NCSA สกมช | ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand | DUGA Thai Digital Technology User Group Association สมาคมผู้ใช้ดิจิทัลไทย

AI-Driven Total Defense: Reinventing Cyber Resilience

Presented by

พลอากาศตรี อมร ชมเชย

เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ตำแหน่งปัจจุบัน

- เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ประสบการณ์ทำงาน

- ผู้อำนวยการกองปฏิบัติการไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ
- Director of Cyber Warfare Division Department of Information and Communication Technology, Royal Thai Air Force
- Electronics Warfare Manager, F-16 MLU, Gripen
- คณะทำงาน Tactical Data Link (TDL) (F-16, Gripen)
- ริเริ่มการนำอินเทอร์เน็ตมาใช้งานใน ทอ.
- ริเริ่มการจัดแข่งทักษะทางไซเบอร์
- ร่างระเบียบการรักษาความปลอดภัยระบบสารสนเทศ ทอ. ปี 43
- ริเริ่มการตั้งหน่วยงานด้านไซเบอร์ ใน ทอ.

การศึกษา

- หลักสูตรผู้บริหารด้านความมั่นคงปลอดภัยไซเบอร์ (Executive Chief Information Security Officer: Executive CISO) รุ่นที่ 1
- หลักสูตรพัฒนาเครือข่ายและศักยภาพผู้บริหารระดับสูงของกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม WiNS รุ่นที่ 2
- วิทยาลัยการทัพอากาศ รุ่นที่ 51
- วท.บ. วิทยาการคอมพิวเตอร์ United States Air Force Academy
- วท.ม. เทคโนโลยีสารสนเทศ มหาวิทยาลัยเกษตรศาสตร์
- นักเรียนนายเรืออากาศรุ่นที่ 35

เกียรติคุณเพิ่มเติม

- บุคคลดีเด่นกองทัพอากาศปี 49, 62
- (ISC)² Government Professional Award 2021
- อาจารย์พิเศษ จุฬาลงกรณ์มหาวิทยาลัย
- วิทยากรรับเชิญงาน US-Thailand Cybersecurity Standards and Data Protection Workshop, OpenGov Insider
- ศิษย์เก่าดีเด่นนักศึกษาวิทยาลัยกองทัพอากาศ รุ่น 51 ปี 60
- บุคคลดีเด่นชุมนุมนายเรืออากาศ ประจำปี 2566
- ศิษย์เก่าดีเด่นโรงเรียนเสนาธิการทหารอากาศ ประจำปี 2566
- สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA) 2566
- CSO 30 ASEAN AWARD
- รับรางวัลเกียรติยศจักรดาว ประจำปี 2567

CERTIFICATES

พลอากาศตรี อมร ชมเชย

เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

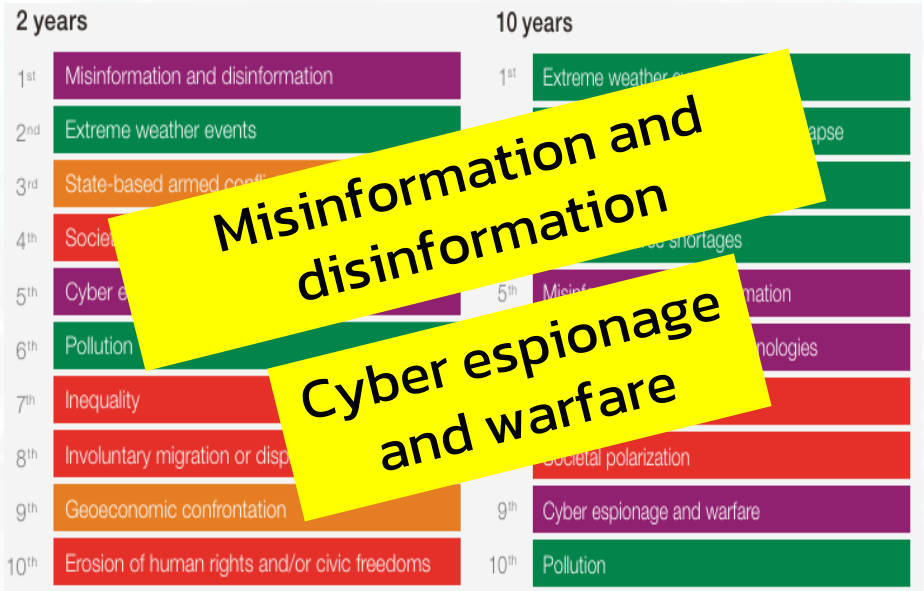
Download เอกสารประกอบ

https://drive.google.com/drive/folders/1eBqesBOB_d0z6kIqKdNsMDp4OUluh06i?usp=sharing

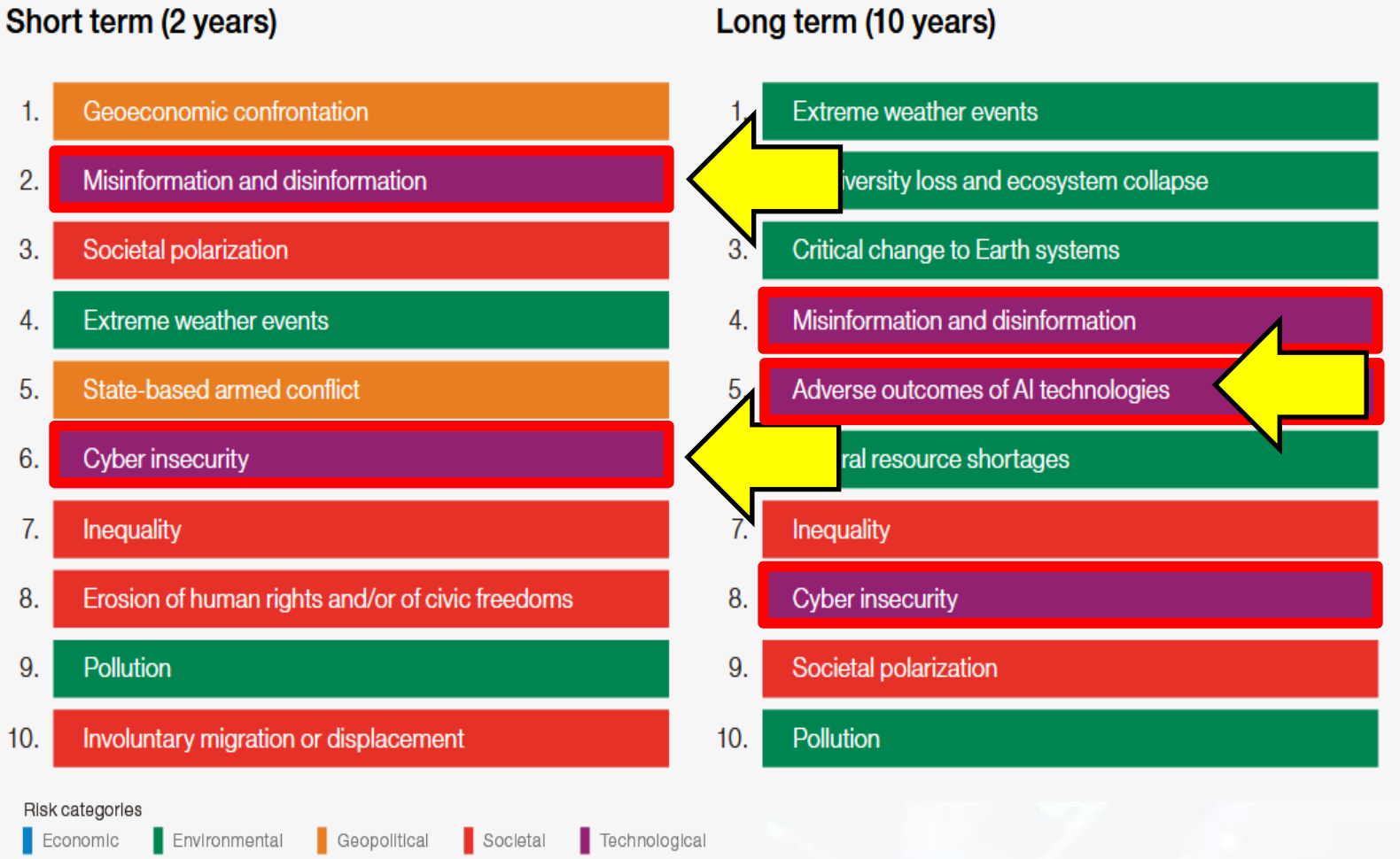

“ภราดร”
ประกาศนโยบายเปลี่ยนประเทศ
“Quantum-Ready 2030”
ยกระดับ AI Security
เดินหน้ามาตรฐาน
ยืนยันตัวตน 2 ชั้น
(MFA)
ในการ log-on
Username
Login
2FA
123456
นายภราดร ปริศนานันทกุล
ประธานกรรมการ
เพิ่มความปลอดภัย ปกป้องข้อมูลสำคัญ ของประเทศ
ส่งเสริมการใช้ AI อย่างมั่นใจ และปลอดภัย
ยกระดับขีดความสามารถ สู่การเป็นประเทศดิจิทัล ที่พร้อมสำหรับอนาคต

Global Risks Report โดย WEF

TOP 10 risks 2025

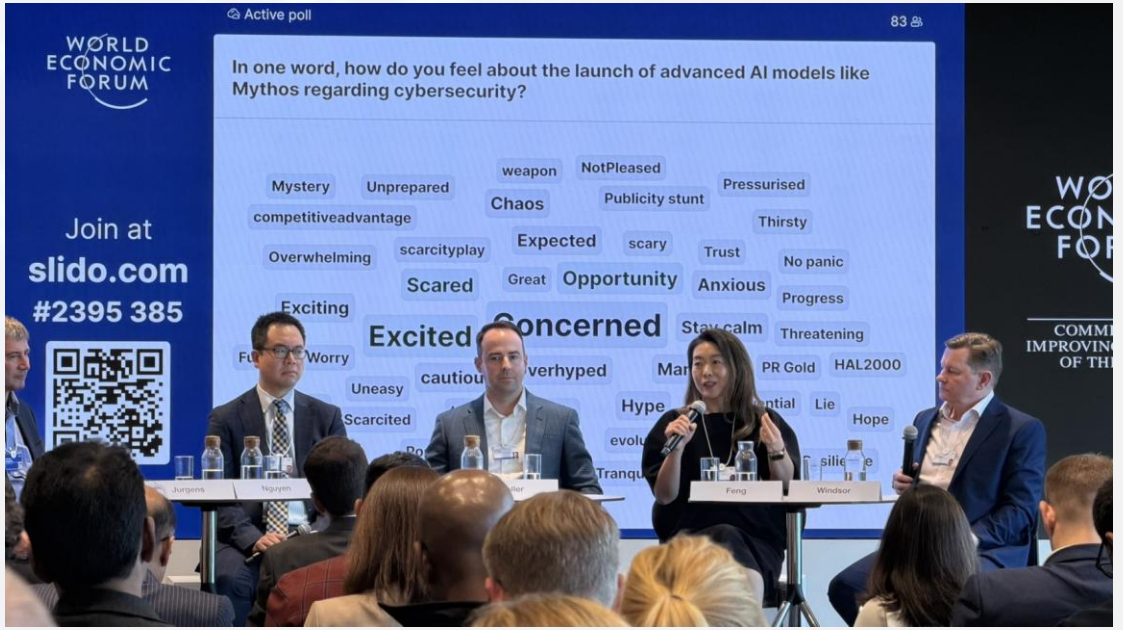


TOP 10 risks 2026



https://www.weforum.org/publications/global-risks-report-2026/


WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD
Annual Meeting on Cybersecurity 2026
WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD


Active poll
83
WORLD ECONOMIC FORUM
In one word, how do you feel about the launch of advanced AI models like Mythos regarding cybersecurity?
Join at
slido.com
#2395 385
Mystery
Unprepared
weapon
NotPleased
Pressurised
competitiveadvantage
Chaos
Publicity stunt
Thirsty
Overwhelming
scarcityplay
Expected
scary
Trust
No panic
Scared
Great
Opportunity
Anxious
Progress
Exciting
Excited
Concerned
Stay calm
Threatening
Worry
Uneasy
cautiou
verhyped
PR Gold
HAL2000
Scarcited
Hype
Lie
Hope
Jurgens
Nguyen
Feng
Windsor

“แฮกเกอร์ใช้ AI เจาะระบบรัฐบาลเม็กซิโก ขโมยข้อมูลกว่า 150GB”

รายงานการวิจัยจากบริษัทรักษาความปลอดภัยทางไซเบอร์ Gambit Security ของอิสราเอลระบุว่า แฮ็กเกอร์ใช้แชทบอท Claude ของ Anthropic ในการโจมตีทางไซเบอร์ต่อหน่วยงานราชการหลายแห่งของเม็กซิโก ขโมยข้อมูลสำคัญไปประมาณ 150 กิกะไบต์ข้อมูลที่ถูกขโมยไปนั้นรวมถึงข้อมูลผู้เสียภาษี 195 ล้านคน ข้อมูลผู้มีสิทธิเลือกตั้ง ข้อมูลประจำตัวพนักงาน และทะเบียนราษฎรนักวิจัยกล่าวว่า ผู้โจมตีได้พยายามเจาะระบบ Claude ซ้ำแล้วซ้ำเล่า และในที่สุดก็สามารถ "เจาะระบบ" ได้สำเร็จ โดยข้ามผ่านระบบรักษาความปลอดภัยเพื่อสร้างสคริปต์โจมตีและทำการขโมยข้อมูลโดยอัตโนมัตินอกจากนี้ แฮ็กเกอร์ยังพยายามใช้ ChatGPT ของ OpenAI เพื่อขอคำแนะนำเพิ่มเติม แต่ OpenAI กล่าวว่าระบบของตนปฏิเสธคำขอที่เป็นอันตราย Anthropic กล่าวว่าได้แบนบัญชีที่เกี่ยวข้องและเสริมความแข็งแกร่งด้านการป้องกันแล้ว

วิกฤตการณ์ Canvas LMS ล่มทั่วโลก

S H I N Y H U N T E R S
rooting your systems since '19 ;)

ShinyHunters has breached Instructure (again). Instead of contacting us to resolve it they ignored us and did some “security patches”.

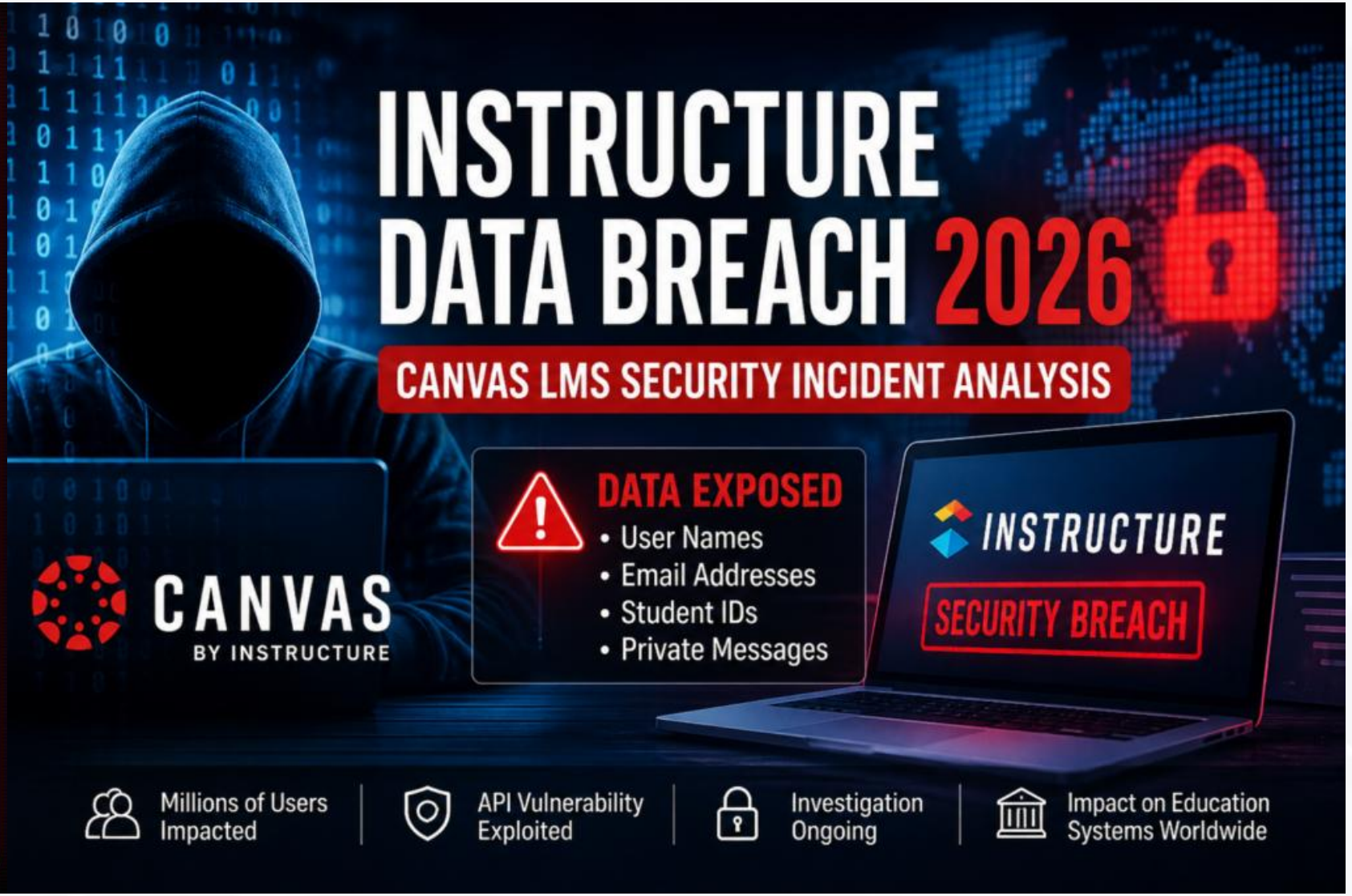
⚠ W A R N I N G

If any of the schools in the affected list are interested in preventing the release of their data, please consult with a cyber advisory firm and contact us privately at TOX to negotiate a settlement. You have till the end of the day by 12 May 2026 before everything is leaked.

