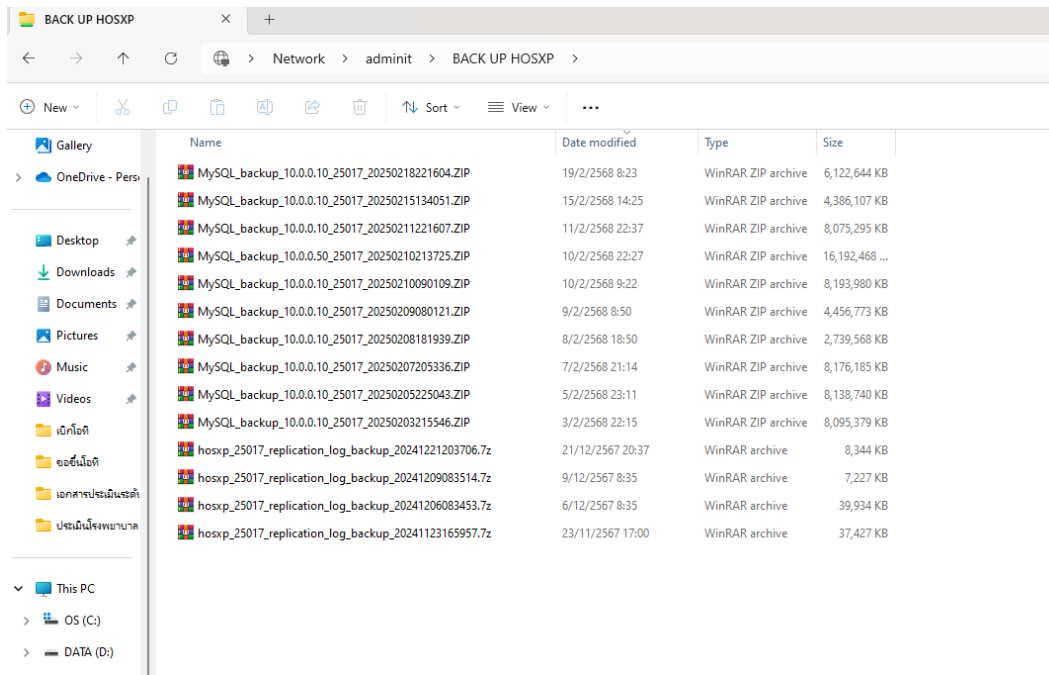


สำนักงานสาธารณสุขจังหวัดน่าน ปีงบประมาณ พ.ศ. ๒๕๖๙

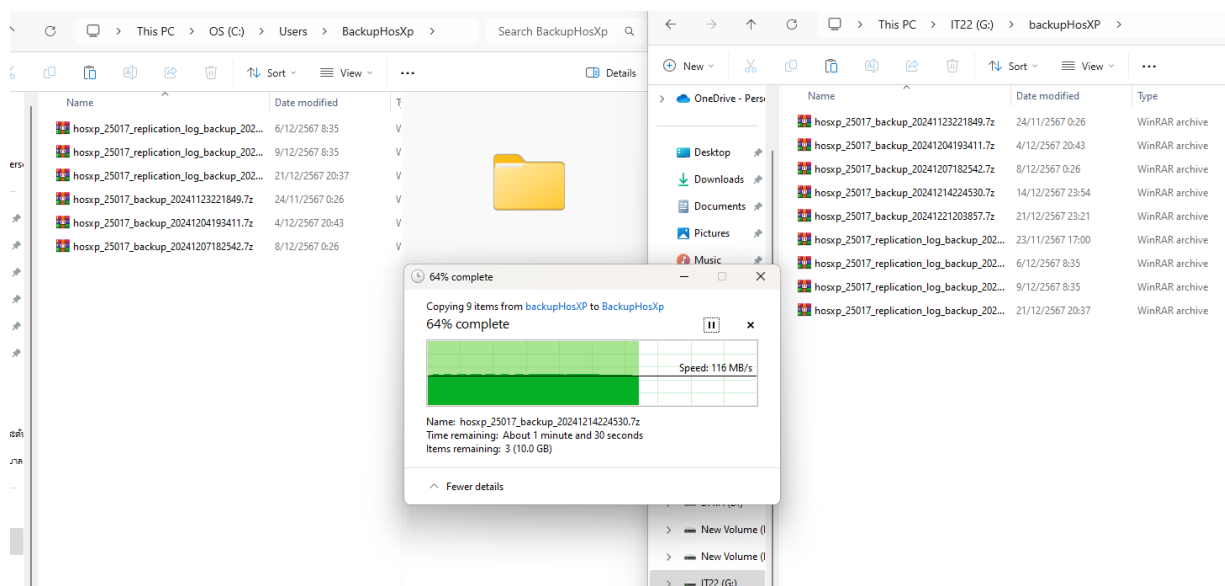
๑. backup

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

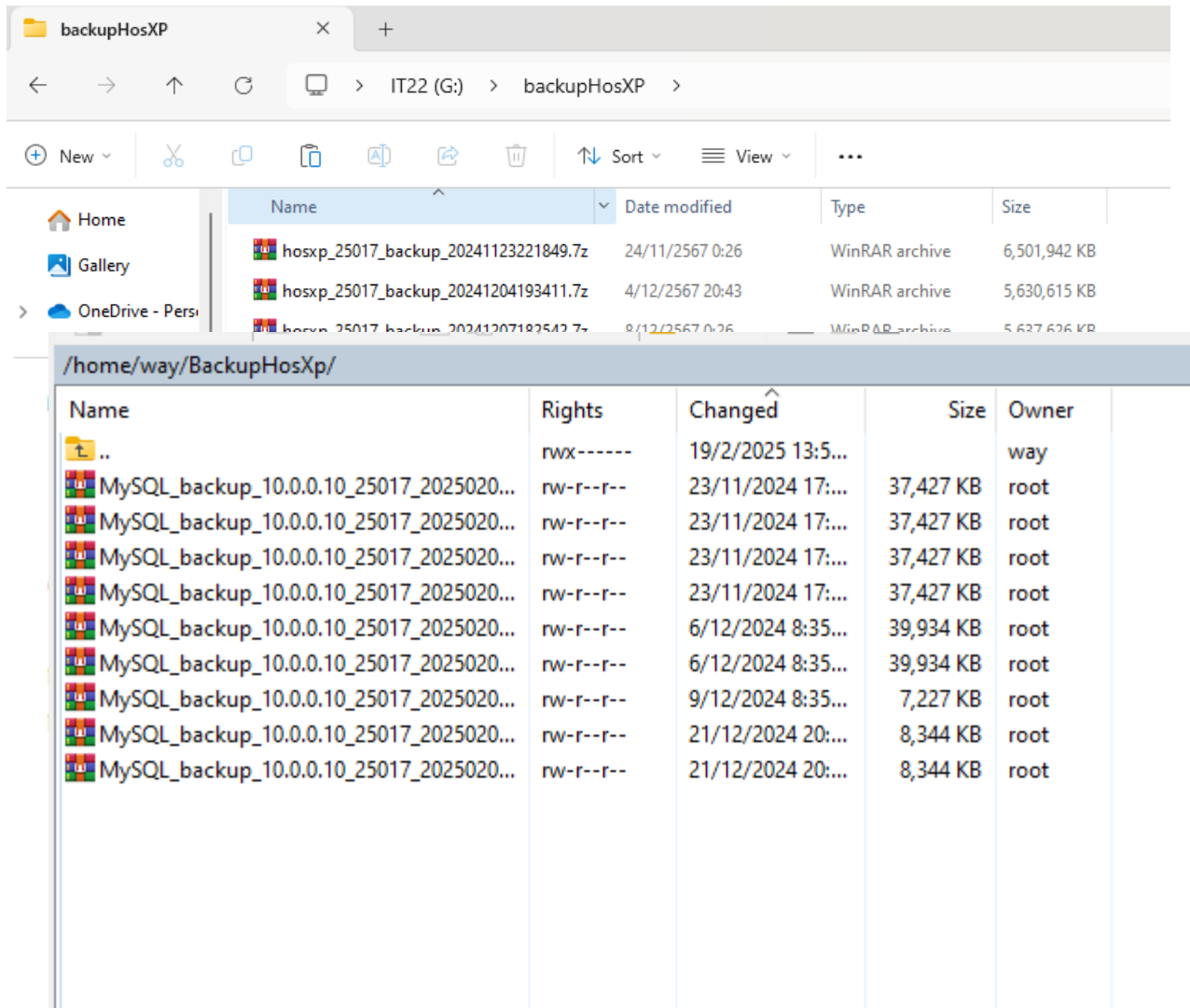
๑.๑ สำเนาข้อมูลไว้บนระบบ ๓ ชุด



๑.๒ สำเนาข้อมูลไว้บนเทคโนโลยีต่างกัน ๒ ชุด ซึ่ง ชุดแรกจะอยู่ที่เครื่อง linux ชุดที่ ๒ จะอยู่ที่ windows



๑.๓ สำเนาข้อมูลไว้แบบ Offline ชนิด external-HDD



The screenshot shows a file explorer window with the address bar indicating the path: IT22 (G:) > backupHosXP. The main pane displays a list of files:

