การตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

และแผนการรับมือภัยคุกคามทางไซเบอร์ ปี 2569

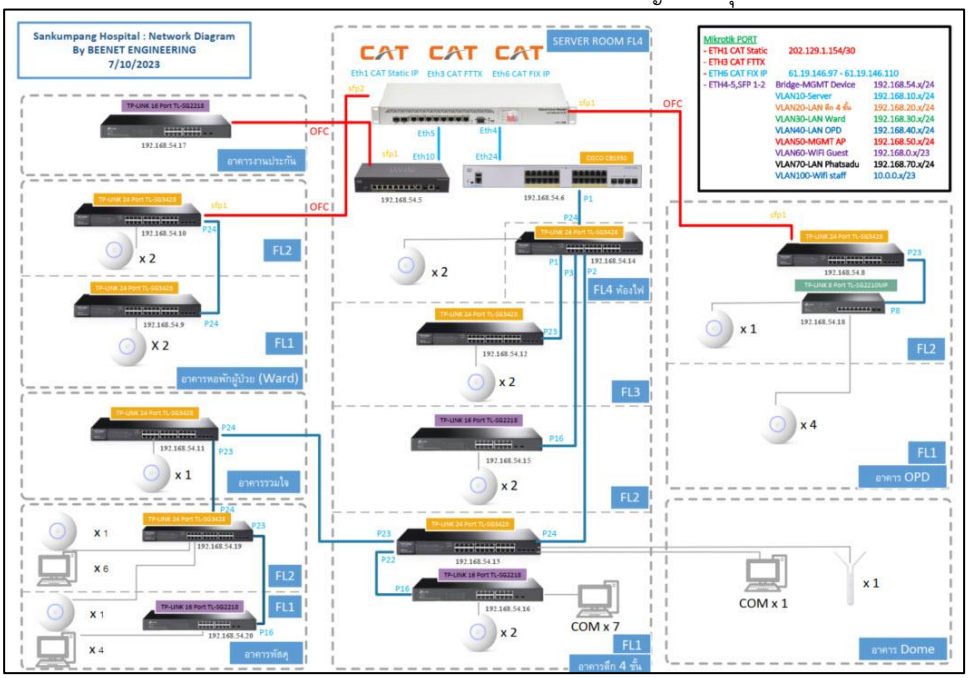
.....

Antivirus Software	
ประเด็นการประเมิน	**รายละเอียดการประเมิน**
โปรแกรมป้องกันไวรัส หรือ แอนติไวรัส คอยตรวจจับป้องกัน และกาจัดโปรแกรม คุกคามทางคอมพิวเตอร์ หรือมัลแวร์	มีการติดตั้ง Anti-Virus หรือ EDR หรือ XDR บน เครื่องคอมพิวเตอร์ของระบบที่สำคัญ 1. Review Alert Report 2. Update Program Anti-Virus, EDR/XER 3. Schedule Update Database Signature

โรงพยาบาลสันกำแพงเลือกใช้ซอฟต์แวร์ Antivirus Microsoft Defender ที่มีอยู่กับ Microsoft Windows โดยออกแบบมาเพื่อปกป้องระบบจากภัยคุกคาม เช่น มัลแวร์ ขั้นตอนการ โจมตีที่ซับซ้อน (APT) และ ransomware อย่างครอบคลุม

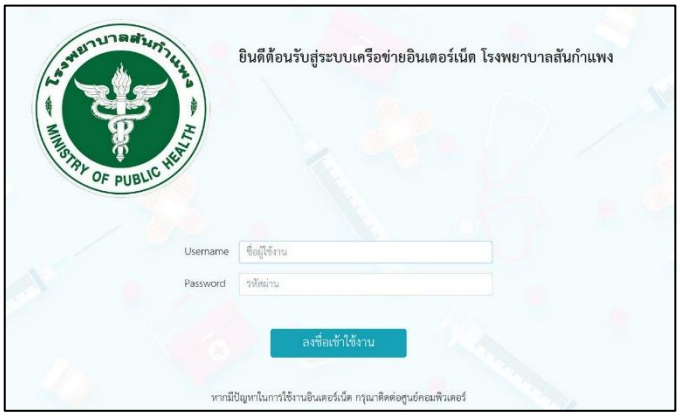
Access Control (Public & Private)	
ประเด็นการประเมิน	**รายละเอียดการประเมิน**
การควบคุมอุปกรณ์หรือการเข้าถึงระบบ ผ่านทางช่องทาง Public/Private ทั้งภายในประเทศและต่างประเทศ	มีการควบคุม Policy การเข้าถึงระบบที่สำคัญทั้งทาง Public และ Private 1. Open Port Access จากภายนอกเท่าที่จำเป็น เช่น HTTPS (๔๔๓) 2. IP Address Filter กำหนดขอบเขตการใช้งาน IP Address ที่สามารถเข้าใช้งานในระบบได้ เช่น IP Location, Geometric 1. Enable IDS/IPS 2. ใช้ระบบ VPN (Virtual Private Network) สำหรับการ เข้าถึง Server/Application ภายใน ผ่านโปรโตคอล IPsec/SSL 5. มีการแบ่งโซน Network ภายใน รวมถึงมี Firewall กั้น ระหว่างโซนภายในที่สำคัญ 6. User Access Account กำหนดสิทธิการใช้งานเท่าที่ จำเป็น เช่น Role Base / Group Base 7. User Password Policy กำหนดการใช้งานพาสเวิด เช่น กำหนดความยาวอย่างน้อย ๑๒ ตัวอักษร, Hash MD๕, SHA-๒๕๖ 8. Time Sync 9. Change Default Accounts 10. Review Privilege Accounts 11. Review Logs Access 12. Feeds IOC (Option)

มีการการแยก Server zone ออกจากสำนักงาน เพื่อง่ายต่อการจัดการและลดปัญหาภัยคุกคามที่อาจจะมาจากฝั่ง Client

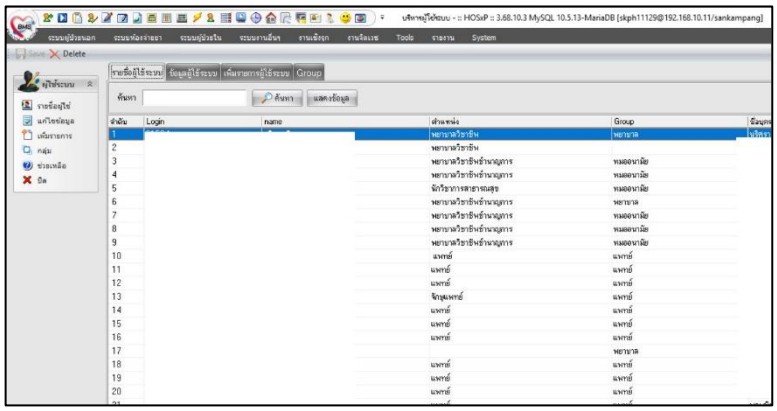


Privileged Access Management (PAM)	
ประเด็นการประเมิน	**รายละเอียดการประเมิน**
การรักษาความปลอดภัยของข้อมูล ติดตาม ตรวจหาและป้องกันการใช้สิทธิการเข้าถึงทรัพยากรที่สำคัญในระดับสูง	มีการควบคุมการเข้าถึงระบบโดยใช้งานสิทธิระดับ Least Privilege ดังนี้ 1. ดำเนินการ Disable Administrator / Root / Admin 2. มีการกำหนด Role-base access ในการเข้าถึงระบบเท่าที่มีจำเป็น 3. มี Access Rights Matrix ของระบบ 4. มีการตั้ง Password อย่างน้อย ๑๒ ตัว (ตัวอักษรใหญ่, เล็ก, อักขระพิเศษ, ตัวเลข) ๑๒ , มีการเข้ารหัส Password MD ๕,SHA-๒๕๖ 5. Expire Sessions Time out 6. Review Privilege Accounts 7. Review กิจกรรมผู้ใช้งานในระบบ