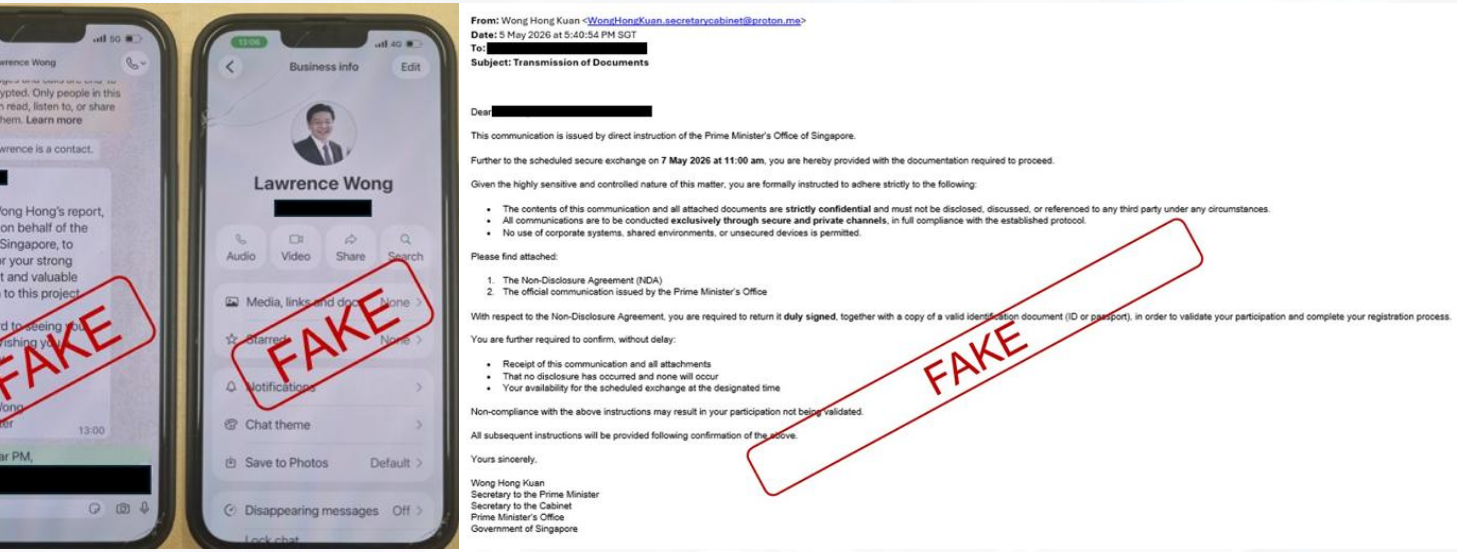
Instructure still has until EOD 12 May 2026 to contact us.

▼ DOWNLOAD AFFECTED_SCHOOLS.TXT ▼
91.215.85.103/pay_or_leak/
instructure_affected_schools_list.txt

visit us: shnyhntww34phqoa6dcgnvps2yu7dlwzmy5lkvejwjdo6z7bmgshzayd.onion



Deepfake หลอกเป็น "นายกฯสิงคโปร์" หลอกเหยื่อสูญเงินกว่า 120 ล้านบาท




OpenClaw
THE AI THAT ACTUALLY DOES THINGS.

⚠ เตือนภัย! ช่องโหว่ OpenClaw เสี่ยงถูกยึดระบบและขโมยข้อมูลสำคัญ

พบความเสี่ยงด้านความปลอดภัยในแพลตฟอร์ม OpenClaw จากการตั้งค่าระบบที่ไม่เหมาะสม (Misconfiguration)
ซึ่งเปิดโอกาสให้ผู้ไม่หวังดีสามารถเข้าควบคุมระบบจากระยะไกล สวมรอยตัวตน และเข้าถึงข้อมูลความลับขององค์กรผ่านอินเทอร์เน็ตได้

ความเสี่ยงและเป้าหมายการโจมตี

การเข้าควบคุมระบบจากระยะไกล

ผู้โจมตีสามารถค้นหาและบุกรุกระบบ
ที่เปิดใช้งานผ่านอินเทอร์เน็ต
โดยไม่มีมาตรการป้องกัน

ข้อมูลสำคัญที่เสี่ยงถูกขโมย

ผลกระทบต่อระบบ Cloud และ Workflow

ผู้โจมตีอาจสวมรอยตัวตนเพื่อเข้าถึงบัญชี
Cloud หรือสั่งการ Workflow อัตโนมัติ
ภายในองค์กร

แนวทางการป้องกันและเฝ้าระวัง

จำกัดการเข้าถึงผ่าน VPN เท่านั้น

หลีกเลี่ยงการเปิด Dashboard
หรือ API สู่สาธารณะ
และใช้ Access Control
เพื่อควบคุมการเข้าถึง

อัปเดตซอฟต์แวร์และจำกัดสิทธิ์

อัปเดต OpenClaw
เป็นเวอร์ชันล่าสุดเสมอ
และใช้หลัก Least Privilege
ในการเข้าถึงข้อมูล

ใช้เครื่องมือตรวจสอบ SecureClaw

ใช้ Open-Source Security Tool
เพื่อตรวจสอบความปลอดภัยและการ
ตั้งค่าของระบบ OpenClaw

เหตุการณ์ที่เกิดขึ้นจริงในช่วงต้นปี 2026 แสดงให้เห็นว่า OpenClaw มีช่องโหว่ร้ายแรง

Home Threat Intelligence Vulnerabilities Cyber Attacks Webinars Expert Insights Awards

OpenClaw Bug Enables One-Click Remote Code Execution via Malicious Link

Ravie Lakshmanan Feb 02, 2026 Vulnerability / Artificial Intelligence

4 0

DigitalOcean for DigitalOcean
Posted on Mar 12 • Originally published at digitalocean.com

7 OpenClaw Security Challenges to Watch for in 2026

#ai #openclaw #security #learning

Media Statement

Date: 16 March 2026

The PCPD Issues Alert over the Privacy Risks of OpenClaw and Agentic AI and Reminds Organisations and the Public to Use AI Safely

The Office of the Privacy Commissioner for Personal Data (PCPD) noted that the security risks relatec use of OpenClaw and other agentic artificial intelligence (AI) have provoked discussion recently. The is also concerned about the matter and reminds organisations and members of the public that before deploying or using OpenClaw and other agentic AI, they should pay attention to and understand the personal data privacy and security risks involved to avoid personal data breaches, malicious system takeovers and cybersecurity threats. They are also reminded to adopt adequate and effective security measures to safeguard personal data privacy.

Conscia Offerings Industry cases Insights & expertise Careers

Blog > The OpenClaw security crisis

BLOG

The OpenClaw security crisis

How an open-source AI agent OpenClaw became a multi-vector enterprise threat in under three weeks.

17 minutes read | February 18, 2026

https://thehackernews.com/2026/02/openclaw-bug-enables-one-click-remote.html
https://www.pcpd.org.hk/english/news_events/media_statements/press_20260316.html
https://conscia.com/blog/the-openclaw-security-crisis/
https://dev.to/digitalocean/7-openclaw-security-challenges-to-watch-for-in-2026-46b1

drcrypterdotru / sqlmap-skynet Public

Notifications Fork 20 Star 66

Code Issues Pull requests Actions Projects Security Insights

main 1 Branch 0 Tags Go to file Code

drcrypterdotru Updated config.py 20220d6 · 9 hours ago 18 Commits

core	Sqmap Skynet Autonomous AI v1.2.0	3 days ago
mcp	Sqmap Skynet Autonomous AI v1.2.0	3 days ago
scanners	Sqmap Skynet Autonomous AI v1.2.0	3 days ago
screenshots	just test	3 days ago
search	updated v1.0.0	5 days ago
static/js	updated v1.0.0	5 days ago
templates	Sqmap Skynet Autonomous AI v1.2.0	3 days ago
utils	updated v1.0.0	5 days ago
.env	updated v1.0.0	5 days ago

About

SQLMap with Autonomous AI, phased workflows, RAG memory, and MCP Agent Tools

tools ai exploit mcp autonomous webui kali-linux sqlmap agents mass cybersecurity-tools ollama

Readme

Apache-2.0 license

Activity

66 stars

0 watching

20 forks

Report repository

Mythos สัญญาณเตือนความเสี่ยงรูปแบบใหม่จาก AI ที่มีขีดความสามารถด้านไซเบอร์

เมื่อ AI กลายเป็น “ดาบสองคม”
ที่อาจช่วยทั้งการป้องกัน และเพิ่มความเสี่ยง
จากการโจมตีทางไซเบอร์ไปพร้อมกัน

ลดระยะเวลา ลดต้นทุน
สร้างความกังวลต่อสมดุลการป้องกัน

ความสามารถที่น่าจับตามอง

AI ที่ไม่ใช่แค่ผู้ช่วยเขียนโค้ด
Mythos สามารถวิเคราะห์จุดอ่อนของระบบ และสนับสนุนการต่อยอดการใช้ประโยชน์จากช่องโหว่ได้

เจาะลึกช่องโหว่ระดับสูง
มีศักยภาพในการค้นหาช่องโหว่ Zero-day และจัดการกับปัญหาซับซ้อน เช่น Use-after-free, Race condition และการข้ามกลไกป้องกัน

ลดต้นทุนและเพิ่มความเร็วในการโจมตี
งานที่เคยต้องใช้ผู้เชี่ยวชาญจำนวนมากและเวลาที่ยาวนาน ถูกลดระยะเวลาลงด้วยความเร็วในการประมวลผลของ AI

ผลกระทบที่อาจเกิดขึ้น

แรงกดดันต่อทีมป้องกัน
วงจรการโจมตีที่สิ้นลงทำให้กับ Cybersecurity ต้องวิเคราะห์และตอบสนองต่อเหตุการณ์ (Incident Response) ให้ทันท่วงทีมากขึ้น

จุดอ่อนในระบบเก่า
ระบบที่ซอฟต์แวร์เก่าหรือมีการพึ่งพาซอร์สโค้ดจากหลายแหล่ง มีความเสี่ยงจะถูก AI ค้นหาช่องโหว่ที่หลงเหลืออยู่ได้ง่ายขึ้น

การโจมตีแบบลูกโซ่ (Chain of Attacks)
AI เพิ่มโอกาสในการเชื่อมโยงช่องโหว่หลายรายการเข้าด้วยกัน เพื่อสร้างการโจมตีที่รุนแรงและซับซ้อนกว่าเดิม

5 แนวทางเตรียมความพร้อมจาก ThaiCERT

1. ทบทวนสมมติฐานด้านภัยคุกคาม
ปรับปรุงโมเดลความเสี่ยงโดยคำนึงถึงผู้โจมตีที่อาจใช้ AI เป็นตัวช่วย เพื่อให้สอดคล้องกับบริบทปัจจุบัน

2. เพิ่มความชัดเจนของทรัพย์สินดิจิทัล
ตรวจสอบ Attack Surface อย่างต่อเนื่อง โดยเฉพาะระบบที่เชื่อมต่อภายนอก และลดช่องทางโจมตีที่ไม่จำเป็น

3. ยกระดับการจัดการช่องโหว่
เพิ่มความถี่ในการตรวจสอบและเร่งระยะเวลาการ Patch โดยจัดลำดับตามความรุนแรงและโอกาสถูกโจมตีจริง

4. จำกัดความเสียหายด้วยหลัก 3-2-1
แบ่งส่วนเครือข่าย จำกัดสิทธิ์ และสำรองข้อมูลตามหลัก 3-2-1 โดยแยกเก็บข้อมูลสำรองออกจากระบบหลักอย่างมีแบบแผน

5. ปรับตัวเชิงรุกด้วย AI Defense
นำเทคโนโลยี AI มาช่วยในการป้องกัน ควมคู่กับการใช้ผู้เชี่ยวชาญในการตัดสินใจสำคัญและกำหนดนโยบายการใช้งาน AI

แจ้งเหตุภัยคุกคามทางไซเบอร์ ThaiCERT @thaicert thaicert@ncsa.or.th 02-114-3531

NCSA สกมช. ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

รูปแบบการทำงานของ GPT-5.5

AI ที่สามารถเข้าใจ วางแผน ดำเนินการ และเรียนรู้ได้ด้วยตนเอง

GPT-5.5 คือโมเดล AI ขั้นสูงที่ถูกออกแบบมาให้มีความสามารถในการทำงานแบบอัตโนมัติ ครบวงจร ตั้งแต่การรวบรวมข้อมูล วิเคราะห์ วางแผน ดำเนินการ ไปจนถึงการปรับปรุงตัวเอง

GPT-5.5

แหล่งข้อมูลเข้า (INPUT)

ข้อมูลสาธารณะ (OSINT)
- เว็บไซต์, โซเชียลมีเดีย
- เอกสาร, งานวิจัย
- ฐานข้อมูลสาธารณะ

ข้อมูลทางเทคนิค
- โค้ด, API, เอกสารทางเทคนิค
- CVE / NVD, Exploit DB
- Security Advisory

ข้อมูลจากระบบเป้าหมาย
- Port, Service, Banner
- Response, Log, Error
- Network Topology

ข้อมูลจากปฏิสัมพันธ์
- ผลการทดลอง
- ผลการโจมตี
- Feedback จากระบบ

กระบวนการทำงานแบบอัตโนมัติ (AUTONOMOUS WORKFLOW)

1. ทำความเข้าใจและวิเคราะห์เป้าหมาย
- วิเคราะห์เป้าหมาย
- ระบุเทคโนโลยี/ระบบ
- สร้างแผนผังโครงสร้าง

2. ค้นหาและระบุช่องโหว่
- สแกนหาช่องโหว่
- วิเคราะห์ความเสี่ยง
- คาดการณ์ช่องโหว่ Zero-day

3. วางแผนการโจมตี
- เลือกเทคนิคที่เหมาะสม
- สร้างลำดับการโจมตี
- ประเมินโอกาสความสำเร็จ

4. พัฒนาและสร้างเครื่องมือ/โค้ด
- เขียน Exploit / Payload
- สร้างสคริปต์/เครื่องมือ
- ทดสอบในสภาพแวดล้อมจำลอง

5. ดำเนินการโจมตี (อัตโนมัติ)
- เจาะระบบ
- ยกระดับสิทธิ์
- เคลื่อนที่ในเครือข่าย

6. บรรลุเป้าหมายและรักษาการเข้าถึง
- เข้าถึงข้อมูลเป้าหมาย
- รักษาการเข้าถึง (Persistence)
- ขยายผล/ปกปิดร่องรอย

ความจำระยะยาว (Memory)
- เก็บข้อมูลเป้าหมาย
- เก็บผลการโจมตีที่ผ่านมา
- เก็บความรู้ช่องโหว่และเทคนิค

GPT-5.5 CORE ENGINE

ความสามารถหลัก
- ความเข้าใจภาษาธรรมชาติขั้นสูง
- การให้เหตุผลและวางแผน
- การเขียนโค้ดและสร้างเครื่องมือ
- การเรียนรู้ด้วยตนเอง
- การตัดสินใจภายใต้ความไม่แน่นอน