Name	Date modified	Type	Size
hosxp_25017_backup_20241123221849.7z	24/11/2567 0:26	WinRAR archive	6,501,942 KB
hosxp_25017_backup_20241204193411.7z	4/12/2567 20:43	WinRAR archive	5,630,615 KB
hosxp_25017_backup_20241207192542.7z	8/12/2567 0:26	WinRAR archive	5,637,626 KB

Below this, a detailed view of the directory structure is shown for the path /home/way/BackupHosXp/:

Name	Rights	Changed	Size	Owner
..	rwX-----	19/2/2025 13:5...		way
MySQL_backup_10.0.0.10_25017_2025020...	rw-r--r--	23/11/2024 17:...	37,427 KB	root
MySQL_backup_10.0.0.10_25017_2025020...	rw-r--r--	23/11/2024 17:...	37,427 KB	root
MySQL_backup_10.0.0.10_25017_2025020...	rw-r--r--	23/11/2024 17:...	37,427 KB	root
MySQL_backup_10.0.0.10_25017_2025020...	rw-r--r--	23/11/2024 17:...	37,427 KB	root
MySQL_backup_10.0.0.10_25017_2025020...	rw-r--r--	6/12/2024 8:35...	39,934 KB	root
MySQL_backup_10.0.0.10_25017_2025020...	rw-r--r--	6/12/2024 8:35...	39,934 KB	root
MySQL_backup_10.0.0.10_25017_2025020...	rw-r--r--	9/12/2024 8:35...	7,227 KB	root
MySQL_backup_10.0.0.10_25017_2025020...	rw-r--r--	21/12/2024 20:...	8,344 KB	root
MySQL_backup_10.0.0.10_25017_2025020...	rw-r--r--	21/12/2024 20:...	8,344 KB	root



๒. Antivirus Software – coretex XDR by PALO

ASSIGNED PREVENTION POLICY	ENDPOINT NAME	ENDPOINT T...	ENDPOINT STAT...	OPERATING SYSTEM	AGENT VERSION	IP ADDRESS	IPv6 ADDRESS	USER
PRE mlip	mlip	Server	Connected	Ubuntu 22.04	8.6.0.127790	172.16.56.36		
PRE wazuh	wazuh	Server	Connected	Ubuntu 22.04	8.6.0.127790	172.16.56.119		
PRE SAT_system	SAT_system	Server	Connected	Windows Server 2016	8.5.1.4021	172.16.56.20	2001:0:2851:782c:1c47...	
PRE localhost.localdomain	localhost.localdomain	Server	Connected	CentOS 7.2	8.5.1.128396	172.16.56.252		
PRE time-sj	time-sj	Server	Connected	Ubuntu 22.04	8.6.0.127790	172.16.56.222		
PRE Log-sj/NAN-new	Log-sj/NAN-new	Server	Disconnected	CentOS 7.9	8.5.1.128396	172.16.56.223		sjr
PRE data.sjnan	data.sjnan	Server	Connected	CentOS 7.9	8.5.1.128396	172.16.56.21		sjr
PRE grafana-sj/NAN	grafana-sj/NAN	Server	Connected	CentOS 7.9	8.5.1.128396	172.16.56.3		
PRE jump	jump	Server	Connected	Ubuntu 24.04 LTS	8.6.0.127790	172.16.56.118		

- และมีทีม soc จาก vendor coretex ทำการแจ้งเตือน อุบัติการ ให้ทราบเมื่อมีเหตุการณ์น่าสงสัย



LINE Notify

MDR:

Date/Time : 30 Dec 24 10:08

Incident ID : 304

Severity : medium

Site Name : Phuphiang Hospital Nan

ffmpeg.exe

Name : XDR Incident 3742 - 'Execution of an uncommon process at an early startup stage by Windows system binary with suspicious characteristics' generated by XDR Analytics BIOC detected on host server-q involving user iis apppool\neooq_xp

IP Address : 192.168.100.131

Hostname : IT-Remote

Type : Malicious Endpoint Behavior: Endpoint XDR Activity

Action : Detected



MDR Team

#304 XDR Incident 3742 - 'Execution of an uncommon process at an early startup stage by Windows system binary with suspicious characteristics' generated by XDR Analytics BIOC detected on host server-q involving user iis apppool\neooq_xp
อุปกรณ์ต้นทางที่ตรวจพบ : Cortex XDR
หน่วยงาน : โรงพยาบาลกุพิียง จ.น่าน
เวลาที่เกิดเหตุการณ์ : Dec 30th 2024 10:08:12
Host IP : 192.168.100.131
Hostname : Server-Q
Username : IIS APPPOOL\neooq_xp
Action : Detected
Category : Persistence

