



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
- ผู้ใช้งานขาดความตระหนักรู้ด้าน Cyber Security
- อาชญากรไซเบอร์มีเครื่องมือโจมตีที่ทันสมัยมากขึ้น



สาเหตุที่ทำให้เกิดภัยคุกคามทางไซเบอร์

ปัจจัยสำคัญที่ทำให้เกิดภัยคุกคาม

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

เป้าหมายของผู้โจมตี

- ขโมยข้อมูล
- เรียกค่าไถ่
- หลอกลวงทางการเงิน
- ทำลายระบบ
- แอบเข้าควบคุมระบบองค์กร

ตัวอย่างภัยคุกคามทางไซเบอร์

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

ตัวอย่างภัยคุกคามทางไซเบอร์

✓ **Man-in-the-Middle (MITM)** คือ การดักรับข้อมูลระหว่างผู้ใช้งานกับเครื่องคอมพิวเตอร์แม่ข่าย

✓ **SQL Injection** คือ การเจาะฐานข้อมูล ดำเนินการแก้ไข หรือ ลบ ข้อมูลในฐานข้อมูล

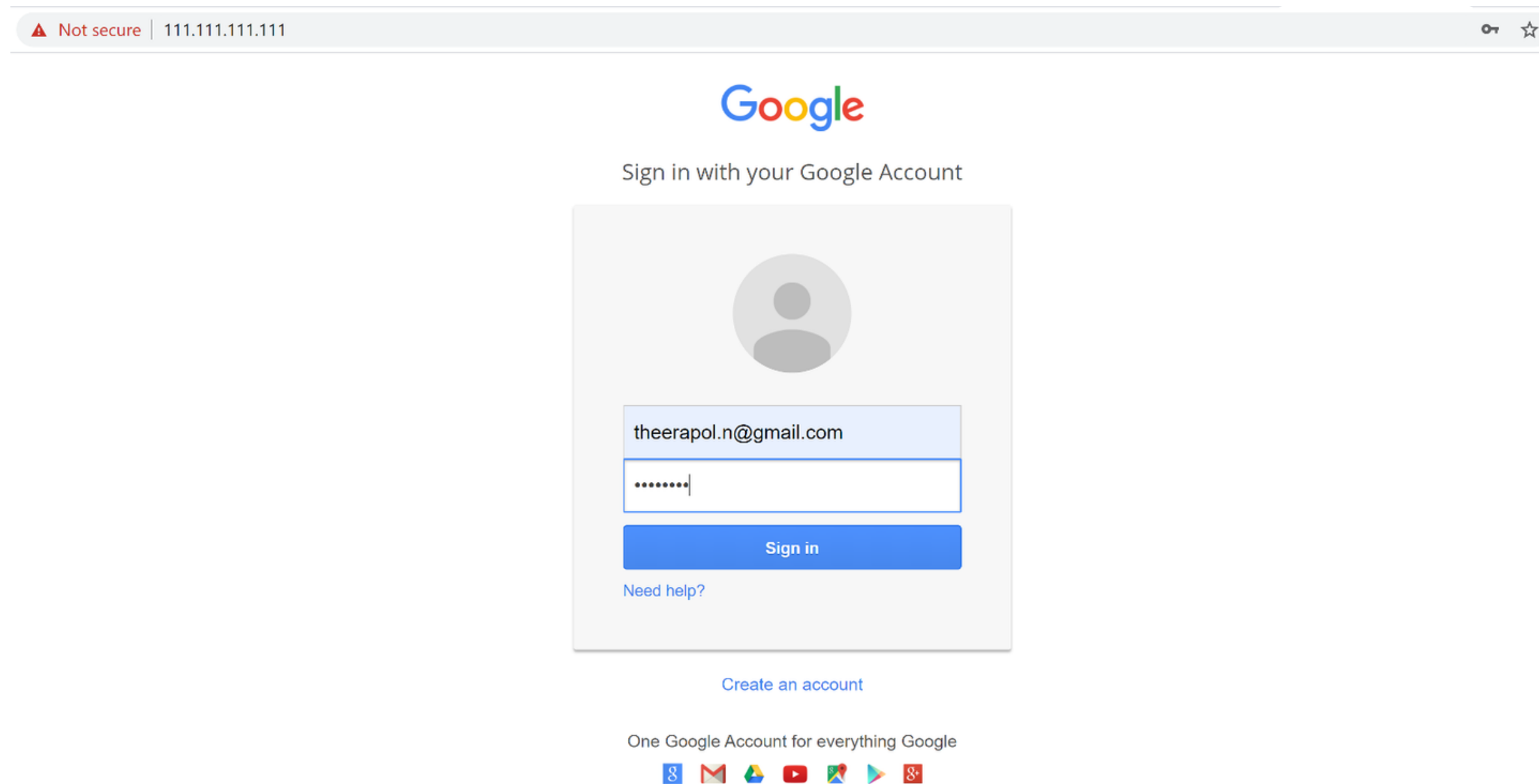
✓ **การเดารหัสผ่าน (Credential Attack)** คือ การเดารหัสผ่านของผู้ใช้จนกว่าจะได้รหัสผ่านที่ถูกต้อง