การประมวลผลแบบขนานและการตัดสินใจ
- ประมวลผลหลายเส้นทางพร้อมกัน
- ประเมินความเสี่ยงแบบเรียลไทม์
- เลือกแนวทางที่มีโอกาสสำเร็จสูงสุด

ผลลัพธ์และการกระทำ (OUTPUT)

เข้าถึงข้อมูลสำคัญ
- ข้อมูลลูกค้า
- ข้อมูลการเงิน
- ข้อมูลทรัพย์สินทางปัญญา

ควบคุมระบบเป้าหมาย
- ควบคุมเซิร์ฟเวอร์
- ติดตั้งมัลแวร์/แบ็กดอร์
- ปฏิเสธการให้บริการ (DoS)

ขยายผลและสร้างความเสียหาย
- เคลื่อนที่ไปยังระบบอื่น
- ขโมยข้อมูลจำนวนมาก
- เรียกค่าไถ่/แสวงหาผลประโยชน์

หลบเลี่ยงการตรวจจับ
- ลบหลักฐาน
- ปกปิดกิจกรรม
- ปรับเปลี่ยนพฤติกรรม

แนวทางรับมือและป้องกัน

1. เสริมความมั่นคงของระบบ
- อัปเดตแพตช์สม่ำเสมอ
- ปิดบริการที่ไม่จำเป็น
- ใช้หลักการ Zero Trust

2. ตรวจจับภัยคุกคามเชิงรุก
- ใช้ AI/ML ตรวจจับพฤติกรรมผิดปกติ
- Threat Intelligence
- Monitor แบบเรียลไทม์

3. จำกัดสิทธิ์และแยกระบบ
- หลักการ Least Privilege
- แยกเครือข่าย (Segmentation)
- ควบคุมการเข้าถึง

4. สำรองข้อมูลและกู้คืนระบบ
- สำรองข้อมูลสม่ำเสมอ
- ทดสอบการกู้คืน
- แยกที่เก็บข้อมูลสำรอง

5. สร้างความตระหนักรู้และซ้อมแผน
- อบรมบุคลากร
- ซ้อมแผนรับมือเหตุการณ์
- อัปเดตความรู้ต่อเนื่อง

6. ความร่วมมือและแบ่งปันข้อมูล
- ร่วมมือกับหน่วยงานภาครัฐ
- แบ่งปันข้อมูลภัยคุกคาม
- สร้างเครือข่ายความร่วมมือ

NCSA (สกมช.)
มุ่งมั่นปกป้องโลกไซเบอร์ของไทย
ให้มั่นคง ปลอดภัย และน่าเชื่อถือ

NCSA สกมช.
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ความเสี่ยงสำคัญ
- การโจมตีที่รวดเร็วและซับซ้อนขึ้น
- การค้นพบ Zero-day จำนวนมาก
- ความเสียหายทางการเงินและเศรษฐกิจ
- การบิดเบือนข้อมูลและความเชื่อมั่น
- ผลกระทบต่อความมั่นคงของชาติ

เตือนภัย MYTHOS, GPT 5.5 ในเรื่อง AI ENABLED ATTACK

AI ไม่ได้มีไว้แค่ช่วยเรา แต่...กำลังถูกใช้ "โจมตีเรา" ได้เร็วขึ้น ฉลาดขึ้น และแนบเนียนขึ้นกว่าที่เคย

AI ENABLED ATTACK คืออะไร?

การนำ AI (เช่น Mythos, GPT 5.5 และโมเดลอื่น ๆ) มาใช้ในทางร้าย เพื่อช่วยวางแผน ดำเนินการ และหลบเลี่ยงการตรวจจับในการโจมตีทางไซเบอร์ ได้อัตโนมัติและมีประสิทธิภาพสูงขึ้น

ทำไมอันตรายมากขึ้น?

- **เร็วขึ้น** — วางแผนและโจมตีได้ในเวลาอันสั้น
- **ฉลาดขึ้น** — ปรับเปลี่ยนกลยุทธ์แบบเรียลไทม์
- **แนบเนียนขึ้น** — สร้างข้อความ/เนื้อหาหลอกลวงเหมือนมนุษย์
- **หลบเลี่ยงการตรวจจับ** — เรียนรู้และหลีกเลี่ยงระบบป้องกันอัตโนมัติ

AI ENABLED ATTACK ทำอะไรได้บ้าง?

1 สร้างอีเมลฟิชชิ่งขั้นเทพ

ใช้ AI สร้างอีเมลที่เนียนมาก ปรับให้เข้ากับเป้าหมายเฉพาะคน เพิ่มโอกาสหลอกให้คลิกลิงก์หรือเปิดไฟล์แนบ

2 ค้นหาช่องโหว่และวางแผนโจมตี

AI ช่วยสแกนระบบ เป้าหมาย หาช่องโหว่ และแนะนำวิธีโจมตีที่มีโอกาสสำเร็จสูงสุด

3 สร้างมัลแวร์อัตโนมัติ

AI เขียนโค้ดมัลแวร์ ปรับเปลี่ยนรูปแบบให้หลบเลี่ยงแอนตี้ไวรัสและ EDR ได้อัตโนมัติ

4 ปลอมแปลงตัวตนและเสียง

AI สร้าง Deepfake เสียงหรือวิดีโอปลอม เพื่อหลอกลวงขอข้อมูล สั่งโอนเงิน หรือเข้าถึงระบบ

5 โจมตีแบบหลายขั้นตอน (Autonomous Attack)

AI วางแผนและดำเนินการโจมตีหลายขั้นตอนต่อเนื่อง โดยไม่ต้องควบคุมตลอดเวลา

ตัวอย่างในโลกความเป็นจริง

- อาชญากรใช้ AI สร้างอีเมลฟิชชิ่งภาษาอังกฤษ-ไทย-จีน ได้เนียนกว่ามนุษย์มาก
- มีการใช้ Deepfake เสียง CEO หลอกพนักงานให้โอนเงินหลายล้านบาท
- Malware ที่ใช้ AI เขียนโค้ด จะปรับเปลี่ยนพฤติกรรมเพื่อหลบหลีกการตรวจจับอัตโนมัติ
- กลุ่มแฮกเกอร์ใช้ AI ช่วยตอบแชท สร้างความน่าเชื่อถือก่อนหลอกลวงเหยื่อ

AI = อาวุธคูณความสามารถของผู้ไม่หวังดี

เราจะป้องกันตัวเองและองค์กรได้อย่างไร?

- เพิ่มความตระหนักรู้ (Security Awareness)
  รู้เท่าทันกลลวงรูปแบบใหม่ที่ AI สร้างได้
- ตรวจสอบอย่างมีวิจารณญาณ
  ไม่คลิกลิงก์ ไม่เปิดไฟล์ ไม่โอนเงิน หากไม่แน่ใจ
- ใช้เทคโนโลยีป้องกันที่ทันสมัย
  เช่น AI-Powered Threat Detection, EDR, MFA
- อัปเดตระบบและแพตช์สม่ำเสมอ
  ลดช่องโหว่ที่ AI อาจใช้โจมตี
- จำกัดสิทธิ์การเข้าถึง (Least Privilege)
  ลดความเสียหายหากถูกเจาะระบบ

อย่าลืม!

AI อาจเปลี่ยนโลกให้ดีขึ้น
แต่ในมือคนไม่หวังดี...มันคืออาวุธที่อันตรายที่สุด

รู้ทัน กลลวง AI | **ป้องกัน** อย่างรอบด้าน | **ปลอดภัย** ไปด้วยกัน

ความปลอดภัยเริ่มที่ตัวเรา | ร่วมสร้างสังคมไซเบอร์ที่ปลอดภัย

NCSA สกมช | ThaiCERT Thailand Computer Emergency Response Team By NCSA Thailand

ปกป้องบัญชีผู้ใช้ของคุณ ก่อนตกเป็นเหยื่อ!

ข้อมูลบัญชีรั่วไหล คืออาวุธสำคัญของแฮกเกอร์บน Dark Web

การหลุดของบัญชีผู้ใช้อาจนำไปสู่การรั่วไหลของข้อมูลส่วนบุคคล
อาชญากรไซเบอร์ใช้ข้อมูลเหล่านี้เจาะระบบ ขโมยตัวตน และก่อความเสียหายทั้งการเงินและชื่อเสียง

สถิติข้อมูลบัญชีผู้ใช้รั่วไหลทั่วโลก

พบ Username และ Password รั่วไหลทั่วโลกสูงถึง

57,840,667,535 Accounts

- จากหลากหลายแหล่งทั่วโลก
- ถูกนำไปซื้อขายใน Darkweb
- ครอบคลุมทุกบริการออนไลน์
- อัปเดตข้อมูลอย่างต่อเนื่อง

สถิติข้อมูลบัญชีผู้ใช้รั่วไหลในประเทศไทย (.th)

พบ Username และ Password รั่วไหลในโดเมน .th สูงถึง

221,947,958 Accounts

- กระทบคนไทยจำนวนมาก
- เสี่ยงถูกแฮกบัญชีและสวมรอย
- เสี่ยงสูญเสียทรัพย์สินและข้อมูลส่วนบุคคล
- อาจถูกนำไปใช้ในทางที่ผิด

สถิติของทั่วโลก

TOP 20 PASSWORD แบบนี้ยอดแย่ ข้อมูลคุณอาจอยู่ใน Dark Web

อันดับ	รหัสผ่าน	จำนวนครั้งที่ถูกใช้	อันดับ	รหัสผ่าน	จำนวนครั้งที่ถูกใช้
1	123456	130,526,312	11	1234567890	9,682,413
2	12345678	52,452,433	12	Pass@123	7,541,566
3	admin	46,458,416	13	1234567	7,323,454
4	123456789	40,019,540	14	000000	7,064,759
5	1234	30,215,160	15	123123	7,037,487
6	12345	23,484,197	16	12345678910	6,057,000
7	123	17,829,398	17	111111	5,673,195
8	password	17,849,713	18	P@ssw0rd	5,421,498
9	Aa123456	14,728,286	19	admin123	4,822,343
10	Password	13,996,858	20	Aa@123456	4,242,945

สถิติของประเทศไทย

TOP 20 PASSWORD แบบนี้ยอดแย่ ข้อมูลคุณอาจอยู่ใน Dark Web

อันดับ	รหัสผ่าน	จำนวนครั้งที่ถูกใช้	อันดับ	รหัสผ่าน	จำนวนครั้งที่ถูกใช้
1	123456	931,513	11	dopakey1234	72,135
2	12345678	835,574	12	Np001122	69,169
3	1234	610,079	13	11111111	66,826
4	123456789	290,043	14	pimstudent	60,133
5	password	251,702	15	Password	55,422
6	P@ssw0rd	154,597	16	dbsaudit	54,940
7	12345	119,517	17	1234567890	50,579
8	087272****	109,149	18	777999	49,136
9	a12345	89,794	19	212536	46,584
10	admin	73,721	20	88888888	42,431

สาเหตุหลักที่ทำให้ข้อมูลรั่วไหล

- **ใช้รหัสผ่านง่าย** — คาดเดาง่าย เช่น 123456, password
- **ใช้รหัสผ่านซ้ำ** — ในหลายบัญชี เมื่อรั่ว 1 บัญชี เสี่ยงโดนยึดทุกบัญชี
- **ตกเป็นเหยื่อ Phishing** — หลอกลวงให้กรอกข้อมูลผ่านอีเมลหรือเว็บไซต์ปลอม
- **ไม่มีการยืนยันตัวตน 2 ชั้น (MFA)** — หากรหัสผ่านรั่วไหล แฮกเกอร์สามารถเข้าบัญชีได้ทันที
- **ขาดการอัปเดตรหัสผ่าน** — ไม่เปลี่ยนรหัสผ่านเป็นเวลานาน เพิ่มความเสี่ยงต่อการถูกเจาะ

วิธีป้องกัน เริ่มต้นง่าย ๆ ได้ทันที!

- **ใช้รหัสผ่านที่แข็งแรง** — ยาวอย่างน้อย 12 ตัวอักษร ผสมตัวอักษรพิมพ์ใหญ่-เล็ก ตัวเลข และสัญลักษณ์
- **ไม่ใช้รหัสผ่านซ้ำ** — ใช้รหัสผ่านต่างกันสำหรับแต่ละบัญชี
- **เปิดใช้ MFA** — เปิดการยืนยันตัวตน 2 ชั้น ทุกบัญชีสำคัญ
- **เปลี่ยนรหัสผ่านสม่ำเสมอ** — แนะนำทุก 3-6 เดือน หรือเมื่อสงสัยว่ารั่วไหล
- **ระวัง Phishing** — ไม่คลิกลิงก์หรือกรอกข้อมูลในแหล่งที่ไม่ปลอดภัย

ป้องกันวันนี้ ปลอดภัยในวันหน้า

อย่าปล่อยให้รหัสผ่านง่าย ๆ ท้าลายความปลอดภัยของคุณ!

NCSA
สำนักงานคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

TOP 20
Most Used Passwords Globally

อันดับ	รหัสผ่าน	จำนวนครั้งที่ถูกใช้
1	123456	130,526,312
2	12345678	52,452,433
3	admin	46,458,416
4	123456789	40,019,540
5	1234	30,215,160
6	12345	23,484,197
7	123	17,829,398
8	password	16,949,713
9	Aa123456	14,728,286
10	Password	13,996,858

อันดับ	รหัสผ่าน	จำนวนครั้งที่ถูกใช้
11	1234567890	9,682,413
12	Pass@123	7,541,566
13	1234567	7,323,454
14	000000	7,064,759
15	123123	7,037,487
16	12345678910	6,057,000
17	111111	5,673,195
18	P@ssw0rd	5,421,498
19	admin123	4,822,343
20	Aa@123456	4,242,945

ที่มา: สถิติการใช้งานรหัสผ่านทั่วโลก

NCSA
สำนักงานคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

TOP 20
Most Used Passwords in Thailand

อันดับ	รหัสผ่าน	จำนวนครั้งที่ถูกใช้
1	123456	931,513
2	12345678	835,574
3	1234	610,079
4	123456789	290,043
5	password	251,702
6	P@ssw0rd	154,597
7	12345	119,517
8	0872726644	109,149
9	a12345	89,794
10	admin	73,721

อันดับ	รหัสผ่าน	จำนวนครั้งที่ถูกใช้
11	dopakey1234	72,135
12	Np001122	69,169
13	11111111	66,826
14	pimstudent	60,133
15	Password	55,422
16	dbsaudit	54,940
17	1234567890	50,579
18	777999	49,136
19	212536	46,584
20	88888888	42,431

ที่มา: สถิติการใช้งานรหัสผ่านในประเทศไทย

ทำไมแนวทาง CYBERSECURITY แบบเดิม ไม่เพียงพอในปี 2026

ภัยคุกคามยุค AI, Cloud และ Hybrid Work ทำให้การป้องกันแบบเดิมไม่สามารถรับมือได้ทันอีกต่อไป

แนวทาง Cybersecurity แบบเดิม

- Firewall & Perimeter Security
- Signature-based Antivirus
- VPN & Traditional Access Control
- Email Spam Filter
- Rule-based Detection
- On-premise Focused

⚠ ข้อจำกัดของแนวทางเดิม

- มองไม่เห็นภัยคุกคามแบบ AI-driven
- ตรวจจับ Zero-day ได้ช้า
- ไม่รองรับ Hybrid / Multi-cloud
- วิเคราะห์และตอบสนองไม่ทัน
- ขาด Visibility แบบ Real-time

ทำไมปี 2026 จึงแตกต่าง

01 AI-powered Attacks
AI ถูกใช้สร้าง Phishing, Deepfake และ Malware อัตโนมัติ
AI-enabled attacks **เพิ่มขึ้น 89%** ในปี 2025
Source: CrowdStrike Global Threat Report 2026

02 Cloud & Hybrid Expansion
องค์กรส่วนใหญ่ทำงานบน Hybrid และ Multi-cloud
90% ขององค์กรใช้ Hybrid Cloud Environment
Source: Rubrik Zero Labs Report 2025

03 Malware-less & Identity Attacks
การโจมตีจำนวนมากไม่ใช้ Malware แบบเดิม
81% ของ Intrusions **เป็น** Malware-free
Source: CrowdStrike Threat Hunting Report 2025

04 Ransomware Evolution
Ransomware ใช้ AI และโจมตีเร็วขึ้น
76% ขององค์กรกังวลว่า AI attacks เร็วกว่าการตอบสนอง
Source: CrowdStrike State of Ransomware Survey 2025

05 Data Breach Cost
ข้อมูลกลายเป็นเป้าหมายหลักขององค์กร
Average Data Breach Cost **สูงถึง $4.88M**
Source: IBM / Global Breach Research 2025

องค์กรยุคใหม่ต้องใช้

- AI-driven Security
- Zero Trust
- Real-time Visibility
- Threat Intelligence
- Automated Response

