MINISTRY OF AGRICULTURE AND COOPERATIVES

Cyber Security

Protecting Our Organization

ความก้าวหน้าของเทคโนโลยีในปัจจุบัน

เทคโนโลยีดิจิทัลที่มีการเปลี่ยนแปลงอย่างรวดเร็ว

- Cloud Computing
- Artificial Intelligence (AI)
- Internet of Things (IoT)
- Mobile Application
- Big Data & Analytics
- Smart Devices
- 5G Network
- Remote Working / Work From Anywhere

สาเหตุที่ทำให้เกิดภัยคุกคามทางไซเบอร์

ปัจจัยสำคัญที่ทำให้เกิดภัยคุกคาม

- การใช้งานอินเทอร์เน็ตอย่างแพร่หลาย
- การเก็บข้อมูลสำคัญในรูปแบบดิจิทัล
- การเชื่อมต่ออุปกรณ์จำนวนมาก
- การใช้งานระบบออนไลน์ตลอดเวลา
- ผู้ใช้งานขาดความตระหนักด้าน Cyber Security
- อาชญากรไซเบอร์มีเครื่องมือโจมตีที่ทันสมัยมากขึ้น

สาเหตุที่ทำให้เกิดภัยคุกคามทางไซเบอร์

ปัจจัยสำคัญที่ทำให้เกิดภัยคุกคาม

- การใช้งานอินเทอร์เน็ตอย่างแพร่หลาย
- การเก็บข้อมูลสำคัญในรูปแบบดิจิทัล
- การเชื่อมต่ออุปกรณ์จำนวนมาก
- การใช้งานระบบออนไลน์ตลอดเวลา
- ผู้ใช้งานขาดความตระหนักด้าน Cyber Security
- อาชญากรไซเบอร์มีเครื่องมือโจมตีที่ทันสมัยมากขึ้น

เป้าหมายของผู้โจมตี

- ขโมยข้อมูล
- เรียกค่าไถ่
- หลอกลวงทางการเงิน
- ทำลายระบบ
- แอบเข้าควบคุมระบบองค์กร