✓ **Zero-Day Attack** คือ การโจมตีช่องโหว่ที่ยังไม่มี patch ของซอฟต์แวร์ หรือระบบปฏิบัติการนั้น ๆ

✓ **Advanced Persistent Threat (APT)** คือ การโจมตีที่ฝังหรือแอบอยู่ในระบบเพื่อขโมยข้อมูลโดยอาจแอบอยู่ในระบบนานเป็นเดือน/ปี

✓ **Session Hijacking** คือ การขโมย Session login ของผู้ใช้


ตัวอย่างภัยคุกคามทางไซเบอร์



ตัวอย่างภัยคุกคามทางไซเบอร์

← 📁 ! 🗑️ 📧 🕒 📧 📧 ⋮

ข้อความแจ้งเตือน > กล่องจดหมาย x

 **root toor** <mynameisroot@hotmail.com>
ถึง ฉัน ▾

อีเมลของคุณอาจถูก hack กรุณายืนยันตัวตน คลิกที่ link [gmail.com](#)

[Mynameisroot](#)
Title
Company


[Mynameisroot](#)
Title
Company
...

[ข้อความตัดทอน] [ดูทั้งข้อความ](#)

⚠ Not secure | 111.111.111.111

Google

Sign in with your Google Account




[Sign in](#)

[Need help?](#)

[Create an account](#)

One Google Account for everything Google



ตัวอย่างภัยคุกคามทางไซเบอร์

The screenshot displays a Linux file manager interface with two image files, `navy.jpg` and `navy2.jpg`. Below the files, two property windows are open. The `navy.jpg` properties window shows a size of 81.0 kB (81,008 bytes) and a modification date of Sun 15 Sep 2019 11:33:26 PM +07. The `navy2.jpg` properties window shows a size of 92.4 kB (92,419 bytes) and a modification date of Sun 01 Mar 2020 11:29:04 AM +07. A terminal window in the background shows the command `steghide info navy2.jpg` being executed, which reveals hidden data in the file:

```
root@Mynameisroot:~/TooL/LAB/test# steghide info navy2.jpg
"navy2.jpg":
  format: jpeg
  capacity: 4.7 KB
  Try to get information about embedded data ? (y/n) y
  Enter passphrase:
  embedded file "maldev.cpp":
    size: 5.0 KB
    encrypted: rijndael-128, cbc
    compressed: yes
root@Mynameisroot:~/TooL/LAB/test#
```

ตัวอย่างภัยคุกคามทางไซเบอร์

The image displays a phishing attack on a Facebook login page. The browser address bar shows a 'Not secure' warning and the IP address 111.111.111.111. The page title is 'facebook' with a 'สร้างบัญชีใหม่' (Create new account) button. The login form is titled 'เข้าสู่ระบบ Facebook' (Log in to Facebook) and contains the following fields and buttons:

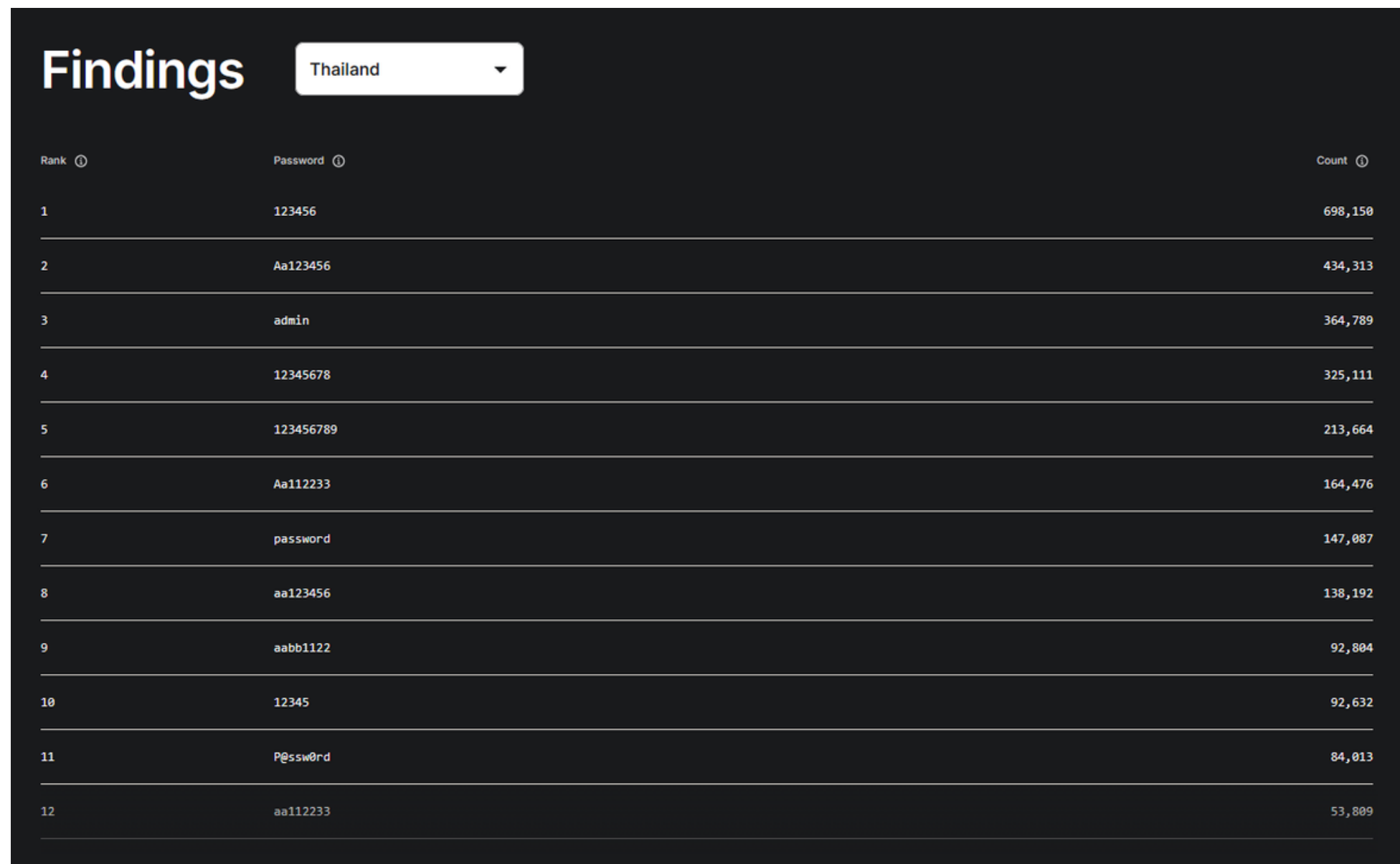
- Username field: `theerapol.n@navy.mi.th`
- Password field: `.....`
- Login button: `เข้าสู่ระบบ`
- Link: `ลืมบัญชีใช่ไหม` (Forgot account?)
- Link: `หรือ` (or)
- Registration button: `สร้างบัญชีใหม่` (Create new account)

