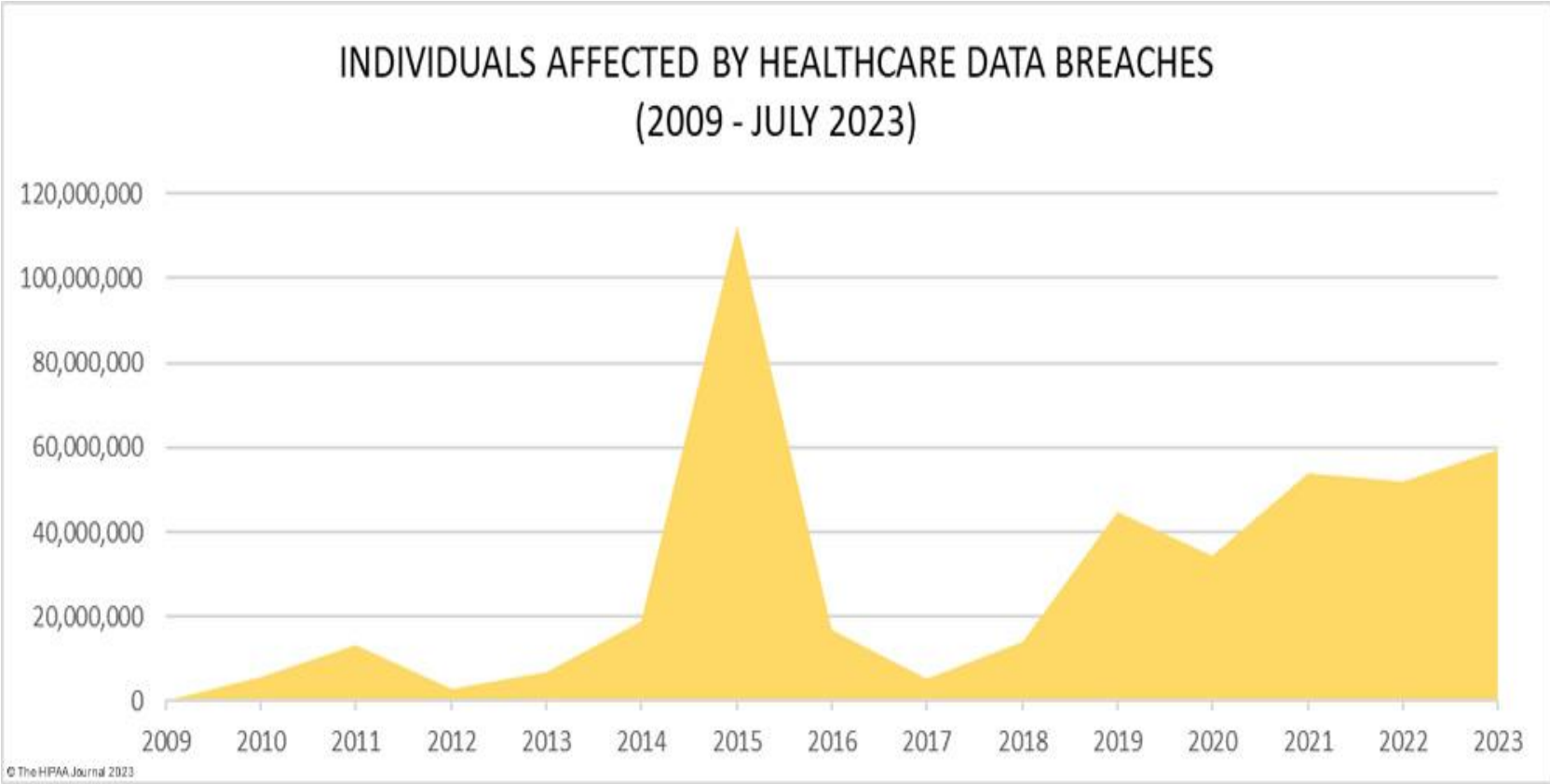
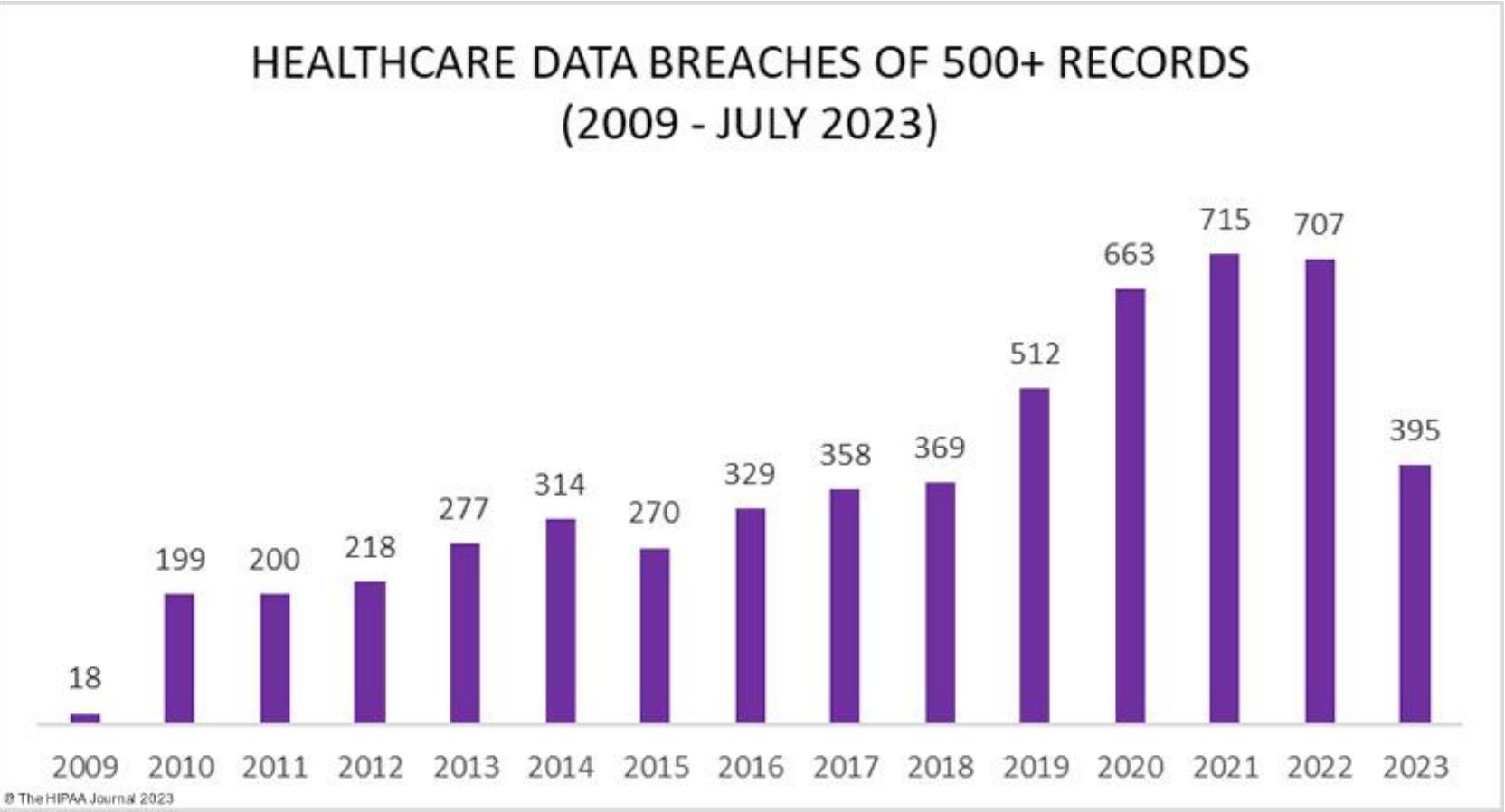


