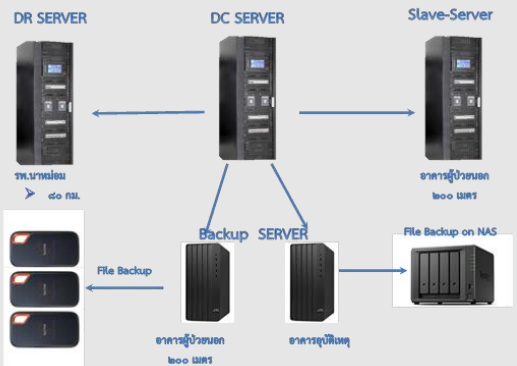
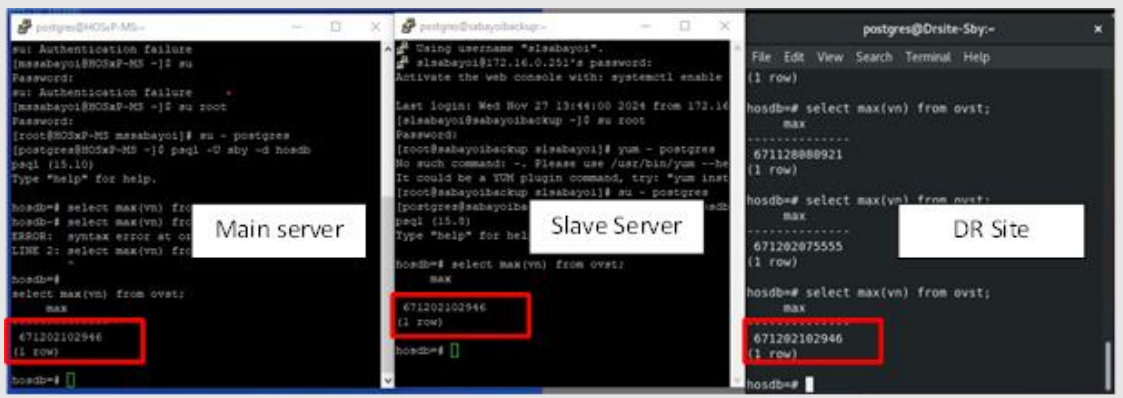
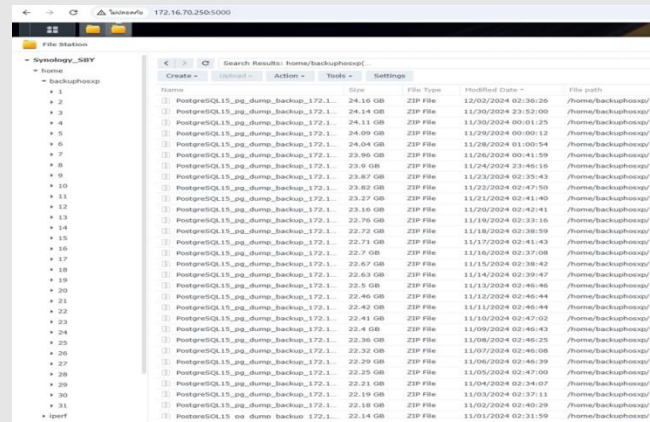


CS.3.1 มีการจัดทำแนวปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Specific information security policy) มีหัวข้อ อย่างน้อยต่อไปนี้ 1) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control) 2)การสำรองข้อมูลเพื่อให้สารสนเทศอยู่ใน สภาพพร้อมใช้งานและการจัดทำแผนเตรียมความพร้อมรับมือ ภัยคุกคาม 3) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

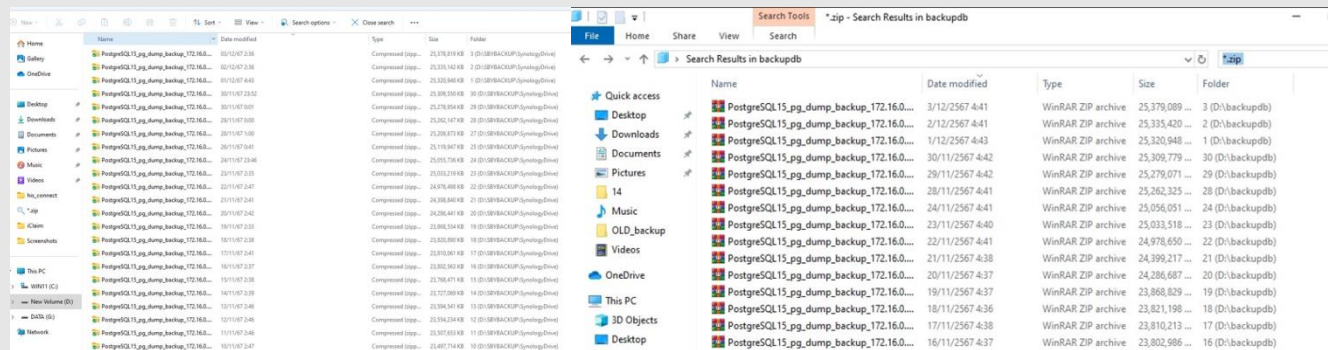
ลำดับ	หัวข้อ	ขอบเขตการดำเนินการ	การแก้ไข	ประเมิน	ผู้รับผิดชอบ
1.	Backup : การสำรองข้อมูลเก็บไว้ที่อื่น เพื่อให้สามารถใช้เพื่อกู้คืนข้อมูลเดิมหลังจากเหตุการณ์ข้อมูลสูญหาย	มีการสำรองข้อมูลอย่างน้อยวันละ 1 ครั้ง และสามารถย้อนหลังได้ 7 วัน เป็นอย่างน้อยตามมาตรฐาน โดยจัดเก็บบนระบบ Logical HDD หรือ Physical HDD และ จัดเก็บ Backup ในรูปแบบ 3-2-1 1. สำเนาข้อมูลไว้บนระบบ 3 ชุด 2. สำเนาข้อมูลไว้บนเทคโนโลยีต่างกัน 2 ชุด 3. สำเนาข้อมูลไว้แบบ Offline หรือ Offsite หรือ Cloud 1 ชุด			
หลักฐาน แผนผังการสำรองข้อมูล  1. สำเนาข้อมูลไว้บนระบบ 3 ชุด  2. สำเนาข้อมูลไว้บนเทคโนโลยีต่างกัน					

2.1 ไฟล์สำรองฐานข้อมูล HIS บน Nas



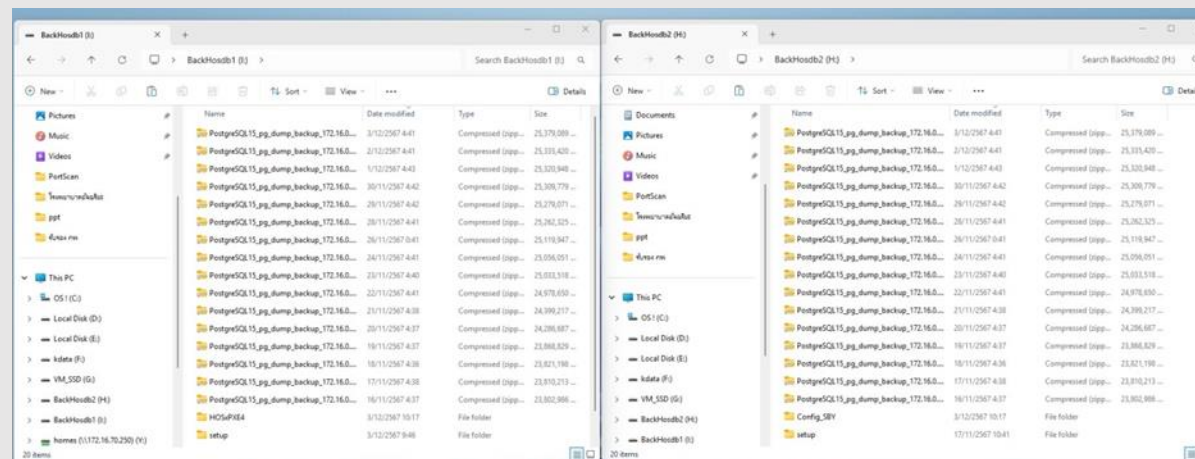
File Name	Size	File Type	Modified Date	File Path
PostgreSQL15_pg_dump_backup_172.16.70.250-0000	24.16 GB	ZIP File	12/02/2024 02:30:26	/home/backups/pgsql/2
PostgreSQL15_pg_dump_backup_172.16.70.250-0001	24.14 GB	ZIP File	11/30/2024 23:52:00	/home/backups/pgsql/30
PostgreSQL15_pg_dump_backup_172.16.70.250-0002	24.11 GB	ZIP File	11/30/2024 00:01:25	/home/backups/pgsql/29
PostgreSQL15_pg_dump_backup_172.16.70.250-0003	24.09 GB	ZIP File	11/29/2024 00:00:12	/home/backups/pgsql/28
PostgreSQL15_pg_dump_backup_172.16.70.250-0004	24.04 GB	ZIP File	11/28/2024 01:00:54	/home/backups/pgsql/27
PostgreSQL15_pg_dump_backup_172.16.70.250-0005	23.90 GB	ZIP File	11/26/2024 00:41:59	/home/backups/pgsql/25
PostgreSQL15_pg_dump_backup_172.16.70.250-0006	23.9 GB	ZIP File	11/24/2024 23:46:16	/home/backups/pgsql/24
PostgreSQL15_pg_dump_backup_172.16.70.250-0007	23.87 GB	ZIP File	11/23/2024 02:35:43	/home/backups/pgsql/23
PostgreSQL15_pg_dump_backup_172.16.70.250-0008	23.82 GB	ZIP File	11/22/2024 02:47:50	/home/backups/pgsql/22
PostgreSQL15_pg_dump_backup_172.16.70.250-0009	23.72 GB	ZIP File	11/21/2024 02:41:40	/home/backups/pgsql/21
PostgreSQL15_pg_dump_backup_172.16.70.250-0010	23.16 GB	ZIP File	11/20/2024 02:42:41	/home/backups/pgsql/20
PostgreSQL15_pg_dump_backup_172.16.70.250-0011	22.76 GB	ZIP File	11/19/2024 02:33:16	/home/backups/pgsql/19
PostgreSQL15_pg_dump_backup_172.16.70.250-0012	22.72 GB	ZIP File	11/18/2024 02:38:59	/home/backups/pgsql/18
PostgreSQL15_pg_dump_backup_172.16.70.250-0013	22.71 GB	ZIP File	11/17/2024 02:41:43	/home/backups/pgsql/17
PostgreSQL15_pg_dump_backup_172.16.70.250-0014	22.7 GB	ZIP File	11/16/2024 02:37:08	/home/backups/pgsql/16
PostgreSQL15_pg_dump_backup_172.16.70.250-0015	22.46 GB	ZIP File	11/15/2024 02:38:42	/home/backups/pgsql/15
PostgreSQL15_pg_dump_backup_172.16.70.250-0016	22.63 GB	ZIP File	11/14/2024 02:39:47	/home/backups/pgsql/14
PostgreSQL15_pg_dump_backup_172.16.70.250-0017	22.5 GB	ZIP File	11/13/2024 02:46:46	/home/backups/pgsql/13
PostgreSQL15_pg_dump_backup_172.16.70.250-0018	22.46 GB	ZIP File	11/12/2024 02:46:44	/home/backups/pgsql/12
PostgreSQL15_pg_dump_backup_172.16.70.250-0019	22.42 GB	ZIP File	11/12/2024 02:46:44	/home/backups/pgsql/11
PostgreSQL15_pg_dump_backup_172.16.70.250-0020	22.41 GB	ZIP File	11/10/2024 02:47:02	/home/backups/pgsql/10
PostgreSQL15_pg_dump_backup_172.16.70.250-0021	22.4 GB	ZIP File	11/09/2024 02:46:43	/home/backups/pgsql/9
PostgreSQL15_pg_dump_backup_172.16.70.250-0022	22.36 GB	ZIP File	11/08/2024 02:46:25	/home/backups/pgsql/8
PostgreSQL15_pg_dump_backup_172.16.70.250-0023	22.32 GB	ZIP File	11/07/2024 02:46:08	/home/backups/pgsql/7
PostgreSQL15_pg_dump_backup_172.16.70.250-0024	22.29 GB	ZIP File	11/06/2024 02:46:39	/home/backups/pgsql/6
PostgreSQL15_pg_dump_backup_172.16.70.250-0025	22.25 GB	ZIP File	11/05/2024 02:47:00	/home/backups/pgsql/5
PostgreSQL15_pg_dump_backup_172.16.70.250-0026	22.21 GB	ZIP File	11/04/2024 02:34:07	/home/backups/pgsql/4
PostgreSQL15_pg_dump_backup_172.16.70.250-0027	22.19 GB	ZIP File	11/03/2024 02:37:11	/home/backups/pgsql/3
PostgreSQL15_pg_dump_backup_172.16.70.250-0028	22.18 GB	ZIP File	11/02/2024 02:40:29	/home/backups/pgsql/2
PostgreSQL15_pg_dump_backup_172.16.70.250-0029	22.14 GB	ZIP File	11/01/2024 02:31:59	/home/backups/pgsql/1

