แนวทางการจัดทำ กระบวนการตอบสนองภัยคุกคามทางไซเบอร์ ของ ทร.

การสัมมนาการพัฒนาขีดความสามารถด้านไซเบอร์ ของ ทร.
ประจำปีงบประมาณ พ.ศ.2569
ระหว่าง 14 – 16 ม.ค.69
ณ ศูนย์สมุททานุภาพ ทร. ต.บางพระ อ.ศรีราชา จ.ชลบุรี

น.ท.หญิง พันธ์รัตน์ อักษรศรีกุล

การศึกษา

- วิทยาศาสตรบัณฑิต (วิทยาการคอมพิวเตอร์) สถาบันราชภัฏสวนดุสิต
- วิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศ) ม.เทคโนโลยีพระจอมเกล้าพระนครเหนือ
- หลักสูตรทั่วไป รุ่นที่ 35* รร.ชต.ยศ.ทร.
- Developing Cyber Organizations and Workforces
  Naval Postgraduate School, Monterey, CA
- หลักสูตรนายทหารอาวุโส รุ่นที่ 57* รร.เสธ.ทร.ยศ.ทร.

การรับราชการ

- 2546 นป.แผนกโปรแกรม ศปกม.สปช.ทร.
- 2552 นป.แผนกโปรแกรม กพน.ศทส.สสท.ทร.
- 2557 นป.แผนกโปรแกรม กพน.สปก.สสท.ทร.
- 2561 นวร.แผนกพัฒนาระบบ กสช.ศชบ.สสท.ทร.
- 2564 หน.ตอบสนองภัยคุกคาม กรช.ศชบ.สสท.ทร.
- 2567 ประจำ สสท.ทร.
- 2568 หน.ตอบสนองภัยคุกคาม กรช.ศชบ.สสท.ทร.
- 2569 หน.พัฒนาระบบ กสช.ศชบ.สสท.ทร. ช่วยราชการ ผ.ตอบสนองภัยคุกคาม กรช.ศชบ.สสท.ทร.

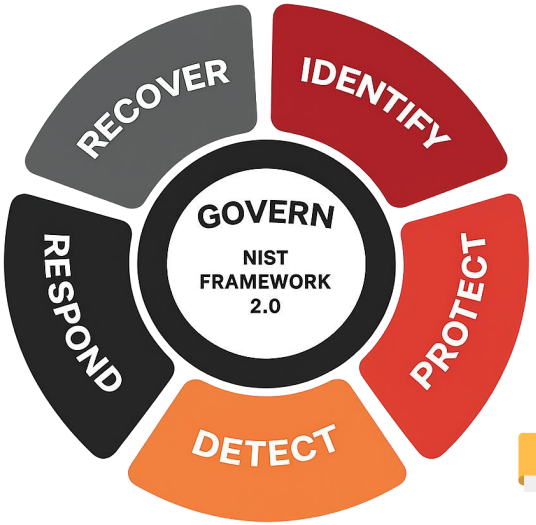
หัวข้อการบรรยาย

- กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ NIST CSF 2.0
- ศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์
- เหตุการณ์ภัยคุกคามทางไซเบอร์ที่สำคัญของ ทร.
- กระบวนการตอบสนองภัยคุกคามด้านไซเบอร์ของ ทร. (ปัจจุบัน)
- (ร่าง) กระบวนการตอบสนองภัยคุกคามด้านไซเบอร์ของ ทร. (ใหม่)
- กลุ่มสัมมนา แนวทางการจัดทำกระบวนการตอบสนองภัยคุกคามทางไซเบอร์ของ ทร.

กรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

The NIST Cybersecurity Framework 2.0 (NIST CSF 2.0)

NIST CSF 2.0



คืออะไร ?

กรอบแนวทางด้านความมั่นคงปลอดภัยไซเบอร์ฉบับปรับปรุงของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐอเมริกา (NIST) ที่ใช้เป็นแนวทางให้หน่วยงานสามารถ บริหารจัดการความเสี่ยงด้านไซเบอร์ (Cybersecurity Risk Management) ได้อย่างเป็นระบบ ครอบคลุมทั้งด้านเทคนิค การบริหาร และธรรมาภิบาล

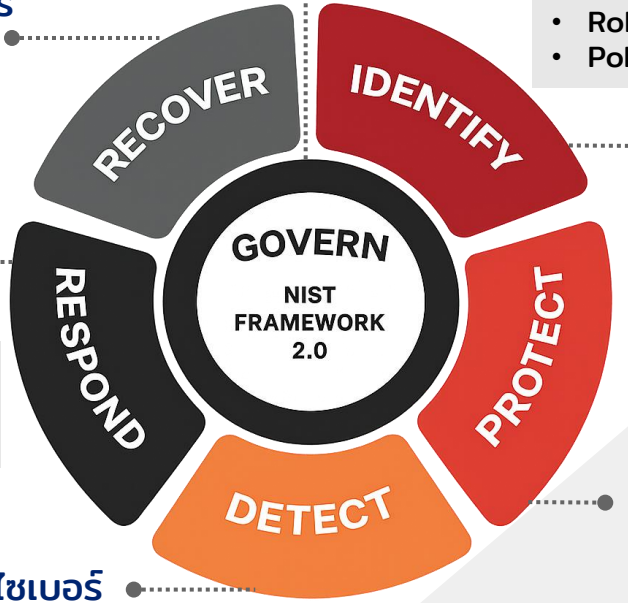
วัตถุประสงค์

- เสริมสร้างความสามารถในการป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูจากภัยคุกคามไซเบอร์
- สนับสนุนการบริหารความเสี่ยงด้านไซเบอร์ในระดับองค์กร
- ใช้ได้กับทุกภาคส่วน ทั้งภาครัฐ เอกชน และโครงสร้างพื้นฐานสำคัญ
- เชื่อมโยงความมั่นคงปลอดภัยไซเบอร์กับเป้าหมายทางธุรกิจและการกำกับดูแลกิจการ

