CYBER SECURITY IN HEALTH

INET
Always by your side

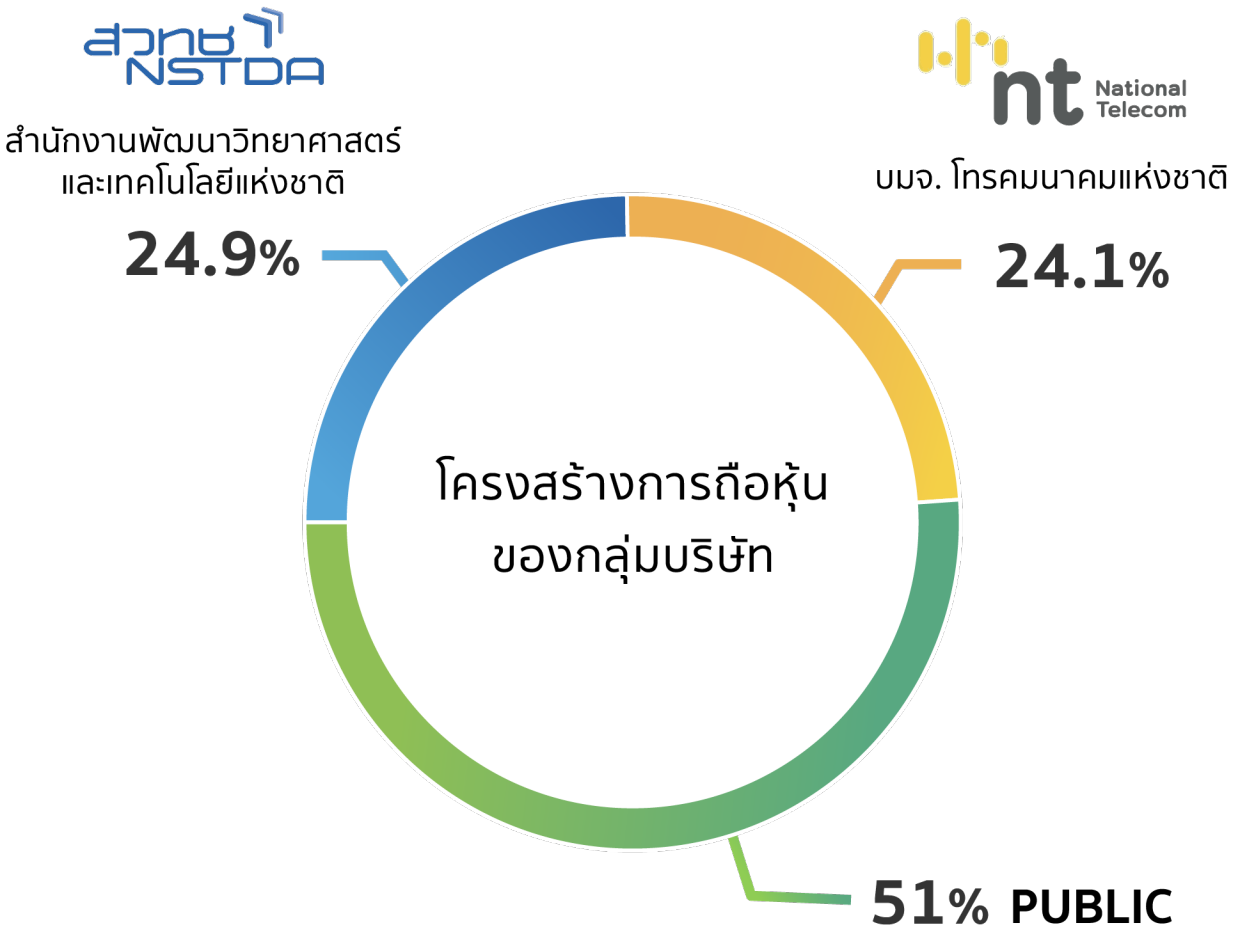
คุณวัลล์ชัย เวชชีวะดำรงค์
รองกรรมการผู้จัดการ
บริษัท อินเทอร์เน็ต ประเทศไทย จำกัด (มหาชน) INET

ประวัติความเป็นมาและโครงสร้างผู้ถือหุ้น

2538
ก่อตั้ง **“ศูนย์บริการอินเทอร์เน็ตประเทศไทย”**
เพื่อให้บริการอินเทอร์เน็ตเชิงพาณิชย์แห่งแรกของประเทศ

2540
เปลี่ยนเป็น **“บริษัท อินเทอร์เน็ตประเทศไทย จำกัด”**
ภายใต้รัฐวิสาหกิจของกระทรวงวิทยาศาสตร์และเทคโนโลยี

2544
แปรรูปเข้าสู่ตลาดหลักทรัพย์มีสถานะเป็นเอกชน และ
เปลี่ยนชื่อเป็น **“บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน)”**



INET Roadmap

INET 3.0

Cloud Fundamental

Year 19th - 21st (2013 - 2015)

Value Partner | Premium Customer

SLA
Customer Satisfaction

IDC | Network | Computing

IT Security

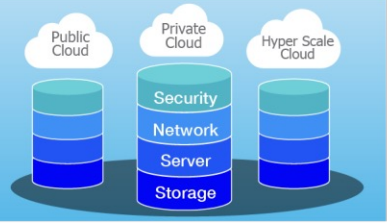
Cloud Architecture

Year 22nd - 24th (2016 - 2018)

Reseller | Strategic Account

Cloud as a Utility

Software-Defined Infrastructure



Multi-Site IDCs

INET 4.0

Cloud Platform

Year 25th - 27th (2019 - 2021)

Public Channel | Private Channel

Value Chain Development

Trusted Platform

Infra structure | Cyber Security | E-Tran saction | Internet of Thing | Big Data

Strategic Partner

Subsidiary

Transition

ONE PLATFORM

Digital Transform

Year 28th - 30th (2022 - 2024)

Value Chain | Innovation Chain

Smart Industrial

Digital Life

Software Integrator | IoT Designer | Data Architecture

Trusted Platform

Digital Life

Year 31st - 33th (2025 - 2027)