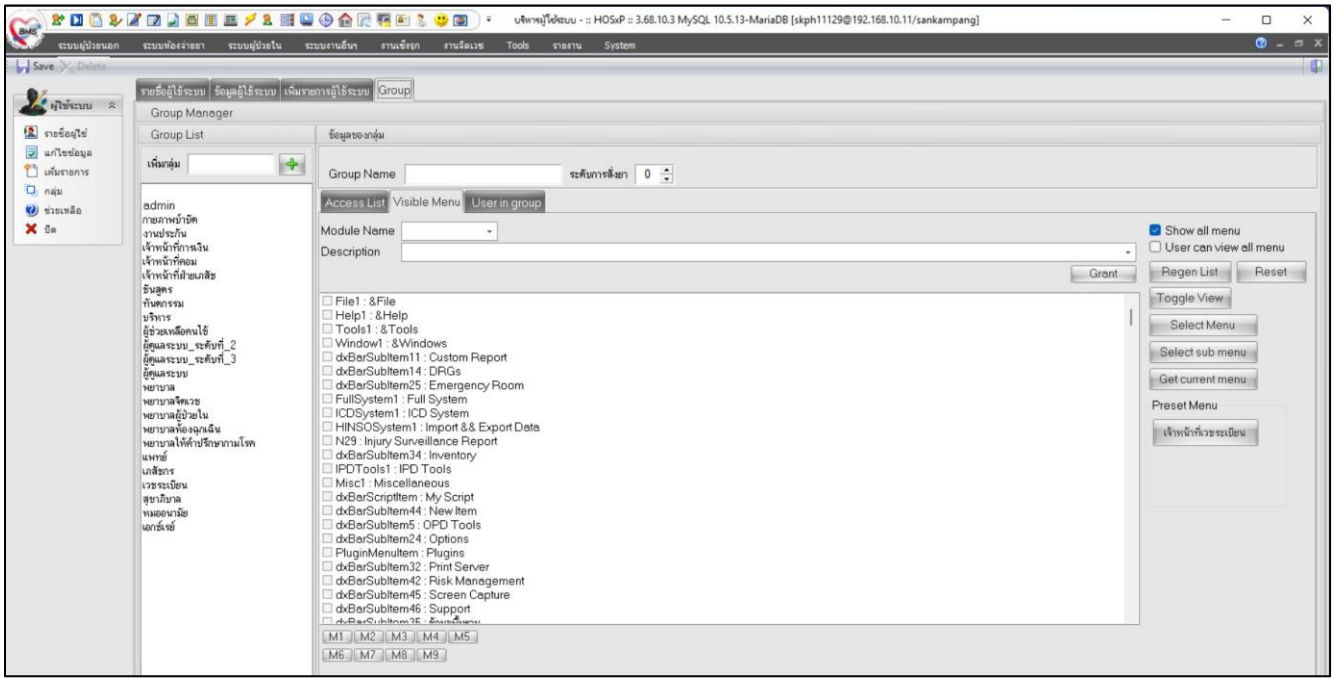
มีระบบ Authen login ในการเข้าใช้งานระบบเครือข่าย internet ภายในเพื่อระบุได้ว่าผู้ใช้งานในระบบเป็นบุคคลากรของโรงพยาบาลและมีสิทธิ์การเข้าถึงระบบเครือข่าย internet



การเข้าถึง HIS



กำหนดสิทธิในการเข้าถึงข้อมูล



Business Continuity Plan (BCP) & Disaster Recovery Plan (DRP)	
ประเด็นการประเมิน	**รายละเอียดการประเมิน**
แผนกำหนดแนวทางการดำเนินการของ หน่วยงาน เมื่อเกิดสภาวะวิกฤตหรือ ภัยต่างๆ ทีส่งผลให้ กระบวนการทำงาน ของหน่วยงานหยุดชะงัก เพื่อให้สามารถ กลับมาดำเนินการได้อย่างต่อเนื่อง	มีการทดสอบ Business Continuity Plan (BCP) และ Disaster Recovery Plan (DRP) อย่างน้อย ปีละ ๑ ครั้ง และ มีการจัดทำ รายงานถึง ขั้นตอนการดำเนินการที่ชัดเจนรวมถึงระยะเวลา ดำเนินการและผู้ทีเกี่ยวข้องในการดำเนินการงานดังนี้ 1. การบริหารจัดการความเสี่ยง (Risk Management) 2. การบริการจัดการด้าน Resource (Resource Management) 3. การวางแผนความต่อเนื่องจำกธุรกิจทเกิดขึ้น (Business Continuity Planning) 4. การทดสอบ (Testing) 5. การปรับปรุงและแก้ไข (Review & Update)

ขั้นตอนการให้บริการของหน่วยงาน เวชระเบียน ในขณะที่ระบบ HIS ไม่สามารถใช้งานได้ ขั้นตอนการให้ปริการหน่วยงาน เวชระเบียน สำหรับผู้ป่วยนอก (OPD)

1. ผู้ป่วยรับใบนำส่งผู้ป่วย (บัตรคิว) ที่โต๊ะประชาสัมพันธ์

2. ผู้ป่วยรับการคัดกรองเบื้องต้นที่จุดคัดกรอง

3. รับหลักฐานในการมารับบริการจากผู้ป่วย ผู้ป่วยจะต้องนำหลักฐานยืนยัน ตัวบุคคลอย่างหนึ่ง อย่างใด ดังต่อไปนี้มาแสดงทุกครั้งที่มารับบริการ

