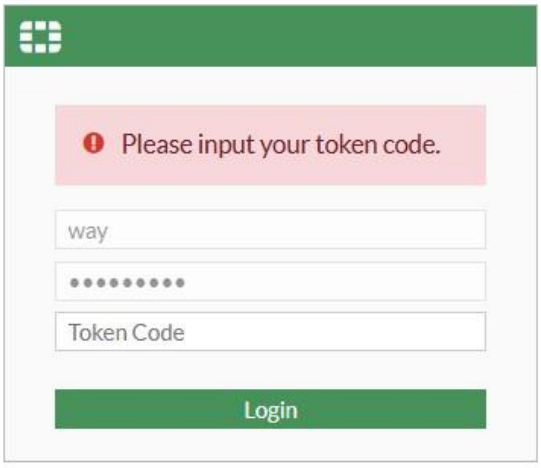
- แผนที่กำหนดแนวทางการ ดำเนินการของหน่วยงาน เมื่อเกิดสภาวะวิกฤตหรือภัยต่าง ๆ ที่ ส่งผลให้กระบวนการทำงานของ หน่วยงานหยุดชะงัก เพื่อให้ สามารถกลับมาดำเนินการได้อย่าง ต่อเนื่อง ดังเอกสารแนบ

๖. OS Patching: การซ่อมแซม จุดบกพร่องของระบบปฏิบัติการ (OS) หรือปรับปรุงระบบปฏิบัติการให้ ทันสมัย และเพิ่มเติมความสามารถใน การใช้งานหรือประสิทธิภาพให้ดีขึ้น ดังภาพ

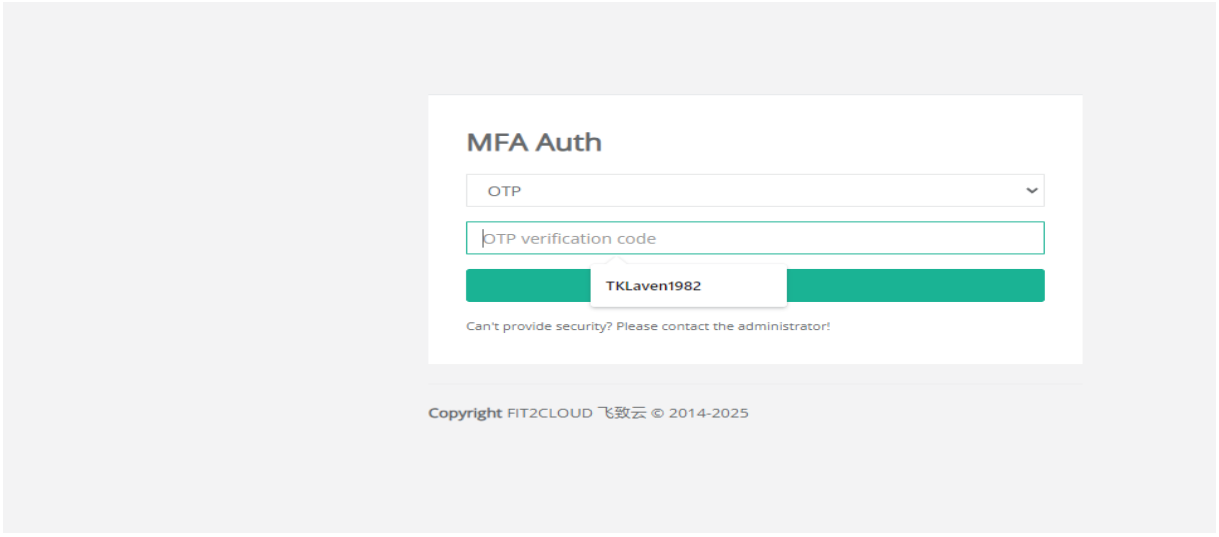


๗. Multi-Factor Authentication (๒FA) : การยืนยันตัวตน ๒ ชั้น เป็นการเข่าสู่ ระบบบัญชีแบบ หลายขั้นตอน ที่กำหนดให้ผู้ใช้ป้อน ข้อมูลเพิ่มเติมนอกเหนือจากรหัสผ่าน

๗.๑ ใช้ forti token เพื่อการเข้าถึง firewall ดังภาพ



๗.๒ ใช้ ๒FA เพื่อการเข้าถึง PAM(jump server)