Tradition Life Value | Modern Life Value

Life Designer

Quality Life

Life Scoring | AI Assistant | OpenLife Data

Digital Life Platform

Cloud Infrastructure Era

Digital Era

Thailand Public Cloud Services – Market Size and Share ranked

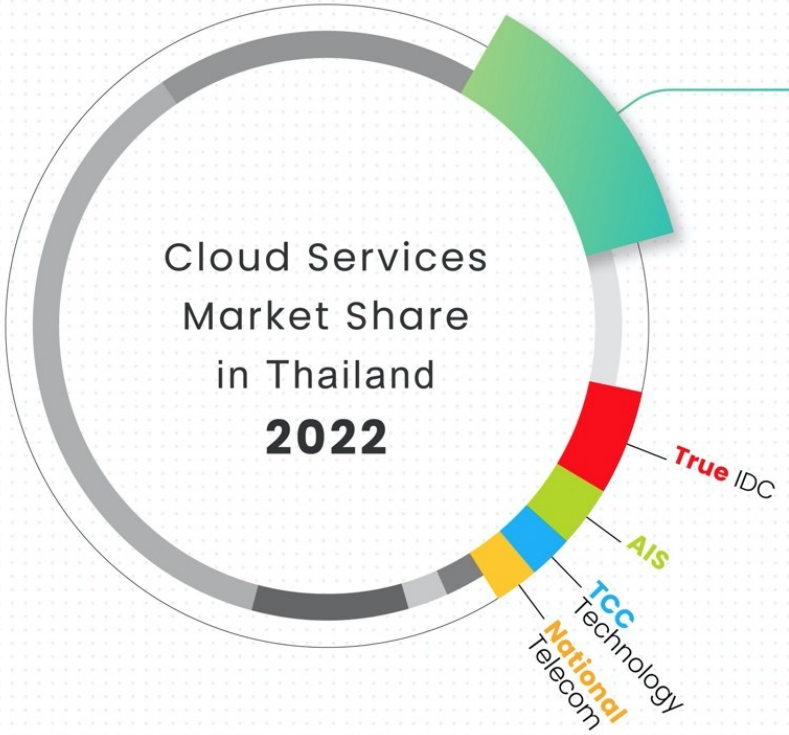
Cloud Services Provider	2019 Market Share(%)	Growth (%) 2018-2019	2020 Market Share(%)	Growth (%) 2019-2020	2021Market Share(%)	Growth (%) 2020-2021	H1:2022 Market Share(%)
Amazon Web Services	29.47	40.48	31.67	33.43	34.11	42.40	36.53
Microsoft	14.57	40.06	15.79	34.53	17.15	43.58	17.66
INET	14.95	49.83	14.81	23.05	13.64	21.77	12.52
Huawei	2.51	1,532.15	4.95	145.03	7.23	92.90	7.70
True IDC	5.39	46.85	5.33	22.93	4.95	22.60	5.02
AIS	3.49	34.01	3.25	15.69	3.08	25.23	3.09
TCC Technology	2.52	36.66	2.50	23.45	2.44	29.16	2.41
National Telecom	2.30	40.99	2.43	31.56	2.42	31.15	2.27
IBM	2.44	42.25	2.35	19.80	2.06	15.64	2.06
Tencent	0.64	-	1.43	179.08	1.96	81.06	2.27
Others	21.73	-5.07	15.47	-11.58	10.96	-6.35	8.45
Total	100.00	-	100.00%	-	100.00%	-	100.00%
IaaS Total Revenue (Million USD)	**158.96**	**31.82%**	**197.39**	**24.18%**	**260.93**	**32.19%**	**156.86**

Note: 'Others' includes all global and local public cloud services providers presenting in Thailand market

Source: IDC Semiannual Public Cloud Services Tracker – 2022, Thailand IaaS Revenue is sales revenue in 2019-H12022

Market Size and Share ranked by Top 5 local players

ส่วนแบ่งตลาด CLOUD SERVICES ในไทย



เทียบผู้ให้บริการภายในประเทศไทย

INET เป็น Local Cloud ที่มีส่วนแบ่ง

มากที่สุดเป็นอันดับ 1 ในประเทศไทย

13.64% | มูลค่า 35.59 Million USD.

INET Compliances

CSA-STAR
CLOUD SECURITY
for Service Provider

ISO/IEC 27001:2013
CLOUD & DATA CENTER
SECURITY Management

ISO 27017:2015
CLOUD Information Security
Management

ISO 27799:2016
Health Informatics Information Security
(Cloud & IDC)

ISO 22301:2012
CLOUD IaaS
Business Continuity
Management

PCI-DSS
Payment Card Industry Data
Security Standard

ISO/IEC 20000-1:2011
CLOUD MANAGEMENT
Enterprise Network Connectivity
and DATA CENTER Management

ISO 27018:2014
Protection of Personally
Identifiable Information
in Public Cloud

SAP Certified
Provider of Hosting Services

SAP Certified
HANA Operations &
CLOUD Operations

IDC Tier III Design
Uptime Institute
INET-IDC3

IDC Tier III Construction
Uptime Institute
INET-IDC3

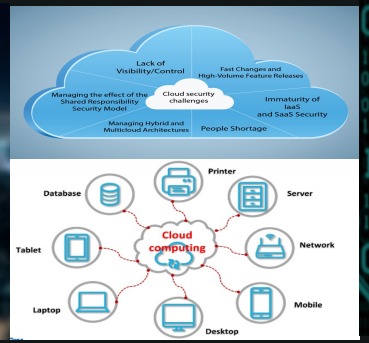
One Conference ได้รับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สำหรับระบบควบคุมการประชุมลับ เวอร์ชั่น 11จาก สพธอ. (ETDA)

CYBER SECURITY TRENDS

Top 10 Cybersecurity Trends 2023 Need to Know

Top 10 Cybersecurity Trends 2023

1. การโจมตีรถยนต์ที่มีระบบขับขี่อัตโนมัติ (Rise of Automotive Hacking)
2. ความสามารถและการใช้งาน AI ที่เพิ่มขึ้น (Potential of Artificial Intelligence)
3. อุปกรณ์สื่อสาร และโทรศัพท์มือถือจะเป็นเป้าในการโจมตีทางไซเบอร์ (Mobile is the New Target)
4. Cloud ยังเป็นเป้าในการโจมตี (Cloud is Also Potentially Vulnerable)
5. ข้อมูลหลุดยังจะมีอยู่ต่อไป (Data Breaches: Prime target)



Top 10 Cybersecurity Trends 2023

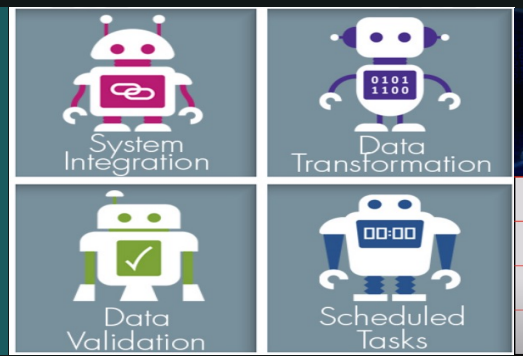
6. IoT และ 5G เทคโนโลยีที่มาพร้อมกับความเสี่ยง (IoT with 5G Network The New Era of Technology and Risk)