การนำไปใช้

- ใช้เป็นกรอบอ้างอิงในการจัดทำนโยบาย Cybersecurity
- ใช้ประเมินระดับความพร้อม (Cybersecurity Maturity)
- ใช้เป็นกรอบจัดทำกระบวนการตอบสนองภัยคุกคามทางไซเบอร์
- ใช้ร่วมกับ SIEM, SOAR และ Incident Response Framework (เช่น NIST SP 800-61)

NIST CSF 2.0



การกำกับดูแลภายใต้บริบทของหน่วยงาน

- Organization Context
- Risk
- Roles
- Policy

การระบุทรัพย์สินและประเมินความเสี่ยงของหน่วยงาน

- การระบุทรัพย์สิน (Assets)
  - Data, Hardware, Software, People
- การประเมินความเสี่ยง (Risk)
  - Attack Surface Management (ASM)
  - Vulnerability Assessment (VA)

การใช้มาตรการป้องกันเพื่อบริหารจัดการความเสี่ยง

- Cryptography
- Multi-Factor Authentication
- Backup

การค้นหาและวิเคราะห์การโจมตีทางไซเบอร์

- Monitor System
  - Endpoint Detection and Response (EDR)
  - Network Detection and Response (NDR)
  - Threat Intel (TI)
  - Attack Surface Management (ASM)

SIEM

การตอบสนองเหตุการณ์โจมตีทางไซเบอร์

- Management System (MGMT)
- Analyze
  Mitigation

SOAR

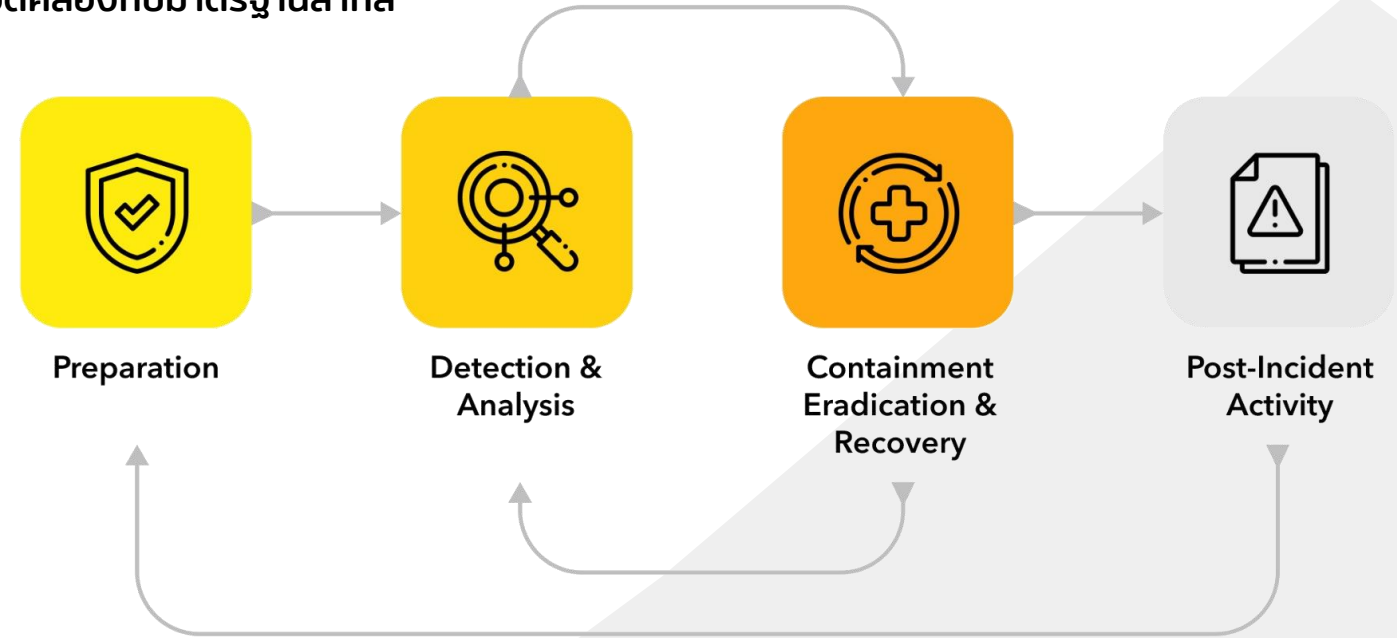
การฟื้นฟูระบบ บริการ และการดำเนินงานให้กลับสู่ภาวะปกติ

- Restore
- Verify
- Communication

NIST Incident Response Plan

คืออะไร ?

แผนการดำเนินงานที่กำหนดกระบวนการ ขั้นตอน และแนวทางในการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ เพื่อให้สามารถควบคุม แก้ไข และฟื้นฟูผลกระทบจากเหตุการณ์ได้อย่างมีประสิทธิภาพ และสอดคล้องกับมาตรฐานสากล



ที่มา : NIST Special Publication 800-61 Revision 2 Computer Security Incident Handling Guide (NIST SP 800-61 Rev. 2)

NIST Incident Response Plan

Preparation

1. การเตรียมความพร้อม

- จัดทำ Incident Response Policy และ Plan
- จัดตั้งทีม Incident Response
- จัดเตรียมเครื่องมือ เช่น SIEM, EDR, NDR, SOAR
- ฝึกอบรมบุคลากรและทดสอบแผนอย่างสม่ำเสมอ

Detection & Analysis

2. การตรวจจับและวิเคราะห์

- ตรวจจับเหตุการณ์จาก Log, Alert, Threat Intelligence
- วิเคราะห์และยืนยันว่าเป็น Incident หรือไม่
- ประเมินระดับความรุนแรงและผลกระทบ
- บันทึกเหตุการณ์และหลักฐานที่เกี่ยวข้อง

