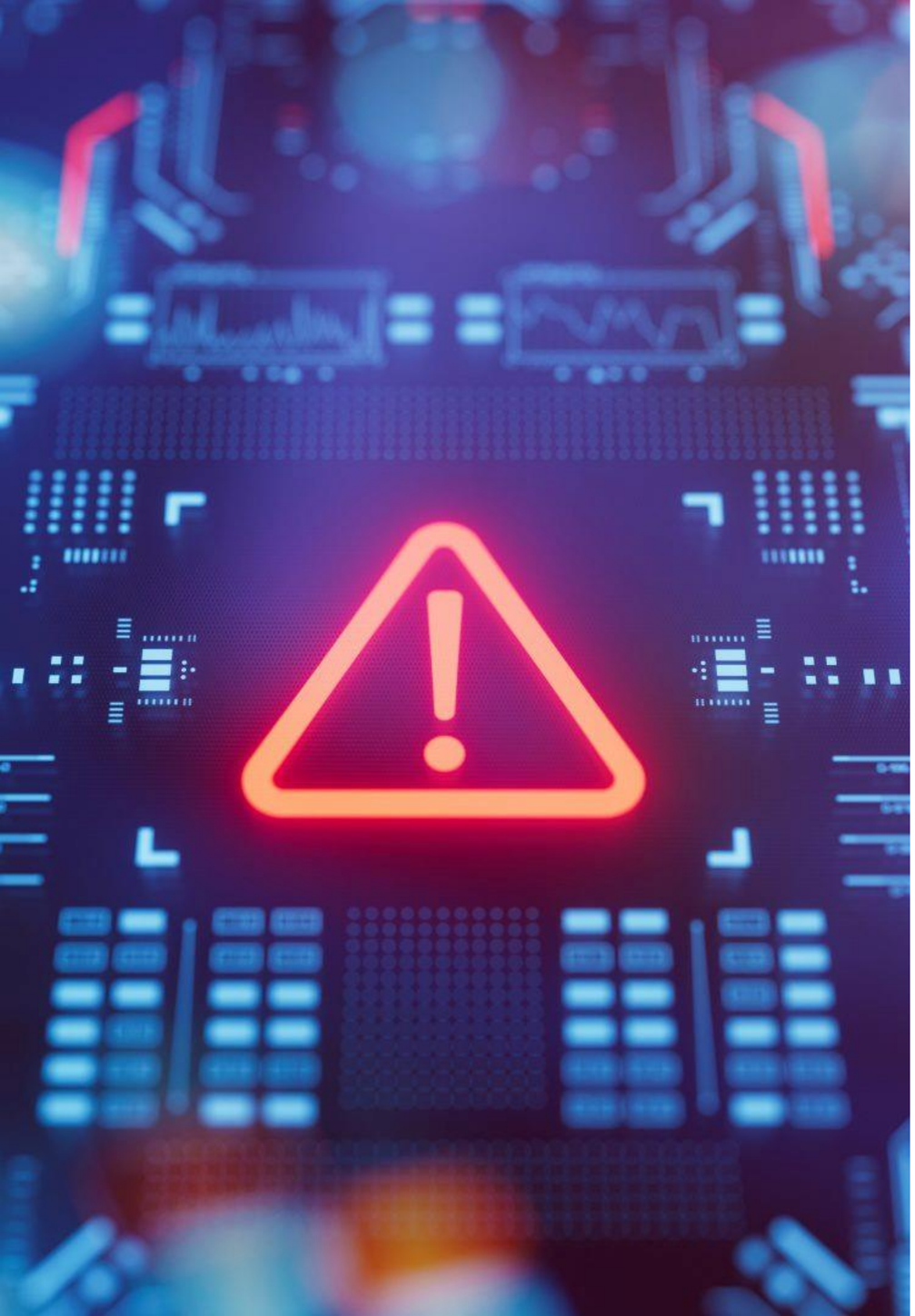
ACTION PLAN FOR INCIDENT RESPONSE: PLANS, STEP, TEAM AND TOOLS

PRESENTATION

แผนเผชิญและรับมือกับเหตุถูกโจมตี ถูกคุกคามทางไซเบอร์ อย่างฉุกเฉิน เร่งด่วน และรอบด้านนั้น จากตัวอย่างจริง ทำอย่างไร

https://www.ncsa.or.th

https://www.facebook.com/NCSA.Thailand

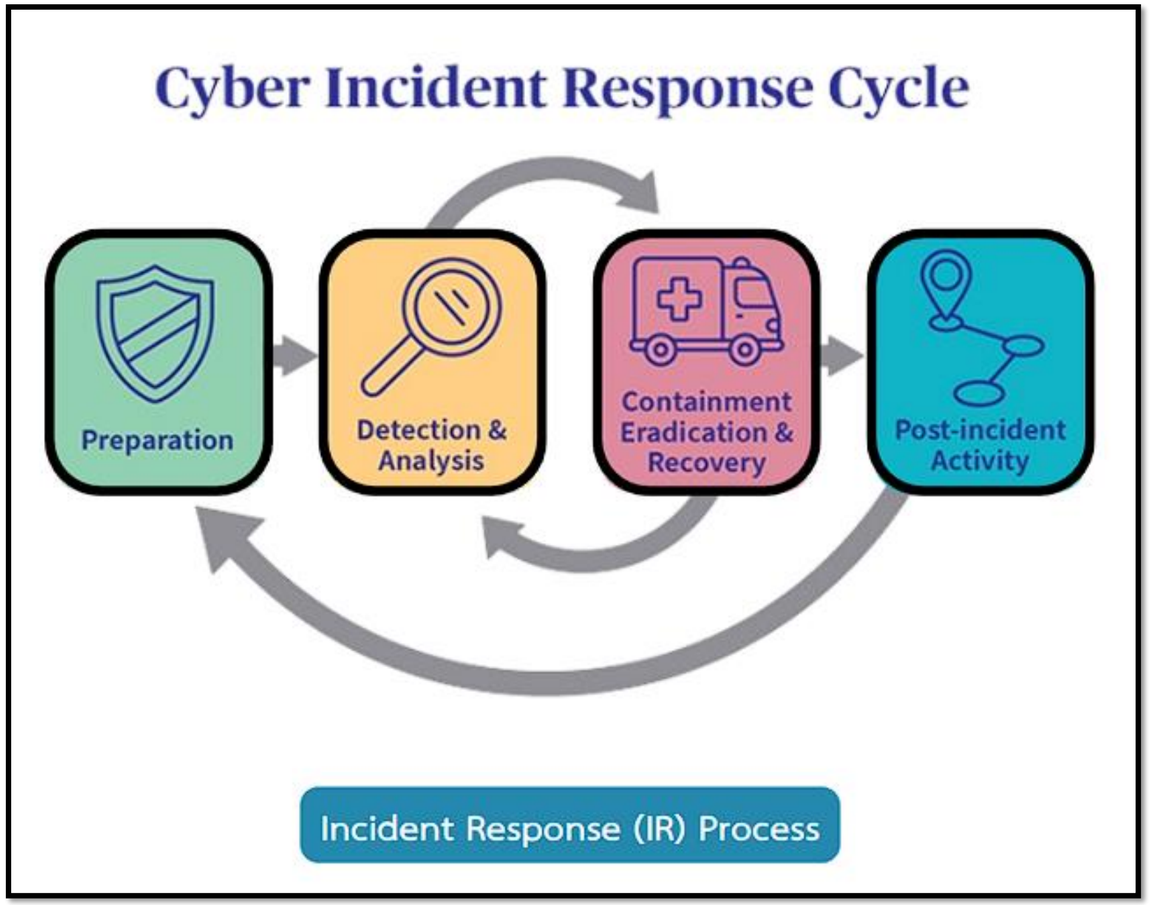


แผนการดำเนินการตอบสนองต่อเหตุการณ์ (Incident Response Action Plan)

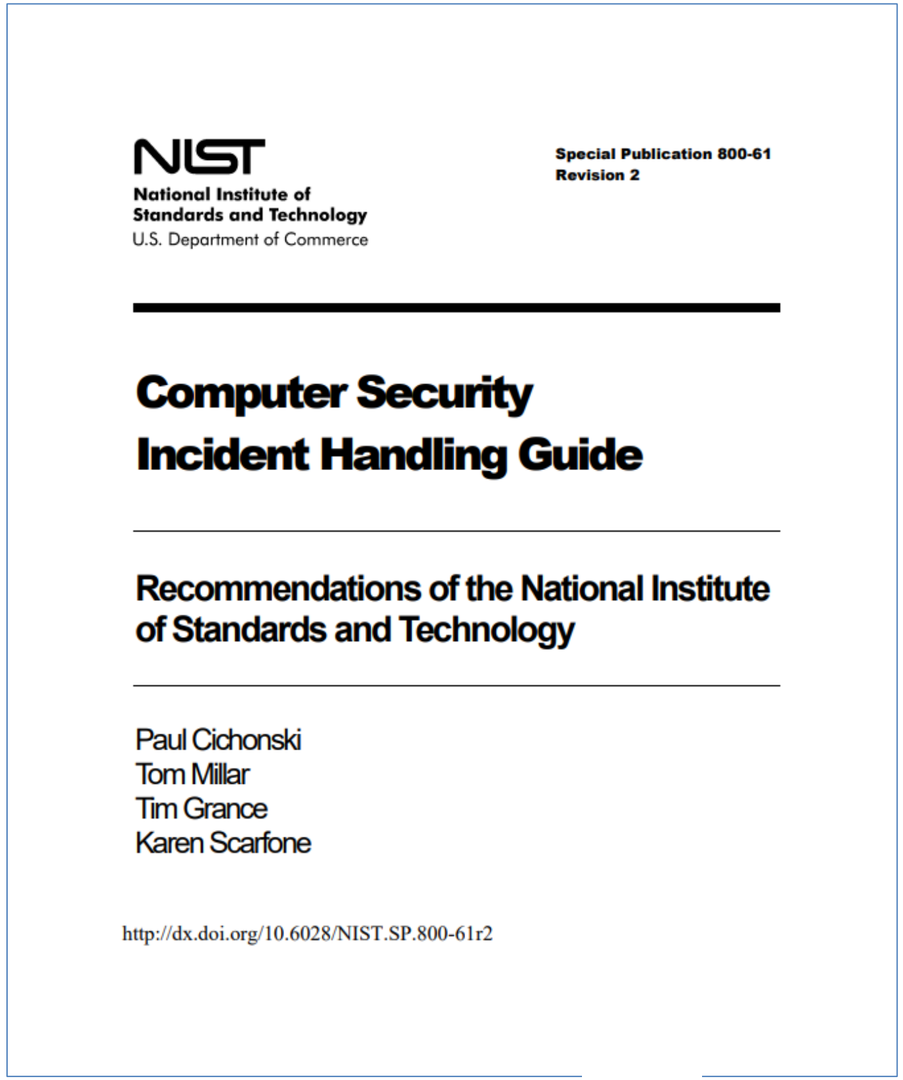
ในยุคดิจิทัลที่เต็มไปด้วยภัยคุกคามทางไซเบอร์ ภัยพิบัติทางธรรมชาติ และอุบัติเหตุต่างๆ องค์กรต่างๆ จำเป็นต้องมีแผนการดำเนินการตอบสนองต่อเหตุการณ์ (Incident Response Action Plan) ที่ครอบคลุม รอบด้าน เพื่อรับมือกับสถานการณ์ฉุกเฉินเหล่านี้ แผนดังกล่าวจะช่วยให้องค์กรสามารถระบุ ควบคุม ฟื้นฟู วิเคราะห์ และจัดทำเอกสารเกี่ยวกับเหตุการณ์ได้อย่างมีประสิทธิภาพ ลดความเสียหาย และปกป้องข้อมูลและระบบขององค์กร