Overlaid on the right side of the browser window is a terminal window titled `root@Mynameisroot: ~/Downloads/social-engineer-toolkit`. It displays the output of a social engineering tool, including the following parameters and findings:

```
PARAM: display=  
PARAM: enable_profile_selector=  
PARAM: isprivate=  
PARAM: legacy_return=0  
PARAM: profile_selector_ids=  
PARAM: return_session=  
POSSIBLE USERNAME FIELD FOUND: skip_api_login=  
PARAM: signed_next=  
PARAM: trynum=1  
PARAM: timezone=-420  
PARAM: lgndim=eyJ3IjoxNTM2LCJhIjo4NjQsImF3IjoxNTM2LCJhaCI6ODY0LCJjIjoyNH0=  
PARAM: lgnrnd=093649_P4Bk  
PARAM: lgnjs=1582998078  
POSSIBLE USERNAME FIELD FOUND: email=theerapol.n@navy.mi.th  
POSSIBLE PASSWORD FIELD FOUND: pass=pass1234  
PARAM: prefill_contact_point=theerapol.n@navy.mi.th  
PARAM: prefill_source=browser_dropdown  
PARAM: prefill_type=contact_point  
PARAM: first_prefill_source=browser_dropdown  
PARAM: first_prefill_type=contact_point  
PARAM: had_cp_prefilled=true  
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false  
PARAM: ab_test_data=AAAAffAf/Af/AAAFaFAffAAAAAAAAAAAAAAAAAAAAcJ/OAHAHCAB  
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

ตัวอย่างภัยคุกคามทางไซเบอร์

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



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

The screenshot shows the VirusTotal interface for a file analysis. The file name is 'maldev.exe' with a SHA-256 hash of '26fbb7c3aef88c3b1bcdcf4af7312a7b407ff2fef5a84c307a73fdd6c479996e'. The file size is 14.00 