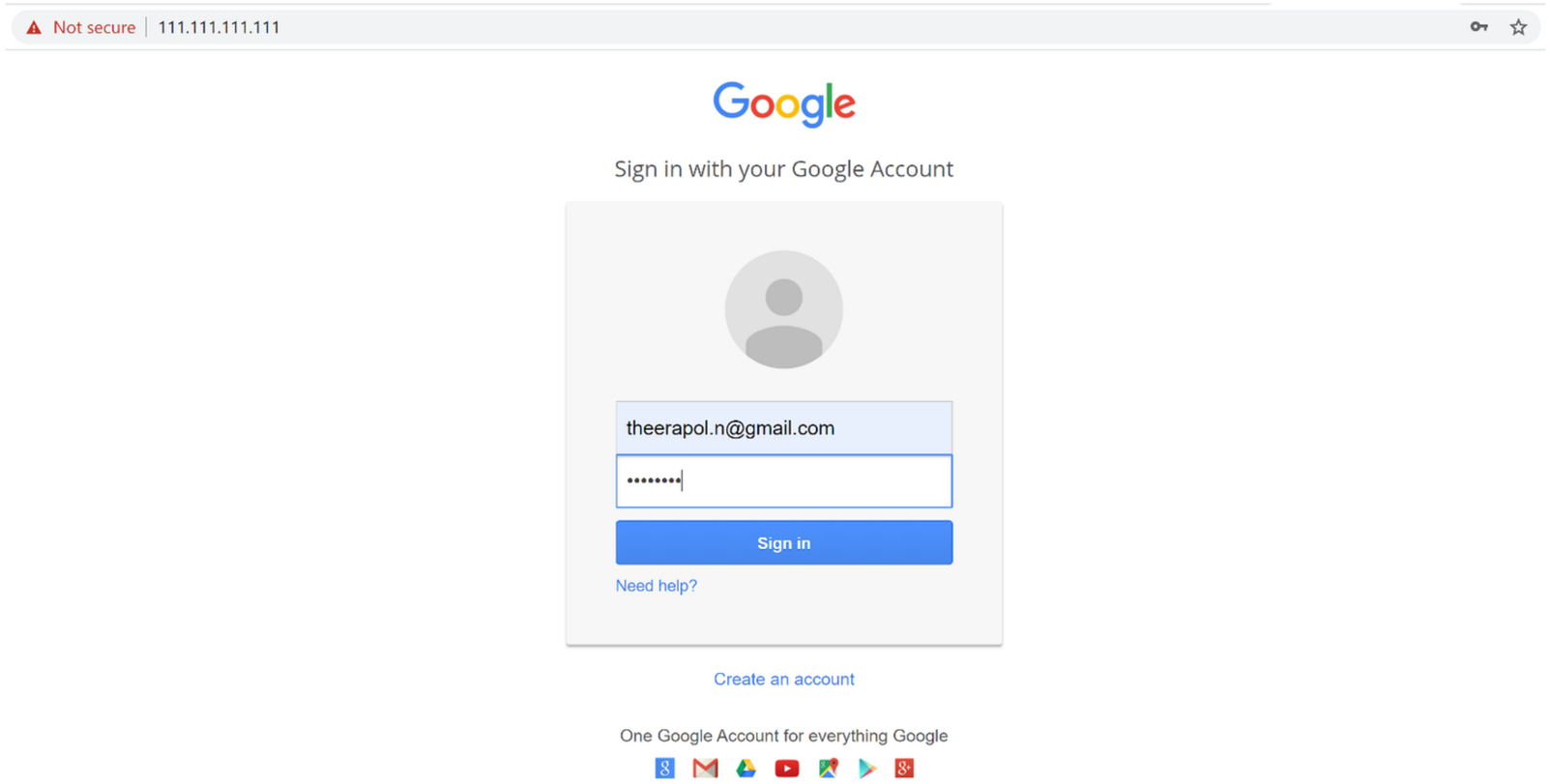
ตัวอย่างภัยคุกคามทางไซเบอร์

- **มัลแวร์ (Malware)** คือ ซอฟต์แวร์ที่ถูกสร้างขึ้นเพื่อทำอันตรายต่อระบบคอมพิวเตอร์ ข้อมูล
- **อีเมลหรือข้อความหลอกลวง (Phishing&Social Engineering)** เป็นการแอบอ้างหน่วยงานหรือผู้บังคับบัญชาขโมยรหัสผ่านและข้อมูล
- **การกระทำโดยบุคคลภายใน (Insider Threat)** คือ การขโมยข้อมูล หรือการโจมตีจากบุคคลภายใน
- **แรนซัมแวร์ (Ransomware)** เป็นการเข้ารหัสไฟล์ทั้งหมด เรียกเงินเพื่อปลดล็อก
- **DNS Spoofing / DNS Poisoning** คือ การเปลี่ยน DNS ให้ผู้ใช้เข้าเว็บไซต์ปลอม
- **DDoS (Distributed Denial of Service)** คือการโจมตีด้วยวิธีการสร้าง Traffic จำนวนมากใส่ระบบทำให้ระบบหยุดการให้บริการ

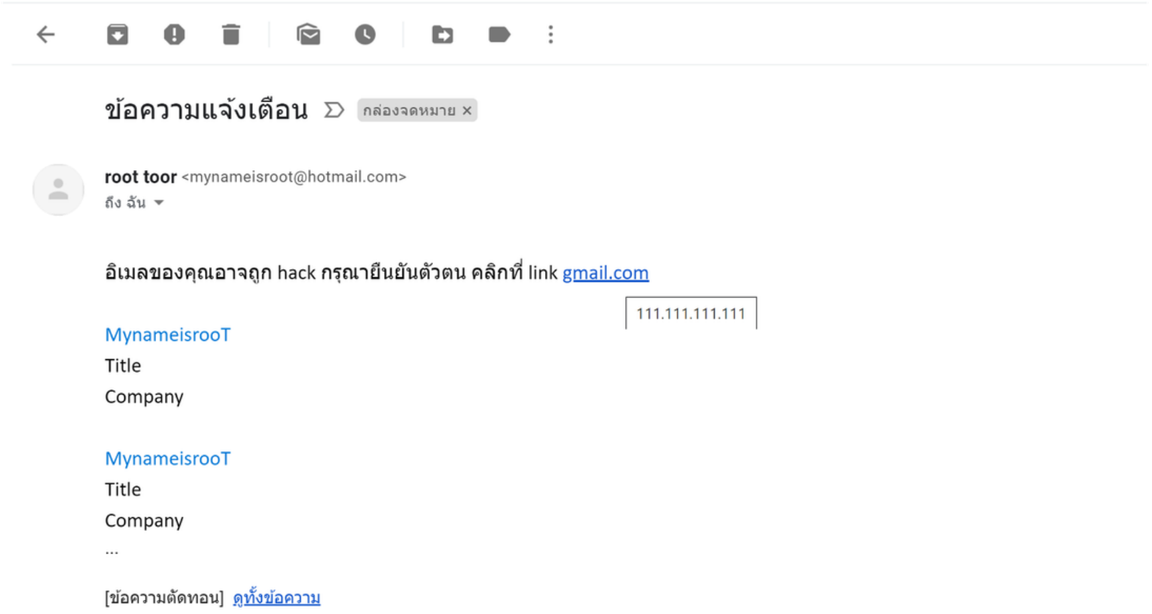
ตัวอย่างภัยคุกคามทางไซเบอร์

- **Man-in-the-Middle (MITM)** คือ การดักรับข้อมูลระหว่างผู้ใช้งานกับเครื่องคอมพิวเตอร์แม่ข่าย
- **การเดารหัสผ่าน (Credential Attack)** คือ การเดารหัสผ่านของผู้ใช้จนกว่าจะได้รหัสผ่านที่ถูกต้อง
- **Advanced Persistent Threat (APT)** คือ การโจมตีที่ฝังหรือแอบอยู่ในระบบเพื่อขโมยข้อมูลโดยอาจแอบอยู่ในระบบนานเป็นเดือน/ปี
- **SQL Injection** คือ การเจาะฐานข้อมูล ดำเนินการแก้ไข หรือ ลบ ข้อมูลในฐานข้อมูล
- **Zero-Day Attack** คือ การโจมตีช่องโหว่ที่ยังไม่มี patch ของซอฟต์แวร์ หรือระบบปฏิบัติการนั้น ๆ
- **Session Hijacking** คือ การขโมย Session login ของผู้ใช้