3.1 บัตรประจำตัวประชาชน

3.2 บัตรโรงพยาบาล

3.3 สูติบัตร

3.4 เอกสารอื่น ๆ ที่มีรูปที่ทางราชการออกให้และสามารถยืนยันตัวบุคคลได้

4. เจ้าหน้าที่ทำการตรวจสอบผู้ป่วยว่าเป็นผู้ป่วยรายใหม่หรือรายเก่า

4.1 ผู้ป่วยรายใหม่

1) กรอกข้อมูลผู้ป่วยลงในแบบบันทึกผู้ป่วยรายไม่

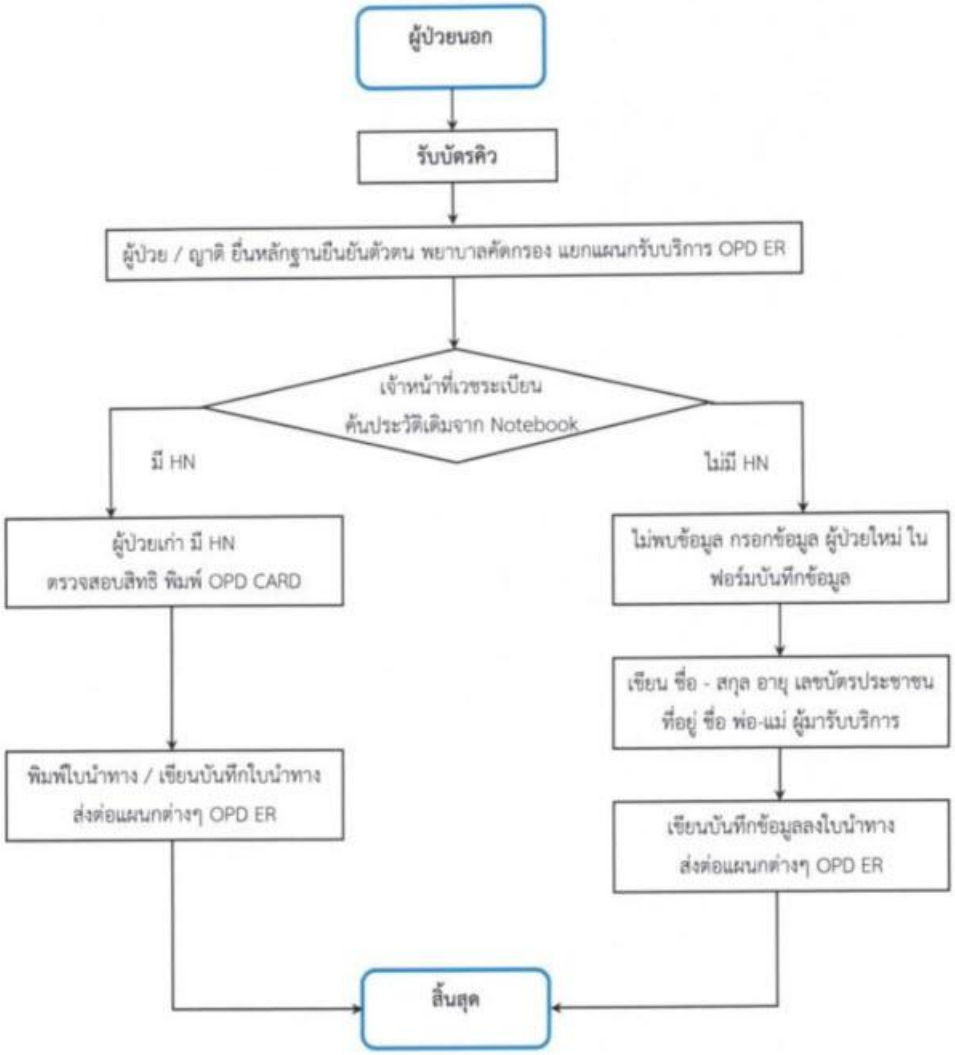
2) ทำการเขียน ชื่อ-สกุล อายุ ลงในใบนำส่งผู้ป่วย

4.2 ผู้ป่วยรายเก่า

ส่งใบนำส่งไปยังแผนกผู้ป่วยนอกซักประวัติ เพื่อส่งพบแพทย์ บันทึกข้อมูล

การรักษา และการสั่งยาในใบนำส่งผู้ป่วย กรณีผู้ป่วยมาตามนัดให้เลื่อนนัดผู้ป่วย

แผนการดำเนินงานหน่วยงาน เวชระเบียน เมื่อระบบ HIS ไม่สามารถใช้ได้ ผู้ป่วยนอก



หน่วยงานผู้ป่วยนอก (OPD)

ขั้นตอนการให้บริการของหน่วยงาน ผู้ป่วยนอก ในขณะที่ระบบไม่สามารถใช้งานได้

1. รับเอกสารผู้ป่วยจากหน่วยงาน เวชระเบียน

2. พยาบาลซักประวัติ เขียนบันทึกลงในใบนำส่งผู้ป่วย

3. ส่งผู้ป่วยพบแพทย์เพื่อตรวจรักษา

4. พยาบาลจุดรับ Order แพทย์ตรวจสอบเอกสารที่แพทย์ทำการรักษาถ้าผู้ป่วยต้องมี Xray หรือ สั่ง LAB หัตถการ Admit REFER ให้ดำเนินการดังนี้

4.1 แพทย์สั่งตรวจ X-Ray สั่งตรวจ LAB หรือส่งทำหัตถการ ให้ดำเนินการดังนี้ 4.1.1 ส่งต่อผู้ป่วยไปหน่วยงาน X-Ray หรือ ห้องปฏิบัติการ LAB 4.1.2 ส่งทำหัดการที่ห้องทำหัตถการ

4.1.3 ผู้ป่วยตรวจเสร็จ ส่งผู้ป่วยพบแพทย์ตรวจรักษาอีกครั้ง

4.2 แพทย์ตรวจเสร็จแล้วให้รับยากลับบ้าน หรือมีนัดมาติดตามการรักษา

4.2.1 ส่งต่อผู้ป่วยไปรับยาที่ห้องจ่ายยา

4.2.2 ทำการเขียนใบนัดให้มารับบริการในครั้งต่อไป

4.3 แพทย์ตรวจแล้วสั่งนอนโรงพยาบาลรับการรักษาต่อ 4.3.1 ให้ญาติไปยื่นเอกสารรับยาที่ห้องจ่ายยา 4.3.2 เจ้าหน้าที่จัดทำเอกสาร เพื่อลงทะเบียน Admit

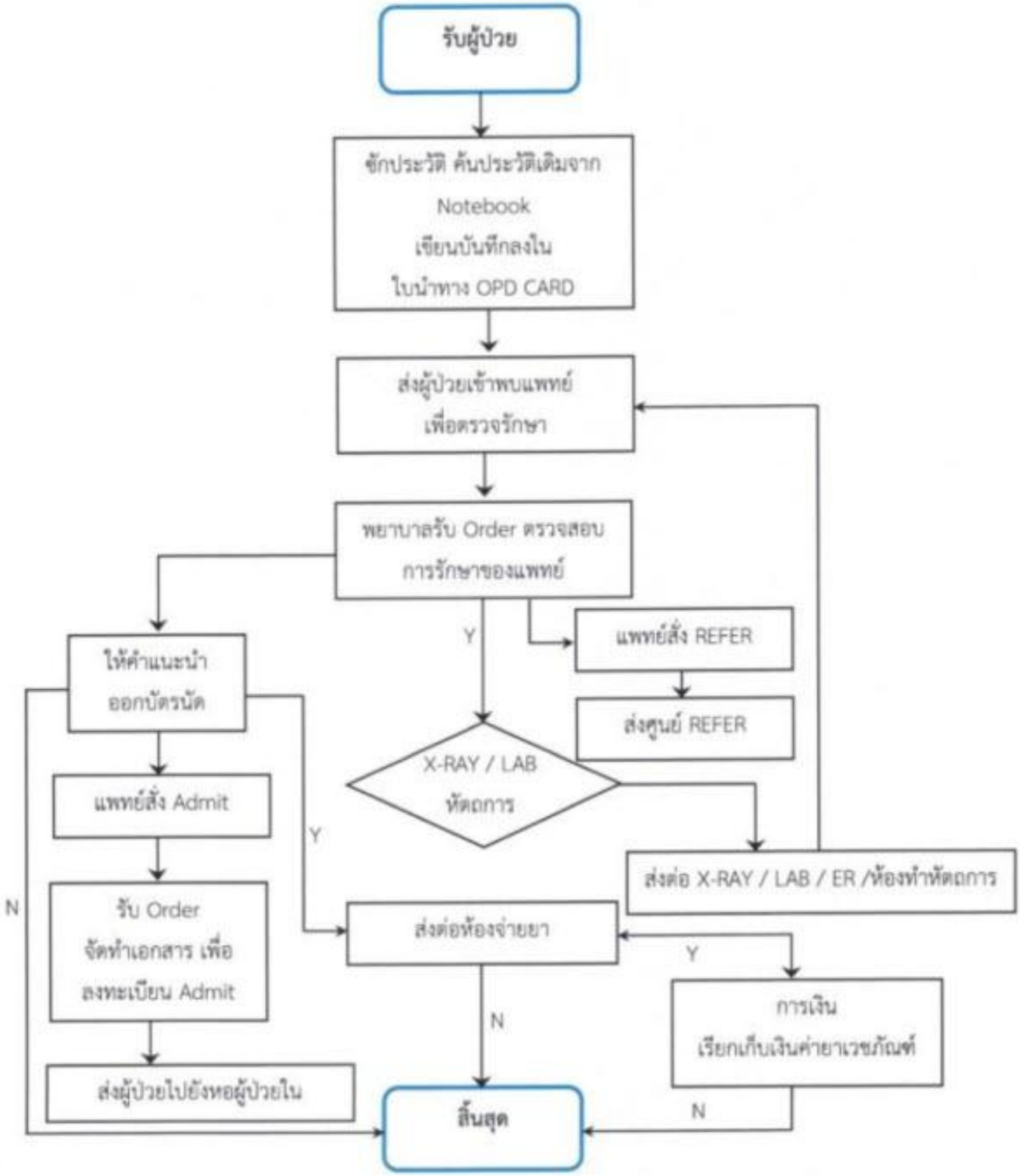
4.4 แพทย์ตรวจแล้วส่งต่อไปรับการรักษาโรงพยาบาลอื่น