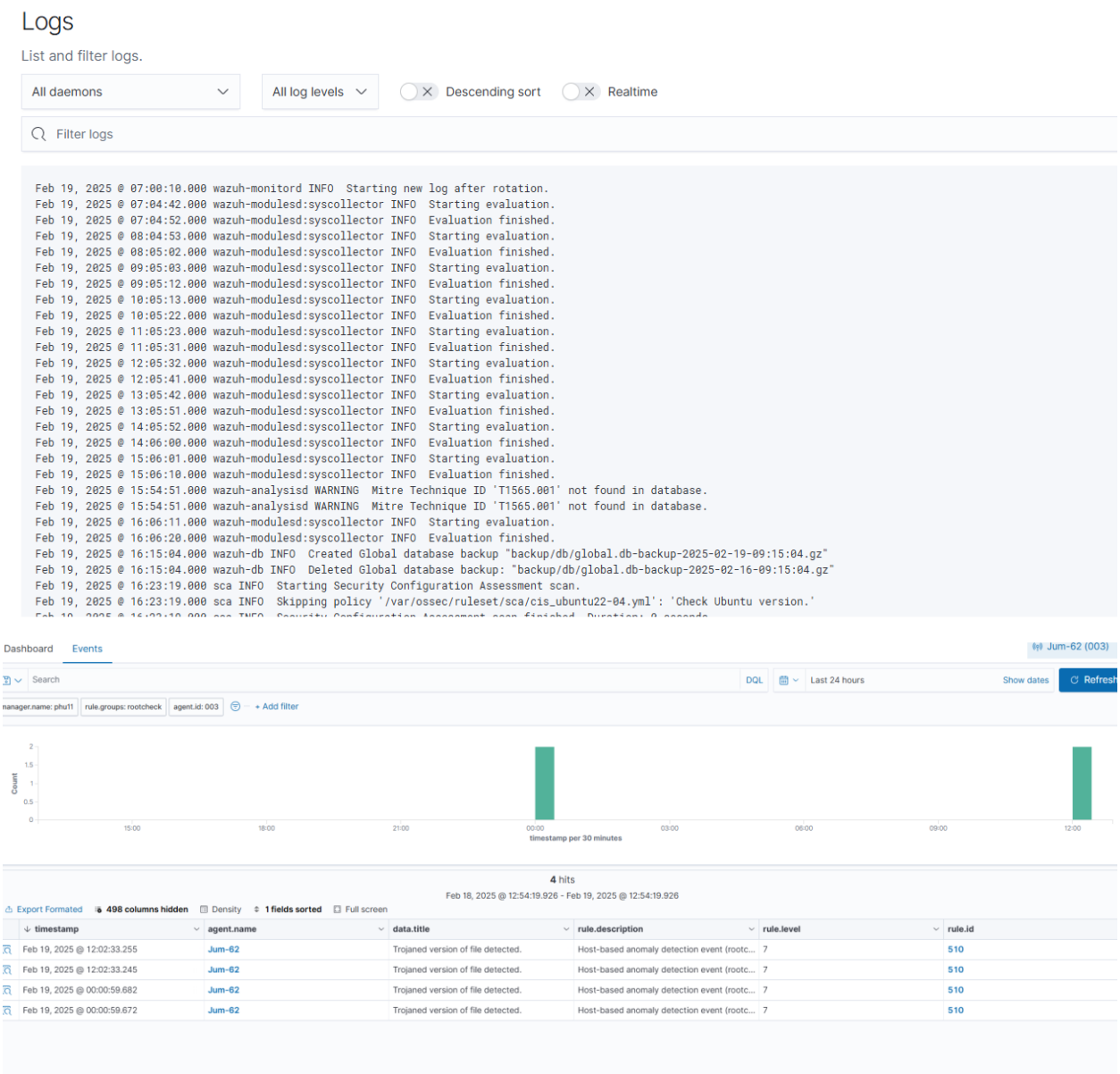


๘. Web Application Firewall (WAF) : ระบบป้องกันการโจมตีทางไซเบอร์ สำหรับเว็บแอพพลิเคชั่นโดยเฉพาะ เพื่อป้องกันการโจมตีไปยัง ระบบเว็บแอปพลิเคชั่นของหน่วยงาน

- โรงพยาบาลภูเพียง ได้ดำเนินการใช้งาน WAF กับทางศูนย์เทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงสาธารณสุข

๙. Log Management : การจัดเก็บข้อมูลจราจรทาง คอมพิวเตอร์

โรงพยาบาลภูเพียง ได้จัดทำ log การยืนยันตัวตนไว้ที่ระบบ wazuh เพื่อเก็บข้อมูลการจราจร ภายในสำนักงาน ดังภาพ



Files (4798)

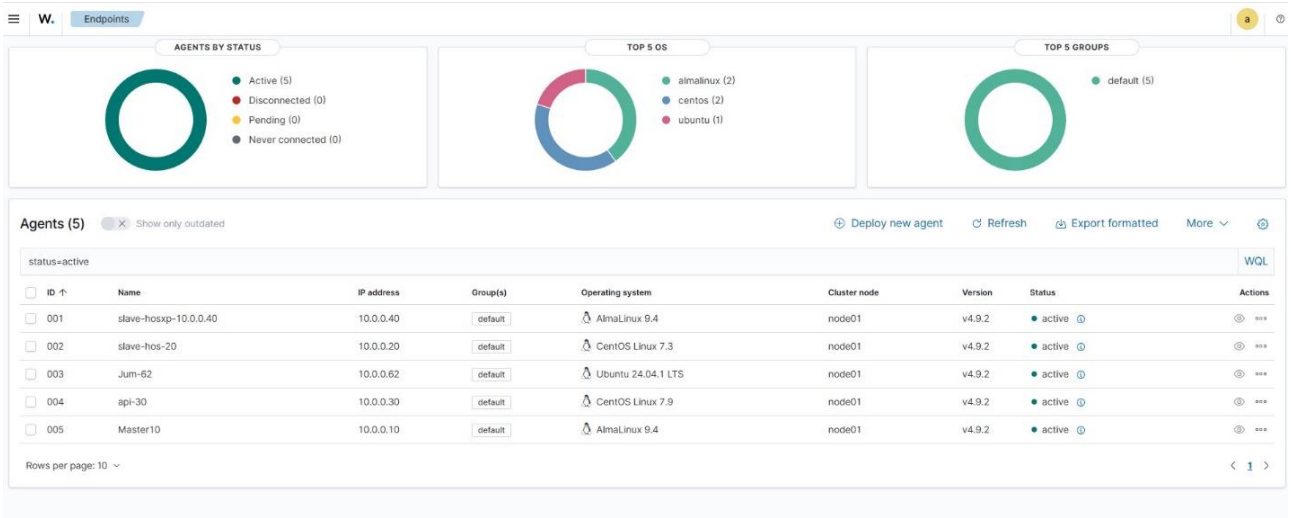
Refresh Export fo

Search

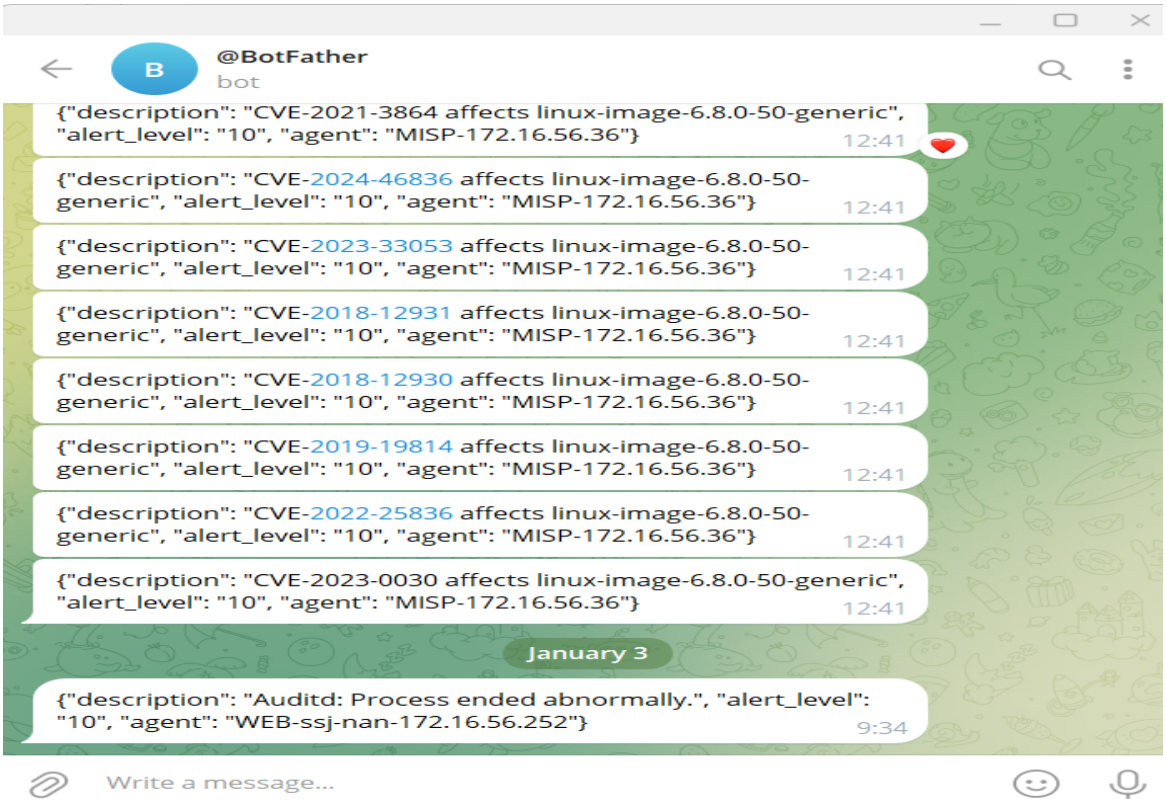
File	Last Modified	User	User ID	Group	Group ID	Size
/bin	Apr 22, 2024 @ 20:08:03.000	root	0	root	0	7
/boot/System.map-6.8.0-51-generic	Dec 1, 2024 @ 01:21:46.000	root	0	root	0	9072978
/boot/System.map-6.8.0-52-generic	Jan 11, 2025 @ 00:18:33.000	root	0	root	0	9072978
/boot/config-6.8.0-51-generic	Dec 1, 2024 @ 01:21:46.000	root	0	root	0	287413
/boot/config-6.8.0-52-generic	Jan 11, 2025 @ 00:18:33.000	root	0	root	0	287413
/boot/efi/EFI/Boot/bootx64.efi	Jan 9, 2025 @ 04:40:04.000	root	0	root	0	966664
/boot/efi/EFI/Boot/fbx64.efi	Jan 9, 2025 @ 04:40:04.000	root	0	root	0	88344
/boot/efi/EFI/Boot/mmx64.efi	Jan 9, 2025 @ 04:40:04.000	root	0	root	0	856280
/boot/efi/EFI/Microsoft/Boot/BCD	Jan 8, 2025 @ 21:27:48.000	root	0	root	0	32768