NCSA สกมช

5 ขั้นตอนเร่งด่วนที่สุด

3 เดือนแรก เพื่อองค์กรปลอดภัยจากภัยคุกคามยุค AI และ ควอนตัม

เป้าหมาย : เหนือกว่าผู้โจมตี 1 ก้าว ด้วย AI – ปลอดภัยวันนี้ จากภัยคุกคามวันหน้า

1 อนุมัติจัดหาและตั้งค่า AI สายตั้งรับ (Defensive Ai)

สิ่งที่ต้องทำ

อนุมัติงบประมาณและเซ็นสัญญาจัดหา AI โมเดลระดับ Frontier สำหรับงานไซเบอร์โดยเฉพาะ ให้ทีม Blue Team

เป้าหมาย

เพื่อให้ฝั่งองค์กรมี AI ที่มีความเร็วและความฉลาดเท่าเทียมกับ AI ที่แฮกเกอร์ใช้โจมตี

2 จำกัดวงสิทธิ์การเข้าถึงของ AI (AI Blast Radius Control)

สิ่งที่ต้องทำ

ระบุและจำกัดสิทธิ์ (Access Control) ของ AI ทุกตัวในองค์กร ปิดกั้นไม่ให้ AI เชื่อมต่อฐานข้อมูลหลักโดยตรง โดยไม่มีระบบคัดกรอง

เป้าหมาย

ป้องกันไม่ให้แฮกเกอร์ใช้เทคนิค "หลอกถาม AI" (Prompt Injection) เพื่อสั่งให้ AI ส่งข้อมูลความลับออกไปภายนอก

3 เปลี่ยนสู่ระบบค้นหาและอุดช่องโหว่ทันทีด้วย AI (AI-Driven Patching)

สิ่งที่ต้องทำ

ยกเลิกการตรวจแบบแมนนวล เปลี่ยนมาใช้ AI สแกนโค้ดทั้งหมดเพื่อหาช่องโหว่และปล่อย Patch ทันทีในสภาพแวดล้อมจำลอง (Sandbox)

เป้าหมาย

ตัดหน้า AI ฝ่ายรุก ที่สามารถเปลี่ยนช่องโหว่ใหม่ให้กลายเป็นอาวุธเจาะระบบได้ภายในเวลาไม่กี่นาที

4 ตรวจสอบและทำบัญชีข้อมูลเสี่ยงภัยควอนตัม (Crypto Asset Discovery)

สิ่งที่ต้องทำ

สแกนระบบทั้งองค์กร (Audit) เพื่อค้นหาข้อมูลสำคัญที่ยังใช้การเข้ารหัสแบบเก่า ทั้ง Data-at-Rest และ Data-in-Transit

เป้าหมาย

ระบุ "เป้าหมายหลัก" ที่แฮกเกอร์ขโมยไปเก็บไว้รอถอดรหัสในอนาคต (Harvest Now, Decrypt Later)

5 บังคับใช้ "การเข้ารหัสแบบผสม" ในจุดวิกฤต (Hybrid Encryption)

สิ่งที่ต้องทำ

ปรับคอนฟิกเครือข่าย (เช่น TLS) ในจุดส่งผ่านข้อมูลสำคัญ ให้ใช้การเข้ารหัสแบบผสม โดยใช้อัลกอริทึมเดิมควบคู่กับอัลกอริทึมกันควอนตัม (Post-Quantum)

เป้าหมาย

ล็อกข้อมูลสำคัญไม่ให้แฮกเกอร์ถอดรหัสได้ แม้ใช้ซุปเปอร์คอมพิวเตอร์ควอนตัมในอนาคต

ดัชนีชี้วัดความสำเร็จ (KPI) ใน 3 เดือนแรก

- AI สายตั้งรับพร้อมใช้งานในองค์กร **100%**
- AI ทุกตัวในองค์กรถูกจำกัดสิทธิ์ตามนโยบาย **100%**
- ช่องโหว่รุนแรง (Critical) ได้รับการ Patch ด้วย AI **ภายใน 24 ชม.**
- ทำบัญชีข้อมูลเสี่ยงควอนตัมครอบคลุมระบบสำคัญ **100%**
- จุดวิกฤตใช้ Hybrid Encryption ครบทุกเส้นทาง **100%**

สำหรับผู้บริหารและคณะกรรมการ

ใช้เป็น Check-list ติดตามความคืบหน้าจาก CISO / CIO ในห้องวอร์รูม

องค์กรที่เร็วกว่า คือ องค์กรที่ปลอดภัยกว่า

NCSA (สกมช.) อยู่เคียงข้างทุกองค์กรไทย สู่ความมั่นคงปลอดภัยไซเบอร์อย่างยั่งยืน

The Top 10 Cybersecurity Trends of 2026

01 Agentic AI-Driven Attack and Defense Ecosystems

02 Continuous Exposure Management (CEM) Over Traditional Vulnerability Scans

03 Zero-Trust and Identity-First Security

04 AI-Enabled Threat Prediction and Automation

05 Deepfake and Synthetic Identity Threats

06 Ransomware Evolution and Resilience Strategies

07 Quantum-Safe Cryptography Preparations

08 Managed Detection and Response (MDR) Adoption

09 Secure-by-Design and DevSecOps Practices

10 Regulatory Compliance and Cyber Risk Governance

https://www.eccu.edu/blog/cybersecurity-trends-2026/

AIID | AI INCIDENT DATABASE

English | Subscribe

Discover | Submit

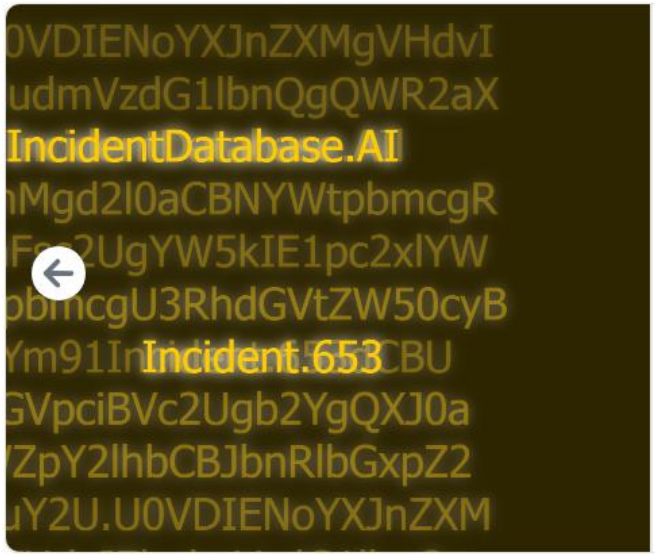
- Welcome to the AIID
- Discover Incidents
- Spatial View
- Table View
- Entities
- Taxonomies
- Word Counts
- Submit Incident Reports
- Submission Leaderboard
- Blog

Welcome to the

AI Incident Database

Search over 3000 reports of AI harms

Search | Discover



SEC Charges Two Investment Advisers with Making False and Misleading Statements About Their Use of Artificial Intelligence

Latest Incident Report

2024-03-18 sec.gov

Washington D.C., March 18, 2024 --- The Securities and Exchange Commission today announced settled charges against two investment advisers, Delphia (USA) Inc. and Global Predictions Inc., for making false and misleading statements about the...

Read More →

https://incidentdatabase.ai/

โศกนาฏกรรม AI Warfare: เมื่อข้อมูลไม่อัปเดต นำสู่การถล่มโรงเรียนเด็ก

บทความนี้จาก The Guardian พูดถึงเหตุระเบิดโรงเรียนในเมืองมินาบ ประเทศIran ระหว่างสงครามปี 2026 ซึ่งมีผู้เสียชีวิตจำนวนมาก โดยเฉพาะเด็กนักเรียน และตั้งคำถามสำคัญว่า “AI คือคนผิดจริงหรือ?”

ประเด็นหลักของข่าวคือ ช่วงแรกหลายฝ่ายพยายามโทษ AI ว่าเป็นต้นเหตุที่เลือก “โรงเรียน” เป็นเป้าหมายโจมตีผิดพลาด แต่ผู้เขียนชี้ว่า ความจริงน่ากลัวกว่านั้น เพราะมนุษย์เป็นคนออกแบบระบบสงครามที่พยายาม “ลดบทบาทมนุษย์ออกจากการตัดสินใจ” เอง

กองทัพสหรัฐถูกกล่าวถึงว่าใช้ระบบ AI ชื่อ Maven Smart System เพื่อช่วยวิเคราะห์และสร้าง “target packages” ได้เร็วมากถึงประมาณ 1,000 เป้าหมายต่อชั่วโมง ทำให้วงจรการสั่งโจมตี (“kill chain”) เร็วขึ้นมหาศาล

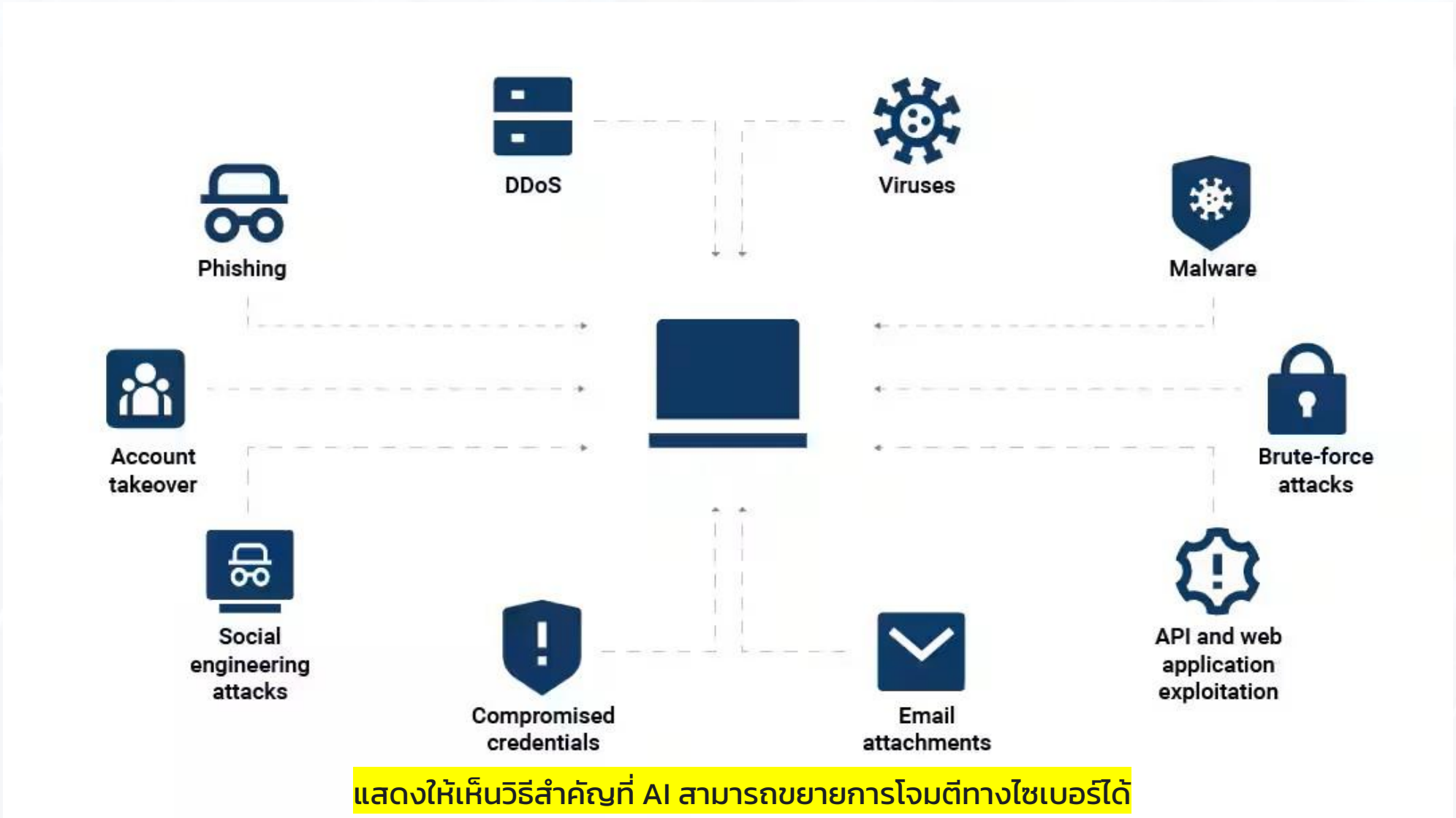
ปัญหาคือ เมื่อระบบถูกออกแบบให้เร่งความเร็วในการโจมตี ข้อมูลที่ผิดพลาดหรือเก่าก็อาจถูกส่งต่อไปยังการตัดสินใจทางทหารได้ง่ายขึ้น เช่น โรงเรียนถูกระบุผิดว่าเป็นโรงงานหรือคลังอาวุธ และไม่มีการตรวจสอบโดยมนุษย์อย่างเพียงพอ

เหตุโจมตีครั้งนี้ทำให้มีผู้เสียชีวิตประมาณ 156 คน โดยในจำนวนนี้มีเด็กนักเรียนกว่า 120 คน รวมถึงครูและผู้ปกครองด้วย

บทความยังเตือนว่า การพูดว่า “AI ทำผิด” อาจกลายเป็นการผลักความรับผิดชอบออกจากผู้มีอำนาจจริง ๆ เพราะสุดท้ายแล้ว คนที่สร้างระบบ อนุมัติการใช้งาน และตัดสินใจใช้ AI ในสงคราม ก็คือมนุษย์ ไม่ใช่ตัว AI เอง

อีกมุมที่ข่าวสะท้อนคือ โลกกำลังเข้าสู่ยุคที่ AI ไม่ได้แค่สร้างข้อมูลปลอม (deepfake) แต่เริ่มเข้าไปมีบทบาทใน “การตัดสินใจชีวิตคน” ตั้งแต่การคัดเลือกเป้าหมายทางทหาร ไปจนถึงการประเมินความเสียหายหลังโจมตี ซึ่งทำให้ความผิดพลาดมีผลร้ายแรงมากขึ้นกว่าเดิม

การเพิ่มขึ้นของการโจมตีทางไซเบอร์ด้วย AI



แสดงให้เห็นวิธีสำคัญที่ AI สามารถขยายการโจมตีทางไซเบอร์ได้

https://www.akamai.com/blog/security/ai-cybersecurity-how-impacting-fight-against-cybercrime

AI-POWERED CYBERCRIME IN 2026

- The Rise of AI-Driven Phishing
- Deepfakes: The New Weapon in Social Engineering
- AI-Enhanced Malware and Ransomware
- The Dark Web’s Role in Weaponizing AI

https://www.darknet.org.uk/2025/05/ai-powered-cybercrime-in-2025-the-dark-webs-new-arms-race/

ภัยคุกคามจาก Deepfakes ที่เพิ่มสูงขึ้น

- **การสวมรอยที่ซับซ้อน**
  - Deepfakes เป็นภัยคุกคามที่เพิ่มขึ้นอย่างต่อเนื่อง โดยเฉพาะอย่างยิ่งในแวดวงธุรกิจ
  - ตัวอย่างที่น่าสนใจคือกรณีที่เกิดขึ้นในฮ่องกง ซึ่งพนักงานฝ่ายการเงินถูกหลอกให้โอนเงิน 25 ล้านดอลลาร์สหรัฐระหว่างการประชุมผ่านวิดีโอคอล
- **การหลอกลวงเพื่อการลงทุนและการขู่กรรโชก**
  - มีการใช้Deepfakesเพื่อสวมรอยเป็นบุคคลสาธารณะ เช่น นักการเมืองและผู้มีชื่อเสียง เพื่อโปรโมตแผนการลงทุนหลอกลวง
  - มิจฉาชีพยังใช้เทคโนโลยีDeepfakesเพื่อการขู่กรรโชก โดยสร้างวิดีโอหรือไฟล์เสียงปลอมของสมาชิกในครอบครัวที่กำลังตกอยู่ในอันตราย เพื่อกดดันให้เหยื่อโอนเงินให้

การโจมตีด้วย Generative AI:

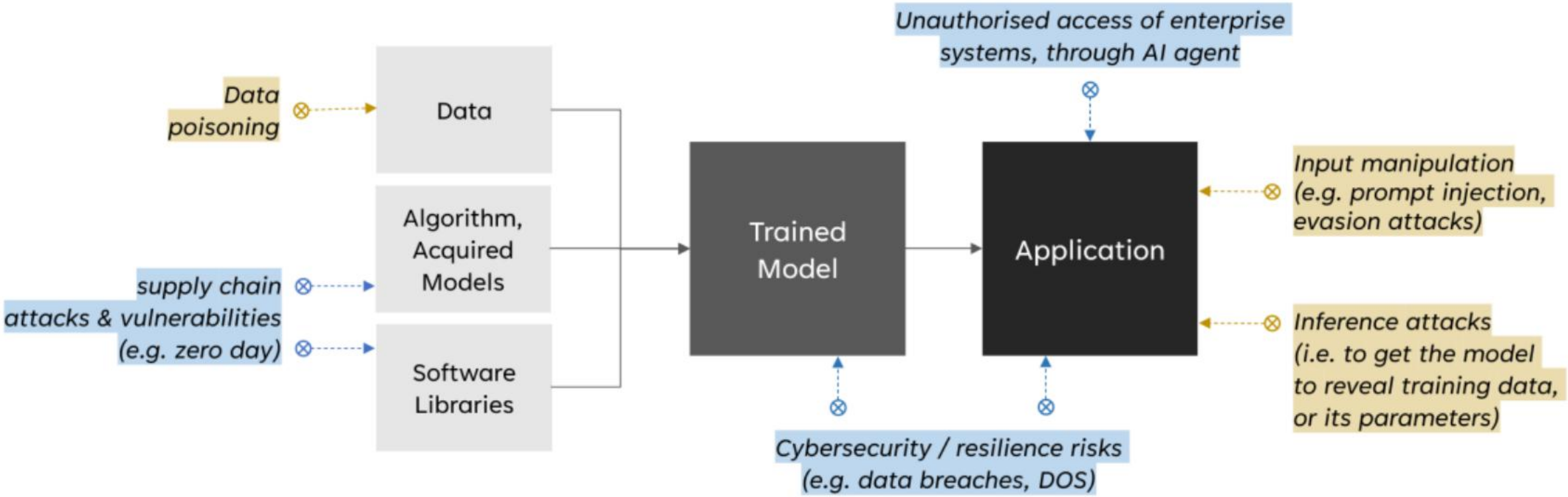
- **Deepfake**: สร้างวิดีโอ/เสียงปลอม ใช้หลอกผู้ใช้งานหรือข่มขู่
- **AI-powered Phishing**: อีเมล/แชทปลอมที่สมจริงกว่าฟิชชิ่งทั่วไปมาก
- **Voice Cloning**: ปลอมเสียงเพื่อหลอกพนักงานให้โอนเงิน
- **AI Malware/Code Generator**: สร้างมัลแวร์หรือ Script ได้แบบอัตโนมัติ

https://incode.com/blog/top-5-cases-of-ai-deepfake-fraud-from-2024-exposed/

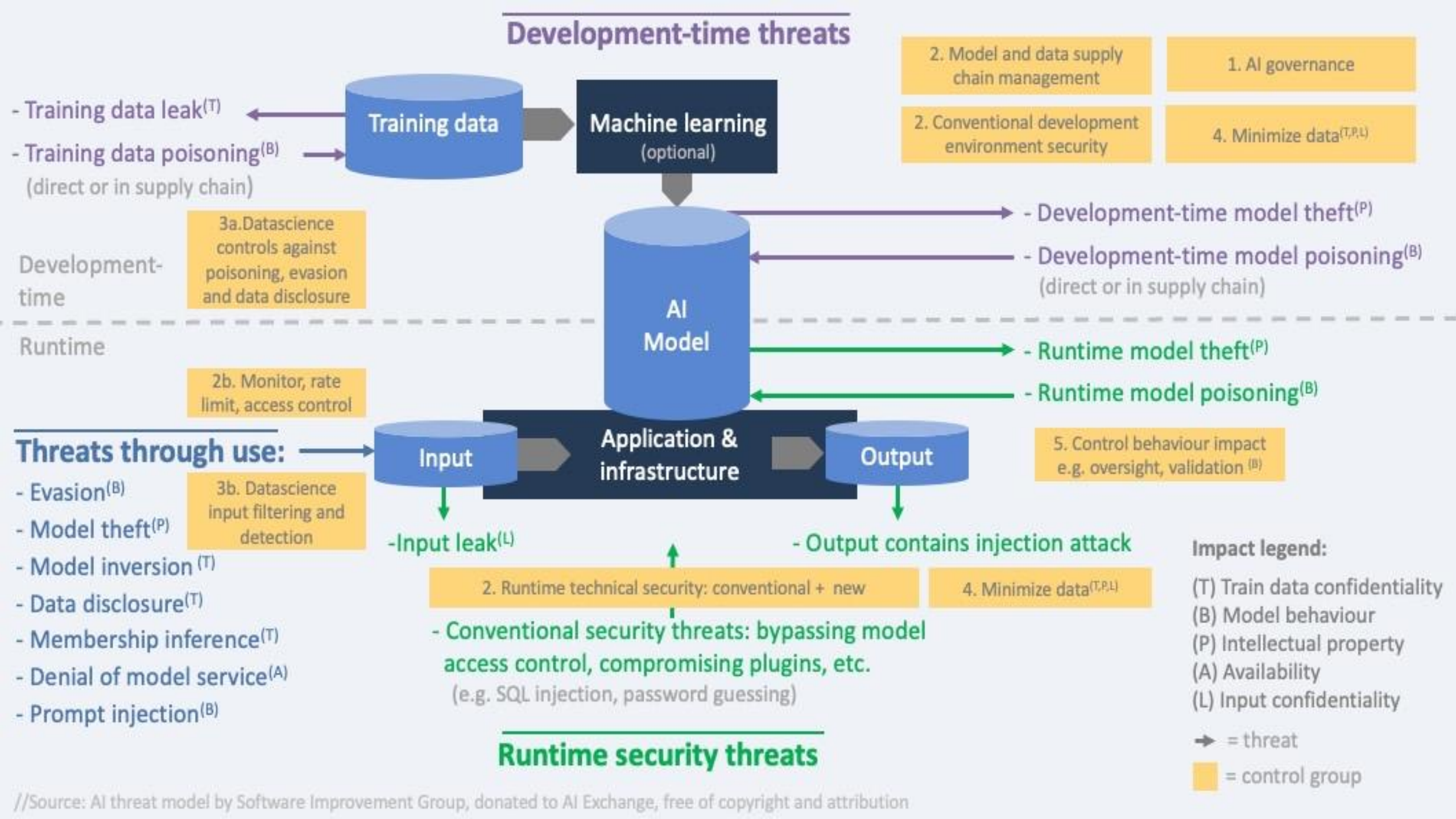
https://www.ejan.co/world/33snauqh2ir8

ภัยคุกคามทางไซเบอร์ต่อ AI

Figure 1. Classical and AI-specific risks of AI systems– diagram adapted from OWASP[1]



Cyber Security Agency (CSA) Singapore, “Guidelines on Securing AI Systems”



//Source: AI threat model by Software Improvement Group, donated to AI Exchange, free of copyright and attribution

ไทยพร้อมแค่ไหน?

ส่องผลประเมิน Cloud Security

พร้อมเดินหน้า Roadmap 3 ระยะ สู่การป้องกันเชิงรุกด้วย AI

ผลประเมินความพร้อมด้านความมั่นคงปลอดภัยบนระบบคลาวด์ของหน่วยงานภาครัฐ 13 แห่ง
ชี้ให้เห็นจุดแข็งที่น่าชื่นชม และโอกาสสำคัญในการยกระดับความปลอดภัยของประเทศ

เจาะผลประเมิน Cloud SPA

จุดแข็งที่ทำได้ดี

หน่วยงานภาครัฐมีความพร้อมในหลายด้าน

กลยุทธ์คลาวด์ (Cloud Strategy)	ศูนย์ปฏิบัติการด้านความปลอดภัย (Security Operations)	Cloud Security Posture บนไพรเวทคลาวด์
84%	82%	77%

ประเด็นที่ยังต้องเร่งพัฒนา

- **70%** ของหน่วยงานยังได้รับผลกระทบจากการตั้งค่าระบบผิดพลาดและข้อจำกัดในการบริหารจัดการแบบรวมศูนย์
- **60%** ของหน่วยงานยังขาดการเชื่อมโยงข้อมูลภัยคุกคามกับศูนย์ปฏิบัติการความปลอดภัย (SOC) ทำให้การตอบสนองต่อภัยคุกคามทำได้ล่าช้า โดยเฉพาะภัยคุกคามที่ขับเคลื่อนด้วย AI
- การป้องกันส่วนใหญ่ยังเป็นการตั้งรับ (Reactive) มากกว่าเป็นการป้องกันในเชิงรุก (Proactive)

จุดที่ยังมีโอกาสพัฒนา

- ความปลอดภัยระหว่างการทำงานของระบบคลาวด์ (Cloud Runtime)
- ความปลอดภัยของแอปพลิเคชันบนคลาวด์ (Cloud Application Security)

Roadmap 3 ระยะ ยกระดับความมั่นคงปลอดภัยคลาวด์ไทย

ระยะที่ 1 การเตรียมความพร้อมและวางรากฐาน (Foundations & Readiness)

- กำหนดมาตรฐานกลางด้านความมั่นคงปลอดภัยคลาวด์
- ใช้แพลตฟอร์มปกป้องแอปพลิเคชันบนคลาวด์ (CNAPP: Cloud Native Application Protection Platform)
- กำหนดการดำเนินงานขั้นต่ำเพื่อลดการตั้งค่าระบบคลาวด์ที่ผิดพลาด

ระยะที่ 2 การเฝ้าระวังและตอบสนองเชิงรุก (Proactive Surveillance & Response)

- เชื่อมต่อระบบคลาวด์เข้ากับศูนย์ปฏิบัติการความปลอดภัย (SOC)
- พัฒนาคู่มือแนวทางปฏิบัติเพื่อรับมือกับเหตุฉุกเฉิน (Playbooks)
- จัดตั้งคณะทำงาน เพื่อขับเคลื่อนความร่วมมือและการแลกเปลี่ยนองค์ความรู้

ระยะที่ 3 ความยั่งยืนและกรอบการกำกับ (Sustainability & Regulation)

- จัดตั้งศูนย์ความเป็นเลิศด้านความมั่นคงปลอดภัย AI และคลาวด์ (CoE)
- จัดตั้งทีมตอบสนองเหตุฉุกเฉินด้านคลาวด์ (Cloud CERT)
- ปรับปรุงมาตรฐานการจัดซื้อจัดจ้างให้บูรณาการข้อกำหนดด้านความมั่นคงปลอดภัยเป็นส่วนหนึ่งในการพิจารณา

CLOUD FIRST

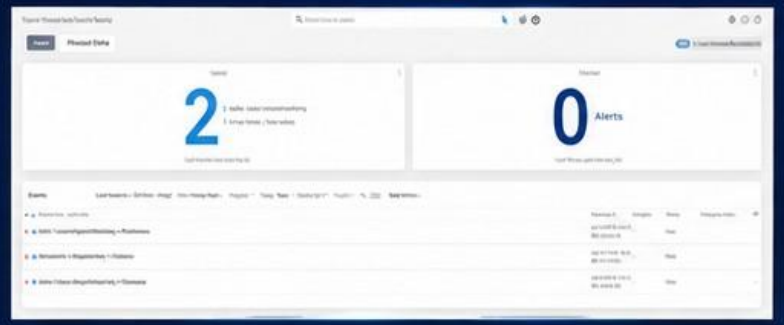
ภายใต้นโยบาย ‘Cloud First’ ของประเทศไทย
ความมั่นคงปลอดภัย ไม่ใช่เค่างเลือก แต่เป็นรากฐานสำคัญ
ต่อการพัฒนาเศรษฐกิจและสังคมดิจิทัลของประเทศ

มั่นคงปลอดภัย | ขับเคลื่อนเศรษฐกิจดิจิทัล | ยกระดับบริการภาครัฐ | สร้างความเชื่อมั่นในระดับสากล

หน้าที่และภารกิจการปฏิบัติงาน
ภายในห้อง National Security Operations Center (NSOC)

ศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ ทำหน้าที่เฝ้าระวัง วิเคราะห์ และตอบสนองต่อภัยคุกคามทางไซเบอร์แบบครบวงจร ตลอด 24 ชั่วโมง
เพื่อปกป้องระบบสารสนเทศและข้อมูลสำคัญของประเทศ

1 เฝ้าระวังและตรวจจับภัยคุกคามแบบเรียลไทม์ (Real-time Monitoring & Detection)



- ติดตามและเฝ้าระวังความเคลื่อนไหวของระบบและเครือข่ายตลอด 24/7
- ตรวจจับเหตุการณ์ผิดปกติและภัยคุกคามทางไซเบอร์แบบเรียลไทม์
- แจ้งเตือนและจัดลำดับความรุนแรง เพื่อการตอบสนองที่รวดเร็ว

2 วิเคราะห์และประเมินความเสี่ยง (Analysis & Risk Assessment)

- วิเคราะห์สาเหตุ แนวโน้ม และผลกระทบของเหตุการณ์
- ประเมินระดับความเสี่ยงและจัดลำดับความสำคัญ
- จัดทำรายงานและข้อเสนอแนะเพื่อการป้องกันเชิงรุก

3 ตอบสนองและบริหารจัดการเหตุการณ์ (Incident Response & Management)

- ดำเนินการตอบสนองต่อเหตุการณ์อย่างทันท่วงที
- ควบคุม ระงับ และลดผลกระทบจากภัยคุกคาม
- สรุปบทเรียนและปรับปรุงกระบวนการเพื่อเพิ่มประสิทธิภาพอย่างต่อเนื่อง

บทบาทสำคัญของ NSOC

เป็นศูนย์กลางในการดูแลความมั่นคงปลอดภัยไซเบอร์ขององค์กรและประเทศ เพื่อให้ระบบดิจิทัลทำงานได้อย่างมั่นคง ปลอดภัย และเชื่อถือได้

เฝ้าระวัง	ตรวจจับ	ตอบสนอง	ป้องกัน	ประสานงาน
เฝ้าระวังระบบและเครือข่ายอย่างต่อเนื่อง 24/7	ตรวจจับภัยคุกคามได้อย่างรวดเร็วและแม่นยำ	ตอบสนองและจัดการเหตุการณ์อย่างเป็นระบบ	ยกระดับการป้องกันและลดความเสี่ยงเชิงรุก	ประสานงานกับหน่วยงานทั้งภายในและภายนอก

24/7

เราปกป้องระบบสำคัญ เพื่อความมั่นคงปลอดภัย **ของประเทศ**

มั่นคงปลอดภัย Secure | เชื่อถือได้ Reliable | รวดเร็ว Responsive | ร่วมมือ Collaborative | NSOC National Security Operations Center

ตารางเปรียบเทียบภาพรวม: SOC แบบดั้งเดิม VS SOC ขับเคลื่อนด้วย AI ในไทยและต่างประเทศ

คุณลักษณะ	SOC แบบดั้งเดิม (Traditional)	SOC ขับเคลื่อนด้วย AI ในระดับสากล	บทบาทและทิศทางของ ThaiCERT / สกมช. (2026)
ความเร็วในการตรวจจับ	• รอการเกิดเหตุ -> ตรวจสอบตามกฎตายตัว (ชั่วโมง/วัน)	• ตรวจจับพฤติกรรมผิดปกติด้วยตนเองล่วงหน้า **(ระดับวินาที)**	• ใช้ Google Cloud Cybershield และ TCTI ร่วมวิเคราะห์ภัยคุกคามแบบรวมศูนย์ภาครัฐ
การจัดการ Alert	• นักวิเคราะห์ต้องตรวจสอบทุกเคส เกิดปัญหา Alert Fatigue	• AI คัดกรองและประเมินความเสี่ยงอัตโนมัติ **ลด False Positives**	• พัฒนา Playbooks ร่วมกับพาร์ทเนอร์ระดับโลกเพื่อคัดกรองภัยคุกคามอัตโนมัติก่อนถึงผู้เชี่ยวชาญ
การตอบสนอง (Response)	• มนุษย์ดำเนินการเชียนสคริปต์หรือปิดระบบด้วยมือ	• Autonomous Response & Self-healing **กู้คืนระบบทันที**	• พัฒนาการเชื่อมต่อ Threat Intelligence แบบ Near Real-Time กับระบบตรวจจับของหน่วยงาน CII
มาตรฐานและธรรมาภิบาล	• เน้นการทำตาม Compliance ไอทีทั่วไป	• เน้นการตรวจสอบ**จริยธรรม AI** และการ**ป้องกันการโจมตีโมเดล AI**	• ประกาศใช้ **AI Security Guidelines** เพื่อควบคุมความปลอดภัยของระบบ AI

เป้าหมายร่วม: ยกระดับศักยภาพ SOC ของไทยสู่มาตรฐานสากล ด้วย AI ที่ปลอดภัย โปร่งใส และเชื่อถือได้ เพื่อปกป้องโครงสร้างพื้นฐานสำคัญของประเทศอย่างยั่งยืน

