NCSA สกมช

กรอบแนวทางการป้องกันภัยคุกคามทางไซเบอร์ (MITRE D3FEND)

วันที่ 14 มกราคมคม 2569 เวลา 09.00 – 11.00 น.
ณ ศูนย์สมุททานุภาพกองทัพเรือ
ตำบลบางพระ อำเภอศรีราชา จังหวัดชลบุรี

นายปิยชาติ วิสุทธิอารีย์รักษ์
เจ้าหน้าที่กลุ่มวิชาชีพเฉพาะด้านไซเบอร์

นาย ปิยชาติ วิสุทธิอารีย์รักษ์

Mr. Piyachart Visuttiarreerak

ตำแหน่ง: เจ้าหน้าที่กลุ่มวิชาชีพเฉพาะด้านไซเบอร์

ฝ่าย: ตอบสนองรับมือภัยคุกคามทางไซเบอร์และสืบสวนและตรวจพิสูจน์หลักฐานทางไซเบอร์ (สกมช.)

การศึกษา: บริหารธุรกิจบัณฑิต (ระบบสารสนเทศ)

ประสบการณ์การทำงาน

ประสบการณ์การทำงานด้านความมั่นคงปลอดภัยไซเบอร์

- สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
  - เข้าร่วมปฏิบัติงานกับศูนย์ปฏิบัติการบูรณาการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ศบอท.)
  - เข้าร่วมปฏิบัติการตัดวงจรแอปดูดเงิน
- บริษัท คาราบาวตะวันแดง จำกัด
  - ดูแลระบบการจัดการบริการไอที - IT Service Management Software (ITSM)
  - พัฒนากระบวนการ การบริหารจัดการทรัพย์สินไอที - IT Asset Management (ITAM)

Certificates Received

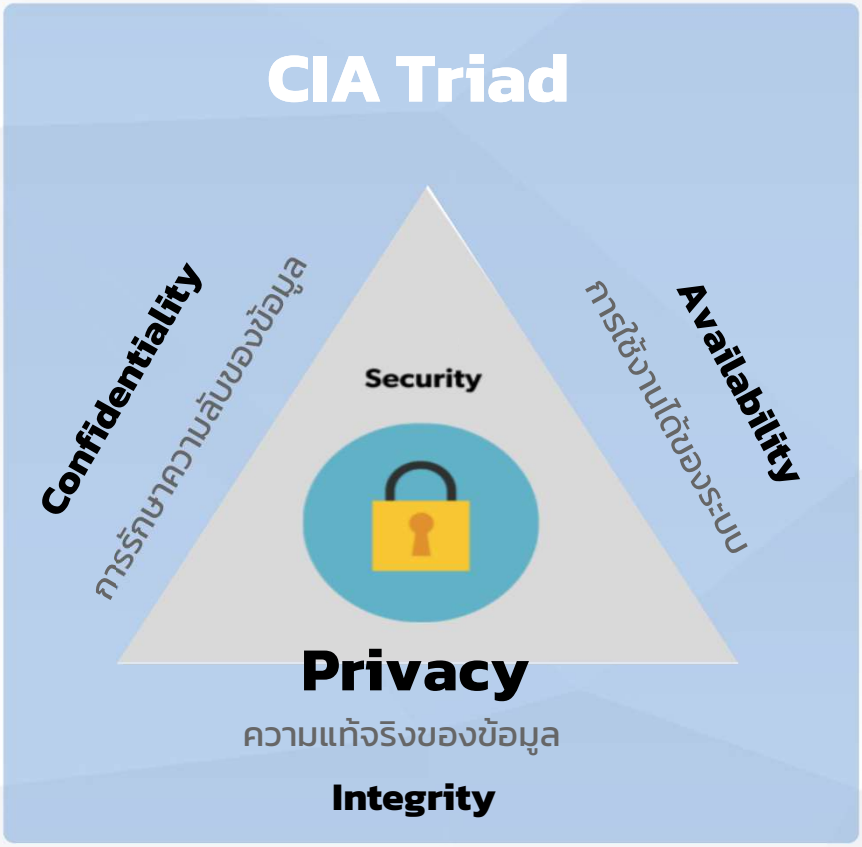
ประกาศนียบัตรและการอบรมทางไซเบอร์

- CompTIA Security+ – CompTIA
- Certified in Cybersecurity (CC) – ISC2
- Lead Auditor ISO 27001:2022 - Exemplar Global
- SANS FOR572 Advance Network Forensics: Threat Hunting, Analysis and Incident Response
- Web Application Penetration Testing – Mahidol University
- Network & Cyber Security – Jodoi Training Center

วัตถุประสงค์

1. อธิบายแนวคิดและบทบาทของกรอบ MITRE D3FEND
2. เข้าใจความสัมพันธ์ระหว่าง Model (ความเข้าใจระบบ), Defensive Tactics และการตอบสนองต่อภัยคุกคามทางไซเบอร์
3. วิเคราะห์และเชื่อมโยงภัยคุกคามทางไซเบอร์กับแนวทางการป้องกันและตอบสนองตามกรอบ MITRE D3FEND
4. ประยุกต์ใช้กรอบ D3FEND เพื่อยกระดับกระบวนการตรวจจับ, ควบคุมสถานการณ์ และฟื้นฟูระบบ

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์



Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น

- ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็น ความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น
- เบอร์โทรของพนักงานในบริษัท จัดเป็น ข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน

Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มี ความถูกต้องอย่างต่อเนื่อง เช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ตัวอย่างเช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

การรักษาความปลอดภัยทางไซเบอร์คืออะไร

Cyber Security คือ ความมั่นคงปลอดภัยทางไซเบอร์ ที่ต้องการป้องกันและการรักษาความปลอดภัยของระบบคอมพิวเตอร์ ระบบเครือข่าย และข้อมูลที่เกี่ยวข้อง โดยจุดประสงค์ คือ เพื่อป้องกันการเข้าถึง การแก้ไข การเปลี่ยนแปลง หรือการทำลายข้อมูลจากบุคคลที่ไม่ได้รับอนุญาต หรือบุคคลที่ต้องการเข้าถึงข้อมูลเพื่อวัตถุประสงค์ที่ไม่เหมาะสม

ทั้งนี้หลายองค์กร ต่างให้ความสำคัญเรื่องระบบรักษาความปลอดภัยของข้อมูลไม่แพ้กัน เพราะหากลูกค้าหรือผู้ใช้บริการโดนโจรกรรมข้อมูลทางอิเล็กทรอนิกส์ไป อาจทำให้องค์กรเสียชื่อได้ เพราะฉะนั้น Cyber Security จึงมีความสำคัญ

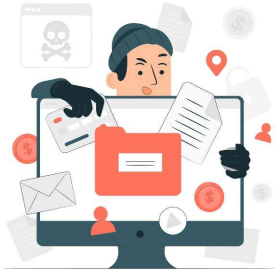
"ภัยคุกคามทางไซเบอร์" หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

สถานการณ์ภัยคุกคามไซเบอร์ระดับโลก

Ransomware เป็นการโจมตีที่มีสัดส่วนสูงสุด 23% ตามด้วย Data Theft และ Server Access ซึ่งมีสัดส่วน 13% และ 10% ตามลำดับ

1. Ransomware

ไฟล์ถูกเข้ารหัสทำให้ผู้ใช้งานไม่สามารถเปิดไฟล์ได้ โดยผู้ใช้งานจะต้องจ่ายเงินตามข้อความ “เรียกค่าไถ่” เพื่อปลดล็อคกู้ข้อมูลคืนมา



2. Data Theft

ส่วนใหญ่เกิดจากบุคคลภายในองค์กร ด้วยมองว่าข้อมูลเป็นสิทธิ์ของตน เนื่องจากเป็นผู้จัดทำขึ้น หรือจงใจละเมิดการเข้าถึงข้อมูลเพื่อเปิดเผยการประพฤติมิชอบของนายจ้างจากมุมมองของสังคม

3. Server Access

การเข้าถึงระบบโดยไม่ได้รับอนุญาต ซึ่งอาจจมีจุดประสงค์ในการขโมยข้อมูล แก้ไขปรับเปลี่ยน หรือทำให้หยุดชะงักไม่สามารถให้บริการแก่ผู้ใช้งานได้

ภาพรวมของ Cybersecurity ในปัจจุบัน

ภัยคุกคามทางไซเบอร์มีความซับซ้อนและหลากหลายมากขึ้น

- รูปแบบการโจมตีพัฒนาอย่างต่อเนื่อง เช่น Ransomware-as-a-Service (RaaS), AI-driven phishing, และ Supply Chain Attacks
- กลุ่มแฮกเกอร์มักทำงานแบบองค์กร มีเป้าหมายชัดเจน และวางแผนระยะยาว

เป้าหมายหลักของการโจมตีเปลี่ยนไป

- จากองค์กรขนาดใหญ่ → สู่ธุรกิจขนาดกลางและเล็ก (SMEs)
- จากข้อมูลส่วนตัว → สู่การเจาะระบบโครงสร้างพื้นฐานสำคัญ เช่น พลังงาน, ระบบสาธารณสุข, การเงิน

การเปลี่ยนแปลงของสภาพแวดล้อมการทำงาน

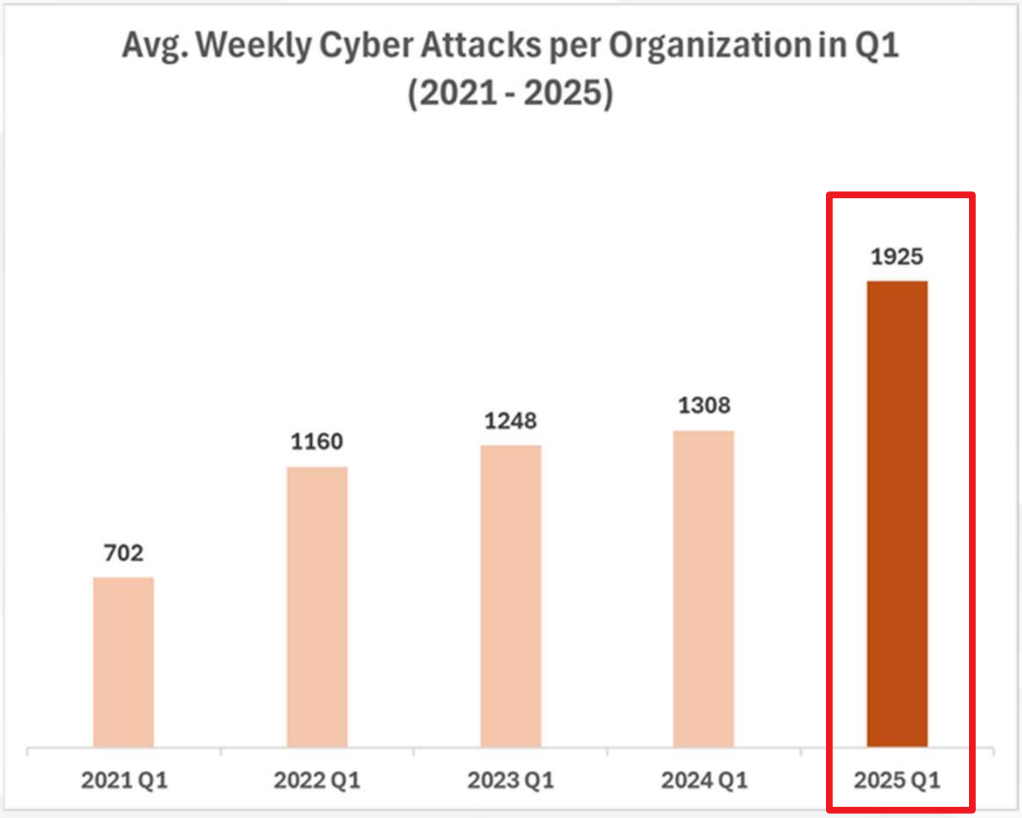
- การทำงานแบบ Hybrid หรือ Remote Work ทำให้ขอบเขตการรักษาความปลอดภัยยากขึ้น
- อุปกรณ์ส่วนตัวของพนักงานกลายเป็นจุดอ่อนใหม่ (BYOD: Bring Your Own Device)

การใช้ AI และ Automation ในการรักษาความปลอดภัย

- ระบบ AI เริ่มมีบทบาทในการตรวจจับพฤติกรรมผิดปกติ
- แต่ในขณะเดียวกัน แฮกเกอร์ก็ใช้ AI ในการโจมตี เช่น Deepfake, Phishing ด้วยข้อความสมจริง

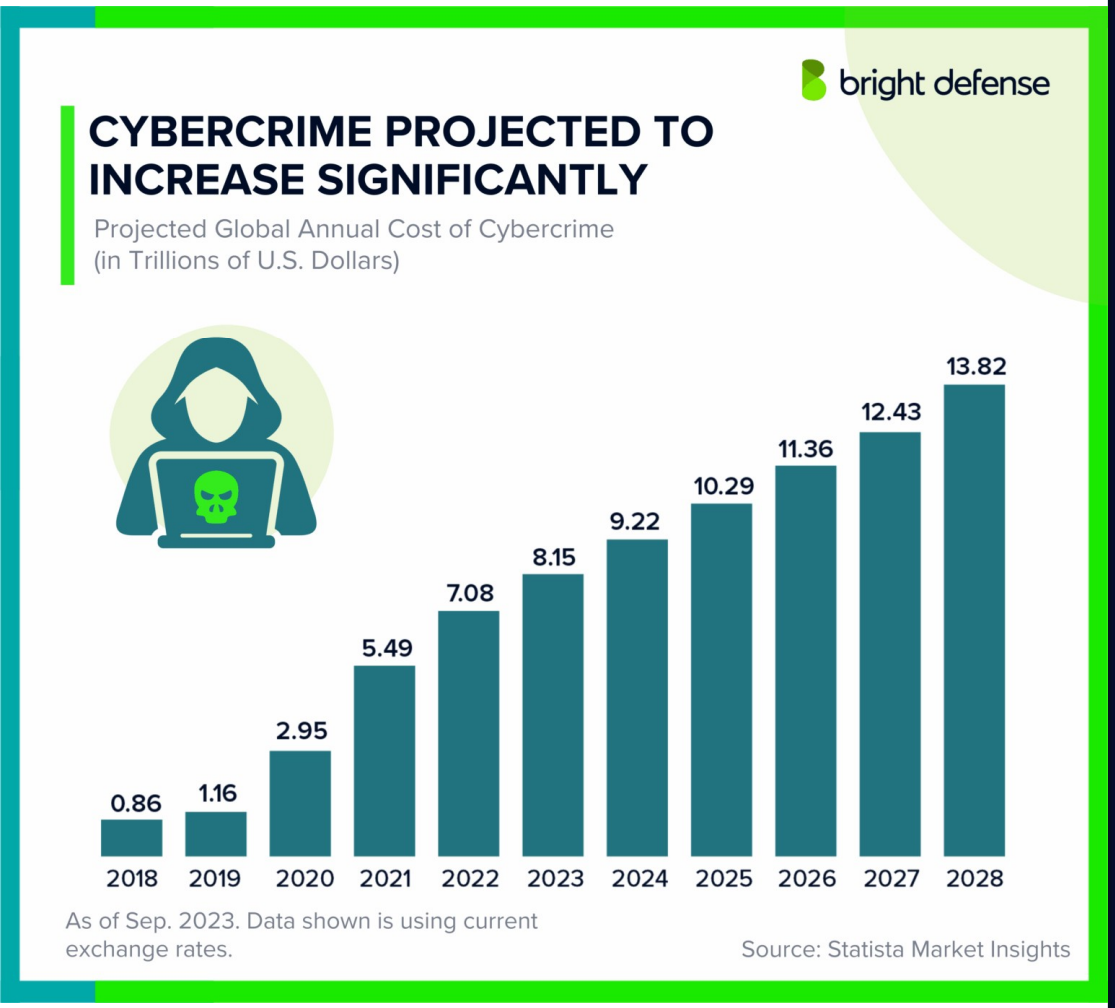
https://www.getastra.com/blog/security-audit/cyber-crime-statistics/
https://www.thesslstore.com/blog/cyber-crime-statistics/

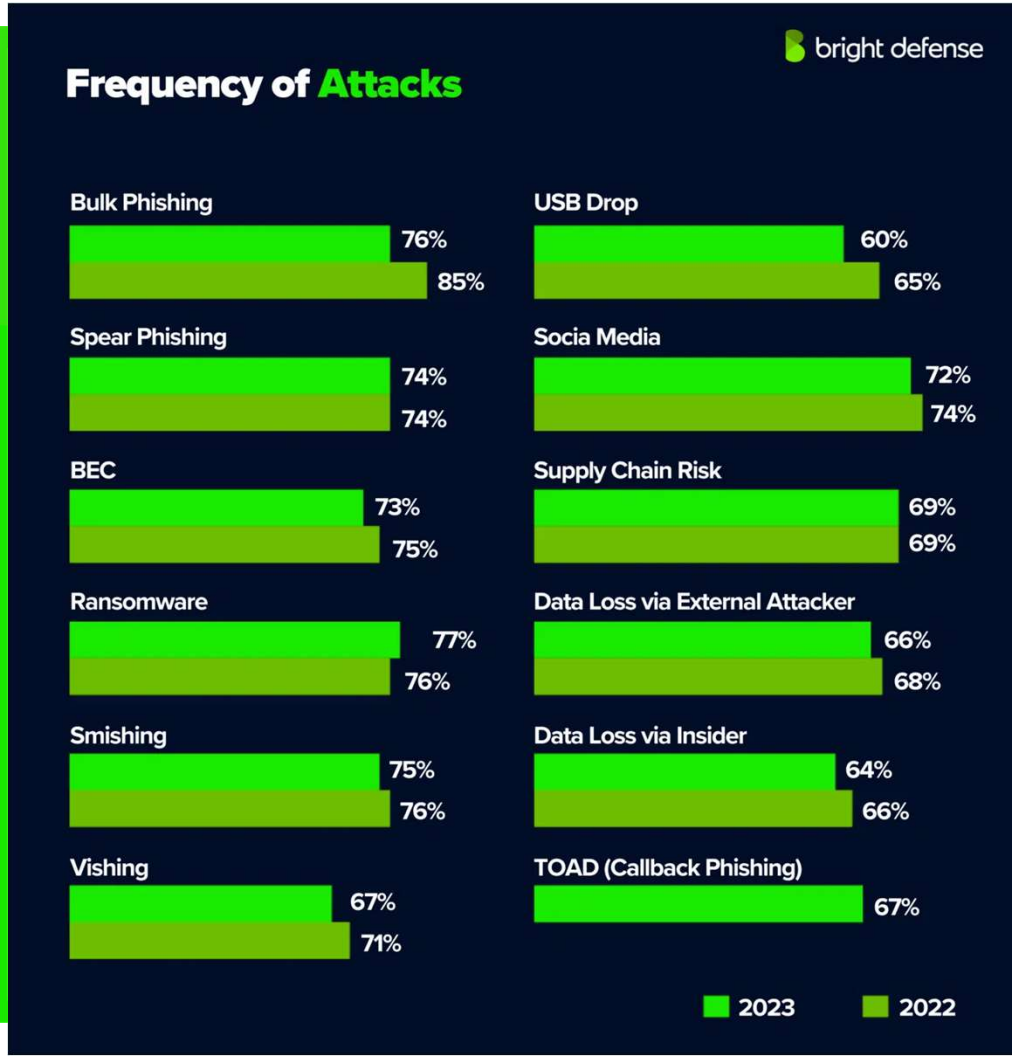
การโจมตีทางไซเบอร์ทั่วโลกประจำไตรมาสที่ 1 ปี 2025



- **การโจมตีทางไซเบอร์พุ่งสูง** : ในไตรมาสที่ 1 ปี 2568 การโจมตีทางไซเบอร์ต่อองค์กรเพิ่มขึ้น 47% โดยมีค่าเฉลี่ยการโจมตี 1,925 ครั้งต่อสัปดาห์
- **ภาคส่วนที่ได้รับผลกระทบมากที่สุด** : ภาคการศึกษาพบการโจมตีมากที่สุด โดยมีการโจมตี 4,484 ครั้งต่อสัปดาห์ รองลงมาคือภาครัฐและโทรคมนาคมโดยมีการโจมตี 2,678 และ 2,664 ครั้งตามลำดับ
- **การเติบโตของการโจมตีในระดับภูมิภาค** : แอฟริกามีค่าเฉลี่ยสูงสุดที่ 3,286 การโจมตีต่อสัปดาห์ ในขณะที่ละตินอเมริกาพบการเพิ่มขึ้น เทียบกับปีก่อนหน้า สูงสุดที่ 108%
- **Ransomware เพิ่มขึ้น** : การโจมตี Ransomwareเพิ่มขึ้น 126% โดยอเมริกาเหนือคิดเป็น 62% ของเหตุการณ์ทั่วโลก และสินค้าอุปโภคบริโภคและบริการเป็นกลุ่มเป้าหมายมากที่สุด
- **ข้อมูลรั่วไหล**

https://blog.checkpoint.com/research/q1-2025-global-cyber-attack-report-from-check-point-software-an-almost-50-surge-in-cyber-threats-worldwide-with-a-rise-of-126-in-ransomware-attacks/