Action Plan สำหรับการทำ Incident Response ครบถ้วน รอบด้าน มีขั้นตอนอะไรบ้าง อย่างไร

กระบวนการตอบสนองและรับมือภัยคุกคามทางไซเบอร์



NIST SP 800 – 61 **Computer Security Incident Handling Guide**



NIST SP 800 – 61 **Rev 2**

PROJECTS

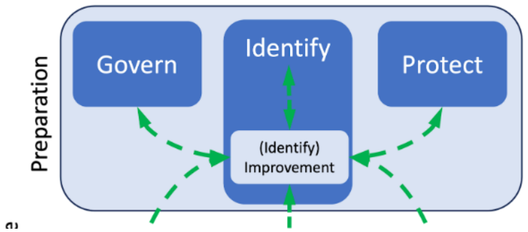
Incident Response

Overview

NIST has released a new draft of Special Publication (SP) 800-61 Revision 3 for public comment! Your comments on *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile* are welcome through May 20, 2024.

NIST SP 800-61 Revision 3 seeks to assist organizations with incorporating cybersecurity incident response recommendations and considerations throughout their cybersecurity risk management activities as described by the NIST Cybersecurity Framework (CSF) 2.0. Doing so can help organizations prepare for incident responses, reduce the number of incidents that occur and the impact of the incidents that occur, and improve the efficiency and effectiveness of their incident detection, response, and recovery activities. Once this publication is finalized, it will supersede SP 800-61 Revision 2, *Computer Security Incident Handling Guide*.

The new incident response life cycle model used in this publication is shown in the figure. The top half reflects that the preparation activities in Govern, Identify, and Protect are not part of the incident response life cycle; they are much broader cybersecurity risk management activities that also support incident response. The new response life cycle for each incident is shown in the bottom half of the figure: Detect, Respond, and Recover. Finally, the need for continuous improvement is indicated by the Improvement Category within the Identify Function and the dashed green lines. Lessons learned from performing all activities in all Functions are fed into Improvement, and those lessons learned are analyzed and prioritized, then used to inform all the Functions.



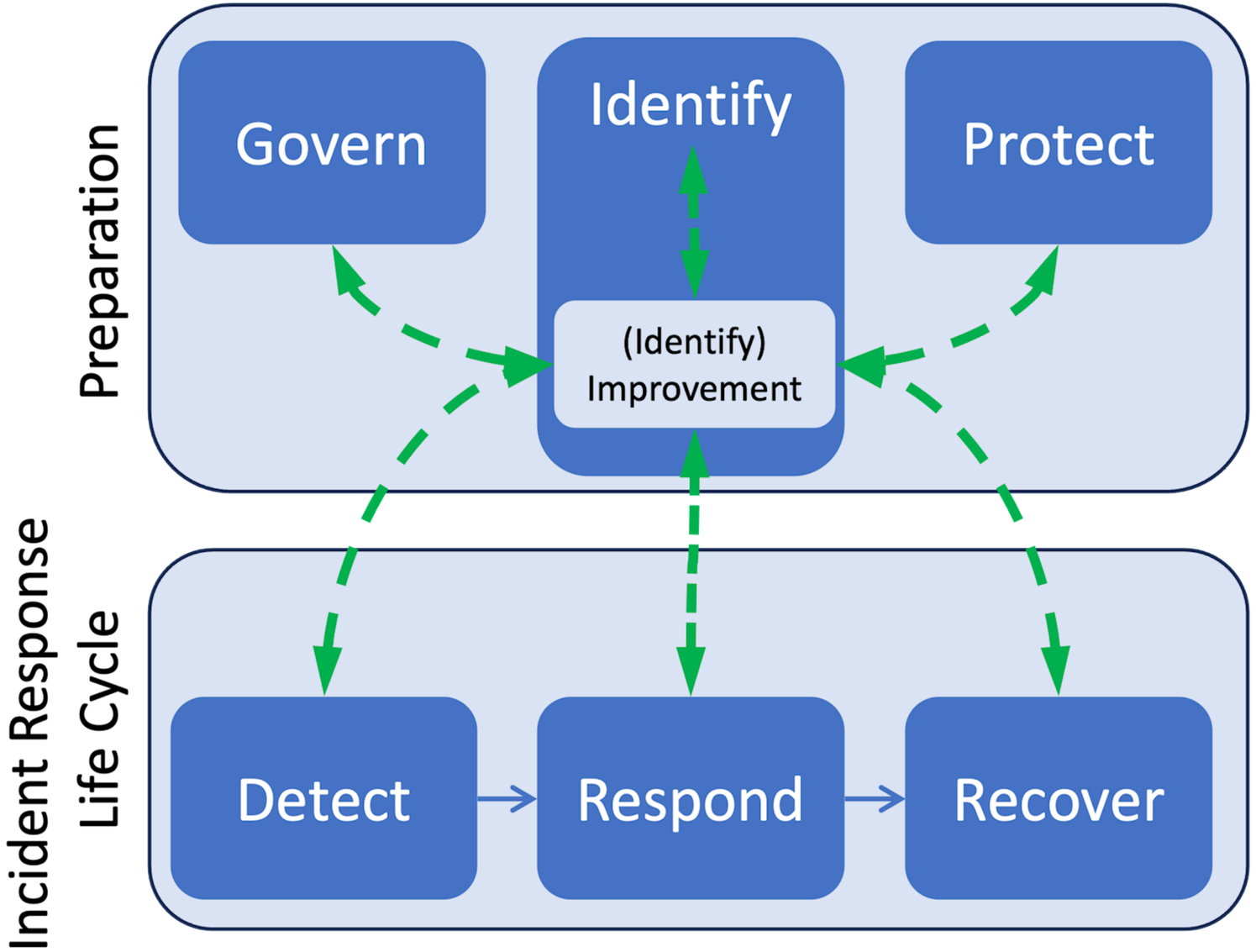
PROJECT LINKS
Overview
News & Updates
Publications
ADDITIONAL PAGES
Preparation Resources
Life Cycle Resources

GROUP
Security Components and Mechanisms

TOPICS
Security and Privacy: incident response, threats, vulnerability management
Applications: cybersecurity framework, forensics

RELATED PROJECTS
Cybersecurity Framework
Log Management
Mobile Forensics
National Vulnerability Database
Ransomware Protection and Response

NIST SP 800-61 Revision 3 seeks to assist organizations with incorporating cybersecurity incident response recommendations and considerations throughout their cybersecurity risk management activities as described by the NIST Cybersecurity Framework (CSF) 2.0. Doing so can help organizations prepare for incident responses, reduce the number of incidents that occur and the impact of the incidents that occur, and improve the efficiency and effectiveness of their incident detection, response, and recovery activities. Once this publication is finalized, it will supersede SP 800-61 Revision 2, Computer Security Incident Handling Guide.



The new incident response life cycle model used in this publication is shown in the figure. The top half reflects that the preparation activities in Govern, Identify, and Protect are not part of the incident response life cycle; they are much broader cybersecurity risk management activities that also support incident response. The new response life cycle for each incident is shown in the bottom half of the figure: Detect, Respond, and Recover. Finally, the need for continuous improvement is indicated by the Improvement Category within the Identify Function and the dashed green lines. Lessons learned from performing all activities in all Functions are fed into Improvement, and those lessons learned are analyzed and prioritized, then used to inform all the Functions.

https://csrc.nist.gov/pubs/sp/800/61/r3/ipd

NIST

Search CSRC

CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

PUBLICATIONS

NIST SP 800-61 Rev. 3 (Initial Public Draft)

Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile

Date Published: April 3, 2024

Comments Due: May 20, 2024 (public comment period is CLOSED)

Email Questions to: 800-61-comments@nist.gov

Author(s)

Alexander Nelson (NIST), Sanjay Rekhi (NIST), Murugiah Souppaya (NIST), Karen Scarfone (Scarfone

DOCUMENTATION

Publication:

https://doi.org/10.6028/NIST.SP.800-61r3.ipd

Download URL

กระบวนการตอบสนองและรับมือภัยคุกคามทางไซเบอร์

การเตรียมความพร้อม (Preparation)

1. การจัดเตรียมเครื่องมือและสิ่งอำนวยความสะดวกในการสื่อสารของบุคลากรผู้ทำหน้าที่รับมือ และตอบสนองต่อเหตุภัยคุกคามทางไซเบอร์
2. อุปกรณ์และซอฟต์แวร์สำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์
3. แหล่งข้อมูลในการวิเคราะห์เหตุภัยคุกคามทางไซเบอร์
4. ซอฟต์แวร์สำหรับการบรรเทาเหตุภัยคุกคาม เช่น ไฟล์ disk image ของระบบปฏิบัติการ (OS) และ แอปพลิเคชัน (Application) เพื่อใช้ในการกู้คืนและฟื้นฟูระบบ

Step #1: Preparation

No organization can spin up an effective incident response on a moment's notice. A plan must be in place to both prevent and respond to events.

Define the CSIRT (Computer Security Incident Response Team)

To act quickly and completely while an incident is unfolding, everyone on the CSIRT needs to know their responsibilities and the decisions that are theirs to make.

The CSIRT should include a cross section of business and technical experts with the authority to take action in support of the business. Members should include representatives from management, technical, legal, and communications disciplines, as well as security committee liaisons. All departments affected by an incident should be in the loop and everyone should have a decision matrix to guide their actions during and after the incident.

The plan should also define who is in charge and who has the authority to make certain critical decisions. Those aren't things to figure out–let alone argue over–in the heat of the moment.

Develop and update a plan

Ensure plans and other supporting documents exist and are updated periodically to remain current. All relevant personnel should have access to the parts of the plan that pertain to their responsibilities and should be alerted when the plan is revised. There should be a feedback loop that is enacted after every significant incident in order to improve the plan continuously.

