R9 CYBER SECURITY PLATFORM

CTMR จังหวัดสุรินทร์

การพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ เขตสุขภาพที่ 9 ด้วยแพลตฟอร์ม
CTMR : Cyber Threat Monitoring Response

ประชุมคณะกรรมการวางแผนและประเมินผล (กวป.) เดือนมกราคม 2569
วันจันทร์ที่ 26 มกราคม 2569 เวลา 13.30 น.

ประเด็นการนำเสนอ

01.

เกณฑ์ CTAM+

Cyber Technical Assessment Matrix Plus

เกณฑ์ประเมินไซเบอร์สำนักงานปลัดกระทรวงสาธารณสุข

ปีงบประมาณ 2569

02.

ตัวชี้วัด

ร้อยละของหน่วยงานที่ผ่านเกณฑ์มาตรฐานความมั่นคง

ปลอดภัยไซเบอร์ระดับสูง เป้าหมายร้อยละ 100

03.

R9 Cyber Security Platform

CTMR : Cyber Threat Monitoring Response

04.

Cybersecurity จังหวัดสุรินทร์

Timeline และขอความร่วมมือเพื่อดำเนินการ

เกณฑ์ประเมินไซเบอร์สำนักงานปลัดกระทรวงสาธารณสุข 2569

(Cybersecurity Technical Asessment Matrix Plus : CTAM +)

1. **Backup**
   การสำรองข้อมูลเก็บไว้ที่อื่น เพื่อให้สามารถใช้เพื่อกู้คืนข้อมูลเดิมหลังจากเหตุการณ์ข้อมูลสูญหาย
2. **Antivirus Software**
   โปรแกรมป้องกันไวรัส หรือ แอนติไวรัส คอยตรวจจับป้องกัน และกำจัดโปรแกรมคุกคามทางคอมพิวเตอร์
3. **Acess Control**
   การควบคุมอุปกรณ์หรือการเข้าถึงระบบผ่านทางช่องทาง Public/Private ทั้งภายในประเทศและต่างประเทศ
4. **Privileged Access Management (PAM)**
   การรักษาความปลอดภัยของข้อมูล ติดตาม ตรวจหา และป้องกันการใช้สิทธิ์การเข้าถึงทรัพยากรที่สำคัญ
5. **Business Continuity Plan (BCP) Disaster Recovery Plan (DRP)**
   แผนที่กำหนดแนวทางการดำเนินการของหน่วยงาน เมื่อเกิดสภาวะวิกฤต
6. **OS Patching**
   การซ่อมแซมจุดบกพร่องของระบบปฏิบัติการ (OS)หรือปรับปรุงระบบปฏิบัติการให้ทันสมัย
7. **Multi-Factor Authentication (2FA)**
   การยืนยันตัวตน 2 ชั้น เป็นการเข้าสู่ระบบบัญชีแบบ หลายขั้นตอน
8. **Web Application Firewall (WAF)**
   ระบบป้องกันการโจมตีทางไซเบอร์สำหรับเว็บแอพพลิเคชั่นโดยเฉพาะ
9. **Log Management**
   จัดเก็บ Log การใช้งานให้เป็นไปตาม พ.ร.บ. คอมพิวเตอร์ฯ อย่างน้อย 90 วัน
10. **Security Information & Even Management (SIEM)**
    มีระบบวิเคราะห์และตรวจจับภัยคุกคามจาก log ของ Server
11. **Vulnerability Assessment (VA Scan)**
    สแกนหาช่องโหว่ประจำปี และดำเนินการปิดช่องโหว่ให้ได้ตามมาตรฐาน

+

01 สำรวจและปิดระบบงานที่ไม่ได้ใช้งานเพื่อป้องกันการเข้าถึงข้อมูล

02 อัปเดตซอฟต์แวร์หรือแพตช์ ด้านความปลอดภัยอยู่เสมอ

03 Network Segmentation การแบ่งแยกเครือข่ายระบบสำคัญ ออกจากเครือข่ายระบบอื่น

04 ใช้ซอฟต์แวร์ถูกลิขสิทธิ์

05 Penetration Testing ทดสอบเจาะระบบสำคัญ หรือ ที่มีความเสี่ยง และแก้ไขช่องโหว่หรือความเสี่ยงนั้น

06 มีนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล รวมถึง การส่งเสริมให้เกิดการพัฒนาบุคลากรด้านดังกล่าว