4.4.1 ตรวจสอบความถูกต้องใบส่งตัว

44.2 ส่งต่อศูนย์ REFER

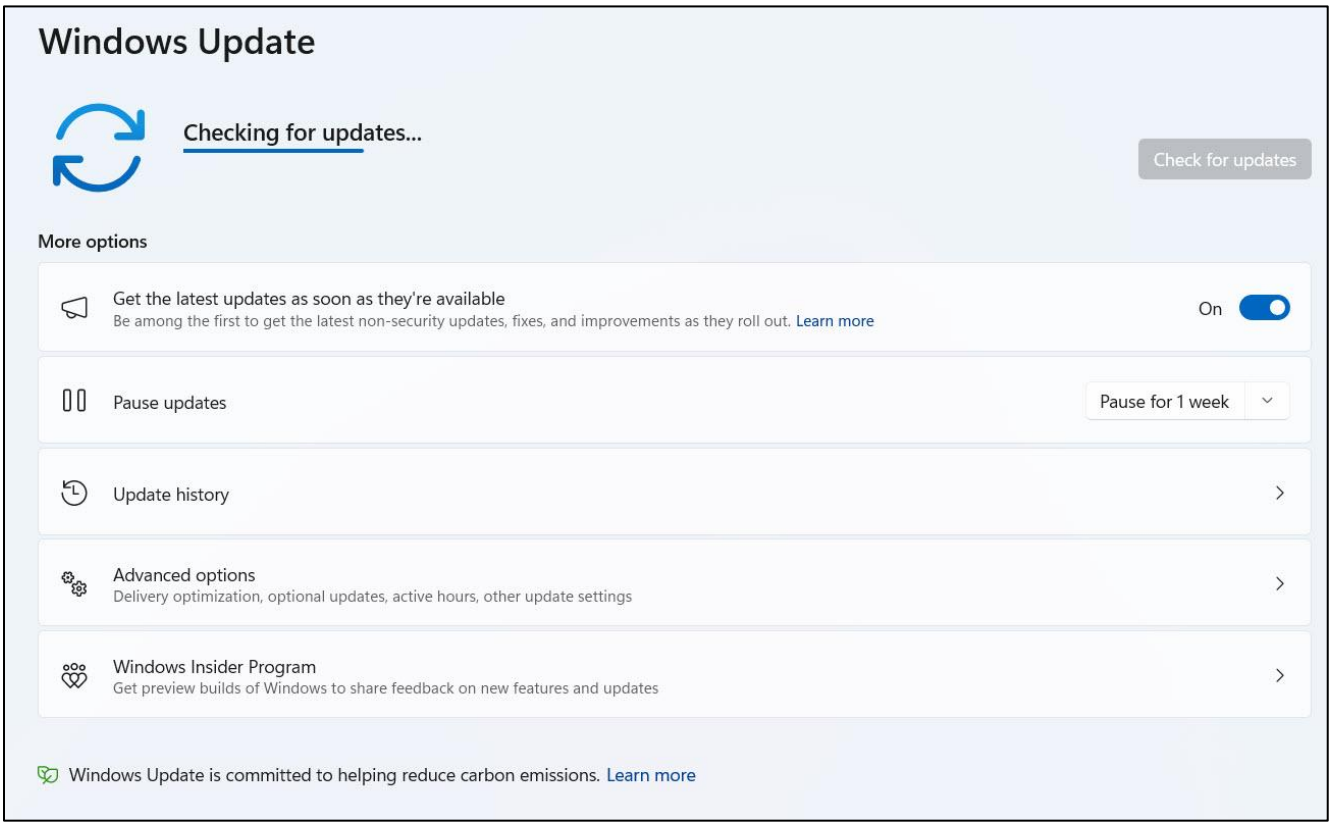
4.5 กรณีไม่มียาหรือค่าใช้จ่ายในการรักษาพยาบาลให้จำหน่ายกลับบ้าน