Step #1: Preparation *(cont.)*

Acquire and Maintain the Proper Infrastructure and Tools

Have the capabilities to detect and investigate incidents, as well as to collect and preserve evidence. To determine if an attacker is in your environment, it's critical that you have endpoint security technology that provides total visibility into your endpoints and collects incident data.

Without the right tools, and processes to guide their use, you'll be ill-equipped to investigate how attackers are accessing your environment, how to mitigate an attacker's existing access, or how to prevent future access.

Always Improve Skills and Support Training

Ensure the IR team has the appropriate skills and training. This includes exercising the IR plan from time to time. It also includes staffing the IR team, with either in-house staff or through a third-party provider, to accommodate the time away from the job necessary in order to maintain certifications and leverage other educational opportunities.

Possess Up-to-Date Threat Intelligence Capabilities

Threat intelligence capabilities help an organization understand the kinds of threats it should be prepared to respond to. Threat intelligence should integrate seamlessly into endpoint protection and use automated incident investigations to speed breach response. Automation enables a more comprehensive analysis of threats in just minutes, not hours, so an organization can outpace advanced persistent threats (APTs) with smarter responses.

กระบวนการตอบสนองและรับมือภัยคุกคามทางไซเบอร์

การตรวจจับและวิเคราะห์ (Detection & Analysis)

1. การกำหนดจุด และวิธีการที่จะใช้ในการตรวจจับ Incident
2.การวิเคราะห์เหตุภัยคุกคามหรือความผิดปกติ
3.การบันทึกข้อมูลเหตุการณ์ภัยคุกคาม
4.การวิเคราะห์ผลกระทบ และการจัดลำดับความสำคัญของ Incident
5.การติดต่อประสานงาน และแจ้งข้อมูลให้กับบุคลากรด้านอื่นๆ

Step #2. Detection & Analysis

The second phase of IR is to determine whether an incident occurred, its severity, and its type. NIST outlines five steps within this overall phase:

- **Pinpoint signs of an incident (precursors and indicators):** Precursors and indicators are specific signals that an incident is either about to occur, or has already occurred.
- **Analyze the discovered signs:** Once identified, the IR team has to determine if a precursor or indicator is part of ar attack or if it is a false positive.
- **Incident documentation:** If the signal proves valid, the IR team must begin documenting all facts in relation to the incident and continue logging all actions taken throughout the process.
- **Incident prioritization:** NIST designates this step as the most critical decision point in the IR process. The IR team can't simply prioritize incidents on a first come, first serve basis. Instead, they must score incidents on the impact it will have on the business functionality, the confidentiality of affected information, and the recoverability of the incident.
- **Incident notification:** After an incident has been analyzed and prioritized, the IR team should notify the appropriate departments/individuals. A thorough IR plan should already include the specific reporting requirements.

กระบวนการตอบสนองและรับมือภัยคุกคามทางไซเบอร์

การควบคุมความเสียหายการจำกัด แก้ไข ภัยคุกคามและการกู้คืน (Containment, Eradication & Recovery)

1. ปิดระบบ (Shut Down)
2. ตัดการเชื่อมต่อทางเครือข่ายทั้งหมด (Network disconnection)
3. หยุดการทำงานของฟังก์ชันที่เกี่ยวข้อง (Disabling Certain Functions)
4. Redirect Network Traffic และ/หรือความสนใจของผู้บุกรุกไปยัง Blackhole / Sandbox / Honeypot

Step #3. Containment, Eradication, & Recovery

The purpose of the containment phase is to halt the effects of an incident before it can cause further damage. Once an incident is contained, the IR team can take the time necessary to tailor its next steps. These should include taking any measures necessary to address the root cause of the incident and restore systems to normal operation.

Develop containment, eradication, and recovery strategies based on criteria such as:

- the criticality of the affected assets
- the type and severity of the incident
- the need to preserve evidence
- the importance of any affected systems to critical business processes
- the resources required to implement the strategy

กระบวนการตอบสนองและรับมือภัยคุกคามทางไซเบอร์

การดำเนินการหลังจากการรับมือ และตอบสนองต่อภัยคุกคามทางไซเบอร์เสร็จสิ้น (Post-Incident Activity)

ทีมรับมือและผู้ที่เกี่ยวข้องทั้งหมดควรมีการประชุมหารือเพื่อแลกเปลี่ยนข้อมูลความคิดเห็น ในการนำไปพัฒนาปรับปรุงแนวทางในการรับมือ และตอบสนองต่อภัยคุกคามทางไซเบอร์

Step #4. Post-Incident Activity

Every incident should be an opportunity to learn and improve, but many organizations give short shrift to this step. Adversaries are always evolving, and IR teams need to keep up with the latest techniques, tactics, and procedures.

A lessons learned meeting involving all relevant parties should be mandatory after a major incident and desirable after less severe incidents with the goal of improving security as a whole and incident handling in particular. In the case of major attacks, involve people from across the organization as necessary and make a particular effort to invite people whose cooperation will be needed during future incidents.

During the meeting, review:

- what happened and when
- how well the IR team performed
- what information was missing when it was needed
- what actions slowed recovery
- what could be done differently
- what can be done to prevent future incidents
- what precursors or indicators can be looked for in the future

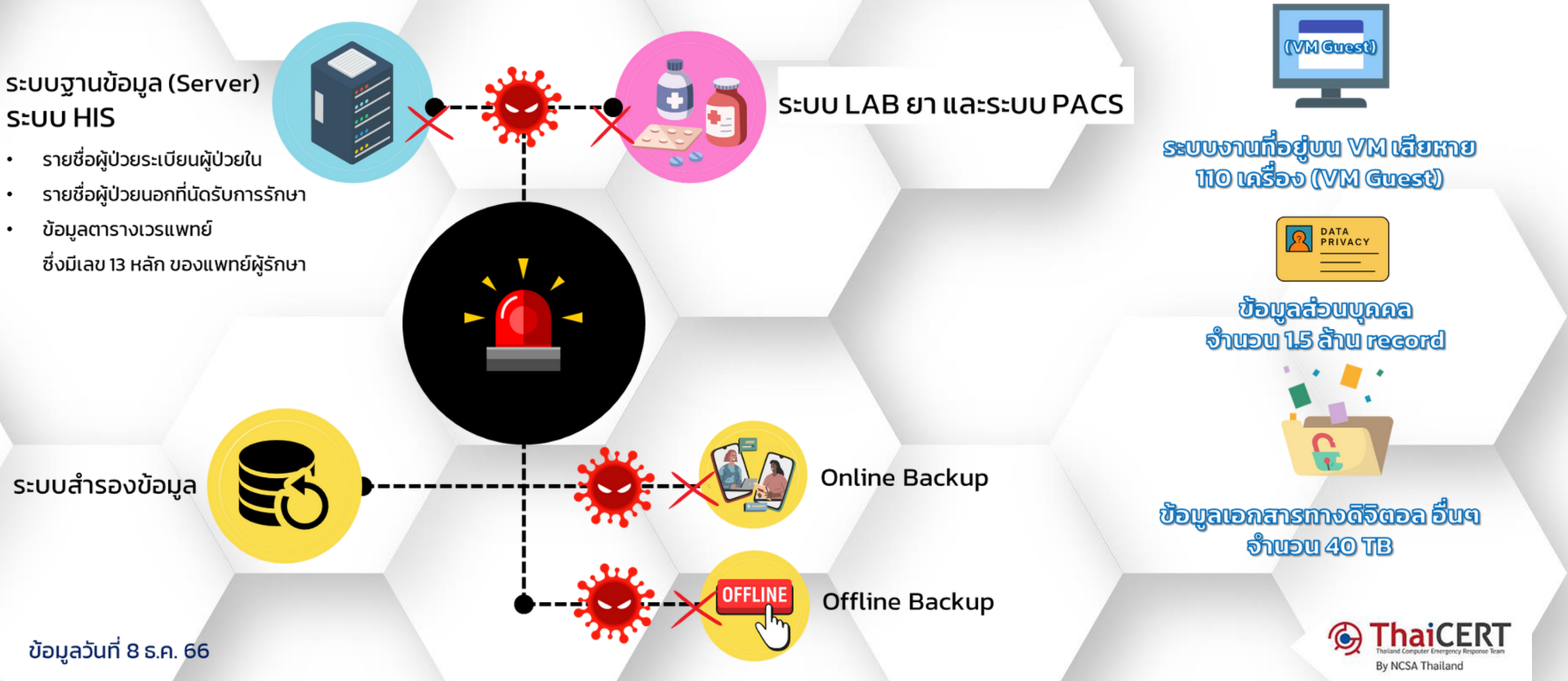
The results of these meetings can become an important training tool for new hires. They can also be used to update policies and procedures and create institutional knowledge that can be useful during future incidents.