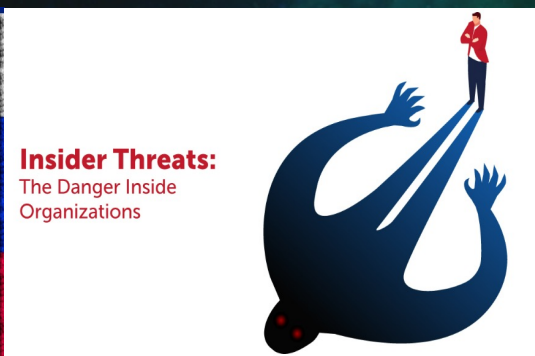
7. การใช้งาน Software Robot จะมากขึ้น (Automation and Integration)

8. Ransomware ยังเป็นภัยคุกคามอยู่อย่างต่อเนื่อง (Targeted Ransomware)

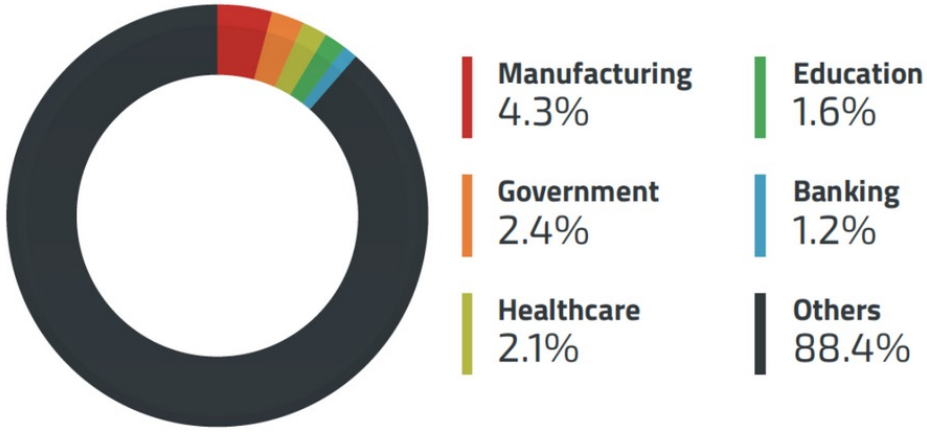
9. แฮ็กเกอร์ที่มีเงินทุนและได้รับการสนับสนุนจากรัฐ (State-Sponsored Cyber Warfare)

10. แฮ็กจากข้างใน (Insider Threats)

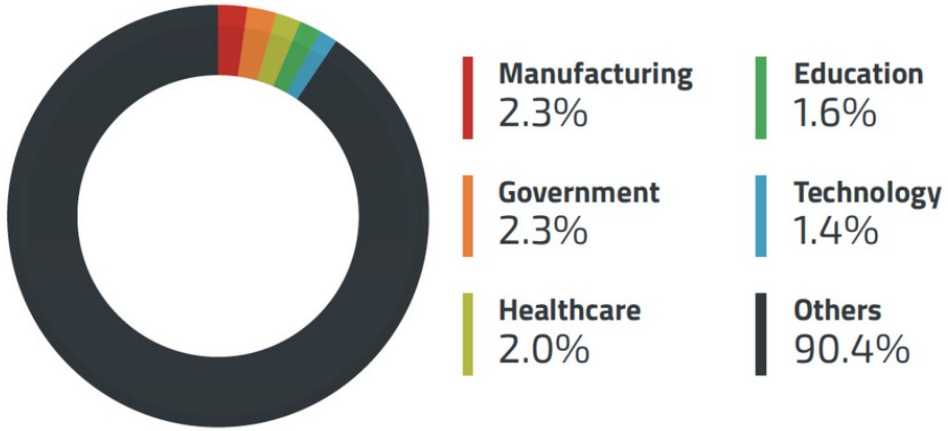




A comparison of the top 5 industries with the highest number of malware detections



1H 2021



1H 2022

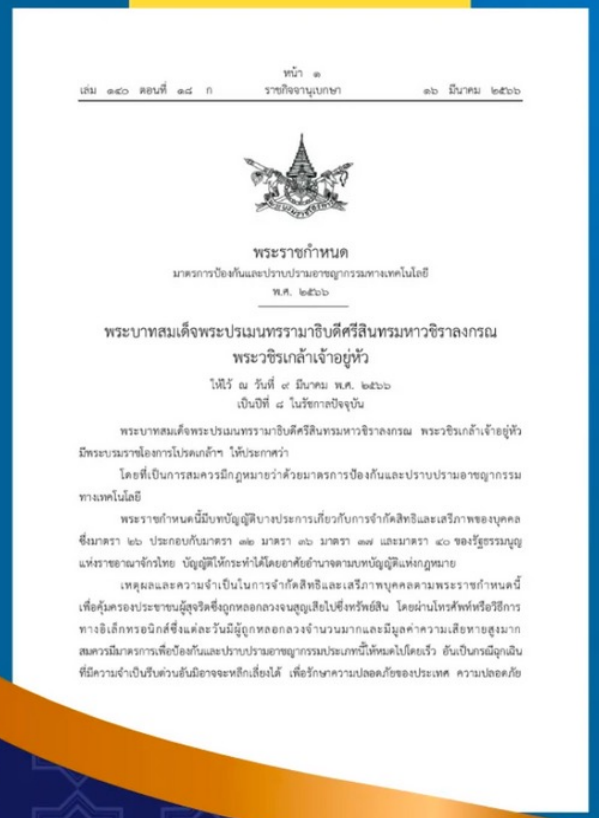
Source: Trend Micro 2022 Cybersecurity Report

มูลค่าความเสียหาย จากการถูกโจมตีทางไซเบอร์ของบริษัทไทย

มูลค่าความเสียหาย (เหรียญสหรัฐ)	%
น้อยกว่า 1 แสน	9
1 แสน - 4.99 แสน	6
5 แสน - 9 แสน	18
1 ล้าน - 2.4 ล้าน	40
2.5 ล้าน - 4.9 ล้าน	17
5 ล้าน - 9.9 ล้าน	4
มากกว่า 10 ล้าน	6

ที่มา : ซิสโก้

ประชาชาติกราฟิก



หน้า ๑
เล่ม ๑๔๐ ตอนที่ ๑๘ ก ราชกิจจานุเบกษา ๑๖ มีนาคม ๒๕๖๖

พระราชกำหนด
มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี
พ.ศ. ๒๕๖๖

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๙ มีนาคม พ.ศ. ๒๕๖๖
เป็นปีที่ ๘ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

พระราชกำหนดนี้มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล ซึ่งมาตรา ๒๖ ประกอบกับมาตรา ๓๒ มาตรา ๓๖ มาตรา ๓๗ และมาตรา ๔๐ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย บัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย

เหตุผลและความจำเป็นในการจำกัดสิทธิและเสรีภาพบุคคลตามพระราชกำหนดนี้ เพื่อคุ้มครองประชาชนผู้สุจริตซึ่งถูกหลอกลวงจนสูญเสียไปซึ่งทรัพย์สิน โดยผ่านโทรศัพท์หรือวิธีการทางอิเล็กทรอนิกส์ซึ่งแต่ละวันมีผู้ถูกหลอกลวงจำนวนมากและมีมูลค่าความเสียหายสูงมาก สมควรมีมาตรการเพื่อป้องกันและปราบปรามอาชญากรรมประเภทนี้ให้หมดไปโดยเร็ว อันเป็นกรณีฉุกเฉินที่มีความจำเป็นรีบด่วนอันมิอาจจะหลีกเลี่ยงได้ เพื่อรักษาความปลอดภัยของประเทศ ความปลอดภัย

พระราชกำหนด

มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

พ.ศ. ๒๕๖๖

การกระทำความผิดเกี่ยวกับ พ.ร.บ. คอมพิวเตอร์ พร้อมบทลงโทษ

มาตรา	ประเด็นความผิดตาม พรบ.คอมพิวเตอร์	โทษจำคุก	โทษปรับ
5	ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน	ไม่เกิน 6 เดือน	ไม่เกิน 10,000 บาท
7	"ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน"	ไม่เกิน 2 ปี	ไม่เกิน 40,000 บาท
9	ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่น โดยมิชอบ เช่น การแก้ไขข้อมูลทางคอมพิวเตอร์หรือปล่อยไวรัส (Viruses,Worms,Trojan)	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
10	ผู้ใดกระทำด้วยประการ ใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ เช่น การทำ DOS	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
11	"ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข" ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท "ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นอันมีลักษณะเป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ โดยไม่เปิดโอกาสให้ผู้รับสามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย"	-	ไม่เกิน 100,000 บาท

ที่มา : พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ 2562

กำหนดลักษณะภารกิจ/บริการ 7 ประเภท ที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)

ประเภท	ด้านความมั่นคงของรัฐ	ด้านบริการภาครัฐที่สำคัญ	ด้านการเงินการธนาคาร	ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม	ด้านการขนส่งและโลจิสติกส์	ด้านพลังงานและสาธารณูปโภค	ด้านสาธารณสุข
CII Regulator	ก.กลาโหม ก.ดิจิทัล ฯลฯ	ก.ดิจิทัล ก.การคลัง	ธปท ก.ล.ต. คปภ.	กสทช	ก.คมนาคม	ก.พลังงาน ก.มหาดไทย	ก. สาธารณสุข
CII Operator	DSI, สำนักงานตรวจคนเข้าเมือง (ตม.)	กรมบัญชีกลาง, กรมสรรพากร, สำนักงานหลักประกันสุขภาพแห่งชาติ	ธนาคาร	INET, AIS, DTAC, TRUE	บจก. ทางด่วนและรถไฟฟ้ากรุงเทพ, การรถไฟแห่งประเทศไทย	การไฟฟ้านครหลวง การไฟฟ้าส่วนภูมิภาค,การประปานครหลวง	โรงพยาบาล

SIEM หรือ Security Information and Event Management
คือ ระบบที่ใช้ในการจัดการกับ Log และ Event ต่าง ๆ ทำหน้าที่วิเคราะห์หาความเชื่อมโยงของ Event ที่เกี่ยวข้องกับความปลอดภัยทั้งหมด ให้ทีมทราบเมื่อมี Event ที่ผิดปกติ ทำให้องค์กรสามารถป้องกัน และตอบสนองภัยคุกคามได้อย่างรวดเร็ว

SOC หรือ Security Operation Center คือ ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ที่ตรวจจับทุกความเคลื่อนไหวที่ผิดปกติ ทำหน้าที่เฝ้าระวังและป้องกันระบบหรืออุปกรณ์สำคัญขององค์กรจากการถูกบุกรุกหรือการเข้าถึงโดยไม่ได้รับอนุญาต ซึ่งหากมีเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident) SOC จะทำหน้าที่ประเมิน ตรวจสอบและแก้ไขเหตุการณ์ที่เกิดขึ้น เพื่อลดผลกระทบและความเสียหายที่อาจเกิดขึ้นกับองค์กรให้อยู่ในระดับที่ไม่รุนแรง

CSIRT ย่อมาจาก Computer Security Incident Response Team (ชื่อทั่วไปของ CERT เนื่องจาก CERT ถูกจดทะเบียนเป็นเครื่องหมายการค้า) คือทีมผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ ที่สามารถรับมือและแก้ไขเหตุภัยคุกคาม ประกอบด้วยบุคลากรที่มีความรู้และทักษะในการรับมือ เหตุภัยคุกคาม ให้ความช่วยเหลือผู้รับบริการในการ ฟื้นตัวจากการเจาะระบบ