ตัวชี้วัด

ไตรมาส 1

โรงพยาบาลระดับ M1, S และ A ผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสูง **ร้อยละ 80**

รอบ 3 เดือน

รอบ 6 เดือน

ไตรมาส 2

สำนักงานสาธารณสุขจังหวัด และสำนักงานเขตสุขภาพ ผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสูง **ร้อยละ 80**

รอบ 9 เดือน

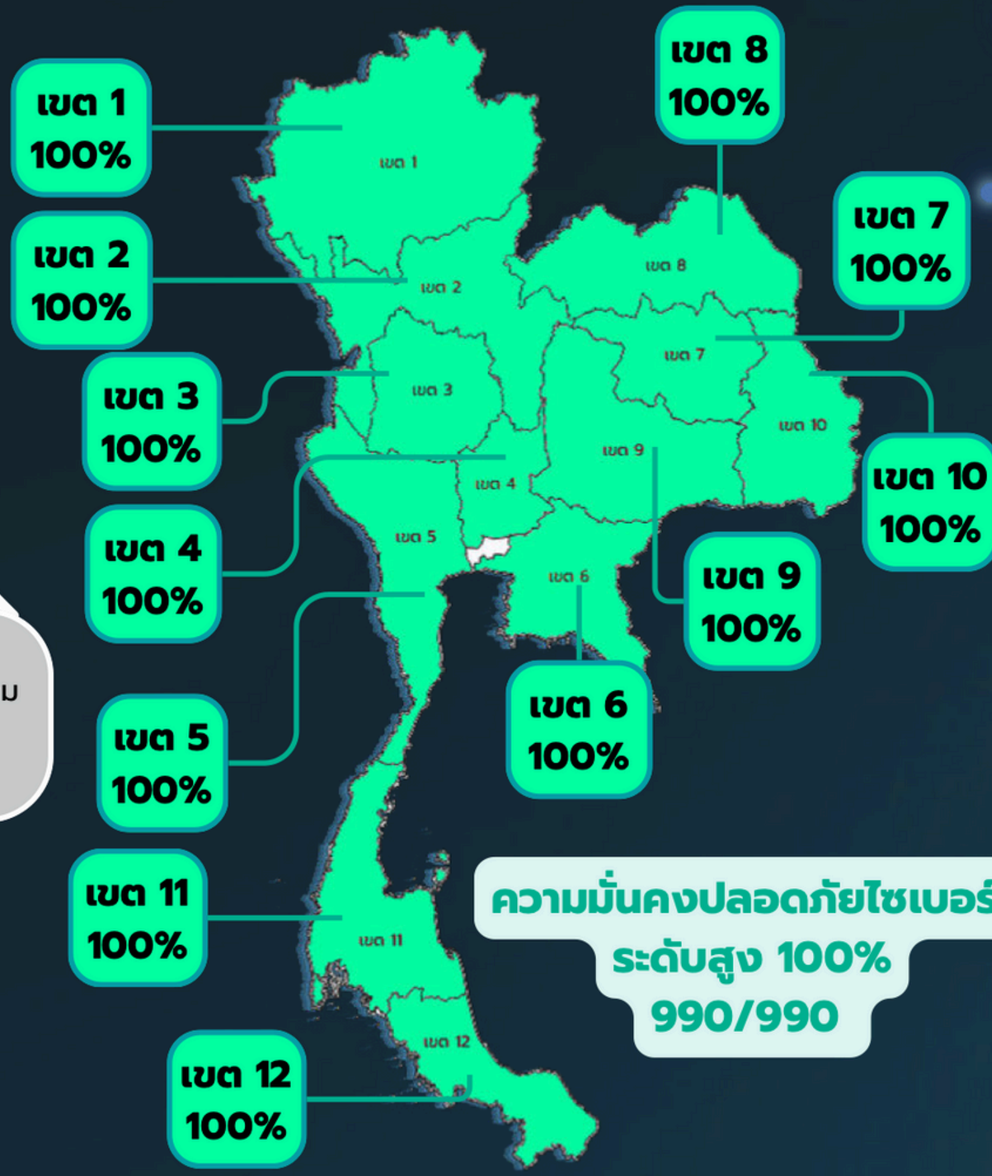
ไตรมาส 3

โรงพยาบาลชุมชน ผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสูง **ร้อยละ 80**

