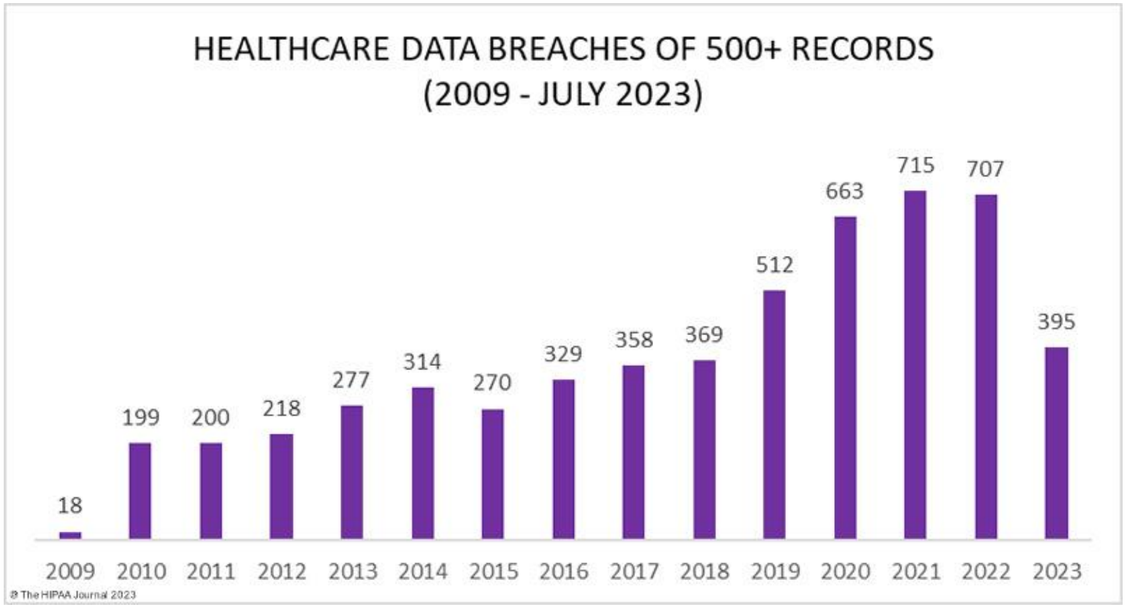
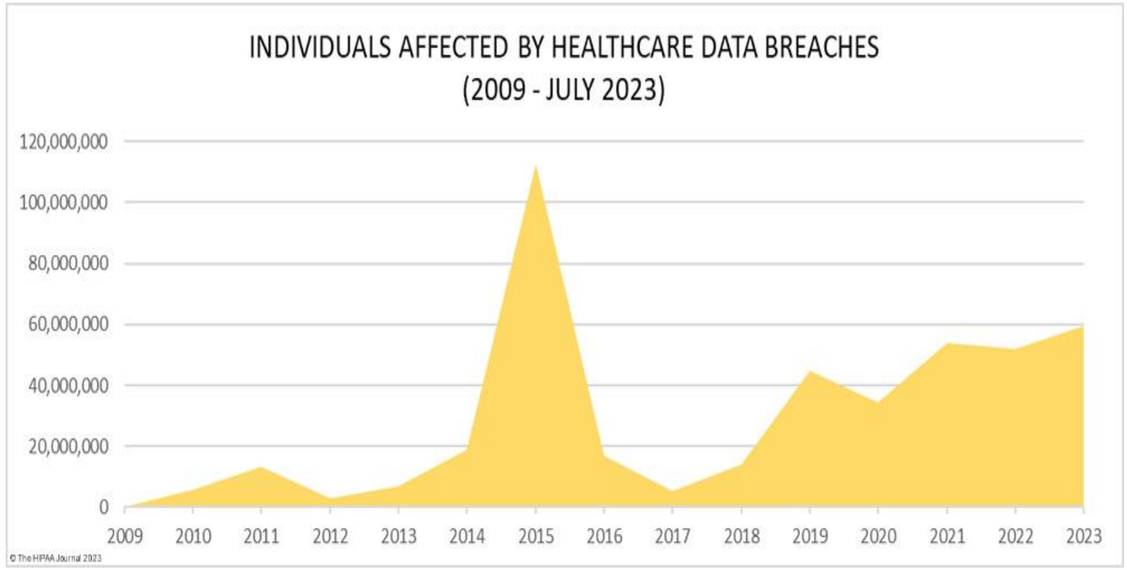
Restoring Trust and Data Privacy & Security after Massive Data Breach Incident