ตัวอย่างภัยคุกคามทางไซเบอร์



ตัวอย่างภัยคุกคามทางไซเบอร์



ข้อความแจ้งเตือน กล่องจดหมาย ×

root toor <mynameisroot@hotmail.com>
ถึง ฉัน

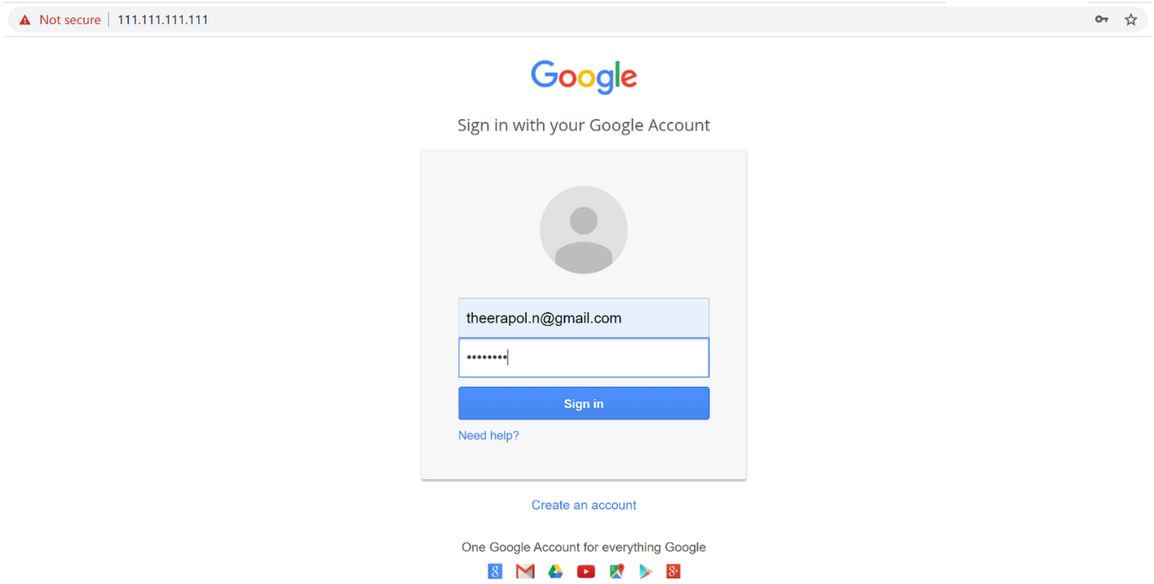
อิเมลของคุณเอาจถูก hack กรุณายืนยันตัวตน คลิกที่ link gmail.com

111.111.111.111

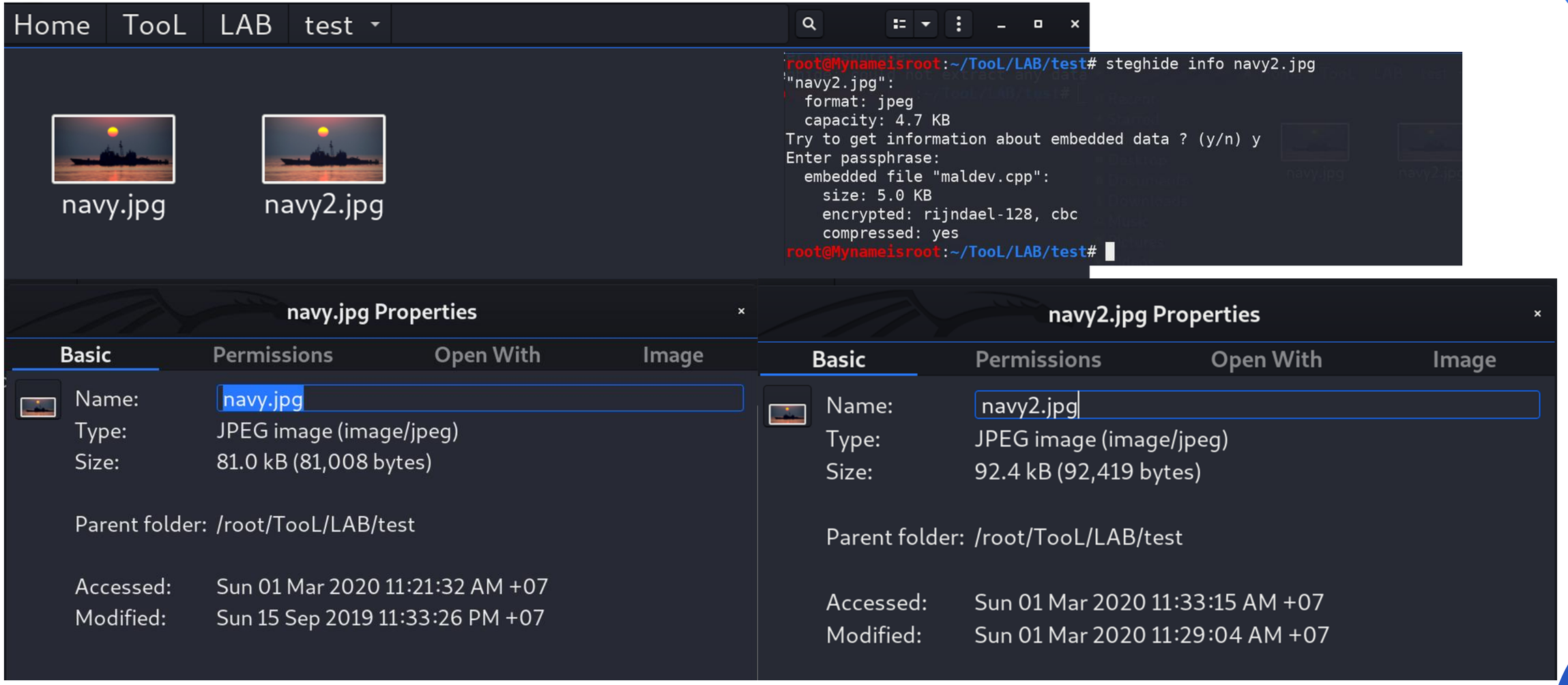
MynameisrooT
Title
Company

MynameisrooT
Title
Company
...