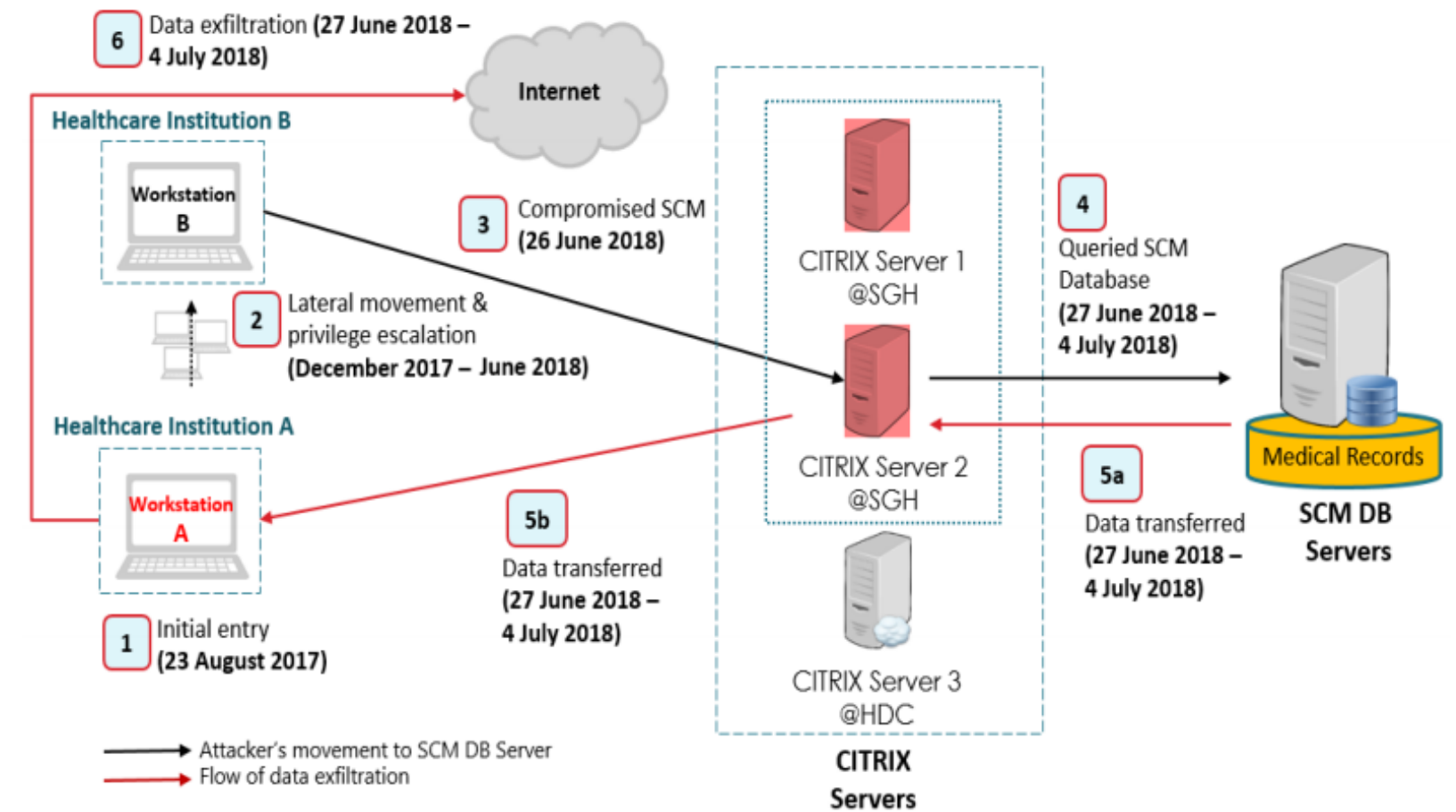
Restoring Trust and Data Privacy & Security after Massive Data Breach Incident