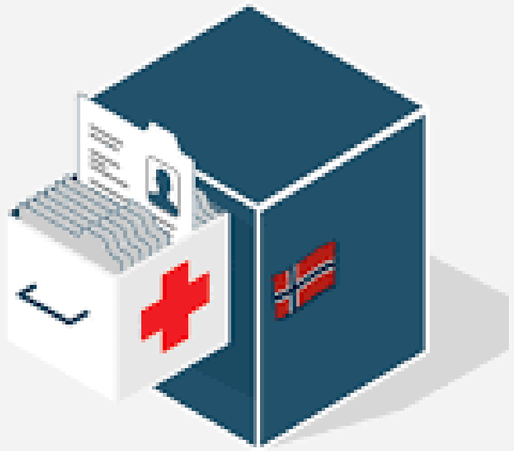




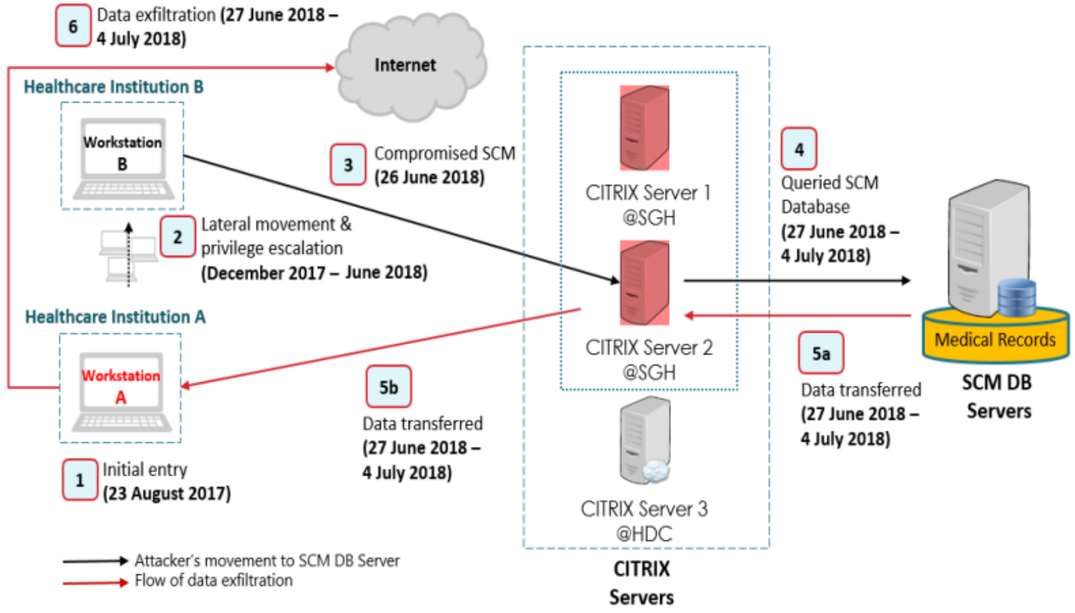
Rank	Name of Covered Entity	Year	Covered Entity Type	Individuals Affected	Type of Breach
1	**Anthem Inc.**	2015	**Health Plan**	78,800,000	**Hacking/IT Incident**
2	**American Medical Collection Agency**	2019	**Business Associate**	26,059,725	**Hacking/IT Incident**
3	**HCA Healthcare**	2023	**Business Associate**	11,270,000	**Hacking/IT Incident**
4	**Premera Blue Cross**	2015	**Health Plan**	11,000,000	**Hacking/IT Incident**
5	**Excellus Health Plan, Inc.**	2015	**Health Plan**	10,000,000	**Hacking/IT Incident**
6	**Managed Care of North America (MCNA Dental)**	2023	**Business Associate**	8,923,662	**Ransomware attack**
7	**PharMerica**	2023	**Healthcare Provider**	5,815,591	**Ransomware attack**
8	**Science Applications International Corporation**	2011	**Business Associate**	4,900,000	**Loss**
9	**University of California, Los Angeles Health**	2015	**Healthcare Provider**	4,500,000	**Hacking/IT Incident**
10	**Community Health Systems Professional Services Corporations**	2014	**Business Associate**	4,500,000	**Hacking/IT Incident**