KB and it was uploaded on 2020-03-01 at 01:42:56 UTC. A red box highlights the URL 'www.virustotal.com' in the browser's address bar. The main content area shows a '25 / 71' detection score and a 'Community Score' of 0. Below this, a table lists the detection results from various engines.

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Acronis		ⓘ Suspicious	Ad-Aware ⓘ Gen:Variant.Fugrafa.7472
ALYac		ⓘ Gen:Variant.Fugrafa.7472	SecureAge APEX ⓘ Malicious
Arcabit		ⓘ Trojan.Fugrafa.D1D30	BitDefender ⓘ Gen:Variant.Fugrafa.7472
BitDefenderTheta		ⓘ Gen:NN.ZexaF.34090.aCW@a4MPwKn	Bkav ⓘ W32.AIDetectVM.malware
Comodo		ⓘ MalCrypt.Indusl@1qrz1	Cylance ⓘ Unsafe
Emsisoft		ⓘ Gen:Variant.Fugrafa.7472 (B)	Endgame ⓘ Malicious (high Confidence)
eScan		ⓘ Gen:Variant.Fugrafa.7472	ESET-NOD32 ⓘ A Variant Of Win32/Agent.TSR
F-Secure		ⓘ Heuristic.HEUR/AGEN.1044684	FireEye ⓘ Generic.mg.8d6cad4830aa4c72
GData		ⓘ Gen:Variant.Fugrafa.7472	MAX ⓘ Malware (ai Score=83)
Microsoft		ⓘ Trojan:Win32/Wacatac.C!ml	NANO-Antivirus ⓘ Trojan.Win32.Fugrafa.gcptxy

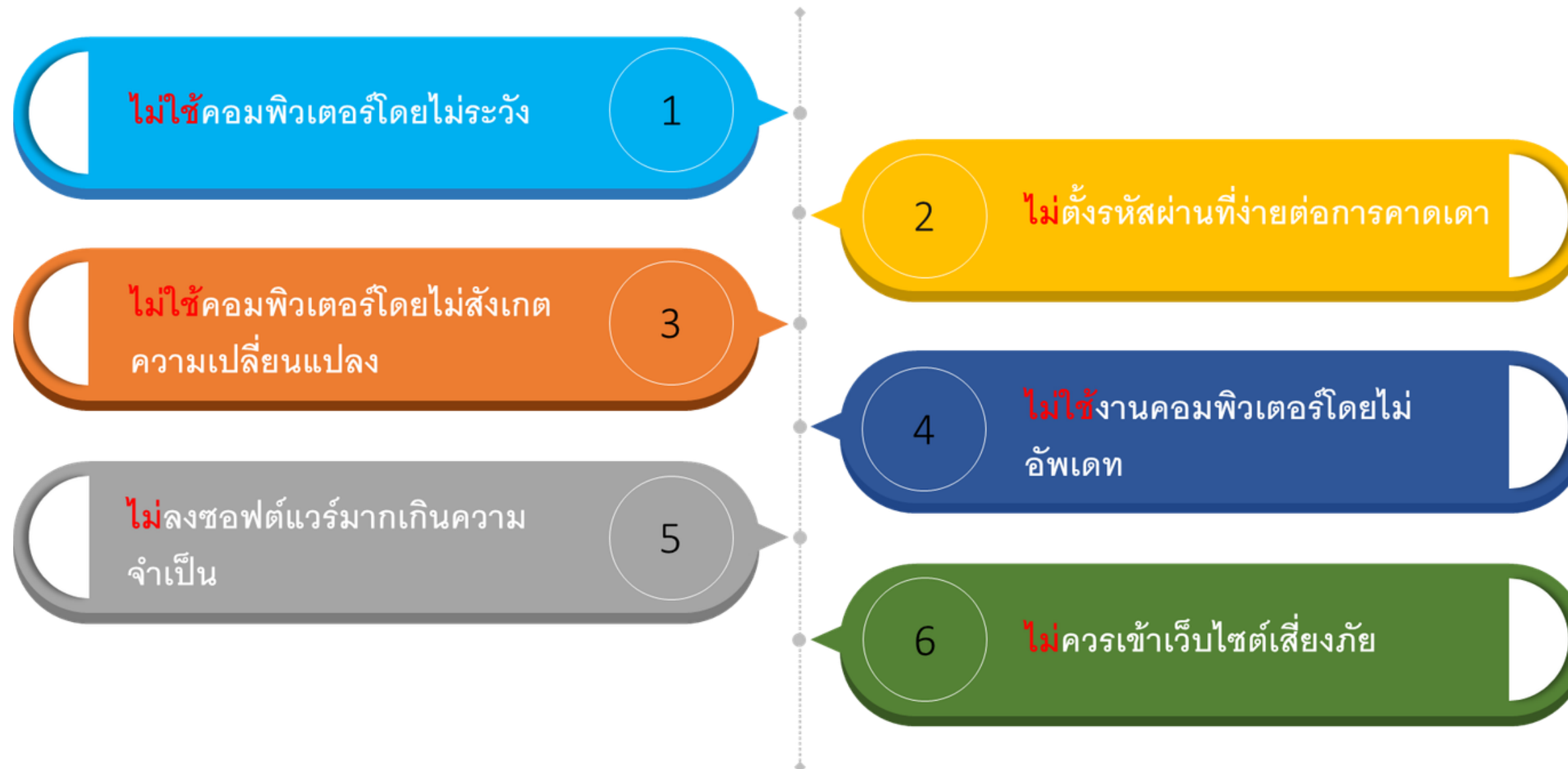


สรุปสถานการณ์ภัยคุกคามทางไซเบอร์

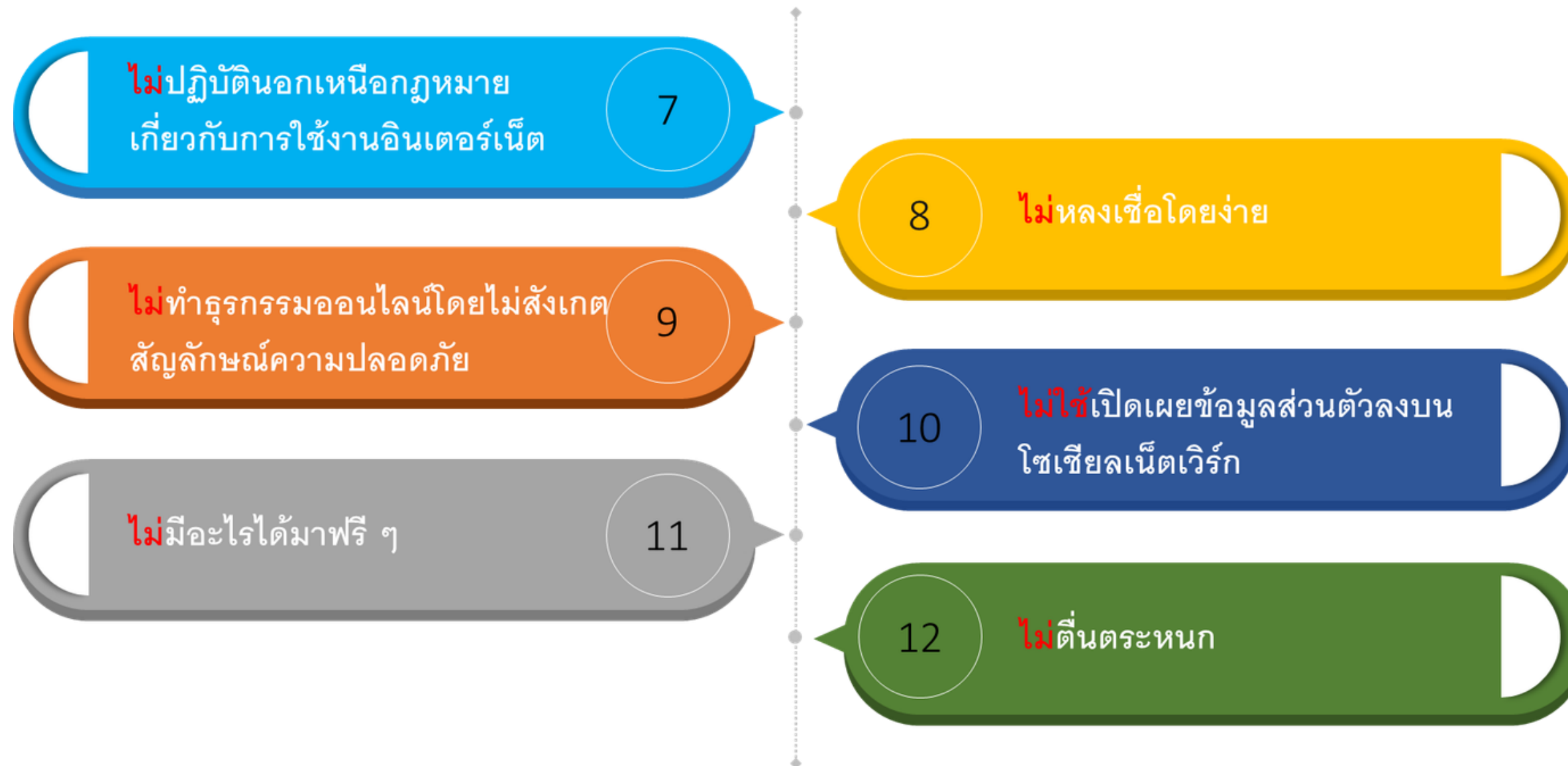


ที่มา: [HTTPS://WWW.FACEBOOK.COM/NCSA.THAILAND/POSTS/-เปิดสถิติ-3485-สถานการณ์ภัยคุกคามทางไซเบอร์ในห้วงที่ผ่านมา-มีภัยรูปแบบใดบ้าง-นี้/1152916677029996/](https://www.facebook.com/NCSA.THAILAND/POSTS/-เปิดสถิติ-3485-สถานการณ์ภัยคุกคามทางไซเบอร์ในห้วงที่ผ่านมา-มีภัยรูปแบบใดบ้าง-นี้/1152916677029996/)

ข้อควรระวัง



ข้อควรระวัง

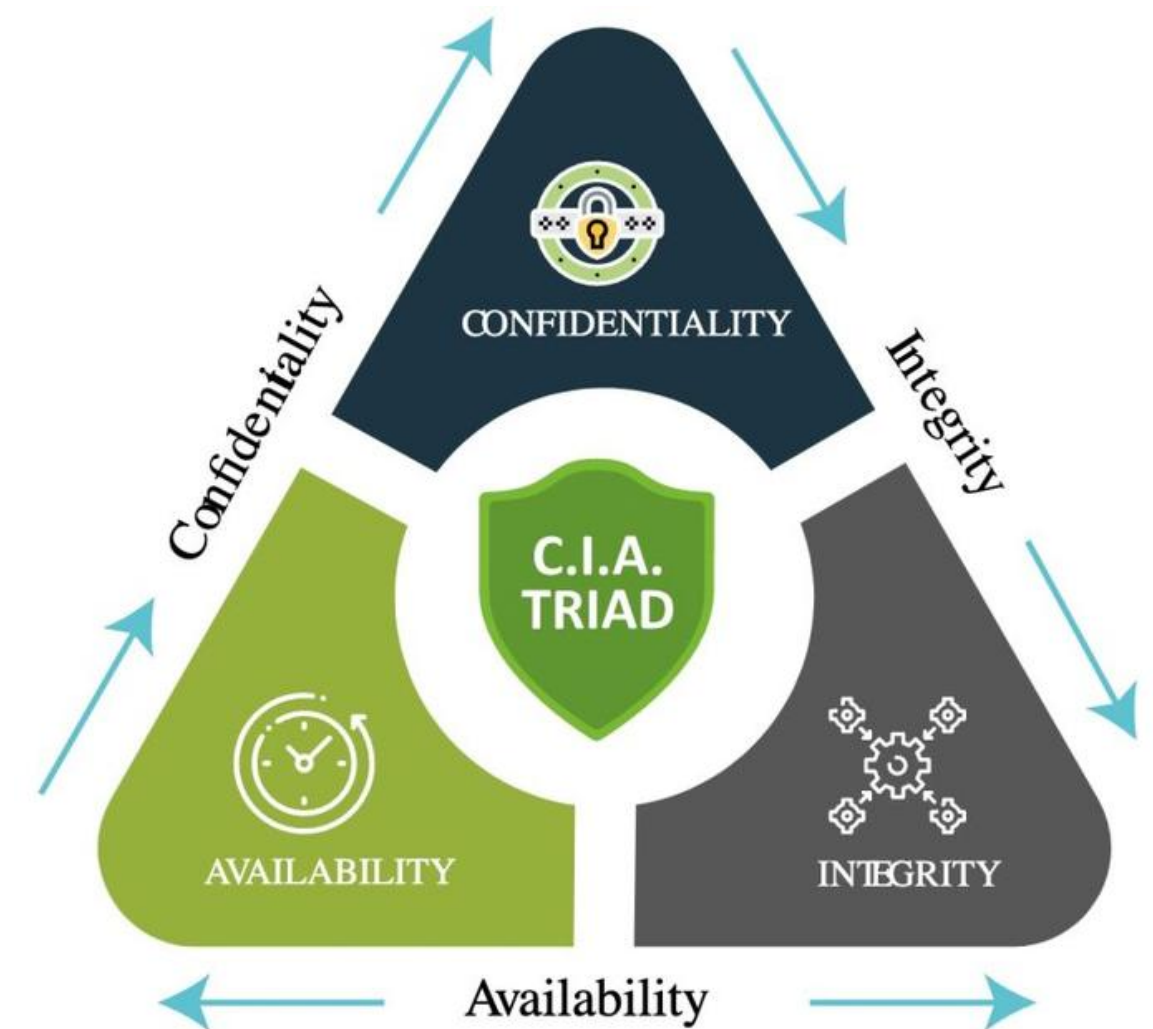