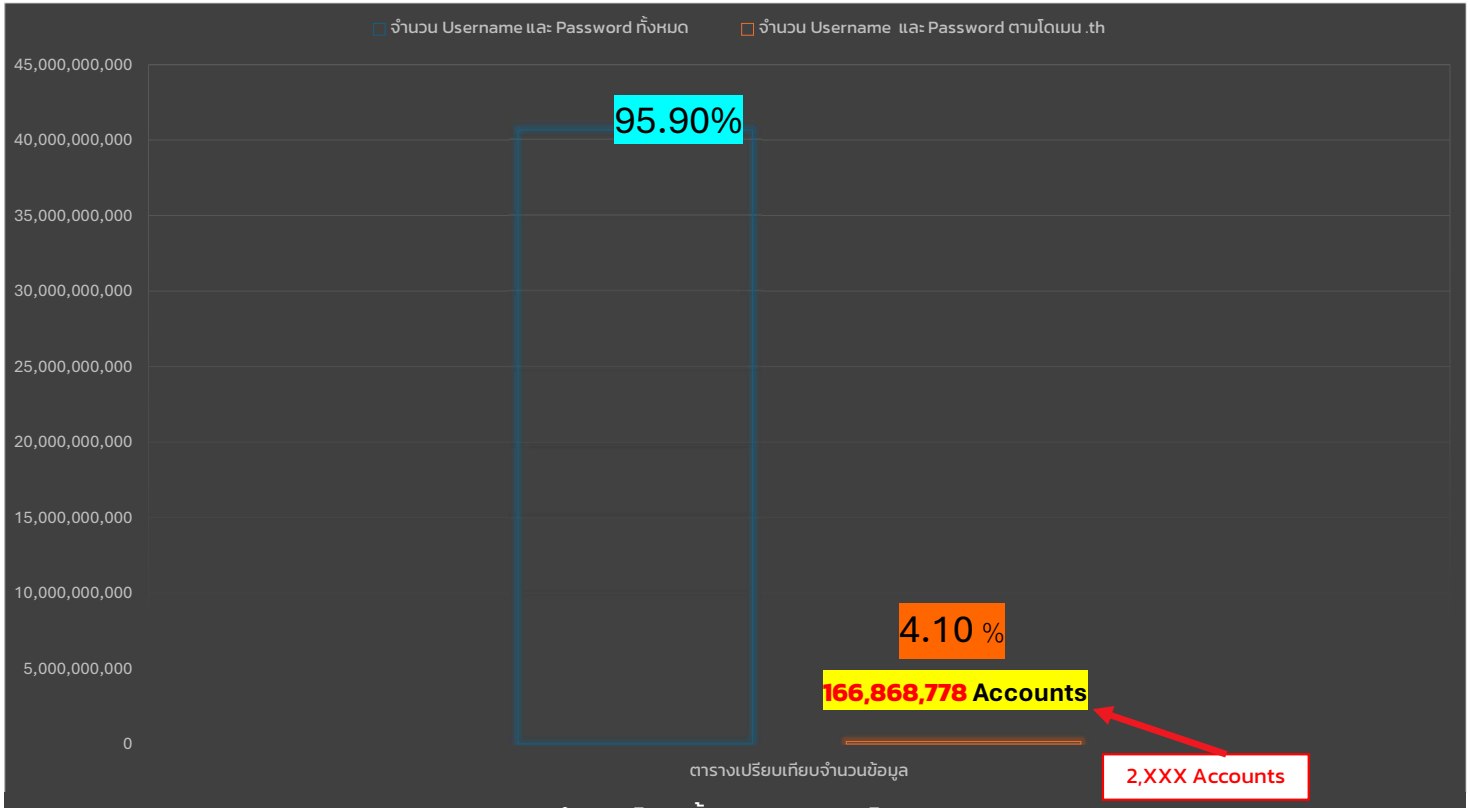




https://www.brightdefense.com/resources/cybercrime-statistics/

สถิติภัยคุกคามทางไซเบอร์Credential Leaks Trends

ตารางเปรียบเทียบจำนวนข้อมูล



จำนวนไฟล์ทั้งหมด 6,209 ไฟล์

จำนวน Username และ Password ทั้งหมด 40,679,503,009 Accounts

จำนวน Username และ Password ตามโดเมน .th 166,868,778 Accounts

```
Credential Leak all
batch 1 : 11298979814
batch 2 : 11194362311
batch 3 : 12023374050
batch 4 : 5995918056
all sum = 40,512,634,231 records

Only Top Level Domain .th
batch 1 : 50547776
batch 2 : 42239381
batch 3 : 41541102
batch 4 : 26719249
all th sum = 161,047,508 records
```

ค่าจำนวนของ credential leak ทั้งหมด จะได้มาจากแบ่งการทำงานเป็น 4 รอบ โดยแต่ละรอบจะแยกเป็นกลุ่ม(batch) แต่ละกลุ่มจะมีไฟล์ที่ไม่ซ้ำกัน เมื่อคำนวณเสร็จจะนำค่าทั้งหมดมารวมกัน และออกมาเป็นจำนวนของ credential leak ทั้งหมด

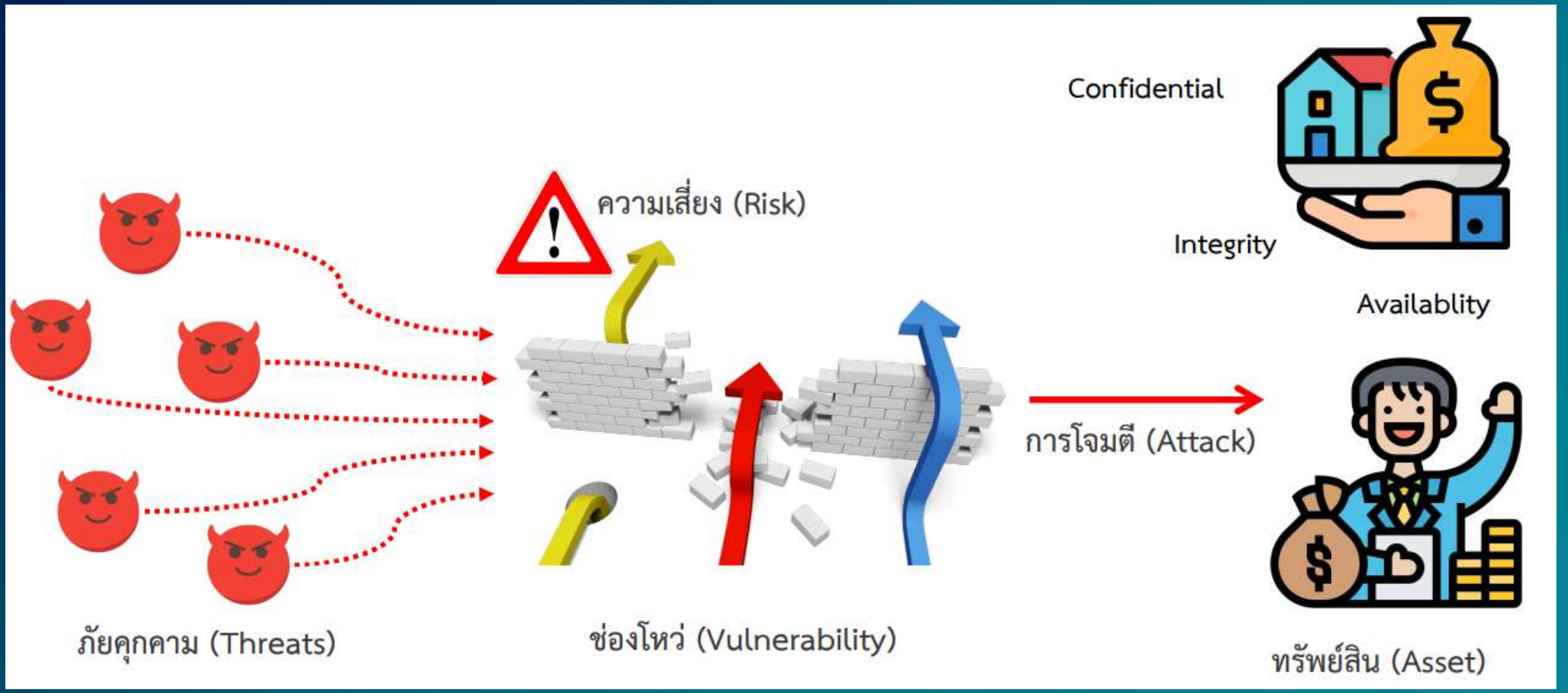
จำนวนข้อมูลที่รั่วไหลในปี 2025 **มากกว่าปี 2024 ประมาณ 80,524 เท่า**

Global Risks Cyber Security

Source: https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf

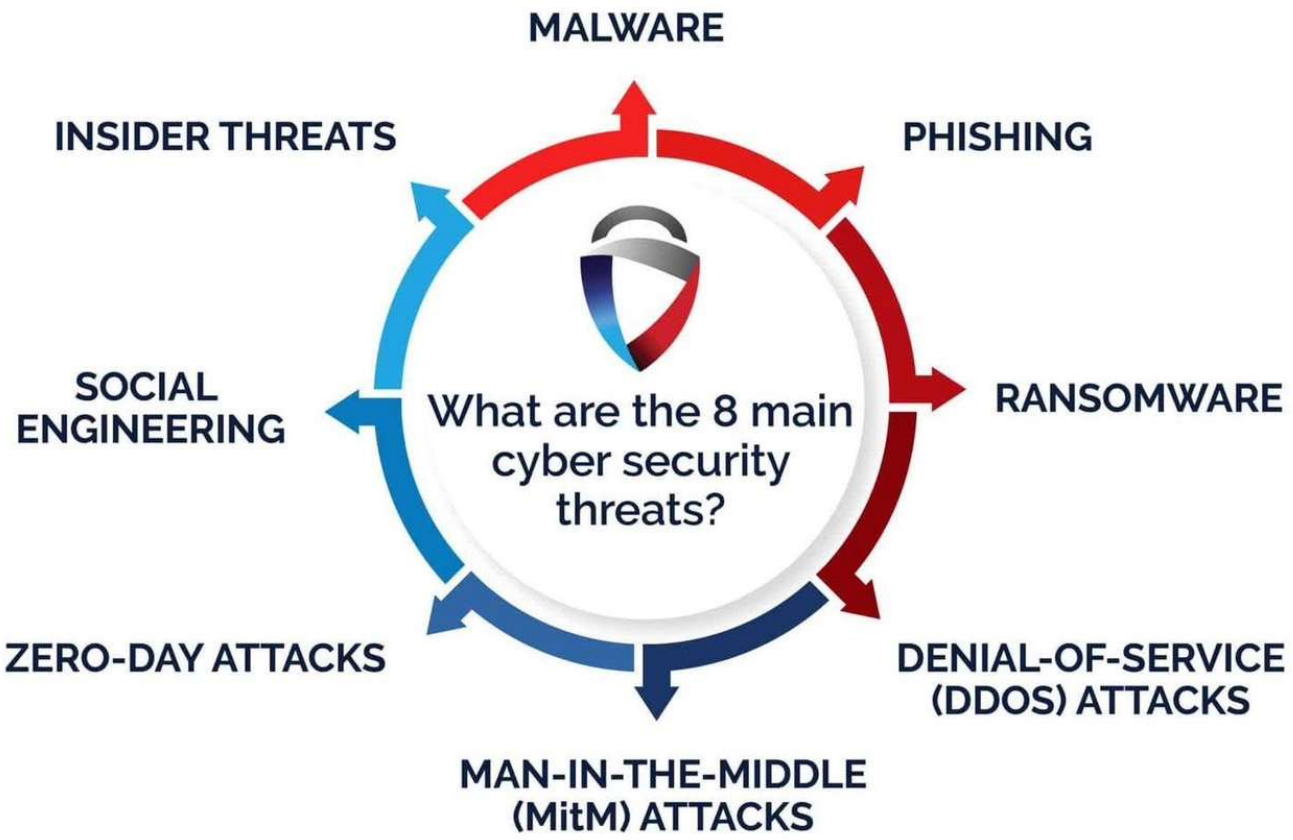
NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

Asset + Threat + Vulnerability = Risk



NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

Cyber Security threats

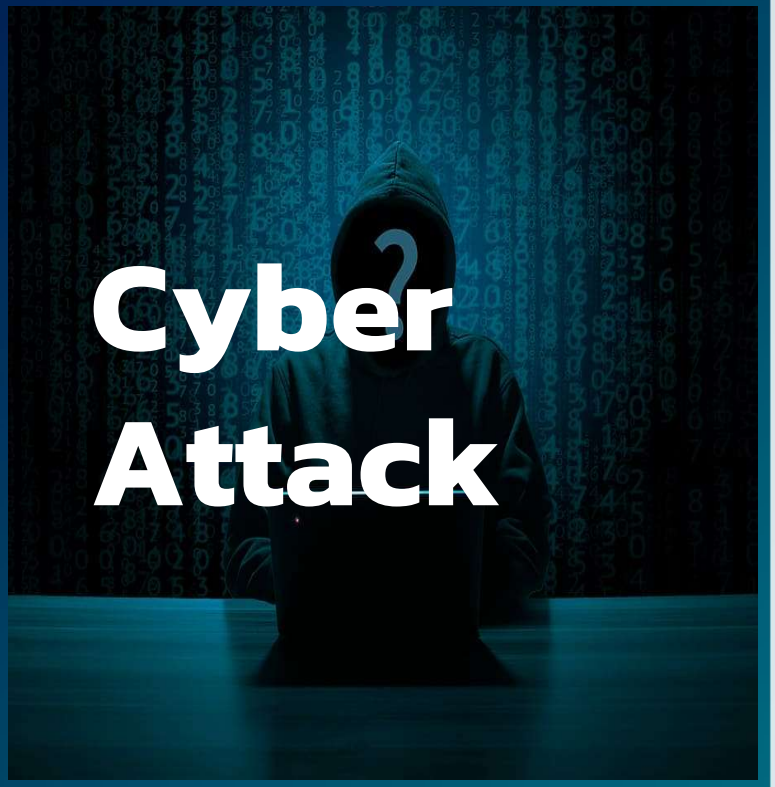


ภัยคุกคามมีหน้าตาอย่างไร? ใครคือผู้ไม่หวังดี?

1. **กลุ่มแฮกเกอร์จากต่างชาติที่รัฐบาลหนุนหลัง:** มุ่งโจมตีเพื่อผลประโยชน์ทางการเมืองหรือเศรษฐกิจ โดยใช้วิธีที่ซับซ้อนและโจมตีอย่างต่อเนื่อง
2. **โจรไซเบอร์:** มุ่งเน้นเรื่องเงินเป็นหลัก ใช้เครื่องมืออย่าง "ไวรัสเรียกค่าไถ่" (Ransomware) หรือ "เว็บปลอมหลอกเอาข้อมูล" (Phishing)
3. **กลุ่มแฮกเกอร์ที่เคลื่อนไหวเพื่ออุดมการณ์:** โจมตีเพื่อสร้างความปั่นป่วน (เช่น ทำให้เว็บล่ม) หรือเพื่อประกาศจุดยืนทางสังคม/การเมืองของตน
4. **คนในองค์กรที่สร้างความเสียหาย:** อาจเกิดจากความตั้งใจร้ายหรือความประมาทเลินเล่อของบุคลากรเอง ที่ใช้สิทธิ์ของตนเข้าถึงและทำลายระบบ

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

เป้าหมาย ของ Cyber Threats



•**บุคคล** : ผู้โจมตีอาจกำหนดเป้าหมายเป็นรายบุคคลเพื่อผลประโยชน์ส่วนตัว เช่น โดยการขโมยข้อมูลรับรองการเข้าสู่ระบบหรือเรียกค่าไถ่ข้อมูลส่วนบุคคล

•**ข้อมูลส่วนบุคคล** : ผู้โจมตีอาจพยายามขโมยข้อมูลส่วนบุคคลที่ละเอียดอ่อน เช่น ข้อมูลรับรองการเข้าสู่ระบบ ข้อมูลทางการเงิน และหมายเลขประกันสังคม เพื่อขายในตลาดมืดหรือใช้เพื่อขโมยข้อมูลประจำตัว

•**ทรัพย์สินทางปัญญา** : ผู้โจมตีอาจพยายามขโมยข้อมูลที่เป็นกรรมสิทธิ์ เช่น ความลับทางการค้าและเทคโนโลยีที่เป็นกรรมสิทธิ์ เพื่อให้ได้เปรียบในการแข่งขันหรือขายข้อมูลให้กับบุคคลอื่น

•**โครงสร้างพื้นฐานที่สำคัญ** : การโจมตีทางไซเบอร์บนโครงสร้างพื้นฐานที่สำคัญ เช่น โครงข่ายไฟฟ้า โรงบำบัดน้ำ และระบบขนส่ง สามารถส่งผลกระทบร้ายแรงและทำให้การทำงานของการบริการที่จำเป็นหยุดชะงักได้

•**หน่วยงานรัฐบาลและองค์กรทางการเมือง** : ผู้โจมตีอาจกำหนดเป้าหมายหน่วยงานรัฐบาลและองค์กรทางการเมืองเพื่อขโมยข้อมูลที่ละเอียดอ่อนหรือขัดขวางการดำเนินงานของหน่วยงาน

•**ธุรกิจ** : การโจมตีทางไซเบอร์ต่อธุรกิจอาจทำให้สูญเสียข้อมูลที่ละเอียดอ่อน สูญเสียทางการเงิน และทำลายชื่อเสียงของบริษัท

แรนซัมแวร์ (Ransomware)

มัลแวร์ประเภทหนึ่งที่ป้องกันหรือจำกัดสิทธิ์ผู้ใช้งาน
คอมพิวเตอร์ไม่ให้เข้าถึงระบบ ไฟล์ หรือเอกสาร
ของตัวเอง โดยการล็อกหน้าจอของระบบหรือล็อก
ไฟล์ของผู้ใช้จนกว่าจะยอมจ่ายเงินค่าไถ่คืนมา
จึงถูกเรียกอีกชื่อได้ว่า "มัลแวร์เรียกค่าไถ่"

แนวทางป้องกันแรนซัมแวร์

- อัปเดตระบบปฏิบัติการและแพตช์ความปลอดภัยอย่างสม่ำเสมอ
- สำรองข้อมูล (Backup) ไว้ในที่ปลอดภัย
- ใช้ Multi-Factor Authentication (MFA) เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต
- ฝึกอบรมพนักงานให้รู้จักวิธีป้องกัน Phishing และ Social Engineering
- ใช้ซอฟต์แวร์ป้องกันมัลแวร์และไฟร์วอลล์

#แรนซัมแวร์ยังคงเป็นภัยคุกคามที่สำคัญ และมีแนวโน้มพัฒนากลยุทธ์ใหม่ๆ เพื่อหลบเลี่ยงมาตรการป้องกัน ดังนั้นองค์กรและบุคคลทั่วไปควรตื่นตัวและเตรียมพร้อมรับมืออยู่เสมอ

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

การขโมยข้อมูลตัวตน (Identity Theft)

การขโมยข้อมูลตัวตน (Identity Theft) เป็นการที่ผู้ไม่ประสงค์ดี ได้นำข้อมูลและรูปภาพของบุคคลนั้นไปใช้โดยไม่ได้รับอนุญาต เพื่อหาผลประโยชน์และสร้างความเสียหาย ทำให้บุคคลนั้นโดนลดความน่าเชื่อถือในสังคม สาเหตุหนึ่งที่ผู้ไม่ประสงค์ดีนั้นสามารถขโมยข้อมูลตัวตนไปได้ คือ การเปิดเผยข้อมูลส่วนตัวลงบนสื่อสังคมออนไลน์มากเกินไป

Identity Theft : สาเหตุจากการเปิดเผยข้อมูลส่วนตัวในสื่อสังคมออนไลน์ และการล่อลวงด้วยวิธีการต่าง ๆ เพื่อให้ได้ข้อมูล

วิธีป้องกันการขโมยข้อมูลตัวตน

1. ใช้รหัสผ่านที่แข็งแรงและไม่ใช้ซ้ำ – ใช้ Multi-Factor Authentication (MFA)
2. ระวังอีเมลและข้อความต้องสงสัย – อย่าคลิกลิงก์ที่ไม่น่าเชื่อถือ
3. ตรวจสอบบัญชีธนาคารและเครดิตสม่ำเสมอ – หากพบธุรกรรมผิดปกติให้แจ้งธนาคารทันที
4. หลีกเลี่ยงการเปิดเผยข้อมูลส่วนตัวในที่สาธารณะ – เช่น การโพสต์เลขบัตรประชาชนหรือบัตรเครดิตบนโซเชียลมีเดีย
5. อัปเดตซอฟต์แวร์และใช้โปรแกรมป้องกันไวรัส