SingHealth

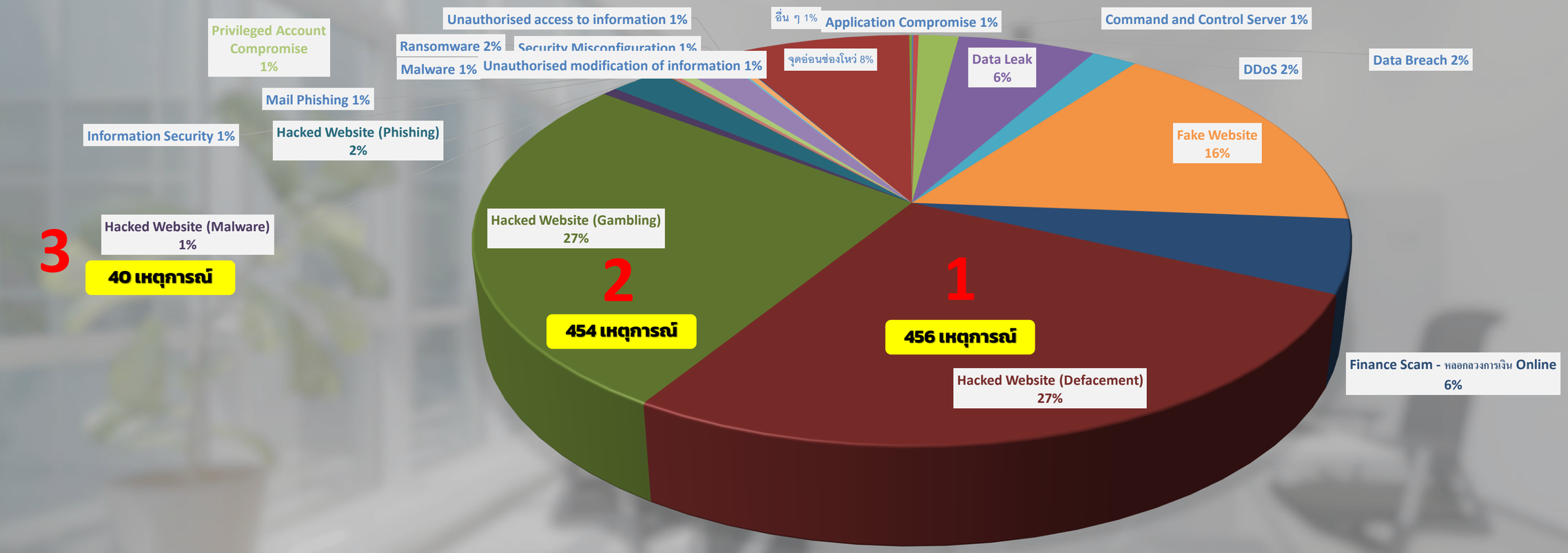
Healthcare Data Breach



SinHealth Data Breach 2018



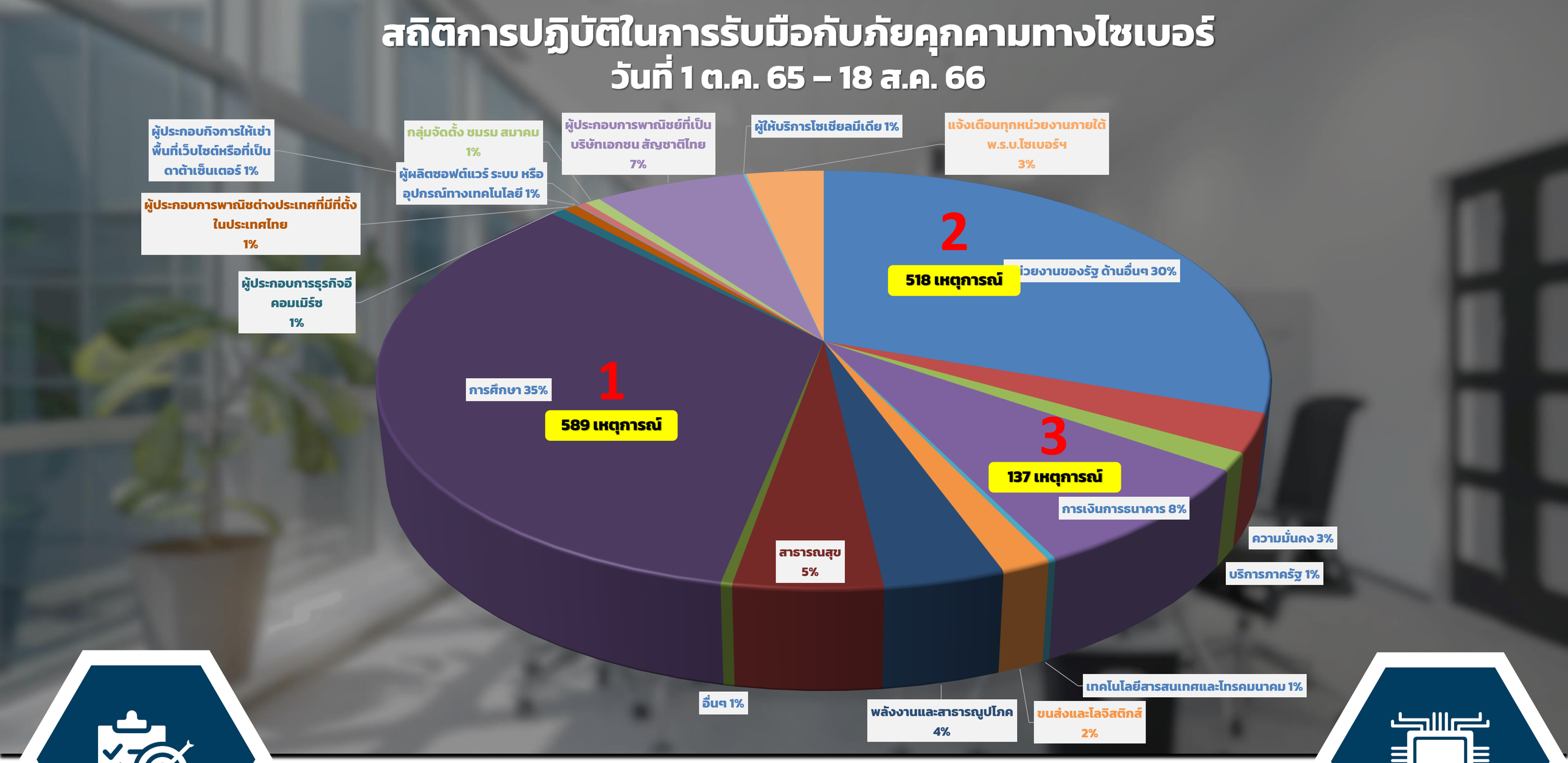
สถิติการปฏิบัติในการรับมือกับภัยคุกคามทางไซเบอร์
วันที่ 1 ต.ค. 65 – 18 ส.ค. 66



รวมทั้งสิ้น 1,703 เหตุการณ์

➢ Hacked Website (Phishing, Defacement, Gambling)	961 เหตุการณ์
➢ Fake Website	275 เหตุการณ์
➢ จุดอ่อนช่องโหว่	137 เหตุการณ์
➢ Data Leak	103 เหตุการณ์
➢ Finance Scam - หลอกลวงการเงิน Online	98 เหตุการณ์
➢ DDoS	34 เหตุการณ์
➢ Ransomware	34 เหตุการณ์
➢ Data Breach	30 เหตุการณ์
➢ อื่น ๆ	31 เหตุการณ์