รายละเอียดของเหตุการณ์ :

Cortex XDR ตรวจพบที่ Host : Server-Q (192.168.100.131) โดยมี User : IIS APPPOOL\neooq_xp เป็นผู้ใช้งาน พบการเรียกใช้งาน Process ffmpeg.exe ที่ Path : "C:\Windows\System32\inetsrv\w3wp.exe" จากการตรวจสอบ พบกระบวนการที่ผิดปกติเกี่ยวกับ SID ผู้ใช้ภายใน และ พบกระบวนการ w3wp.exe ถูกดำเนินการภายใน 224 วินาทีหลังจากการ Boot Causality Group Owner (CGO): w3wp.exe ที่กำหนดเวลาไว้
ข้อเสนอแนะ :
1.ตรวจสอบการทำงานของเครื่อง Hostname : Server-Q (192.168.100.131) ว่าเป็นการรันใช้งานที่เป็นปกติหรือไม่
2.ทำการลบหรือ...

ดูเพิ่มเติม

๓. Access Control (Public และ Private)

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

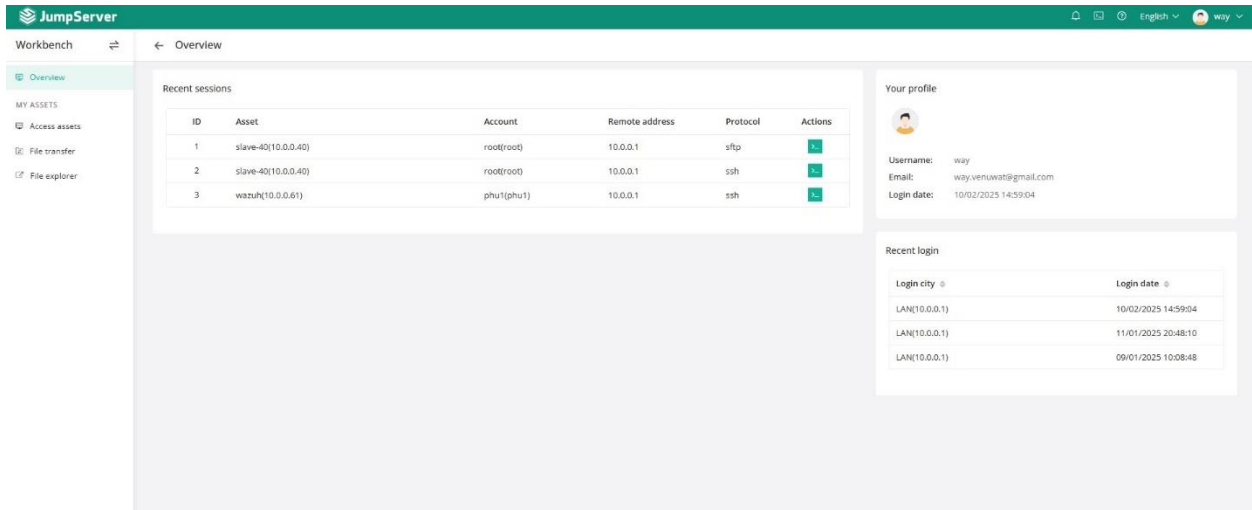
๓.๑ ขาเข้าจากภายนอกไปยัง server zone มีการเปิดใช้งานเฉพาะ port ที่จำเป็นเท่านั้น ดังภาพ