Containment Eradication & Recovery

3. การควบคุมเหตุการณ์

- จำกัดขอบเขตความเสียหาย เช่น แยกระบบที่ถูกโจมตี

การกำจัดสาเหตุ

- กำจัดมัลแวร์ ปิดช่องโหว่ แก้ไขการตั้งค่าที่ผิดพลาด

การฟื้นฟูระบบ

- กู้คืนระบบและข้อมูล
- ตรวจสอบให้ระบบกลับสู่สภาวะปกติอย่างปลอดภัย

Post-Incident Activity

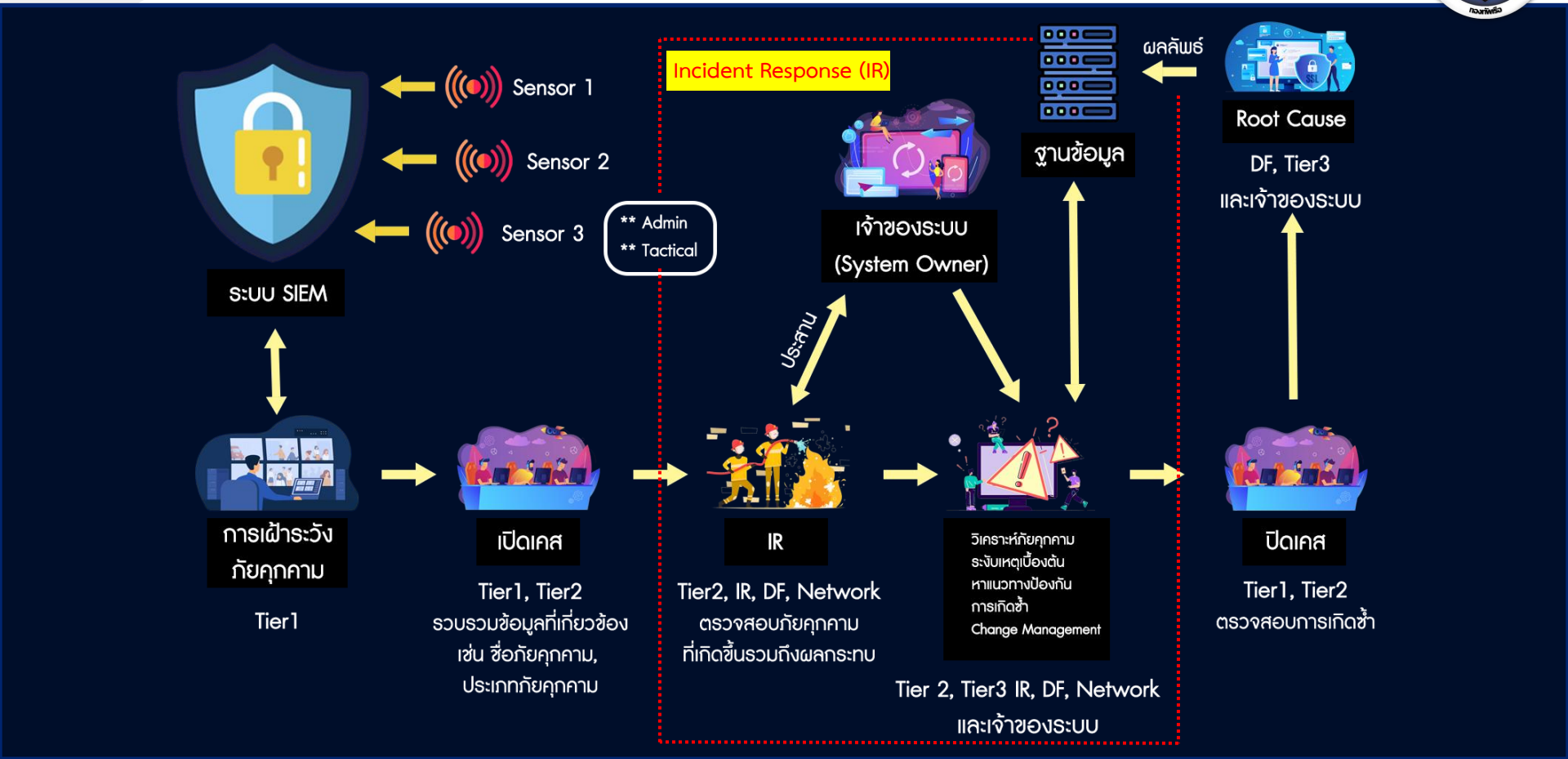
4. การดำเนินการหลังเหตุการณ์

- วิเคราะห์บทเรียนที่ได้รับ (Lessons Learned)
- ปรับปรุงแผนและกระบวนการตอบสนอง
- จัดทำรายงานสรุปเหตุการณ์
- เสริมมาตรการป้องกันเพื่อป้องกันเหตุซ้ำ

ศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

CSOC

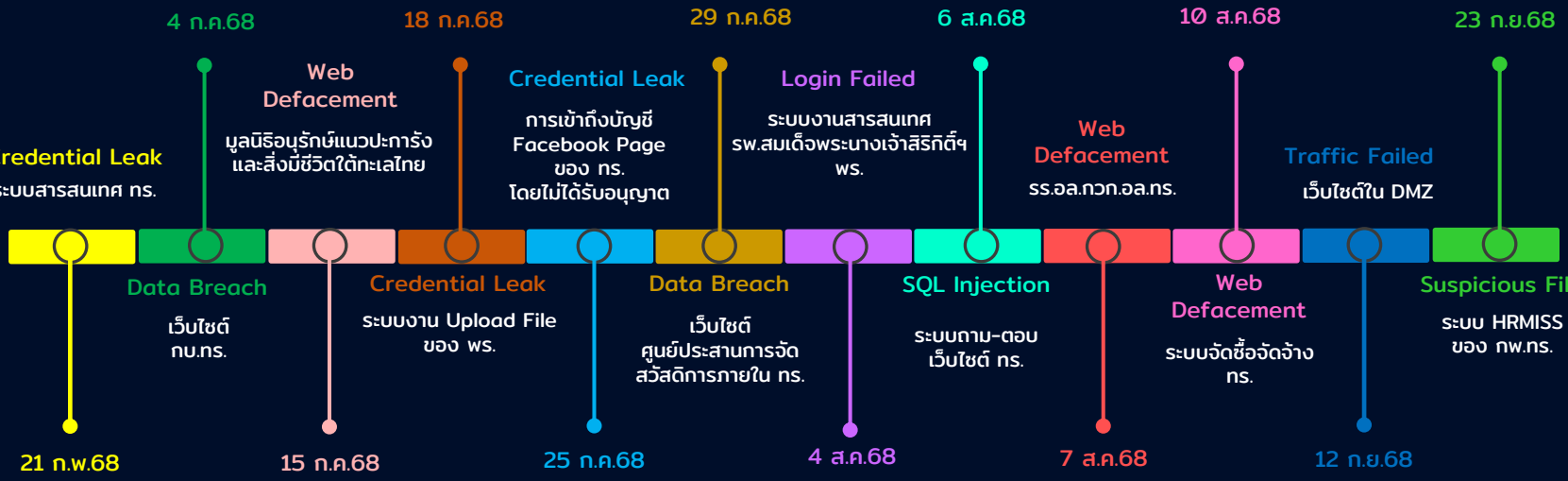
CSOC


Incident Response (IR)
Sensor 1
Sensor 2
Sensor 3
** Admin
** Tactical
ระบบ SIEM
การเฝ้าระวังภัยคุกคาม
Tier1
เปิดเคส
Tier1, Tier2
รวบรวมข้อมูลที่เกี่ยวข้อง
เช่น ชื่อภัยคุกคาม,
ประเภทภัยคุกคาม
ประสาน
เจ้าของระบบ
(System Owner)
IR
Tier2, IR, DF, Network
ตรวจสอบภัยคุกคาม
ที่เกิดขึ้นรวมถึงผลกระทบ
ฐานข้อมูล
วิเคราะห์ภัยคุกคาม
ระงับเหตุเบื้องต้น
หาแนวทางป้องกัน
การเกิดซ้ำ
Change Management
Tier 2, Tier3 IR, DF, Network
และเจ้าของระบบ
ผลลัพธ์
Root Cause
DF, Tier3
และเจ้าของระบบ
ปิดเคส
Tier1, Tier2
ตรวจสอบการเกิดซ้ำ

เหตุการณ์ภัยคุกคามทางไซเบอร์ที่สำคัญของ ทร.

เหตุการณ์ภัยคุกคามทางไซเบอร์ที่สำคัญของ ทร.

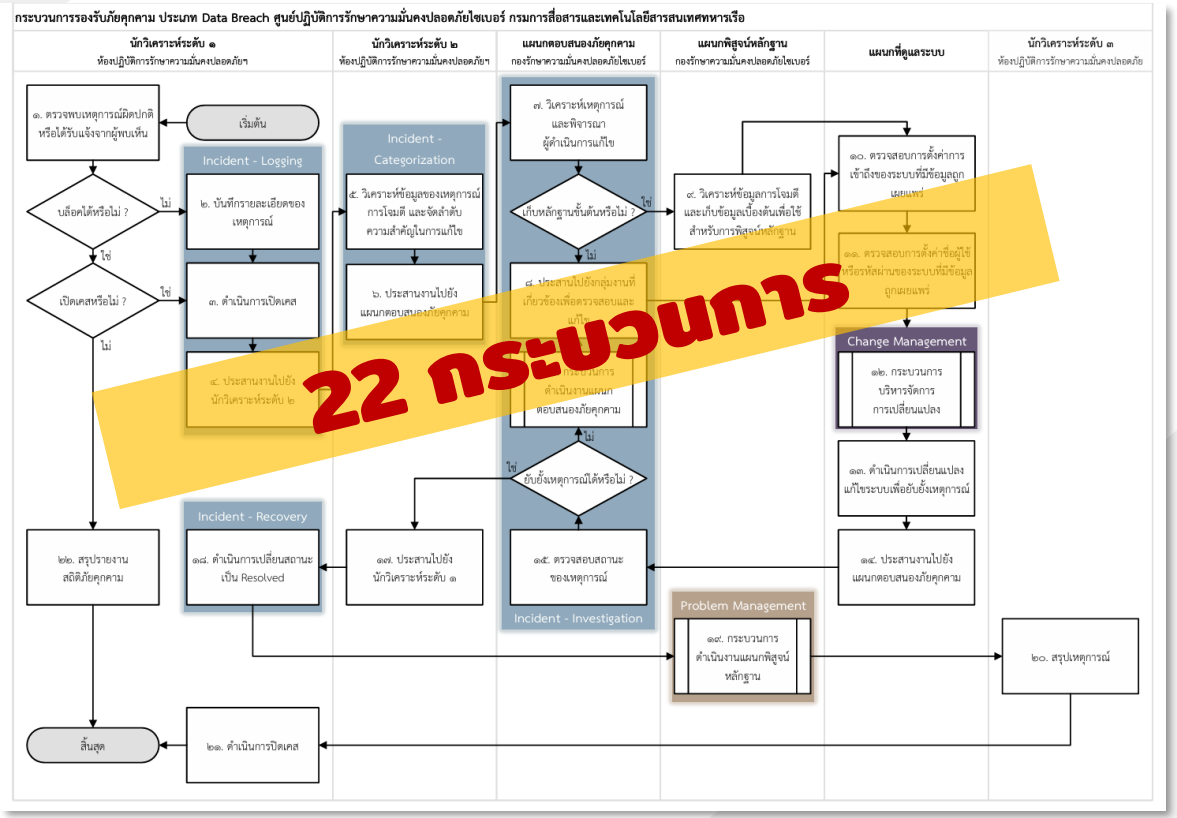
การตอบสนองภัยคุกคามด้านไซเบอร์ แก้ปัญหา กู้คืน ฟื้นฟูเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ จากภัยคุกคามไซเบอร์ โดยมีเหตุการณ์สำคัญ จำนวน 12 เหตุการณ์ ได้แก่



กระบวนการตอบสนองภัยคุกคามด้านไซเบอร์ของ ทร. (ปัจจุบัน)