2.2 ไฟล์สำรองฐานข้อมูล HIS บน PC 1 อาคารอุบัติเหตุ, ไฟล์สำรองฐานข้อมูล HIS บน PC 1 อาคารผู้ป่วยนอก



Name	Date modified	Type	Size	Folder
PostgreSQL15_pg_dump_backup_172.16.70.250-0000	3/12/2567 4:41	WinRAR ZIP archive	25,379,089	3 (D:\backups)
PostgreSQL15_pg_dump_backup_172.16.70.250-0001	2/12/2567 4:41	WinRAR ZIP archive	25,335,420	2 (D:\backups)
PostgreSQL15_pg_dump_backup_172.16.70.250-0002	1/12/2567 4:43	WinRAR ZIP archive	25,320,948	1 (D:\backups)
PostgreSQL15_pg_dump_backup_172.16.70.250-0003	30/11/2567 4:42	WinRAR ZIP archive	25,309,779	30 (D:\backups)
PostgreSQL15_pg_dump_backup_172.16.70.250-0004	29/11/2567 4:42	WinRAR ZIP archive	25,279,071	29 (D:\backups)
PostgreSQL15_pg_dump_backup_172.16.70.250-0005	28/11/2567 4:41	WinRAR ZIP archive	25,262,325	28 (D:\backups)
PostgreSQL15_pg_dump_backup_172.16.70.250-0006	24/11/2567 4:41	WinRAR ZIP archive	25,056,051	24 (D:\backups)
PostgreSQL15_pg_dump_backup_172.16.70.250-0007	23/11/2567 4:40	WinRAR ZIP archive	25,033,518	23 (D:\backups)
PostgreSQL15_pg_dump_backup_172.16.70.250-0008	22/11/2567 4:41	WinRAR ZIP archive	24,978,650	22 (D:\backups)
PostgreSQL15_pg_dump_backup_172.16.70.250-0009	21/11/2567 4:38	WinRAR ZIP archive	24,999,217	21 (D:\backups)
PostgreSQL15_pg_dump_backup_172.16.70.250-0010	20/11/2567 4:37	WinRAR ZIP archive	24,286,687	20 (D:\backups)
PostgreSQL15_pg_dump_backup_172.16.70.250-0011	19/11/2567 4:37	WinRAR ZIP archive	23,868,829	19 (D:\backups)
PostgreSQL15_pg_dump_backup_172.16.70.250-0012	18/11/2567 4:36	WinRAR ZIP archive	23,821,198	18 (D:\backups)
PostgreSQL15_pg_dump_backup_172.16.70.250-0013	17/11/2567 4:38	WinRAR ZIP archive	23,810,213	17 (D:\backups)
PostgreSQL15_pg_dump_backup_172.16.70.250-0014	16/11/2567 4:37	WinRAR ZIP archive	23,802,986	16 (D:\backups)

2.3 ไฟล์สำรองฐานข้อมูล HIS บน External Hard Disk



Name	Date modified	Type	Size
PostgreSQL15_pg_dump_backup_172.16.70.250-0000	3/12/2567 4:41	Compressed (zipped) file	25,379,089
PostgreSQL15_pg_dump_backup_172.16.70.250-0001	2/12/2567 4:41	Compressed (zipped) file	25,335,420
PostgreSQL15_pg_dump_backup_172.16.70.250-0002	1/12/2567 4:43	Compressed (zipped) file	25,320,948
PostgreSQL15_pg_dump_backup_172.16.70.250-0003	30/11/2567 4:42	Compressed (zipped) file	25,309,779
PostgreSQL15_pg_dump_backup_172.16.70.250-0004	29/11/2567 4:42	Compressed (zipped) file	25,279,071
PostgreSQL15_pg_dump_backup_172.16.70.250-0005	28/11/2567 4:41	Compressed (zipped) file	25,262,325
PostgreSQL15_pg_dump_backup_172.16.70.250-0006	24/11/2567 4:41	Compressed (zipped) file	25,119,947
PostgreSQL15_pg_dump_backup_172.16.70.250-0007	23/11/2567 4:41	Compressed (zipped) file	25,056,051
PostgreSQL15_pg_dump_backup_172.16.70.250-0008	22/11/2567 4:41	Compressed (zipped) file	25,033,518
PostgreSQL15_pg_dump_backup_172.16.70.250-0009	21/11/2567 4:38	Compressed (zipped) file	24,978,650
PostgreSQL15_pg_dump_backup_172.16.70.250-0010	20/11/2567 4:37	Compressed (zipped) file	24,999,217
PostgreSQL15_pg_dump_backup_172.16.70.250-0011	19/11/2567 4:37	Compressed (zipped) file	24,286,687
PostgreSQL15_pg_dump_backup_172.16.70.250-0012	18/11/2567 4:36	Compressed (zipped) file	23,868,829
PostgreSQL15_pg_dump_backup_172.16.70.250-0013	17/11/2567 4:38	Compressed (zipped) file	23,821,198
PostgreSQL15_pg_dump_backup_172.16.70.250-0014	16/11/2567 4:37	Compressed (zipped) file	23,810,213

3. สำเนาข้อมูลไว้แบบ Offline หรือ Offsite หรือ Cloud 1 ชุด

ข้อมูล DR Site Server ตั้งอยู่ที่	รพ.นาหม่อม ระยะทาง 81 กิโลเมตร การ Sync ข้อมูลผ่านระบบ VPN
-----------------------------------	--

2. **Antivirus Software**
: โปรแกรมป้องกันไวรัส หรือ แอนติไวรัส คอยตรวจจับ ป้องกัน และกำจัดโปรแกรม
คุกคามทางคอมพิวเตอร์หรือมัลแวร์

มีการติดตั้ง Anti-Virus หรือ EDR หรือ XDR บนเครื่องอุปกรณ์ที่สำคัญ

1. Review Alert Report
2. Update Program Anti-Virus, EDR/XER
3. Schedule Update Database Signature

หลักฐาน

SOPHOS

Dashboards

My Products

Threat Analysis Center

Alerts

Reports

People

Devices

Computers and servers

View and manage your computers and servers

Delete

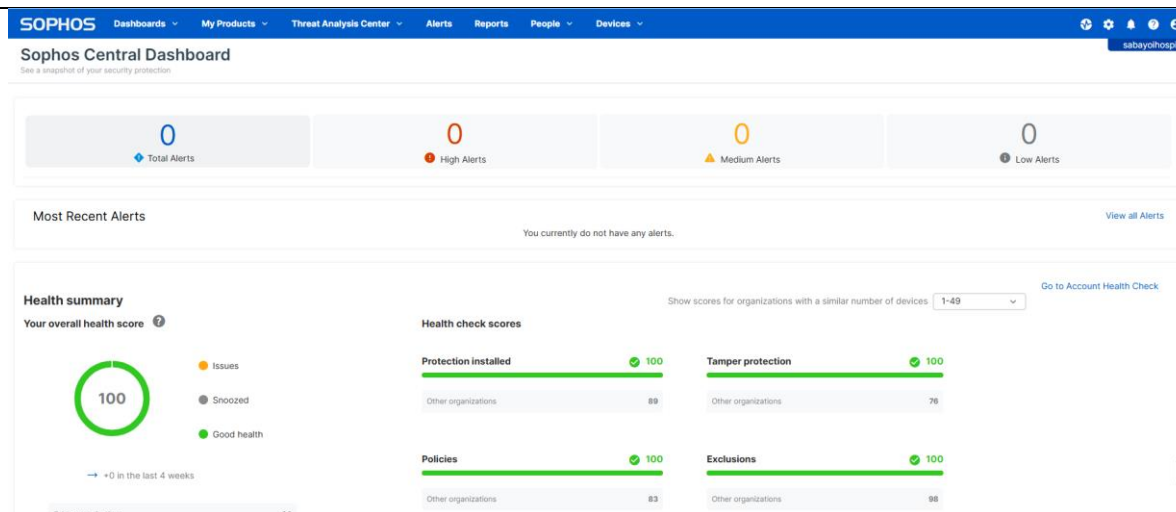
Manage software

Edit tamper protection

Reset health status

Retrieve recovery key

☐		Name	Type	Operating System	Last active	IP address	Tamper protecti...	Last user	Protection
☐		Drsite-Sby		AlmaLinux 8.10 (...)	Online	192.168.1.50 ...	Not applicable		XDR
☐		BackupXe		AlmaLinux 8.10 (...)	Online	192.168.122.1 ...	Not applicable		XDR
☐		BMS-Restore		AlmaLinux 8.10 (...)	Online	192.168.122.1 ...	Not applicable		XDR
☐		sabayolbackup		AlmaLinux 8.10 (...)	Online	192.168.122.1 ...	Not applicable		XDR
☐		serverPCU		Windows Server...	Online	172.16.0.248 ...	On		XDR
☐		HOSxP-MS		AlmaLinux 8.8 (...)	Online	192.168.122.1 ...	Not applicable		XDR
☐		HOSxP-SL		AlmaLinux 8.8 (...)	Online	192.168.122.1 ...	Not applicable		XDR