สถิติการปฏิบัติในการรับมือกับภัยคุกคามทางไซเบอร์
วันที่ 1 ต.ค. 65 – 18 ส.ค. 66



รพ.เพชรบูรณ์ ขอโทษ ปมโดนแฮกข้อมูลคนไข้ชี้เป็นข้อมูลทั่วไป ไม่มีผลต่อการรักษา

5 กันยายน 2564 มีการประกาศขายข้อมูลคนไข้โรงพยาบาลเพชรบูรณ์ทางอินเทอร์เน็ต **ขนาดข้อมูล 3.75 กิกะไบต์ จำนวน 16 ล้านเรคคอร์ด จาก 146 ฐานข้อมูล ในราคา 500$** ทางโรงพยาบาลฯ จึงรีบดำเนินการตรวจสอบโดยเร่งด่วน มีการจัดตั้งคณะกรรมการแก้ไขปัญหาภาวะคุกคามทางไซเบอร์ เพื่อตรวจสอบข้อเท็จจริงและประเมินความเสียหายที่เกิดขึ้น ข้อมูลที่มีการเผยแพร่ในอินเทอร์เน็ตแสดงข้อมูลทั่วไปของประชาชนที่มารับบริการและเจ้าหน้าที่บางส่วน ในขั้นต้นมีการปิดกั้นการเข้าถึงอินเทอร์เน็ตจากภายนอก ตรวจสอบความเสียหายระบบภายในโรงพยาบาล มีการตรวจสอบความปลอดภัยด้านไซเบอร์ ตรวจสอบระบบที่ข้อมูลรั่วไม่ให้มีการแฮกข้อมูลอยู่ในระบบ ผลการตรวจสอบไม่พบความเสียหายกับระบบปฏิบัติการที่ใช้ในการดูแลรักษาผู้ป่วย และจากการตรวจสอบขั้นต้นข้อมูลที่ประกาศขายเป็น**ข้อมูลเกี่ยวกับรายชื่อประชาชนที่มารับบริการโรงพยาบาลชื่อแพทย์ที่ดูแล และตารางเวรแพทย์ ข้อมูลสัญญาณชีพวันเวลาที่มารับบริการสิทธิการรักษา เลขประจำตัวผู้ป่วย ไม่ใช่ฐานข้อมูลการรักษา ไม่มีรายละเอียดเกี่ยวกับการวินิจฉัยและรักษาโรค** เป็นข้อมูลทั่วไปที่ไม่มีผลกระทบต่อการดูแลรักษา

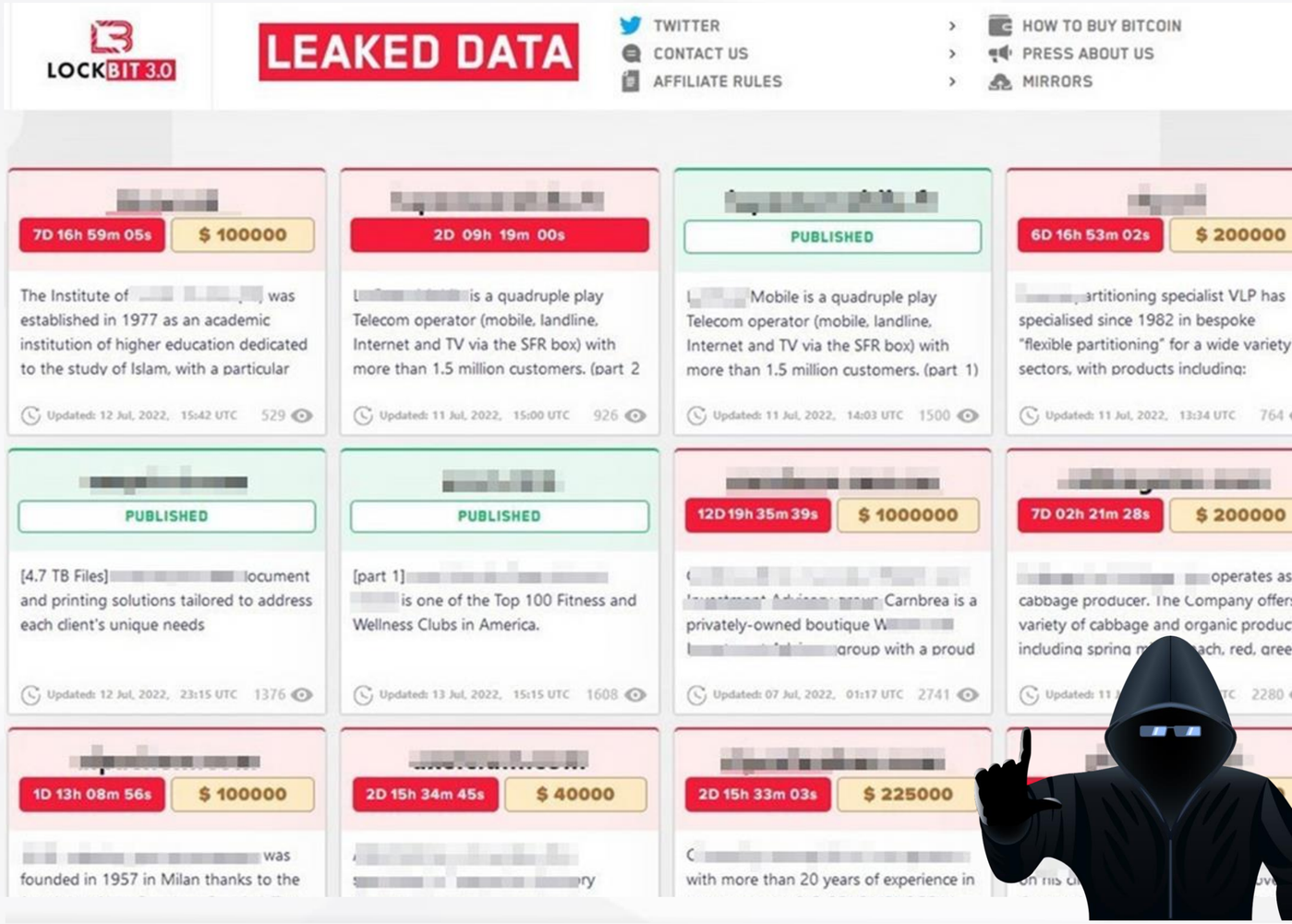
ยอดค่าไถ่หรือความเสียหายโดยประมาณ บน LOCKBIT 2.0 และ 3.0