/boot/efi/EFI/Microsoft/Boot/BCD.LOG1	Jul 11, 2024 @ 10:33:32.000	root	0	root	0	8192
/boot/efi/EFI/Microsoft/Boot/BCD.LOG2	Jul 11, 2024 @ 10:33:32.000	root	0	root	0	0
/boot/efi/EFI/Microsoft/Boot/BOOTSTAT.DAT	Aug 21, 2024 @ 23:15:08.000	root	0	root	0	65536
/boot/efi/EFI/Microsoft/Boot/CIPolicies/Active/{5DAC656C-21AD-4A02-AB49-649917162E70}.cip	May 7, 2022 @ 19:20:02.000	root	0	root	0	10564
/boot/efi/EFI/Microsoft/Boot/CIPolicies/Active/{82443e1e-8a39-4b4a-96a8-f40ddc00b9f3}.cip	Dec 4, 2023 @ 20:23:54.000	root	0	root	0	31285
/boot/efi/EFI/Microsoft/Boot/CIPolicies/Active/{CDD5CB55-DB68-4D71-AA38-3DF2B6473A52}.cip	May 7, 2022 @ 19:20:02.000	root	0	root	0	10972

๑๐. Security Information & Event Management (SIEM) : ระบบที่ใช้ในการจัดการกับ Log และ Event ต่างๆ ที่คอยทำหน้าที่วิเคราะห์หาความเชื่อมโยงของ Event ต่าง ๆ ที่เกี่ยวข้องกับความปลอดภัยทั้งหมด ไปจนถึงการ Alert ระบุตำแหน่งของภัยคุกคามให้ทราบ เมื่อมี Event ที่ผิดปกติ ทำให้สามารถป้องกัน และตอบสนองภัยคุกคามได้ อย่างรวดเร็ว