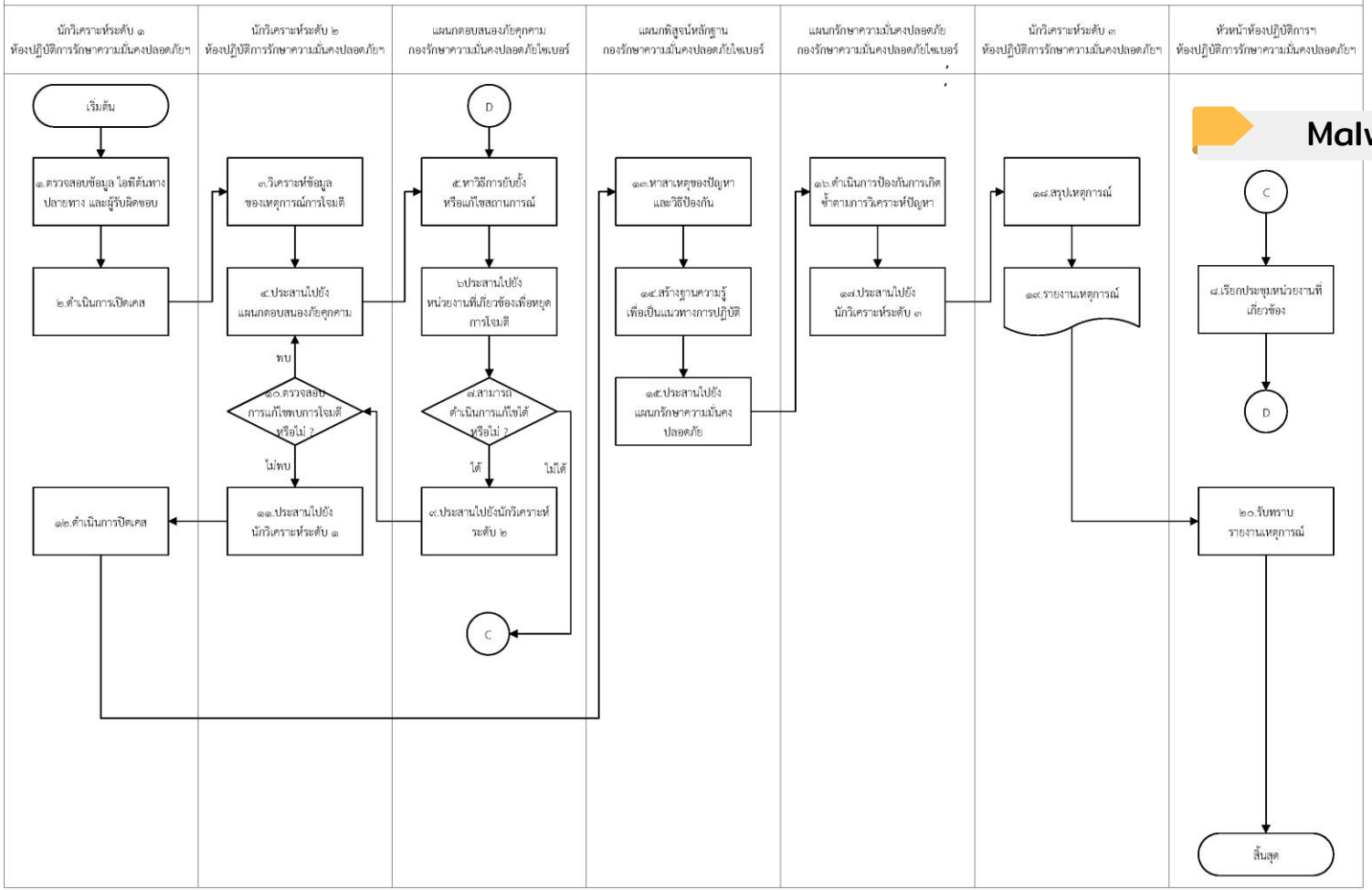
Incident Response Process

กระบวนการตอบสนองภัยคุกคามด้านไซเบอร์ของ ทร.



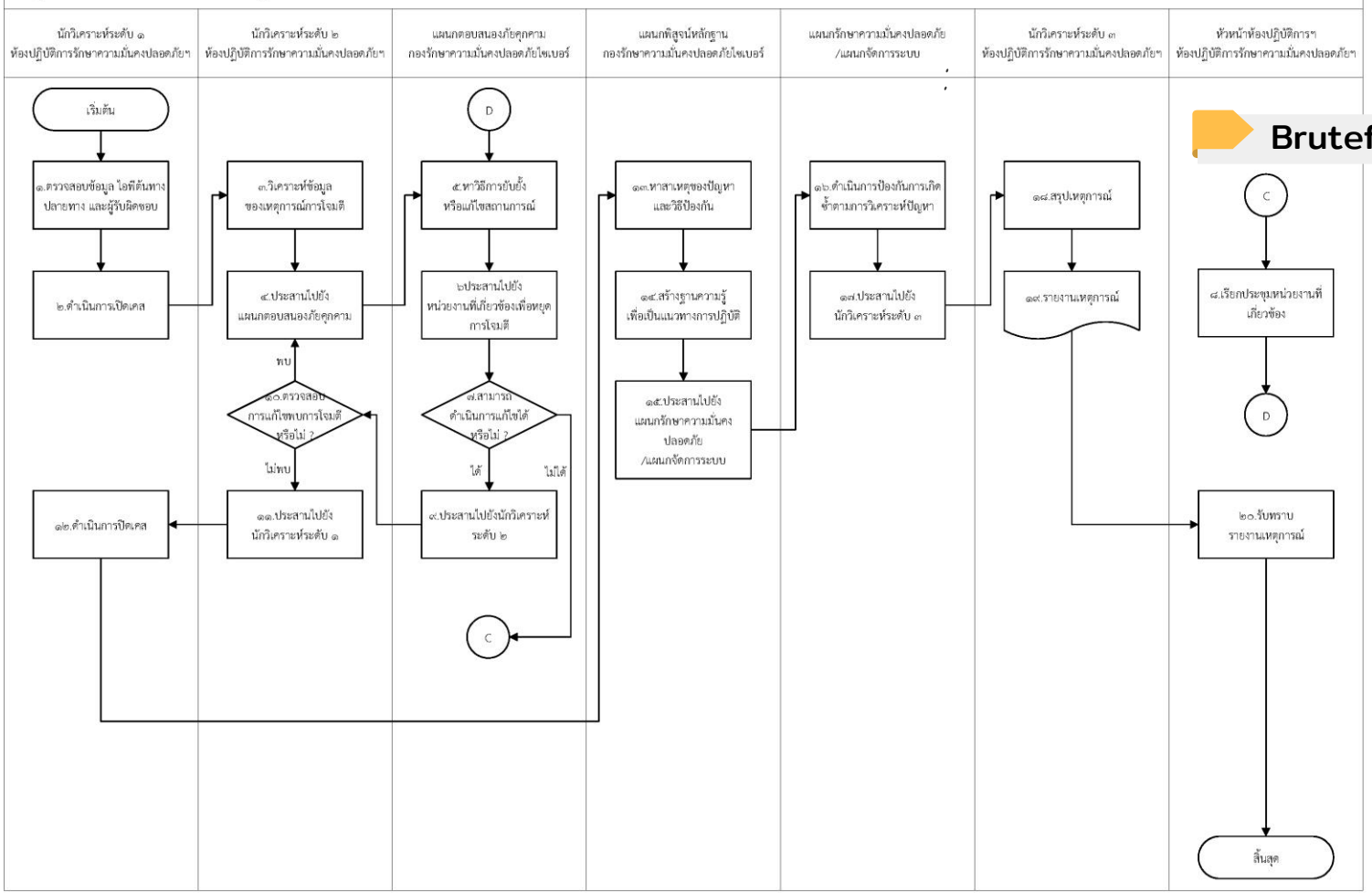
- Botnet
- Spam Mail
- Exploit
- Data Breach
- Ransomware
- Web Defacement
- Malware
- Phishing
- DoS & DDoS
- SQL Injection & Cross-Site Scripting (XSS)
- ...