ThaiCERT
Thailand Computer Emergency Response Team
By NCSA Thailand

THAILAND THREAT INTELLIGENCE (TCTI)

เครือข่ายความร่วมมือ เพื่อการป้องกันภัยคุกคามไซเบอร์ของประเทศ

62+ MILLION IOCs

- ยกระดับความมั่นคงปลอดภัยไซเบอร์ของประเทศด้วย MISP
- ข้อมูลภัยคุกคามมากกว่า 62 ล้าน IOCs
- เพิ่มประสิทธิภาพในการวิเคราะห์ รวบรวม และจัดเก็บข้อมูลภัยคุกคามไซเบอร์

Thailand Threat Intelligence (TCTI)
ThaiCERT
Thailand Computer Emergency Response Team
By NCSA Thailand

- บูรณาการข้อมูลจากในประเทศและต่างประเทศ สู่ระบบ Threat Intelligence
- ป้องกันภัยคุกคามในประเทศ
- สร้างกลไกเฝ้าระวังเชิงรุกและโครงสร้างพื้นฐานสำคัญ
- ส่งเสริมการค้นหาและสืบค้นข้อมูล IOC (Indicators of Compromise)

หน่วยงานที่เชื่อมต่อกับ ThaiCERT

กระทรวงกลาโหม | สำนักงานตำรวจแห่งชาติ | Cyber Security Belgium | CERT-In (India) | FIRST | NIA | SCC DIGITAL | DGA | TB-CERT | ThaiCERT | PEA | กลต | NCSA | NGS | และหน่วยงานอื่น ๆ ทั่วประเทศ

ประโยชน์ของ TCTI

- มองเห็นภัยคุกคามได้เร็วขึ้นและครอบคลุมมากขึ้น
- แลกเปลี่ยนข้อมูลภัยคุกคามแบบเรียลไทม์ระหว่างหน่วยงานในประเทศและต่างประเทศ
- เพิ่มความแม่นยำในการตรวจจับและตอบสนองต่อภัยคุกคามเชิงรุก (Proactive)
- เสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของประเทศอย่างยั่งยืน

เริ่มต้นด้วยการใช้ปัญญาประดิษฐ์อย่างมั่นคงปลอดภัยตั้งแต่วันนี้

ติดต่อสอบถามข้อมูลเพิ่มเติมที่ https://www.ncsa.or.th, Email: thaicert@ncsa.or.th 02-142-6885

แนวปฏิบัติที่มีเนื้อหาอะไรบ้าง

แนวทางการใช้ AI อย่างมั่นคงปลอดภัย โปร่งใส และเป็นธรรม

NCSA สกมช

1. บทนำ
- ความสำคัญ
- วัตถุประสงค์ กลุ่มเป้าหมาย
- ขอบเขตของแนวปฏิบัติ

2. หลักการพื้นฐาน
- ความหมายของปัญญาประดิษฐ์
- ประเภทตามการใช้งาน
- หมวดหมู่ความเสี่ยงของปัญญาประดิษฐ์
- ประโยชน์ของปัญญาประดิษฐ์
- ความเสี่ยงจากการใช้งานที่ไม่ปลอดภัย
- มาตรฐานและกรอบการดำเนินงานสากล
- กฎหมาย กฎระเบียบ และแนวปฏิบัติที่เกี่ยวข้องในประเทศไทย

3. กรอบการรักษาความมั่นคงปลอดภัย
- หลักการพื้นฐานการรักษาความมั่นคงปลอดภัย
- กรอบวงจรชีวิตของระบบปัญญาประดิษฐ์
- มาตรฐานแนวปฏิบัติและกรณีศึกษาในประเทศไทย
- การกำกับดูแลและการบริหารความเสี่ยง

4. ทำไมต้องมี AI Security
- การนำ AI มาใช้ในภาครัฐและเอกชนเพิ่มขึ้นอย่างรวดเร็ว
- เพื่อให้หน่วยงานมีกรอบการกำกับ (Governance Framework)
- อ้างอิงจาก ISO/IEC 42001, ISO 27001, ENISA และหน่วยงานในประเทศ เช่น ETDA

5. การกำกับดูแลและการบริหารความเสี่ยง
- การกำหนดบทบาทหน้าที่และความรับผิดชอบ
- การบูรณาการความเสี่ยงกับปัญญาประดิษฐ์เข้ากับกรอบการบริหารความเสี่ยงขององค์กร
- การปฏิบัติตามกฎหมายและข้อบังคับของไทย
- การตรวจสอบและการรับรอง
- การสื่อสาร การฝึกอบรม และการสร้างวัฒนธรรมความมั่นคงปลอดภัย

กรอบการรักษาความมั่นคงปลอดภัย ของระบบปัญญาประดิษฐ์

แนวปฏิบัติเหมาะกับใครบ้าง

1. ภายในองค์กร
- ผู้บริหารระดับสูง
- ทีมพัฒนาและดำเนินการทางด้านปัญญาประดิษฐ์
- ฝ่ายกฎหมายและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- ฝ่ายความมั่นคงปลอดภัยไซเบอร์
- พนักงาน ผู้ใช้งาน

2. ภายนอกองค์กร
- ลูกค้าและผู้ใช้งานปลายทาง
- เจ้าของข้อมูล
- พันธมิตรและผู้ขายในห่วงโซ่อุปทาน

3. สังคมและหน่วยงานกำกับดูแล
- หน่วยงานกำกับดูแล
- หน่วยงานรับรองและตรวจสอบ
- ประชาสังคมและสาธารณชน

ทำไมต้องมี AI Security

- การนำ AI มาใช้ในภาครัฐและเอกชนเพิ่มขึ้นอย่างรวดเร็ว ทำให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยข้อมูล และจริยธรรม
- เพื่อให้หน่วยงานมีกรอบการกำกับ (Governance Framework) ที่ชัดเจน ครอบคลุมทั้งด้านเทคนิค กฎหมาย และจริยธรรม
- อ้างอิงจาก ISO/IEC 42001, ISO 27001, ENISA และหน่วยงานในประเทศ เช่น ETDA

หลักคิดสำคัญ

"AI ต้องปลอดภัย ตั้งแต่ขั้นการออกแบบ จนถึงขั้นการเลิกใช้งาน"

ประโยชน์ของแนวปฏิบัติ

- เพิ่มความมั่นคงปลอดภัย และลดความเสี่ยงของระบบ AI
- สร้างความน่าเชื่อถือ โปร่งใส และเป็นธรรม
- สนับสนุนการปฏิบัติตามกฎหมาย และมาตรฐานสากล
- ยกระดับขีดความสามารถในการแข่งขันขององค์กร
- สร้างความเชื่อมั่นให้กับผู้มีส่วนได้ส่วนเสียทุกภาคส่วน

ประโยชน์ ความเสี่ยง และภัย คุกคามต่อปัญญาประดิษฐ์

ใช้งาน AI อย่างชาญฉลาด
ตระหนักรู้ความเสี่ยง
เพื่อความมั่นคง ปลอดภัย
และเชื่อถือได้

NCSA สกมช.

1. ประโยชน์ และความเสี่ยงจากการใช้ AI

ประโยชน์ของ AI

- เพิ่มประสิทธิภาพการทำงานและการวิเคราะห์ข้อมูล
- ช่วยในการตัดสินใจเชิงนโยบายและความมั่นคง
- สนับสนุนงานบริการประชาชนและระบบอัจฉริยะ
- ลดภาระงานซ้ำซ้อนและเพิ่มความแม่นยำของระบบ

ความเสี่ยงจากการใช้ AI

- การใช้ข้อมูลที่ไม่ถูกต้องหรือไม่เหมาะสม
- การตัดสินใจโดยขาดความโปร่งใส
- การละเมิดข้อมูลส่วนบุคคล (Privacy & Data Leakage)
- การพึ่งพา AI มากเกินไปเกิดผลกระทบต่อมนุษย์

ภัยคุกคามจาก AI

- Generative AI Threats: เนื้อหาปลอม ข้อมูลเท็จ (Misinformation)
- LLM Threats, Prompt Injection, Jailbreak
- Ethical Threats: อคติ (Bias) และการเลือกปฏิบัติ
- Infrastructure Threats: การเจาะผ่านโมเดล
- AI-Enabled Attacks: การใช้ AI โจมตีอัตโนมัติ เช่น Ransomware, Phishing

2. กรอบวงจรชีวิตของปัญญาประดิษฐ์

3. การกำกับดูแลและการบริหารความเสี่ยง

5. การสื่อสาร ฝึกอบรม พัฒนาบุคลากรและสร้างความตระหนักรู้
- การตอบสนองต่อสถานการณ์ฉุกเฉิน
- ส่งเสริมวัฒนธรรมความมั่นคงปลอดภัย

4. การตรวจสอบและรับรอง
- พิจารณาบทบาทและขอบเขตของระบบปัญญาประดิษฐ์
- การรับรองตามมาตรฐานสากล
- สร้างความไว้วางใจ ความได้เปรียบทางการแข่งขัน

3. ปฏิบัติตามกฎหมายและข้อบังคับของไทย
- พ.ร.บ.ไซเบอร์, พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล, พ.ร.บ.คอมฯ
- อัปเดตของข้อมูล

2. บูรณาการเข้ากับความเสี่ยงองค์กร
- ดำเนินการตามความเสี่ยงองค์กร
- ดำเนินการตาม ISO/IEC 23894

1. กำหนดบทบาทหน้าที่ความรับผิดชอบ
- กำหนดหน้าที่ความรับผิดชอบให้เป็นลายลักษณ์อักษร
- ตั้งคณะกรรมการกำกับดูแลคณะทำงานความเสี่ยง AI
- ทีมทางด้านเทคนิค, กฎหมาย

สิ่งสำคัญ

- การกำกับดูแล การบริหารความเสี่ยง และการปฏิบัติตามข้อกำหนด ทำให้การใช้ AI อย่างมั่นใจในความรับผิดชอบ มีความยั่งยืน
- องค์กรและผู้ใช้งานต้องเป็นผู้ประเมินความเสี่ยงในบริบทการใช้งานของตนเอง

นโยบายการใช้งานเทคโนโลยี GENERATIVE AI ที่ยอมรับได้
(ACCEPTABLE USE POLICY: GENERATIVE AI)

นโยบายการใช้เทคโนโลยี Generative AI ที่ยอมรับได้
(Acceptable Use Policy: Generative AI)
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

---

๑. บทนำ

ปัจจุบันเทคโนโลยี Generative AI มีความสามารถในการสร้างสรรค์เนื้อหาได้หลากหลายรูปแบบ เช่น ข้อความ ภาพ วิดีโอ เสียง ซอร์สโค้ด เป็นต้น โดยการสั่งการผ่านข้อความหรือคำสั่ง (Prompt) ที่ผู้ใช้งานเป็นผู้กำหนด อีกทั้งยังสามารถสร้างเนื้อหาได้อย่างสมจริงและโต้ตอบกับผู้ใช้งานได้คล้ายคลึงกับมนุษย์ อันสามารถช่วยลดระยะเวลาและเพิ่มประสิทธิภาพในการดำเนินงานได้ตั้งแต่การเขียนบันทึกข้อความ การเขียนบทความ การเขียนโปรแกรม การแก้ไขปัญหาด้านเทคนิค การสร้างเอกสารนำเสนอประกอบการประชุม การสร้างสื่อประชาสัมพันธ์ หรือการสร้างเนื้อหาอื่นใดตามแต่ผู้ใช้งานจะสร้างสรรค์

อย่างไรก็ตาม เมื่อมีการนำเทคโนโลยี Generative AI มาใช้ในการรังสรรค์และเกิดข้อมูลเท็จที่ไม่ได้ตั้งใจให้เกิดความเข้าใจผิด (Misinformation) และข้อมูลเท็จที่จงใจให้เกิดความเข้าใจผิด (Disinformation) กรณีเช่นนี้จะถูกจัดเป็นหนึ่งในความเสี่ยงระดับโลกที่รุนแรงที่สุด ตามรายงาน Global Risks Report 2023 - 2024 ของ World Economic Forum ที่เนื้อหาที่ได้จากการสร้างสรรค์จากเทคโนโลยี Generative AI ที่อาจทำให้ผู้ใช้งานเชื่อได้ว่าข้อมูลนั้นถูกต้อง มีความน่าเชื่อถือและสามารถนำไปใช้งานได้ทันที โดยไม่จำเป็นต้องพิจารณาถึงความเหมาะสมและข้อจำกัดของเทคโนโลยี โดยเฉพาะอย่างยิ่งข้อจำกัดทั้งด้านภาษาไทย ความเข้าใจในบริบทหรือวัฒนธรรมของประเทศไทย หรือบริบทของหน่วยงานซึ่งอาจก่อให้เกิดผลกระทบในเชิงลบต่อบุคคล องค์กร สังคมและประเทศชาติ เช่น

Template นโยบายการใช้เทคโนโลยี Generative AI ที่ยอมรับได้ (Acceptable Use Policy: Generative AI)

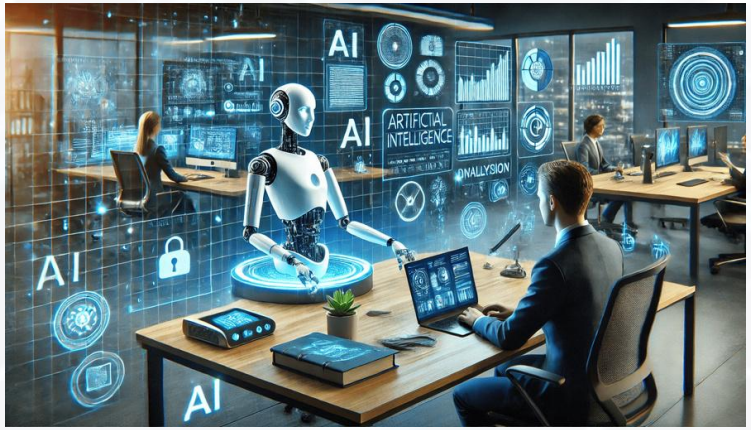
PDF

MS Word

นโยบายการใช้งานเทคโนโลยี GENERATIVE AI ที่ยอมรับได้
(ACCEPTABLE USE POLICY: GENERATIVE AI)

หลักการสำคัญสำหรับแนวทางการใช้ Generative AI ภายในสำนักงาน

- **ศึกษาและเข้าใจ**: ทำความเข้าใจ Generative AI (ประเภท, ศักยภาพ, ข้อจำกัด) ก่อนใช้งาน
- **ประยุกต์ใช้เหมาะสม**: ใช้ Generative AI สนับสนุนงานตามภารกิจของสำนักงาน



- **มีธรรมาภิบาล**: ใช้งานอย่างโปร่งใส, มีความรับผิดชอบ, และคำนึงถึงความมั่นคงปลอดภัย
- **ปฏิบัติตามกฎ**: สอดคล้องตามกฎหมาย, ข้อบังคับ, ระเบียบ, ประกาศ, และคำสั่งที่เกี่ยวข้องทั้งหมด

ข้อห้ามในการใช้ Generative AI: เพื่อความปลอดภัยและรับผิดชอบ

- ห้ามใช้แทนการตัดสินใจ ในเรื่องเสี่ยงสูง (กฎหมาย, การแพทย์, การเงิน, ผลกระทบต่อชีวิต/ทรัพย์สิน/สิทธิ)
- ห้ามสร้างข้อมูลเท็จ/เนื้อหาเสียหาย ที่นำไปสู่ความเข้าใจผิด/ขัดแย้ง
- ห้ามใช้/เปิดเผยข้อมูลลับ ของสำนักงาน
- ห้ามใช้ข้อมูลส่วนบุคคล โดยไม่ได้รับอนุญาต/ผิดกฎหมาย PDPA
- ห้ามใช้ในทางขัดต่อธรรมาภิบาล/จริยธรรม หรือมีเจตนาไม่สุจริต
- ห้ามละเมิดลิขสิทธิ์/ทรัพย์สินทางปัญญา
- ห้ามสร้างเนื้อหาส่งเสริมการเหยียด (เชื้อชาติ, ศาสนา, เพศ, etc.)
- ห้ามใช้ในการกระทำผิดกฎหมาย

นโยบายการใช้งานเทคโนโลยี GENERATIVE AI ที่ยอมรับได้
(ACCEPTABLE USE POLICY: GENERATIVE AI)