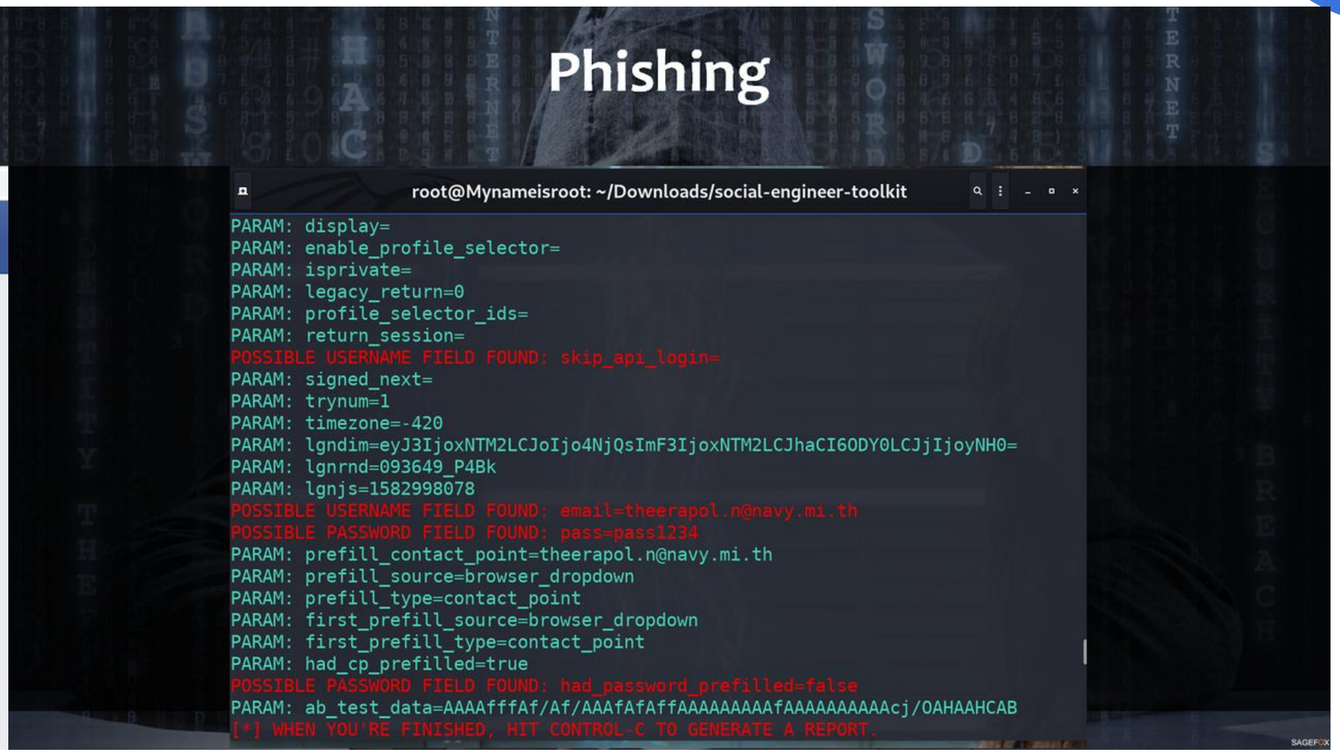
[ข้อความตัดทอน] ดูทั้งข้อความ



ตัวอย่างภัยคุกคามทางไซเบอร์

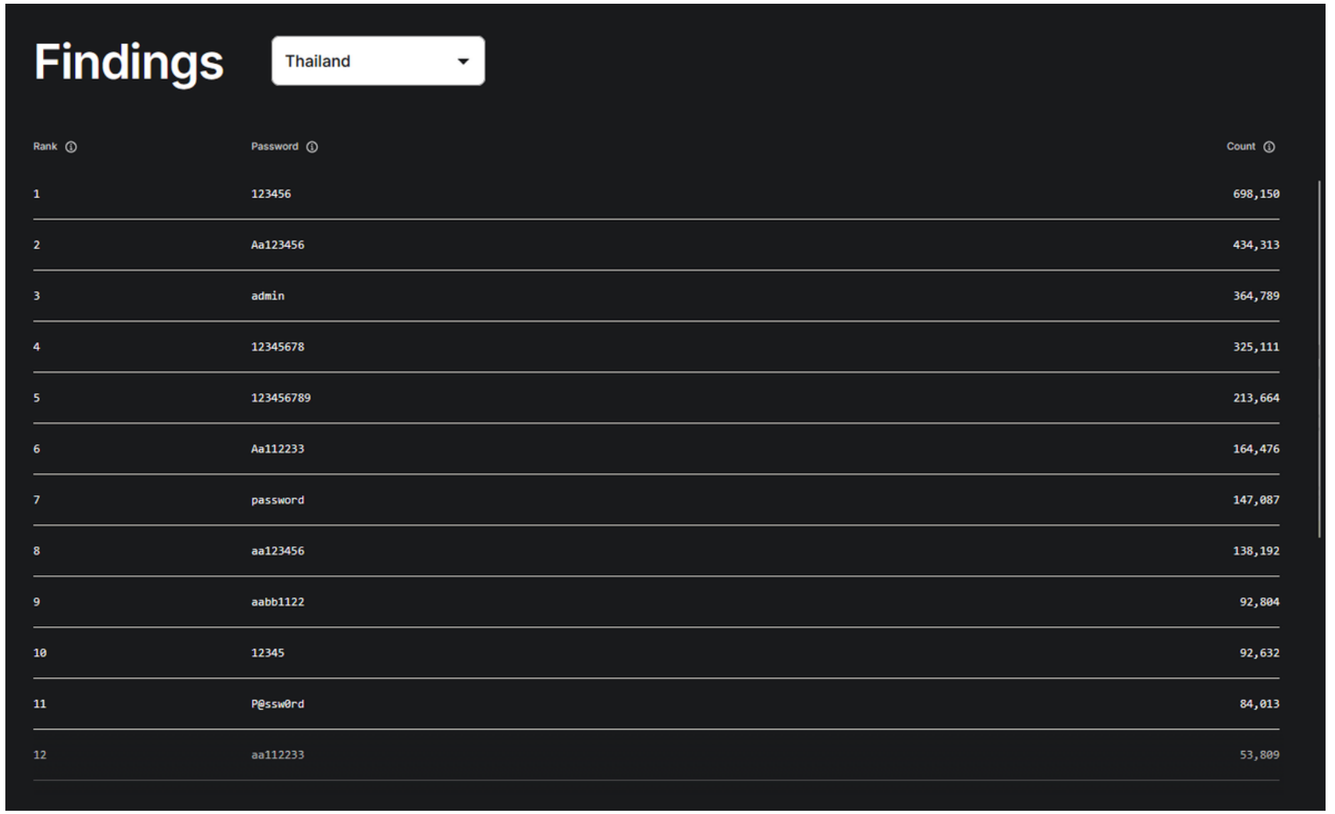


ตัวอย่างภัยคุกคามทางไซเบอร์



ตัวอย่างภัยคุกคามทางไซเบอร์

https://nordpass.com/most-common-passwords-list/

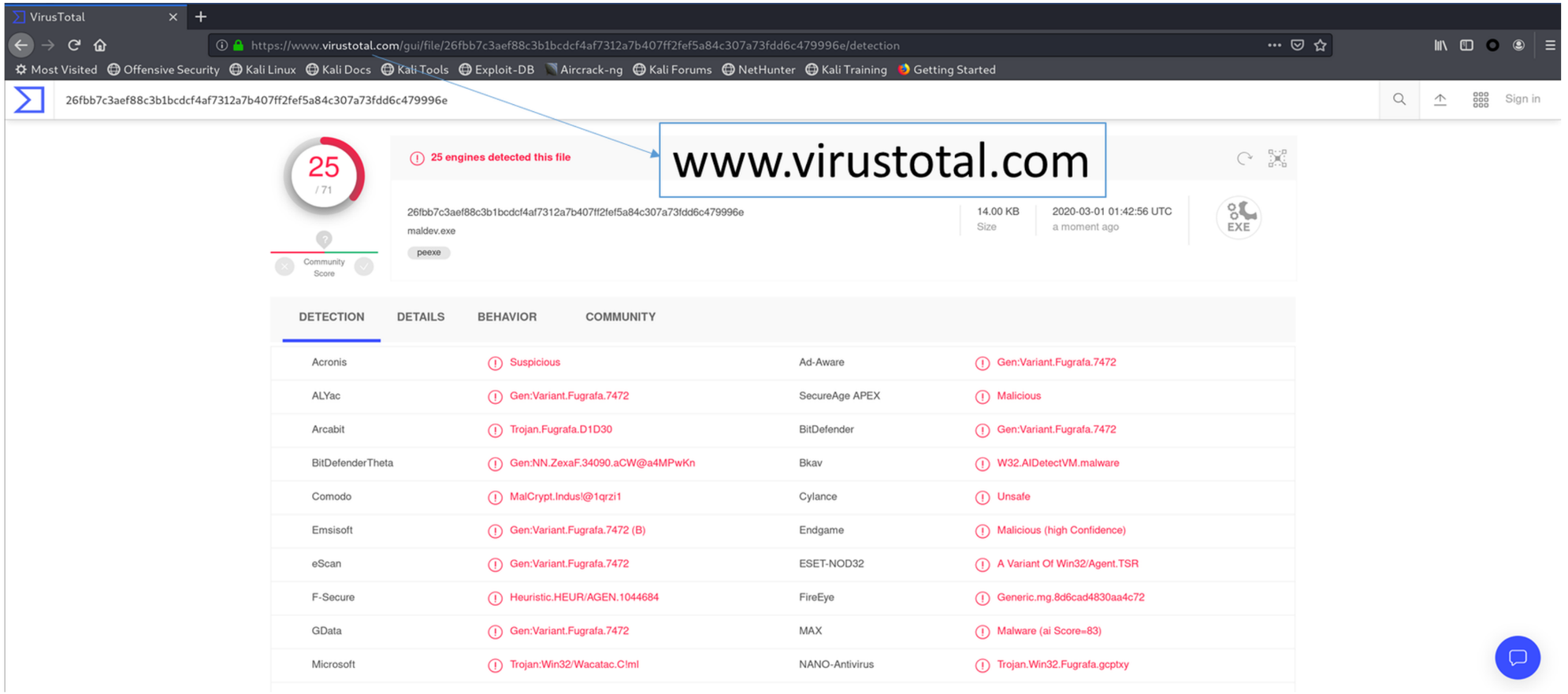


Findings

Thailand

Rank	Password	Count
1	123456	698,150
2	Aa123456	434,313
3	admin	364,789
4	12345678	325,111
5	123456789	213,664
6	Aa112233	164,476
7	password	147,087
8	aa123456	138,192
9	aabb1122	92,804
10	12345	92,632
11	P@ssw0rd	84,013
12	aa112233	53,809

ตัวอย่างภัยคุกคามทางไซเบอร์



สรุปสถานะการณ์ภัยคุกคามทางไซเบอร์

