การเชื่อมต่อเครือข่ายแลกเปลี่ยนข้อมูลข่าวกรองด้านภัยคุกคามทางไซเบอร์

(Malware Information Sharing Platform : MISP)

กลุ่มงานสุขภาพดิจิทัล

การเชื่อมต่อ MISP กับ สกมช. เพื่อภูมิคุ้มกันไซเบอร์ไทย

การเปลี่ยนแปลงสู่ระบบดิจิทัลทำให้ภัยคุกคามทางไซเบอร์ทวีความรุนแรงขึ้น สกมช. จึงพัฒนาแพลตฟอร์ม MISP
เพื่อเป็นศูนย์กลางการแลกเปลี่ยนข้อมูลภัยคุกคาม (Threat Intelligence) ช่วยให้องค์กรสามารถรับมือและป้องกันภัยไซเบอร์ได้อย่างทันท่วงที

ความท้าทายและบทบาทของแพลตฟอร์ม MISP

- **ภัยคุกคามไซเบอร์กวีความรุนแรงและซับซ้อน**



การเติบโตของเว็บและแอปพลิเคชันเพิ่มช่องโหว่
ที่ส่งผลกระทบต่อความมั่นคงและเศรษฐกิจ

- **MISP ศูนย์กลางแลกเปลี่ยนข้อมูลภัยคุกคาม**



MISP Platform

แพลตฟอร์มรวมรวม วิเคราะห์ และส่งต่อ Threat
Intelligence อย่างเป็นระบบและมีบาตรฐาน



ประโยชน์หลักของการเชื่อมต่อกับ MISP

- **รับการแจ้งเตือนล่วงหน้าและตอบสนองเชิงรุก**



เข้าถึงข้อมูลภัยคุกคามล่าสุดเพื่อป้องกันและแก้ไข
สถานการณ์ได้ทันท่วงที

- **ยกระดับความร่วมมือและพัฒนาทักษะบุคลากร**



แลกเปลี่ยนข้อมูลกับเครือข่ายความปลอดภัยไซเบอร์
เพื่อสร้างภูมิคุ้มกันที่แข็งแกร่งอย่างยั่งยืน

Gemini Notebook

1.หน่วยงานแจ้งความพร้อม
แจ้งชื่อหน่วยงาน จังหวัด
ชื่อ-สกุล ตำแหน่ง เบอร์โทร
อีเมลของผู้ปฏิบัติไปที่
health-cirt@moph.go.th

3.ศทส..ตรวจสอบข้อมูล
และเอกสารที่เกี่ยวข้อง
เพื่อยืนยันความครบถ้วน
และแจ้งกลับหน่วยงาน

5.ศทส.ทำการทดสอบ
การเชื่อมต่อระบบMISP
ระหว่างหน่วยงานกับศทส.
เพื่อให้แน่ใจว่าสามารถทำงาน
ได้อย่างถูกต้องและปลอดภัย



2.ศทส.ติดต่อกลับทางอีเมล
พร้อมจัดส่งแบบฟอร์มให้
กรอกข้อมูลและรายละเอียด
ที่จำเป็นต้องจัดเตรียม เช่น
การตั้งค่าเครือข่ายและระบบ
เฝ้าระวัง รักษาความปลอดภัยฯ

4.หน่วยงานจัดส่งauth key
และIP PublicของระบบMISP
ที่จะใช้ในการเชื่อมต่อ
กลับทางอีเมล

6.ทดสอบ
การเชื่อมต่อเรียบร้อย
และระบบทำงานได้
จึงถือว่าเสร็จสิ้น