Security Operation Center Practices and Frameworks

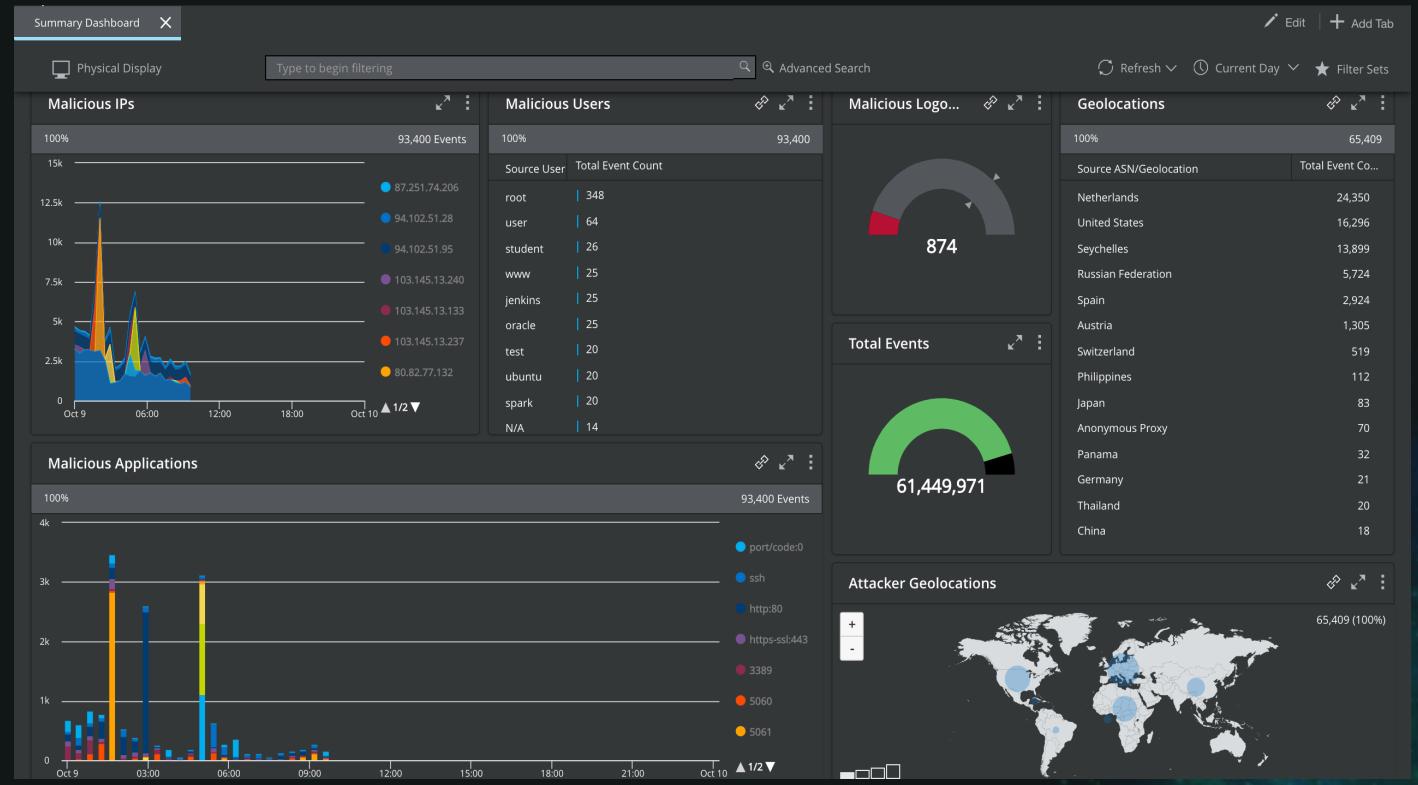
Cybersecurity Framework

Source: https://www.nist.gov/cyberframework

Incident Handling

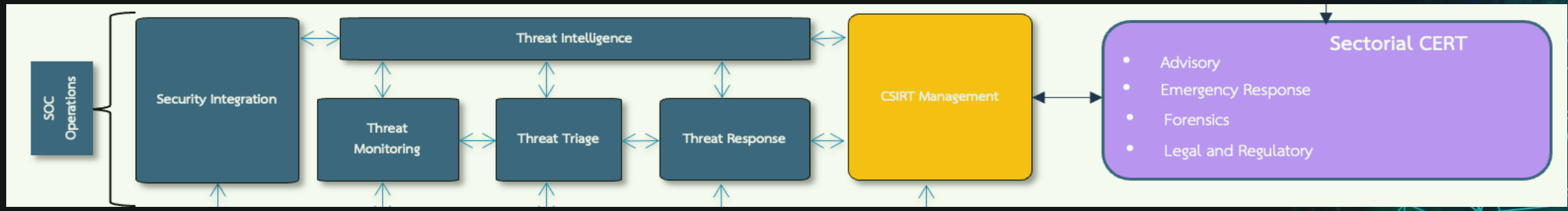
Source: https://www.sans.org/reading-room/whitepapers/incident/paper/33901

Security Operation Center (SOC)



การวิเคราะห์พฤติกรรมที่เป็นภัยคุกคาม (Threat Behavior Analysis)

ตัวอย่าง Dashboard แสดงข้อมูลการตรวจพบภัยคุกคาม (Threat) เข้ามาโจมตีระบบคอมพิวเตอร์ของลูกค้า



THE COMPONENTS OF SECURITY OPERATIONS CENTER

Log Collector Client Log Files

Technology

- Threat Intelligent (External ,Internal Threat Data)
- Content pack

People

- Certified People
- More experiences

Processes

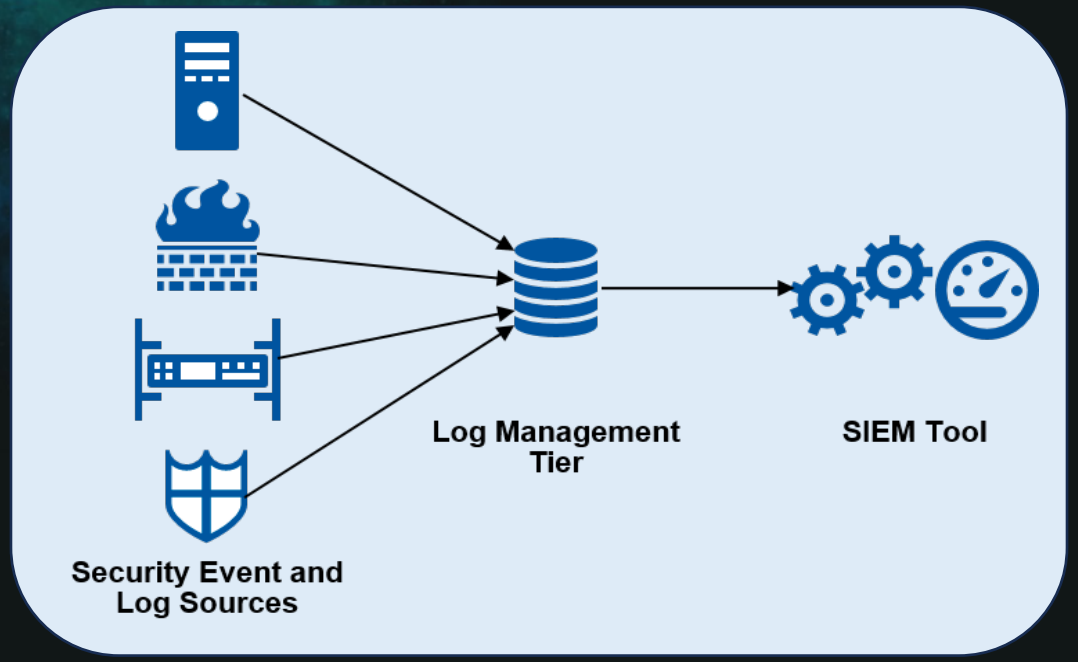
- NIST Cyber Security Framework
- Incident Response
- ISO/IEC 20000-1:2018
- ISO/IEC 27001:2013
- ISO/IEC 27701:2019

Customer

- Monthly report
- Incident report
- Incident response report
- Security NEWS

SIEM
(Security Information and Event Management)

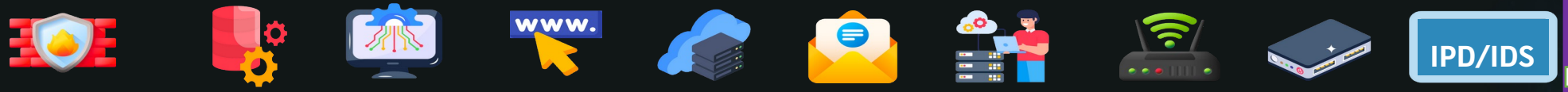
ภาพตัวอย่างการ Detective ในระบบ SIEM โดย alert ผ่านระบบ chat



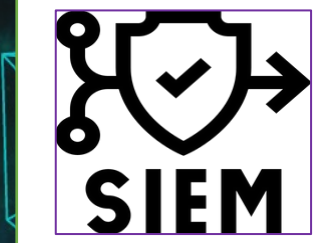
Bot alert: *🔴 [redacted] Log ssh Alert 🔴*
Event Logs ssh previously 20 Minute ago
Platform : [redacted] (Intel)
Vcenterip : [redacted]
Total : 2
Message : SSH login has failed
Host :
- [redacted] = 2
Source IP: [redacted]
Detail :
- 2023-08-21 18:18:34 SSH login has failed for [redacted]
- 2023-08-21 18:18:36 SSH login has failed for [redacted]

Bot alert: *🔴 [redacted] Log Alert 🔴*
Event Logs previously 10 Minute ago
Platform : [redacted] (Intel)
Vcenterip : [redacted]
Total : 1
Message : Remote access for ESXi local user account 'root' has been locked
Host :
- [redacted] = 1
Source IP: [redacted]
Detail :
- 2023-08-21 18:18:36 Remote access for ESXi local user account 'root' has been locked for 900 seconds after 80 failed login attempts.