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
Deny	virtual-wan-link	server_zone (dmz)	all	Server_Zone	always	Whitelist-port	DENY		
botnet	server_zone (dmz)	virtual-wan-link	all	Blockchain-Crypto.Mining.Pool Botnet-C&C.Server Phishing-Phishing.Server Spam-Spamming.Server	always	Internet Service	DENY		
	Office_HosXp (internal)	virtual-wan-link	all	Blockchain-Crypto.Mining.Pool Botnet-C&C.Server Phishing-Phishing.Server Spam-Spamming.Server	always	Internet Service	DENY		
HosXp-to-DMZ	Office_HosXp (internal)	server_zone (dmz)	HosXp	dmz	always	ALL	ACCEPT	Enabled	default certificate-inspe
Queue	virtual-wan-link	Office_HosXp (internal)	all	queue80	always	ALL	ACCEPT	Enabled	default certificate-inspe
Blockip_BlackList	virtual-wan-link	Office_HosXp (internal)	group_ipblacklist_moph	all	always	ALL	DENY		
VPN-to-HosXp	SSL-VPN tunnel interface (ssl.root)	Office_HosXp (internal)	sslvpn_group SSLVPN_TUNNEL_ADDR1	HosXp	always	ALL	ACCEPT	Disabled	default certificate-inspe
sslvpn-2-dmz	SSL-VPN tunnel interface (ssl.root)	server_zone (dmz)	sslvpn_group SSLVPN_TUNNEL_ADDR1	dmz	always	ALL	ACCEPT	Enabled	default certificate-inspe
VPN-to-MGMT	SSL-VPN tunnel interface (ssl.root)	MGMT (internal5)	sslvpn_group SSLVPN_TUNNEL_ADDR1	MGMT	always	ALL	ACCEPT	Enabled	certificate-inspe
HosXp-to-SDWAN	Office_HosXp (internal)	virtual-wan-link	HosXp	all	always	ALL	ACCEPT	Enabled	default default certificate-inspe
MGMT-to-SDWAN	MGMT (internal5)	virtual-wan-link	MGMT	all	always	ALL	ACCEPT	Enabled	no-inspection
SDWAN-to-MGMT	virtual-wan-link	MGMT (internal5)	all	MGMT	always	SNMP HTTP HTTPS PING SSH TELNET	ACCEPT	Enabled	default certificate-inspe

๓.๒ ขาเข้าจากภายในไปยัง server zone มีการเปิดใช้งานเฉพาะ port ที่จำเป็นเท่านั้น ดังภาพ

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
HosXp-to-DMZ	Office_HosXp (internal)	server_zone (dmz)	HosXp	dmz	always	ALL	ACCEPT	Enabled	default default certificate-inspe
Queue	virtual-wan-link	Office_HosXp (internal)	all	queue80	always	ALL	ACCEPT	Enabled	default certificate-inspe
Blockip_BlackList	virtual-wan-link	Office_HosXp (internal)	group_ipblacklist_moph	all	always	ALL	DENY		
VPN-to-HosXp	SSL-VPN tunnel interface (ssl.root)	Office_HosXp (internal)	sslvpn_group SSLVPN_TUNNEL_ADDR1	HosXp	always	ALL	ACCEPT	Disabled	default certificate-inspe
sslvpn-2-dmz	SSL-VPN tunnel interface (ssl.root)	server_zone (dmz)	sslvpn_group SSLVPN_TUNNEL_ADDR1	dmz	always	ALL	ACCEPT	Enabled	default certificate-inspe
VPN-to-MGMT	SSL-VPN tunnel interface (ssl.root)	MGMT (internal5)	sslvpn_group SSLVPN_TUNNEL_ADDR1	MGMT	always	ALL	ACCEPT	Enabled	certificate-inspe
HosXp-to-SDWAN	Office_HosXp (internal)	virtual-wan-link	HosXp	all	always	ALL	ACCEPT	Enabled	default default certificate-inspe
MGMT-to-SDWAN	MGMT (internal5)	virtual-wan-link	MGMT	all	always	ALL	ACCEPT	Enabled	no-inspection
SDWAN-to-MGMT	virtual-wan-link	MGMT (internal5)	all	MGMT	always	SNMP HTTP HTTPS PING SSH TELNET	ACCEPT	Enabled	default certificate-inspe
WIFI-to-SDWAN	WIFI (internal2)	virtual-wan-link	WIFI	all	always	ALL	ACCEPT	Enabled	default default certificate-inspe