แผนการดำเนินงานหน่วยงานผู้ป่วยนอก (OPD) เมื่อระบบ HIS ไม่สามารถใช้ได้



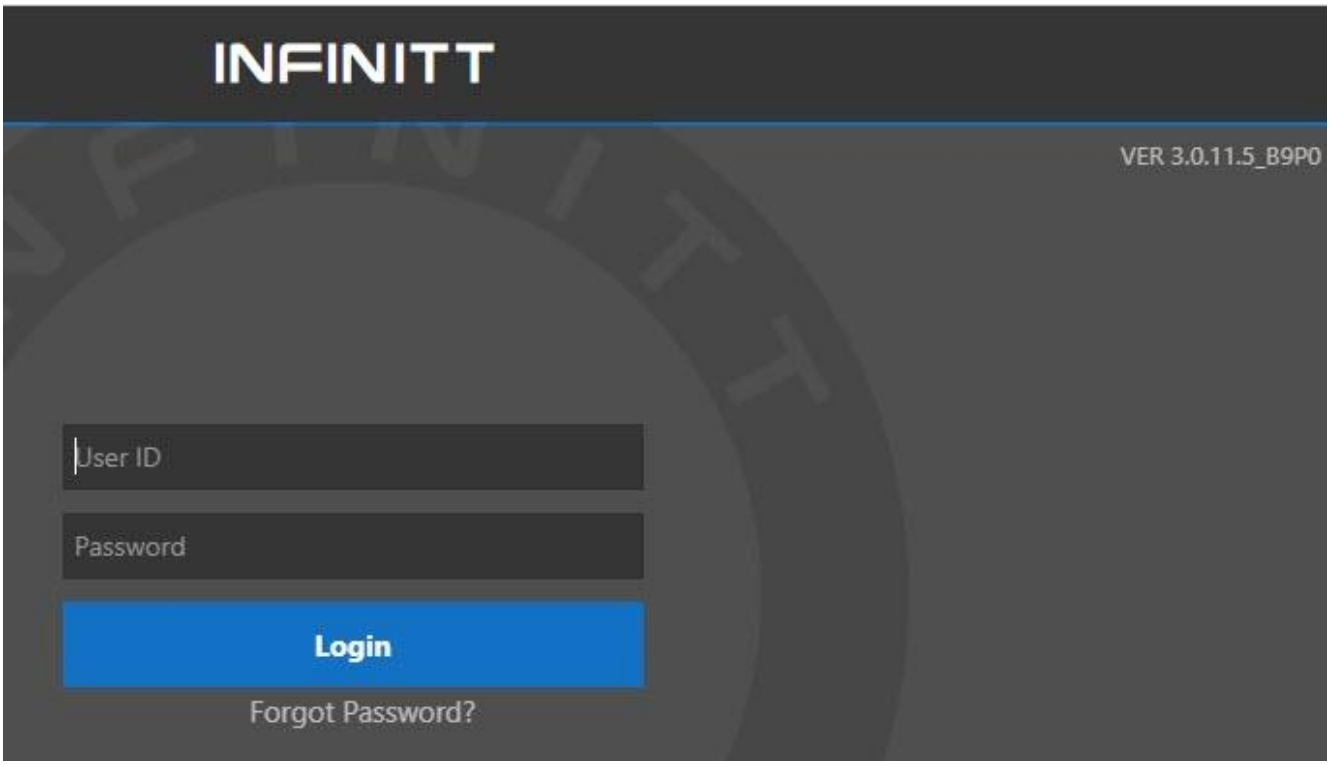
OS Patching	
ประเด็นการประเมิน	**รายละเอียดการประเมิน**
การซ่อมแซมจดบกพรองของ ระบบปฏิบัติการ (OS) หรือ ปรับปรง ระบบปฏิบัติการให้ทันสมัย และเพิมเติม ความสามารถในการใช้งานหรือ ประสิทธิภาพให้ดีขึ้น	มีการอัปเดต Security Patching 1. Firewall patching (Firmware) 2. Operation patching 3. Application patching 4. Software patching 5. Change Management

Operation patching Windows 11 (ล่าสุด) และมีการอัพเดท windows อยู่สม่ำเสมอ



Application & Software patching HOSxP

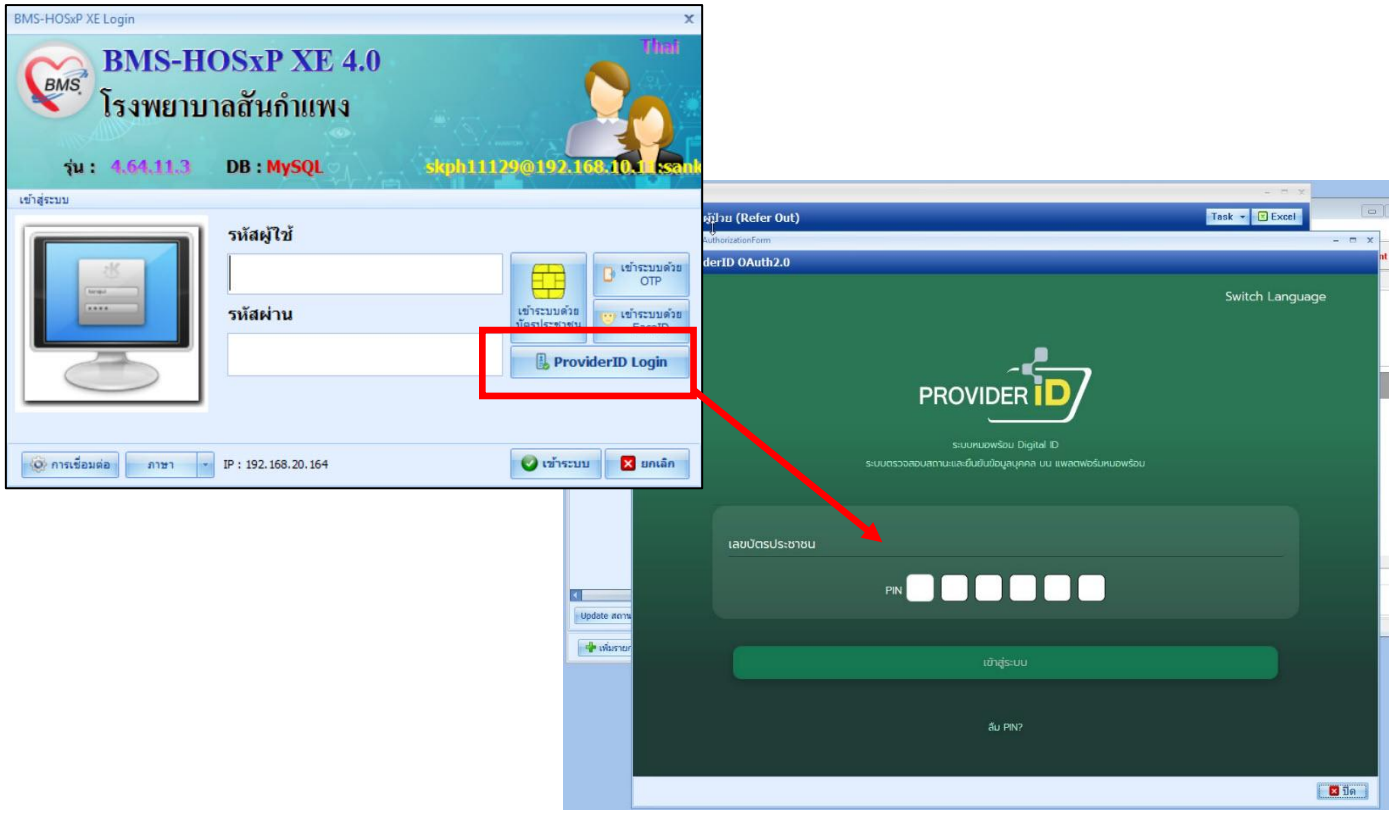
PACs



Multi-Factor Authentication (2FA)	
ประเด็นการประเมิน	**รายละเอียดการประเมิน**
การยืนยันตัวตน 2 ชั้น เป็นการ เข้าสู่ระบบบัญชีแบบหลายขั้นตอน ทีกำหนดให้ผู้ใช้ป้อนข้อมูลเพิ่มเติม นอกเหนือจำกรหัสผาน	มีการใช้งานระบบ Multi-Factor Authentication (๒FA) เพื่อยืนยันตัวตน ๒ ชั้นในการเข้าถึงระบบต่างๆ สาหรับ Admin ที่ใช้งานระบบอย่างน้อยดังนี้ 1. การ Login แบบ Multi-factor ไปยังระบบ VPN Access 2. การ Login แบบ Multi-factor ไปยังอุปกรณ์ Network 3. การ Login แบบ Multi-factor ไปยังอุปกรณ์ Security 4. การ Login แบบ Multi-factor ไปยัง Hypervisor 5. การ Login แบบ Multi-factor ไปยัง Operating system