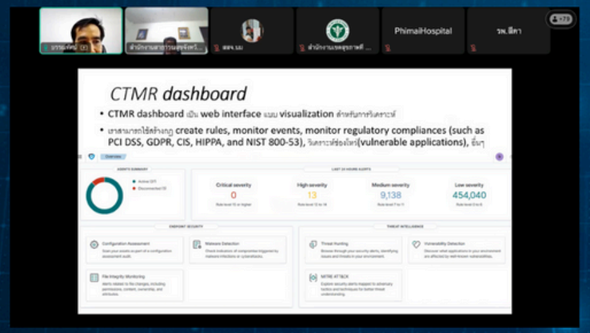
รอบ 12 เดือน

ไตรมาส 4

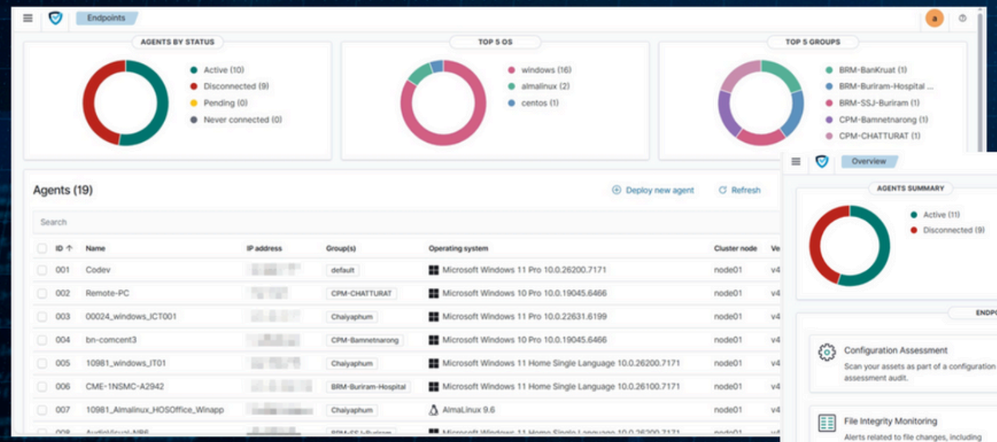
หน่วยงาน ผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสูง **ร้อยละ 100**



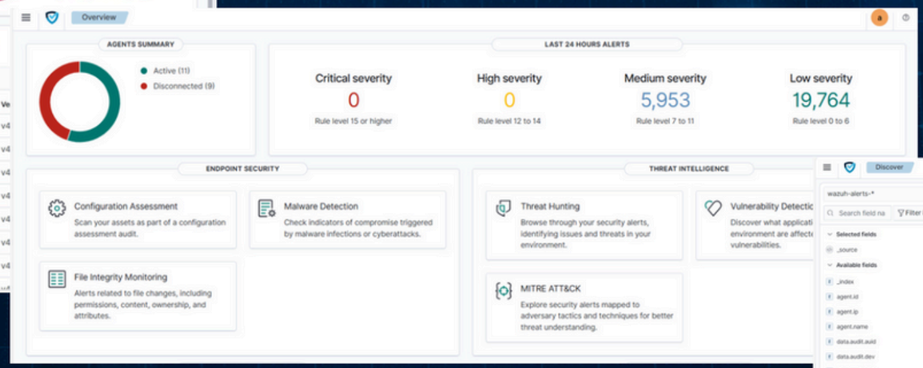
Cyber Security Platform CTMR



มีการประชุมแนะนำการติดตั้งระบบ Cyber Security CTMR
เมื่อวันที่ 25/11/2568



Dashdoard แสดงอุปกรณ์เชื่อมต่อ
ทุกจังหวัด



ภาพรวมความเสี่ยงด้านไซเบอร์

รายละเอียดความเสี่ยง

Cyber Security Platform

Cyber Security CTMR

- **SIEM**
  Security information and event management
- **XDR**
  Extended Detection and Response
- **Antivirus**
  Full interface protection with Windows Security and ClamAV, Update, Scan, and Action
- **Log Management**
  Build for log centerise integrated with firewall, OS, Antivirus
- **VA Scan**
  Build for Vulnerability of your environment
- **Report**
  Create a report to use as evidence
- **API**
  API command set for connecting to AI module
- **WAF + OWASP CRS**
  Comprehensive Protection for All Types of Web Servers
- **SOAR**
  Security Orchestration, Automation, and Response
- **Agent AI**
  Analyze the summary, interpret the issues, and suggest corrective actions.