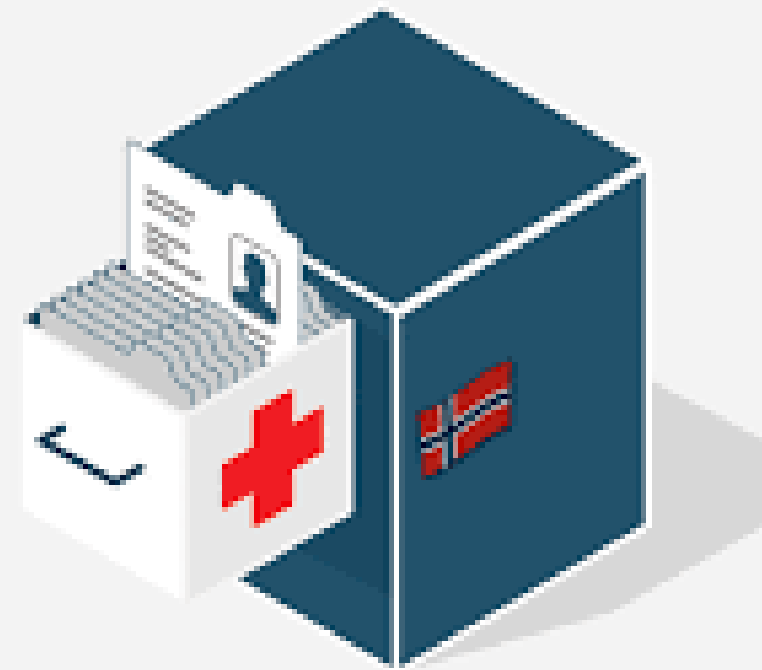
Rank	Name of Covered Entity	Year	Covered Entity Type	Individuals Affected	Type of Breach
1	Anthem Inc.	2015	Health Plan	78,800,000	Hacking/IT Incident
2	American Medical Collection Agency	2019	Business Associate	26,059,725	Hacking/IT Incident
3	HCA Healthcare	2023	Business Associate	11,270,000	Hacking/IT 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