Function	Category	Category
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

ตัวอย่างเหตุการณ์ โรงพยาบาลแห่งหนึ่ง Ransomware

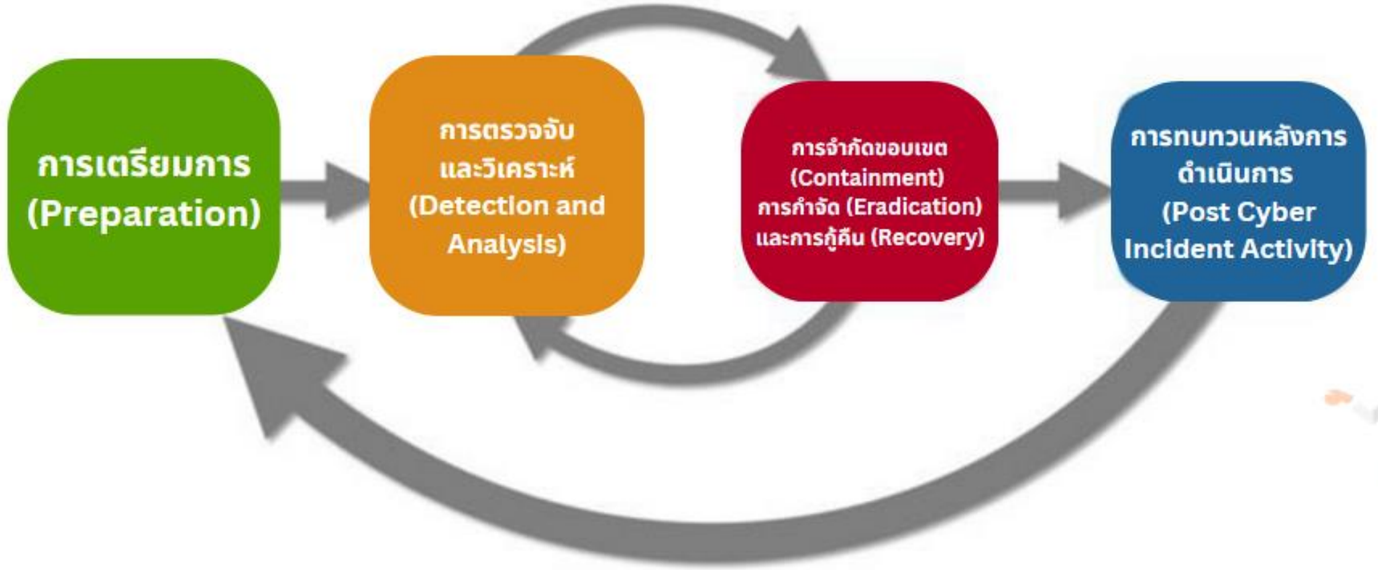
EXAMPLE

เมื่อวันที่ 9 ธ.ค.66 หน่วยงานรัฐด้านสาธารณสุข เผชิญเหตุการณ์ร้ายแรง เมื่อระบบเครือข่ายถูกบุกรุกและโจมตีด้วย Ransomware ส่งผลให้ระบบงานสำคัญและระบบสำรองข้อมูลได้รับความเสียหายทั้งหมด เหตุการณ์นี้สร้างความเสียหายร้ายแรงต่อข้อมูลผู้ป่วย ข้อมูลการรักษา และข้อมูลอื่นๆ อีกมากมายถูกบุกรุกเครือข่าย และโจมตีระบบงานต่างๆ ด้วย Ransomware ส่งผลให้ระบบงานสำคัญระบบสำรองข้อมูลได้รับความเสียหายทั้งหมด ข้อมูลที่ได้รับผลกระทบ ได้แก่ ระบบเวชระเบียน ประกอบด้วย รายชื่อผู้ป่วยระเบียนผู้ป่วยใน รายชื่อผู้ป่วยนอกที่นัดรับการรักษา ข้อมูลตารางเวรแพทย์ซึ่งมีเลข 13 หลักของแพทย์ผู้รักษา ระบบ Lab ยา และระบบ PACS ระบบสำรองข้อมูลรูปแบบออนไลน์ และออฟไลน์ ซึ่งทำให้เกิดความเสียหายกับระบบที่อยู่บน VM Guest 110 เครื่อง ข้อมูลส่วนบุคคล จำนวน 1.5 ล้าน Record และข้อมูลเอกสารทางดิจิทัล อื่น ๆ จำนวน 40 TB



กรอบการรับมือเหตุภัยคุกคามทางไซเบอร์ (Incident Response Framework)

ประกอบด้วย 4 ขั้นตอนเพื่อให้แน่ใจว่ามีแนวทางที่สอดคล้องกันและเป็นระบบ (Consistent and Systematic Approach) โดยเทียบเคียงกับประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 ได้ดังนี้

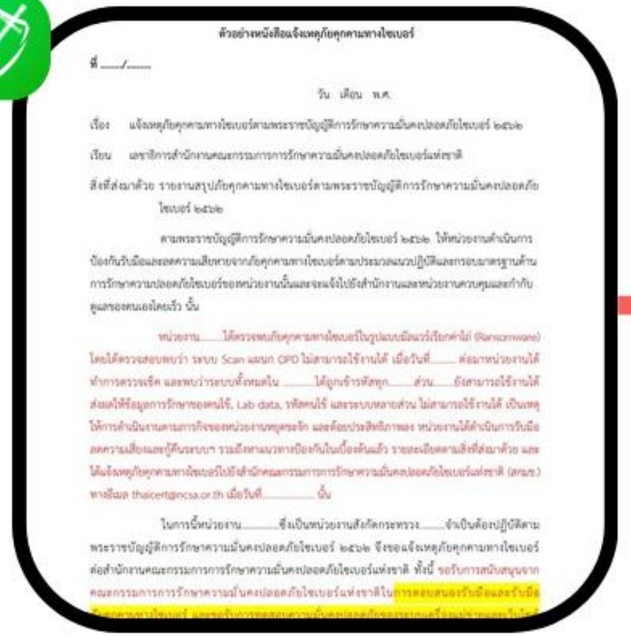


ขั้นตอนการดำเนินมาตรการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์
(Incident Handling Cycle)

การเตรียมการ (Preparation)

ขั้นตอนที่ 1 – รายละเอียดการเตรียมการ (Preparation)

จำเป็นอย่างยิ่งที่จะต้องจัดตั้งทีมจัดการเหตุภัยคุกคามทางไซเบอร์ (Cyber Incident Response Team (CIRT)) กำหนดแนวการสื่อสารที่เหมาะสม สื่อสารบริการที่จำเป็นเพื่อสนับสนุนกิจกรรมการรับมือ และจัดหาเครื่องมือที่จำเป็น


ตัวอย่างหนังสือแจ้งเหตุภัยคุกคามทางไซเบอร์

ที่ ...../.....

วัน เดือน พ.ศ.

เรื่อง แจ้งเหตุภัยคุกคามทางไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ๒๕๖๒

เรียน เลขาธิการสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สิ่งที่ส่งมาด้วย รายงานสรุปภัยคุกคามทางไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ๒๕๖๒

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ๒๕๖๒ ให้หน่วยงานดำเนินการป้องกันรับมือและลดความเสียหายจากภัยคุกคามทางไซเบอร์ตามประมวลแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความปลอดภัยไซเบอร์ของหน่วยงานนั้นและจะแจ้งไปยังสำนักงานและหน่วยงานควบคุมและกำกับดูแลของตนโดยเร็ว นั้น

หน่วยงาน.....ได้ตรวจพบภัยคุกคามทางไซเบอร์ในรูปแบบมัลแวร์เรียกค่าไถ่ (Ransomware) โดยได้ตรวจสอบพบว่า ระบบ Scan แฝนก OPD ไม่สามารถใช้งานได้ เมื่อวันที่..... ต่อมาหน่วยงานได้ทำการตรวจเช็ค และพบว่าระบบทั้งหมดใน.....ได้ถูกเข้ารหัสทุก.....ส่วน.....ยังสามารถใช้งานได้ส่งผลให้ข้อมูลการรักษาของคนไข้, Lab data, รหัสคนไข้ และระบบหลายส่วน ไม่สามารถใช้งานได้ เป็นเหตุให้การดำเนินงานตามภารกิจของหน่วยงานหยุดชะงัก และด้อยประสิทธิภาพลง หน่วยงานได้ดำเนินการรับมือลดความเสี่ยงและกู้คืนระบบฯ รวมถึงหามาตรการป้องกันในเบื้องต้นแล้ว รายละเอียดตามสิ่งที่ส่งมาด้วย และได้แจ้งเหตุภัยคุกคามทางไซเบอร์ไปยังสำนักคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ทางอีเมล thaicert@ncsa.or.th เมื่อวันที่..... นั้น

ในการนี้หน่วยงาน.....ซึ่งเป็นหน่วยงานสังกัดกระทรวง.....จำเป็นต้องปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ๒๕๖๒ จึงขอแจ้งเหตุภัยคุกคามทางไซเบอร์ต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ทั้งนี้ รอรับการสนับสนุนจากคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในการตอบสนองรับมือและรับมือ

รับหนังสือขอรับการสนับสนุนจากฝ่ายเฝ้าระวัง (SOC)

จัดการประชุมหารือหาแนวทางรับมือภัยฯทางไซเบอร์

การตรวจจับและวิเคราะห์ (Detection and Analysis)

ขั้นตอนที่ 2 – การตรวจจับและวิเคราะห์ (Detection and Analysis)

การตรวจจับและระบุเหตุการณ์และการดำเนินการประเมินควรดำเนินการเพื่อยืนยันการมีอยู่ของภัยคุกคามทางไซเบอร์ การประเมินควรรวมถึงการกำหนดขอบเขต ผลกระทบ และขอบเขตของ ความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ ในกรณีที่อาจมีการดำเนินการทางกฎหมาย หลักฐานดิจิทัล จะได้รับการเก็บรักษาไว้ และการวิเคราะห์ทางนิติวิทยาศาสตร์อาจดำเนินการตามข้อกำหนดทางกฎหมายและกฎระเบียบที่เกี่ยวข้อง

เข้าพื้นที่ติดตั้งอุปกรณ์ตรวจจับภัยฯทางไซเบอร์

จัดทีม Monitor รายวัน (ไม่มีวันหยุด) เพื่อวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ หาสาเหตุของการโจมตี

EXAMPLE

สกมช. เข้าพื้นที่เพื่อตรวจสอบเหตุการณ์ ให้การช่วยเหลือหน่วยงาน และติดตั้งอุปกรณ์ Threat Hunting Framework (THF) Deception และระบบ EDR เพื่อตรวจจับภัยคุกคามทางไซเบอร์ให้ภายในเครือข่ายกับหน่วยงาน และดำเนินการติดตาม วิเคราะห์ และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์จากอุปกรณ์ และจะรายงานผลการตรวจจับให้กับ เพื่อใช้เป็นข้อมูล ในการพิจารณาดำเนินการแก้ไข

ติดตั้ง Agent ที่มอบให้

นำ Firewall เป็น Gateway

แก้ไขนามสกุลไฟล์

ทดลองแก้ไขนามสกุลไฟล์ผ่าน

ข้อมูลโคลน (Clone Data)

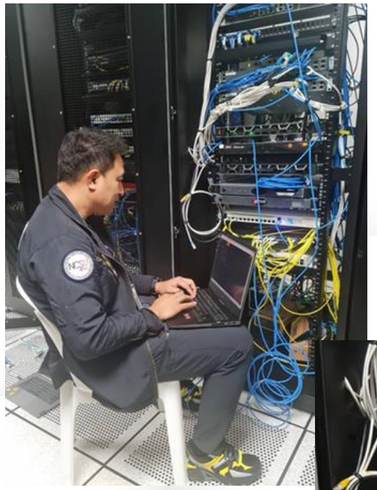
ทำสำรวจความเสียหาย

ทำสำรวจความเสียหาย และผลกระทบ

เบื้องต้นอย่างละเอียด

ร่างถ้อยคำแถลง

เพื่อลดแรงกดดันจากสถานการณ์



การจำกัดขอบเขต (Containment) การกำจัด (Eradication) และการกู้คืน (Recovery)

ขั้นตอนที่ 3 – การจำกัดขอบเขต (Containment) การกำจัด (Eradication) และการกู้คืน (Recovery)

ให้คำแนะนำและเฝ้าระวังอย่างต่อเนื่อง เพื่อรับมือกับภัยคุกคามทางไซเบอร์

ประกอบไปด้วย 3 ขั้นตอนย่อย ดังนี้

ขั้นตอนที่ 3.1 – การจำกัดขอบเขต (Containment))