DATA COLLECTION



Firewall | Database | Endpoint | WWW | File server | Email | Management Server | Routers | Switches | IPS/IDS



CSIRT

COMPUTER SECURITY INCIDENT RESPONDE TEAM

เพื่อตอบสนองและจัดการกับเหตุการณ์ที่เกิดขึ้นเกี่ยวกับความปลอดภัย หรือ Incidents ที่เกิดขึ้นในระบบคอมพิวเตอร์และเครือข่ายขององค์กร ซึ่งอาจเป็นการโจมตีจากภายนอกหรือเป็นเหตุการณ์จากภายใน ซึ่งอาจส่งผลกระทบต่อความปลอดภัยขององค์กร

CYBERCRIME

อาชญากรรมไซเบอร์ (Cybercrime) หมายถึง การกระทำที่มีคอมพิวเตอร์เป็นเครื่องมือ หรือมีคอมพิวเตอร์เป็นเป้าหมายในการกระทำผิด โดยเฉพาะอย่างยิ่งการกระทำผิดผ่านทางอินเทอร์เน็ต ซึ่งอาชญากรรมไซเบอร์มีทั้งการประกอบอาชญากรรมที่มีอยู่เดิมอยู่แล้วและพัฒนามาใช้ช่องทางออนไลน์

CSIRT FRAMEWORK

PREVENTIVE

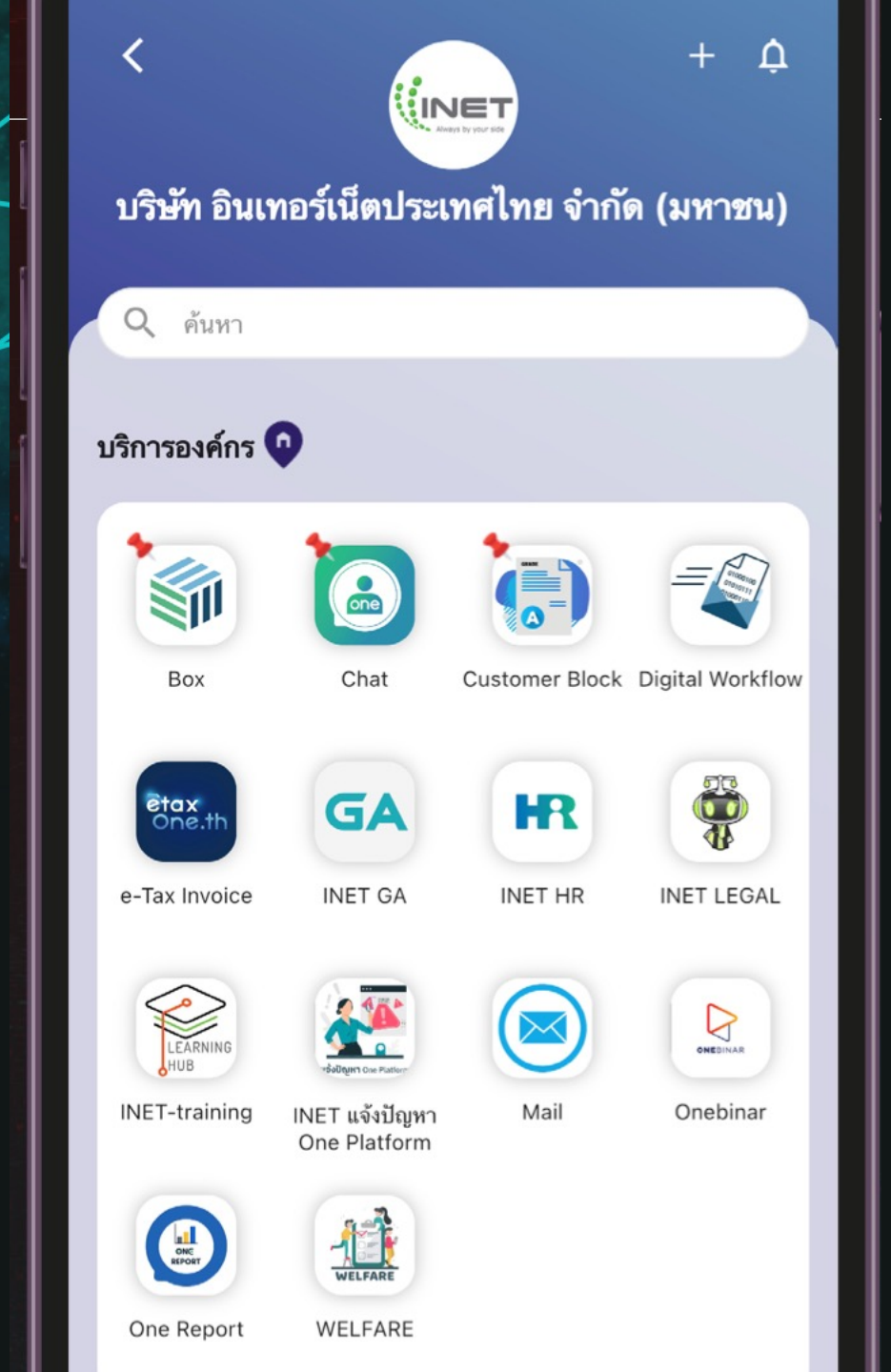
ป้องกันการเข้าถึงระบบ
(Authentication)