SinHealth Data Breach 2018

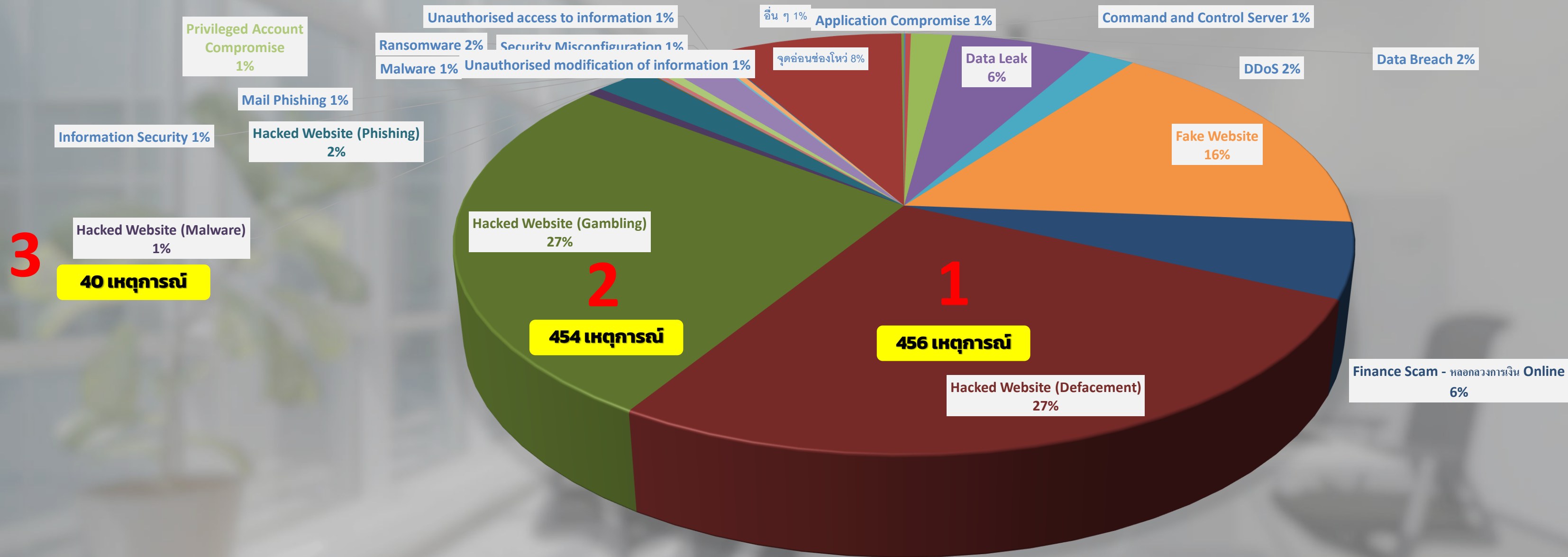



SingHealth
Healthcare Data Breach



สถิติการปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์

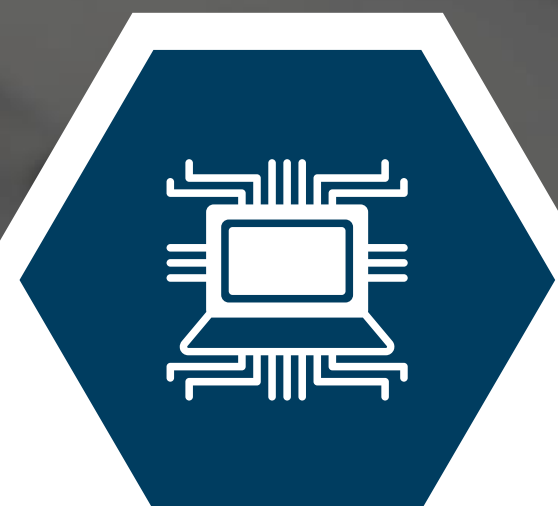
วันที่ 1 ต.ค. 65 – 18 ส.ค. 66



รวมทั้งสิ้น 1,703 เหตุการณ์

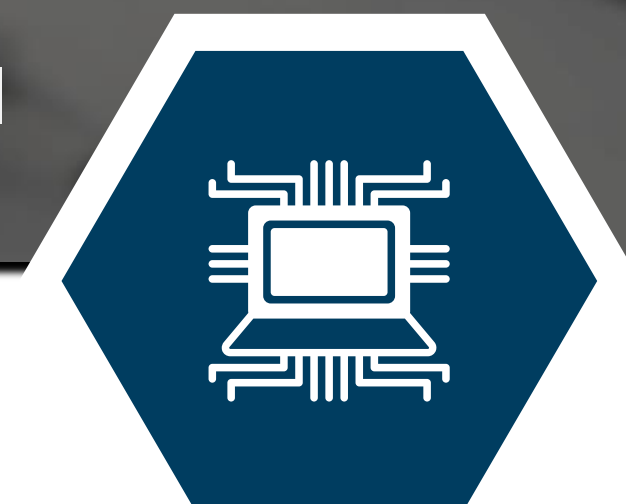
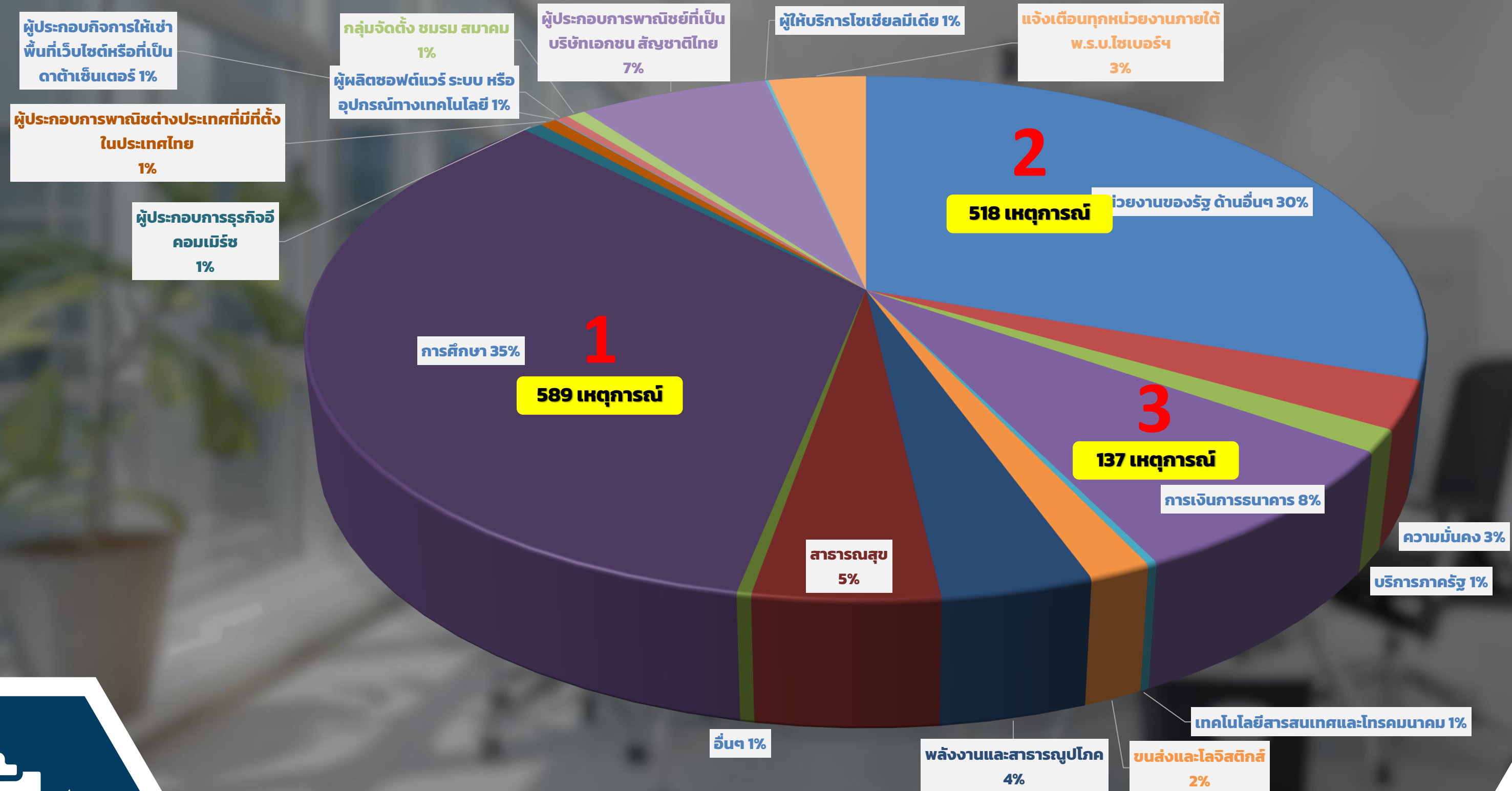
- Hacked Website (Phishing, Defacement, Gambling)
- Fake Website
- จุดอ่อนช่องโหว่
- Data Leak
- Finance Scam - หลอกลวงการเงิน Online
- DDoS
- Ransomware
- Data Breach
- อื่น ๆ

961 เหตุการณ์
275 เหตุการณ์
137 เหตุการณ์
103 เหตุการณ์
98 เหตุการณ์
34 เหตุการณ์
34 เหตุการณ์
30 เหตุการณ์
31 เหตุการณ์