การจำกัดขอบเขตเหตุการณ์เป็นสิ่งจำเป็นเพื่อลดและแยกความเสียหายที่เกิดขึ้น ต้องดำเนินการตามขั้นตอนเพื่อให้แน่ใจ ว่าขอบเขตของเหตุการณ์ไม่กระจายไปถึงระบบอื่น ๆ และทรัพยากรสารสนเทศ จำเป็นต้องมีการวิเคราะห์สาเหตุที่แท้จริง (Root Cause Analysis) ก่อนที่จะก้าวข้ามขั้นตอนการจำกัดขอบเขต และอาจต้องใช้ผู้เชี่ยวชาญจากบุคคลภายนอก

ขั้นตอนที่ 3.2 – การกำจัด (Eradication)

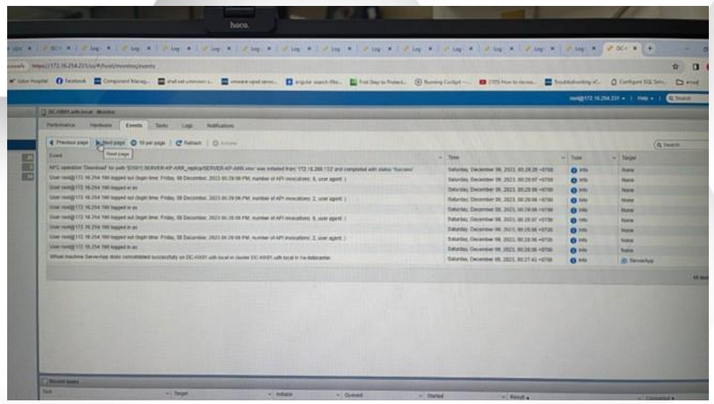
การกำจัดต้องมีการลบ (Removal) หรือจัดการ (Addressing) ส่วนประกอบและอาการ ของภัยคุกคามทางไซเบอร์ทั้งหมด นอกจากนี้ ต้องดำเนินการตรวจสอบความถูกต้อง (Validation) เพื่อให้แน่ใจว่าภัยคุกคามทางไซเบอร์จะไม่เกิดขึ้นอีก

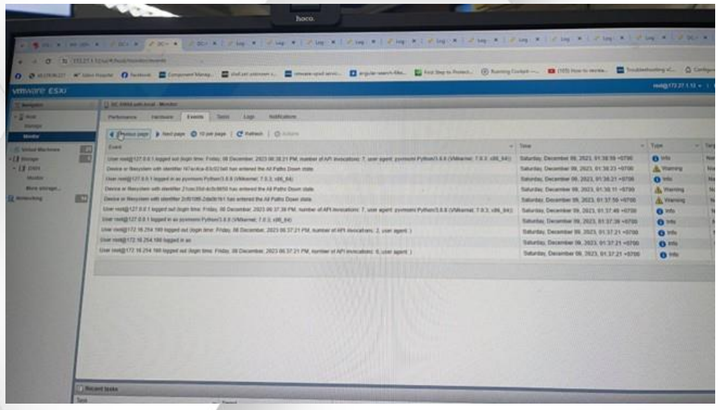
ขั้นตอนที่ 3.3 – การกู้คืน (Recovery)

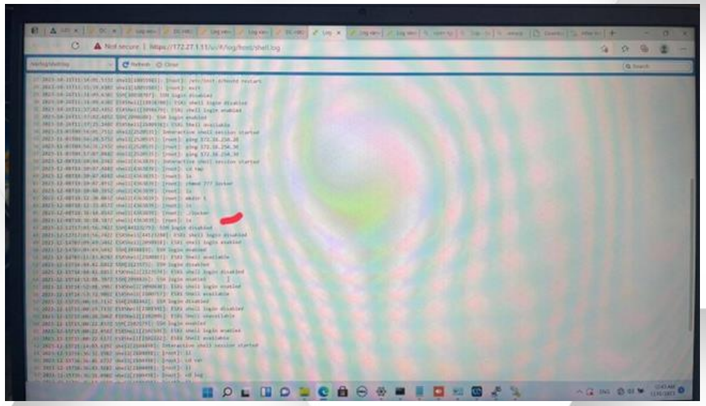
การกู้คืนเกี่ยวข้องกับขั้นตอนที่จำเป็นในการกู้คืนข้อมูลและระบบให้อยู่ในสถานะการทำงานที่ดี ซึ่งช่วยให้การดำเนินธุรกิจสามารถกลับมาดำเนินการได้

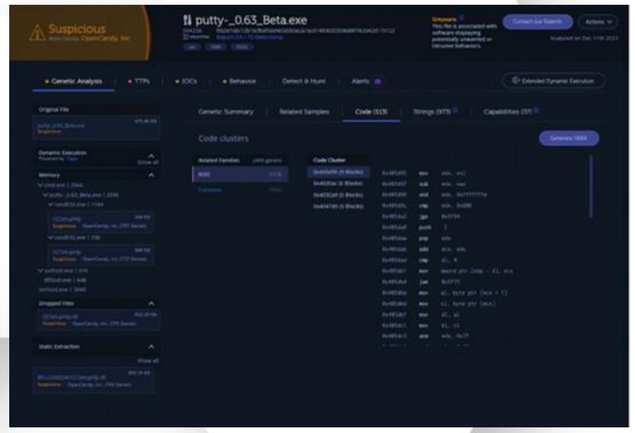
EXAMPLE

ผลการตรวจสอบวิเคราะห์โดย สกมช.พบว่า มีการเข้าระบบผ่าน User: root ซึ่งผู้โจมตีมีเป้าหมายที่เครื่องจำลอง VMware พบว่าไฟล์ต้องสงสัยคือ Putty ซึ่งได้ผลลัพธ์ของค่า Hash ไม่ตรงกับไฟล์ของแท้ ดังภาพจึงสรุปได้ว่าอาจเป็น Malware ที่ผู้ไม่หวังดีโจมตีหน่วยงาน







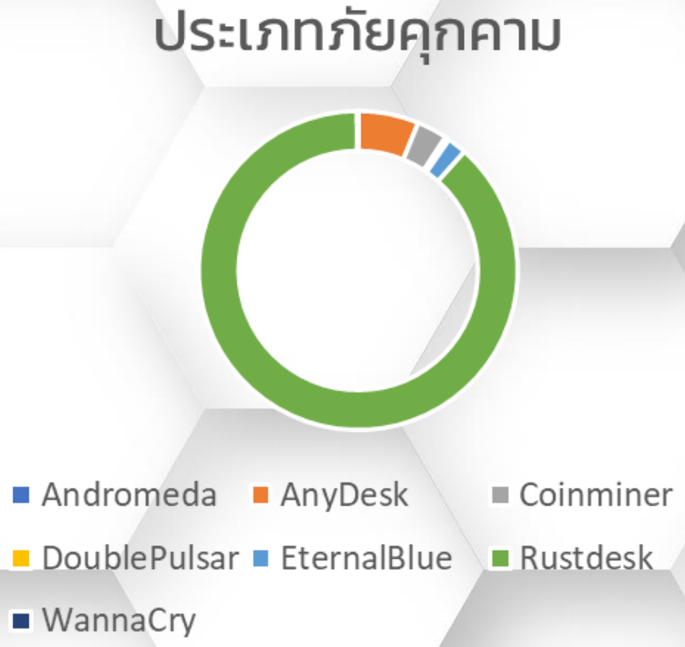


EXAMPLE

Threat hunting framework (THF)
สำหรับตรวจจับและวิเคราะห์พฤติกรรมภัยคุกคามไซเบอร์ การเข้าถึงข้อมูลจากผู้โจมตี และสามารถ ตรวจสอบระบุภัยคุกคามในระบบได้ในเวลาที่แน่นอน

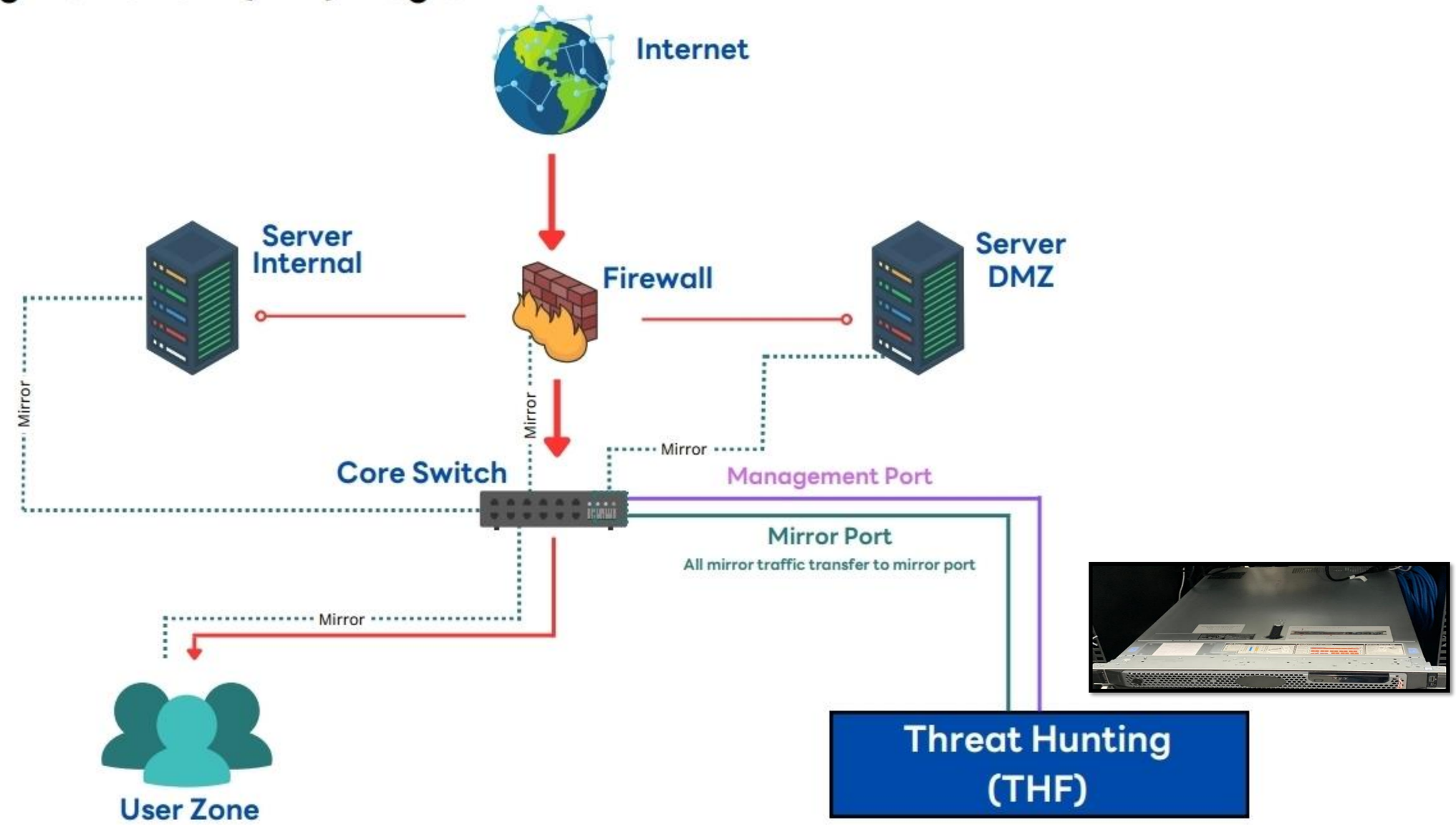
ผลการวิเคราะห์ผ่านอุปกรณ์ Threat hunting framework (THF)