ในปี 2022 จาก 14 หน่วยงาน

ประมาณ 619,000,000 บาท

ในปี 2023 จาก 6 หน่วยงาน

ประมาณ 181,000,000 บาท



ความเสียหายจากLOCKBIT 2.0 และ 3.0

รวม 800,000,000 บาท

สรุปหน้าที่ของหน่วยงานที่เกี่ยวข้องตาม พ.ร.บ.ไซเบอร์ 62

หน่วยงาน Regulator

กำกับดูแล
13(5) กำหนดมาตรฐานที่เหมาะสม
9(8), 49 กำหนดเกณฑ์รอง, รายงาน
53 ตรวจสอบมาตรฐานขั้นต่ำ
54 ตรวจสอบความมั่นคงปลอดภัย

ป้องกัน
43 ดำเนินการตามนโยบายและแผน
44–45 ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน
46 แจ้งรายชื่อบริหารและปฏิบัติการไปยัง สกมช.
52 รับแจ้งรายชื่อและข้อมูลติดต่อจาก CII

รับมือ
57–58 รับแจ้งเหตุภัยคุกคามทางไซเบอร์
59 ร่วมกับ Sectoral CERT รวบรวมข้อมูล ตรวจสอบ ... ช่วยเหลือ CII

Sectoral CERT

รับมือ
50 ลักษณะ หน้าที่และความรับผิดชอบของ Sectoral CERT
52 รับแจ้งรายชื่อและข้อมูลติดต่อฯ จาก CII
59 ร่วมกับ Reg รวบรวมข้อมูล ตรวจสอบ ... ช่วยเหลือ CII

หน่วยงาน CII

ป้องกัน
43 ดำเนินการตามนโยบายและแผน
44–45 ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน
46 แจ้งรายชื่อบริหารและปฏิบัติการไปยัง สกมช.
54 ประเมินความเสี่ยง และตรวจสอบ

(ต่อ)
52 แจ้งรายชื่อและข้อมูลติดต่อเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ดูแลระบบ ไปยัง สกมช., Reg, Sectoral CERT

รับมือ
56 กลไกหรือขั้นตอนเพื่อการเฝ้าระวัง
57 รายงานเหตุต่อ สกมช. และ Reg
58 ป้องกัน รับมือ ลดความเสี่ยง

ประมวลแนวทางปฏิบัติ การรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา 44 ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง อย่างน้อยต้องประกอบด้วยเรื่อง ดังต่อไปนี้
(1) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือ ผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง
(2) แผนการรับมือภัยคุกคามทางไซเบอร์

1

แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

2

การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

3

แผนการรับมือภัยคุกคามทางไซเบอร์

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา ๑๓ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) มีหน้าที่และอำนาจ ดังต่อไปนี้
(๔) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

ในการกำหนด**กรอบมาตรฐาน**ตามวรรคหนึ่ง (๔) ให้คำนึงถึง**หลักการบริหารความเสี่ยง** โดยอย่างน้อยต้องประกอบด้วย**วิธีการและมาตรการ** ดังต่อไปนี้

(๑) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

(๒) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

(๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

(๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

(๕) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

NIST Cybersecurity Framework

Source: "NIST Framework for improving critical infrastructure cybersecurity", www.nist.gov/

Functions
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

Cybersecurity Framework (CSF) Core Functions:

Identify—Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities.