3.	Access Control (Public และ Private) : การควบคุมอุปกรณ์หรือการเข้าถึงระบบผ่านทางช่องทาง Public/Private ทั้งภายใน ประเทศ และ ต่างประเทศ	มีการควบคุม Policy การเข้าถึงระบบที่สำคัญทั้งทาง Public และ Private 1. มีการควบคุมการเข้าถึงห้องเครื่องคอมพิวเตอร์แม่ข่าย 2. IP Address Filter กำหนดขอบเขตการใช้งาน IP Address ที่สามารถเข้าใช้งานในระบบได้ เช่น IP Location, Geometric 3. ดำเนินการกำหนด White list Port และไม่เปิด Port ที่มีความเสี่ยงต่อการโดนโจมตี ดี ปัจจุบันได้แก่ 7, 19, 20, 21, 22, 23, 25, 37, 53, 69, 79, 80, 110, 111, 135, 137, 138, 139, 445, 161, 443, 512, 513, 514, 1433, 1434, 1723, 3389, 8080 (หากมีความจำเป็นในการเปิดจะต้องทำการกำหนด Source และ Destination ให้ชัดเจน) 4. มีการแบ่งโซน Network ระหว่างอุปกรณ์แม่ข่าย (Server) และอุปกรณ์ลูกข่าย 5. มีการใช้งาน VPN ในการเข้าถึงอุปกรณ์แม่ข่าย (Server) แทนการใช้งานผ่าน Public 6. User Access Accounts กำหนดสิทธิการใช้งานเท่าที่จำเป็น เช่น Role Base / Group Base 7. User Password Policy กำหนดการใช้งานพาสเวิร์ด เช่น กำหนดความยาวอย่างน้อย 12 ตัวอักษร, Hash MD5, SHA-256 8. Time Sync			
----	---	---	--	--	--

หลักฐาน

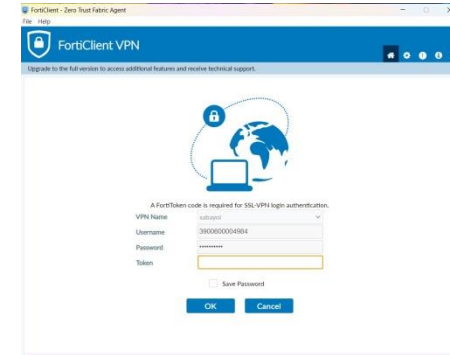
3.1 การควบคุมการเข้าถึงห้องเครื่องคอมพิวเตอร์แม่ข่าย



สแกนลายนิ้วมือ



กล้องวงจรปิด



การเข้าถึง Network

3.2. IP Address Filter กำหนดขอบเขตการใช้งาน IP Address ที่สามารถใช้งานในระบบได้ เช่น IP Location, Geometric

Name	From	To	Source	Destinat...	Schedule	Service	Action
Block_country90	Sabayoi-SD-WAN_Zone	Vlan 90	China Russia Nigeria Romania Ukraine	all	always	ALL	DENY
Block_contry800	Sabayoi-SD-WAN_Zone	Vlan 800	China Russia Nigeria Romania Ukraine	all	always	ALL	DENY
Block_contry700	Sabayoi-SD-WAN_Zone	Vlan 700	China Russia Nigeria Romania Ukraine	all	always	ALL	DENY

Geometric

BlockBit

Comments: webbit 6/255

Categories

- Business (157, 11)
- Email (76, 11)
- Mobile (3)
- Proxy (188)
- Storage.Backup (152, 20)
- VoIP (23)
- Cloud.IT (73, 12)
- Game (83)
- Network.Service (338)
- RemoteAccess (96)
- Update (48)
- Web.Client (24)
- Collaboration (265, 13)
- GeneralInterest (254, 15)
- P2P (55)
- Social.Media (113, 29)
- Video.Audio (149, 16)
- Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

Priority	Details	Type	Action
1	BitTorrent Resilio Bitcoin Bitcomet/HTTPSeed	Application	Block

App filter

Edit Web Filter Profile

Name: default

Comments: Default web filtering. 22/255

Feature set: Flow-based Proxy-based

FortiGuard Category Based Filter

Allow users to override blocked categories

Static URL Filter

Block invalid URLs

URL Filter

URL	Type	Action	Status
www.lazada.co.th	Simple	Block	Enable
lazada.	Wildcard	Block	Enable
shopee.	Wildcard	Block	Enable
www.pantipmarket.com	Simple	Block	Enable
www.komvy.com	Simple	Block	Enable
www.kaldee.com	Simple	Block	Enable
www.tarad.com	Simple	Block	Enable
www.cmart.co.th	Simple	Block	Enable
www.kingpower.com	Simple	Block	Enable

Block malicious URLs discovered by FortiSandbox

Content Filter

WEB filter

Allow 100 NAT	Vlan 100	Sabayoi-SD-WAN_Zone	Academic_group Admin_group Dental_group Doctor_group Nurse_group Pharmacy_group User-Authen all	all	always	ALL	ACCEPT	Enabled	default DNSblockweb BlockBit default certificate-inspection
Allow 200 NAT	Vlan 200	Sabayoi-SD-WAN_Zone	Academic_group Admin_group Dental_group Doctor_group Nurse_group Pharmacy_group User-Authen all	all	always	ALL	ACCEPT	Enabled	default DNSblockweb BlockBit default certificate-inspection
Allow 300 NAT	Vlan 300	Sabayoi-SD-WAN_Zone	Academic_group Admin_group Dental_group Doctor_group Nurse_group Pharmacy_group User-Authen all	all	always	ALL	ACCEPT	Enabled	default DNSblockweb BlockBit default certificate-inspection

DNS filter

Name: DNSblockweb

Comments: Default dns filtering. 22/255

Redirect botnet C&C requests to Block Portal

Enforce 'Safe Search' on Google, Bing, YouTube

FortiGuard Category Based Filter

Static Domain Filter

Domain Filter

Domain	Type	Action	Status
lazada.	wildcard	Redirect to Block Portal	Enable
fn328.	wildcard	Redirect to Block Portal	Enable
w88top.	wildcard	Redirect to Block Portal	Enable
bk8thalfan.	wildcard	Redirect to Block Portal	Enable
hthai888.	wildcard	Redirect to Block Portal	Enable
jbo089.	wildcard	Redirect to Block Portal	Enable
dafapromo.	wildcard	Redirect to Block Portal	Enable
ms8got.	wildcard	Redirect to Block Portal	Enable
huc99.	wildcard	Redirect to Block Portal	Enable

3.3 ดำเนินการกำหนด White list Port และไม่เปิด Port ที่ ี่มี มีความเสี่ยงต่อการโดนโจมตี

```
C:\>C:\WINDOWS\system32\cmd. x + v
C:\> nmap -p- 172.16.0.1
Starting Nmap 7.94 ( https://nmap.org ) at 2024-11-05 14:54 SE Asia Standard Time
Nmap scan report for 172.16.0.2
Host is up (0.00081s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE
111/tcp   open  rpcbind
2231/tcp  open  wimaxisncp
5432/tcp  open  postgresql
6432/tcp  open  pgbouncer

Nmap done: 1 IP address (1 host up) scanned in 17.15 seconds

C:\> nmap -p- 172.16.0.1
Starting Nmap 7.94 ( https://nmap.org ) at 2024-11-05 14:55 SE Asia Standard Time
Nmap scan report for 172.16.0.1
Host is up (0.00056s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE
111/tcp   open  rpcbind
2231/tcp  open  wimaxisncp
5432/tcp  open  postgresql
6432/tcp  open  pgbouncer

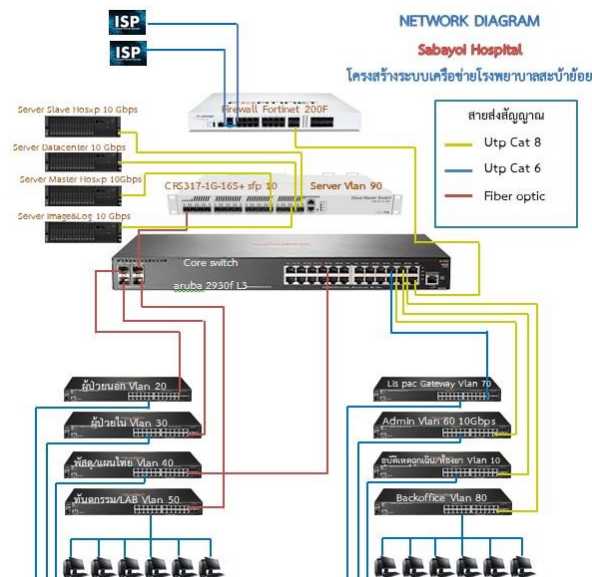
Nmap done: 1 IP address (1 host up) scanned in 17.83 seconds

C:\> nmap -p- 172.16.0.1
Starting Nmap 7.94 ( https://nmap.org ) at 2024-11-05 14:55 SE Asia Standard Time
Nmap scan report for 172.16.0.1
Host is up (0.000936s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
111/tcp   open  rpcbind
2231/tcp  open  wimaxisncp
5432/tcp  open  postgresql

Nmap done: 1 IP address (1 host up) scanned in 16.91 seconds
```

[illegible]