การโจมตี 23,357 เหตุการณ์



อันดับภัยคุกคาม
1.Remote Desktop
2.Coinminer
3.Echo response

Threat Hunting Framework (THF) Diagram



EXAMPLE

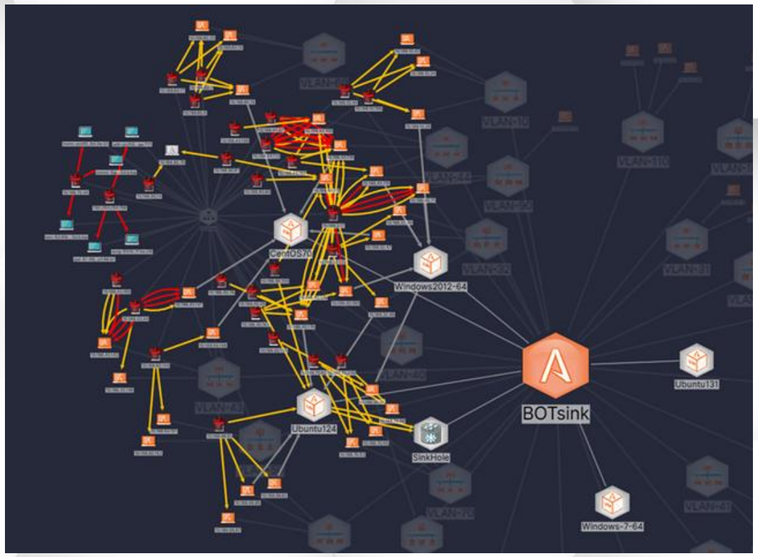
Attivo Networks Deception เป็นระบบป้องกันภัยคุกคามไซเบอร์เชิงรุกที่ใช้เทคโนโลยี Deception หรือการลวงตาหลอกล่อผู้โจมตี ระบบจะสร้าง "เหยื่อล่อ" (Decoy) ที่เหมือนจริงเลียนแบบระบบและข้อมูลสำคัญในเครือข่าย เมื่อผู้โจมตีพยายามเข้าถึงเหยื่อล่อ ระบบ จะตรวจจับและแจ้งเตือนผู้ดูแลระบบทันที ช่วยให้สามารถระบุ ตรวจสอบ และหยุดยั้งภัยคุกคามได้อย่างรวดเร็ว

ผลการวิเคราะห์ผ่านอุปกรณ์ Attivo Networks Deception

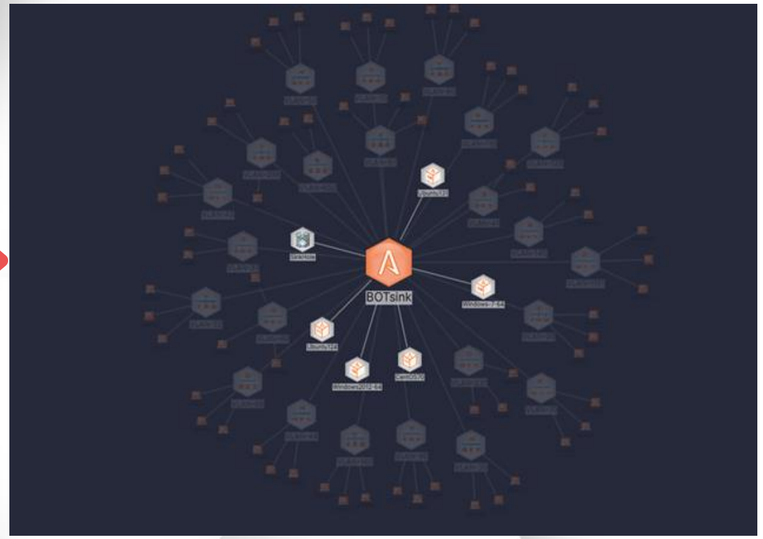
การโจมตี 4,885 เหตุการณ์

อันดับภัยคุกคาม
1.Network Monitoring – Inbound MYSQL
2.Database authentication failure
3.Domain A record found
4.DNS Response
5.ARP Flood

ประเภท OS ที่ถูกโจมตี
1.CentOS 7.0
2.Ubuntu 13.1
3.Ubuntu 12.4

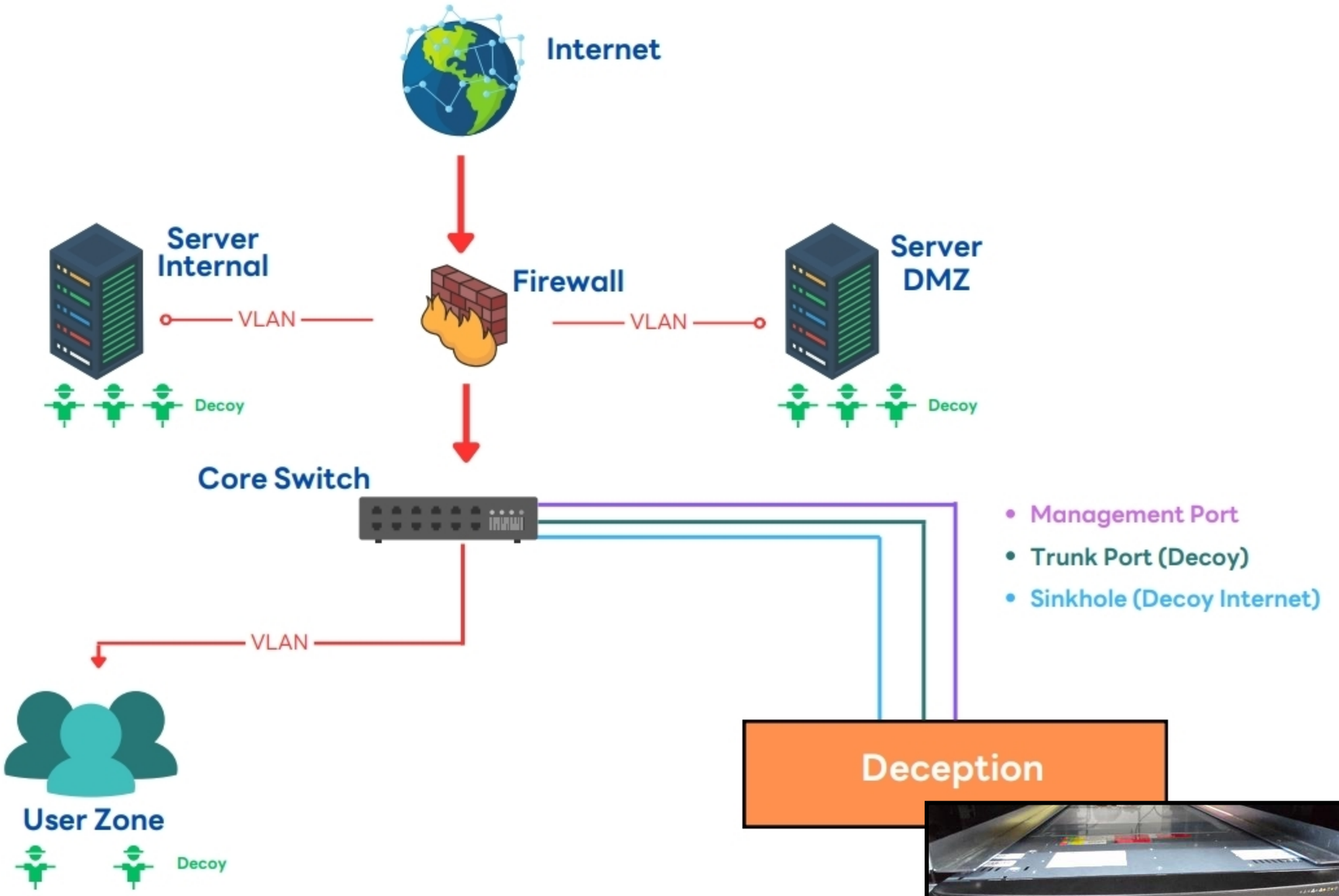


สัปดาห์แรกหลังติดตั้งอุปกรณ์



ปัจจุบัน

Deception Diagram

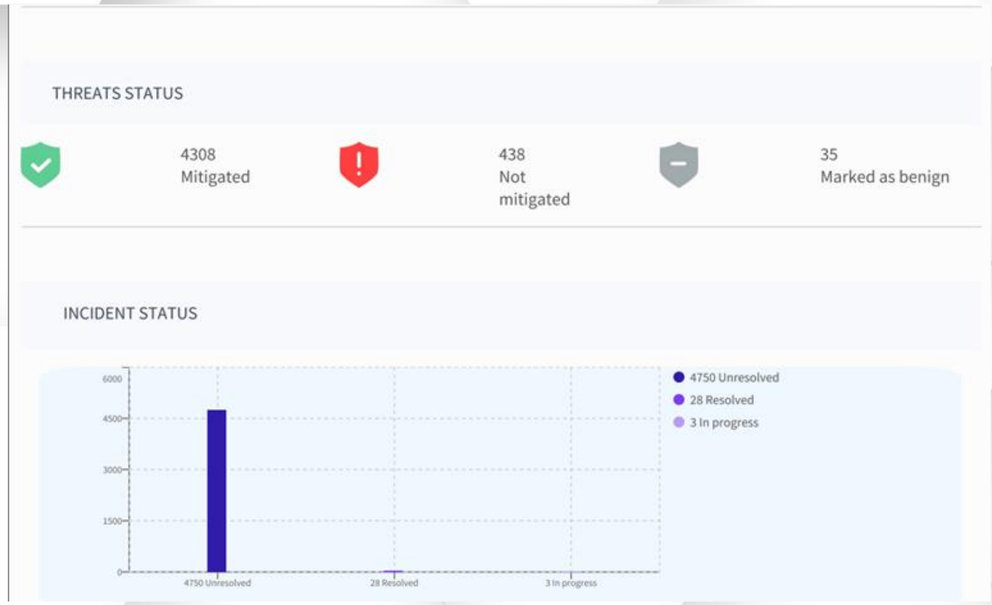


EXAMPLE

Endpoint Detection and Response (EDR) เปรียบเสมือนผู้พิทักษ์อัจฉริยะ คอยสแกนอุปกรณ์ของอย่างละเอียด ค้นหาไฟล์และโปรแกรมที่น่าสงสัย วิเคราะห์พฤติกรรมของโปรแกรม เปรียบเทียบกับข้อมูลภัยคุกคามที่รู้จัก จับพิรุธของมัลแวร์ จึงสามารถตรวจจับภัยคุกคามได้อย่างแม่นยำ