จังหวัดที่สนใจเข้าร่วม Cyber Security CTMR

CTAM TO CTMR
Checklist

1. RED

- [ ] Backup
- [x] Antivirus Software
- [x] Access Control (Public and Private)
- [x] Privileged Access Mnagement (PAM) - 2FA, MFA

2. YELLOW

- [ ] Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)
- [ ] OS Patching
- [x] Multi-Factor Authentication (MFA)
- [x] Web Application Firewall (WAF)
- [x] Log Management
- [x] SIEM
- [x] VA Scan

3. GREEN

- [ ] Software Update
- [x] Pen-Test
- [ ] DR Site

วงเงินงบประมาณ

53,500 บาท / โรงพยาบาล / ปี
(ราคารวมภาษีมูลค่าเพิ่ม) ไม่รวม **Cloud Server**

จังหวัดนครราชสีมา

- 53,500 x 36 = **1,926,000 บาท ต่อปี**

จังหวัดชัยภูมิ

- 53,500 x 17 = **909,500 บาท ต่อปี**

จังหวัดบุรีรัมย์

- 53,500 x 24 = **1,284,000 บาท ต่อปี**

จังหวัดสุรินทร์

- 53,500 x 18 = **963,000 บาท ต่อปี**

รวมค่าใช้จ่ายทั้งหมด 5,082,500 บาท

Cyber Security Platform CTMR

(อยู่ระหว่างการประเมินเครื่องคอมพิวเตอร์)

ส่งข้อมูลแล้ว **98** เครื่อง

จังหวัดนครราชสีมา

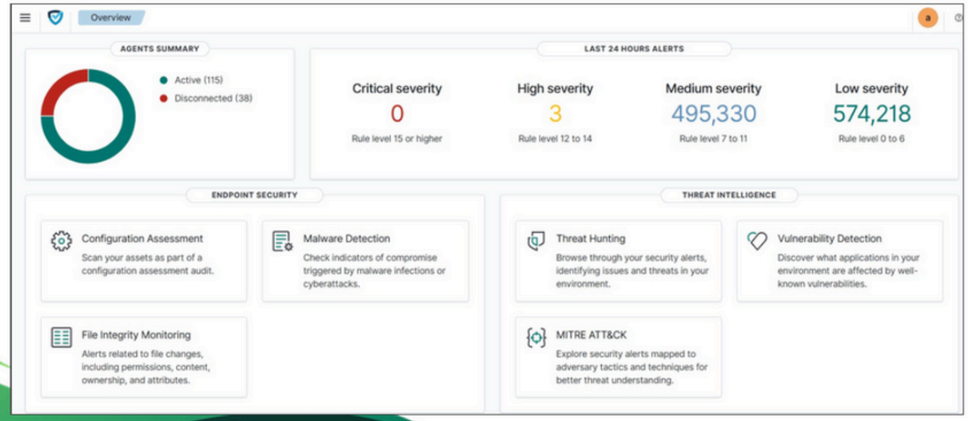
- ส่งข้อมูลแล้ว **82** เครื่อง

จังหวัดชัยภูมิ

- ดำเนินการแล้ว **15** เครื่อง

จังหวัดบุรีรัมย์

- ดำเนินการแล้ว **1** เครื่อง



เหตุการณ์สำคัญ

การเข้าจาก IP ภายนอก

- Source IP: 61.19.30.xxx
- ประเทศ: Thailand
- User ที่ Login: root

รูปแบบเหตุการณ์

- พยายามใส่รหัสผ่านผิดหลายครั้งแล้ว Login สำเร็จด้วยรหัสผ่านจริง

เวลาเกิดเหตุ

- 21 ม.ค. 2026 เวลา ~18:08 น.