ที่มา: HTTPS://WWW.FACEBOOK.COM/NCSA.THAILAND/POSTS/-เปิดสถิติ-3485-สถานการณ์ภัยคุกคามทางไซเบอร์ในห้วงที่ผ่านมา-มีภัยรูปแบบใดบ้าง-น้/1152916677029996/

ข้อควรระวัง

1. ไม่ใช้คอมพิวเตอร์โดยไม่ระวัง
2. ไม่ตั้งรหัสผ่านที่ง่ายต่อการคาดเดา
3. ไม่ใช้คอมพิวเตอร์โดยไม่สังเกตความเปลี่ยนแปลง
4. ไม่ใช้งานคอมพิวเตอร์โดยไม่อัพเดท
5. ไม่ลงซอฟต์แวร์มากเกินความจำเป็น
6. ไม่ควรเข้าเว็บไซต์เสี่ยงภัย

ข้อควรระวัง


ไม่ปฏิบัตินอกเหนือกฎหมาย เกี่ยวกับการใช้งานอินเตอร์เน็ต
7
8
ไม่หลงเชื่อโดยง่าย
ไม่ทำธุรกรรมออนไลน์โดยไม่สังเกต สัญลักษณ์ความปลอดภัย
9
10
ไม่ใช้เปิดเผยข้อมูลส่วนตัวลงบน โซเชียลเน็ตเวิร์ก
ไม่มีอะไรได้มาฟรี ๆ
11
12
ไม่ตื่นตระหนก