ผลการวิเคราะห์ผ่านอุปกรณ์ Endpoint Detection and Response (EDR)

การโจมตี 4,871 เหตุการณ์



	NAME	THREATS	UNIQUE THREATS	POLICY MODE
	DESKTOP-LSHNS3F	588	555	Protect/Detect
	DESKTOP-6825VFM	504	441	Protect/Detect
	DESKTOP-97DLF73	260	241	Protect/Detect
	DESKTOP-3296OC0	132	92	Protect/Detect
	DESKTOP-JI9HEPC	116	1	Protect/Detect

อุปกรณ์ที่มีความเสี่ยง

จัดหมวดหมู่ของภัยคุกคาม

EXAMPLE

สถานการณ์ภาพรวม วันที่ 14 ธ.ค. 66

จากการดำเนินการในการตอบสนอง และรับมือต่อเหตุการณ์การโจมตีที่เกิดขึ้นยังไม่มีผลกระทบต่อระบบการทำงานของ รพ.แห่งหนึ่ง จนถึงขั้นเป็นภัยคุกคามระดับวิกฤติ โดยได้ทำการกู้คืนระบบ HIS หรือระบบสารสนเทศรพ.ได้แล้ว 100% สามารถใช้งานข้อมูลปัจจุบันได้ ด้านภาพรวมของระบบหลักอื่น ๆ ดำเนินการกู้คืนแล้วเกินกว่า 90% และอยู่ในระหว่างเร่งดำเนินการแก้ไขเพื่อให้ระบบงานอื่น ๆ กลับมาให้บริการเป็นปกติ รวมถึงจัดให้มีการเฝ้าระวัง ระบบต่าง ๆ อย่างเข้มงวด เพื่อป้องกันการเกิดเหตุซ้ำต่อไป

สถานการณ์ภาพรวมภายหลังสถานการณ์สิ้นสุด

ทำการกู้คืนระบบทั้งหมดแล้วเกือบ 100% ซึ่งระบบที่ทำการกู้คืนกลับมาแล้ว ได้แก่

- ข้อมูล 1.5 ล้าน (100%)

ระบบที่ไม่สามารถกู้คืนได้ ได้แก่

- VM Guest 110 เครื่อง
- ข้อมูลทางดิจิตอล 40 TB

แต่ไม่มีผลกระทบกับระบบที่ให้บริการแก่ประชาชน เนื่องจากสามารถจัดทำขึ้นใหม่ได้

การทบทวนหลังการดำเนินการ (Post Cyber Incident Activity)

ขั้นตอนที่ 4 – การทบทวนหลังการดำเนินการ (Post Cyber Incident Activity)

การทบทวนหลังการดำเนินการเกี่ยวข้องกับการทบทวนบทเรียนที่เรียนรู้รวมถึงการวิเคราะห์หลังเหตุการณ์เกี่ยวกับระบบที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์และระบบอื่น ๆ ที่อาจมีความเสี่ยง บทเรียนที่เรียนรู้จากภัยคุกคามทางไซเบอร์นั้นจะถูกสื่อสารไปยังผู้บริหารระดับสูงและแผนปฏิบัติการที่พัฒนาขึ้นเพื่อปรับปรุงแนวทางปฏิบัติในการรับมือเหตุภัยคุกคามทางไซเบอร์ในอนาคตและลดความเสี่ยง


รายงาน
การวิเคราะห์เหตุการณ์ภัยคุกคามในการตอบสนองและรับมือภัยคุกคามทางไซเบอร์

ส่วนที่ 4 ข้อเสนอแนะ ในการตอบสนอง และรับมือเหตุการณ์

ข้อแนะนำในการดำเนินการที่ทันสมัยและรู้ศัพท์ระบบเข้มแข็งเทคนิค ในการมีลูกบุกรุกเครือข่าย และถูกโจมตีด้วย Ransomware

- ปรับปรุงการตั้งค่า Policy ของอุปกรณ์ตรวจจับและรักษาความมั่นคงปลอดภัย เช่น อุปกรณ์ Firewall, Endpoint Security ให้มีความเข้มงวด และเฝ้าระวังมากขึ้น
- ติดตั้งระบบ Security ที่เฝ้าระวังเพิ่มเติม เช่น WAF เพื่อช่วยในการตรวจจับและป้องกันการโจมตีระดับเว็บแอพลิเคชัน
- ติดตั้ง และตั้งค่าระบบเฝ้าระวัง (Monitor) การแจ้งเตือน เครือข่ายและระบบงานต่าง ๆ เช่น Network Monitor และ SIEM หรือเทคโนโลยี Extended Detection and Response (XDR)
- บล็อกกั้นการเข้าถึงระบบจาก Remote Access ที่มาจากนอก โดยเฉพาะ Source IP ที่มาจากต่างประเทศ หากจำเป็นต้องใช้บริการ ควรควบคุมการเข้าถึงและจำกัดสิทธิ์อย่างเข้มงวด
- สำรองข้อมูลแบบออฟไลน์ ทำการเข้าหัวข้อข้อมูล และทดสอบความพร้อมใช้งานและความสมบูรณ์ของการสำรองข้อมูลในสถานการณ์การกู้คืนระบบ ทดสอบขั้นตอนการสำรองข้อมูลเป็นประจำ
- จัดเตรียมแผนรับมือเหตุการณ์ทางไซเบอร์ขั้นพื้นฐาน (IRP) เป็นประจำ และแผนการสื่อสารที่เกี่ยวข้องที่รวมถึงขั้นตอนการตอบสนอง และการแจ้งเตือนสำหรับกรณีถูกโจมตีด้วย Ransomware หรือการละเมิดข้อมูล
- ตรวจสอบให้แน่ใจว่าองค์กรมีแนวทางการจัดการสินทรัพย์ที่ครอบคลุม
- ใช้หลักการสิทธิ์น้อยที่สุดกับทุกระบบ และบริการเพื่อให้ผู้ใช้มีเพียงการเข้าถึงที่จำเป็นในการปฏิบัติงาน
- ผู้ดูแลมักจะได้รับโจรน่าจากปัญหาที่ให้สิทธิ์พิเศษสำหรับการโจมตีด้วย Ransomware ทั่วทั้งเครือข่าย
- ตรวจสอบให้แน่ใจว่าโซนเซอร์ไวเซอร์ทั้งหมด และโครงสร้างพื้นฐานด้านไอทีที่เกี่ยวข้อง รวมถึงเครือข่ายและส่วนประกอบการจัดเก็บข้อมูลได้รับการปรับปรุงให้มีความมั่นคงปลอดภัย ซึ่งกลยุทธ์ของแพลตฟอร์มที่เกิดขึ้นในปัจจุบันเริ่มมีการกำหนดเป้าหมายซอฟต์แวร์ VMware ESXi, ไฮเปอร์ไวเซอร์ และเครื่องมือและระบบจัดการศูนย์ข้อมูลอื่น ๆ ซึ่งช่วยให้สามารถเข้าหัวโครงสร้างพื้นฐานได้อย่างรวดเร็ว
- ใช้สถาปัตยกรรมแบบ Zero Trust เพื่อป้องกันการเข้าถึงข้อมูล และบริการโดยไม่ได้รับอนุญาต มีการบังคับใช้การควบคุมการเข้าถึงแบบละเอียดที่สุด

จัดทำแผนรับมือ เพื่อป้องกันการเกิดเหตุซ้ำ

กระบวนการที่สำคัญ ในขั้นตอน After-Action Review ในกรณีเหตุภัยคุกคามดังกล่าว

ขั้นตอนที่ 1 การทบทวนหลังการดำเนินการ (After-Action Review Process)

การทบทวนหลังการดำเนินการเป็นการติดตามผล (Follow-up) ซึ่งประกอบด้วยการรายงานและการวิเคราะห์หลังภัยคุกคามทางไซเบอร์เกี่ยวกับระบบที่เป็นเป้าหมายของภัยคุกคามทางไซเบอร์และ ระบบอื่น ๆ ที่อาจมีความเสี่ยง วัตถุประสงค์ของขั้นตอนนี้คือการปรับปรุงอย่างต่อเนื่องในการดำเนินการด้านความมั่นคงปลอดภัย ความสามารถในการรับมือ และขั้นตอนต่าง ๆเอกสาร (Documentation) รายละเอียดทั้งหมดที่เกี่ยวข้องกับกระบวนการรับมือเหตุภัยคุกคามทางไซเบอร์จะต้องได้รับ การจัดทำเป็นเอกสารอย่างเป็นทางการและเป็นไฟล์เพื่อให้ง่ายต่อการอ้างอิง ต้องบำรุงรักษารายการต่อไปนี้เมื่อทำได้

1) เหตุการณ์ของระบบทั้งหมด (All System Events) ดูจากบันทึกการตรวจสอบ (Audit Records) หรือล็อก (Log)
2) การดำเนินการทั้งหมด รวมถึงวันที่และเวลาที่ดำเนินการ
3) การสื่อสารภายนอกทั้งหมด
4) บันทึกของผู้สืบสวนสอบสวนที่รวบรวม
5) การเบี่ยงเบนใด ๆ จาก SOP และการให้เหตุผล
รายงานภัยคุกคามทางไซเบอร์ที่จัดทำเป็นเอกสารต่อไปนี้จะถูกเขียนโดย CIRT เมื่อสิ้นสุดการตอบสนอง (Response)
1) คำอธิบายลำดับเหตุการณ์ที่แน่นอน
2) วิธีการค้นพบ
3) มาตรการป้องกันที่มีใช้งานอยู่
4) การประเมินเพื่อพิจารณาว่าการกู้คืนเพียงพอหรือไม่และควรพิจารณาข้อเสนอแนะอื่นใด
วัตถุประสงค์ของรายงาน คือ เพื่อระบุจุดที่อาจต้องปรับปรุงในการรับมือเหตุภัยคุกคามทางไซเบอร์และขั้นตอนการรายงาน ดังนั้น การทบทวนรายงานโดยฝ่ายบริหารควรจัดทำเป็นเอกสารพร้อมกับบทเรียน ที่ได้รับ เพื่อปรับปรุงพื้นที่ที่ระบุและใช้เป็นข้อมูลอ้างอิงสำหรับภัยคุกคามทางไซเบอร์ในอนาคต