3.4 มีการแบ่งโซน Network ระหว่างอุปกรณ์แม่ข่าย (Server) และอุปกรณ์ลูกข่าย



<https://172.16.60.254:8443/interface>

Create New

Edit

Delete

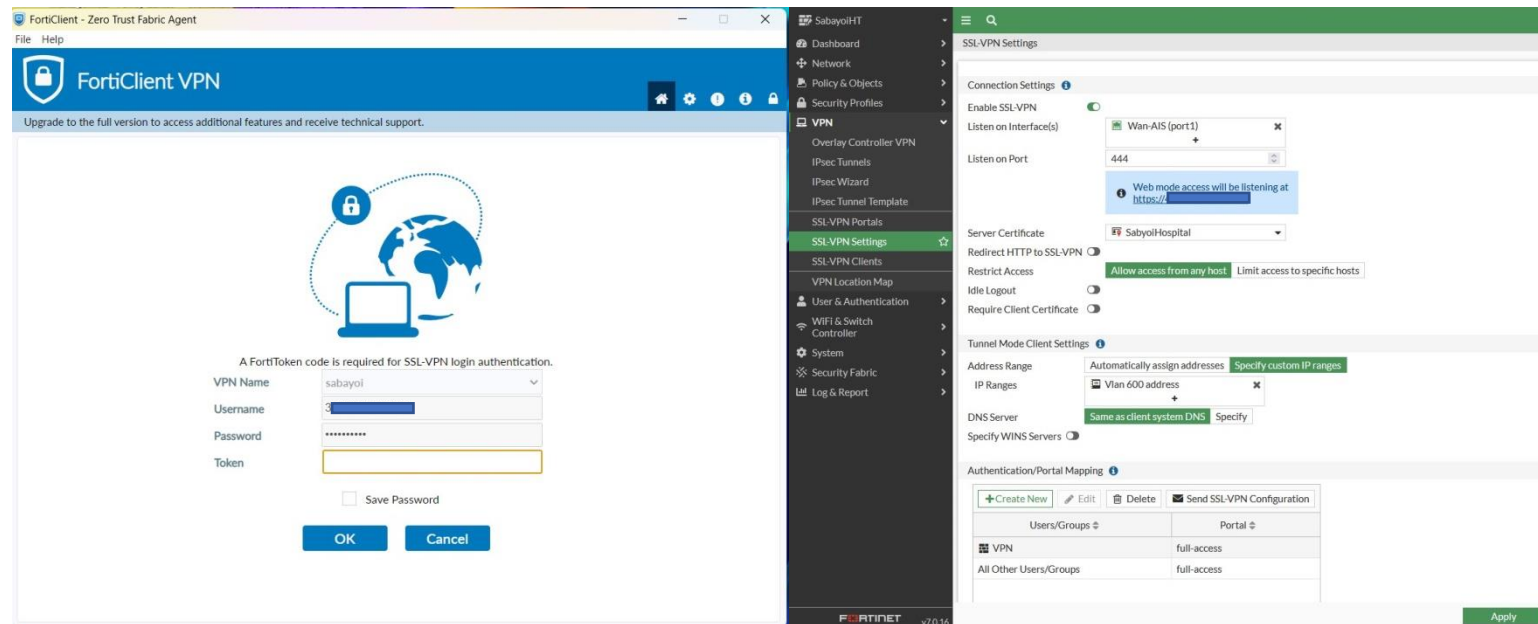
Integrate Interface

Search

Group By Type

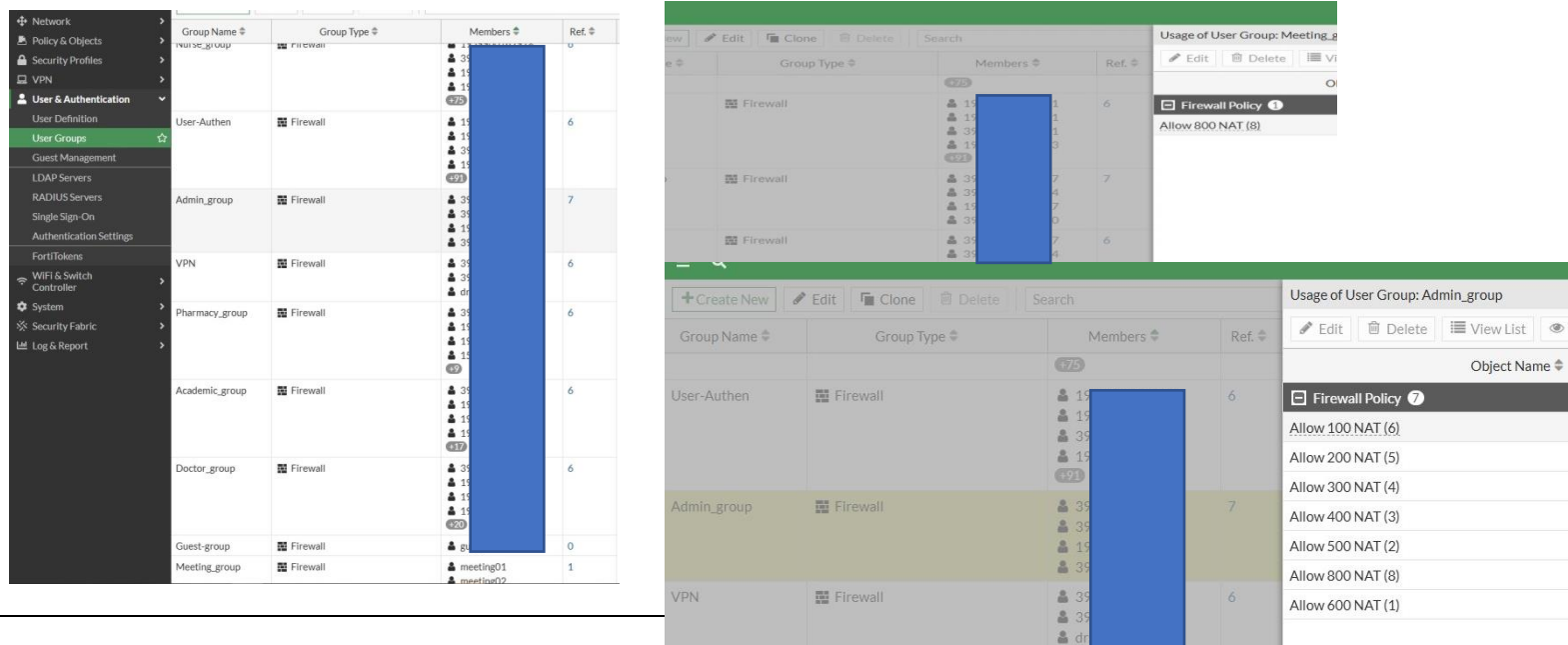
Name	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
Vlan 90	VLAN		172.16.0.1/255.255.252.0		PING HTTPS SSH HTTP	2	172.16.0.2-172.16.3.254	29
Vlan 100	VLAN		172.16.10.254/255.255.255.0		PING	28	172.16.10.2-172.16.10.254	21
Vlan 200	VLAN		172.16.20.254/255.255.255.0		PING	22	172.16.20.2-172.16.20.254	18
Vlan 300	VLAN		172.16.30.254/255.255.255.0		PING	20	172.16.30.2-172.16.30.254	12
Vlan 400	VLAN		172.16.40.254/255.255.255.0		PING	12	172.16.40.2-172.16.40.254	8
Vlan 500	VLAN		172.16.50.254/255.255.255.0		PING	26	172.16.50.2-172.16.50.254	18
Vlan 600	VLAN		172.16.60.254/255.255.255.0		PING HTTPS Security Fabric Connection	3	172.16.60.2-172.16.60.254	30
Vlan 700	VLAN		172.16.70.254/255.255.255.0		PING	1	172.16.70.2-172.16.70.254	23
Vlan 800	VLAN		172.16.80.254/255.255.255.0		PING	24	172.16.80.2-172.16.80.254	12

3.5 มีการใช้งาน VPN ในการเข้าถึงอุปกรณ์แม่ข่าย (Server) แทนการใช้งานผ่าน Public



การใช้งาน VPN to factor authentication

3.6 User Access Accounts กำหนดสิทธิการใช้งานเท่าที่จำเป็น เช่น Role Base / Group Base



3.7 User Password Policy กำหนดการใช้งานพาสเวิร์ด เช่น กำหนดความยาวอย่างน้อย 12 ตัวอักษร, Hash MD5, SHA-256

Username

User Account Status ↑ Enabled ↓ Disabled

User Type Local User

Password

User Group ☒ Admin_group ☒ VPN +

☒ Two-factor Authentication

Authentication Type FortiToken Cloud FortiToken

Token

Email Address

Username

User Account Status ↑ Enabled ↓ Disabled

User Type Local User

Password

User Group ☒ Academic_group +

3.8 Time Sync

```
mssabayoi@HOSxP-MS:/home/mssabayoi
Using username "mssabayoi".
mssabayoi@172.16.0.250's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Fri Dec 6 11:01:55 2024 from 172.16.60.4
[mssabayoi@HOSxP-MS ~]$ su root
Password:
[root@HOSxP-MS mssabayoi]# sudo systemctl status chronyd
● chronyd.service - NTP client/server
   Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled; vendor pre
   Active: active (running) since Tue 2024-12-03 13:45:10 +07; 2 days ago
     Docs: man:chronyd(8)
           man:chrony.conf(5)
   Main PID: 681945 (chronyd)
      Tasks: 1 (limit: 1644954)
     Memory: 920.0K
    CGroup: /system.slice/chronyd.service
            └─681945 /usr/sbin/chronyd

Warning: Journal has been rotated since unit was started. Log output is incomplete
lines 1-12/12 (END)
```

```
dcsabayoi@BMS-Restore:/home/dcsabayoi
sudo: systemctl: command not found
[root@BMS-Restore dcsabayoi]# sudo systemctl status chronyd
● chronyd.service - NTP client/server
   Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled; vendor pre
   Active: active (running) since Mon 2024-11-25 08:30:00 +07; 1 weeks 4 days ap
     Docs: man:chronyd(8)
           man:chrony.conf(5)
   Main PID: 3159830 (chronyd)
      Tasks: 1 (limit: 1232091)
     Memory: 988.0K
    CGroup: /system.slice/chronyd.service
            └─3159830 /usr/sbin/chronyd

Nov 25 08:30:00 BMS-Restore chronyd[3159830]: Frequency 15.465 +/- 0.036 ppm re
Nov 25 08:30:00 BMS-Restore chronyd[3159830]: Using right/UTC timezone to obtai
Nov 25 08:30:00 BMS-Restore systemd[1]: Started NTP client/server.
Nov 25 08:32:40 BMS-Restore chronyd[3159830]: Selected source 203.185.67.115 (c
Nov 25 08:32:40 BMS-Restore chronyd[3159830]: System clock wrong by 262.945661
Nov 25 08:37:03 BMS-Restore chronyd[3159830]: System clock was stepped by 262.9
Nov 25 08:37:03 BMS-Restore chronyd[3159830]: System clock TAI offset set to 37
Nov 25 09:19:44 BMS-Restore chronyd[3159830]: Selected source 164.115.133.40 (t
Nov 26 16:34:17 BMS-Restore chronyd[3159830]: Selected source 164.115.133.41 (t
Nov 29 18:11:07 BMS-Restore chronyd[3159830]: Selected source 164.115.133.40 (t
lines 1-21/21 (END)
```