DETECTIVE

การค้นหาความผิดปกติ
รู้เร็ว รู้พฤติกรรม

CORRECTIVE

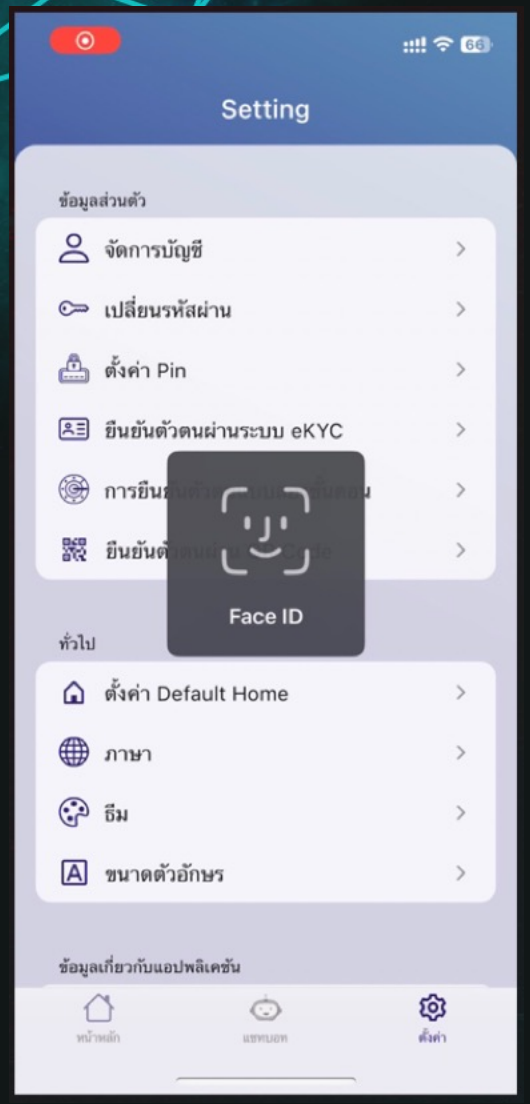
แก้ไขปัญหาได้
ทันที รวดเร็ว

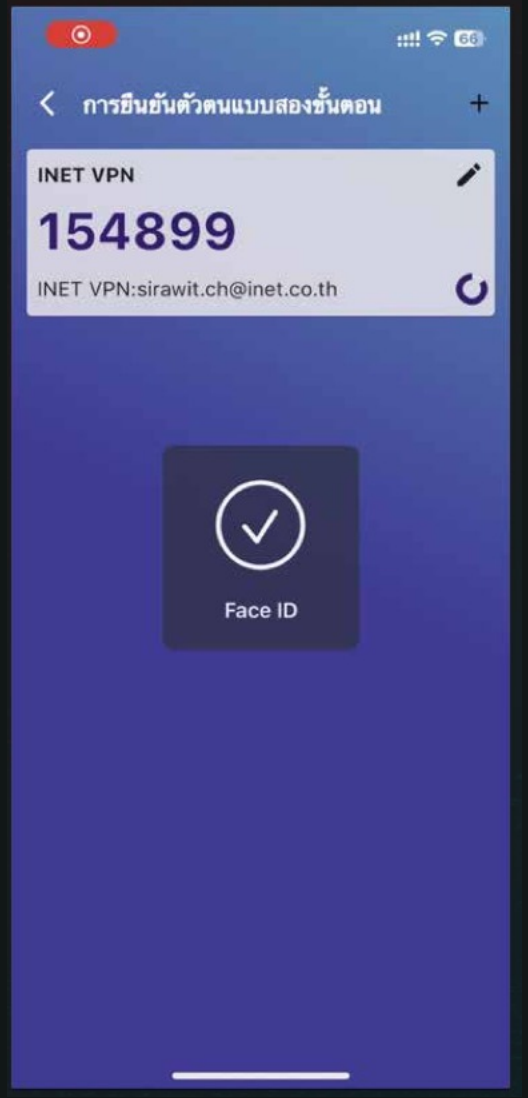


แนวทางการปฏิบัติ

ปรับวิธีการยืนยันตัวตนเพื่อเข้าสู่ระบบ (Authentication) รวมถึงการเข้าถึงข้อมูล รับส่งข้อมูล ของพนักงานทั้งองค์กร ผ่านเครื่องมือของบริษัทเท่านั้น