สถิติการปฏิบัติในการรับมือกับภัยคุกคามทางไซเบอร์

วันที่ 1 ต.ค. 65 – 18 ส.ค. 66



รพ.เพชรบูรณ์ ขอโทษ ปมโดนแฮกข้อมูลคนไข้เป็นข้อมูลทั่วไป ไม่มีผลต่อการรักษา



5 กันยายน 2564 มีการประกาศขายข้อมูลคนไข้โรงพยาบาลเพชรบูรณ์ทางอินเทอร์เน็ต **ขนาดข้อมูล 3.75 กิกะไบต์ จำนวน 16 ล้านเรคคอร์ด จาก 146 ฐานข้อมูล ในราคา 500\$** ทางโรงพยาบาลฯ จึงรับดำเนินการตรวจสอบโดยเร่งด่วน มีการจัดตั้งคณะกรรมการแก้ไขปัญหาคูหาจะคุกคามทางไซเบอร์ เพื่อตรวจสอบข้อเท็จจริงและประเมินความเสียหายที่เกิดขึ้น ข้อมูลที่มีการเผยแพร่ในอินเทอร์เน็ตแสดงข้อมูลทั่วไปของประชาชนที่มาใช้บริการและเจ้าหน้าที่บางส่วน ในขั้นต้นมีการปิดกั้นการเข้าถึงอินเทอร์เน็ตจากภายนอก ตรวจสอบความเสียหายระบบภายในโรงพยาบาล มีการตรวจสอบความปลอดภัยด้านไซเบอร์ ตรวจสอบระบบที่ข้อมูลรั่วไม่ให้มีการแฮกข้อมูลอยู่ในระบบ ผลการตรวจสอบไม่พบความเสียหายกับระบบปฏิบัติการที่ใช้ในการดูแลรักษาผู้ป่วย และจากการตรวจสอบขั้นต้นข้อมูลที่ประกาศขายเป็น**ข้อมูลเกี่ยวกับรายชื่อประชาชนที่มาใช้บริการ โรงพยาบาลชื่อแพทย์ที่ดูแล และตารางเวรแพทย์ ข้อมูลสัญญาณชีพวันเวลาที่มารับบริการสิทธิการรักษา เลขประจำตัวผู้ป่วย ไม่ใช่ฐานข้อมูลการรักษา ไม่มีรายละเอียดเกี่ยวกับการวินิจฉัยและรักษาโรค เป็นข้อมูลทั่วไปที่ไม่มีผลกระทบต่อ การดูแลรักษา**



ยอดค่าไถ่หรือความเสียหายโดยประมาณ
บน LOCKBIT 2.0 และ 3.0



ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the fee for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger

ในปี 2022 จาก 14 หน่วยงาน
ประมาณ 619,000,000 บาท

ในปี 2023 จาก 6 หน่วยงาน
ประมาณ 181,000,000 บาท

The screenshot shows the LOCKBIT 3.0 website with a header containing the logo, 'LEAKED DATA', and links for Twitter, Contact Us, Affiliate Rules, How to Buy Bitcoin, Press About Us, and Mirrors. The main content is a grid of 12 listings, each with a timer, a ransom amount, and a brief description of the leaked data. A cartoon hacker character is overlaid on the bottom right of the grid.

Timer	Ransom Amount	Description
7D 16h 59m 05s	\$ 100000	The Institute of [redacted] was established in 1977 as an academic institution of higher education dedicated to the study of Islam, with a particular
2D 09h 19m 00s		[redacted] is a quadruple play Telecom operator (mobile, landline, Internet and TV via the SFR box) with more than 1.5 million customers. (part 2)
PUBLISHED		[redacted] Mobile is a quadruple play Telecom operator (mobile, landline, Internet and TV via the SFR box) with more than 1.5 million customers. (part 1)
6D 16h 53m 02s	\$ 200000	[redacted] partitioning specialist VLP has specialised since 1982 in bespoke "flexible partitioning" for a wide variety of sectors, with products including:
PUBLISHED		[4.7 TB Files] [redacted] document and printing solutions tailored to address each client's unique needs
PUBLISHED		[part 1] [redacted] is one of the Top 100 Fitness and Wellness Clubs in America.
12D 19h 35m 39s	\$ 1000000	[redacted] Investment Advisory group, Carnbrea is a privately-owned boutique W [redacted] group with a proud
7D 02h 21m 28s	\$ 200000	[redacted] operates as a cabbage producer. The Company offers a variety of cabbage and organic products including spring m [redacted] red, aree
1D 13h 08m 56s	\$ 100000	[redacted] was founded in 1957 in Milan thanks to the
2D 15h 34m 45s	\$ 40000	[redacted]
2D 15h 33m 03s	\$ 225000	[redacted] with more than 20 years of experience in

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 แจ้งรายชื่อและข้อมูลติดต่อเจ้าของ
กรรมสิทธิ์ 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

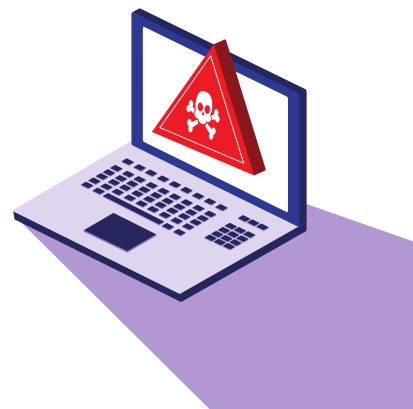
- (1) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง
- (2) แผนการรับมือภัยคุกคามทางไซเบอร์

1



แผนการตรวจสอบด้าน
การรักษาความมั่นคง
ปลอดภัยไซเบอร์

2



การประเมินความเสี่ยง
ด้านการรักษาความมั่นคง
ปลอดภัยไซเบอร์

3



แผนการรับมือภัย
คุกคามทางไซเบอร์

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา ๑๓ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) มีหน้าที่และอำนาจ ดังต่อไปนี้