การขโมยข้อมูลตัวตนเป็นภัยคุกคามที่สามารถสร้างความเสียหายทางการเงินและชื่อเสียงของเหยื่อได้ ดังนั้นการป้องกันที่ดีคือการรักษาความปลอดภัยของข้อมูลส่วนตัว ไม่เปิดเผยข้อมูลให้บุคคลที่ไม่น่าเชื่อถือ และใช้มาตรการความปลอดภัยทางไซเบอร์อย่างเหมาะสม

การหลอกลวง (Phishing)

การหลอกลวง (Phishing) เป็นการหลอกลวงของผู้โจมตีผ่านทางอีเมล หรือเว็บไซต์ที่คล้ายกับของจริง เพื่อให้เหยื่อเป้าหมาย กรอกข้อมูลส่วนตัวลงไป โดยส่วนใหญ่จะเป็นข้อมูลเกี่ยวกับการทำธุรกรรมกับธนาคาร หรือที่เกี่ยวข้องกับการใช้ข้อมูลส่วนตัว

วิธีสังเกตว่าอีเมลหรือเว็บไซต์เป็น phishing สังเกตุดังนี้

ตรวจสอบที่อยู่อีเมลว่าใครเป็นคนส่ง เป็นอีเมลที่รู้จักหรือไม่ หากพบว่าเป็นอีเมลที่ไม่รู้แหล่งที่มา ไม่ควรคลิกลิงก์ หรือเปิดไฟล์แนบในอีเมลนั้น

ตรวจสอบ URL ของเว็บไซต์นั้นว่าเป็น URL ของเว็บไซต์ทางการหรือไม่ หากไม่ใช่ ไม่ควรกรอกข้อมูลลงในเว็บไซต์นั้น

วิธีป้องกันการโจมตีแบบ Phishing

- **ตรวจสอบอีเมลอย่างละเอียด** – อย่าเปิดลิงก์หรือดาวน์โหลดไฟล์แนบจากอีเมลที่น่าสงสัย
- **ใช้ Multi-Factor Authentication (MFA)** – แม้รหัสผ่านรั่วไหลก็ยังมีการป้องกันเพิ่มเติม
- **หลีกเลี่ยงการให้ข้อมูลทางโทรศัพท์หรือ SMS** – ธนาคารและองค์กรจริงจะไม่ขอข้อมูลผ่านช่องทางเหล่านี้
- **อัปเดตซอฟต์แวร์และแอนตี้ไวรัสสม่ำเสมอ** – เพื่อป้องกันมัลแวร์ที่อาจมาพร้อมกับ Phishing
- **ฝึกอบรมพนักงานเกี่ยวกับ Social Engineering** – ลดโอกาสที่องค์กรจะถูกโจมตี

Phishing เป็นหนึ่งในภัยคุกคามที่พบได้บ่อยที่สุดและยังคงพัฒนาอย่างต่อเนื่อง การเพิ่มความระมัดระวังและใช้มาตรการรักษาความปลอดภัยที่เหมาะสมจะช่วยลดความเสี่ยงของการถูกโจมตีได้

การโจมตีในรูปแบบ DoS และ DDoS

Countermeasures for DoS and DDoS

Denial-of-Service (DoS)

- สร้างหลุมเพื่อทำการกรองข้อมูลและอนุญาตให้เส้นทางที่มีสิทธิ์ผ่าน
- ปิดกั้นหน่วยข้อมูลขาเข้าต่อหมายเลขพอร์ต
- ใช้ระบบตรวจจับการบุกรุก เพื่อตรวจจับและป้องกันการโจมตี

Distributed DoS (DDoS)

- การป้องกันการโจมตีแบบ DDoS อาจพิจารณาใช้ Content Delivery Network (CDN) หรือเครือข่ายคอมพิวเตอร์แม่ข่ายขนาดใหญ่ ที่กระจายตัวกันอยู่ทั่วโลก ซึ่งเครื่องคอมพิวเตอร์แม่ข่ายเหล่านี้ จะเชื่อมต่อกันผ่านอินเทอร์เน็ต เพื่อทำหน้าที่ในการส่งข้อมูลให้ไปถึงผู้รับปลายทางให้เร็วที่สุด รวมทั้งเพิ่มประสิทธิภาพในการเข้าถึงข้อมูลเหล่านั้นได้ตลอดเวลา

วิธีป้องกันการโจมตี DoS และ DDoS

🔒 **1. ใช้ Web Application Firewall (WAF)** – ป้องกันการโจมตีระดับแอปพลิเคชัน
🔒 **2. ใช้ Load Balancer และ CDN** – กระจายทราฟฟิกเพื่อลดผลกระทบของ DDoS
🔒 **3. เปิดใช้งาน Rate Limiting** – จำกัดจำนวนคำขอจากไอพีเดียวกัน
🔒 **4. ใช้บริการป้องกัน DDoS** – เช่น Cloudflare, AWS Shield หรือ Akamai
🔒 **5. ตรวจสอบและตอบสนองเร็ว** – ใช้ระบบตรวจจับภัยคุกคามแบบเรียลไทม์

DoS และ DDoS เป็นภัยคุกคามที่อาจทำให้ธุรกิจและบริการออนไลน์หยุดชะงักได้ การเตรียมระบบป้องกันที่ดีและใช้เทคโนโลยีที่ทันสมัยจะช่วยลดความเสี่ยงจากการโจมตีเหล่านี้

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

การโจมตีในรูปแบบ Injection

ในการพัฒนาระบบ หากไม่มีการตรวจสอบข้อมูลที่ถูกนำเข้าไปประมวลผล ก็จะมีโอกาสทำให้ผู้ไม่ประสงค์ดีสามารถที่จะปรับแต่ง หรือแก้ไขข้อมูลนำเข้าเหล่านั้นให้อยู่ในรูปแบบภาษาที่ทำให้โปรแกรมทำงานผิดพลาดได้ เช่น การโจมตีที่เรียกว่า SQL Injection ที่ผู้ไม่ประสงค์ดีสามารถเข้าถึง แก้ไข หรือลบข้อมูลในฐานข้อมูลได้ ซึ่งรวมไปถึง ภาษา XML หรือ LDAP Protocol ที่ถูกนำมาใช้ในการเก็บข้อมูลต่าง ๆ

SQL Injection : ผู้ไม่ประสงค์ดี เข้าถึงข้อมูลในฐานข้อมูลได้

วิธีป้องกัน Injection Attack

1. ใช้ Parameterized Queries หรือ Prepared Statements
2. กรองข้อมูลที่รับเข้าทุกช่องทาง (Input Validation & Sanitization)
3. ใช้ Content Security Policy (CSP) เพื่อป้องกัน XSS
4. จำกัดสิทธิ์ของบัญชีที่ใช้รันแอปพลิเคชัน
5. อัปเดตซอฟต์แวร์และแพตช์ช่องโหว่สม่ำเสมอ

การโจมตีแบบ **Injection Attack** เป็นหนึ่งในภัยคุกคามที่อันตรายที่สุด แฮ็กเกอร์สามารถใช้ช่องโหว่นี้เพื่อเข้าถึงข้อมูลที่สำคัญหรือควบคุมระบบได้ การป้องกันต้องใช้การ **ตรวจสอบและกรองข้อมูลที่รับเข้าอย่างเข้มงวด** รวมถึง **ใช้แนวทางการเขียนโค้ดที่ปลอดภัย**

การโจมตีในรูปแบบ Zero-Day Exploits

การโจมตีในรูปแบบ Zero-Day มักจะเกิดขึ้นกับช่องโหว่ที่ถูกค้นพบโดยผู้ไม่ประสงค์ดี โดยที่ผู้ผลิตซอฟต์แวร์ยังไม่ทราบว่าซอฟต์แวร์ของตนมีช่องโหว่ หรือบางกรณีอาจจะเกิดขึ้นโดยที่ผู้ผลิตซอฟต์แวร์รู้ดีว่าผลิตภัณฑ์ของตนมีช่องโหว่ แต่ยังไม่สามารถพัฒนาโปรแกรมปิดช่องโหว่ (Patch) ได้

ผู้ไม่ประสงค์ดีจะพัฒนาโปรแกรมที่ใช้ในการเจาะระบบออกมา เรียกว่า Zero-Day Exploit ซึ่งในบางครั้งจะมีการแจกจ่ายไปยังผู้ไม่ประสงค์ดีรายอื่น ๆ เพื่อนำไปโจมตีระบบ หรืออาจเก็บไว้เพื่อจำหน่าย เพื่อใช้เป็นเครื่องมือในการโจมตีเป้าหมายที่เฉพาะเจาะจงต่อไป

Zero-Day Exploits : ช่องโหว่ที่ค้นพบโดยผู้ไม่ประสงค์ดีก่อนผู้ผลิตที่จะพัฒนาโปรแกรมปิดช่องโหว่ (Patch)

วิธีป้องกันการโจมตี Zero-Day

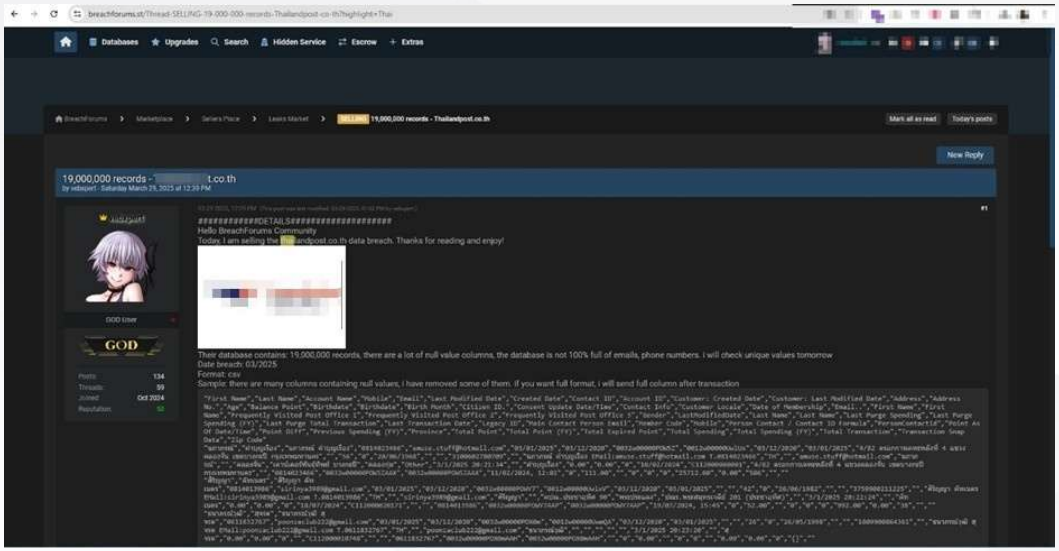
- ✅ 1. อัปเดตซอฟต์แวร์และแพตช์ความปลอดภัยเสมอ
- ✅ 2. ใช้ Next-Gen Antivirus และ EDR (Endpoint Detection & Response)
- ✅ 3. จำกัดสิทธิ์ของผู้ใช้ในระบบ
- ✅ 4. ใช้ Firewall และ Intrusion Detection System (IDS)
- ✅ 5. ฝึกอบรมพนักงานเกี่ยวกับ Phishing และ Social Engineering
- ✅ 6. ใช้ Threat Intelligence & Zero-Day Protection

Zero-Day Exploits เป็นการโจมตีที่รุนแรงและยากต่อการป้องกันเพราะใช้ช่องโหว่ที่ยังไม่มีแพตช์แก้ไข **องค์กรและบุคคลทั่วไปต้องใช้มาตรการป้องกันหลายชั้น** เพื่อจำกัดความเสียหายจากการโจมตีรูปแบบนี้

ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์

ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์

DATA BREACH



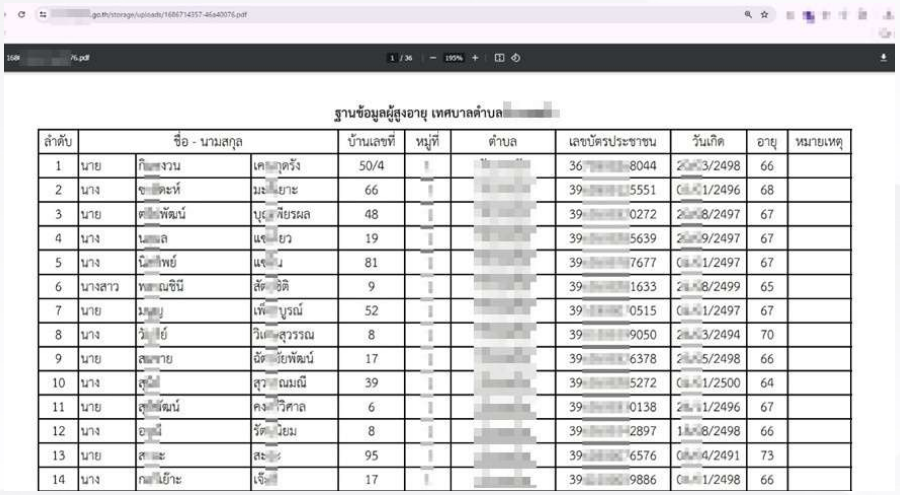
First Name	Last Name	Account Name	Mobile	Email	Last Modified Date	Created Date	Contact ID	Account ID	Customer: Created Date
นภ	ค	นภ บุญเรือง	81 66	am il.com	03 25	03/ 0	00 V5Z	00 lUx	03/ 20
ศิริ	ค	ศิริญ นคร	81 86	siri om	03 25	03/ 0	00 VY7	00 lxV	03/ 20
ธน	ณ	ธนา สุจร	61 97	poo ail.com	03 25	03/ 0	00 k0m	00 mQA	03/ 20
ปิย	ร	ปิยร รัตน	88 24	mo m	15 23	03/ 0	00 KTF	00 msd	03/ 20
สริ	ร	อ ลาย	สริ รัพลาย	65 54	kw l.com	19 25	03/ 0	00 kvm	00 nLA	03/ 20
ปา	ร	ณ	ปาร ษา	61 91	taw ail.com	01 25	03/ 0	00 VOM	00 nnk	03/ 20
อุด	ก	อ ด	อุดม ารสุด	86 84	djd m	07 25	03/ 0	00 r4	00 oGS	03/ 20
นัน	ก	ห	นันท องดี	92 04	par il.com	07 25	03/ 0	00 Jj	00 oj7	03/ 20
บุล		ล วล	บุลก วนวล	90 22	boo ail.com	03 24	03/ 0	00 mA	00 pBY	03/ 20
มา	ป	บุร ญ	มาปิ จเจริญ	85 92	e_t m	04 25	03/ 0	00 Eg	00 pe4	03/ 20
กัล	ณ	เพ็ญ จา	กัลค ลงดีลา	61 45	ch gmail.com	03 25	03/ 0	00 h8	00 q6W	03/ 20
สุภ		วัฒ ยอง	สุภา ยเยือง	81 15	itw com	20 25	03/ 0	00 9k	00 qZ8	03/ 20
สิท	ง	ใจ	สิทธ ทเล	98 57	kar com	07 25	03/ 0	00 cO	00 r2B	03/ 20
กัท		สุร ผี	กัทร งษ์	80 05	nar 8@gmail.c	03 25	03/ 0	00 53	00 rUR	03/ 20
วรร	ก	ฝา นิ	วรรณ ขัยภูมิ	64 22	wa l.com	03 25	03/ 0	00 Xj	00 rx7	03/ 20
สิท	ง	บุ กอบ	สิทธ ปประกอบ	92 35	buc com	03 25	03/ 0	00 l0Q	00 sPo	03/ 20
นิ	ก	พิม โพธิ์	นิจ ภพัทราโพธิ์	93 83	nij mail.com	22 25	03/ 0	00 lSz	00 ssN	03/ 20
พิร	ม์	บุล ตร	พิรด นมุตร	97 57	pad .com	01 25	03/ 0	00 lvh	00 tL5	03/ 20

Citizen ID.	Consent Update Date/Time	Contact Info	Customer	Date of Mer	Email..	First Name	First Name	Frequently Use
31 09		EMail:amus mail.com T.08	TH		amus otma			<img src="/res
37 25		Mail:sirinya com T.08140	TH		sirin mail.c			<img src="/res
18 61		EMail:poonz mail.com T.06	TH		poor @gm			<img src="/res
15 01		Mail:molwipe m T.0889426	TH		molw il.co			<img src="/res
17 79	24/0 5:37	EMail:kwan ail.com T.065	TH	24 21	kwar mail.			<img src="/res
19 19		Mail:taw_tawi l.com T.0611	TH		taw otma			<img src="/res
16 51	09/1):02	EMail:djdjxuc m T.086467	TH	09 21	djdjx l.com			<img src="/res
19 87	07/0 5:33	Mail:panida.r .com T.09207	TH	07 24	092 ostf			<img src="/res
19 11		Mail:bookbo ail.com T.090	TH		book @gm			<img src="/res
11 39	27/0 45	EMail:e_tingl om T.085999	TH	27 22	e_tin il.co			<img src="/res
18 11		EMail:chevyh @gmail.com T	TH		chev 46@			<img src="/res
35 50		Mail:itw2014 com T.08128	TH		itw2 mail.c			<img src="/res
17 41	30/0 5:45	Mail:kareem com T.09851	TH	30 23	081 ostf			<img src="/res
11 45		Mail:namkhin 3@gmail.com	TH		nam n020			<img src="/res
13 58		EMail:wanw ail.com T.064	TH		wan mail.			<img src="/res
34 49		EMail:budc ail.com T.092	TH		budc mail.			<img src="/res
34 17	08/0 11	EMail:nijpr @gmail.com	TH	08 24	093 ostf			<img src="/res

ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์

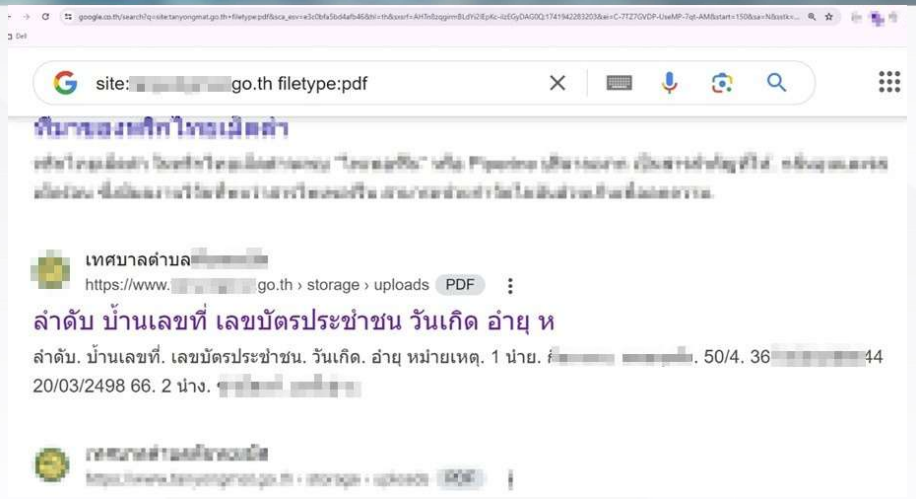
DATA LEAK

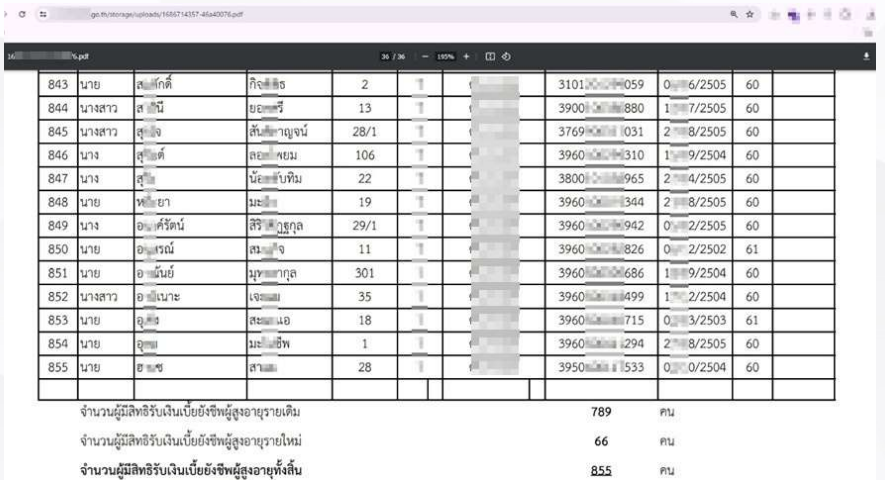
site: .go.th filetype:pdf
หรือ xlsx



ฐานข้อมูลผู้สูงอายุ เทศบาลตำบล

ลำดับ	ชื่อ - นามสกุล		บ้านเลขที่	หมู่ที่	ตำบล	เลขบัตรประชาชน	วันเกิด	อายุ	หมายเหตุ
1	นาย		50/4			36 8044	3/2498	66	
2	นาง		66			39 5551	1/2496	68	
3	นาย		48			39 0272	8/2497	67	
4	นาง		19			39 5639	9/2497	67	
5	นาง		81			39 7677	1/2497	67	
6	นางสาว		9			39 1633	8/2499	65	
7	นาย		52			39 0515	1/2497	67	
8	นาง		8			39 9050	3/2494	70	
9	นาย		17			39 6378	5/2498	66	
10	นาง		39			39 5272	1/2500	64	
11	นาย		6			39 0138	1/2496	67	
12	นาง		8			39 2897	8/2498	66	
13	นาย		95			39 6576	4/2491	73	
14	นาง		17			39 9886	1/2498	66	