Protect—Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

Detect—Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Respond—Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Recover—Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Raising Awareness

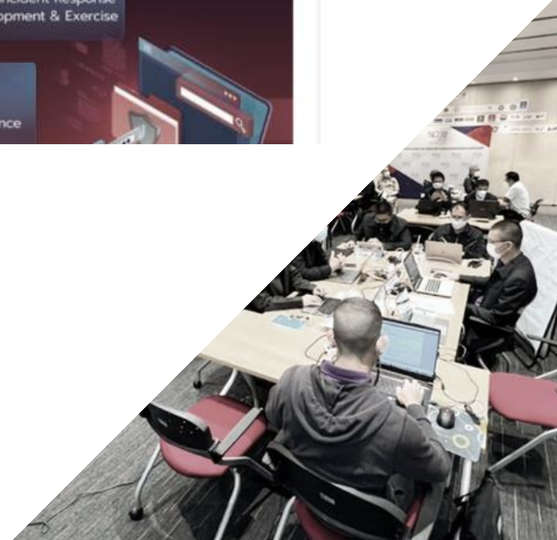
สกมช. พัฒนาบุคลากรของหน่วยงานระบบโครงสร้างพื้นฐานสำคัญ เพื่อรับมือ Ransomware ! คัดคนระดับหัวกะทิ ร่วมกิจกรรม Capacity Building และ CERT CII Cyber Training ฝึกการตอบสนอง รับมือภัยคุกคามจากทีมผู้เชี่ยวชาญ จาก บริษัท Retrospect Labs ประเทศออสเตรเลีย