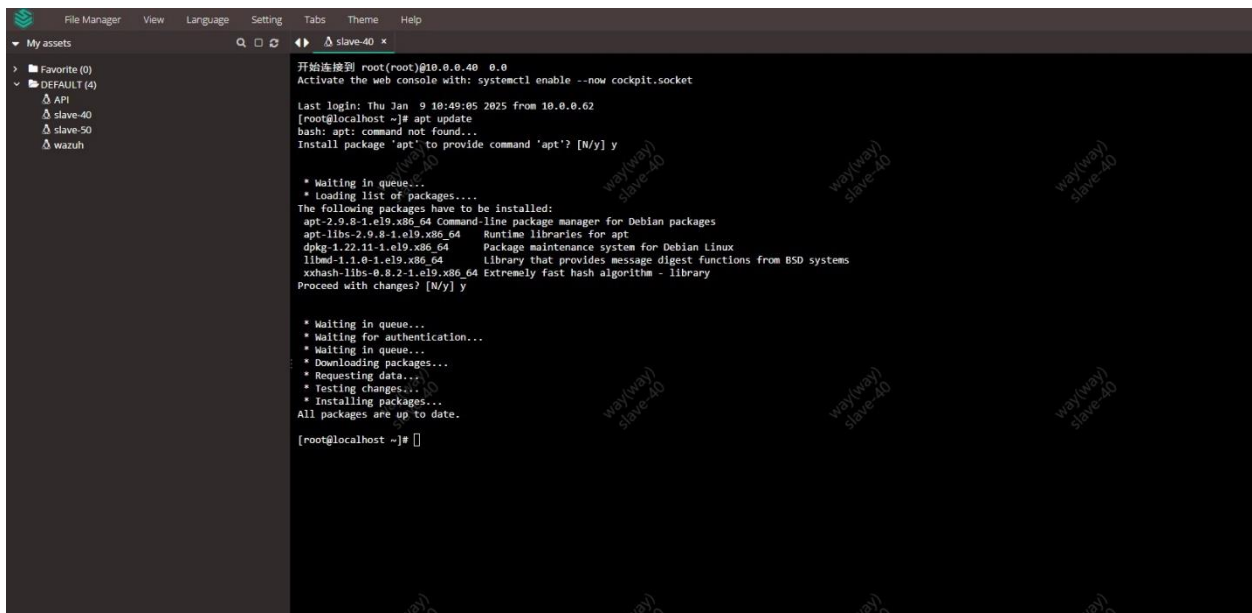
๔. Privileged Access Management (PAM) ใช้ jump ในการเข้าถึงการใช้งาน server โดยตรง เพราะจะมีการเก็บ log ของผู้ที่เข้าใช้งาน ว่าใช้คำสั่งอะไรไปบ้าง ดังภาพ



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

- แผนที่กำหนดแนวทางการ ดำเนินการของหน่วยงาน เมื่อเกิดสภาวะวิกฤตหรือภัยต่าง ๆ ที่ ส่งผลให้ กระบวนการทำงานของ หน่วยงานหยุดชะงัก เพื่อให้ สามารถกลับมาดำเนินการได้อย่าง ต่อเนื่อง ดังเอกสารแนบ

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



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

๗.๑ ใช้ forti token เพื่อการเข้าถึง firewall ดังภาพ

A screenshot of a login interface. At the top left is a logo consisting of a grid of squares. Below it is a red banner with a white exclamation mark icon and the text "Please input your token code." Below the banner are three input fields: the first contains the text "way", the second contains a series of dots, and the third is labeled "Token Code". At the bottom is a green button with the text "Login".

๗.๒ ใช้ ๒FA เพื่อการเข้าถึง PAM(jump server)

A screenshot of an "MFA Auth" form. It features a dropdown menu with "OTP" selected. Below it is an input field for the "OTP verification code". A green button with the text "TKLaven1982" is positioned below the input field. At the bottom of the form, there is a link that says "Can't provide security? Please contact the administrator!". Below the form, there is a copyright notice: "Copyright FIT2CLOUD 飞致云 © 2014-2025".

๘. Web Application Firewall (WAF) : ระบบป้องกันการโจมตีทางไซเบอร์ สำหรับเว็บแอปพลิเคชันโดยเฉพาะ เพื่อป้องกันการโจมตีไปยัง ระบบเว็บแอปพลิเคชันของหน่วยงาน

- โรงพยาบาลภูเก็ต ได้ดำเนินการใช้งาน WAF กับทางศูนย์เทคโนโลยีสารสนเทศ สำนักงาน ปลัดกระทรวงสาธารณสุข

๙. Log Management : การจัดเก็บข้อมูลจราจรทาง คอมพิวเตอร์

โรงพยาบาลภูเก็ต ได้จัดทำ log การยืนยันตัวตนไว้ที่ระบบ wazuh เพื่อเก็บข้อมูลการจราจร ภายในสำนักงาน ดังภาพ

Logs

List and filter logs.