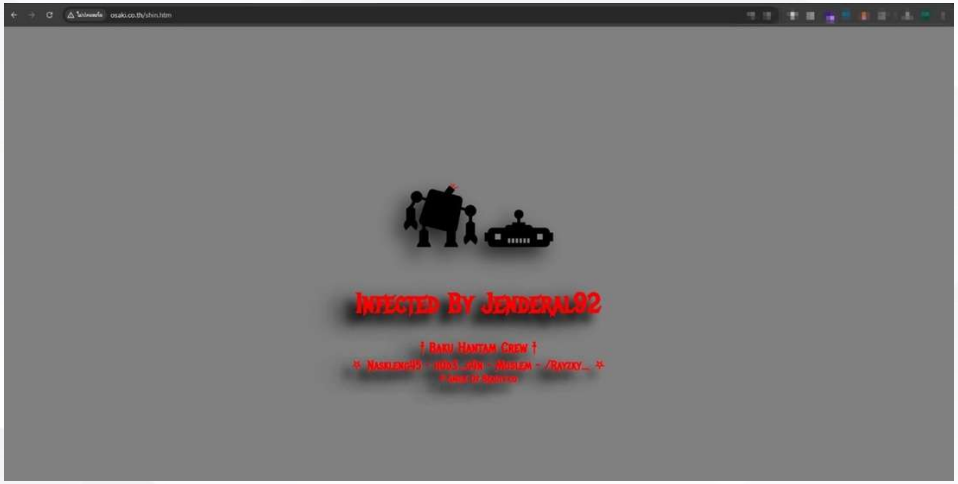
843	นาย		2			3101 059	6/2505	60
844	นางสาว		13			3900 880	7/2505	60
845	นางสาว		28/1			3769 031	8/2505	60
846	นาง		106			3960 310	9/2504	60
847	นาง		22			3800 965	4/2505	60
848	นาย		19			3960 344	8/2505	60
849	นาง		29/1			3960 942	2/2505	60
850	นาย		11			3960 826	2/2502	61
851	นาย		301			3960 686	9/2504	60
852	นางสาว		35			3960 499	2/2504	60
853	นาย		18			3960 715	3/2503	61
854	นาย		1			3960 294	8/2505	60
855	นาย		28			3950 533	0/2504	60
	จำนวนผู้มีสิทธิรับเงินเบี้ยยังชีพผู้สูงอายุรายเดิม					789	คน	
	จำนวนผู้มีสิทธิรับเงินเบี้ยยังชีพผู้สูงอายุรายใหม่					66	คน	
	จำนวนผู้มีสิทธิรับเงินเบี้ยยังชีพผู้สูงอายุทั้งสิ้น					855	คน	

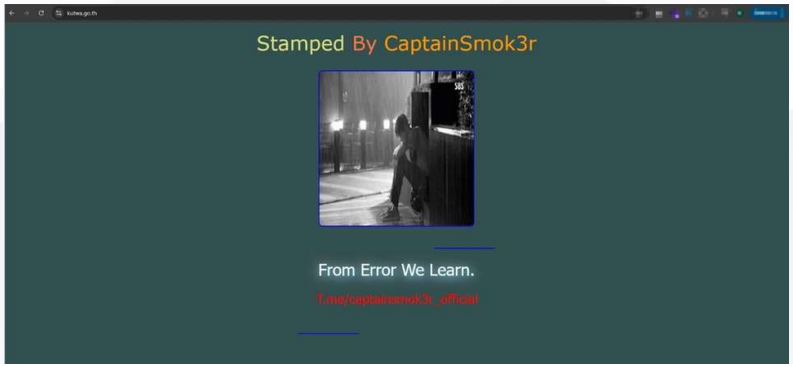
ข้อมูลผู้ใช้งานระบบของกระทรวงสาธารสุขรวมกว่า 1 ล้านรายการ

1000618	https://envoccsurvey.ddc.moph.g
1000619	https://dashboard.anamai.moph.g
1000620	https://inspection.moph.go.th/e-i
1000621	http://www.pro.moph.go.th/w54/
1000622	https://savethai.anamai.moph.g
1000623	https://stopcovid.anamai.moph.g
1000624	http://bkhdc2.moph.go.th/cockpi
1000625	https://3doctor.hss.moph.go.th/
1000626	https://stopcovid.anamai.moph.g
1000627	https://esta.hss.moph.go.th/serv
1000628	https://ilabplus.dmsc.moph.go.th
1000629	https://kkpho.moph.go.th/planfin
1000630	ttps://ltc.anamai.moph.go.th/fo
1000631	

ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์

HACKED WEBSITE (DEFACEMENT)

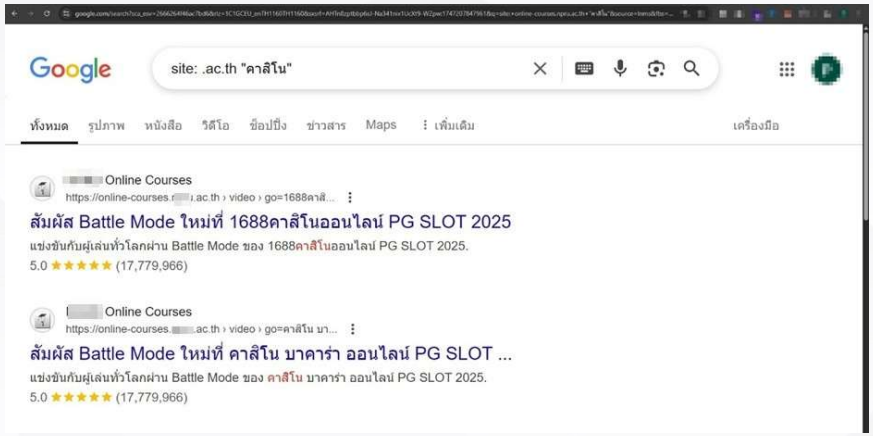


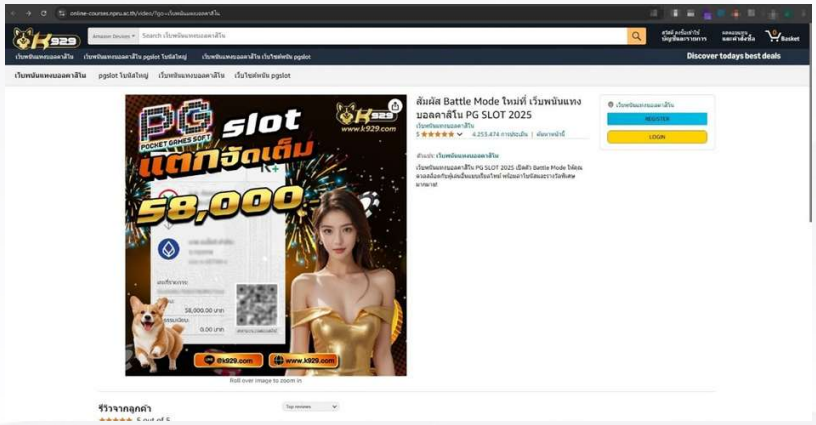


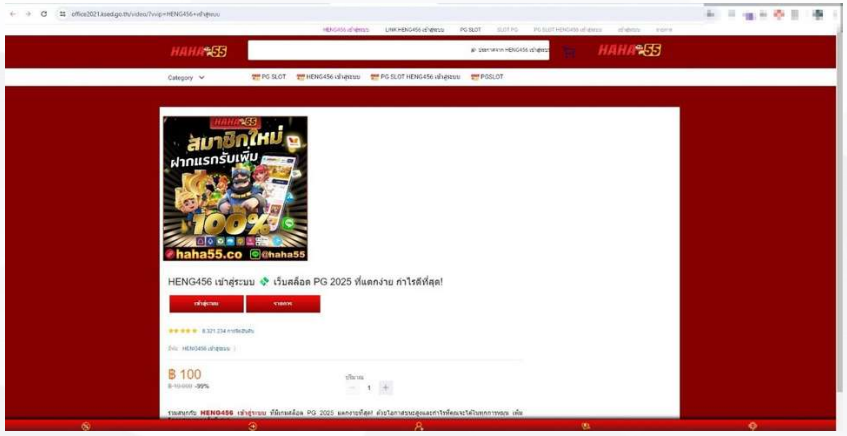
ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์

HACKED WEBSITE (GAMBLING)

site: .go.th หรือ .ac.th
“คาสิโน” slot บาคาร่า
sbobet เป็นต้น







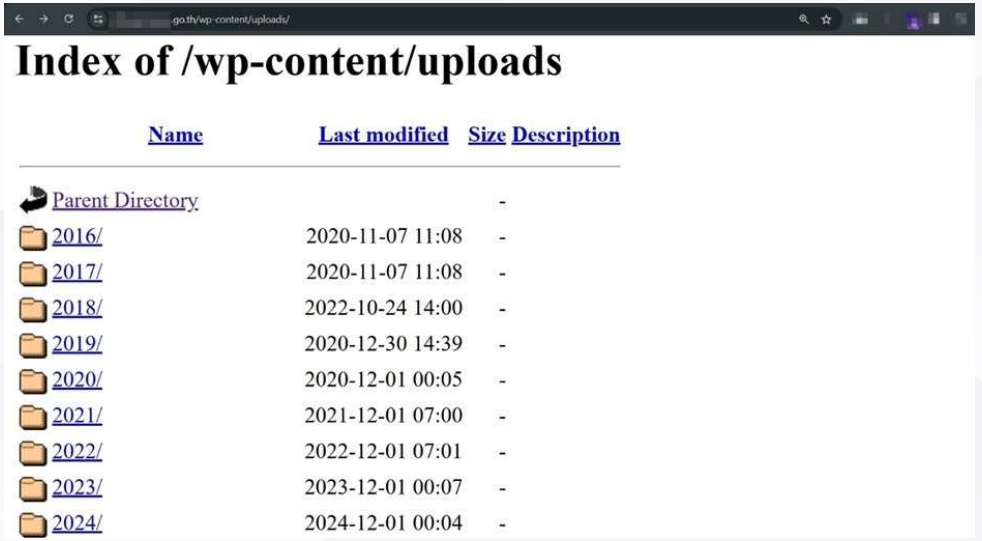
ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์

SECURITY MISCONFIGURATION

DIRECTORY LISTING

Index of /Web2024

Name	Last modified	Size	Description
Parent Directory		-	
Executive_office/	2023-03-11 10:57	-	
Facebook Messenger C..>	2023-06-28 16:59	1.2K	
Facebook Messenger C..>	2022-07-18 10:29	1.1K	
Logo.png	2020-06-23 09:59	93K	
PM25.php	2024-03-12 09:17	10K	
UpRightSchool/	2022-06-14 13:50	-	
_groups/	2022-06-14 13:50	-	
about.html	2020-06-19 11:07	23K	

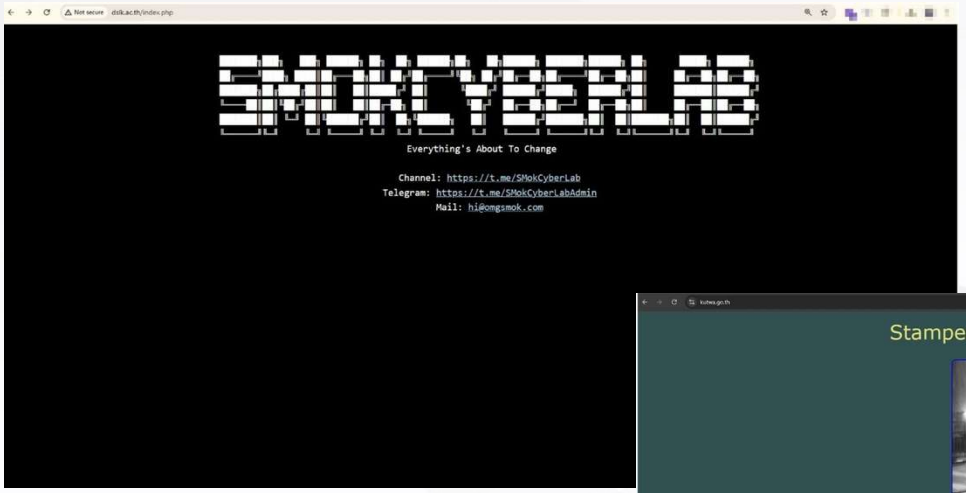


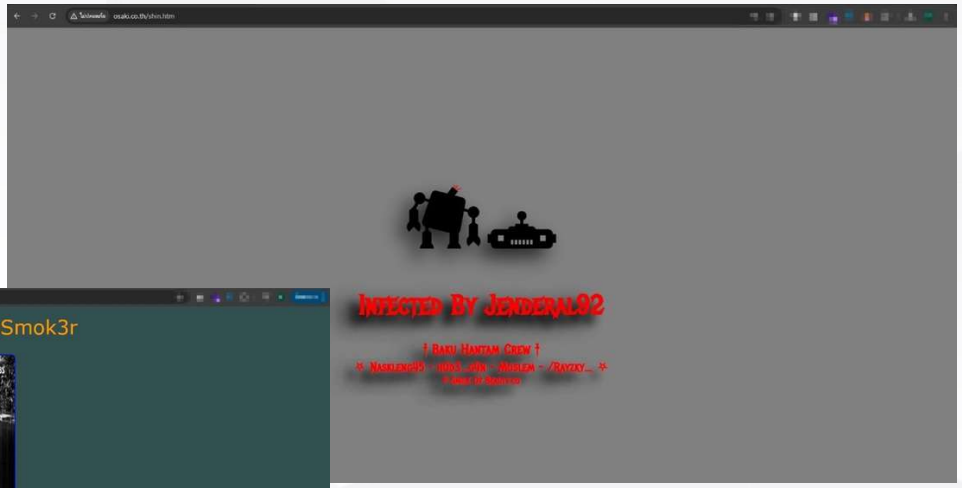
Index of /wp-content/uploads

Name	Last modified	Size	Description
Parent Directory		-	
2016/	2020-11-07 11:08	-	
2017/	2020-11-07 11:08	-	
2018/	2022-10-24 14:00	-	
2019/	2020-12-30 14:39	-	
2020/	2020-12-01 00:05	-	
2021/	2021-12-01 07:00	-	
2022/	2022-12-01 07:01	-	
2023/	2023-12-01 00:07	-	
2024/	2024-12-01 00:04	-	

ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์

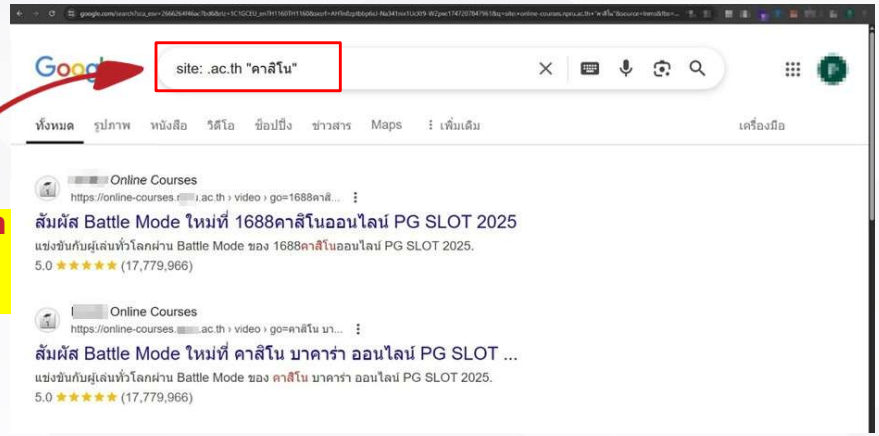
HACKED WEBSITE (DEFACEMENT)



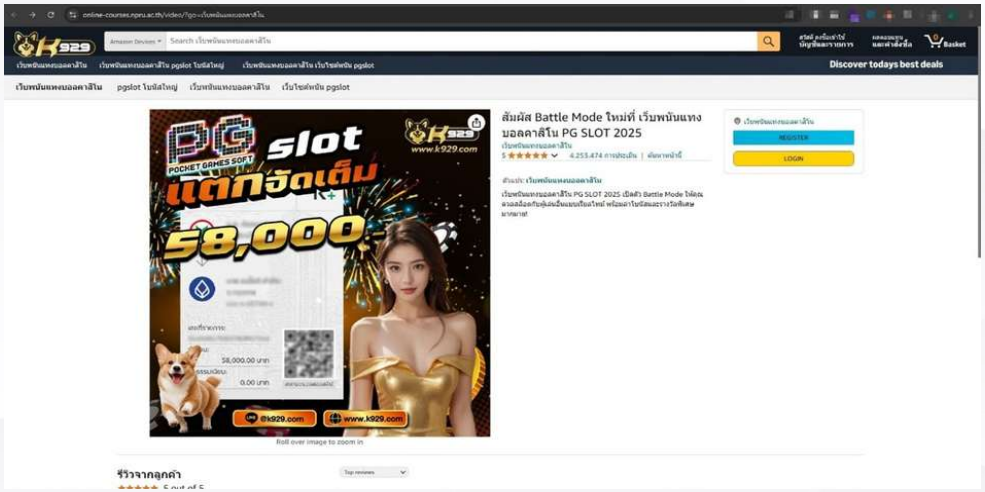


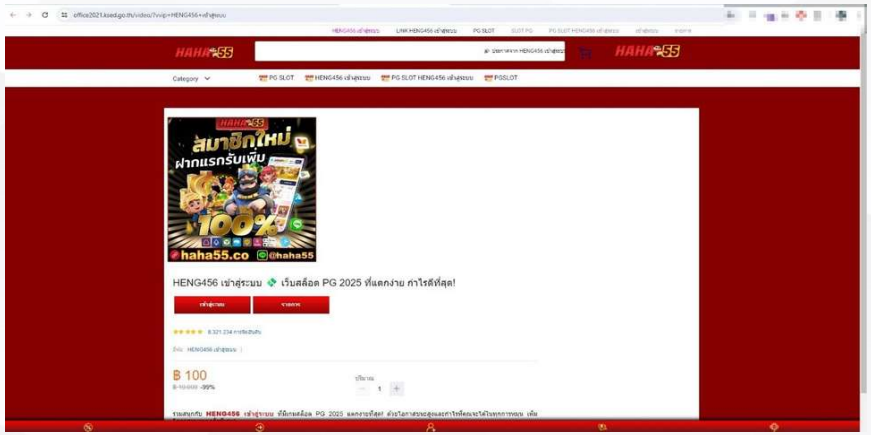
ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์

HACKED WEBSITE (GAMBLING)



site: .go.th หรือ .ac.th "คาสิโน" slot บาคาร่า sbobet เป็นต้น





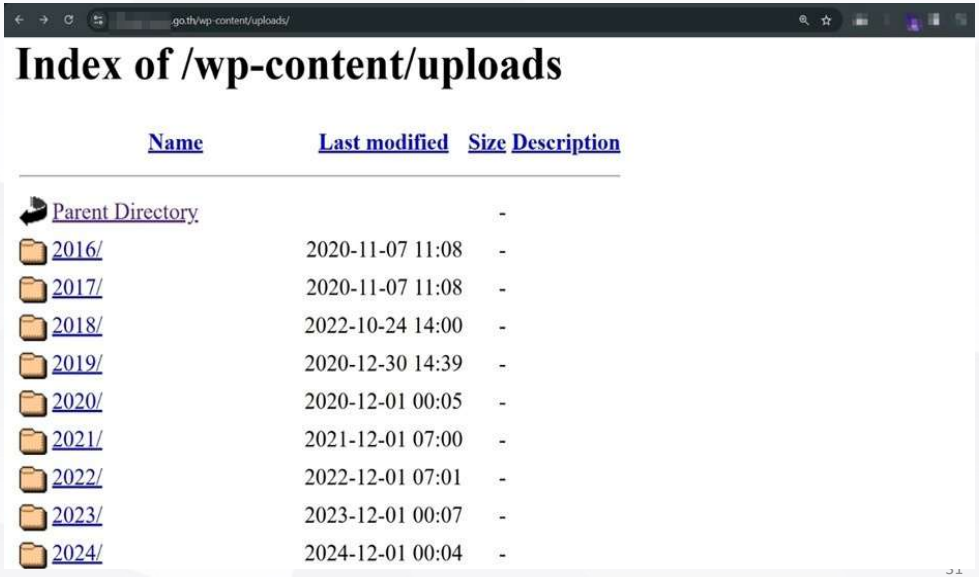
ตัวอย่างรูปแบบภัยคุกคามทางไซเบอร์

SECURITY MISCONFIGURATION

DIRECTORY LISTING

Index of /Web2024

Name	Last modified	Size	Description
Parent Directory		-	
Executive_office/	2023-03-11 10:57	-	
Facebook Messenger C..>	2023-06-28 16:59	1.2K	
Facebook Messenger C..>	2022-07-18 10:29	1.1K	
Logo.png	2020-06-23 09:59	93K	
PM25.php	2024-03-12 09:17	10K	
UpRightSchool/	2022-06-14 13:50	-	
_groups/	2022-06-14 13:50	-	
about.html	2020-06-19 11:07	23K	