4.	Privileged Access Management (PAM) : โซลูชันการรักษาความปลอดภัยของข้อมูลประจำตัวที่ช่วยปกป้ององค์กรจากภัยคุกคามทางไซเบอร์ด้วยการติดตาม ตรวจสอบ และป้องกัน การใช้สิทธิ์การเข้าถึงทรัพยากรที่สำคัญในระดับสูง	มีการควบคุมการเข้าถึงระบบโดยใช้งานสิทธิ์ระดับ Least Privilege ดังนี้ 1. ดำเนินการ Disable Administrator / Root / Admin 2. มีการกำหนด Role-base access ในการเข้าถึงระบบเท่าที่มีจำเป็น 3. มีการตั้ง Password อย่างน้อย 12 ตัว (ตัวอักษรใหญ่, เล็ก, อักขระพิเศษ, ตัวเลข) 12, มีการเข้ารหัส Password MD5,SHA-256 4. Expire Sessions Time out			
----	---	---	--	--	--

หลักฐาน

4.1 ดำเนินการ Disable Administrator / Root / Admin

```

GNU nano 2.9.8
$OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 2231
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# This system is following system-wide crypto policy. The changes to
# crypto properties (Ciphers, MACs, ...) will not have any effect here.
# They will be overridden by command-line options passed to the server
# on command line.
# Please, check manual pages for update-crypto-policies(8) and sshd_config(5).

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

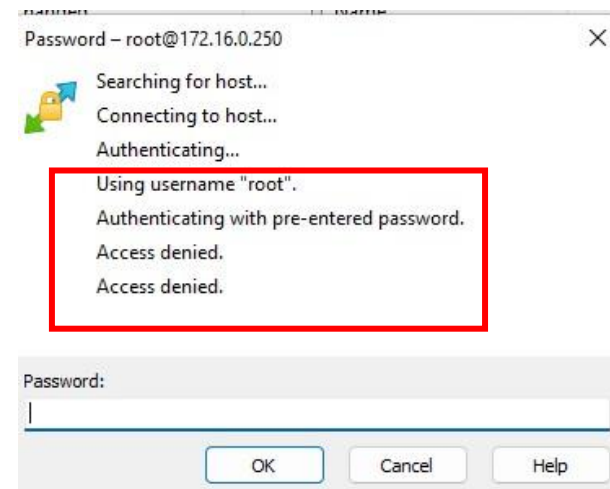
# Authentication:
#
#loganoticeTime 30m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

```

```

slsabayoi@sabayoibackup:~
Last login: Wed Nov  6 13:59:50 2024 from 172.16.60.4
[salsabayoi@sabayoibackup ~]$ cat /etc/passwd
#root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown

```



4.2 มีการกำหนด Role-base access ในการเข้าถึงระบบเท่าที่มีจำเป็น

Group Manager			
Filter			
ค้นหา แสดง Excel Export			
ลำดับ	รหัสกลุ่ม	ชื่อกลุ่ม	จำนวน User
1	OPD	User : OPD พยาบาล	85
2	REFER	User : REFER ศูนย์ส่งต่อ	68
3	IPD	User : IPD พยาบาล	66
4	FINANCE	User : FN การเงิน	63
5	ER	User : ER ห้องฉุกเฉิน	33
6	DOCTOR	User : DOCTOR ห้องตรวจแพทย์	29
7	IPD	User : IPD LR ห้องคลอด	26
8	LAB	User : LAB ห้องปฏิบัติการ	19
9	OPD	User : ผู้ช่วยเภสัชกร	17
10	SUPER USER	Super User : ผู้ดูแลระบบ (ADMIN)	17
11	CARD	User : CARD ห้องเวชระเบียน	16
12	PCU	User : PCU พยาบาล	12
13	PT OT	User : PT กายภาพบำบัด	12
14	LAB	User : LAB - ดูข้อมูลปกติ	11
15	DENT	User : DENT ทันตแพทย์	10
16	RX	User : RX เภสัชกรรม	10
17	DENT	User : DENT เจ้าหน้าที่งานทันตสาธารณสุข	10
18	LAB	User : LAB - ดูข้อมูลปกติกลุ่ม 1 (คนไข้ HIV)	9

HOSxP User Account

ข้อมูลผู้ใช้งาน

ชื่อผู้ใช้งาน น.ส. โทรศัพท์

รหัส Login nongmuay รหัสผ่าน ***** มือถือ Fax

รหัสบุคลากร E-mail

ชื่อบุคลากรทางการแพทย์ น.ส. ☒ Auto Logout 15 นาที

☒ Active User ☐ Lab Staff Authentication Type

☐ แจ้งเตือน Login

กลุ่มผู้ใช้งาน

กลุ่มผู้ใช้งาน

ลำดับ	ชื่อกลุ่ม
> 1	User : OPD ER ผู้ช่วยเภสัชกร - (ไม่อนุมัติให้ส่ง LAB/XRAY ได้)

4.3 มีการตั้ง Password อย่างน้อย 12 ตัว (ตัวอักษรใหญ่, เล็ก, อักขระพิเศษ, ตัวเลข) 12

52	Line Token สำหรับแจ้งเตือนการส่งออกข้อมูลภายนอก	00qe4g45W3LYjixVj
53	Line Token ที่ต้องการให้ส่งเมื่อมีการรายงานผลระบาดวิท	
54	Line Token ที่ต้องการให้ส่งเมื่อมีการแก้ไข System Sett	00qe4g45W3LYjixVj
55	Line Token สำหรับแจ้งเตือน Lookup Table Change	00qe4g45W3LYjixVj
56	บังคับใช้ข้อกำหนดการกำหนดรหัสผ่าน	✓
57	อายุของรหัสผ่านจากวันที่กำหนดครั้งสุดท้าย (วัน)	60
58	ความยาวต่ำสุดของรหัสผ่าน	12
59	บังคับรหัสผ่านต้องมีตัวอักษรพิมพ์ใหญ่และพิมพ์เล็ก	✓
> 60	รหัสผ่านที่กำหนดใหม่ห้ามซ้ำกับรหัสผ่านเดิม	✓

HOSxPUserPreferences

HOSxPSystemSettingMainForm - BMS-HOSxP XE 4.0 : Sby...

เปลี่ยนรหัสผ่าน

เปลี่ยนรหัสผ่าน

รหัสผ่านใหม่

รหัสผ่านใหม่

เงื่อนไขของรหัสผ่าน

มีตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก
ความยาวต้องไม่น้อยกว่า : 12
ต้องเปลี่ยนใหม่ทุก 60 วัน

HOSxPSystemSettingMainForm - BMS-HOSxP XE 4.0 : Sby...

เปลี่ยนรหัสผ่าน

เปลี่ยนรหัสผ่าน

รหัสผ่านใหม่

รหัสผ่านใหม่

เงื่อนไขของรหัสผ่าน

มีตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก
ความยาวต้องไม่น้อยกว่า : 12
ต้องเปลี่ยนใหม่ทุก 60 วัน

4.4 Expire Sessions Time out

17	ห้ามส่งตรวจผู้ป่วยหากมีเลขที่บัตรประชาชนที่ไม่ถูกต้อง	✓
18	เลขที่ Refer ไปสถานพยาบาลอื่น ออกตามปีงบประมาณ	✓
19	Lock ช่องค่านำหน้าห้ามพิมพ์เอง	✓
20	แสดงสิทธิติดตัวผู้ป่วยที่ Information Frame	✓
21	ใช้ระบบตรวจสอบสิทธิ สปสช. V2	✓
22	ระยะเวลาที่ Lock Visit เอาไว้ (นาที)	10
23	ปิดการบันทึกรหัส ICD10 ที่ Doctor workbench	

HOSxP User Account

ข้อมูลผู้ใช้งาน

ชื่อผู้ใช้งาน น. [] โทรศัพท์ []

รหัส Login nongmuay รหัสผ่าน **** มือถือ [] Fax []

รหัสนักการ [] E-mail []

ชื่อบุคลากรทางการแพทย์ น. [] ☒ Auto Logout 15 นาที Load

☒ Active User ☐ Lab Staff Authentication Type []

☐ แจ้งเตือน Login

กลุ่มผู้ใช้งาน สาขาที่ใช้งานได้ ห้องที่เข้าใช้ได้ Inventory ลายเซ็น

ลำดับ ชื่อกลุ่ม

> User : OPD ER ผู้ช่วยเหลือนักไข้ - (ไม่อนุมัติให้ส่ง LAB/XRAY ได้)

5. Business Continuity Plan (BCP) และ Disaster Recovery Plan (DRP) : แผนที่กำหนดแนวทางการ ดำเนินการของหน่วยงาน เมื่อเกิดสภาวะวิกฤตหรือภัยต่าง ๆ ที่ ส่งผลให้กระบวนการทำงานของ หน่วยงานหยุดชะงัก เพื่อให้ สามารถกลับมาดำเนินการได้อย่าง ต่อเนื่อง
- มีการทดสอบ Business Continuity Plan (BCP) และ Disaster Recovery Plan (DRP) อย่างน้อย ปีละ 1 ครั้ง และ มีการจัดทำรายงานถึง ขั้นตอนการดำเนินการที่ชัดเจนรวมถึง ระยะเวลาดำเนินการและผู้ที่เกี่ยวข้องในการดำเนินการงานดังนี้
1. การบริหารจัดการความเสี่ยง (Risk Management)
 2. การบริหารจัดการด้าน Resource (Resource Management)
 3. การวางแผนความต่อเนื่องจากธุรกิจที่เกิดขึ้น (Business Continuity Planning)
 4. การทดสอบ (Testing)

หลักฐาน

แผนแผนบริหารความต่อเนื่องในการให้บริการ (BCP)

<http://sabayoihospital.com/th/?p=4926>

แผนกู้คืนระบบสารสนเทศโรงพยาบาล (DRP)

<http://sabayoihospital.com/th/?p=4929>

การซ้อมแผน



6.	OS Patching : การซ่อมแซมจุดบกพร่องของระบบปฏิบัติการ (OS) หรือปรับปรุงระบบปฏิบัติการให้ทันสมัย และเพิ่มเติมความสามารถในการใช้งานหรือประสิทธิภาพให้ดีขึ้น	มีการอัปเดต Security Patching 1. Firewall patching (Firmware) 2. Operation patching 3. Application patching	ระบบ Window OS ผ่านแล้ว (ตรวจสอบ วันที่ update) ระบบ LINUX รอเปลี่ยน HIS	ผ่านแล้ว ✓	ลืทธิชัย
----	--	--	--	---------------	----------