ข้อควรระวัง

13 รหัสผ่านควรเป็นความลับ

14 ไม่หลงผิดไปกับสิ่งผิดกฎหมาย

15 เสพสื่ออย่างมีวิจารณญาณ

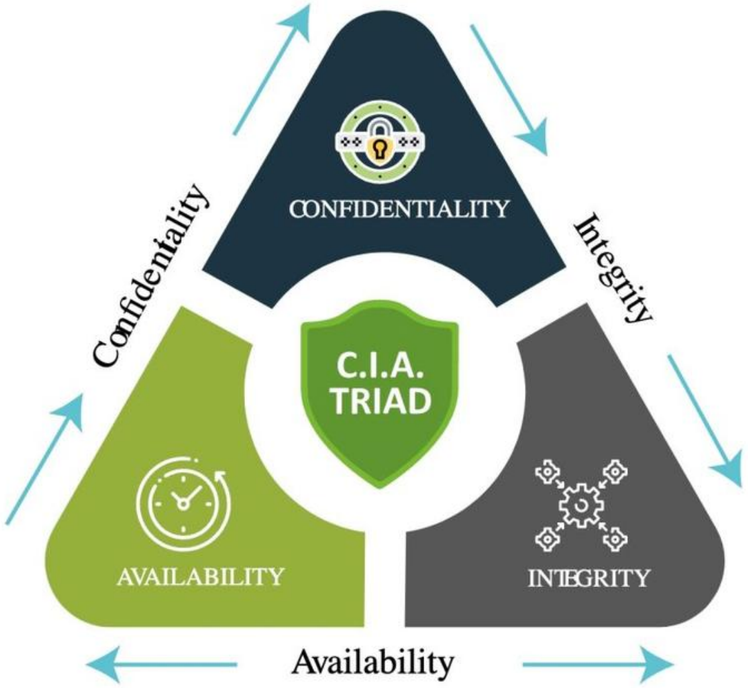
16 โพสต์สิ่งใดให้ทำด้วยความระมัดระวัง

17 แชร์ต่ออย่างมีสติ

18 รู้เท่าทันสื่อสังคมออนไลน์

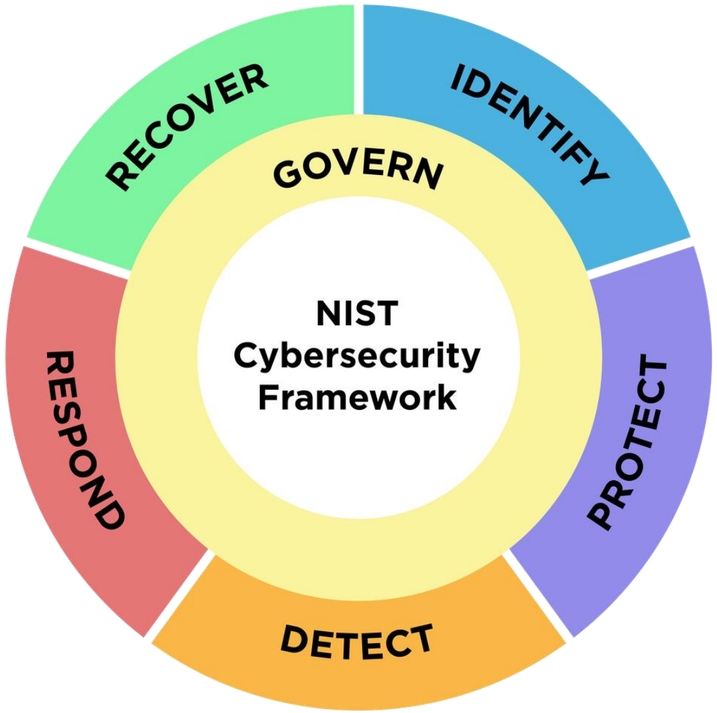
แนวคิดหลักในด้านความปลอดภัยไซเบอร์

- Confidentiality (การรักษาความลับ) หมายถึงการปกป้องข้อมูลหรือระบบให้สามารถเข้าถึงได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น
- Integrity (ความถูกต้องและความครบถ้วน) หมายถึงการป้องกันไม่ให้ข้อมูลหรือระบบถูกดัดแปลงแก้ไขโดยไม่ได้รับอนุญาต และการตรวจสอบให้แน่ใจว่าข้อมูลที่เก็บไว้หรือส่งต่อยังคงความถูกต้องและครบถ้วนเสมอ
- Availability (ความพร้อมใช้งาน) หมายถึงการทำให้ข้อมูลหรือระบบสามารถเข้าถึงและใช้งานได้เมื่อผู้ใช้ต้องการ