- สำนักงานสาธารณสุขจังหวัดน่าน ใช้ wazuh เพื่อทำระบบ SIEM เพื่อดูการจราจรของ server และตรวจสอบถึงภัยคุกคาม เพื่อจะหาจุดป้องกันในระบบ server ดังภาพ



และได้กำหนดการตั้งค่าให้ wazuh alert to telegram เมื่อมี level การคุกคามใน level ๑๐ ขึ้นไป ดังภาพ



๑๑. Vulnerability Assessment (VA Scan) : การตรวจสอบช่องโหว่ของระบบ เพื่อให้ทราบถึงความเสี่ยง จุดอ่อน และระดับความรุนแรง ของผลกระทบ ที่อาจเกิดขึ้นจากการถูกโจรกรรม ข้อมูลและการโจมตีทางไซเบอร์

- โรงพยาบาลภูเพียง ทำ VA เพื่อหาช่องโหว่และทำการ update patch และปิดจุดเสี่ยง ดังภาพ

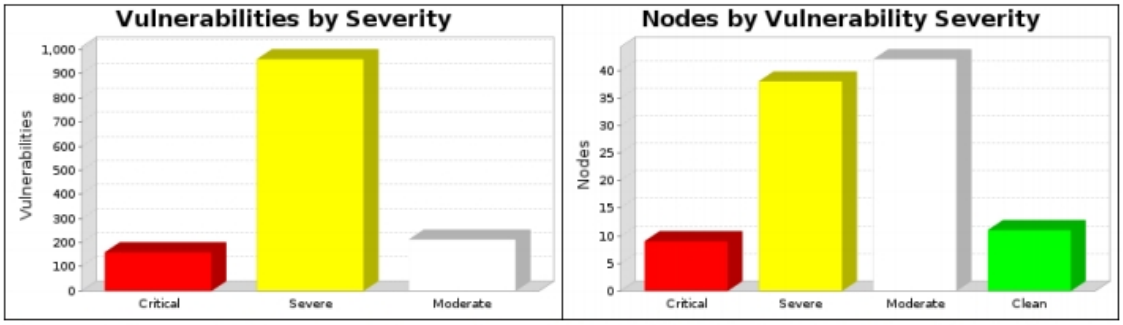
1. Executive Summary

This report represents a security audit performed by InsightVM from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

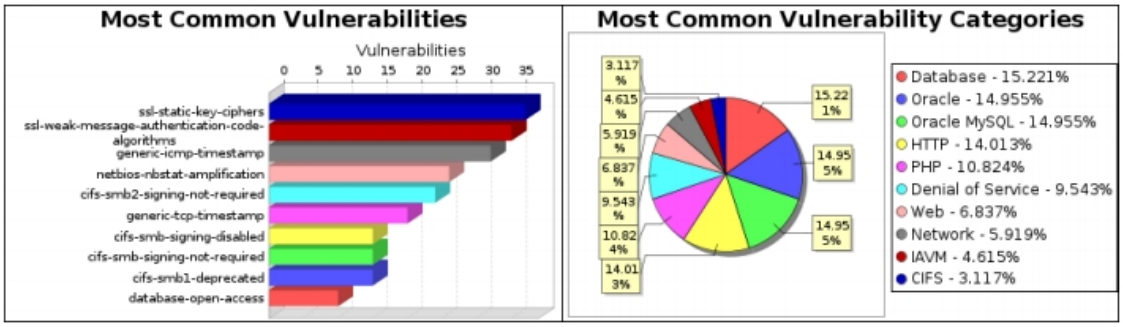
Site Name	Start Time	End Time	Total Time	Status
Phuphiang Hospital	October 03, 2024 16:53, ICT	October 03, 2024 17:22, ICT	29 minutes	Success

There is not enough historical data to display overall asset trend.

The audit was performed on 53 systems, 53 of which were found to be active and were scanned.



There were 1,333 vulnerabilities found during this scan. Of these, 160 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 960 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 213 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities. Critical vulnerabilities were found to exist on 9 of the systems, making them most susceptible to attack. 38 systems were found to have severe vulnerabilities. Moderate vulnerabilities were found on 42 systems. No vulnerabilities were found on the remaining 11 systems.



There were 37 occurrences of the ssl-static-key-ciphers vulnerability, making it the most common vulnerability. There were 630 vulnerability instances in the Database category, making it the most common vulnerability category.