Rule ที่แจ้ง

- Multiple authentication failures followed by a success

สรุปเหตุการณ์สำคัญ

- IT สสจ.นครราชสีมา มีรับมือการเข้าระบบจากการใส่รหัสผ่านผิดหลายครั้ง

มาตรการแก้ไขเร่งด่วน (Immediate Action)

1. ปิดการเข้าใช้งานระบบด้วยบัญชี root ผ่าน SSH
2. เปลี่ยนรหัสผ่านบัญชีผู้ดูแลระบบทั้งหมด
3. ตรวจสอบระบบย้อนหลัง user / process / cron / log ว่ามีความผิดปกติหรือไม่

CYBERSECURITY จังหวัดสุรินทร์

การขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ จังหวัดสุรินทร์

ปีงบประมาณ 2569

ก.พ.
2569

ส่งหลักฐานการประเมิน CTAM+

- โรงพยาบาลจัดส่งเอกสารหลักฐาน มาที่ สสจ.
- คณะกรรมการ CISO ประชุมพิจารณาตามเกณฑ์
- ส่งคณะกรรมการ CISO ระดับเขต ฯ พิจารณา

ก.พ.
2569

สำรวจและติดตั้ง CTMR

- สำรวจจำนวนเครื่องคอมพิวเตอร์ทั้งหมด
- ดำเนินการติดตั้ง Agent
- อบรมการใช้งานระบบ

มี.ค.
2569

จัดตั้ง Response Team

- จัดทำทำเนียบบุคลากร ที่มีความรู้ ความสามารถ หรือผ่านการอบรมเกี่ยวกับ Cybersecurity ระดับสูง
- จัดตั้ง Response ทีมระดับจังหวัด
- จัดทำกระบวนการ Monitoring & Response

ประเด็นขอความร่วมมือ
โรงพยาบาลทุกแห่ง

ส่งเอกสารและหลักฐาน CTAM+

- ประสานบริษัท ขอเอกสารและหลักฐาน
- ส่งมาที่ Email : spho.digitalhealth@moph.go.th
- ภายในวันที่ 15 กุมภาพันธ์ 2569
- แจ้งผู้ประสาน : นายรัชมงคล พุ่มคุ้ม โทร 085 910 2241

กรอกข้อมูล และติดตั้ง CTMR

- กรอกข้อมูลจำนวนเครื่องคอมพิวเตอร์ของโรงพยาบาล
- ดำเนินการติดตั้ง Agent
- ผู้ประสาน : นายรัชมงคล พุ่มคุ้ม โทร 085 910 2241

THANKYOU

ขอบคุณครับ

BACKUP

ข้อมูลเพิ่มเติม

กลไกการดำเนินการ

01. หน่วยงานดำเนินการให้ระบบเครือข่ายคอมพิวเตอร์และสารสนเทศตามเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ และประเมินตนเอง หรือให้ผู้เชี่ยวชาญที่เป็นผู้ตรวจประเมิน

02. มีคณะทำงานดำเนินงานความมั่นคงปลอดภัยไซเบอร์ในระดับจังหวัด ทำหน้าที่ให้ความช่วยเหลือหน่วยงานในพื้นที่ โดยมีคณะทำงานระดับเขตสุขภาพ เป็นเครือข่ายกำกับดูแลหน่วยงานในพื้นที่

03. ส่งผลการประเมินมาให้ ศทส.สป.สธ. ที่ แบบฟอร์มการประเมินระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ (CTAM+ : Cybersecurity Technical Assessment Matrix Plus) ปี 2569 **https://moph.link/9X8aC_WaV** ทุกวันพฤหัสบดี หรือ ช่องทางอื่นตามที่ ศทส.สป.สธ. แจ้งเพิ่มเติม

04. ศทส.สป.สธ. จะยืนยันผลการประเมินของหน่วยงานทุกศุกร์โดยแสดงผลที่ https://ict.moph.go.th/th/extension/1763

คู่มือการตรวจประเมินระดับการรักษาความมั่นคงปลอดภัยไซเบอร์
Cybersecurity Technical Assessment Matrix Plus : CTAM+

SCAN HERE

https://moph.link/Rw3I2-gYI

คู่มือการตรวจประเมินระดับการรักษาความมั่นคงปลอดภัยไซเบอร์

คู่มือสำหรับประเมินมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานสาธารณสุข โดยกำหนดเกณฑ์ที่ทุกหน่วยงานต้องทำให้ครบเพื่อ “ผ่านมาตรฐานระดับสูง” จุดประสงค์หลักคือให้หน่วยงานสามารถป้องกัน ตรวจจับ และรับมือเหตุการณ์ทางไซเบอร์ได้อย่างมีประสิทธิภาพ