Multi-Factor Authentication (2FA) : การยืนยันตัวตน 2 ชั้น เป็นการเข้าสู่ระบบบัญชีแบบหลายขั้นตอนที่กำหนดให้ผู้ใช้ป้อนข้อมูลเพิ่มเติมนอกเหนือจากรหัสผ่าน

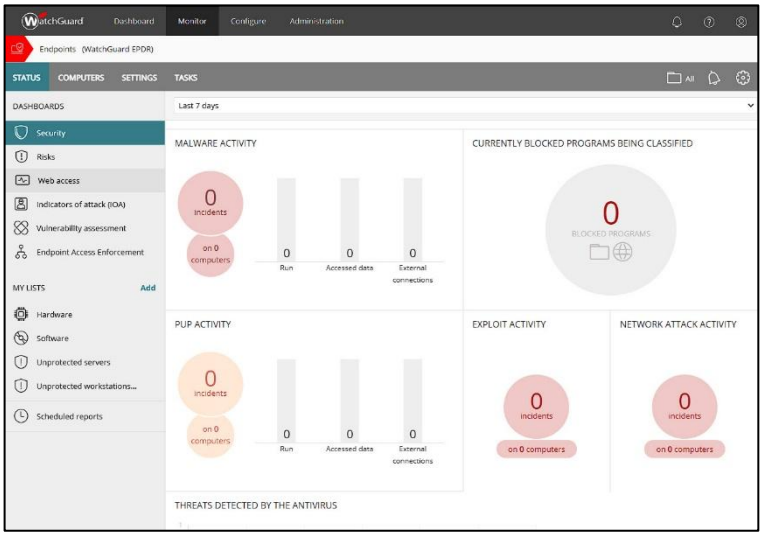
มีการเปิดใช้งานระบบ Provider id ของ HIS ระบุเลขบัตรประชาชนเพื่อส่งรหัส OTP ยืนยันการเข้าใช้งานไปที่แอพลิเคชั่นหมอพร้อมของผู้ใช้งาน



Web Application Firewall (WAF)	
ประเด็นการประเมิน	**รายละเอียดการประเมิน**
ระบบป้องกันการโจมตีทางไซเบอร์ สำหรับเว็บแอพพลิเคชันโดยเฉพาะ เพื่อป้องกันการโจมตีไปยังระบบเว็บแอปพลิเคชันของหน่วยงาน	มีการใช้งาน Web Application Firewall (WAF) กรณีที่มีระบบเป็น Web Application เพื่อป้องกันการโจมตีตามมาตรฐาน OWASP Top ๑๐ ได้เป็นอย่างน้อยตามรายละเอียด 1. Review Attack Report 2. Add Source IP Blocklists

Web Application Firewall (WAF) : ระบบป้องกันการโจมตีทางไซเบอร์สำหรับเว็บแอพลิเคชั่นโดยเฉพาะเพื่อป้องกันการโจมตีไปยังระบบแอปพลิเคชันของหน่วยงาน

มีระบบ Web Application Firewall (WAF) ของ watchguard ในการป้องกันการโจมตี จากMALWARE ACTIVITY, PUP ACTIVITY, EXPLOIT ACTIVITY, NETWORK ATTACK ACTIVITY และยังมี CURRENTLY BLOCKED PROGRAMS ที่อาจเป็นอันตราย และมี ใบรับรอง HOSTING ที่ใช้บริการ

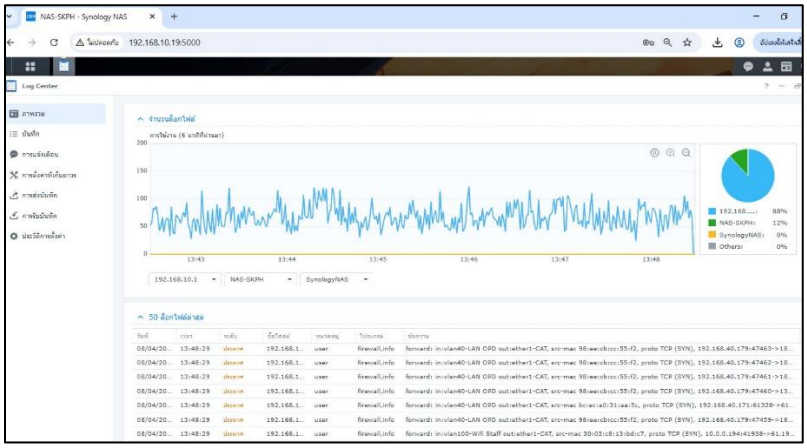


Log Management	
ประเด็นการประเมิน	**รายละเอียดการประเมิน**
การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์	มีระบบการจัดเก็บ Log อินเทอรเน็ต และคอมพิวเตอร์ตาม พ.ร.บ. คอมฯ อย่างน้อย ๙๐ วัน 1. System Logs 2. Access Logs 3. Authentication Logs 4. Authorization Logs 5. Error Logs 6. Applications Logs

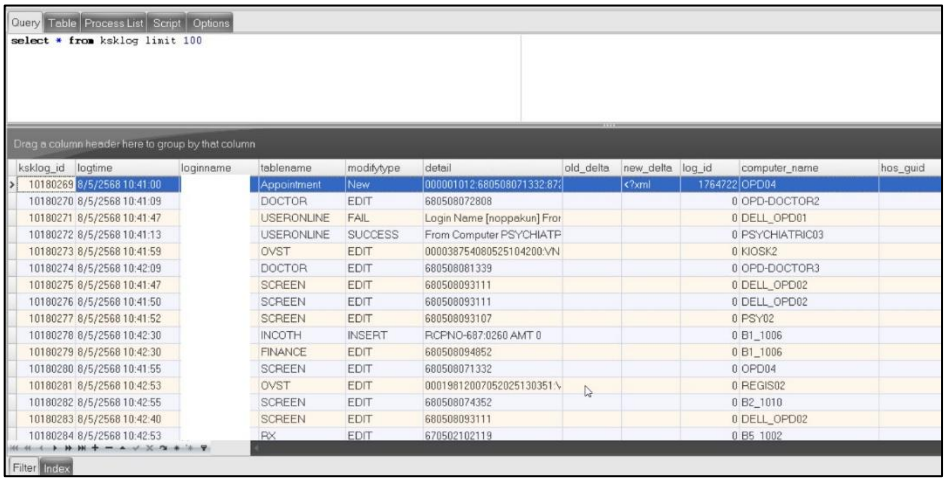
Log Management : การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

มีระบบตรวจสอบ Log Management : Synology Assistant ปฏิบัติการบน NAS ตรวจสอบLog การเข้าใช้งานทุก User ภายในเครือข่าย