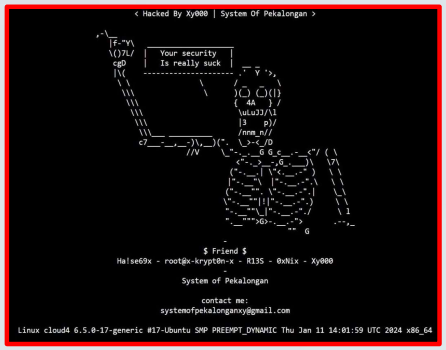


Index of /wp-content/uploads

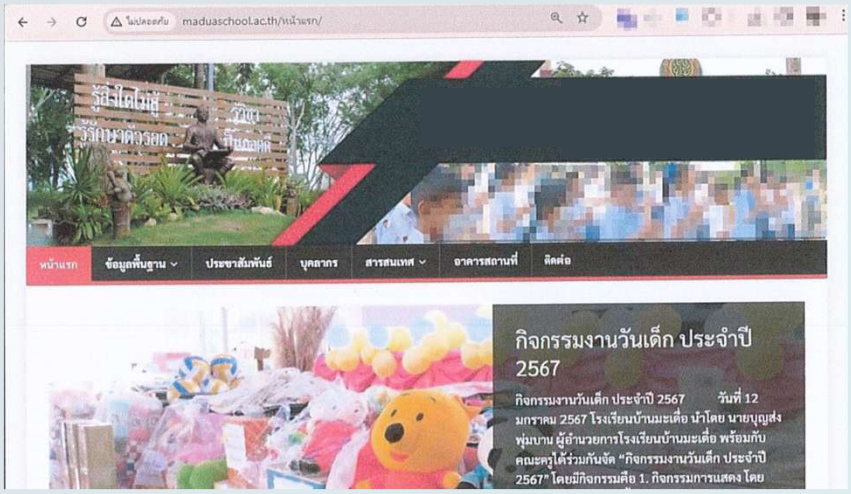
Name	Last modified	Size	Description
Parent Directory		-	
2016/	2020-11-07 11:08	-	
2017/	2020-11-07 11:08	-	
2018/	2022-10-24 14:00	-	
2019/	2020-12-30 14:39	-	
2020/	2020-12-01 00:05	-	
2021/	2021-12-01 07:00	-	
2022/	2022-12-01 07:01	-	
2023/	2023-12-01 00:07	-	
2024/	2024-12-01 00:04	-	

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

เว็บไซต์ถูกโจมตี ด้วยการเปลี่ยนแปลงหน้าเว็บไซต์และ ฝังเว็บการพนันออนไลน์ พร้อมอวดชื่อบนหน้าเว็บไซต์โรงเรียน

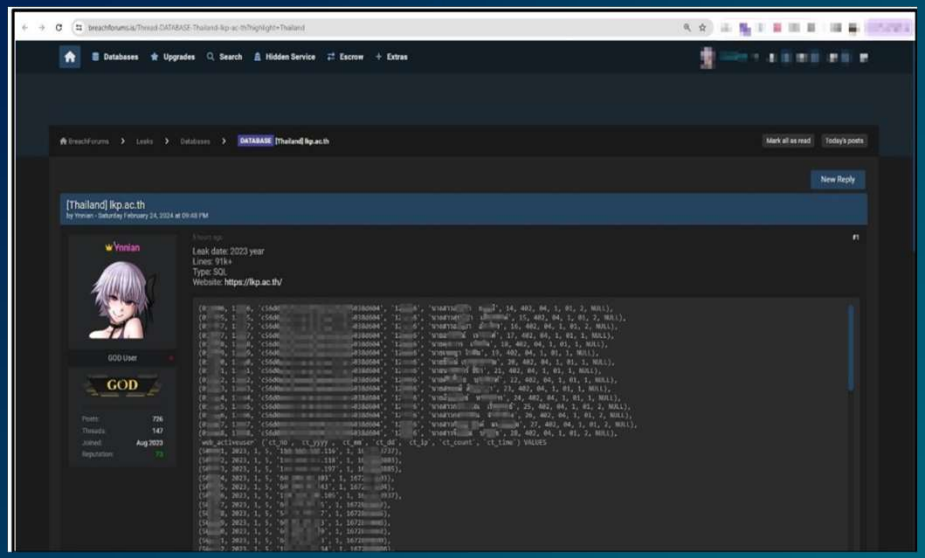


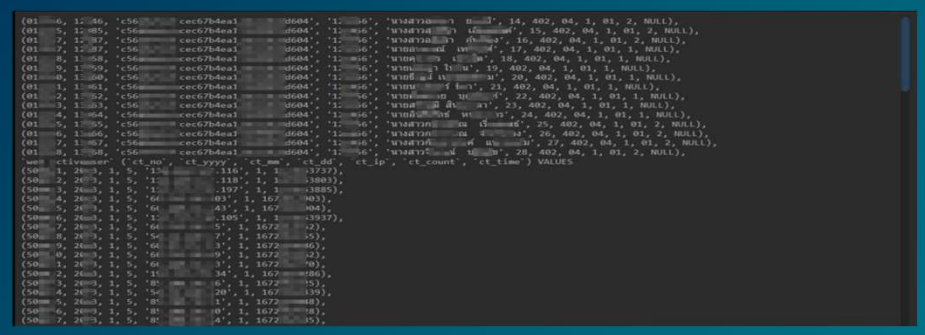
ตรวจพบเว็บไซต์หน่วยงานการศึกษา ถูกโจมตีด้วยการเปลี่ยนแปลงหน้าเว็บไซต์ (Website Defacement) และถูกฝังเว็บพนันออนไลน์

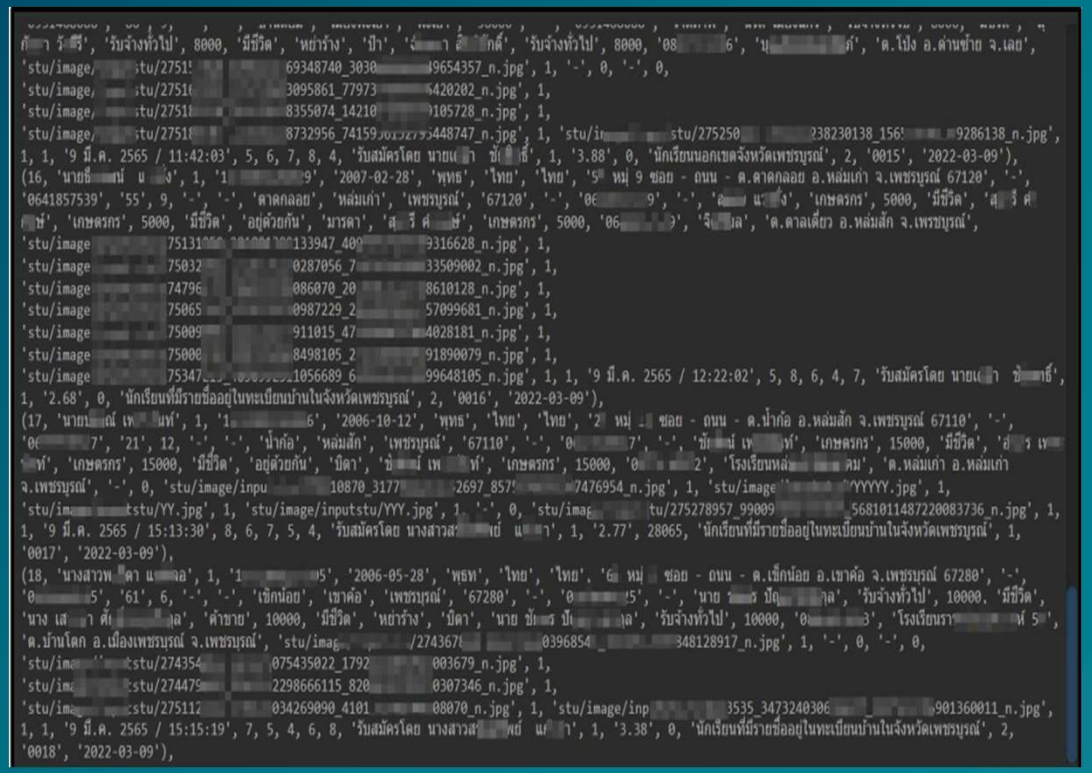


NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

ประกาศขายข้อมูลหน่วยงานการศึกษาจากเว็บไซต์ BreachForums เป็นข้อมูลของโรงเรียนแห่งหนึ่ง

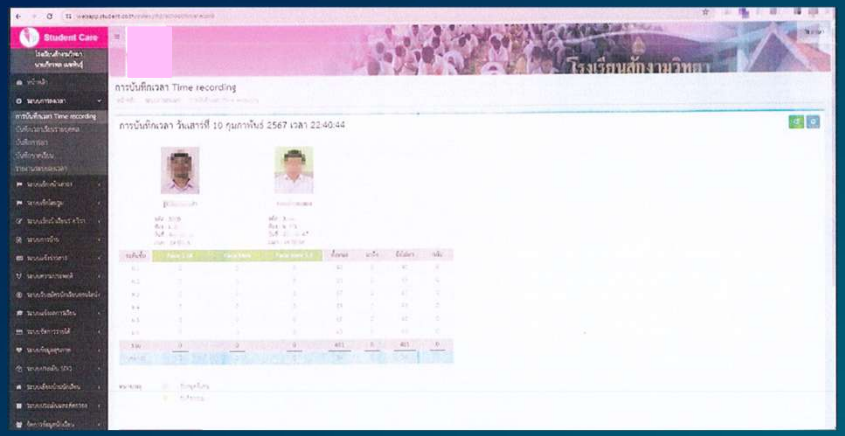


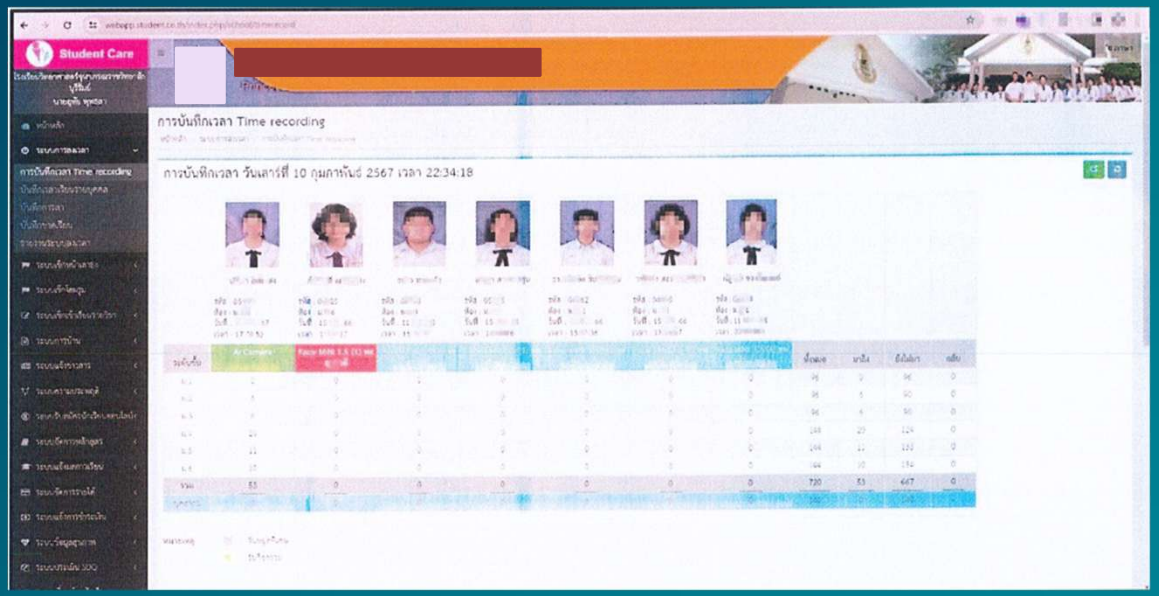


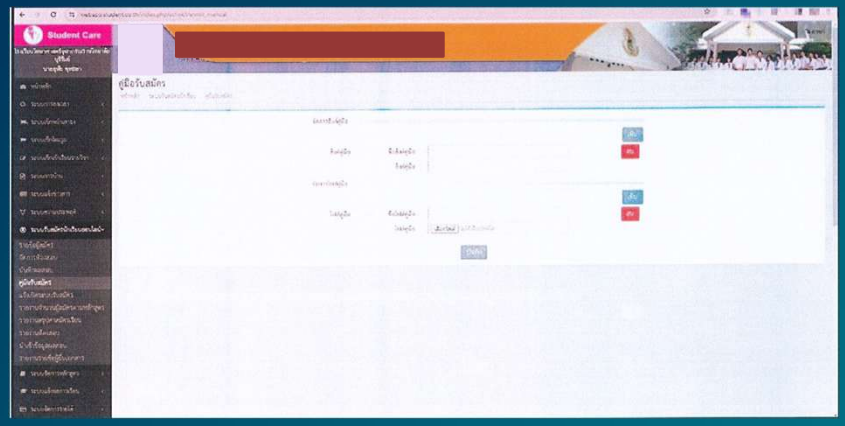


NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

โรงเรียน ใช้ Username และ Password
ด้วยเบอร์ส่วนตัว ระบบจึงเกิดการโดน แฮก มีข้อมูลนักเรียน/ผู้ปกครอง รั่วไหล

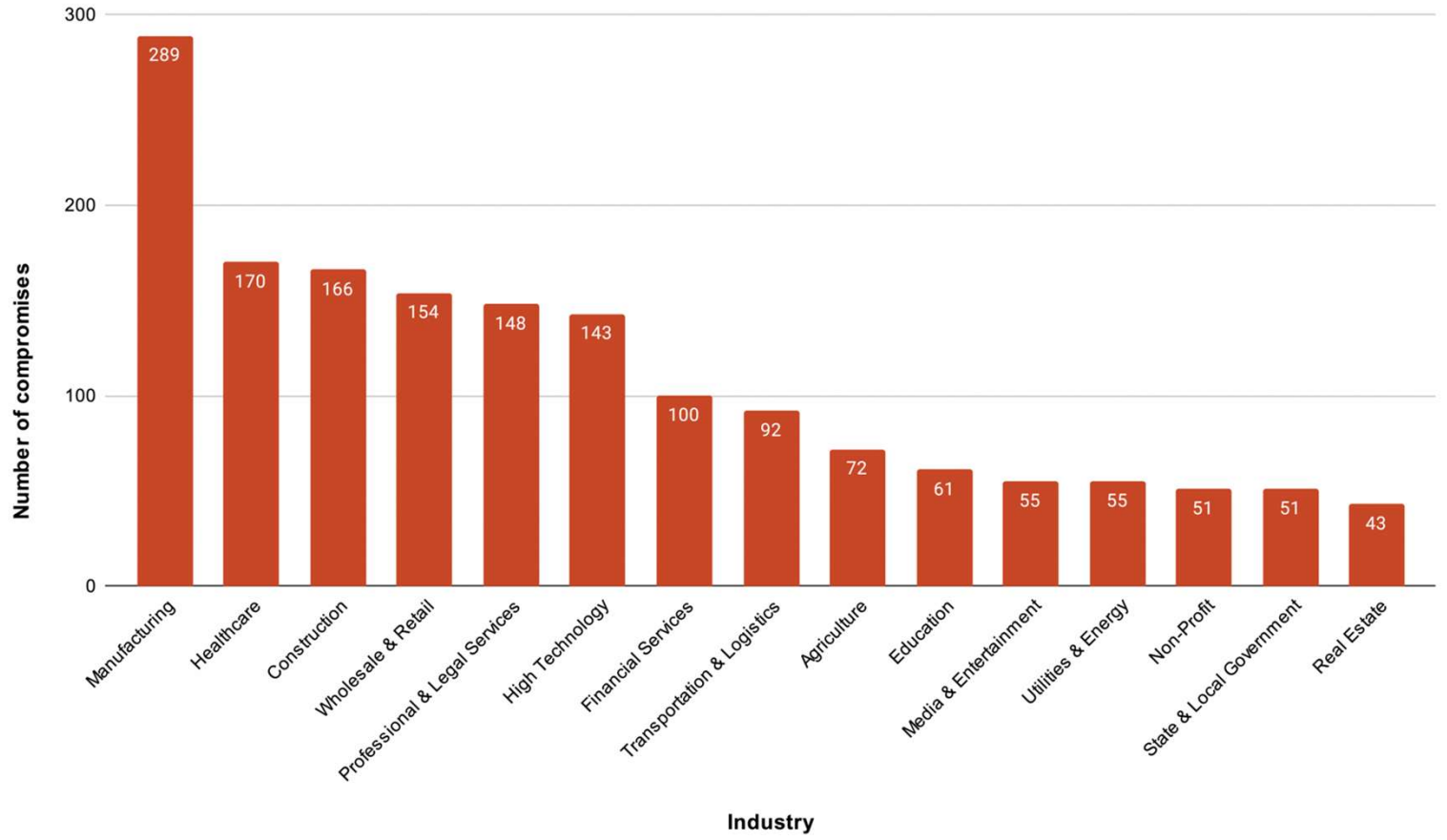


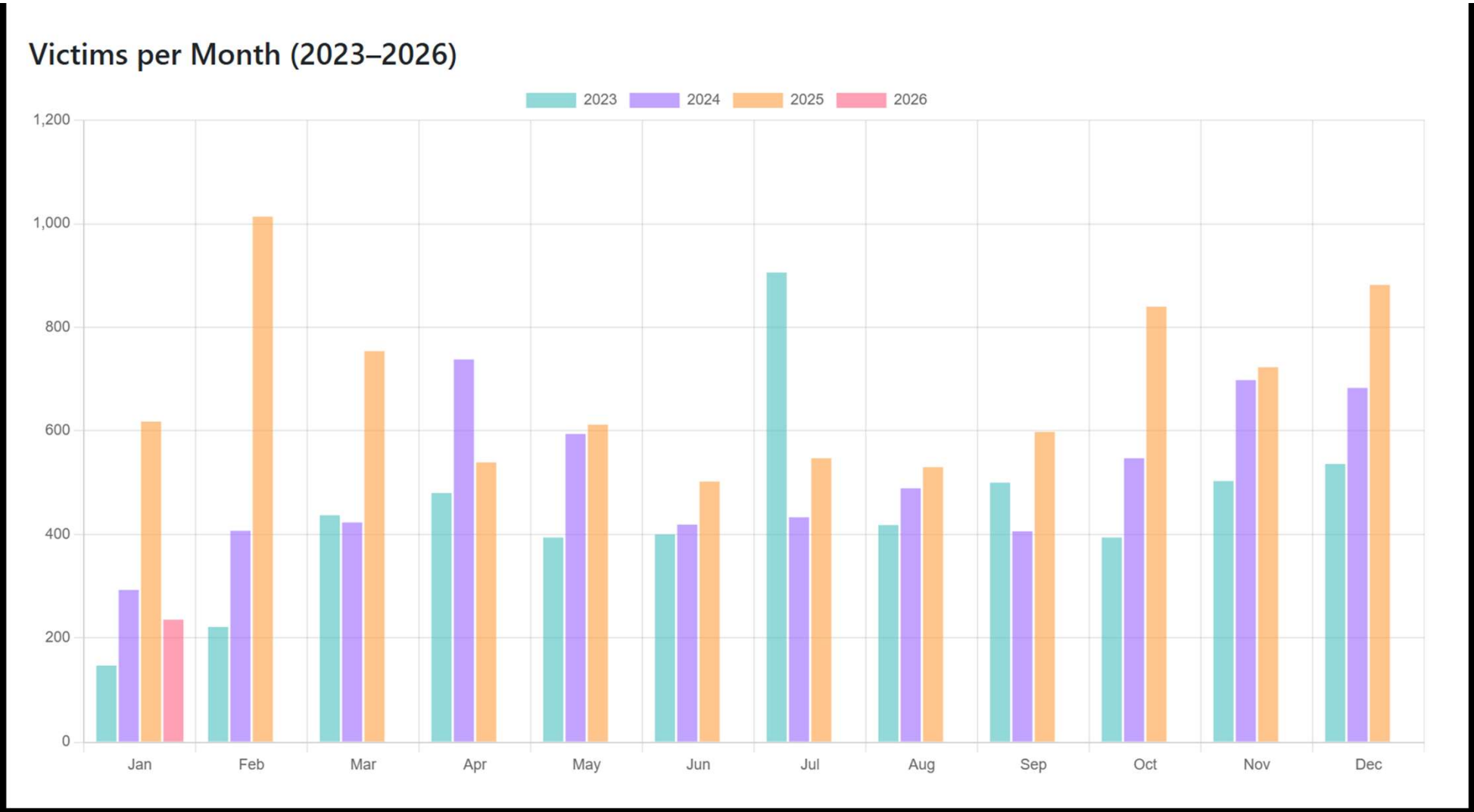




เมื่อวันที่ 10 กุมภาพันธ์ ได้รับแจ้งเหตุภัยคุกคามทางไซเบอร์
พบการเข้าถึงชื่อผู้ใช้งานและรหัสผ่าน ของหน่วยงานการศึกษา
โดย ทางหน่วยงานได้เลือกใช้ชื่อผู้ใช้งานและรหัสผ่านเป็นเบอร์โทรศัพท์ส่วนตัว
ซึ่งเป็นความเสี่ยง ทำให้สามารถโดนเข้าถึงข้อมูลส่วนบุคคลหรือข้อมูลสำคัญ
โดยไม่ได้รับอนุญาต

Industries Most Impacted by Ransomware





https://www.ransomware.live/stats

10 อันดับชื่อผู้ใช้งานที่ถูกใช้ในการเจาะระบบ **(Honey Pot)**

Username	Password
sa	(empty)
root	(empty)
root	root
admin	1111
admin	admin
ProXyusEr	654321
admin	7ujMko0admin
root	12345
root	123456

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

คำแนะนำในการป้องกันองค์กรของ สกมช.