หลักฐาน

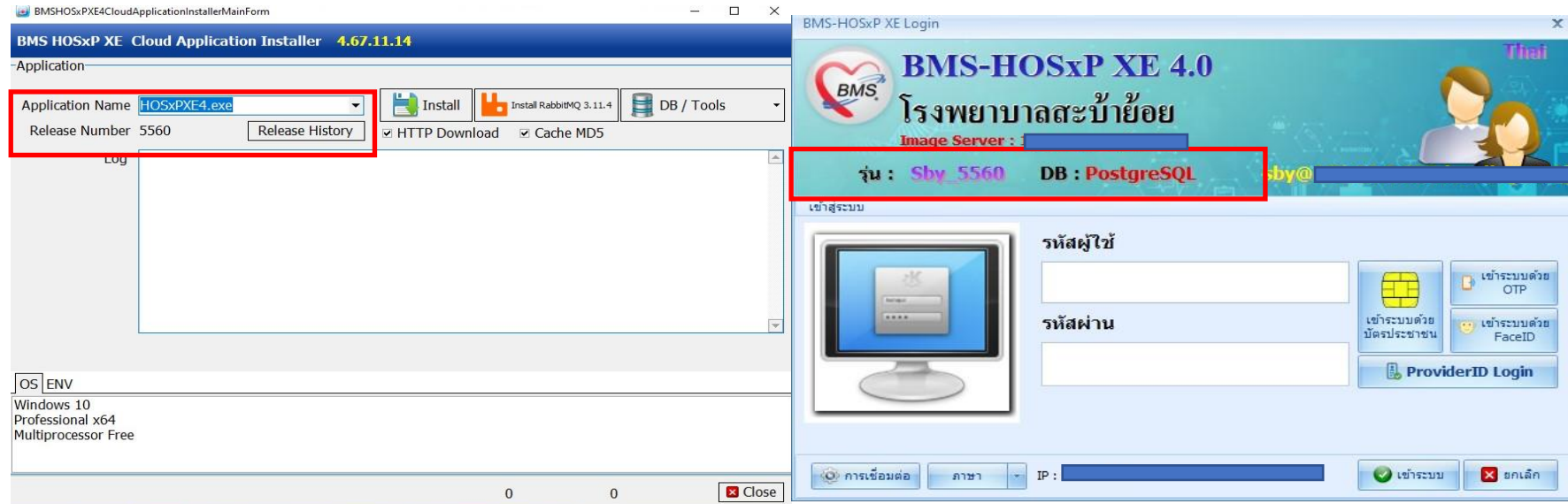
6.1 Firewall patching (Firmware)

The screenshot shows the SabayoiHT dashboard. In the 'System Information' section, the 'Firmware' is listed as 'v7.0.16 build0667 (Mature)', which is highlighted with a red box. Other system details include Hostname: SabayoiHT, Serial Number: FG20, Mode: NAT, System Time: 2024/12/09 08:07:32, Uptime: 43:02:07:43, and WAN IP: 173.243.140.6. The 'Licenses' section shows 'FortiCare Support', 'Firmware & General Updates', 'AntiVirus', and 'Web Filtering' all as active. A 'Security Rating' bar is shown at 50%. The 'FortiGate Cloud' section shows 'Status: Activated', 'Server Location: Global', 'Log Retention: Free License', and 'Storage Used: 208.90 GiB'.

6.2 Operation patching

The image contains two terminal screenshots. The left terminal, titled 'mssabayoi@HOSxP-MS:/home/mssabayoi', shows the output of 'yum update' for various packages including python3-libs, firefox, and platform-python-devel. The right terminal, titled 'dcsabayoi@BMS-Restore:/home/dcsabayoi', shows the output of 'yum update' for the BMS-Restore system. Both terminal outputs for the 'yum update' commands are highlighted with red boxes, indicating successful updates with no dependencies resolved.

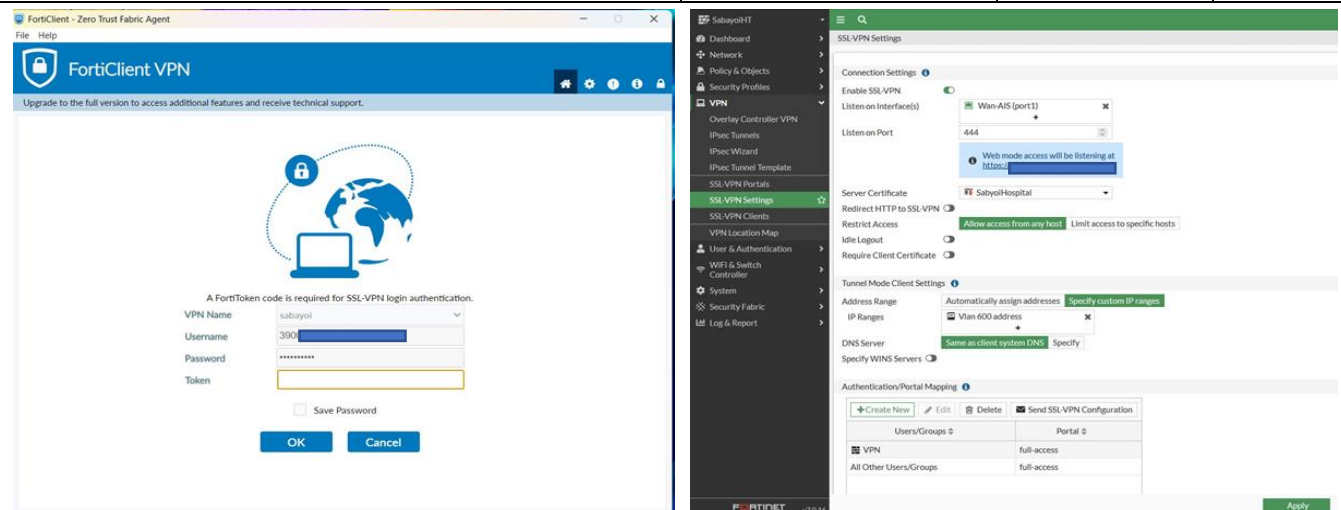
6.3 Application patching



7. Multi-Factor Authentication (2FA) : การยืนยันตัวตน 2 ชั้น เป็นการเข้าสู่ระบบบัญชีแบบหลายขั้นตอนที่กำหนดให้ผู้ใช้ป้อนข้อมูลเพิ่มเติมนอกเหนือจากรหัสผ่าน
- มีการใช้งานระบบ Multi-Factor Authentication (2FA) เพื่อยืนยันตัวตน 2 ชั้นในการเข้าถึงระบบต่างๆ สำหรับ Admin ที่ใช้งานระบบอย่างน้อยดังนี้
1. การ Login แบบ Multi-factor ไปยังระบบ VPN Access
 2. การ Login แบบ Multi-factor ไปยังอุปกรณ์ Security
 3. การ Login แบบ Multi-factor ไปยัง Operating system

หลักฐาน

7.1 การ Login แบบ Multi-factor ไปยังระบบ VPN Access



7.2 การ Login แบบ Multi-factor ไปยังอุปกรณ์ Security

The screenshot shows the FortiGate WebUI configuration page for the 'admin' user. The left sidebar lists various system settings, with 'System' and 'Administrators' expanded. The 'Edit Administrator' page shows the following configuration:

- Username:** admin
- Type:** Local User
- Comments:** Write a comment... (0/255)
- Two-factor Authentication:** Enabled
- Authentication Type:** FortiToken Cloud
- Token:** FTKMC (selected)
- Send Activation Code:** Email (selected), SMS (disabled)
- Notification:** An email with the activation code will be sent to: tawathaichatapol999@gmail.com
- Email Address:** tawathaichatapol999@gmail.com
- SMS:** Disabled

The screenshot shows the FortiGate login page. A red banner at the top says "Please input your token code." Below the banner, there are three input fields:

- Username:** admin
- Password:** (masked with dots)
- Token Code:** (empty)

A green "Login" button is at the bottom.

7.3 การ Login แบบ Multi-factor ไปยัง Operating system

The screenshot shows a PuTTY terminal window titled "172.16.0.241 - PuTTY". The terminal output is as follows:

```
login as: dcsabayoi
Keyboard-interactive authentication prompts from server:
| Password:
| Verification code: 
```

8.	Web Application Firewall (WAF) : ระบบป้องกันการโจมตีทางไซเบอร์ สำหรับเว็บแอปพลิเคชัน โดยเฉพาะ เพื่อป้องกันการโจมตีไปยังระบบเว็บ แอปพลิเคชันของ องค์กร	มีการใช้งาน Web Application Firewall (WAF) กรณีที่มีระบบเป็น Web Application เพื่อป้องกันการ โจมตีตามมาตรฐาน OWASP Top 10 ได้เป็นอย่างดีน้อยตามรายละเอียด 1. Review Attack Report 2. Add Source IP Blocklists			
----	--	--	--	--	--

หลักฐาน

Web Application Firewall (WAF)

Signatures

✎ Edit

🔍 Search

Status	Signature	Action	Severity
Disable	Cross Site Scripting	Monitor	High
Disable	Cross Site Scripting (Extended)	Monitor	High
Enable	SQL Injection	Block	High
Disable	SQL Injection (Extended)	Monitor	High
Enable	Generic Attacks	Block	High
Disable	Generic Attacks(Extended)	Monitor	High
Enable	Trojans	Block	High
Enable	Information Disclosure	Monitor	High
Enable	Known Exploits	Block	High

0% 13

✎ Edit

🔍 Search

Status	Constraint	Limit	Action	Severity
Disable	Illegal Host Name		Block	High
Disable	Illegal HTTP Version		Monitor	High
Disable	Illegal HTTP Request Method		Block	High
Enable	Content Length	67,108,864	Monitor	High
Enable	Header Length	8,192	Monitor	High
Enable	Header Line Length	1,024	Monitor	High
Enable	Number of Header Lines in Request	32	Monitor	High
Enable	Total URL and Body Parameters Length	8,192	Monitor	High
Enable	Total URL Parameters Length	8,192	Monitor	High

Name	From	To	Source	Desti...	Schedule	Serv...	Action	NAT	Security Profiles
Allow 100 NAT	Vlan 100	Sabayoi...	Academi... Admin_g... Dental_g... Doctor_g... Nurse_gr... Pharmac... User-Aut... all	all	always	ALL	✓ ACCE...	✓ Ena...	AV default WEB default DNS DNSblockweb APP BlockBit WAF default SSL certificate-in...
Allow 200 NAT	Vlan 200	Sabayoi...	Academi... Admin_g... Dental_g... Doctor_g... Nurse_gr... Pharmac... User-Aut... all	all	always	ALL	✓ ACCE...	✓ Ena...	AV default WEB default DNS DNSblockweb APP BlockBit WAF default SSL certificate-in...
Allow 300 NAT	Vlan 300	Sabayoi...	Academi... Admin_g... Dental_g... Doctor_g... Nurse_gr... Pharmac... User-Aut... all	all	always	ALL	✓ ACCE...	✓ Ena...	AV default WEB default DNS DNSblockweb APP BlockBit WAF default SSL certificate-in...
Allow 400 NAT	Vlan 400	Sabayoi...	Academi... Admin_g... Dental_g... Doctor_g... Nurse_gr... Pharmac... User-Aut... all	all	always	ALL	✓ ACCE...	✓ Ena...	AV default WEB default DNS DNSblockweb APP BlockBit WAF default SSL certificate-in...