(๔) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

ในการกำหนดกรอบมาตรฐานตามวรรคหนึ่ง (๔) ให้คำนึงถึงหลักการบริหารความเสี่ยง โดยอย่างน้อยต้องประกอบด้วยวิธีการและมาตรการ ดังต่อไปนี้

(๑) การระบุความเสี่ยงที่อาจเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิต ร่างกายของบุคคล

(๒) มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น

(๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

(๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

(๕) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์





Raising Awareness

สกมช. พัฒนาศักยภาพของหน่วยงานระบบโครงสร้างพื้นฐานสำคัญ 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



CYBER SECURITY KNOWLEDGE SHARING 14

QUANTUM COMPUTING

ประโยชน์ ภัยคุกคาม และการรับมือ

วันจันทร์ ที่ 28 กุมภาพันธ์ 2565 เวลา 13.00 - 15.00 น.

ลงทะเบียนและรับชมผ่านทาง Zoom Facebook Live NCSA Thailand

พละศักดิ์ ศรีสุภา เติมรัตน์
CEO & Co-founder Quantum Technology Foundation Thailand (QTF)

ดร.ธีรวัฒน์ ตั้งเกียรติธรรม
CEO & Co-founder Quantum Technology Foundation Thailand (QTF)

ดร.ภูษิต พิชัยกุล
CEO & Co-founder Quantum Technology Foundation Thailand (QTF)

CYBER SECURITY KNOWLEDGE SHARING 15

PDPA

Personal Data Protection Act

วันจันทร์ที่ 28 มีนาคม 2565 เวลา 13.00 - 15.00 น.

ลงทะเบียนและรับชมผ่านทาง Zoom Facebook Live NCSA Thailand

พละศักดิ์ ศรีสุภา เติมรัตน์
CEO & Co-founder Quantum Technology Foundation Thailand (QTF)

ดร.ธีรวัฒน์ ตั้งเกียรติธรรม
CEO & Co-founder Quantum Technology Foundation Thailand (QTF)

ดร.ภูษิต พิชัยกุล
CEO & Co-founder Quantum Technology Foundation Thailand (QTF)

Reskill and Upskill

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

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

NCSA THNCA

ครั้งแรก! สกมช. จัดอบรมพัฒนาความรู้

การรับมือภัยคุกคามด้านไซเบอร์ระบบโครงสร้างพื้นฐานระดับโลก ที่สนับสนุนโดยรัฐบาลออสเตรเลีย (Hand-on Experience)

กิจกรรม Capacity Building NCSA และ CERT CII Cyber Training

ระยะเวลา 3 วัน อบรมแบบ On-site

รุ่นที่ 1 วันที่ 6 - 8 มิถุนายน 2565 / รุ่นที่ 2 วันที่ 27 - 29 มิถุนายน 2565

จำนวนผู้เข้าอบรมรุ่นละ 75-80 คน

วิทยากรหลักประจำหลักสูตร

- 1. Mr. Manoj Kumar Murmu
- 2. Representative for Sectoral CERT in Thailand
- 3. Retrospect Labs Specialist from Australia

คุณสมบัติของผู้เข้าร่วม

- 1. ทำงานเกี่ยวข้องกับ Sectoral CERT ในประเทศไทย หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- 2. มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประมาณ 1-2 ปี
- 3. มีความรู้ในเชิงเทคนิค สำหรับการวิเคราะห์เหตุการณ์ภัยคุกคามด้านไอที

กิจกรรม Day 1

- 1. เปิดกิจกรรม Capacity Building NCSA และ CERT CII Cyber Training
- 2. How to establish the Sectoral CERT
- 3. Panel Discussion: Sharing Experience of CERT Incident Response
- 4. Workshop: Incident Response Plan (IRP) development & Exercise

Day 2

- 1. Introduction to Incident Response frameworks
- 2. Incident Response processes in action (Forensic / Analysis & Evaluation event & evidence Communication / Remediation)

CYBER SECURITY KNOWLEDGE SHARING #16

รู้เท่าทันภัยคุกคามทางไซเบอร์ฉบับพนักงานมืออาชีพ

Cybersecurity for professional employees

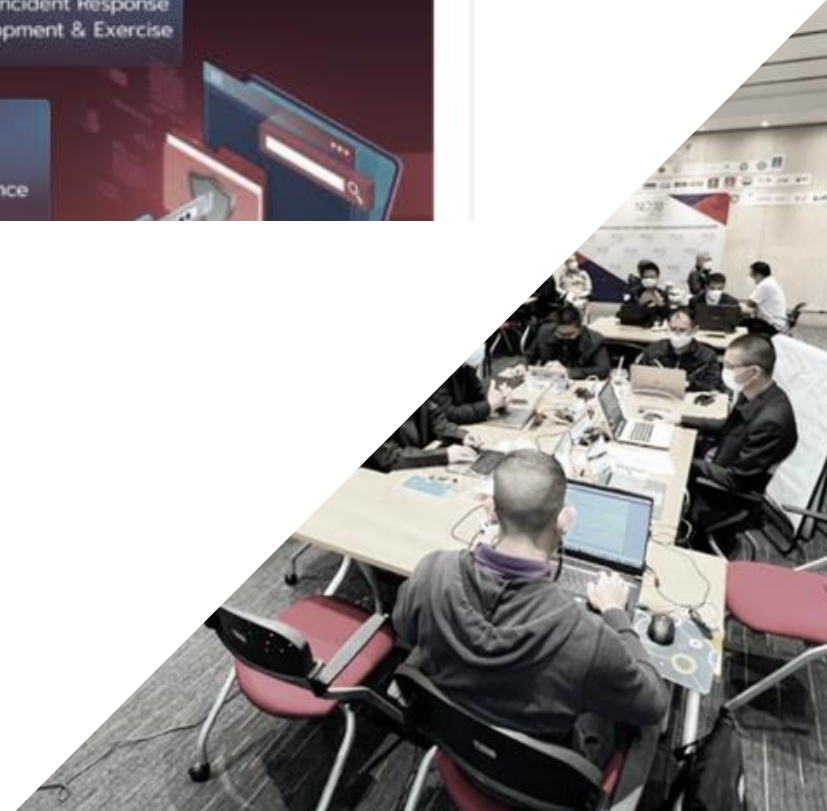
วันพุธที่ 26 เมษายน 2565 เวลา 10.00 - 12.00 น.