ข้อควรระวัง



แนวคิดหลักในด้านความปลอดภัยไซเบอร์

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



NIST Framework

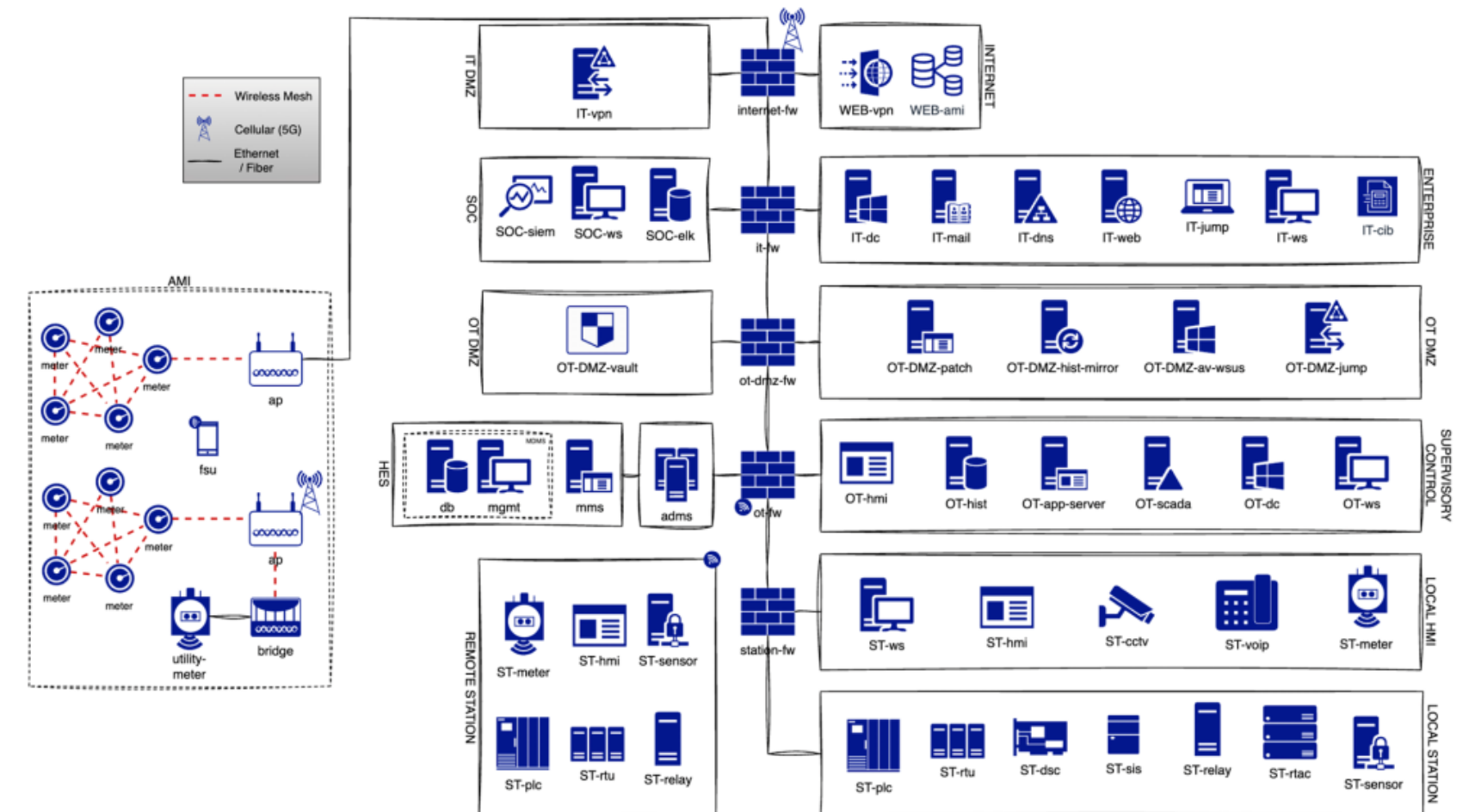
NIST Framework คือกรอบแนวทางด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ที่พัฒนาโดย National Institute of Standards and Technology (NIST) ของสหรัฐอเมริกา ใช้เป็น “มาตรฐานกลาง” สำหรับองค์กรในการป้องกัน ตรวจสอบ และตอบสนองภัยคุกคามไซเบอร์



NIST Framework

1. Identify (ระบุความเสี่ยง)

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



NIST Framework

2. Protect (ป้องกัน)

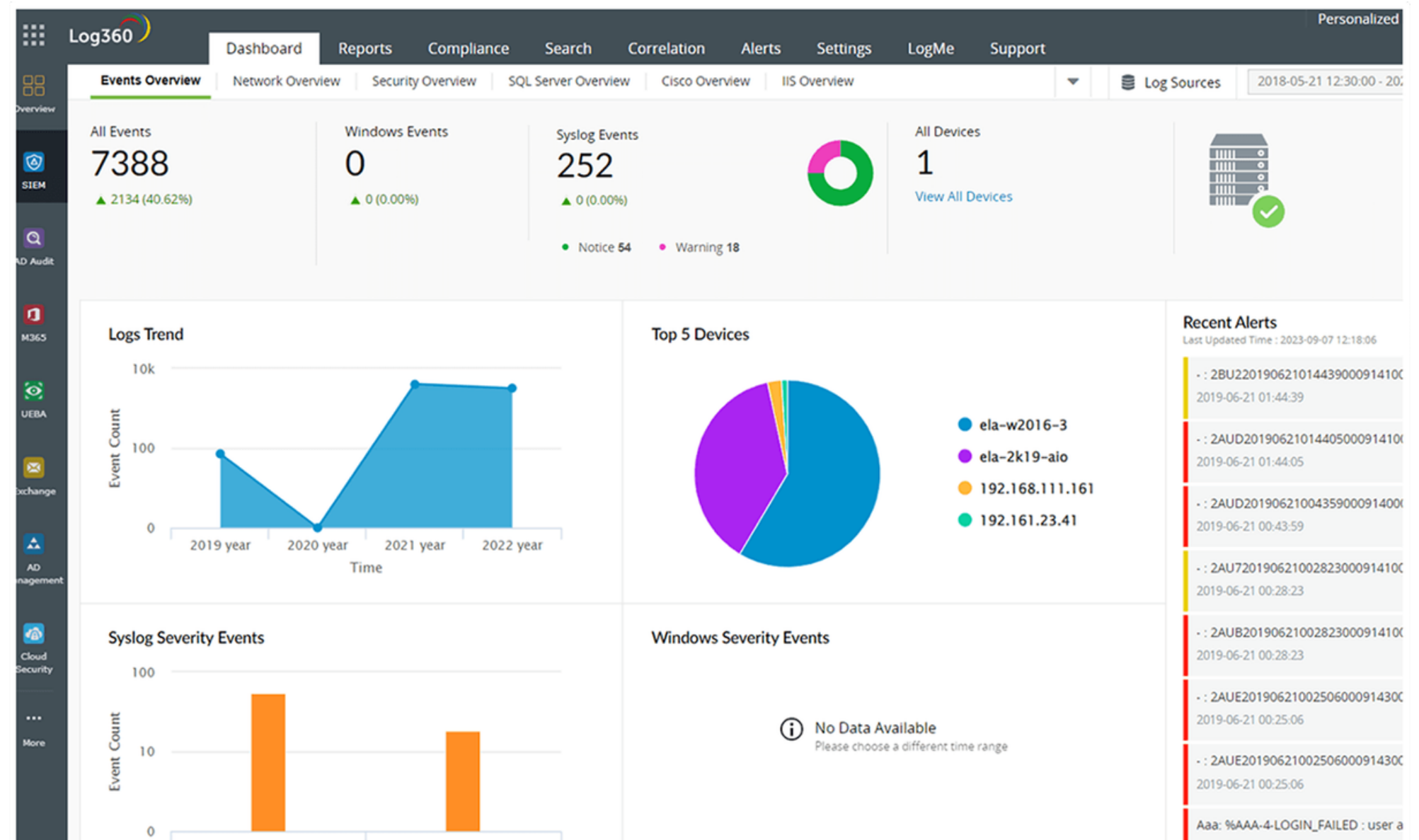
- ควบคุมการเข้าถึง (Access Control)
- ใช้ MFA / Encryption
- Training ผู้ใช้งาน



NIST Framework

3. Detect (ตรวจจับ)

- ตรวจจับเหตุการณ์ผิดปกติ
- Monitoring / Logging