กระบวนการรองรับภัยคุกคาม การโจมตีด้วยแรนซัมแวร์ (Ransomware)
ห้องปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ศูนย์ไซเบอร์ กรมสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ กองทัพเรือ



Malware

กระบวนการรองรับภัยคุกคาม การโจมตีด้วยวิธีการเดาสุ่ม Password (Brute Force)
ห้องปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ศูนย์ไซเบอร์ กรมสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ กองทัพเรือ



Bruteforce

(ร่าง) กระบวนการตอบสนองภัยคุกคามด้านไซเบอร์ของ ทร. (ใหม่)

Incident Response Process

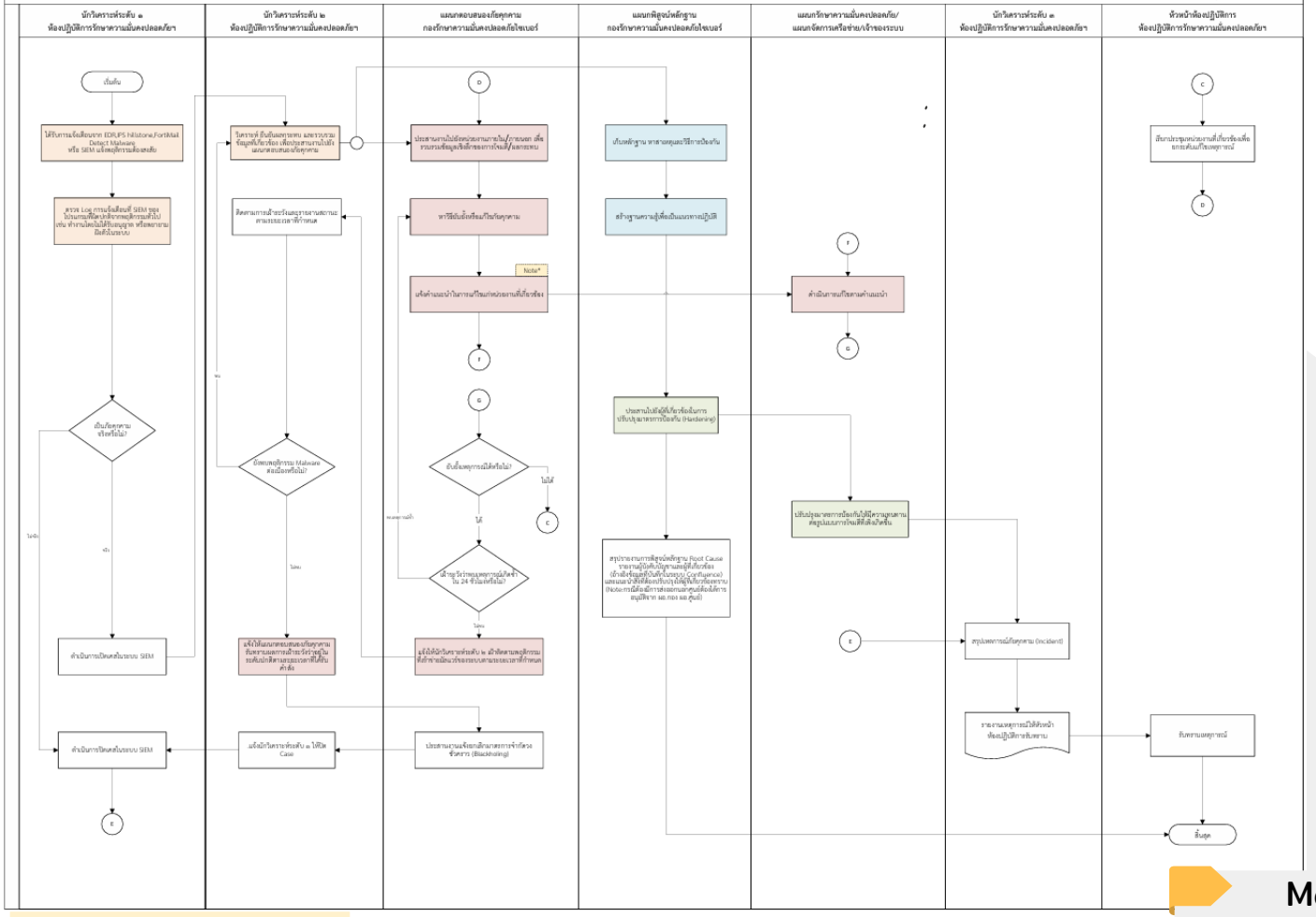
(ร่าง)กระบวนการตอบสนองภัยคุกคามทางไซเบอร์ของ ทร. (ใหม่)