01 อัปเดตซอฟต์แวร์และระบบอยู่เสมอและ หลีกเลี่ยงการดาวน์โหลดและติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์ (Software Updates & Patching)

02 สำรองข้อมูลอย่างปลอดภัยและเป็นประจำ (Data Backup and Disaster Recovery)

03 ยกระดับความปลอดภัยด้วยการยืนยันตัวตน 2 ขั้นตอน (2FA)

04 แต่งตั้งและเสริมบทบาทของ DPO และ CISO

05 จัดตั้ง SOC ตลอดจนตรวจสอบและวิเคราะห์กิจกรรมในเครือข่ายอย่างสม่ำเสมอ

06 จัดการความเสี่ยงจากการใช้ AI อย่างมีจริยธรรม (AI Risk Management)

07 ส่งเสริมการใช้รหัสผ่านที่ปลอดภัยและนโยบาย Zero-Trust

08 มีการกำกับดูและคัดเลือกบริษัทที่มีประสบการณ์และมาตรฐานความปลอดภัย และหลีกเลี่ยงการใช้ข้อมูลจริงในขั้นตอนการพัฒนา

09 ป้องกัน Insider Threat และจัดการ Offboarding อย่างปลอดภัย

10 ให้ความรู้แก่พนักงานและปรับปรุงความรู้ด้านความปลอดภัยไซเบอร์

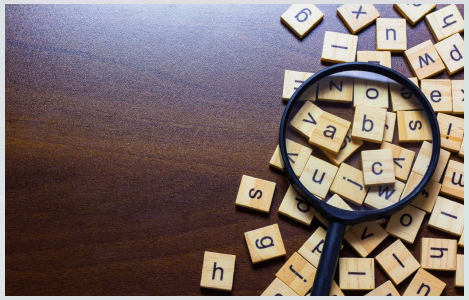
NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

รายงานการแจ้งเหตุข้อมูลการรั่วไหลเหตุเกิดจากการตั้งรหัสที่คาดเดาง่ายเกินไป

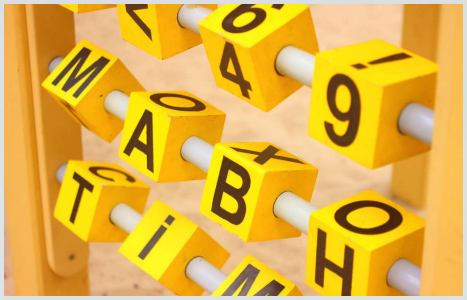
จำนวน 261 หน่วยงาน
มีจำนวน 91,655 user

การตั้งรหัสผ่านที่คาดเดาได้ง่ายยังคงเป็นปัญหาที่พบอย่างต่อเนื่องในปัจจุบัน ซึ่งอาจนำไปสู่ความเสี่ยงด้านความปลอดภัยทางไซเบอร์ จากการศึกษาของ NordPass ในปี 2024 พบว่ารหัสผ่านที่พบบ่อยที่สุดยังคงเป็น "123456" ซึ่งสามารถถูกแฮกได้ภายในเวลาไม่ถึง 1 วินาที

มีประเภทของรหัสผ่าน
เป็นตัวเลขล้วน



มีประเภทของรหัสผ่าน
เป็นตัวอักษรอังกฤษล้วน



มีประเภทของรหัสผ่าน
เป็นตัวเลขและตัวอักษรภาษาอังกฤษ

มีประเภทของรหัสผ่าน
เป็นตัวเลขและตัวอักษรภาษาอังกฤษและอักขระพิเศษ

ติดต่อสอบถามข้อมูลเพิ่มเติมที่ 02-142-6885 coordination_2@ncsa.or.th NCSA Thailand

กรอบแนวทางการป้องกันภัยคุกคามทางไซเบอร์ (MITRE D3FEND Framework)

What is MITRE?

MITRE Corporation
คือองค์กรไม่แสวงหาผลกำไร (Non-profit organization)
จากสหรัฐอเมริกาที่มีบทบาทสำคัญระดับโลกในด้านวิทยาศาสตร์ เทคโนโลยี และความมั่นคง

ภารกิจหลักของ MITRE
MITRE ไม่ได้เป็นหน่วยงานรัฐบาลและไม่ใช่บริษัทเอกชนที่มุ่งเน้นกำไร
แต่ทำหน้าที่เป็น "ที่ปรึกษาที่เชื่อถือได้" (Trusted Advisor) ซึ่งเชื่อมโยงระหว่างภาครัฐ ภาคเอกชน และภาคการศึกษา
เพื่อสร้างนวัตกรรมที่ใช้ได้จริง

ผลงานที่เป็นที่รู้จักระดับโลก (Cybersecurity) ได้แก่:
CVE (Common Vulnerabilities and Exposures):
ระบบหมายเลขมาตรฐานสากลสำหรับระบุช่องโหว่ของซอฟต์แวร์ (เช่น CVE-2023-XXXXX)
MITRE ATT&CK®: กรอบการทำงาน (Framework)
ที่รวบรวมเทคนิคและวิธีการที่แฮกเกอร์ใช้ในการโจมตี เพื่อให้ผู้เชี่ยวชาญนำไปใช้วางแผนป้องกัน

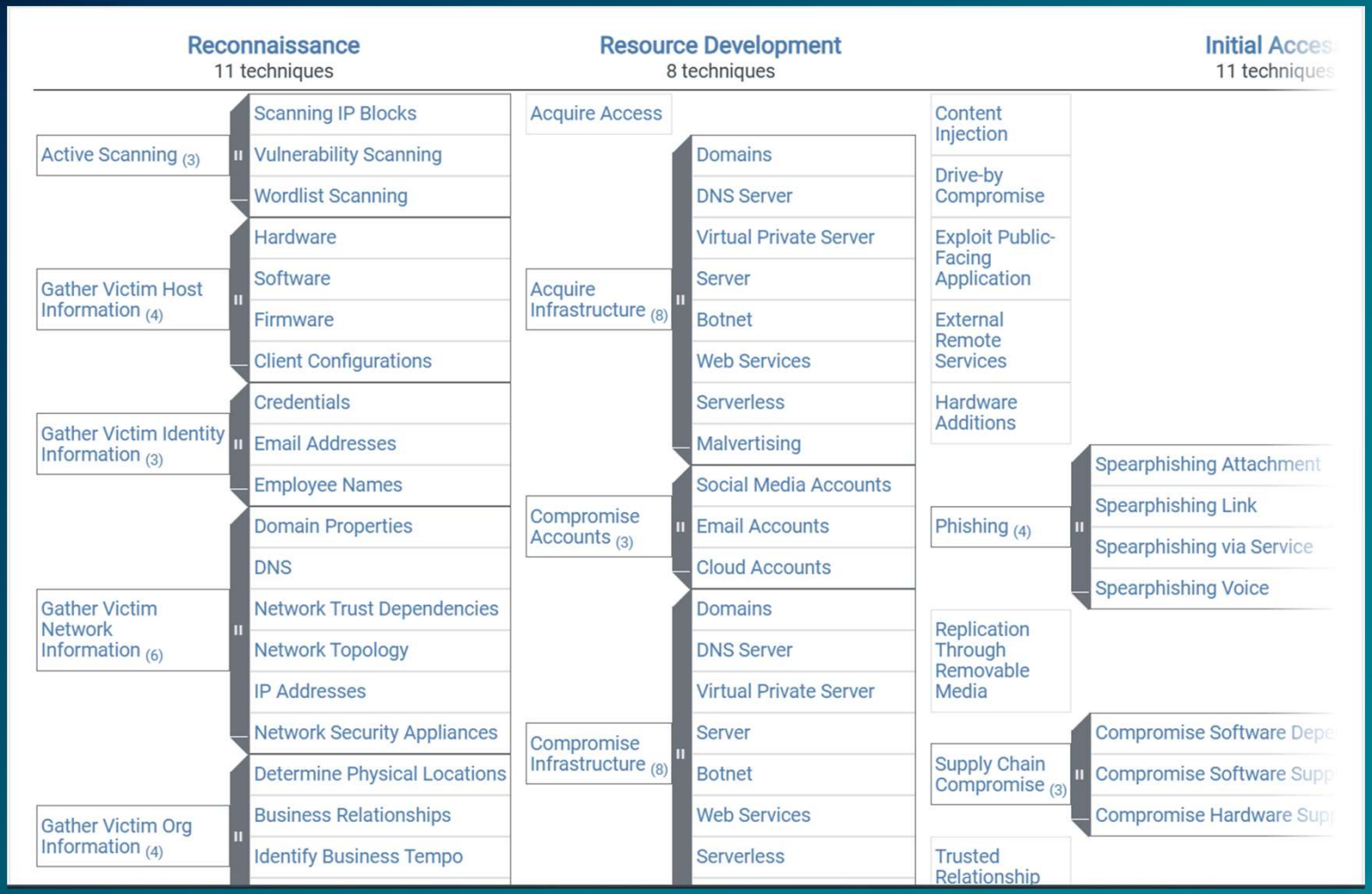

MITRE
ATT&CK®
Adversary Tactics & Techniques
Tactics
Techniques
Procedures
Combat Real-
World Threats
Community Driven
Knowledge

MITRE ATT&CK Tactics in the Enterprise Matrix

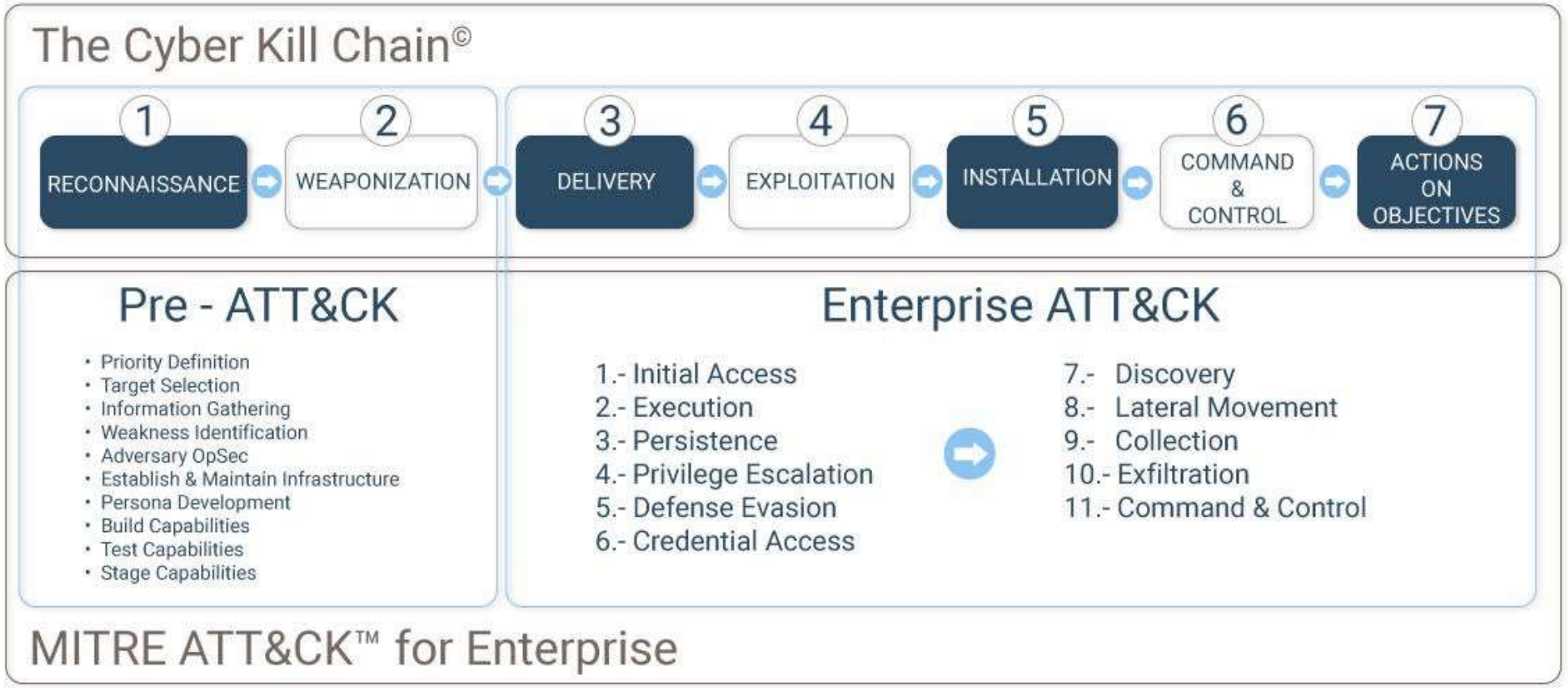
Credit: https://delinea.com/blog/what-is-the-mitre-attack-framework

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

ทำไม ATT&CK อย่างเดียวไม่พอ



The MITRE ATT&CK™ for Enterprise and the Cyber Kill Chain©



Source: MITRE, ATT&CK™ for Enterprise
Lockheed Martin Cyber Kill Chain©

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

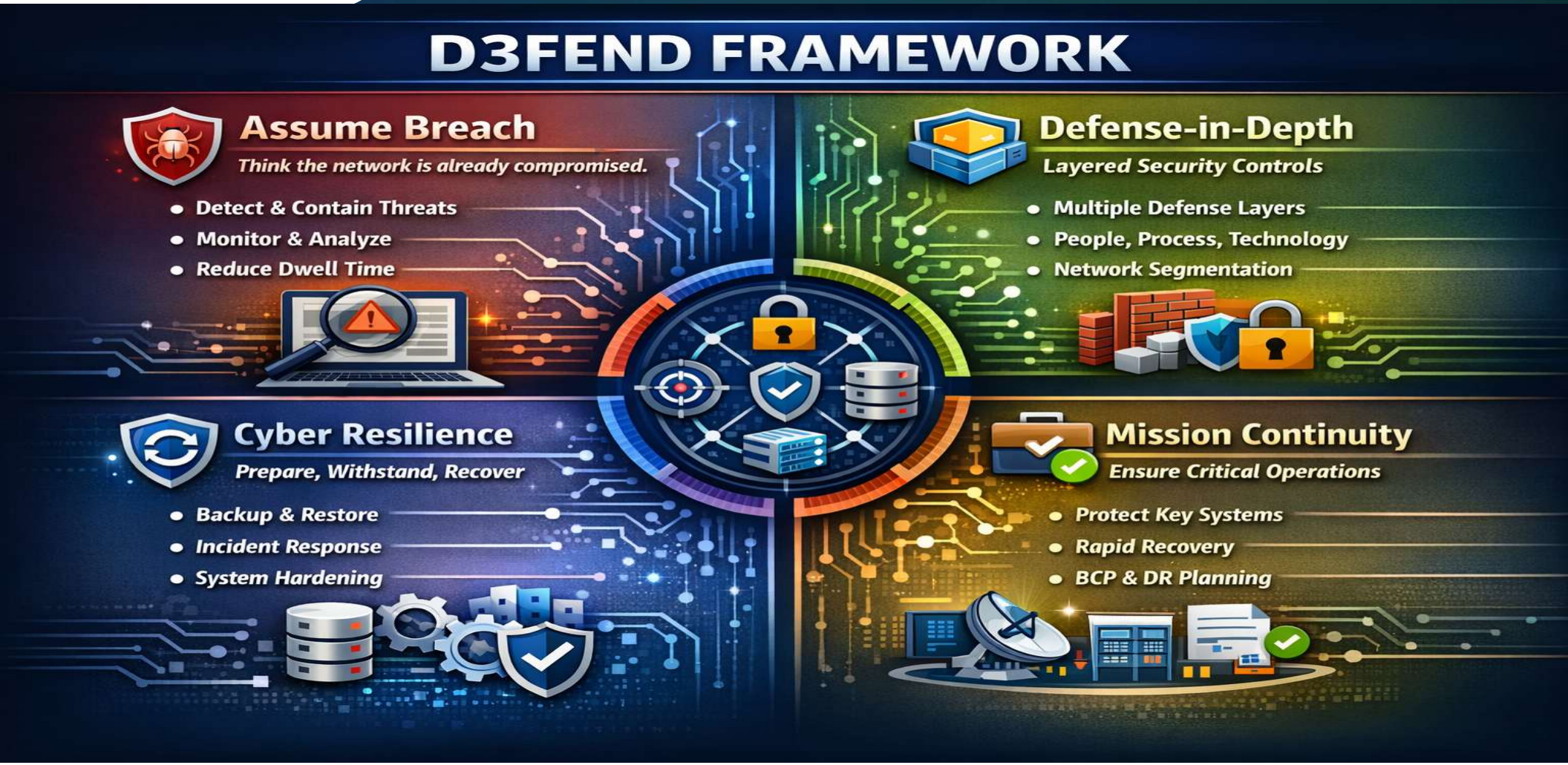
ทำไม ATT&CK อย่างเดียวไม่พอ

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

MITRE D3FEND คืออะไร

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

กรอบแนวคิด D3FEND

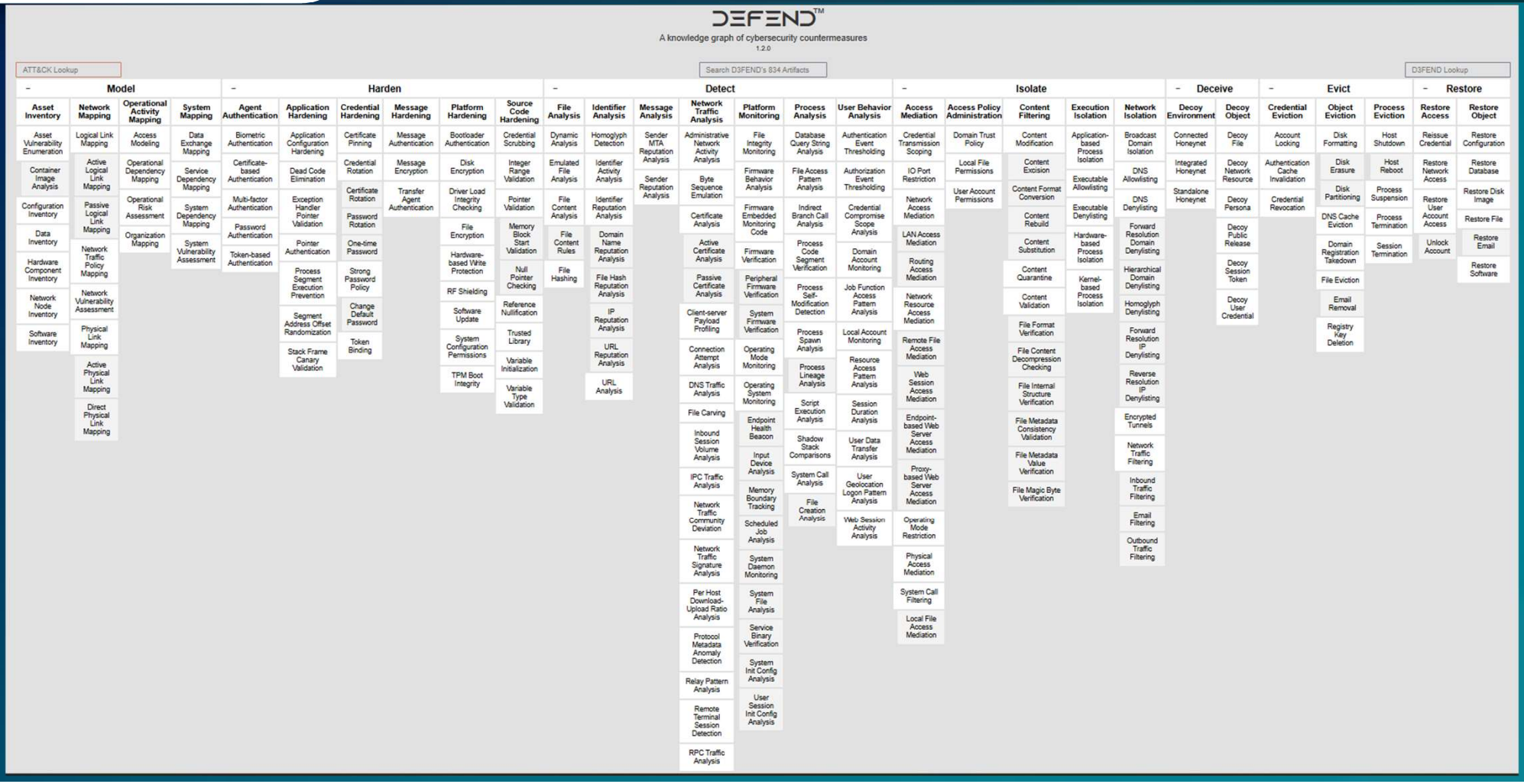


โครงสร้าง MITRE D3FEND


MITRE D3FEND
Structure of D3FEND
Defensive Tactics
Harden
Detect
Isolate
Deceive
Evict
Restore
Defensive Techniques
Encrypt Data
Network Traffic Analysis
File Analysis
Digital Artifacts
Files
0101
0101
1101
Telemetry
Reports