All daemons Descending sort Realtime

Filter logs

```
Feb 19, 2025 @ 07:00:10.000 wazuh-monitord INFO Starting new log after rotation.
Feb 19, 2025 @ 07:04:42.000 wazuh-modulesd:syscollector INFO Starting evaluation.
Feb 19, 2025 @ 07:04:52.000 wazuh-modulesd:syscollector INFO Evaluation finished.
Feb 19, 2025 @ 08:04:53.000 wazuh-modulesd:syscollector INFO Starting evaluation.
Feb 19, 2025 @ 08:05:02.000 wazuh-modulesd:syscollector INFO Evaluation finished.
Feb 19, 2025 @ 09:05:03.000 wazuh-modulesd:syscollector INFO Starting evaluation.
Feb 19, 2025 @ 09:05:12.000 wazuh-modulesd:syscollector INFO Evaluation finished.
Feb 19, 2025 @ 10:05:13.000 wazuh-modulesd:syscollector INFO Starting evaluation.
Feb 19, 2025 @ 10:05:22.000 wazuh-modulesd:syscollector INFO Evaluation finished.
Feb 19, 2025 @ 11:05:23.000 wazuh-modulesd:syscollector INFO Starting evaluation.
Feb 19, 2025 @ 11:05:31.000 wazuh-modulesd:syscollector INFO Evaluation finished.
Feb 19, 2025 @ 12:05:32.000 wazuh-modulesd:syscollector INFO Starting evaluation.
Feb 19, 2025 @ 12:05:41.000 wazuh-modulesd:syscollector INFO Evaluation finished.
Feb 19, 2025 @ 13:05:42.000 wazuh-modulesd:syscollector INFO Starting evaluation.
Feb 19, 2025 @ 13:05:51.000 wazuh-modulesd:syscollector INFO Evaluation finished.
Feb 19, 2025 @ 14:05:52.000 wazuh-modulesd:syscollector INFO Starting evaluation.
Feb 19, 2025 @ 14:06:00.000 wazuh-modulesd:syscollector INFO Evaluation finished.
Feb 19, 2025 @ 15:06:01.000 wazuh-modulesd:syscollector INFO Starting evaluation.
Feb 19, 2025 @ 15:06:10.000 wazuh-modulesd:syscollector INFO Evaluation finished.
Feb 19, 2025 @ 15:54:51.000 wazuh-analysisd WARNING Mitre Technique ID 'T1565.001' not found in database.
Feb 19, 2025 @ 15:54:51.000 wazuh-analysisd WARNING Mitre Technique ID 'T1565.001' not found in database.
Feb 19, 2025 @ 16:06:11.000 wazuh-modulesd:syscollector INFO Starting evaluation.
Feb 19, 2025 @ 16:06:20.000 wazuh-modulesd:syscollector INFO Evaluation finished.
Feb 19, 2025 @ 16:15:04.000 wazuh-db INFO Created Global database backup "backup/db/global.db-backup-2025-02-19-09:15:04.gz"
Feb 19, 2025 @ 16:15:04.000 wazuh-db INFO Deleted Global database backup: "backup/db/global.db-backup-2025-02-16-09:15:04.gz"
Feb 19, 2025 @ 16:23:19.000 sca INFO Starting Security Configuration Assessment scan.
Feb 19, 2025 @ 16:23:19.000 sca INFO Skipping policy '/var/ossec/ruleset/sca/cis_ubuntu22-04.yml': 'Check Ubuntu version.'
```

Dashboard **Events** ## Jum-62 (003)

Search DQL Last 24 hours Show dates Refresh

manager.name: phu11 rule.groups: rootcheck agent.id: 003 + Add filter

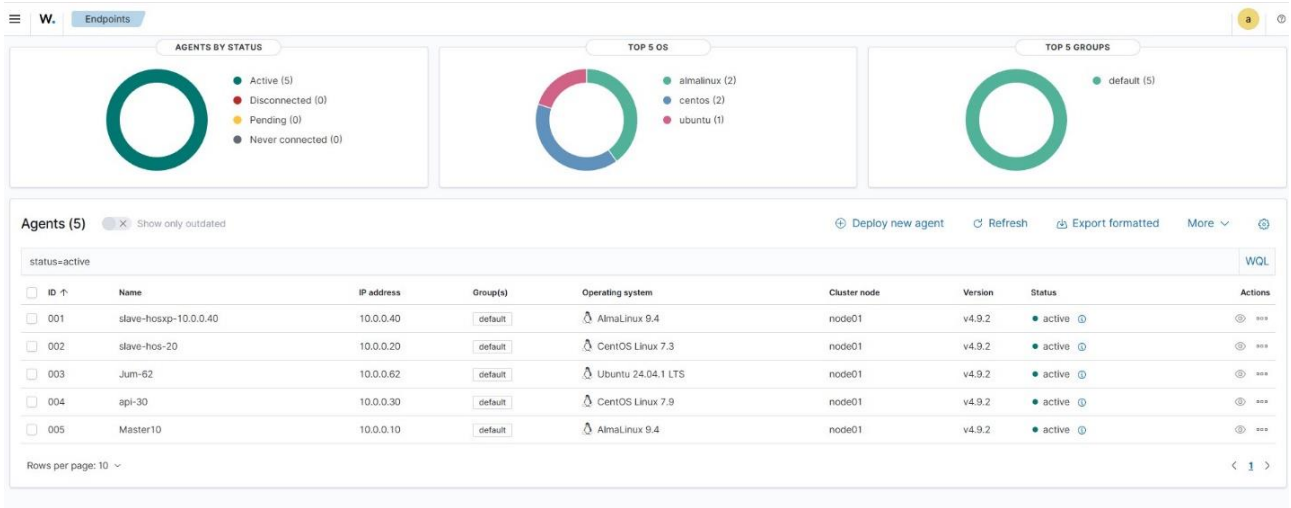
4 hits
Feb 18, 2025 @ 12:54:19.926 - Feb 19, 2025 @ 12:54:19.926