NIST Framework

4. Respond (ตอบสนอง)

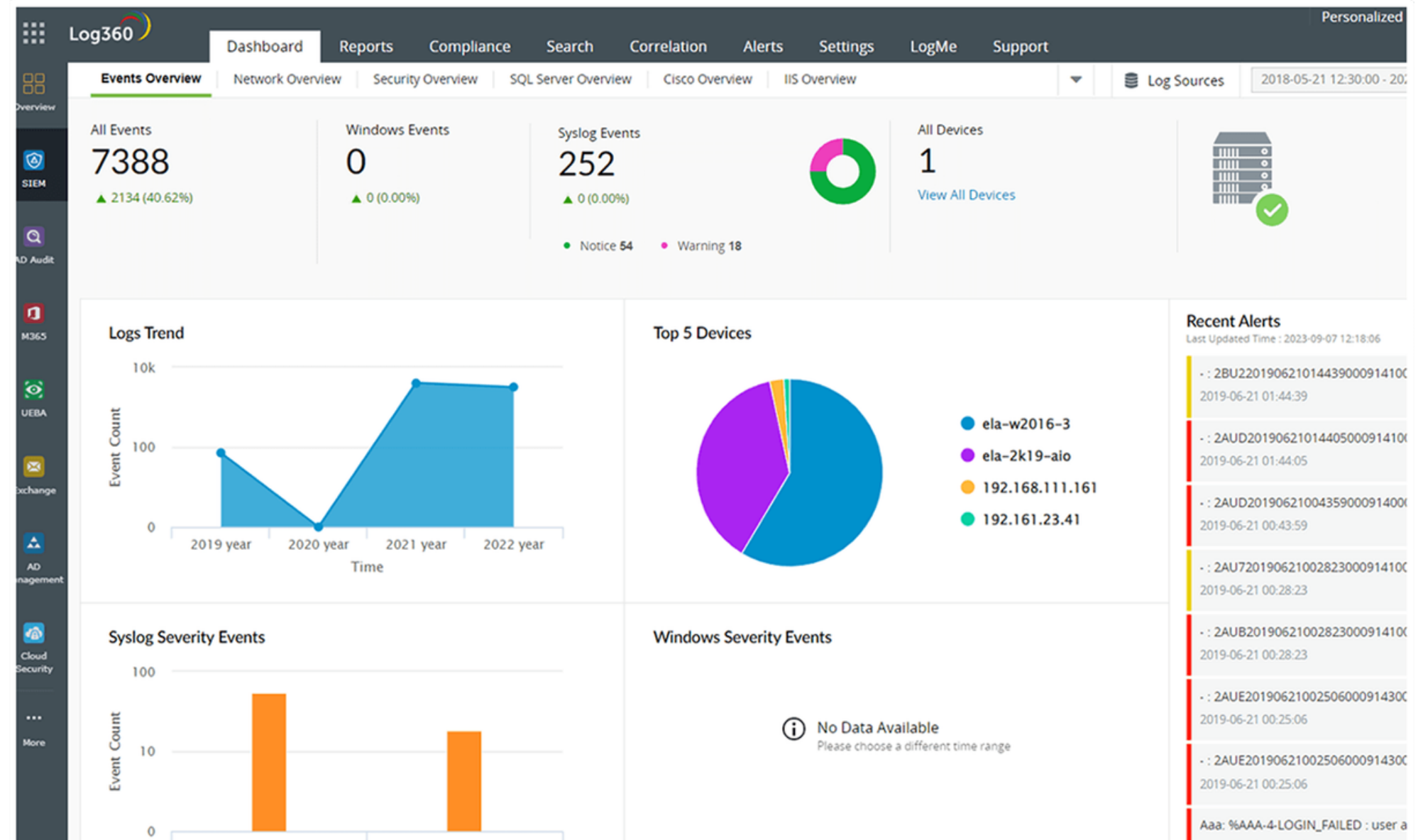
- มี Incident Response Plan
- แจ้งเตือน / แก้ไขปัญหา



NIST Framework

5. Recover (ฟื้นฟู)

- Backup / Restore
- Disaster Recovery Plan



ความสำคัญของ Cyber Security ต่อหน่วยงานภาครัฐ

- 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

- มีการจัดเก็บข้อมูลที่มีความสำคัญตามภารกิจ
 - ข้อมูลส่วนบุคคลของผู้รับบริการ
 - ข้อมูลที่ต้องจัดเก็บตามภารกิจด้านต่าง ๆ



ความสำคัญของ Cyber Security ต่อหน่วยงานภาครัฐ

- ภัยคุกคามทางไซเบอร์มีความซับซ้อนและต่อเนื่องมากขึ้น
- หน่วยงานรัฐเป็นเป้าหมายหลัก
- เกิดขึ้นจากความขัดแย้งระหว่างประเทศ
- ระบบสารสนเทศหลักเป็นเป้าหมายของสงครามไซเบอร์



บทสรุปการป้องกันภัยคุกคามไซเบอร์

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



Q&A

Thank you