ลงทะเบียนและรับชมผ่านทาง Zoom Facebook Live NCSA Thailand

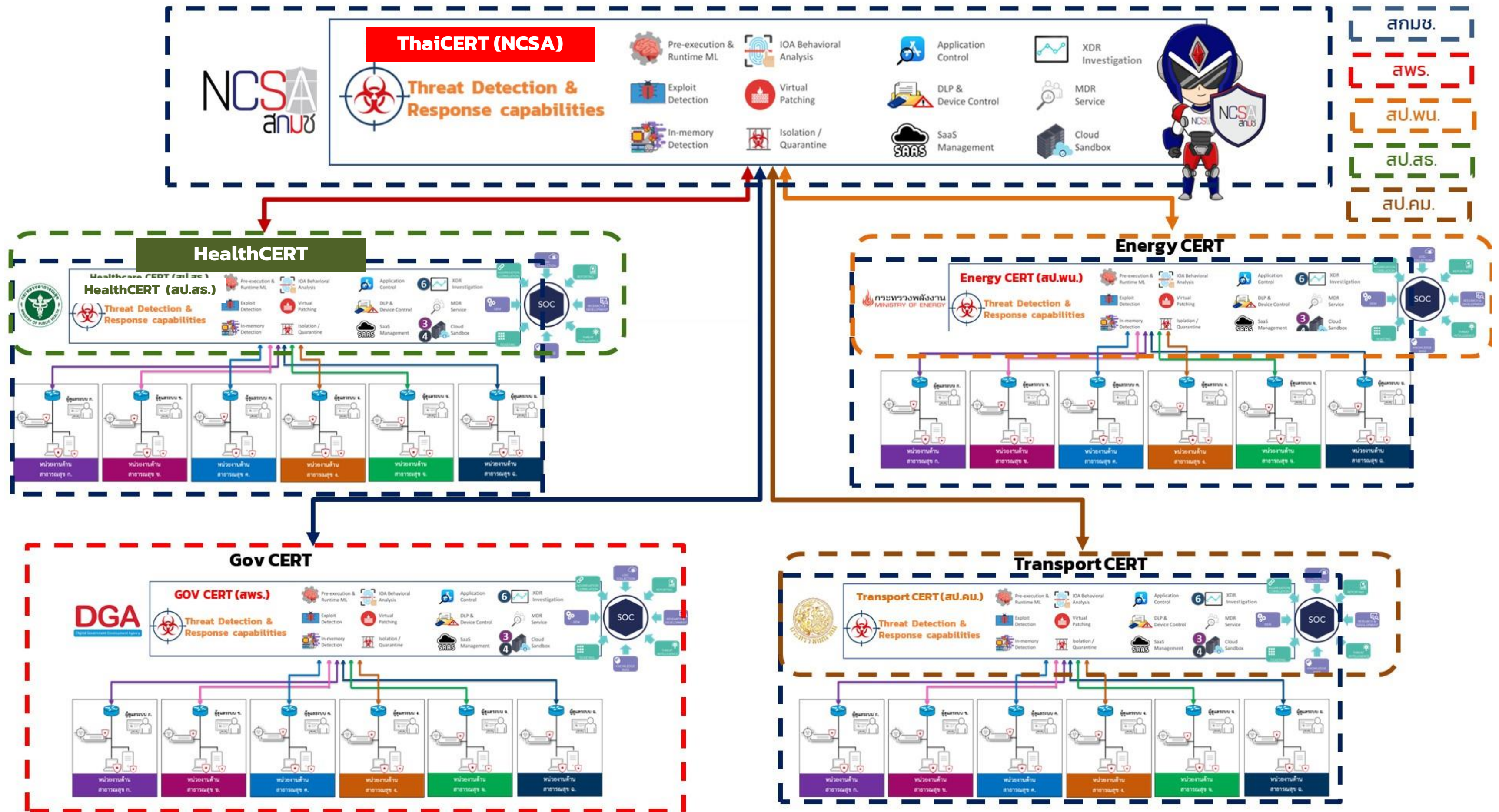
พละศักดิ์ ศรีสุภา เติมรัตน์
CEO & Co-founder Quantum Technology Foundation Thailand (QTF)

ดร.ธีรวัฒน์ ตั้งเกียรติธรรม
CEO & Co-founder Quantum Technology Foundation Thailand (QTF)

ดร.ภูษิต พิชัยกุล
CEO & Co-founder Quantum Technology Foundation Thailand (QTF)