SabayoiHT

Dashboard

Network

Policy & Objects

Firewall Policy

IPv4 Access Control List

IPv4 DoS Policy

ZTNA

Authentication Rules

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

⚙️

🔍

+ Create New

✎ Edit

📄 Clone

🗑️ Delete

🔍 Search

Name	Details	Interfaces	Ser...
IPv4 Virtual IP			
Http Web Sever	49 → 172.16.0.241 (TCP: 80-3306...)	Wan-AIS (port1)	

Network

Policy & Objects

Security Profiles

VPN

User & Authentication

WiFi & Switch Controller

System

Security Fabric

Log & Report

Forward Traffic

Local Traffic

Sniffer Traffic

ZTNA Traffic

Events

AntiVirus

Web Filter

SSL

DNS Query

File Filter

Web Application Firewall

Application Control

🔄

👤

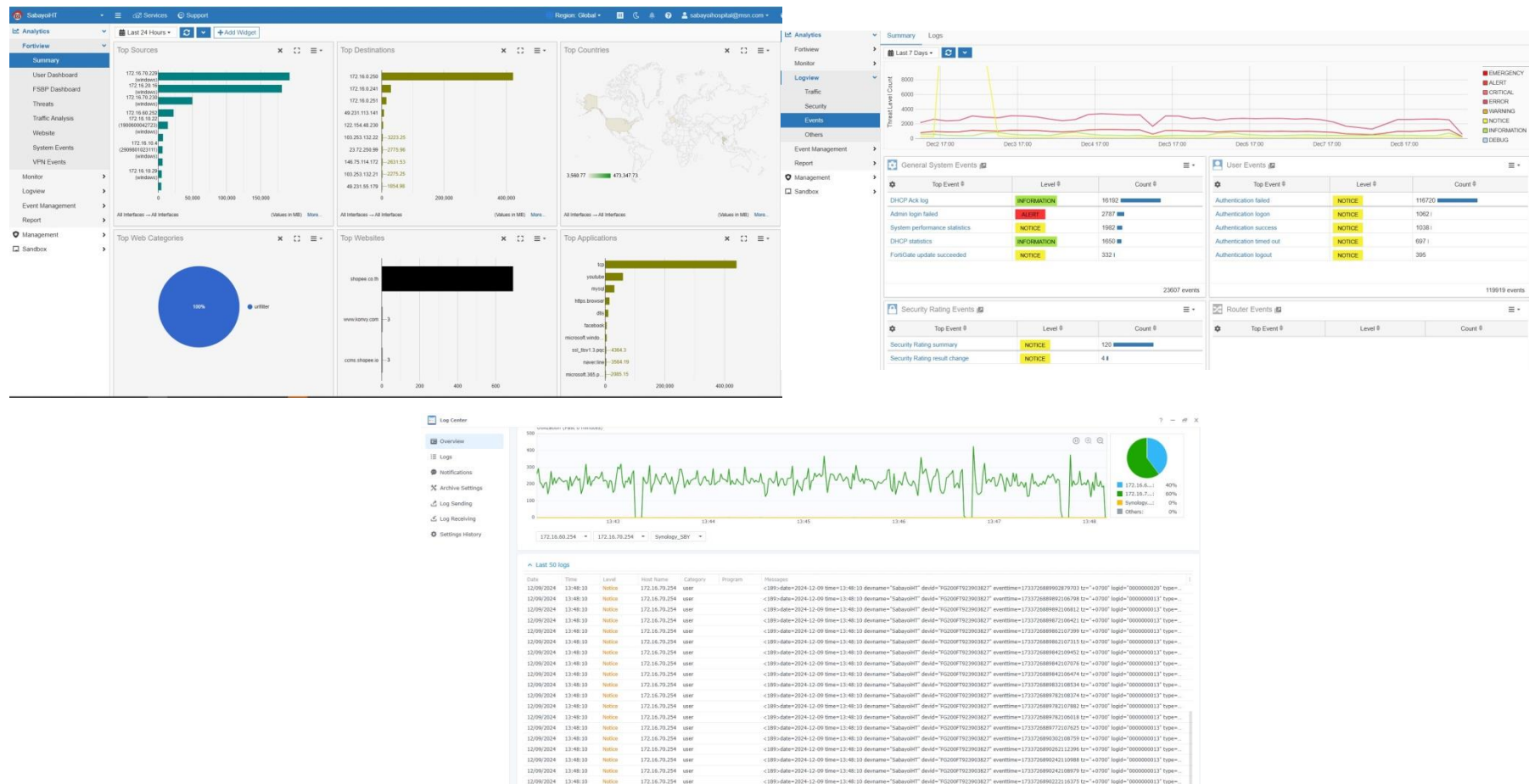
⚙️

➕ Add Filter

Date/Time	Source	Device	Destination	Application Name	Result
20 seconds ago	172.16.10.4	ER	203.157.103.53	HTTP	Deny: policy vio
20 seconds ago	172.16.10.4	ER	203.157.103.53	HTTP	Deny: policy vio
20 seconds ago	2909801023111 (172.16.20.9)	DOCTOR01	20.42.65.91 (self.events.data.microsoft.com)	Microsoft.Porta	✓ 11.89 kB / 5.94
20 seconds ago	172.16.10.4	ER	203.157.103.53	HTTP	Deny: policy vio
20 seconds ago	3901000504685 (172.16.80.8)	DESKTOP-B7PRIS9	172.217.194.91 (sb-ssl.google.com)	YouTube	✓ 29.25 kB / 13.7
21 seconds ago	149.62.45.2		49.231.200.19 (demo.sabayoihospital.com)	tcp/3031	✓
21 seconds ago	149.62.45.2		49.231.200.19 (demo.sabayoihospital.com)	tcp/3031	✓ 44 B / 0 B
21 seconds ago	172.16.10.4	ER	203.157.103.53	HTTP	Deny: policy vio
21 seconds ago	172.16.10.4	Android	157.240.7.33 (chat-e2ee-mini.facebook.com)	HTTPPS	Deny: policy vio
21 seconds ago	172.16.10.4	ER	203.157.103.53	HTTP	Deny: policy vio
21 seconds ago	172.16.10.4	ER	203.157.103.53	HTTP	Deny: policy vio
21 seconds ago	172.16.10.4	ER	203.157.103.53	HTTP	Deny: policy vio
21 seconds ago	172.16.10.4	ER	203.157.103.53	HTTP	Deny: policy vio
21 seconds ago	172.16.10.4	ER	203.157.103.53	HTTP	Deny: policy vio
21 seconds ago	172.16.70.35	WEB-G3	119.63.78.150	tcp/8081	✓
21 seconds ago	172.16.70.35	WEB-G3	119.63.78.150	tcp/8081	✓ 152 B / 0 B
21 seconds ago	172.16.10.4	ER	203.157.103.53	HTTP	Deny: policy vio
21 seconds ago	172.16.10.4	ER	203.157.103.53	HTTP	Deny: policy vio
21 seconds ago	172.16.10.4	ER	203.157.103.53	HTTP	Deny: policy vio
21 seconds ago	172.16.10.4	ER	203.157.103.53	HTTP	Deny: policy vio
21 seconds ago	172.16.10.98	Android10_98	142.251.222.234 (cloudsearch.googleapis.com)	HTTPPS	Deny: policy vio

9.	Log Management : การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์	มีระบบการจัดเก็บ Log อินเทอร์เน็ต และคอมพิวเตอร์ ตาม พ.ร.บ. คอมฯ อย่างน้อย 90 วัน 1. System Logs 2. Access Logs 3. Authentication Logs 4. Authorization Logs 5. Error Logs 6. Applications Logs	-รอกการเปิดของ เดือน ธันวาคม 2567 - โครงการศูนย์เฝ้าระวังป้องกัน และรับมือภัยคุกคามทางด้านไซเบอร์สำหรับโรงพยาบาลรัฐ (Healthcare Cyber Defense Center) - ให้บริษัท ทำระบบ DEMO 2 เดือน		
----	---	---	---	--	--

หลักฐาน



10.	Security Information & Event Management (SIEM) : ระบบที่ใช้ในการจัดการกับ Log และ Event ต่าง ๆ ที่คอยทำหน้าที่วิเคราะห์หาความเชื่อมโยงของ Event ต่าง ๆ ที่เกี่ยวข้องกับความปลอดภัยทั้งหมด ไปจนถึงการ Alert ระบุ ตำแหน่งของภัยคุกคามให้ทราบ เมื่อมี Event ที่ผิดปกติ ทำให้สามารถป้องกัน และตอบสนอง ภัยคุกคามได้อย่างรวดเร็ว	มีระบบ SIEM เพื่อนำมาวิเคราะห์พฤติกรรมของ Cyber Attack บนระบบที่ให้บริการทั้งระดับ Infrastructure และ Operating system (OS) โดยจะต้องครอบคลุมการตรวจจับพื้นฐาน ดังนี้ 1. ตรวจจับและแจ้งเตือนการบุกรุกที่เข้าถึงระบบเครือข่าย การพยายาม Brute force Login เข้า ระบบ และ การ Scan port (port scanning) 2. Malware-Virus Detection ตรวจจับและแจ้งเตือน Malware หรือ Virus จากพฤติกรรมต่างๆ ที่ เกิดขึ้นหรือจาก signature 3. Blacklist IP การตรวจจับและแจ้งเตือนการเข้าถึง IP Address ที่เป็น Blacklist และระบุการ เปิด connection ได้ 4. Unauthorized Access การตรวจจับการเข้าถึงข้อมูลหรือระบบที่ไม่ได้รับอนุญาต หรือไม่มีสิทธิ์เข้าถึง ระบบ 5. DDoS Attack การตรวจจับพฤติกรรมการโจมตีในรูปแบบของ DDoS ได้ ทั้งภายนอกและภายใน 6. Data Breaches การตรวจจับและแจ้งเตือนการละเมิดการเข้าถึงข้อมูลที่สำคัญของระบบที่ไม่อนุญาต ให้เข้าถึง			
-----	---	--	--	--	--

หลักฐาน

W.