Generative AI: ใช้ปลอดภัย มั่นใจ ไร้กังวล

- **ห้ามเปิดเผยข้อมูลอ่อนไหว**: ห้ามนำข้อมูลที่อาจเป็นอันตรายต่อระบบ (รหัสผ่าน, API Key, การตั้งค่าระบบ) ไปใช้กับ Gen AI
- **ตรวจสอบ Source Code**: ตรวจสอบ Source Code ที่ Gen AI สร้างขึ้นอย่างละเอียด (ความถูกต้อง, ช่องโหว่) ก่อนใช้งาน
- **รายงานเหตุละเมิด**: เมื่อพบเหตุการณ์ผิดปกติ/ละเมิดความปลอดภัยที่เกี่ยวกับ Gen AI ให้รายงานผู้บังคับบัญชาทันที และทำตามขั้นตอน (Work Procedure)
- **รักษาความปลอดภัย**: ดำเนินการทุกอย่างให้มั่นคงปลอดภัย (Cybersecurity, ระบบ, ข้อมูล, ด้านอื่นๆ) เมื่อใช้ Gen AI
- **ตรวจสอบต่อเนื่อง**: ตรวจสอบการใช้ Generative AI อย่างสม่ำเสมอ

Generative AI: หน้าที่, ความรับผิดชอบ, และทรัพย์สินทางปัญญา

หน้าที่ & ความรับผิดชอบ:

- **แจ้งผู้บังคับบัญชา**: แจ้งวัตถุประสงค์, ขอบเขต, ลักษณะการทำงานร่วมกับ Gen AI (AI-Human Involvement)
- **ปฏิบัติตามนโยบาย & ตรวจสอบ**: ทำตามนโยบาย, ตรวจสอบเนื้อหาที่ Gen AI สร้างขึ้น (ความถูกต้อง, กฎหมาย, ความเท่าเทียม, ความลับ, ความเสี่ยง)
- **รายงานปัญหา**: รายงานความผิดพลาด/ผลกระทบเชิงลบจาก Gen AI ทันที
- **ติดตาม & ประเมิน**: ผู้บังคับบัญชา/ผู้ใช้ ติดตาม, ทบทวน, ประเมินประสิทธิภาพ Gen AI ต่อเนื่อง
- **ระบุแหล่งที่มา**: ระบุว่า "เนื้อหานี้ได้รับความช่วยเหลือจากเทคโนโลยี Generative AI" เพื่อความโปร่งใส
- **(หน่วยงาน IT) กำหนดแอป**: พิจารณา/นำเสนอ แอป/บริการ Gen AI ที่เหมาะสม

ทรัพย์สินทางปัญญา:

- **ใช้แอปที่กำหนด**: ใช้เฉพาะแอป/บริการ Gen AI ที่สำนักงานกำหนด
- **ไม่ละเมิด**: ระวังไม่ให้เนื้อหาที่ Gen AI สร้างขึ้นละเมิดลิขสิทธิ์/ทรัพย์สินทางปัญญา (ตรวจสอบก่อนใช้งาน/เผยแพร่)

การออกแบบ Playbook ใหม่ในองค์กร

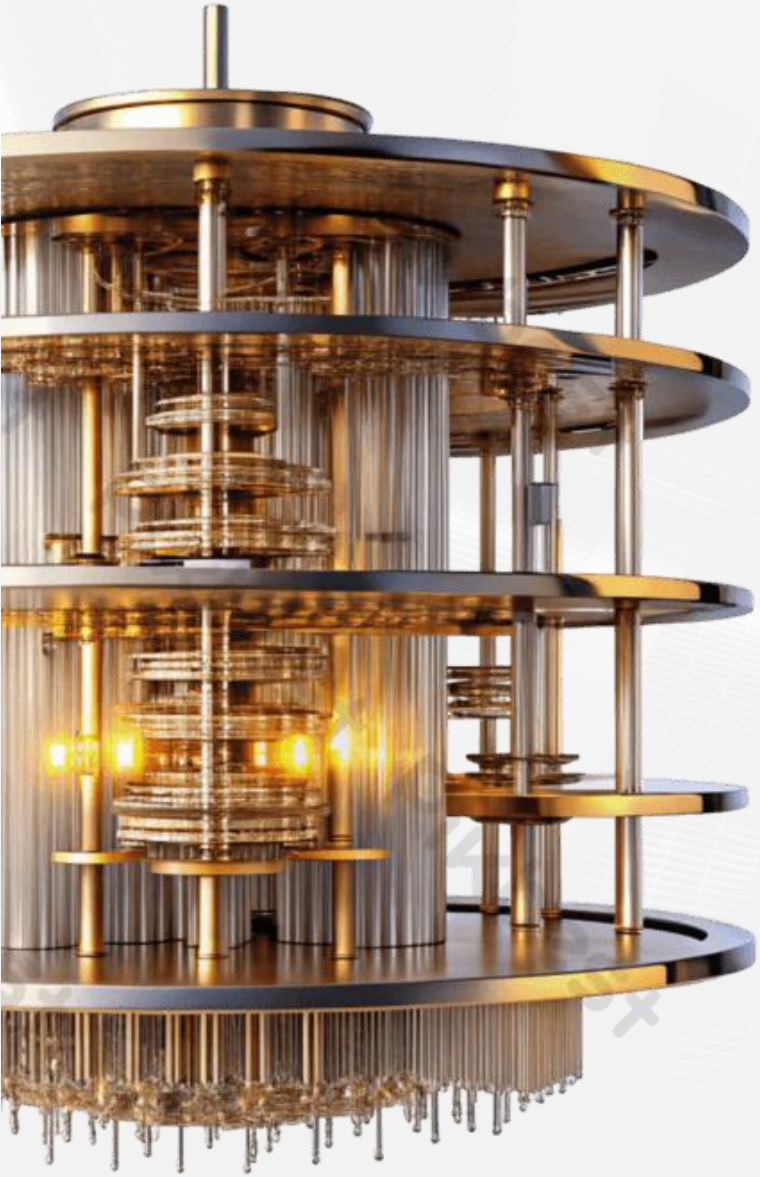
การเปลี่ยนแนวทาง: “Prevent-Detect-Respond” → “Predict-Adapt-Automate”

ความเปลี่ยนแปลง:

- **Prevent-Detect-Respond** คือโมเดลที่เน้นการตั้งรับหลังภัยคุกคามเริ่มขึ้น
- **Predict-Adapt-Automate** คือแนวทางใหม่ที่เน้น
  - **Predict**: ใช้ AI วิเคราะห์แนวโน้มภัยล่วงหน้า เช่น anomaly detection, predictive threat intelligence
  - **Adapt**: ปรับกฎและนโยบายตามพฤติกรรมใหม่ ๆ โดยอัตโนมัติ (เช่น dynamic access control)
  - **Automate**: ใช้ SOAR (Security Orchestration, Automation and Response) ตอบสนองเหตุการณ์โดยไม่ต้องใช้มนุษย์ทุกขั้นตอน

https://www.paloaltonetworks.com/cyberpedia/nist-ai-risk-management-framework

Quantum Computer



Quantum Computing คือเทคโนโลยีการประมวลผลข้อมูลที่ใช้หลักการของควอนตัมเมคานิกส์ (Quantum Mechanics) ซึ่งเป็นสาขาหนึ่งของฟิสิกส์ที่ศึกษาพฤติกรรมของอนุภาคขนาดเล็กมาก ๆ เช่น อะตอมและอิเล็กตรอน ควอนตัมคอมพิวติ้งมีความแตกต่างจากคอมพิวเตอร์แบบดั้งเดิมในหลายด้าน โดยเฉพาะในเรื่องของการประมวลผลข้อมูล

หลักการสำคัญของ Quantum Computing:

1.Qubit (ควอนตัมบิต): ในขณะที่คอมพิวเตอร์แบบดั้งเดิมใช้บิต (bit) ในการประมวลผลข้อมูลซึ่งมีสถานะเป็น 0 หรือ 1 เท่านั้น ควอนตัมคอมพิวติ้งใช้ควอนตัมบิต หรือ qubit ที่สามารถอยู่ในสถานะของ 0, 1 หรือทั้งสองพร้อมกันในเวลาเดียวกัน เรียกว่า Superposition (ภาวะซ้อนทับ)

2.Entanglement (การพัวพัน): เป็นปรากฏการณ์ที่ qubits หลายตัวสามารถเชื่อมโยงกันได้แบบที่การเปลี่ยนแปลงของ qubit หนึ่งจะส่งผลต่ออีก qubit แม้ว่าจะอยู่ไกลกันมากก็ตาม ซึ่งเป็นสิ่งที่ทำให้ควอนตัมคอมพิวเตอร์สามารถประมวลผลข้อมูลได้รวดเร็วและมีประสิทธิภาพมากกว่าคอมพิวเตอร์แบบดั้งเดิม

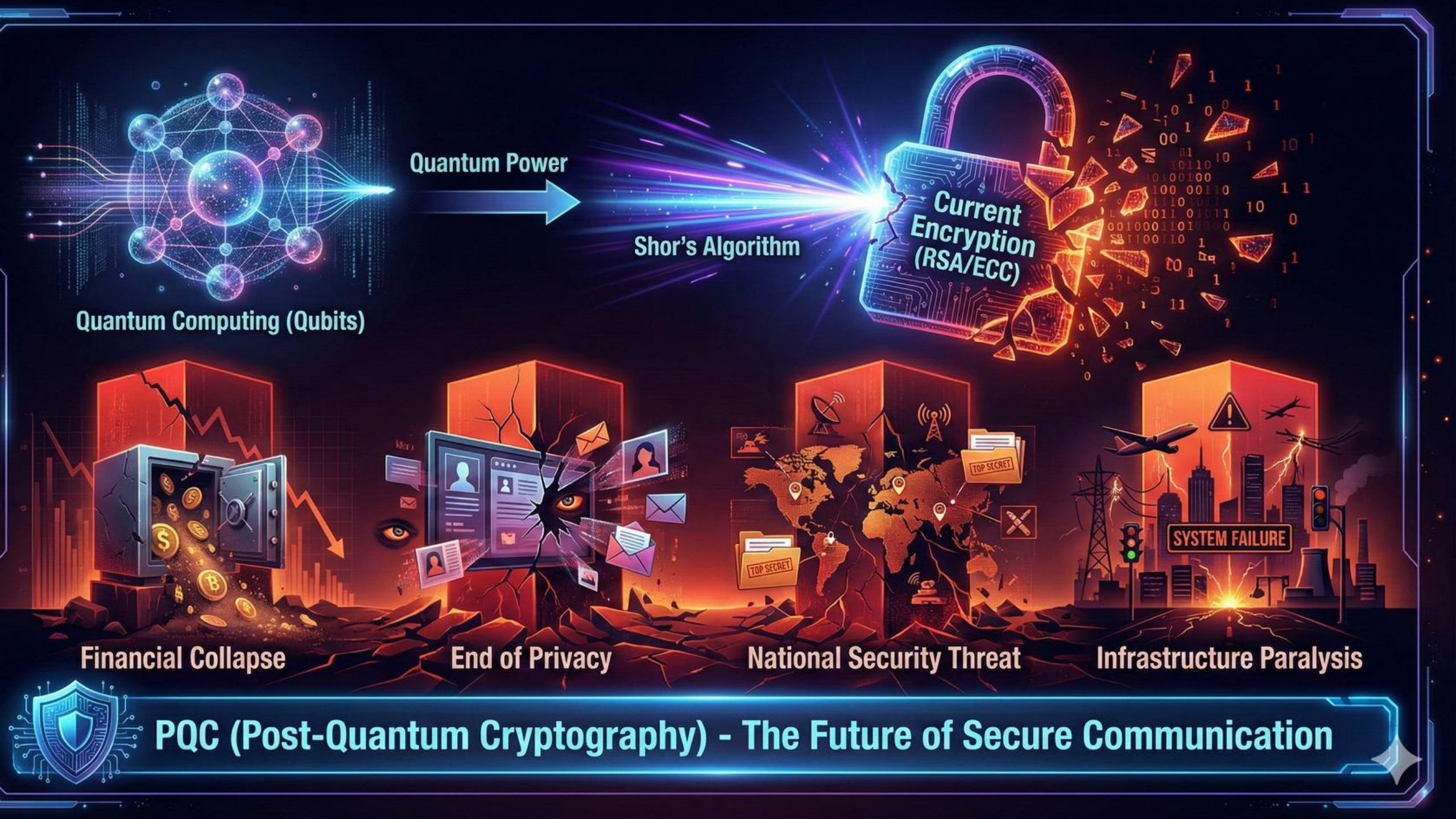
3.Quantum Superposition (ภาวะซ้อนทับ): Qubits สามารถอยู่ในหลายสถานะได้พร้อม ๆ กัน ทำให้สามารถทำการคำนวณได้หลายอย่างในเวลาเดียวกัน ซึ่งต่างจากบิตในคอมพิวเตอร์ทั่วไปที่ต้องทำการคำนวณทีละขั้นตอน

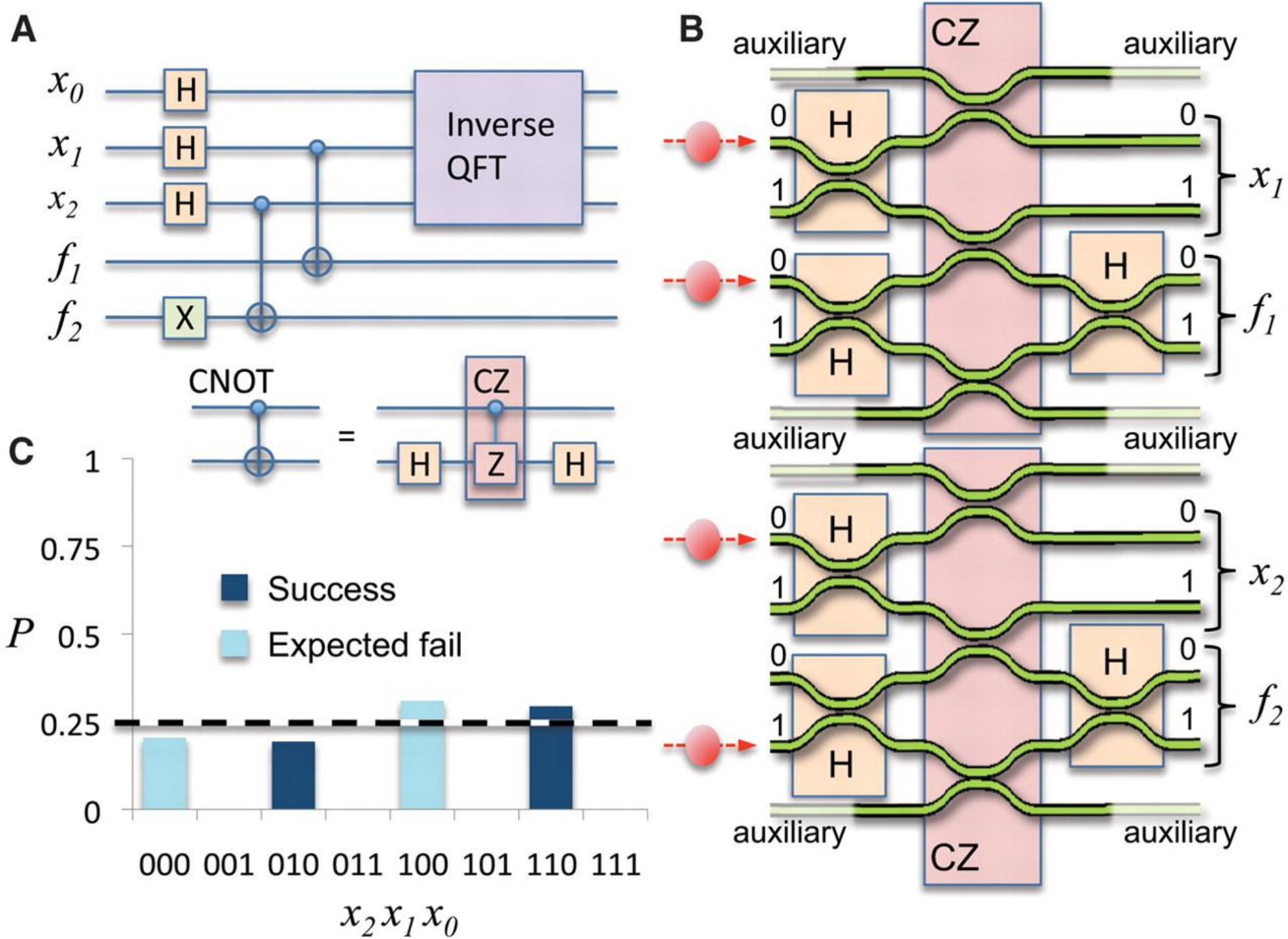
4.Quantum Interference (การแทรกสอดควอนตัม): เป็นเทคนิคที่ใช้ในการเพิ่มโอกาสของผลลัพธ์ที่ถูกต้องโดยการแทรกสอดสถานะควอนตัม

การทำงานของ Quantum Computing:

Quantum Computing มีศักยภาพในการแก้ปัญหาที่ซับซ้อนมาก ๆ เช่น การเข้ารหัสข้อมูล (Cryptography), การค้นหาข้อมูลในฐานข้อมูลขนาดใหญ่, การจำลองโมเลกุลในเคมี และการปรับปรุงประสิทธิภาพของ Machine Learning เป็นต้น

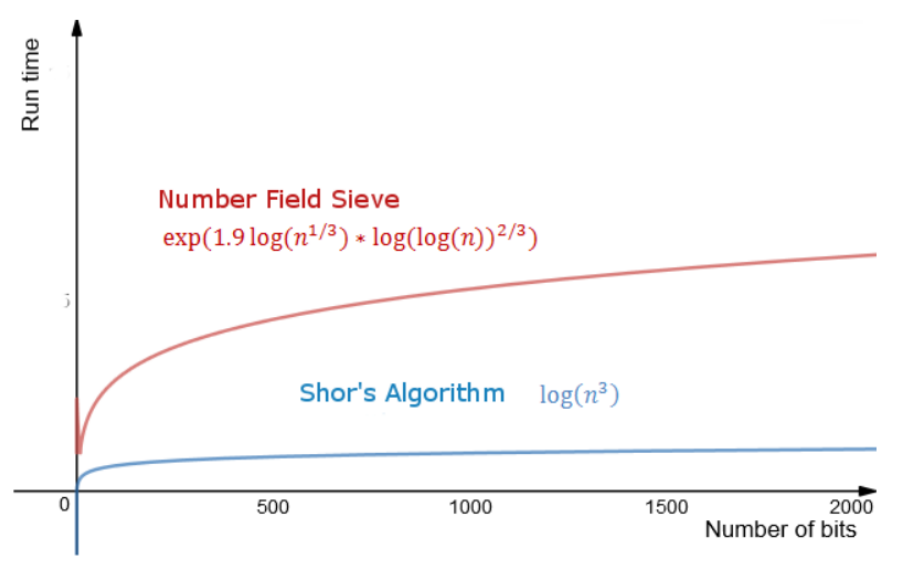
https://www.ibm.com/think/topics/quantum-computing


Quantum Computing (Qubits)
Quantum Power
Shor's Algorithm
Current Encryption (RSA/ECC)
TOP SECRET
TOP SECRET
SYSTEM FAILURE
Financial Collapse
End of Privacy
National Security Threat
Infrastructure Paralysis
PQC (Post-Quantum Cryptography) - The Future of Secure Communication


A
x_0
x_1
x_2
f_1
f_2
H
H
H
X
Inverse QFT
CNOT
=
CZ
H
Z
H
B
auxiliary
CZ
auxiliary
0
1
H
H
H
x_1
f_1
x_2
f_2
auxiliary
CZ
C
1
0.75
0.5
0.25
0
P
Success
Expected fail
000 001 010 011 100 101 110 111
$x_2 x_1 x_0$

Breaking RSA with Quantum Computer

Integer factorization with Shor's algorithm



4,000 – 8,000 logical qubits are needed to break RSA-2048

(Gidney and Ekerå, 2021)

China cracks another quantum code barrier. For how much longer is our data safe?

By setting a new benchmark in quantum cryptology, Chinese researchers may have found new path for encryption research

Reading Time: **4 minutes** Why you can trust SCMP

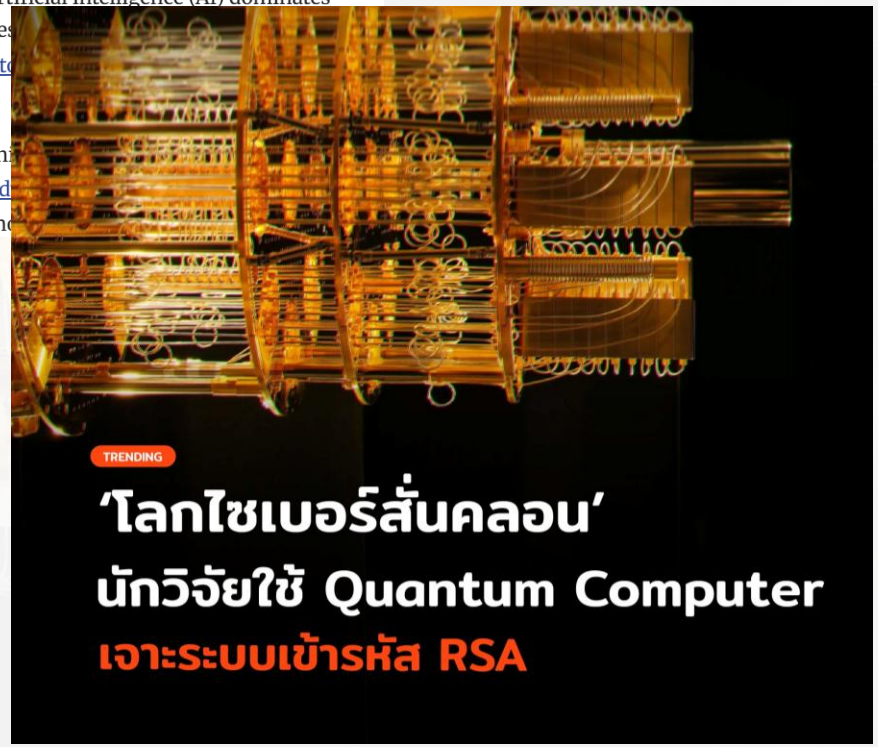
Zhang Tong in Beijing

Published: 8:08pm, 22 Apr 2025 | Updated: 3:59pm, 24 Apr 2025

While the battle for high ground in artificial intelligence (AI) dominates global headlines, a team of Chinese res
advance in the field of quantum crypto
could be even higher.

Professor Wang Chao, of Shanghai Uni
90-bit RSA integer using a D-Wave Ad
achievement that not long ago was th

<u>90-bit</u> RSA integer was broken in April 2025.



https://www.scmp.com/news/china/science/article/3307487/china-cracks-another-quantum-code-barrier-how-much-longer-our-data-safe

CSA sets a countdown clock to Q-day (April 14, 2030)

https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/

ข้อมูลวันที่ 7 พฤษภาคม พ.ศ. 2569

แนวปฏิบัติขั้นตอนการเตรียมความพร้อม

1. จัดทำแผนงาน (Roadmap):

กำหนดบุคลากรเพื่อจัดทำแผนงาน (Roadmap) เตรียมความพร้อมรับมือภัยคุกคามจากคอมพิวเตอร์ควอนตัมตั้งแต่เนิ่นๆ เพื่อให้การเปลี่ยนแปลงเป็นไปอย่างราบรื่นและประเมินค่าใช้จ่ายในการลงทุนได้

2. เสริมสร้างความตระหนักรู้:

ศึกษาและสร้างความรู้ความเข้าใจเกี่ยวกับภัยคุกคามจากคอมพิวเตอร์ควอนตัมให้แก่พนักงานในทุกฝ่าย เพื่อให้สามารถเลือกใช้ซอฟต์แวร์หรือฮาร์ดแวร์ที่มีความปลอดภัยต่อการโจมตีจากควอนตัมได้

3. กำหนดหน้าที่ความรับผิดชอบ:

มอบหมายหน้าที่และความรับผิดชอบให้แก่บุคลากรที่เกี่ยวข้องในแต่ละส่วนงาน เพื่อให้มีความรู้ความเข้าใจเกี่ยวกับเทคโนโลยีระบบรหัสลับที่องค์กรเลือกใช้

4. จัดทำรายการสินทรัพย์ทางสารสนเทศ:

จัดทำรายการสินทรัพย์ไอที (IT asset inventory) ทั้งซอฟต์แวร์และฮาร์ดแวร์ที่เกี่ยวข้องกับระบบรหัสลับ เพื่อทำความเข้าใจวิธีการสร้าง จัดเก็บ และใช้งานกุญแจเข้ารหัสลับในปัจจุบัน

5. ประเมินเทคโนโลยีทางเลือก:

ประเมินและเปรียบเทียบข้อดีข้อเสียของเทคโนโลยี PQC (Post-Quantum Cryptography) หรือ QKD (Quantum Key Distribution) เพื่อเลือกใช้ให้เหมาะสมกับระบบสารสนเทศขององค์กร หรืออาจใช้ระบบความปลอดภัยแบบผสมผสาน (Hybrid Security Approach)

6. ทำการทดลองและทดสอบ:

เริ่มทดลองและทดสอบระบบและเทคโนโลยีที่เกี่ยวข้องได้เลย แม้ว่ามาตรฐานจะยังไม่สมบูรณ์ เพื่อเตรียมความพร้อมสำหรับการเปลี่ยนแปลงในอนาคต และทำความเข้าใจปัญหาที่อาจเกิดขึ้น

7. ติดตามความก้าวหน้าอย่างต่อเนื่อง:

ติดตามความคืบหน้าของแผนงานอย่างต่อเนื่อง พร้อมทั้งประเมินความเสี่ยงและระยะเวลาที่อาจเกิดภัยคุกคามใหม่อยู่เป็นระยะ

https://drive.ncsa.or.th/s/52GYxAqMfDNZjEZ

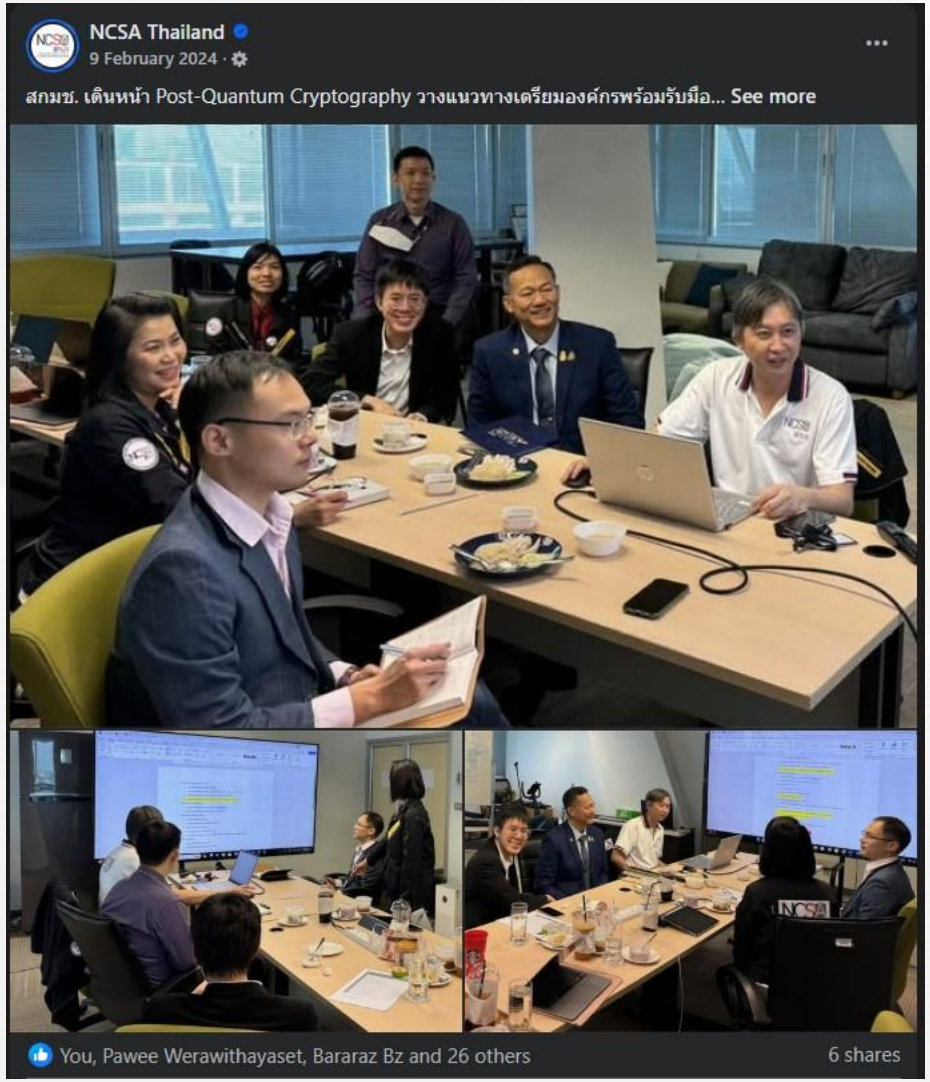
เข้าร่วมการเตรียมความพร้อมระบบสารสนเทศของหน่วยงาน เพื่อเข้าสู่ยุคควอนตัม (PQC)

https://dg.th/8x6heca1f4

สิ่งที่ท่านจะได้รับ

- เห็นตัวอย่างการดำเนินการจริง ตั้งแต่การสำรวจสินทรัพย์ระบบรหัสลับ การจัดลำดับความสำคัญ และการวางแผนการเปลี่ยนผ่าน
- มีแนวทางในการจัดทำแผนการเปลี่ยนผ่านระบบสารสนเทศ
- สิทธิ์สำหรับการใช้ระบบติดตามการดำเนินการเปลี่ยนผ่านระบบสารสนเทศ
- สิทธิ์ในการเข้าใช้ศูนย์ข้อมูลและสาธิต PQC และรับคำแนะนำจากผู้เชี่ยวชาญ

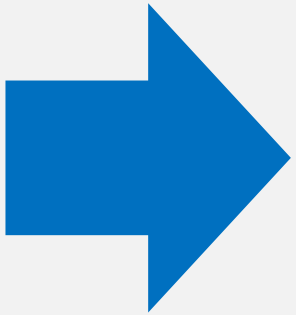
NCSA VS Quantum Computing



สิ่งที่ต้องดำเนินการเร่งด่วน: SSL Certificate Renewal Process

Certificate issued on or after	Certificate issued before	Maximum Validity Period
	March 15, 2026	398 days
March 15, 2026	March 15, 2027	200 days
March 15, 2027	March 15, 2029	100 days
March 15, 2029		47 days

ปัจจุบันต่ออายุ Certificate ทุก 200 วัน



47

เริ่มมีนาคม 2029

ทุกองค์กรต้องทำให้การต่ออายุ Certificate เป็นอัตโนมัติ

https://cabforum.org/working-groups/server/baseline-requirements/documents/CA-Browser-Forum-TLS-BR-2.2.5.pdf

จากการวิเคราะห์สาเหตุกรณีหน่วยงานรัฐและเอกชนในประเทศไทยถูกโจมตีของ ThaiCERT ในปี 2568

ระบบของภาครัฐและเอกชนจำนวนมากทั้งที่จ้างพัฒนาและพัฒนาเองมีความไม่ปลอดภัยและการเขียนโปรแกรมที่ไม่ปลอดภัย

การใช้ซอฟแวร์ที่มีช่องโหว่หรือล้าสมัย

การที่ผู้ดูแลระบบใช้ USERNAME และ PASSWORD เดิมที่ติดมากับอุปกรณ์หรือซอฟต์แวร์

ขาดระบบป้องกันและเฝ้าระวังการถูกโจมตี

การป้องกันการรั่วไหลของข้อมูลจากพนักงานภายใน (Insider Threat)

การใช้งานการเข้ารหัสที่ไม่ปลอดภัยหรือไม่มีการเข้ารหัส

หน่วยงานขาดบุคลากรที่มีความเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

การขาดบุคลากรด้านการคุ้มครองข้อมูลส่วนบุคคล (DPO)

การจัดการสิทธิ์ของพนักงานที่ออกจากงาน (Offboarding)

ขาดมาตรการกำกับดูแลและการป้องกันการเข้าถึงระบบจากบุคคลภายนอก

คำแนะนำในการป้องกันองค์กรของ สกมช. ในปี 2569

01


อัปเดตซอฟต์แวร์และระบบอยู่เสมอและ หลีกเลี่ยงการดาวน์โหลดและติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์ (Software Updates & Patching)

02

สำรองข้อมูลอย่างปลอดภัยและเป็นประจำ (Data Backup and Disaster Recovery)

03

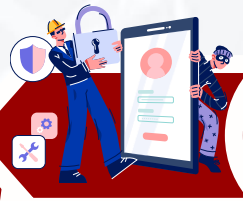
ยกระดับความปลอดภัยด้วยการยืนยันตัวตน 2 ขั้นตอน (2FA)

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

New IR Playbook

Parallel, adaptiveplaybooks

Include unknown / AI-generated attacks

Proactive attack surfacemanagement

Zero Trust & AssumeBreach mindset

Active crisiscommunication plan

Fusion teams (Legal, PR,Executive, OT, IT)


Q&A

Contact us

National Cyber Security Agency - NCSA

NCSA Thailand

Line ID : NCSA Thailand

E-Mail: saraban@ncsa.or.th

02-142-6885

4IoTus (สี่ แอล โอ ทีใหญ่ ยู เอส)