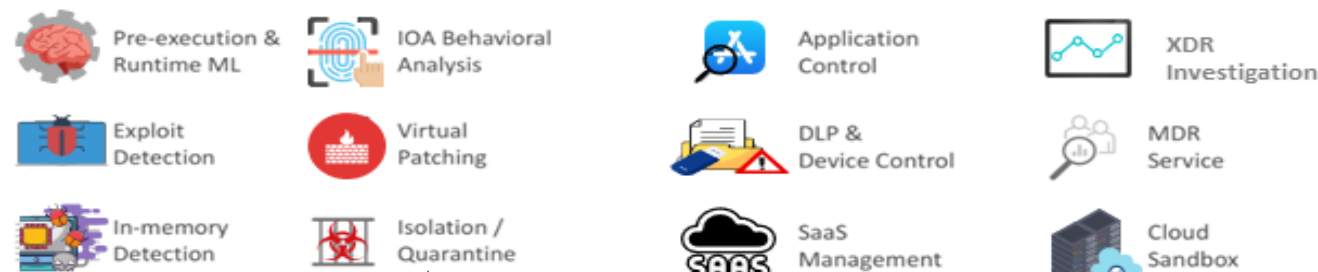


ໜ່ວຍງານ ຕົວກຳປັ້ນ Sectoral CERT ຂອງ ບ່ອນພັດທະນາໜີ້ສິນ ທາງດ້ານ ບໍລິຫານ ທາງດ້ານ ບໍລິຫານ



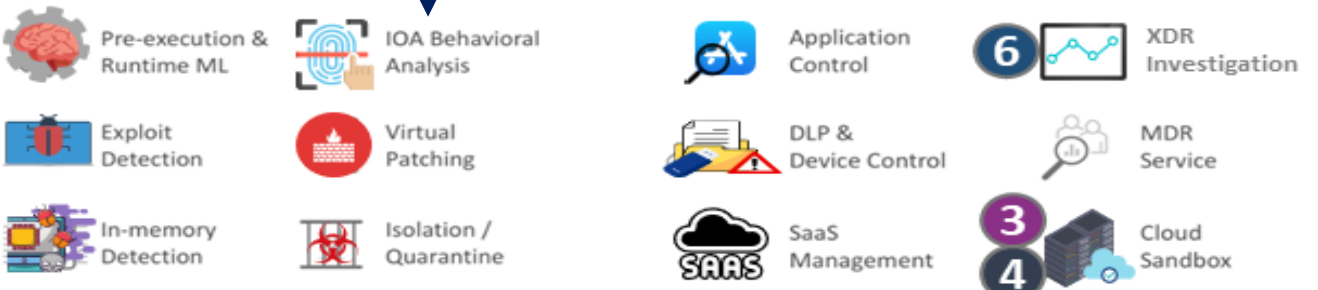
National CERT (NCSA)

Threat Detection & Response capabilities



Healthcare CERT (สอ.ส.)

Threat Detection & Response capabilities



10 โรงพยาบาล

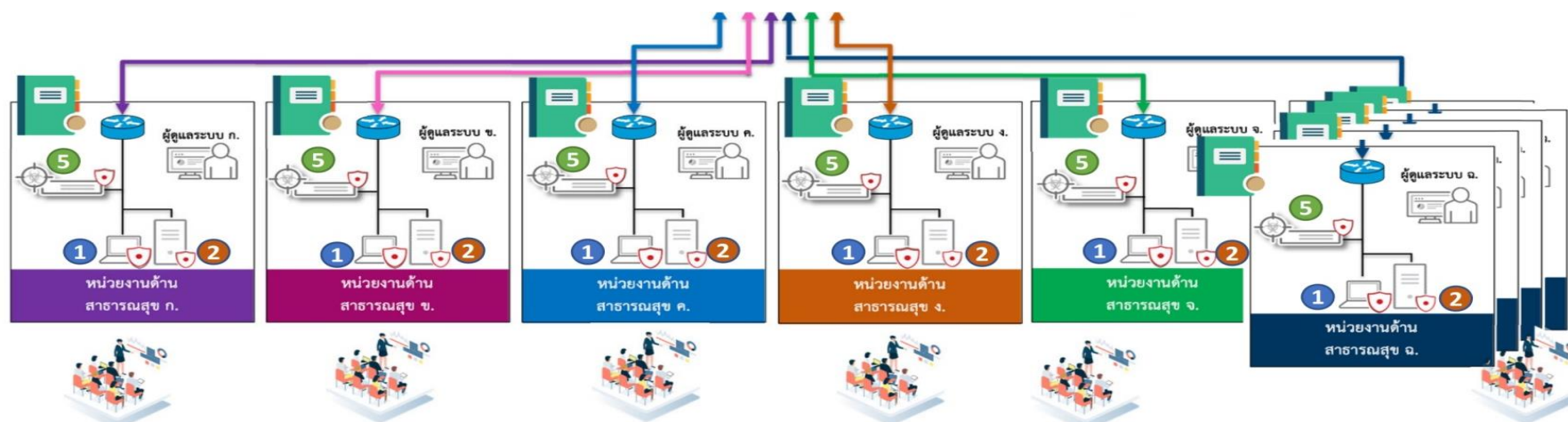
5 โรงพยาบาล

7. SOC as a Service



8. DFIR Team

These five reasons are to be noted. Therefore, learning Cybersecurity is very important Today!



ศูนย์ปฏิบัติการ



ระบบและเครื่องมือที่ใช้ในการปฏิบัติงาน



บริการเฝ้าระวังและให้บริการป้องกันและแก้ไขปัญหาภัยคุกคามทางด้านไซเบอร์

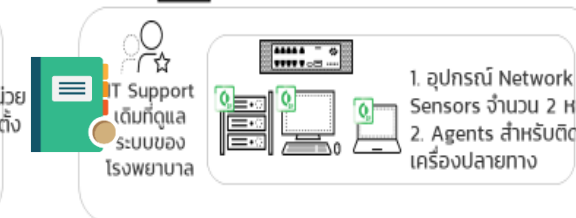
ป้องกันภัยคุกคาม บริการเฝ้าระวังภัยคุกคาม การจัดการภัยคุกคามเชิงรุก การแก้ไขปัญหาภัยคุกคามที่เกิดขึ้น



Private Link
Log
Response
โรงพยาบาล 1



Private Link
Log
Response
โรงพยาบาล 2



Private Link
Log
Response
โรงพยาบาล 3