timestamp	agent.name	data.title	rule.description	rule.level	rule.id
Feb 19, 2025 @ 12:02:33.255	Jum-62	Trojanned version of file detected.	Host-based anomaly detection event (rootc...	7	510
Feb 19, 2025 @ 12:02:33.245	Jum-62	Trojanned version of file detected.	Host-based anomaly detection event (rootc...	7	510
Feb 19, 2025 @ 00:00:59.682	Jum-62	Trojanned version of file detected.	Host-based anomaly detection event (rootc...	7	510
Feb 19, 2025 @ 00:00:59.672	Jum-62	Trojanned version of file detected.	Host-based anomaly detection event (rootc...	7	510

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/ftbx64.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/{CDD5C855-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 ไปจนถึง การ Alert ระบุตำแหน่งของภัยคุกคามให้ทราบ เมื่อมี Event ที่ผิดปกติ ทำให้สามารถป้องกัน และตอบสนองภัย คุกคามได้ อย่างรวดเร็ว

- สำนักงานสาธารณสุขจังหวัดน่าน ใช้ wazuh เพื่อทำระบบ SIEM เพื่อการตรวจของ server และ ตรวจสอบถึงภัยคุกคาม 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 ที่อาจเกิดขึ้นจากการถูกโจมตีทางไซเบอร์
 - โรงพยาบาลเพียง ทำ VA เพื่อหาช่องโหว่และทำการ update patch และปิดจุดเสี่ยง ดังภาพ

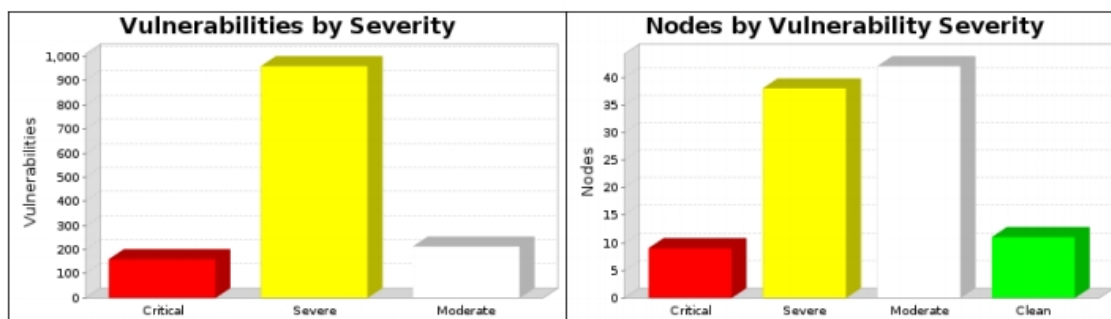
1. Executive Summary

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.

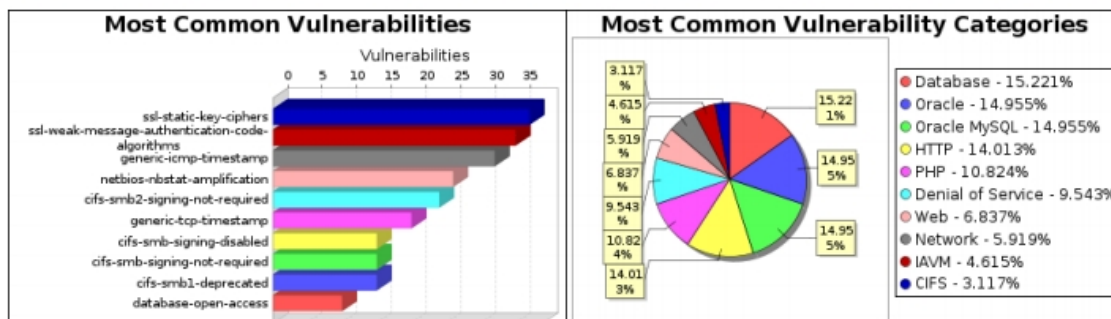
Site Name	Start Time	End Time	Total Time	Status
Phuphiang Hospital	October 03, 2024 16:53, ICT	October 03, 2024 17:22, ICT	29 minutes	Success

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.