NIST Framework

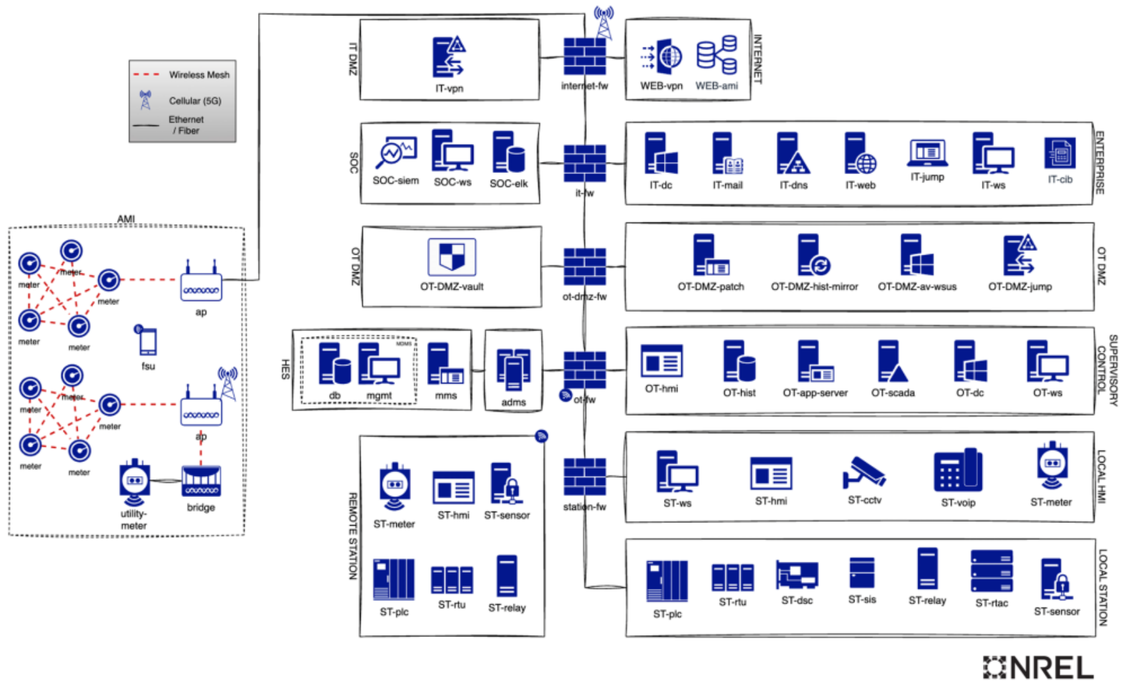
NIST Framework คือกรอบแนวทางด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ที่พัฒนาโดย National Institute of Standards and Technology (NIST) ของสหรัฐอเมริกา ใช้เป็น “มาตรฐานกลาง” สำหรับองค์กรในการป้องกัน ตรวจจับ และตอบสนองภัยคุกคามไซเบอร์



NIST Framework

1. Identify (ระบุความเสี่ยง)

- รู้ว่าองค์กรมีทรัพย์สินอะไร (Assets)
- วิเคราะห์ความเสี่ยง (Risk Assessment)
- กำหนดนโยบายความปลอดภัย



NIST Framework

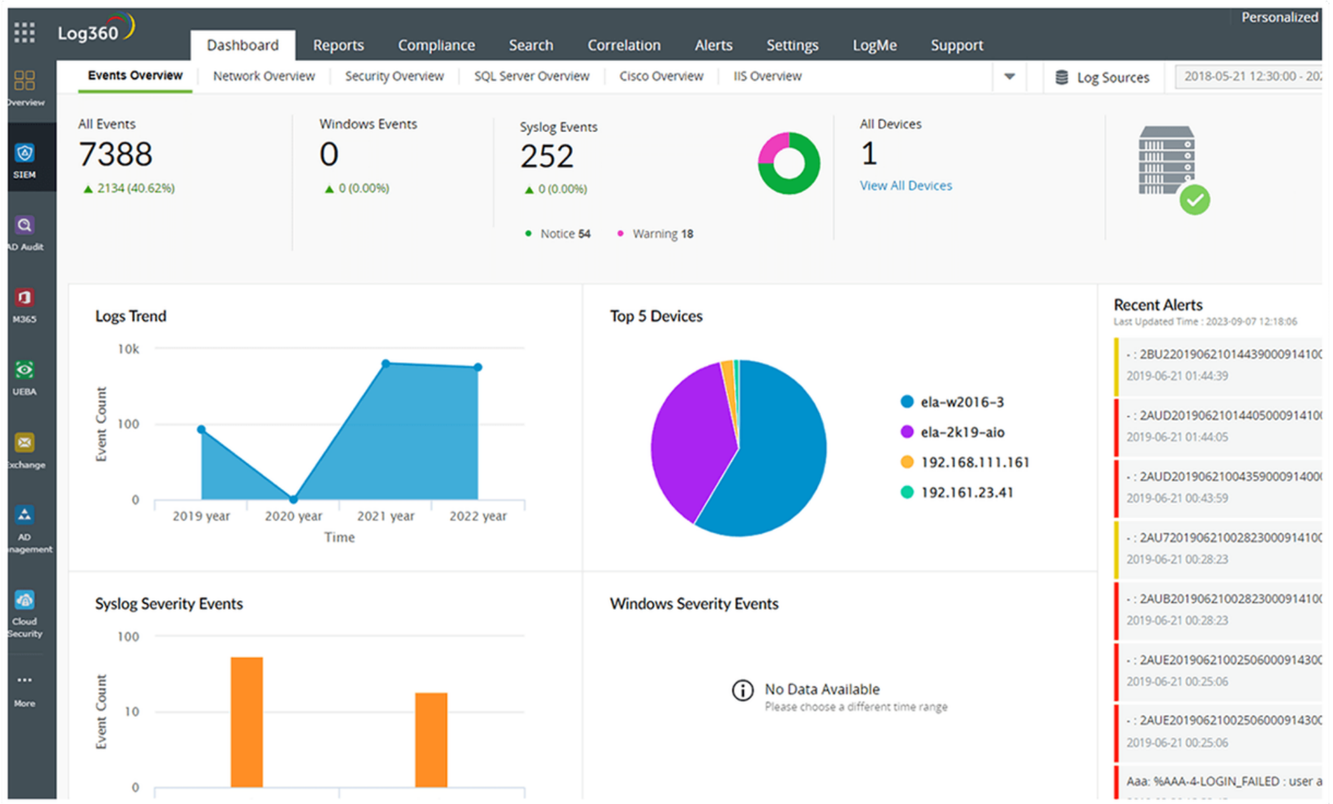
2. Protect (ป้องกัน)