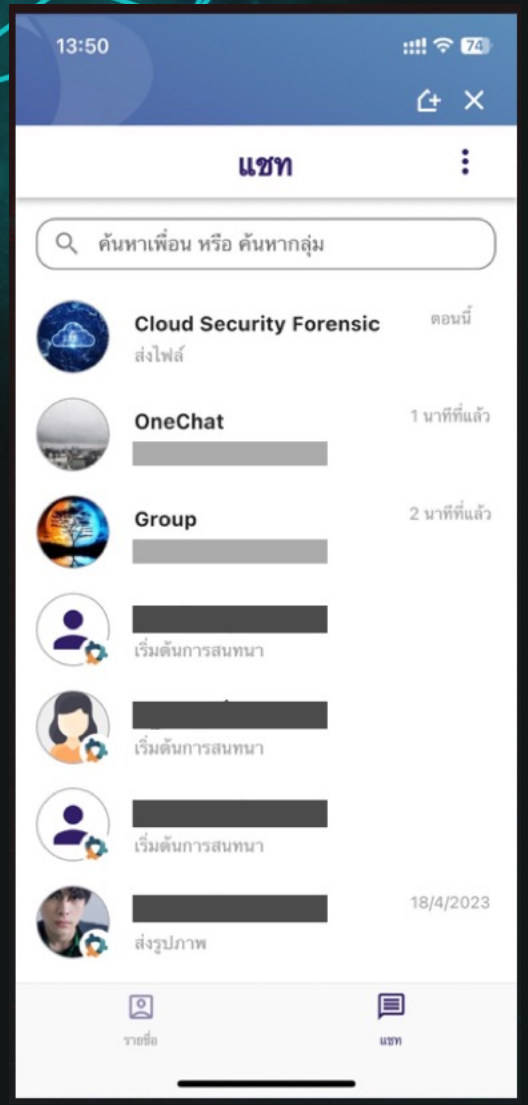
ONE PLATFORM

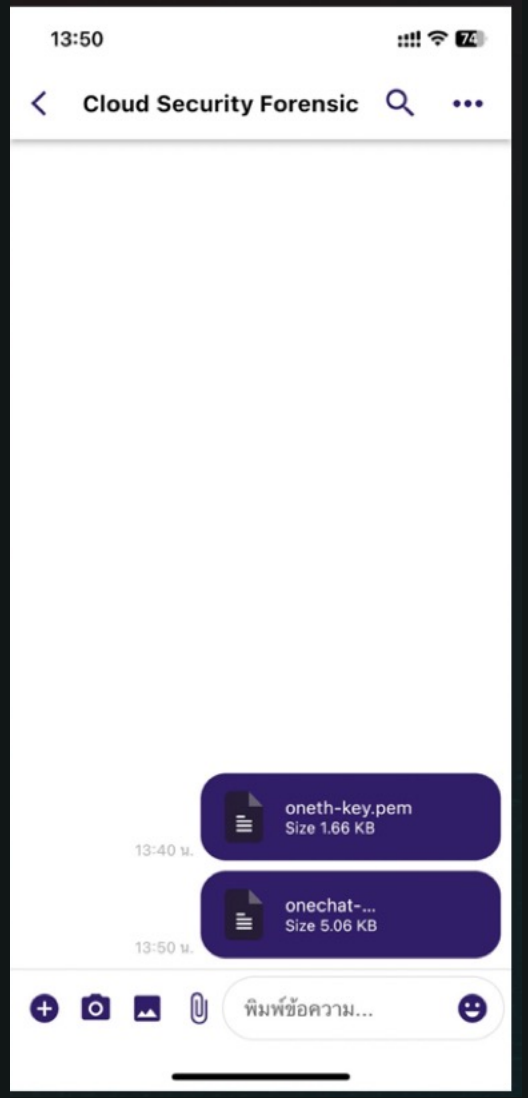




ตัวอย่าง แนวทางการปฏิบัติ

การ Login ด้วย Private Key

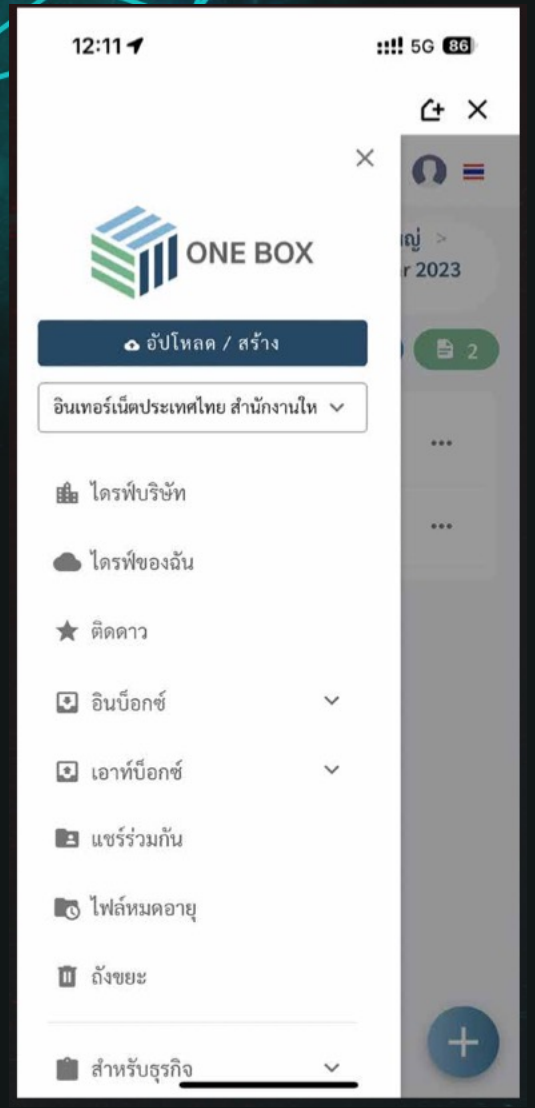


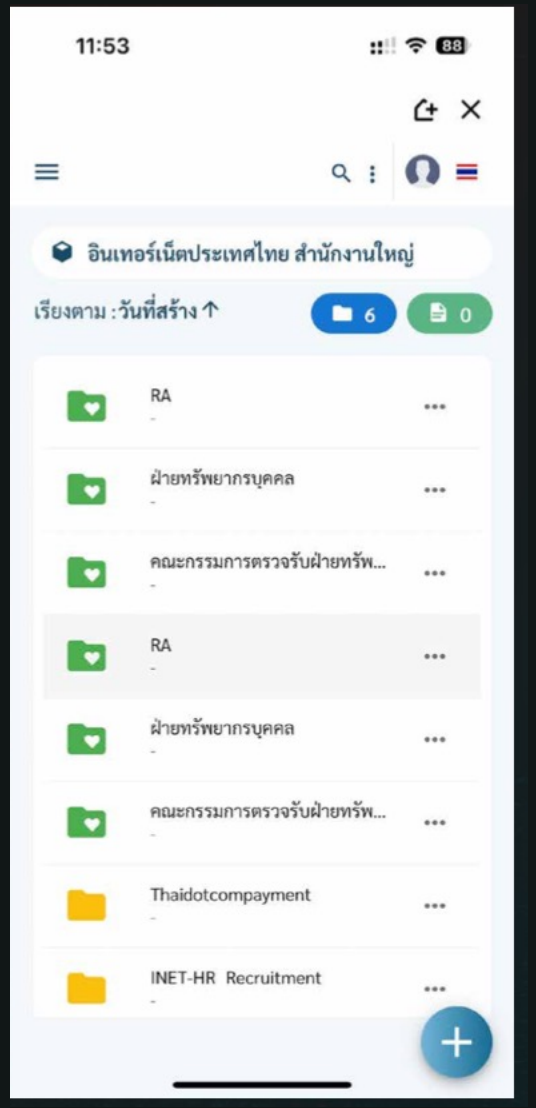


ตัวอย่าง แนวทางการปฏิบัติ

One Chat เพื่อรับส่งข้อมูล หรือ แชร์ ข้อมูลที่เกี่ยวข้องกับเรื่องระบบ ข้อมูลภายในบริษัททดแทน Line

onechat





ตัวอย่าง แนวทางการปฏิบัติ

One Box เพื่อจัดเก็บไฟล์ หรือแชร์ไฟล์ข้อมูลต่างๆ สำหรับการทำงาน

ONE BOX

CORRECTIVE

Business Continuity Plan (BCP)

Pain point

เพื่อช่วยในการเตรียมในการรับมือเมื่อเกิดเหตุการณ์ที่ไม่คาดฝัน ที่อาจจะเกิดขึ้นทำให้มีแผนรองรับที่ชัดเจน และมั่นใจได้ว่าระบบสามารถทำได้ตามกระบวนการหากเกิดเหตุการณ์ที่ไม่คาดฝัน

Business Continuity Plan Framework

Visible

Critical VM (Core service)
Failed-over Expectation
Critical points (Infrastructure)

Controllable

- Critical parameter
- Backup retention

Improvable

- Improve Solution Design
- Re-run BCP Failed-over

Planning

- Action Plan
- BCP Failed-over

สิ่งที่ทางลูกค้าได้รับหลังจาก ทดสอบ Business Continuity Plan (BCP)

- มีกระบวนการทดสอบ Business Continuity Plan (BCP) ของ Service การใช้งานให้ไปตามมาตรฐานการให้บริการระหว่าง INET กับผู้ใช้บริการ
- ข้อมูล Backup ว่ามีความถูกต้อง และ เป็นไปตามปริมาณข้อมูลสูญหายในเวลาที่ยอมรับได้ (RPO : Recovery Point Objective)
- ตรวจสอบในระดับ OS ของ VMs จากการ Backup ว่ามีความพร้อมสำหรับรองรับเหตุการณ์ฉุกเฉิน

THANK YOU