News • ctf.in.th • วันศุกร์ 10 มิถุนายน 2565 • comments off

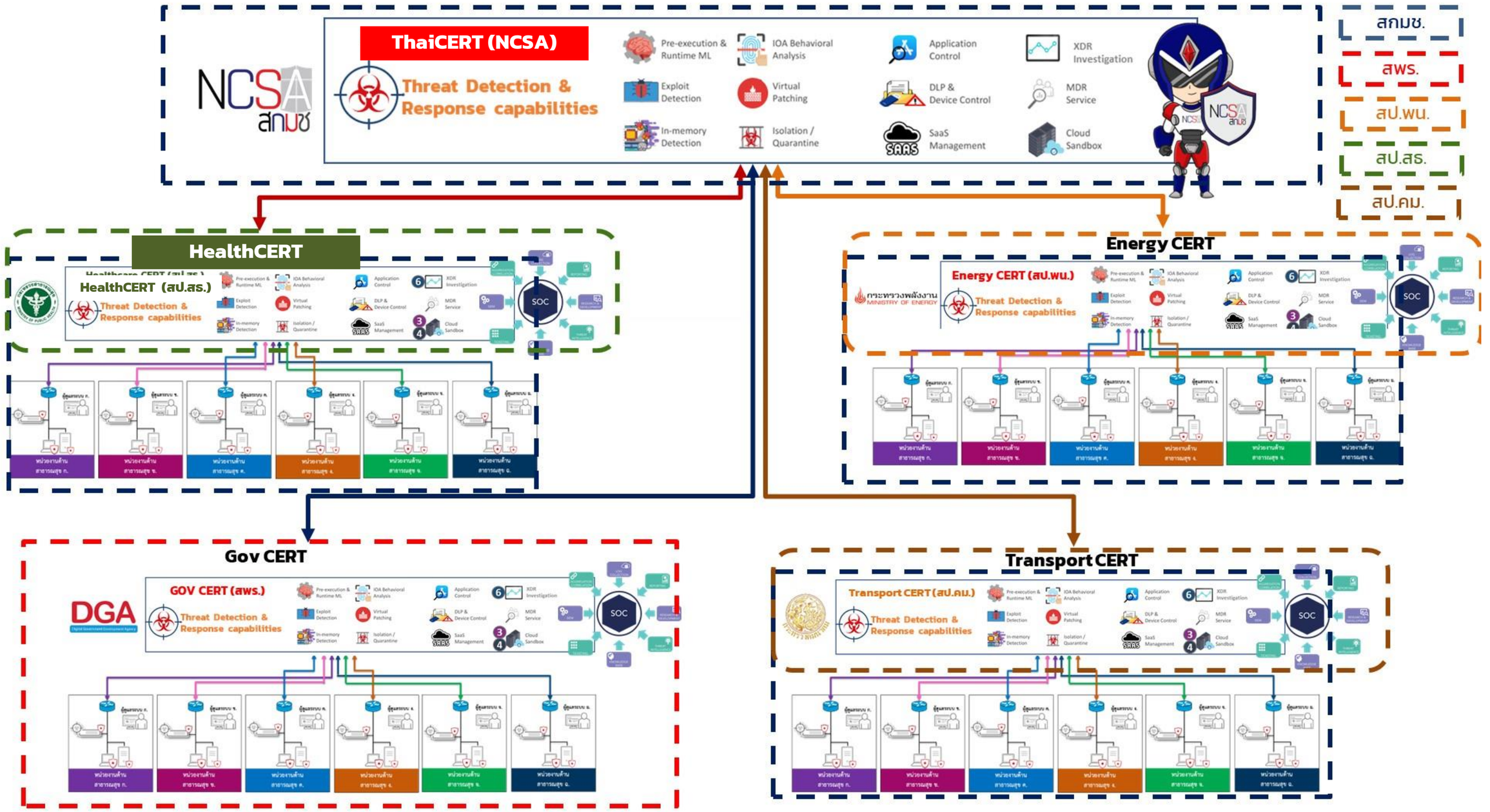
Reskill and Upskill

กิจกรรม Capacity Building NCSA และ CERT CII Cyber Training ของ สกมช.

Course • ctf.in.th • วันพุธ 1 มิถุนายน 2565 • comments off



ระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ Sectoral CERT ระดับชาติ เชื่อมโยงข้อมูลกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ



ThaiCERT
Thailand Computer Emergency Response Team
By NCSA Thailand

National CERT (NCSA)

Threat Detection & Response capabilities

- Pre-execution & Runtime ML
- IOA Behavioral Analysis
- Application Control
- XDR Investigation
- Exploit Detection
- Virtual Patching
- DLP & Device Control
- MDR Service
- In-memory Detection
- Isolation / Quarantine
- SaaS Management
- Cloud Sandbox

Healthcare CERT (สป.สธ.)

Threat Detection & Response capabilities

- Pre-execution & Runtime ML
- IOA Behavioral Analysis
- Application Control
- XDR Investigation
- Exploit Detection
- Virtual Patching
- DLP & Device Control
- MDR Service
- In-memory Detection
- Isolation / Quarantine
- SaaS Management
- Cloud Sandbox

NCSA สกมช

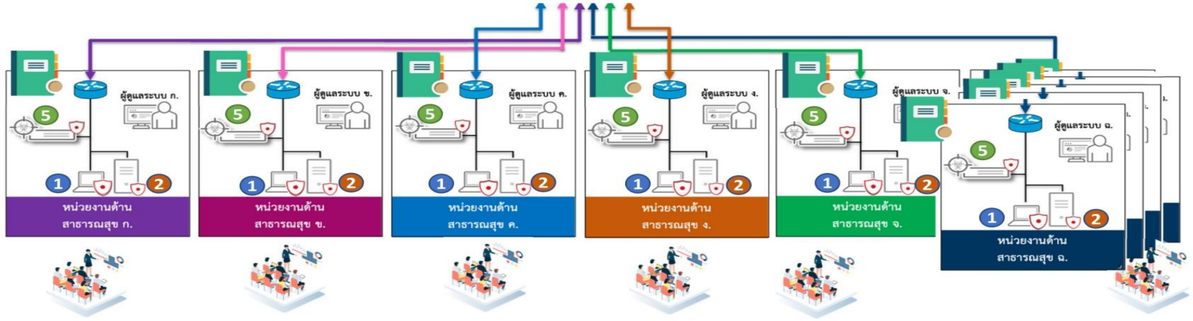
AIT 30 YEARS OF TRUST

TECH PIXEL

10 โรงพยาบาล

7. SOC as a Service

8. DFIR Team



5 โรงพยาบาล