System Logs



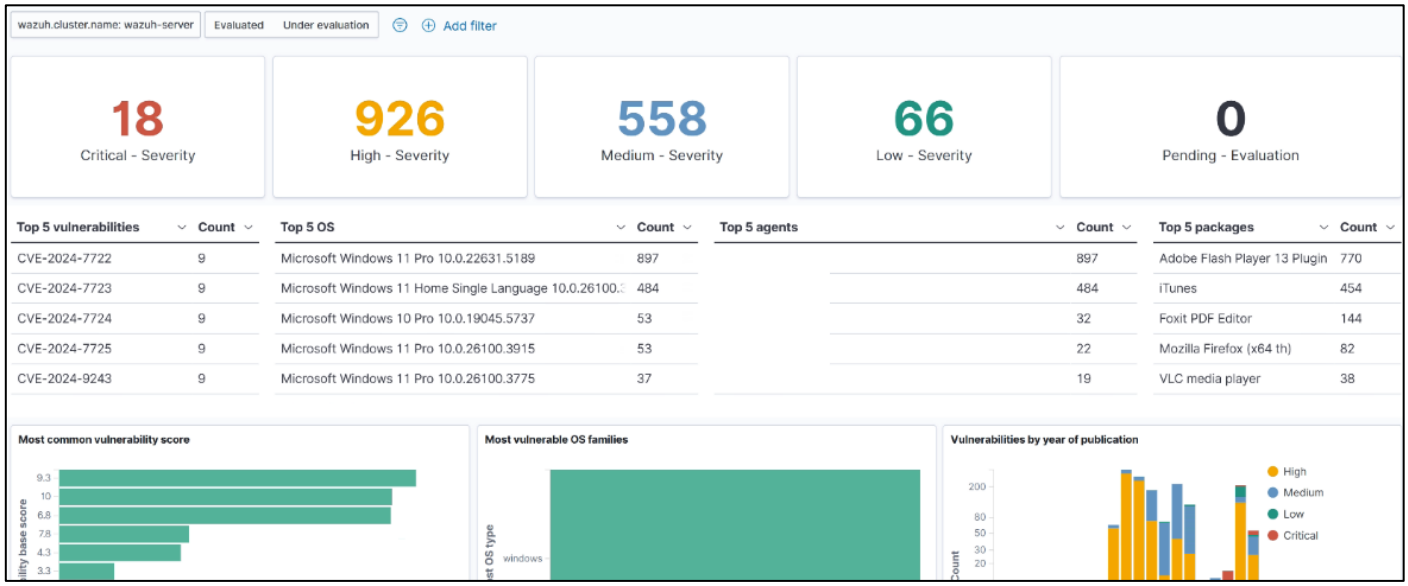
HIS logs



Security Information & Event Management (SIEM)	
ประเด็นการประเมิน	**รายละเอียดการประเมิน**
ระบบที่ใช้ในการจัดการกับ Log และ Event ต่าง ๆ ที่คอยทำหน้าทวิเคราะห์ หาความเชื่อมโยงของ Event ต่างๆ ที่ เกี่ยวข้องกับความปลอดภัยทั้งหมด ไปจนถึงการ Alert ระบุตำแหน่งของ ภัย คุกคามให้ทราบ เมื่อมี Event ที่ผิดปกติ ทำให้สามารถป้องกัน และตอบสนอง ภัย คุกคามได้อย่างรวดเร็ว	มีระบบ SIEM หรือระบบวิเคราะห์ภัยคุกคามทางไซเบอร์ เพื่อ นำมาวิเคราะห์พฤติกรรมของ Cyber Attack บนระบบ ที่ให้บริการทั้งระดับ Infrastructure และ Operating system (OS) โดยจะต้อง คลอบคลุมการตรวจจับพื้นฐาน ดังนี้ 1. ตรวจจับและแจ้งเตือนการบกรกทีเข้าถึงระบบเครื่อขาย การ พยายาม Brute force Login เข้า ระบบ และ การ Scan port (port scanning) 2. Malware-Virus Detection ตรวจจับและแจ้งเตือนMalware หรือ Virus จำกพฤติกรรมต่างๆ ที่เกิดขึ้นหรือจำก signature 3. Blacklist IP การตรวจจับและแจ้งเตือนการเข้าถึง IP Address ทีเป็น Blacklist และระบบการเปิด connection ได้ 4. Unauthorized Access การตรวจจับการเข้าถึงข้อมูลหรือ ระบบที่ไม่ได้รับอนญาต หรือไม่มีสิทธิเข้าถึงระบบ 5. DdoSAttackการตรวจจับพฤติกรรมการโจมตีในรูปแบบของ DDoS ได้ ทั้งภายนอกและภายใน 6. Data Breaches การตรวจจับและแจ้งเตือนการละเมิดการเข้าถึงข้อมูลทีสำคัญของระบบ ทีไม่อนญาตให้เข้าถึง

Security Information & Event Management (SIEM) : ระบบที่ใช้ในการจัดการกับ Log และ Event ต่าง ๆ

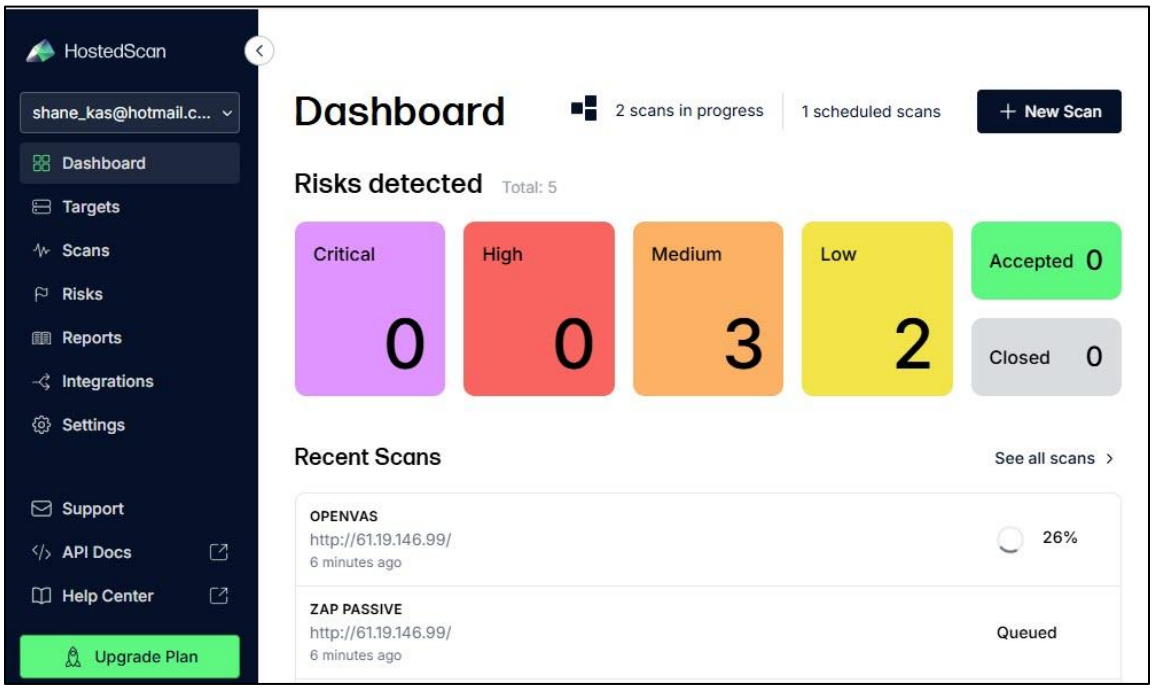
มีระบบ Wazuh ทำหน้าที่วิเคราะห์ Event ต่างๆที่เกี่ยวข้องด้านความปลอดภัยระบบโรงพยาบาลระบุตำแหน่งภัยคุกคามให้ทราบ