- ควบคุมการเข้าถึง (Access Control)
- ใช้ MFA / Encryption
- Training ผู้ใช้งาน

NIST Framework

3. Detect (ตรวจจับ)

- ตรวจจับเหตุการณ์ผิดปกติ
- Monitoring / Logging



NIST Framework

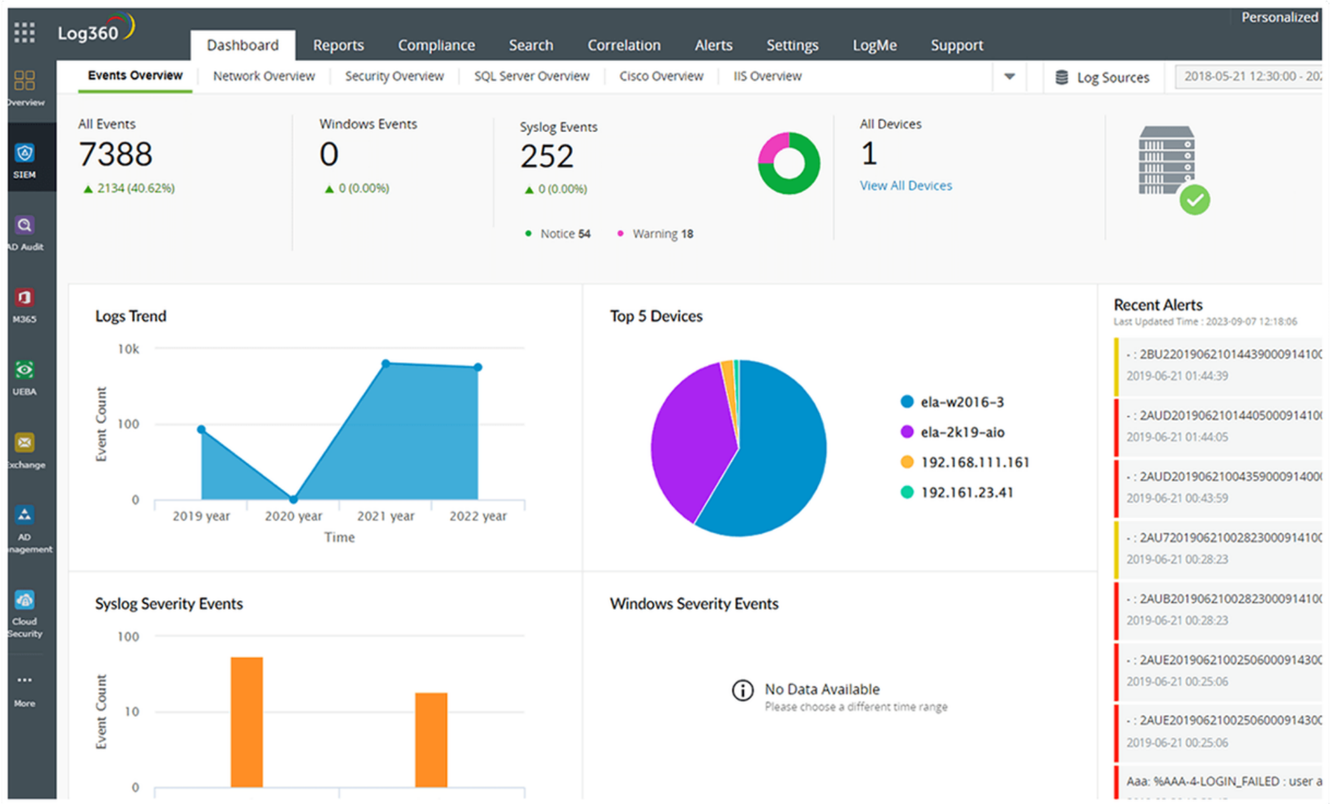
4. Respond (ตอบสนอง)

- มี Incident Response Plan
- แจ้งเตือน / แก้ไขปัญหา

NIST Framework

5. Recover (ฟื้นฟู)

- Backup / Restore
- Disaster Recovery Plan



ความสำคัญของ Cyber Security ต่อหน่วยงานรัฐ

- การปฏิบัติตามกฎหมาย
  - พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี 2550 และแก้ไขเพิ่มเติม ปี 2560
  - พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ ปี 2562
  - พรบ. คุ้มครองข้อมูลส่วนบุคคล ปี 2562
  - พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544, (ฉบับที่ 2) พ.ศ.2551 , (ฉบับที่ 3 และ 4) พ.ศ.2562

ความสำคัญของ Cyber Security ต่อหน่วยงานรัฐ

- มีการจัดเก็บข้อมูลที่มีความสำคัญตามภาระกิจ
  - ข้อมูลส่วนบุคคลของผู้รับบริการ
  - ข้อมูลที่ต้องจัดเก็บตามภาระกิจด้านต่าง ๆ

MINISTRY OF AGRICULTURE AND COOPERATIVES

ความสำคัญของ Cyber Security ต่อหน่วยงานรัฐ

- ภัยคุกคามทางไซเบอร์มีความซับซ้อนและต่อเนื่องมากขึ้น
- หน่วยงานรัฐเป็นเป้าหมายหลัก
- เกิดขึ้นจากความขัดแย้งระหว่างประเทศ
- ระบบสารสนเทศหลักเป็นเป้าหมายของสงครามไซเบอร์

บทสรุปการป้องกันภัยคุกคามไซเบอร์

- ปกป้องข้อมูลสำคัญขององค์กรและประชาชน
- ลดความเสี่ยงจากภัยคุกคามที่ซับซ้อนและเพิ่มขึ้นตลอดเวลา
- รักษาความต่อเนื่องของบริการ (Service Availability)
- สร้างความเชื่อมั่น (Trust) ให้กับผู้ใช้งาน
- ปฏิบัติตามกฎหมายและมาตรฐาน
- ลดความเสียหายทางการเงินและชื่อเสียง
- รองรับการพัฒนา Digital Transformation

Q&A

Thank you