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

MITRE D3FEND Framework



NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

MITRE D3FEND Framework

- Model
- Harden
- Detect
- Isolate
- Deceive
- Evict
- Restore

MITRE ออกแบบ Model เพื่ออธิบายว่าการป้องกันที่ดีต้องอาศัยความเข้าใจ 4 มิติหลักของระบบ

- ทรัพย์สิน (Assets)
- โครงสร้างเชิงตรรกะและกายภาพ (Links)
- การทำงานและการพึ่งพา (Operations)
- ระบบและช่องโหว่ (Systems)

Model สนับสนุน Defensive Tactics ทุกตัว

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

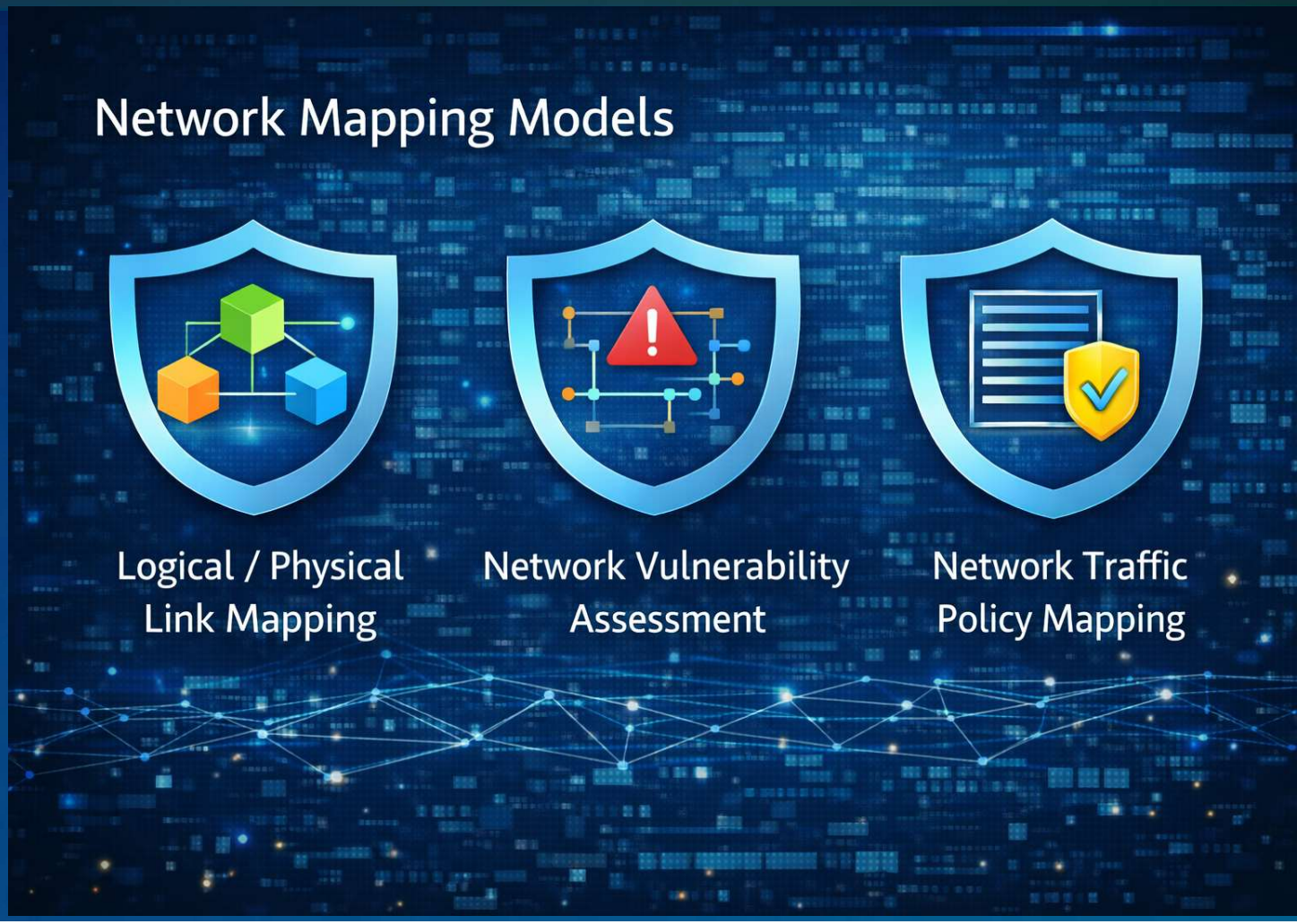
MITRE D3FEND Framework

- Model
- Harden
- Detect
- Isolate
- Deceive
- Evict
- Restore

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

MITRE D3FEND Framework

- Model
- Harden
- Detect
- Isolate
- Deceive
- Evict
- Restore



NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

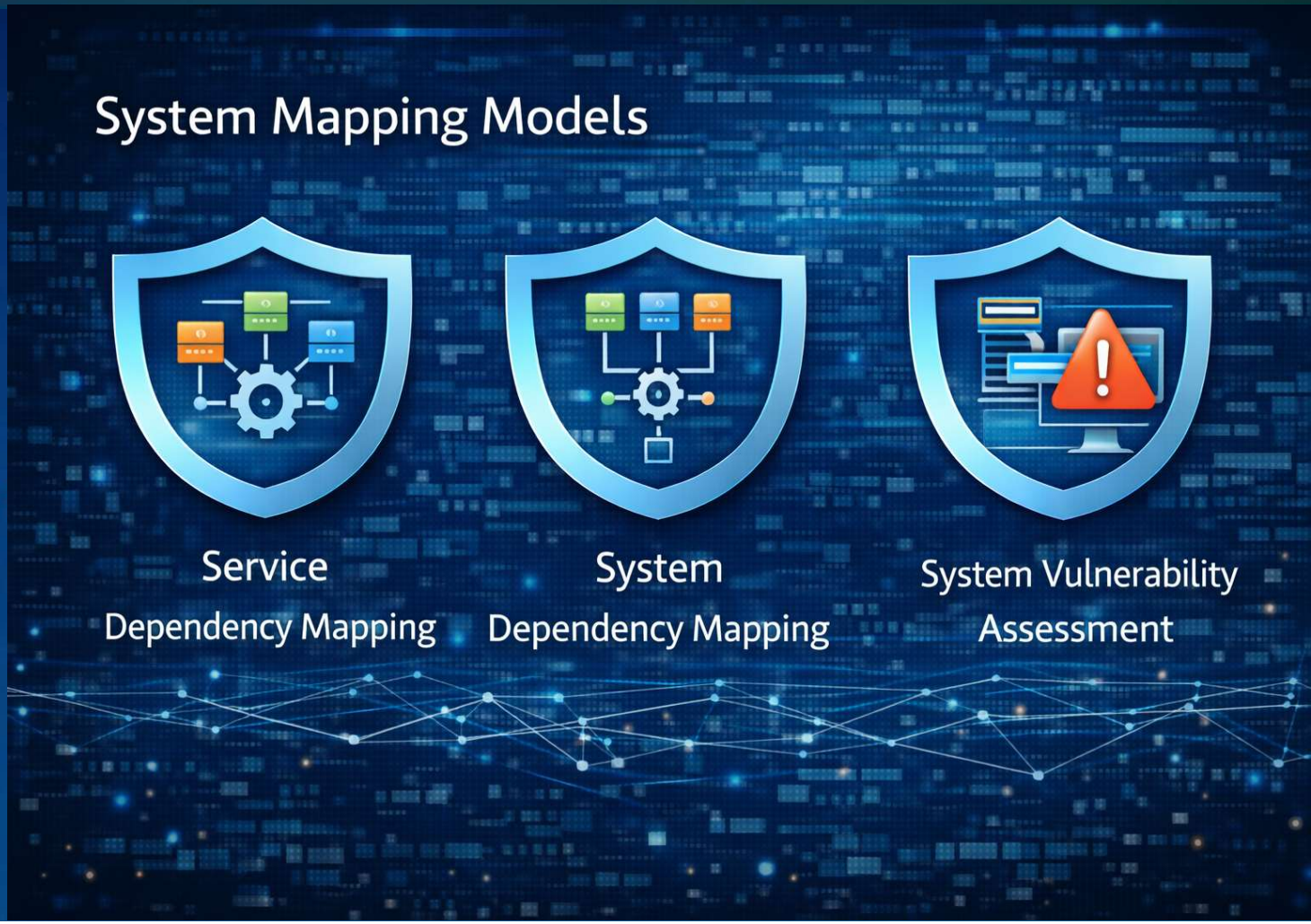
MITRE D3FEND Framework

- Model
- Harden
- Detect
- Isolate
- Deceive
- Evict
- Restore

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

MITRE D3FEND Framework

- Model
- Harden
- Detect
- Isolate
- Deceive
- Evict
- Restore



NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

MITRE D3FEND Framework

- Model
- Harden
- Detect
- Isolate
- Deceive
- Evict
- Restore

Model

Asset Inventory	Network Mapping	Operational Activity Mapping	System Mapping
Asset Vulnerability Enumeration	Logical Link Mapping	Access Modeling	Data Exchange Mapping
Container Image Analysis	Active Logical Link Mapping	Operational Dependency Mapping	Service Dependency Mapping
Configuration Inventory	Passive Logical Link Mapping	Operational Risk Assessment	System Dependency Mapping
Data Inventory	Network Traffic Policy Mapping	Organization Mapping	System Vulnerability Assessment
Hardware Component Inventory	Network Vulnerability Assessment		
Network Node Inventory	Physical Link Mapping		
Software Inventory	Active Physical Link Mapping		
	Direct Physical Link Mapping		

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

Defensive Tactics

- Model
- **Harden**
- Detect
- Isolate
- Deceive
- Evict
- Restore

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

Defensive Tactics

- Model
- **Harden**
- Detect
- Isolate
- Deceive
- Evict
- Restore

Harden

Agent Authentication	Application Hardening	Credential Hardening	Message Hardening	Platform Hardening	Source Code Hardening
Biometric Authentication	Application Configuration Hardening	Certificate Pinning	Message Authentication	Bootloader Authentication	Credential Scrubbing
Certificate-based Authentication	Dead Code Elimination	Credential Rotation	Message Encryption	Disk Encryption	Domain Logic Validation
Multi-factor Authentication	Exception Handler Pointer Validation	Certificate Rotation	Transfer Agent Authentication	Driver Load Integrity Checking	Operational Logic Validation
Password Authentication	Pointer Authentication	Password Rotation		File Encryption	Integer Range Validation
Token-based Authentication	Process Segment Execution Prevention	One-time Password		Hardware-based Write Protection	Pointer Validation
	Segment Address Offset Randomization	Strong Password Policy		Physical Enclosure Hardening	Memory Block Start Validation
	Stack Frame Canary Validation	Change Default Password		RF Shielding	Null Pointer Checking
		Token Binding		Software Update	Reference Nullification
				System Configuration Permissions	Trusted Library
				TPM Boot Integrity	Variable Initialization
					Variable Type Validation

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

MITRE D3FEND Framework

- Model
- Harden
- Detect
- Isolate
- Deceive
- Evict
- Restore

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

MITRE D3FEND Framework

- Model
- Harden
- Detect
- Isolate
- Deceive
- Evict
- Restore

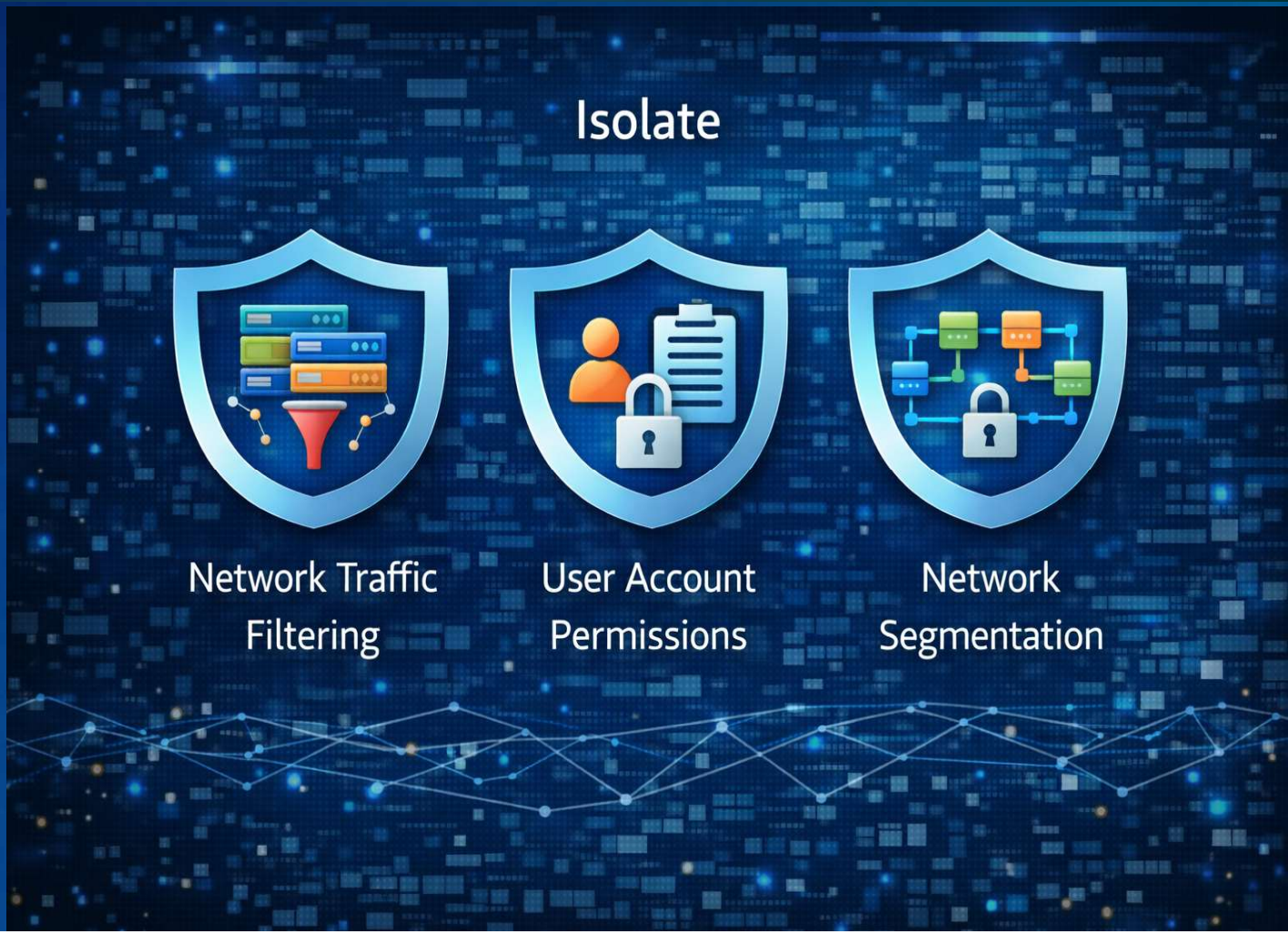
Detect

File Analysis	Identifier Analysis	Message Analysis	Network Traffic Analysis	Physical Access Monitoring	Platform Monitoring	Process Analysis	User Behavior Analysis
Dynamic Analysis	Homoglyph Detection	Sender MTA Reputation Analysis	Administrative Network Activity Analysis	Electronic Lock Monitoring	Application Performance Monitoring	Database Query String Analysis	Authentication Event Thresholding
Emulated File Analysis	Identifier Activity Analysis	Sender Reputation Analysis	Application Protocol Command Analysis	Motion Sensor Monitoring	Application Exception Monitoring	File Access Pattern Analysis	Authorization Event Thresholding
File Content Analysis	Identifier Reputation Analysis		Remote Firmware Update Monitoring	Proximity Sensor Monitoring	File Integrity Monitoring	Indirect Branch Call Analysis	Credential Compromise Scope Analysis
File Content Rules	Domain Name Reputation Analysis		Byte Sequence Emulation	Video Surveillance	Firmware Behavior Analysis	Process Code Segment Verification	Domain Account Monitoring
File Hashing	File Hash Reputation Analysis		Certificate Analysis		Firmware Embedded Monitoring Code	Process Self-Modification Detection	Job Function Access Pattern Analysis
	IP Reputation Analysis		Active Certificate Analysis		Firmware Verification	Process Spawn Analysis	Local Account Monitoring
	URL Reputation Analysis		Passive Certificate Analysis		Peripheral Firmware Verification	Process Lineage Analysis	Resource Access Pattern Analysis
	URL Analysis		Client-server Payload Profiling		System Firmware Verification	Script Execution Analysis	Session Duration Analysis
			Connection Attempt Analysis		Operating Mode Monitoring	Shadow Stack Comparisons	User Data Transfer Analysis
			DNS Traffic Analysis		Operating System Monitoring	System Call Analysis	User Geolocation Logon Pattern Analysis
			File Carving		Endpoint Health Beacon	File Creation Analysis	Web Session Activity Analysis
			Inbound Session Volume Analysis		Input Device Analysis		

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

MITRE D3FEND Framework

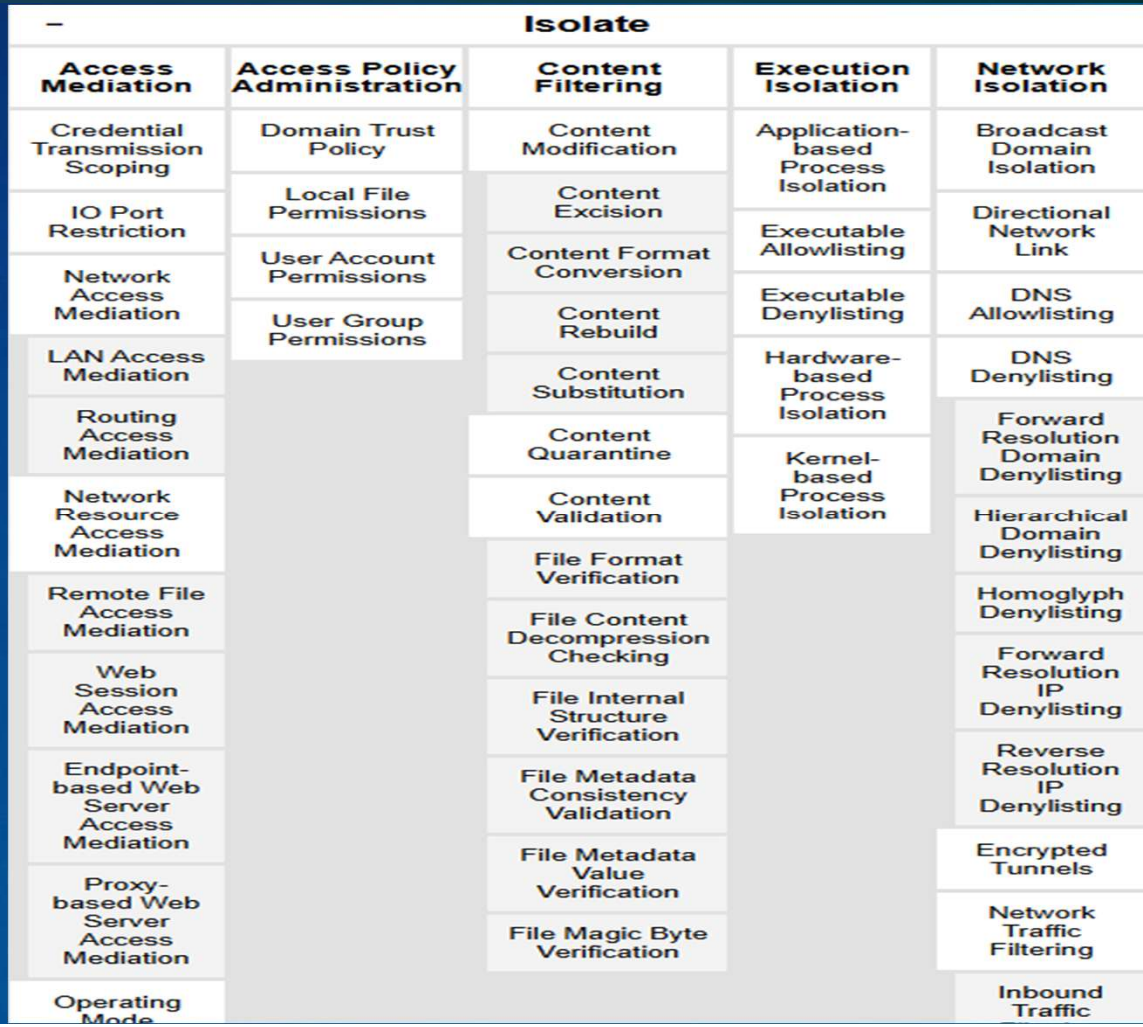
- Model
- Harden
- Detect
- Isolate
- Deceive
- Evict
- Restore



NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

MITRE D3FEND Framework

- Model
- Harden
- Detect
- Isolate
- Deceive
- Evict
- Restore



NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

MITRE D3FEND Framework

- Model
- Harden
- Detect
- Isolate
- Deceive
- Evict
- Restore

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

MITRE D3FEND Framework

- Model
- Harden
- Detect
- Isolate
- Deceive
- Evict
- Restore

– Deceive	
Decoy Environment	**Decoy Object**
Connected Honeynet	Decoy File
Integrated Honeynet	Decoy Network Resource
Standalone Honeynet	Decoy Persona
	Decoy Public Release
	Decoy Session Token
	Decoy User Credential

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

MITRE D3FEND Framework

- Model
- Harden
- Detect
- Isolate
- Deceive
- Evict
- Restore

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

MITRE D3FEND Framework

- Model
- Harden
- Detect
- Isolate
- Deceive
- Evict
- Restore

–	Evict	
Credential Eviction	**Object Eviction**	**Process Eviction**
Account Locking	Disk Formatting	Host Shutdown
Authentication Cache Invalidation	Disk Erasure	Host Reboot
Credential Revocation	Disk Partitioning	Process Suspension
	DNS Cache Eviction	Process Termination
	Domain Registration Takedown	Session Termination
	File Eviction	
	Email Removal	
	Registry Key Deletion	

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

MITRE D3FEND Framework

- Model
- Harden
- Detect
- Isolate
- Deceive
- Evict
- Restore

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

MITRE D3FEND Framework

- Model
- Harden
- Detect
- Isolate
- Deceive
- Evict
- Restore

– Restore

Restore Access	Restore Object
Reissue Credential	Restore Configuration
Restore Network Access	Restore Database
Restore User Account Access	Restore Disk Image
Unlock Account	Restore File
	Restore Email
	Restore Software

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

MITRE D3FEND Framework

MITRE D3FEND Defensive Techniques

Model	Defensive Techniques	D3FEND
Asset Inventory	Vulnerability Assessment	Harden
Operational Activity Mapping	System Mapping	Detect
Network Mapping	Dependency Mapping	Isolate
Organization Mapping	System Mapping	Deceive
Configuration Inventory	Process Knowledge	Evict
Data Inventory	Dependency Mapping	Restore

การเชื่อมโยง MITRE D3FEND กับ MITRE ATT&CK

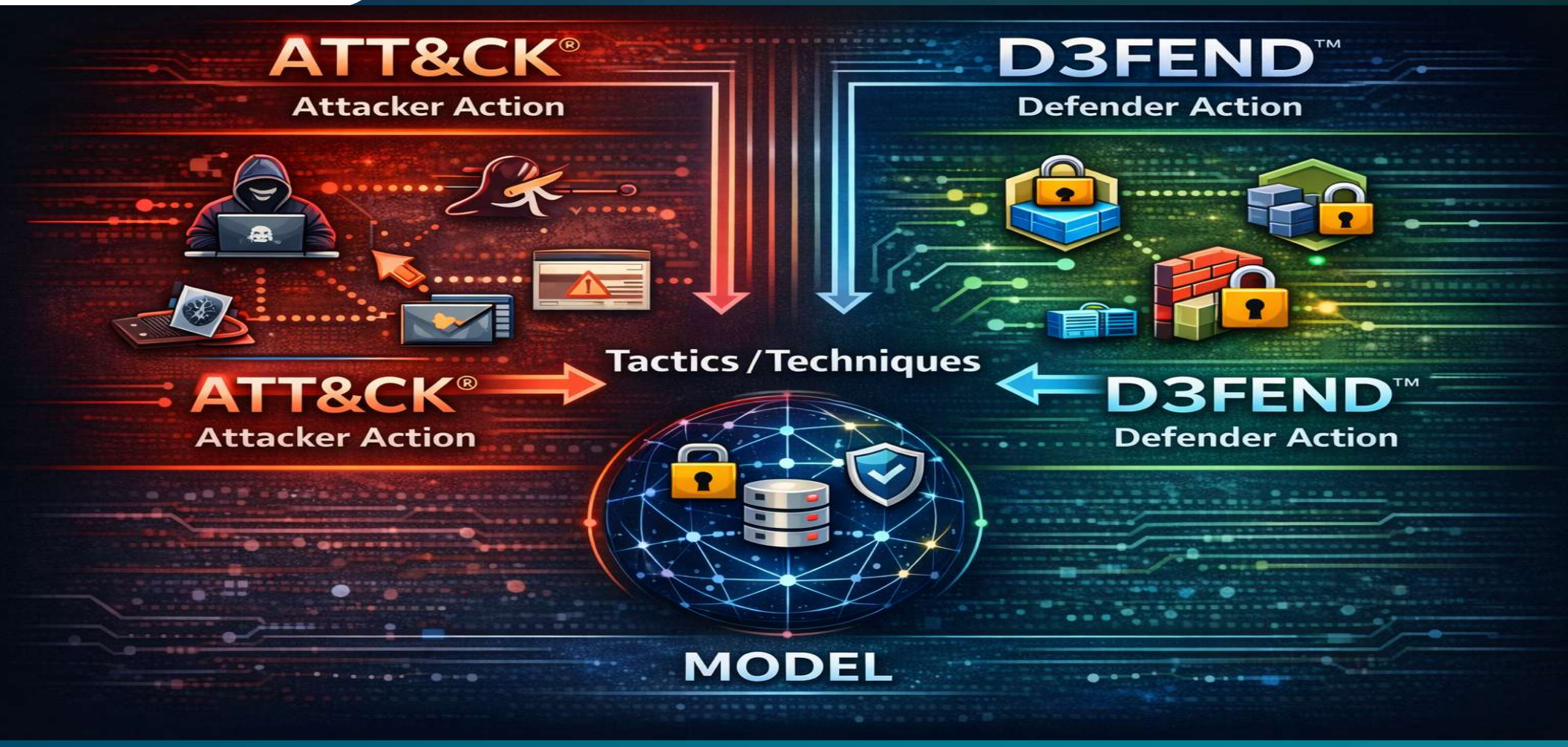
NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

D3FEND vs Framework อื่น

Framework	บทบาท
ATT&CK	Attack
NIST / ISO	Governance
D3FEND	Defense Mechanism

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

ATT&CK ←→ D3FEND Mapping



NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

ATT&CK ←→ D3FEND Mapping

ATT&CK ⟷ D3FEND

ATT&CK	D3FEND
Credential Access	Harden
Discovery	Detect
Lateral Movement	Isolate
Persistence	Evict
Impact	Restore

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

D3FEND ←→ NIST CSF Mapping

D3FEND	NIST CSF
Harden	Protect
Detect	Detect
Isolate	Respond
Deceive	Detect / Respond
Evict	Respond
Restore	Recover
Model Layer	Identify

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

D3FEND ←→ ISO 27001 Mapping

CYBERSECURITY FRAMEWORK MAPPING: D3FEND vs. ISO/IEC 27001:2022

MITRE D3FEND	ISO/IEC 27001:2022
Harden	A.5, A.8 (Access Control, Secure Config
Detect	A.8.15, A.8.16 (Logging & Monitoring)
Isolate	A.5.30 (ICT readiness for BC)
Evict	A.5.26 (Incident Response)
Restore	A.5.30, A.8.13 (Backup & Recovery)
Model Layer	Clause 4–6 (Context, Asset, Risk)

การนำ MITRE D3FEND ไปใช้

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

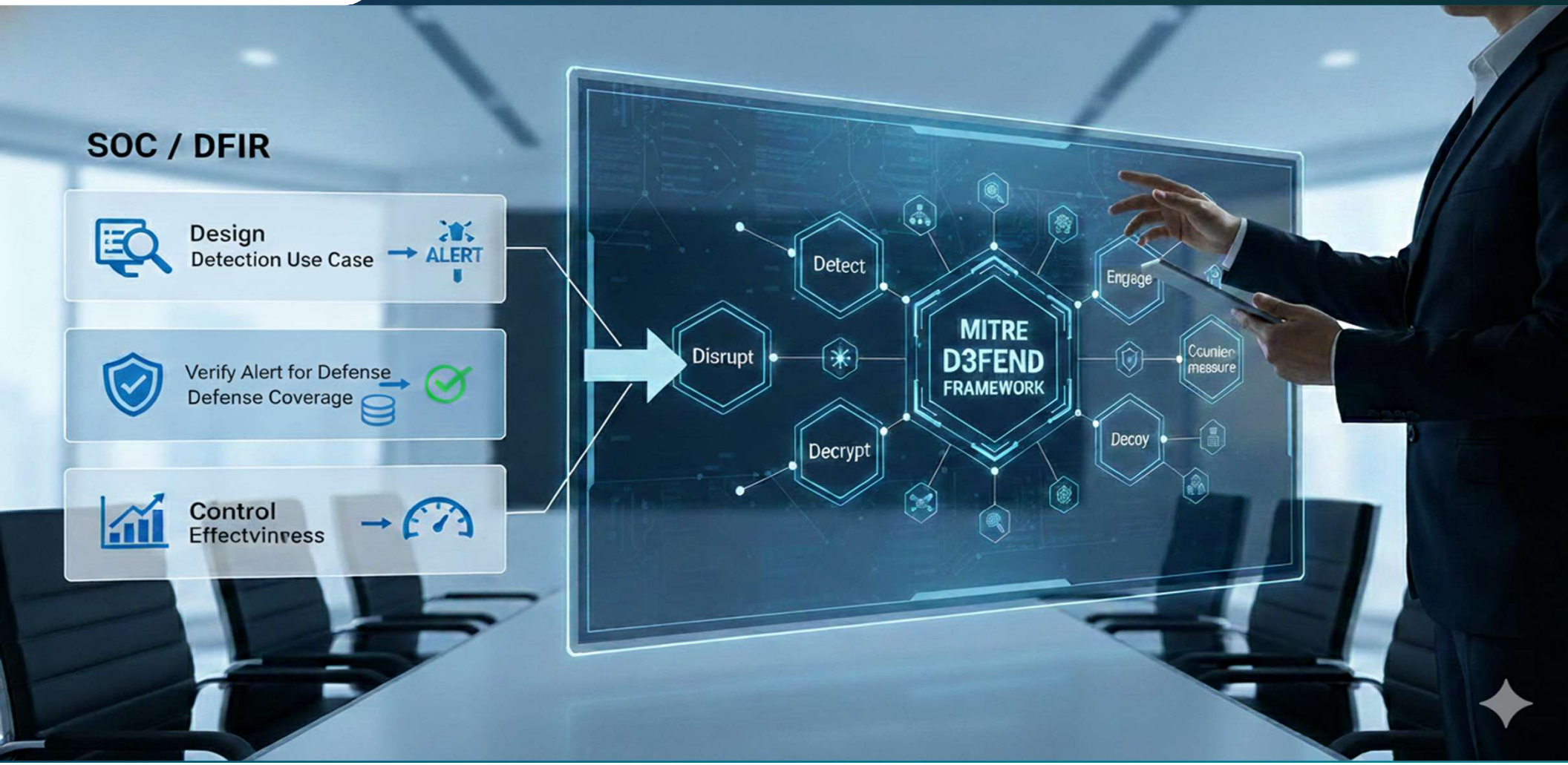
การนำ MITRE D3FEND ไปใช้

Cybersecurity Response Phases

Phase	Cyber	IT	D3FEND
Initial Access	Detect Phishing	Email Config	Detect
Lateral Movement	Analyze Logs	Network Mapping	Isolate
Impact	IR Action	Shutdown Service	Evict
Recovery	Verify Clean	Restore System	Restore

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

การนำ MITRE D3FEND ไปใช้



NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

การนำ MITRE D3FEND ไปใช้

Scenario Walkthrough

NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

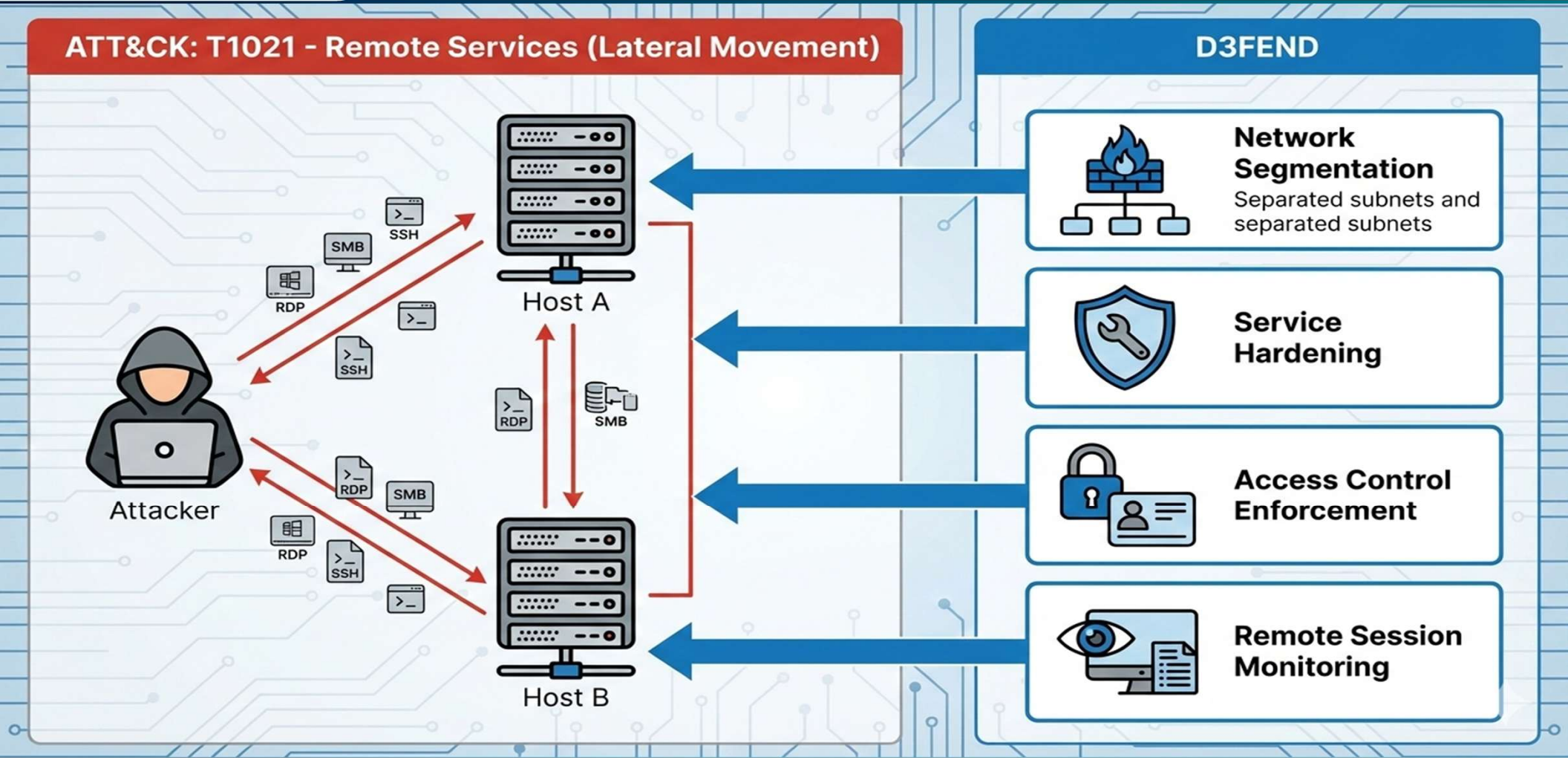
แนวคิด ATT&CK ←→ D3FEND Mapping

ATT&CK: T1110 - Brute Force

D3FEND

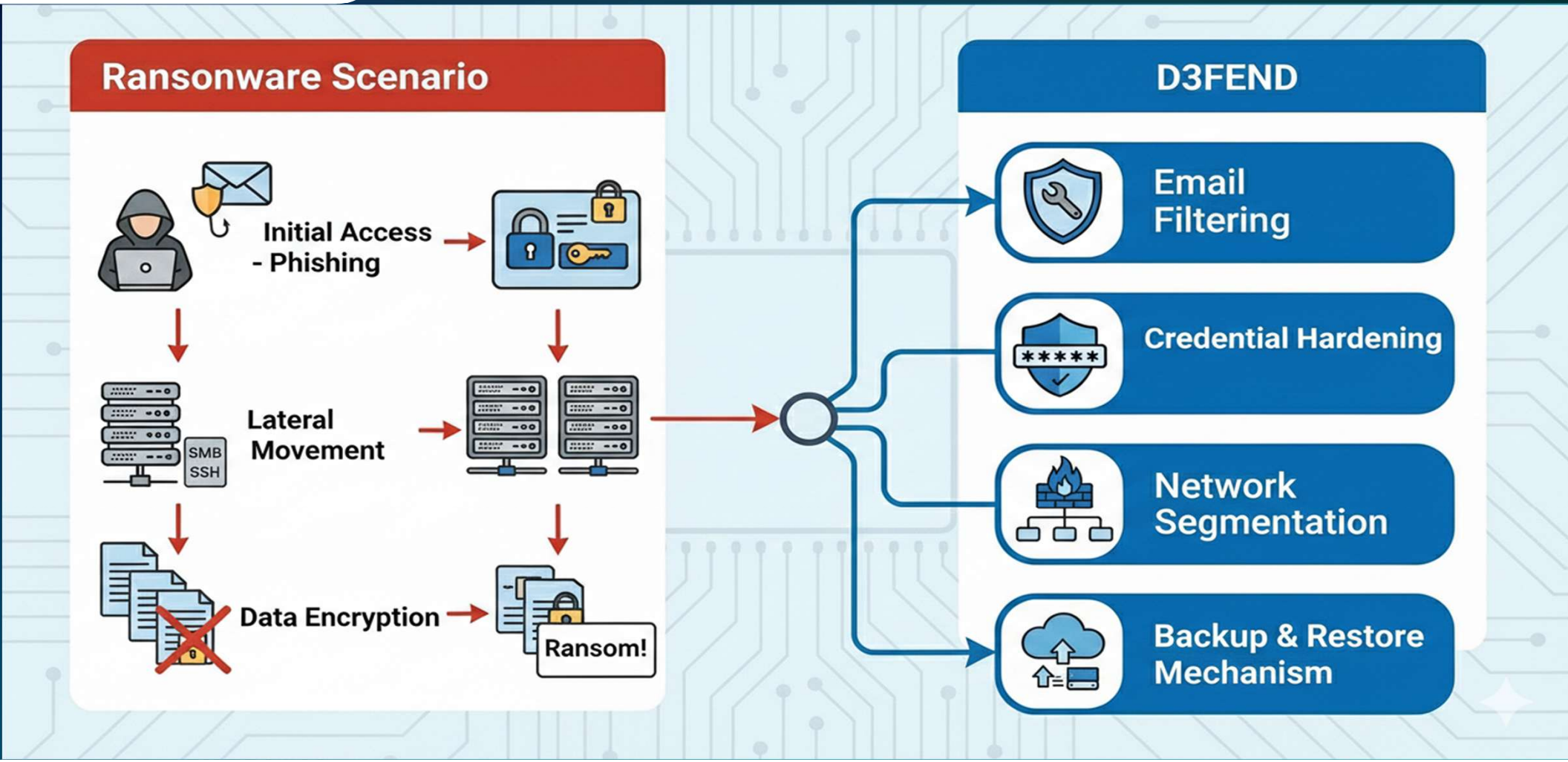
- Credential Hardening
- Authentication Rate Limiting
- Account Lockout Policy
- Authentication Logging

แนวคิด ATT&CK ←→ D3FEND Mapping



NCSA สกมช ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

แนวคิด ATT&CK ←→ D3FEND Mapping



Summary


Q&A


สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พร้อมให้คำปรึกษาและแจ้งเหตุภัยคุกคามทางไซเบอร์ออนไลน์ ให้กับหน่วยงานภาครัฐ และเอกชนแล้ววันนี้ กับ ThaiCERT NCSA และแจ้งเหตุภัยคุกคามทางไซเบอร์ Line Official
ช่องทางการติดต่อการแจ้งเหตุภัยคุกคามทางไซเบอร์
Facebook
ThaiCERT
LINE Official Account
ID Line: @thaicert
ThaiCERT
Email
thaicert@ncsa.or.th
เบอร์โทรศัพท์แจ้งเหตุภัยคุกคามทางไซเบอร์
0-2114-3531
ThaiCERT
Application
THCert HelpDesk
Download on the App Store
GET IT ON Google Play
Download Application THCertHelpDesk
www.ncsa.or.th
Facebook NCSA Thailand