Vulnerability Assessment (VA Scan)	
ประเด็นการประเมิน	**รายละเอียดการประเมิน**
การตรวจสอบชองโหว่ของระบบเพื่อให้ ทราบถึงความเสี่ยงจุดอ่อนและระดับ ความรุนแรงของผลกระทบที่อาจเกิดขึ้น จากการถูกโจรกรรมข้อมูลและการโจมตี ทางไซเบอร์	มีการดำเนินการ Vulnerability Assessment (VA Scan) อย่าง น้อยปีละ 1 ครั้ง โดยจะต้องดำเนินการแก้ไข CVE และช่องโหว่ ต่างๆ ที่เกิดขึ้นโดยให้ความสำคัญกับความเสี่ยงระดับ Critical, High เป็นลำดับแรก 1. Review Vulnerability Assessment Report 2. จัดลำดับความสำคัญ ความเสี่ยงระดับ Critical, High, Medium ,Low กำหนดระยะเวลาในการแก้ไขชองโหว่ 3. การจัดการความเสี่ยง 3.1 ยอมรับความเสี่ยง (Risk Acceptance) 3.2 หลีกเลียงความเสี่ยง (Risk Avoidance) 3.3 ลดความเสี่ยง (Risk Mitigation) 3.4 ถ่ายโอนความเสี่ยง (Risk Transfer)

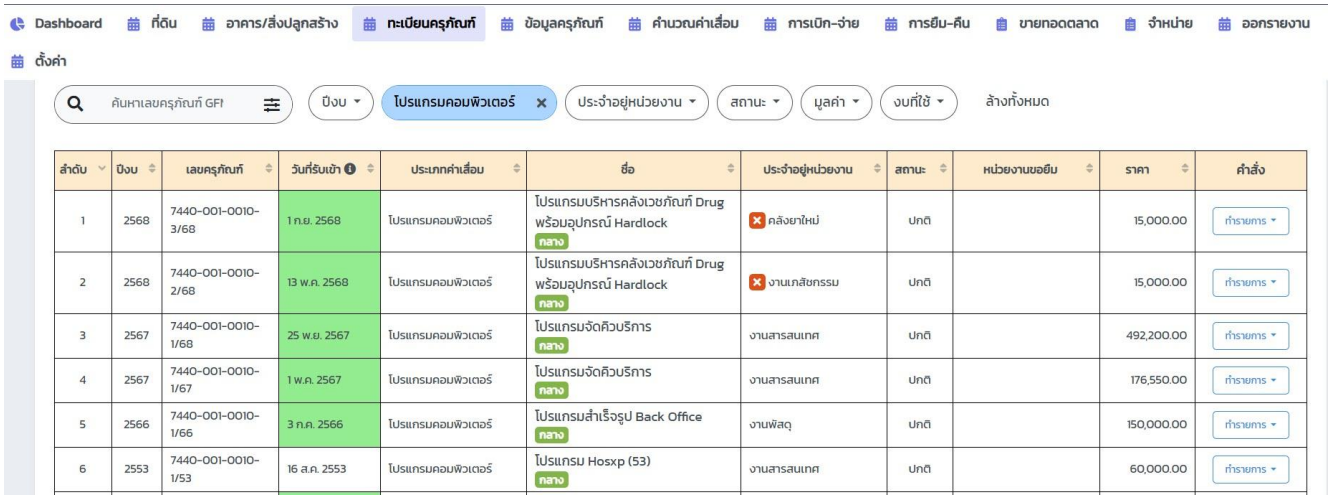
Vulnerability Assessment (VA Scan) : การตรวจสอบช่องโหว่ของระบบเพื่อให้ทราบถึงจุดอ่อน และระดับความรุนแรงของผลกระทบที่อาจเกิดขึ้นจากการถูกโจรกรรมข้อมูลและการโจมตีทางไซเบอร์

มีการ VA Scan โดยใช้ hostedscan.com ตรวจจับโหว่เพื่อดำเนินการแก้ไข



มีการใช้ซอฟต์แวร์ถูกลิขสิทธิ์และมีการจัดการทรัพย์สินซอฟต์แวร์	
ประเด็นการประเมิน	**รายละเอียดการประเมิน**
มีการใช้ซอฟต์แวร์ถูกลิขสิทธิ์สำหรับระบบงานและเครื่องคอมพิวเตอร์ที่สำคัญทั้งหมด และมีการจัดทำรายการทรัพย์สินซอฟต์แวร์ รวมถึงการตรวจสอบสถานะใบอนุญาต (License)	มีการใช้ซอฟต์แวร์ถูกลิขสิทธิ์สำหรับระบบงานและเครื่องคอมพิวเตอร์ที่สำคัญทั้งหมด และมีการจัดทำรายการทรัพย์สินซอฟต์แวร์ รวมถึงการตรวจสอบสถานะใบอนุญาต (License)

ทะเบียนซอฟต์แวร์ที่จัดซื้อ



ลำดับ	ปีงบ	เลขครุภัณฑ์	วันที่รับเข้า	ประเภทค่าเสื่อม	ชื่อ	ประจำอยู่หน่วยงาน	สถานะ	หน่วยงานขอยืม	ราคา	คำสั่ง
1	2568	7440-001-0010-3/68	1 ก.ย. 2568	โปรแกรมคอมพิวเตอร์	โปรแกรมบริหารคลังเวชภัณฑ์ Drug พร้อมอุปกรณ์ Hardlock กลาง	คลังยาใหม่	ปกติ		15,000.00	ทำรายการ
2	2568	7440-001-0010-2/68	13 พ.ค. 2568	โปรแกรมคอมพิวเตอร์	โปรแกรมบริหารคลังเวชภัณฑ์ Drug พร้อมอุปกรณ์ Hardlock กลาง	งานเภสัชกรรม	ปกติ		15,000.00	ทำรายการ
3	2567	7440-001-0010-1/68	25 พ.ย. 2567	โปรแกรมคอมพิวเตอร์	โปรแกรมจัดคิวบริการ กลาง	งานสารสนเทศ	ปกติ		492,200.00	ทำรายการ
4	2567	7440-001-0010-1/67	1 พ.ค. 2567	โปรแกรมคอมพิวเตอร์	โปรแกรมจัดคิวบริการ กลาง	งานสารสนเทศ	ปกติ		176,550.00	ทำรายการ
5	2566	7440-001-0010-1/66	3 ก.ค. 2566	โปรแกรมคอมพิวเตอร์	โปรแกรมสำเร็จรูป Back Office กลาง	งานพัสดุ	ปกติ		150,000.00	ทำรายการ
6	2553	7440-001-0010-1/53	16 ส.ค. 2553	โปรแกรมคอมพิวเตอร์	โปรแกรม Hosxp (53) กลาง	งานสารสนเทศ	ปกติ		60,000.00	ทำรายการ

การทดสอบการเจาะระบบเพื่อให้ทราบถึงจุดอ่อนหรือช่องโหว่ของระบบงาน	
ประเด็นการประเมิน	**รายละเอียดการประเมิน**
การทดสอบการเจาะระบบเพื่อให้ทราบถึงจุดอ่อนหรือช่องโหว่ของระบบงาน	มีการทำ Penetration Testing ของ WebApplication หรือระบบงานอื่น ตามความเหมาะสมในรูปแบบของ Gray box หรือ Black boxอย่างน้อยปีละ 1 ครั้ง และดำเนินการแก้ไขโดยจะต้องไม่มีช่องโหว่ระดับ Severity Critical , Highเกิดขึ้นและไม่มีช่องโหว่ที่เกิดขึ้นตามมาตรฐานOWASP TOP10

มีการทดสอบ Pentest tools ผ่านเว็บไซต์ https://pentest-tools.com/