Preparation	Detection & Analysis	Containment Eradication & Recovery	Post – Incident Activity
• ปรับปรุง (ร่าง) กระบวนการตอบสนองภัยคุกคามทางไซเบอร์ของ ทร. ให้สอดคล้องกับกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ NIST CSF 2.0	• ปรับเพิ่มเงื่อนไขหรือเหตุการณ์ (Trigger) ในการตรวจจับและวิเคราะห์เพื่อให้สามารถระงับ ยับยั้งเหตุการณ์ที่เกิดขึ้นได้ในทันที	• ปรับเพิ่มคำแนะนำในการวิเคราะห์เหตุการณ์ภัยคุกคามทางไซเบอร์เชิงลึกเพื่อให้สามารถดำเนินการตอบสนองภัยคุกคามที่เกิดขึ้นได้อย่างถูกต้องและมีประสิทธิภาพ • ปรับเพิ่มคำแนะนำในการตอบสนองภัยคุกคามทางไซเบอร์ เพื่อระงับ ยับยั้งเหตุการณ์ที่เกิดขึ้นได้อย่างรวดเร็ว	• ปรับเพิ่มการประสานงานและสื่อสารกับหน่วยงานภายนอก ภายหลังจากเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ได้รับการควบคุมและแก้ไขแล้ว เพื่อให้การดำเนินการเป็นไปตามกฎหมาย มาตรฐาน และข้อกำหนดที่เกี่ยวข้อง

กระบวนการรองรับภัยคุกคามการโจมตีรูปแบบ Malware
ห้องปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ศูนย์ไซเบอร์ กรมสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ กองทัพเรือ

Preparation | Detection & Analysis | Containment Eradication & Recovery | Post-Incident Activity

NIST Special Publication (SP) 800-61 Revision 2



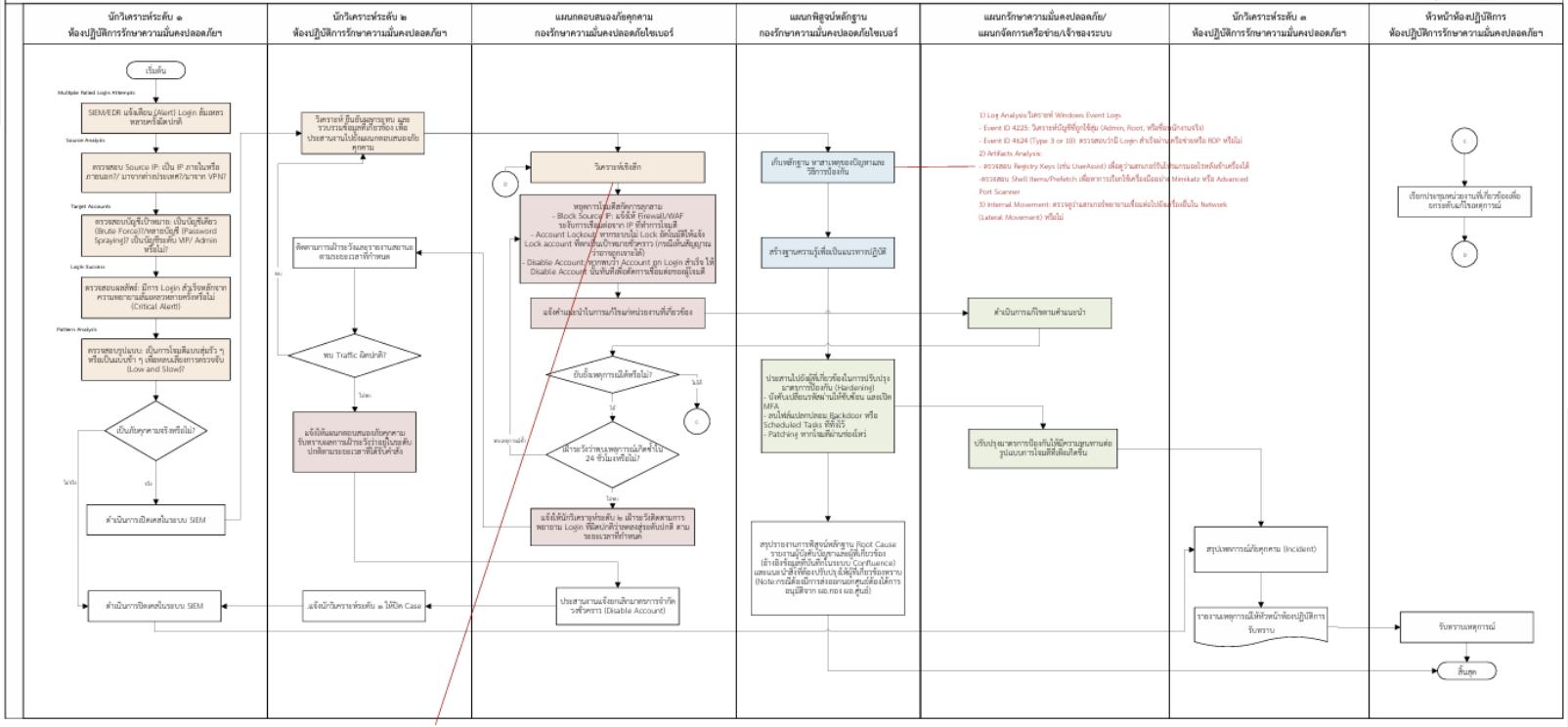
Note*
คำแนะนำเบื้องต้น (Endpoint / Server)
1) แยกเครื่องที่ตรวจพบเหตุออกจากเครือข่ายทันที
2) สแกนและกำจัดมัลแวร์ด้วยโปรแกรมป้องกันไวรัสหรือระบบ EDR อย่างละเอียด