Endpoint Groups

11391_SK_CHP_SABAYOI_HOS

<

11391_SK_CHP_SABAYOI_HOS

Agents

Files

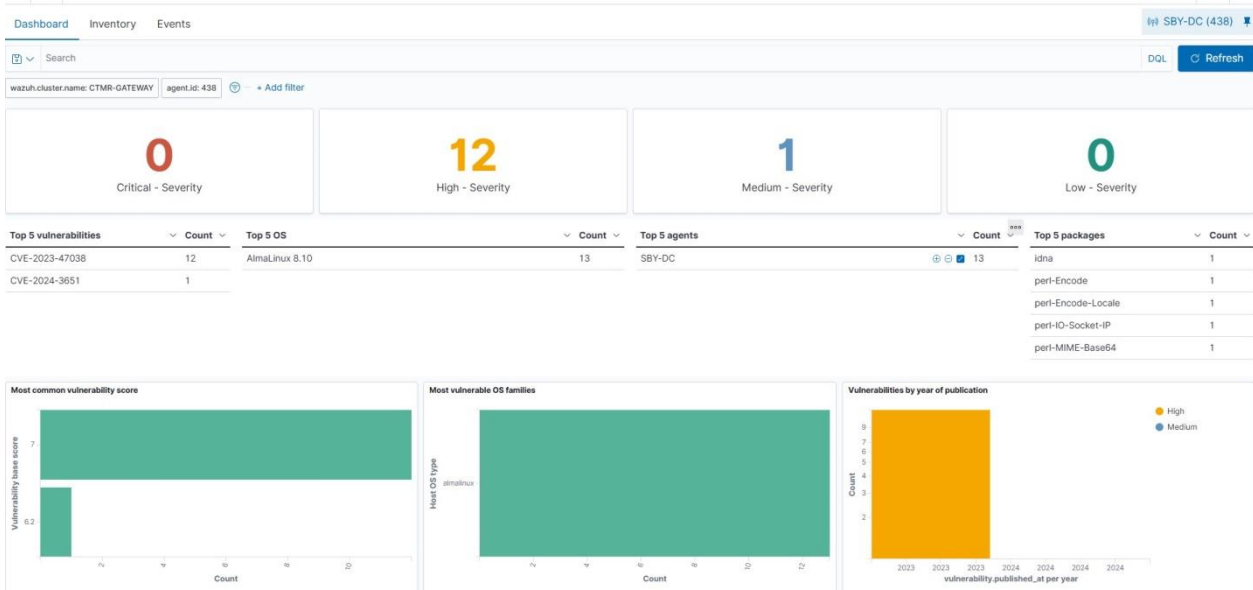
Agents (3)

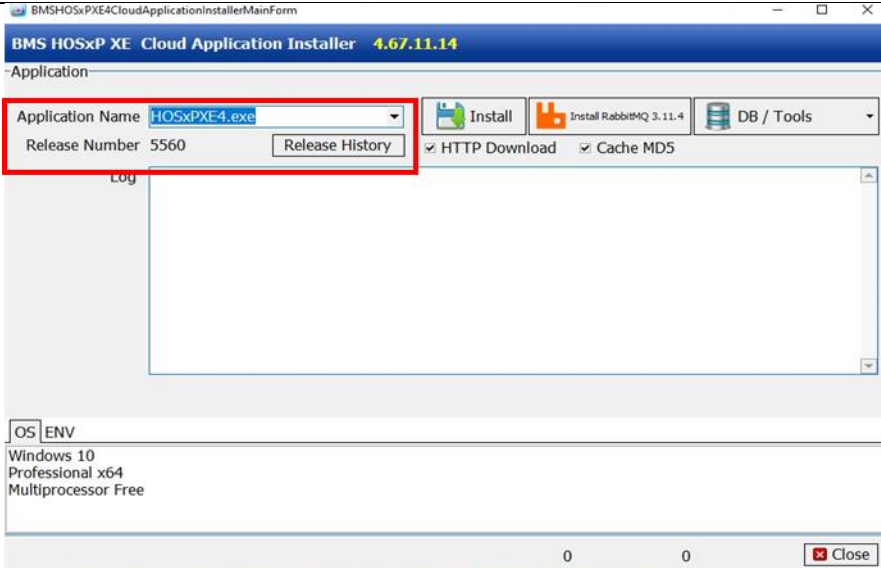
From here you can list and manage your agents

Search

Id ↑	Name	IP address	Operating system	Version	Status
103	HOSxP-MS	172.16.0.250	 AlmaLinux 8.10	v4.9.2	active ⓘ
117	sabayoibackup	172.16.0.251	 AlmaLinux 8.10	v4.9.2	active ⓘ
438	SBY-DC	172.16.0.241	 AlmaLinux 8.10	v4.9.2	active ⓘ

11.	Vulnerability Assessment (VA Scan) : การตรวจสอบช่องโหว่ของระบบเพื่อให้ทราบถึงความเสี่ยงจุดอ่อน และระดับความรุนแรงของผลกระทบที่อาจเกิดขึ้นจาก	มีการดำเนินการ Vulnerability Assessment (VA Scan) อย่างน้อยปีละ 1 ครั้ง โดยจะต้องดำเนินการแก้ไข CVE และช่องโหว่ต่างๆ ที่เกิดขึ้นโดยให้ความสำคัญกับความเสี่ยงระดับ Critical, High เป็นลำดับแรก 1. Review Vulnerability Assessment Report 2. จัดลำดับความสำคัญ ความเสี่ยงระดับ Critical, High, Medium, Low กำหนดระยะเวลาในการแก้ไข ช่องโหว่	โครงการศูนย์เฝ้าระวังป้องกันและรับมือภัยคุกคามทางด้านไซเบอร์สำหรับโรงพยาบาลรัฐ (Healthcare Cyber Defense Center)		
-----	---	---	--	--	--

	การถูกโจรกรรมข้อมูลและการโจมตีทางไซเบอร์	3. การจัดการความเสี่ยง 3.1 ยอมรับความเสี่ยง (Risk Acceptance) 3.2 หลีกเลี่ยงความเสี่ยง (Risk Avoidance) 3.3 ลดความเสี่ยง (Risk Mitigation) 3.4 ถ่ายโอนความเสี่ยง (Risk Transfer)			
หลักฐาน  The screenshot displays a security dashboard with the following components: Summary Cards: Four cards showing severity counts: Critical (0), High (12), Medium (1), and Low (0). Top 5 Vulnerabilities: A table listing CVE-2023-47038 (Count: 12) and CVE-2024-3651 (Count: 1). Top 5 OS: A table listing AlmaLinux 8.10 (Count: 13). Top 5 Agents: A table listing SBY-DC (Count: 13). Top 5 Packages: A table listing idna, perl-Encode, perl-Encode-Locale, perl-IO-Socket-IP, and perl-MIME-Base64, each with a count of 1. Charts: Three charts at the bottom: 'Most common vulnerability score' (bar chart), 'Most vulnerable OS families' (bar chart for AlmaLinux), and 'Vulnerabilities by year of publication' (line chart showing counts for High and Medium severity from 2023 to 2024).					
12.**	Penetration Testing : การทดสอบการเจาะระบบ	มีการทำ Penetration Testing ของ Web Application ในรูปแบบของ Gray box หรือ Black box อย่างน้อยปีละ 1 ครั้ง และดำเนินการแก้ไขโดยจะต้องไม่มีช่องโหว่ระดับ Severity Critical , High เกิดขึ้น และไม่มีช่องโหว่ที่เกิดขึ้นตามมาตรฐาน OWASP TOP10			
13.**	Software Update : การตรวจสอบ Version ของ Software ให้เป็น Version Update ล่าสุด เพื่อปิดช่องโหว่ที่เกิดขึ้นใน Software Version ก่อนหน้า	มีการอัปเดต Software Patching ของระบบ HIS และมีการทำ Penetration Testing อย่างน้อยปีละ 1 ครั้ง หรือมีการออก Major version โดยจะต้องดำเนินการแก้ไขช่องโหว่ในระดับ Severity Critical และ High เป็นอย่างน้อย			

				
14.** Disaster Recovery site (DR) : ศูนย์สำรองข้อมูล สำหรับแก้ไขปัญหาระบบสารสนเทศที่เกิดขึ้นจากภัยพิบัติต่างๆ ให้สามารถทำงานได้อย่างต่อเนื่อง	มีระบบ Disaster Recovery site (DR) ในกรณีฉุกเฉินที่ระบบหลักมีปัญหาและไม่สามารถใช้งานได้ โดย จะต้อง มี DR-Site โดยยึดจากมาตรฐาน ISO27001 และนำมาปรับใช้งานดังนี้ 1. ระยะห่างระหว่าง DC-Site กับ DR-Site ต้องไม่น้อยกว่า 60 กิโลเมตร 2. ต้องมีระบบฐานข้อมูลที่สำคัญอย่างน้อย 1 ระบบขึ้นบน DR-site 3. RTO ต้องเท่ากับหรือไม่มากกว่า = 24 ชั่วโมง หรือขึ้นอยู่กับ Solution 4. RPO ต้องเท่ากับหรือไม่มากกว่า = 24 ชั่วโมง 5. ต้องมีเอกสารสรุปผลการทดสอบการดำเนินการ DR-Site 6. ระบบต้องมีมาตรฐาน ISO ดังนี้เป็นอย่างน้อย 6.1 ISO27001 - Information Security Management System 6.2 ISO27799 - Health Informatics-Information Security Management			



```
postgres@HOSP-M5:~$ su
[postgres@HOSP-M5 ~]$ su postgres
postgres@HOSP-M5 ~$ pgcli -U abay -d hsd
pgcli (15.10)
Type "help" for help.

hsd=# select max(vn) from ovst;
max
-----
671202102946
(1 row)

hsd=#
```

```
postgres@abaybackp:~$ su postgres
postgres@abaybackp:~$ pgcli -U abay -d hsd
pgcli (15.10)
Type "help" for help.

hsd=# select max(vn) from ovst;
max
-----
671202102946
(1 row)

hsd=#
```

```
postgres@Orsite-Sby:~$ su postgres
postgres@Orsite-Sby:~$ pgcli -U abay -d hsd
pgcli (15.10)
Type "help" for help.

hsd=# select max(vn) from ovst;
max
-----
671202102946
(1 row)

hsd=#
```