Malware

กระบวนการรองรับภัยคุกคาม การโจมตีรูปแบบ Password Brute Force
ห้องปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ศูนย์ไซเบอร์ กรมสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ กองทัพเรือ

Preparation | Detection & Analysis | Containment Eradication & Recovery | Post-Incident Activity

NIST Special Publication (SP) 800-61 Revision 2



T2/T3 เพื่อหาว่าผู้โจมตีเข้ามาได้จุดไหน และมีการทำอะไรต่อหลังจากนั้นหรือไม่ ดังนี้

1) Source Analysis: (หาว่าใคร/ระไรทำสิ่งโจมตีเรา)

- **IP Reputation & Intelligence:** นำ Source IP ไปเช็คกับฐานข้อมูล TI (VirusTotal, AbuseIPDB, Talos) เพื่อดูว่า Known Malicious IP, Tor Exit Node หรือ Public Proxy หรือไม่?
- **User-Agent String:** หากเป็นการโจมตีผ่าน Web Portal เช่น M365, VPN Web Log ให้ตรวจสอบ User-Agent ใน Log (หากพบ User-Agent เป็น Library พื้นฐาน (python-requests, curl, Go-http-client) แสดงว่าเป็น Bot
- **Workstation Name:** ใน Windows Log (Event ID 4625) จะมีช่อง Source Network Address และ Workstation Name หากชื่อเครื่องไม่ตรงกับระบบของตน, และดูว่าเป็น การโจมตีจากภายนอก

2) วิเคราะห์พฤติการณ์การโจมตี (Attack Pattern Analysis)

2.1) Horizontal vs Vertical:

- Vertical: พยายามสุ่มรหัสผ่านกับ User เดียว
- Horizontal: ใช้รหัสผ่านชุดเดียวกับ User หลายคน (Password Spraying) ตรวจจับยากกว่า

2.2) Failed Login Sub-Status Codes: ใน Windows Event ID 4625 ให้ดูที่ **Status/Sub-Status Code** เพื่อการแยกแยะ:

- 0xC000006A: รหัสผ่านผิด (Correct username, wrong password) -> **เป็นการเดา**
- 0xC0000064: ไม่มีชื่อผู้ใช้นี้ (User does not exist) -> **ผู้เดาชื่อ User (Enumeration)**
- 0xC0000234: บัญชีถูกล็อก (User account locked out) -> **โจมตีจนระบบป้องกันทำงาน**

3) การตรวจสอบความสำเร็จและการเคลื่อนที่ (Success & Lateral Movement)

หากพบว่ามีการ "Login Success" (Event ID 4624) เกิดขึ้นหลังจาก Failed Login จำนวนมาก ต้องรีบเช็คต่อทันที:

3.1) Login Type: ตรวจสอบว่าเป็นการ Login รูปแบบใดบน

- Type 2: Interactive (พนักงานเรือ)
- Type 3: Network (เช่น การ Map Drive หรือเข้าถึง Resource ผ่านระบบเครือข่าย)
- Type 10: Remote Interactive (RDP) -> **เป็นอันตราย**

3.2) Time Correlation: หลังจาก Login สำเร็จแล้วมีกิจกรรมที่ Process ที่ผิดปกติหรือไม่? (ตรวจสอบผ่าน EDR/Sysmon)

- ตัวอย่าง: มีการใช้ whoami, net user, ipconfig หรือ mimikatz หรือไม่?

- **New Account Creation:** มีการพยายามสร้างบัญชี Admin ใหม่ (Event ID 4720) เพื่อใช้เป็นทางหลัง (Backdoor) หรือไม่?

Bruteforce

กลุ่มสัมมนา

แนวทางการจัดทำกระบวนการตอบสนองภัยคุกคามทางไซเบอร์ ของ ทร.

วัตถุประสงค์

- เพื่อศึกษา วิเคราะห์ และเปรียบเทียบกระบวนการตอบสนองภัยคุกคามทางไซเบอร์ของ ทร. (ปัจจุบัน) กับ (ร่าง) กระบวนการตอบสนองภัยคุกคามทางไซเบอร์ของ ทร. (ใหม่) ตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ NIST CSF 2.0
- เพื่อปรับปรุงกระบวนการตอบสนองภัยคุกคามทางไซเบอร์ของ ทร. ให้สอดคล้องกับบริบทรองรับการปฏิบัติงานจริงและมีประสิทธิภาพ
- เพื่อให้กระบวนการตอบสนองภัยคุกคามทางไซเบอร์ของ ทร. สามารถนำไปปรับใช้กับ นขต.ทร. ได้

ข้อมูลประกอบการสัมมนา

- เอกสารประกอบการบรรยาย
  - NIST Cybersecurity Framework 2.0
  - NIST Incident Response Plan
- ตัวอย่าง กระบวนการตอบสนองภัยคุกคามทางไซเบอร์ของ ทร. (ปัจจุบัน) จำนวน 2 กระบวนการ ได้แก่
  - กระบวนการตอบสนองภัยคุกคามประเภท Malware
  - กระบวนการสอบสนองภัยคุกคามประเภท Bruteforce
- ตัวอย่าง (ร่าง) กระบวนการตอบสนองภัยคุกคามทางไซเบอร์ของ ทร. (ใหม่) จำนวน 2 กระบวนการ ได้แก่
  - กระบวนการตอบสนองภัยคุกคามประเภท Malware
  - กระบวนการสอบสนองภัยคุกคามประเภท Bruteforce

ผลการสัมมนา

Preparation	Detection & Analysis	Containment Eradication & Recovery	Post – Incident Activity

ผลการสัมมนาพิจารณา
(ร่าง) กระบวนการตอบสนองภัยคุกคามฯ

ข้อคิดเห็นและข้อเสนอแนะ

- ข้อคิดเห็น
- ข้อเสนอแนะ

ผลการสัมมนา
ข้อคิดเห็นและข้อเสนอแนะ

จบการบรรยาย

Q & A