ขั้นตอนที่ 2 บทเรียนที่ได้รับและการแก้ไข (Lessons Learned and Remediation)

CIRT จะหารือกับฝ่ายที่เกี่ยวข้อง เช่น เจ้าหน้าที่ด้านเทคนิค ผู้บริหาร ผู้ขาย ทีมรักษาความมั่นคงปลอดภัย เป็นต้น เพื่อรวบรวมบทเรียนที่ได้รับจากภัยคุกคามทางไซเบอร์ดังกล่าวเพื่อลดความเสี่ยง ของเหตุการณ์ในอนาคต ตามความเข้าใจในสาเหตุที่แท้จริง หน่วยงานจะดำเนินการตามขั้นตอนต่าง ๆ เพื่อเสริมสร้างและปรับปรุง ระบบสารสนเทศ นโยบาย ขั้นตอน การป้องกัน และ/หรือการฝึกอบรมตาม ความจำเป็น ในกรณีที่การบรรเทาผลกระทบหรือการเปลี่ยนแปลง ที่เสนอถูกปฏิเสธ จะต้องปฏิบัติตามกระบวนการยอมรับความเสี่ยง ควรมีการวิเคราะห์ภัยคุกคามทางไซเบอร์เพื่อค้นหาแนวโน้ม ควรพิจารณา การดำเนินการแก้ไขสาเหตุ (Corrective Action) ตามความเหมาะสม

การอภิปรายบทเรียนที่ได้รับ ควรครอบคลุม

- **ทบทวนการค้นพบและการรับมือเหตุภัยคุกคามทางไซเบอร์**
- **พนักงานและผู้บริหารทำงานได้ดีเพียงใดและปฏิบัติตามขั้นตอนที่เป็นเอกสารหรือไม่**
- **ทบทวนการกระทำที่ชะลอหรือขัดขวางความพยายามในการกู้คืน**
- **เสนอการปรับปรุงเพื่อการรับมือในอนาคตและความพยายามในการสื่อสาร**
- **คำแนะนำเพื่อเพิ่มความเร็วในการตรวจจับและตอบสนองในอนาคต**
- **คำแนะนำสำหรับความพยายามในการแก้ไขในระยะยาวและระยะสั้น**

เมื่อสิ้นสุดการประชุมบทเรียนที่เรียนรู้ ต้องมีการแก้ไขบางอย่าง ไม่ว่าจะเป็นการแก้ไขปัญหา ติดตั้งการควบคุมการชดเชย (Compensating Controls) หรืออย่างน้อยก็ประเมินและยอมรับความเสี่ยงอย่างเป็นทางการ ต้องมีการเพิ่มข้อเสนอแนะสำหรับความพยายามในการแก้ไขในระยะยาวและระยะสั้นลงในแผนจัดการความเสี่ยง (Treatment Plan) โดยรวม

ควรพิจารณาและรวมการปรับปรุงขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์เมื่อพบส่วนต่าง ๆ ที่สามารถปรับปรุงได้

การแบ่งปันข้อมูลโดยสมัครใจควรเกิดขึ้นเมื่อใดก็ตามที่เป็นไปได้กับผู้มีส่วนได้ส่วนเสียภายนอก เพื่อให้เกิดการรับรู้ถึงสถานการณ์ความมั่นคงปลอดภัยทางไซเบอร์ในวงกว้าง ต้องปรึกษาฝ่ายกฎหมายและการจัดการก่อนที่จะทำเช่นนั้น หากไม่มีนโยบายและกระบวนการแบ่งปันข้อมูลอย่างเป็นทางการ

ขั้นตอนที่ 3 การวิเคราะห์ทางนิติวิทยาศาสตร์และการเก็บรักษาข้อมูล

ในกรณีที่อาจมีการดำเนินการทางกฎหมาย การวิเคราะห์ทางนิติวิทยาศาสตร์ (Forensic Analysis) จะเกิดขึ้นในลักษณะที่จะรักษาหลักฐานดิจิทัล (Preserve Digital Evidence) ที่สอดคล้องกับข้อกำหนดทางกฎหมายและกฎระเบียบที่เกี่ยวข้อง อาจจำเป็นต้องมีที่ปรึกษากฎหมายภายนอกและผู้เชี่ยวชาญ ด้านนิติวิทยาศาสตร์

พิจารณาสิ่งต่อไปนี้เมื่อตัดสินใจว่าจะเก็บหลักฐานที่เกี่ยวข้องกับเหตุการณ์หรือไม่และนานแค่ไหน:

- **การดำเนินคดี (Prosecution) เป็นไปได้ไหมที่ผู้โจมตีจะถูกดำเนินคดี? หากเป็นเช่นนั้น อาจต้องเก็บหลักฐานไว้หลายปี**
- **การเกิดซ้ำ (Reoccurrence) พิจารณาว่าหลักฐานที่รวบรวมอาจเป็นประโยชน์ในกรณีที่ผู้โจมตีหรือการโจมตีที่คล้ายกันจะเกิดขึ้นในอนาคต**
- **นโยบายการเก็บรักษาข้อมูล (Data Retention Policies) พิจารณาเนื้อหาของหลักฐานที่เก็บไว้ เช่น การจับภาพระบบ (System Image Capture) เป็นต้น และนโยบายการเก็บรักษาที่เกี่ยวข้องกับข้อมูลนี้ เช่น นโยบายการเก็บรักษาอีเมล เป็นต้น**
- **ต้นทุน (Cost) ขึ้นอยู่กับชนิดและปริมาณของข้อมูลหรืออุปกรณ์ที่เก็บรักษาไว้เป็นหลักฐาน ต้นทุนอาจเป็นปัจจัยจำกัด**

ขั้นตอน 4 การตัดสินใจที่สำคัญสำหรับการออกจากขั้นตอนบทเรียนที่เรียนรู้

- ผู้บริหารพอใจที่เหตุภัยคุกคามทางไซเบอร์สิ้นสุด
- ผู้จัดการ IR ทำการตัดสินใจสำหรับเหตุภัยคุกคามทางไซเบอร์ที่มีความรุนแรงจำกัด (Limited-severity Incidents)
- CIO เป็นผู้ตัดสินใจสำหรับเหตุภัยคุกคามทางไซเบอร์ระดับร้ายแรงและระดับวิกฤต (Moderate and Critical-severity Incidents)
- มีแผนปฏิบัติการเพื่อตอบสนองต่อปัญหาการดำเนินงาน (Operational Issues) ที่เกิดขึ้นจาก เหตุภัยคุกคามทางไซเบอร์นี้ ณ จุดนี้ ได้เวลากลับสู่ขั้นตอนที่ 1 การเตรียมการ

ความพร้อมที่องค์กรต้องมีและเตรียม นอกจาก IR Action Plan แล้วทรัพยากร ทั้งทีม เครื่องมือ และนโยบายที่สนับสนุน

เนื่องจากการดำเนินการตอบสนองต่อเหตุการณ์อย่างมีประสิทธิผลเป็นการดำเนินการที่ซับซ้อน การสร้างความสามารถในการตอบสนองต่อเหตุการณ์ให้ ประสบความสำเร็จจึงต้องมีการวางแผนและทรัพยากรจำนวนมาก การติดตามการโจมตีอย่างต่อเนื่องถือเป็นสิ่งสำคัญ การสร้างขั้นตอนที่ชัดเจนในการจัดลำดับความสำคัญในการจัดการเหตุการณ์ถือเป็นสิ่งสำคัญ เช่นเดียวกับการนำวิธีการรวบรวม วิเคราะห์ และรายงานข้อมูลที่มีประสิทธิภาพมาใช้ การสร้างความสัมพันธ์และสร้างวิธีการสื่อสารที่เหมาะสมกับกลุ่มภายในอื่น ๆ (เช่น มนุษย์ ทรัพยากร กฎหมาย) และกับกลุ่มภายนอก (เช่น ทีมตอบสนองเหตุการณ์อื่น ๆ การบังคับใช้กฎหมาย) ดังนั้น หน่วยงานจึงควรมี

๑. การจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ โดยมี (Cyber Security Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและข้อมูลติดต่อและการยกระดับการดำเนินการ (Contact Information and Escalation Level) และ
ทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)
(ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น
· ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖
· ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ ดังแนวทางจากการรายงานเหตุภัยคุกคามทางไซเบอร์ (Reporting Incidents)

ทีมรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ (Incident Response Team - IRT)

สำหรับองค์กรขนาดกลางถึงใหญ่ ทีม IRT ควรมีสมาชิกประมาณ 7-10 คน เพื่อให้สามารถตอบสนองต่อเหตุการณ์ได้อย่างครอบคลุมและมีประสิทธิภาพ โดยแบ่งเป็น:

โครงสร้างทีม

- โครงสร้างทีม: ต้องประกอบด้วยสมาชิกที่มีบทบาทและความรับผิดชอบที่ชัดเจน เช่น ผู้จัดการฝ่ายความมั่นคงไซเบอร์, นักวิเคราะห์ความมั่นคงไซเบอร์, ผู้เชี่ยวชาญด้าน Forensic เป็นต้น.

การอบรมและฝึกซ้อม

- การอบรมและฝึกซ้อม: ทีมควรได้รับการฝึกอบรมอย่างต่อเนื่อง และมีการฝึกซ้อมตอบสนองต่อเหตุการณ์จริงเพื่อเตรียมความพร้อม.

ผู้บัญชาการ IR (IR Commander)

- ผู้บัญชาการ IR (IR Commander): ผู้ที่มีความสามารถในการตัดสินใจและประสานงานในการตอบสนองต่อเหตุการณ์.

เครื่องมือและเทคโนโลยี

ระบบตรวจจับและแจ้งเตือน เช่น IDS/IPS (Intrusion Detection System/Intrusion Prevention System), SIEM (Security Information and Event Management)

เครื่องมือวิเคราะห์และสืบสวน เช่น เครื่องมือ Forensic, เครื่องมือวิเคราะห์ Log.

เครื่องมือจำกัดขอบเขตและกู้คืน เช่น ระบบสำรองข้อมูล, ระบบกู้คืนข้อมูล (Backup and Recovery Systems).

นโยบายและขั้นตอนปฏิบัติ

1

นโยบายการตอบสนองต่อเหตุการณ์ เช่น การกำหนดนโยบายที่ชัดเจนสำหรับการตอบสนองต่อเหตุการณ์ภัยคุกคาม.

2

ข้อตกลงระดับการบริการ (SLAs) เช่น การกำหนดข้อตกลงที่ชัดเจนกับผู้ให้บริการเกี่ยวกับการตอบสนองต่อเหตุการณ์.

การประสานงานและการสื่อสาร

01

การสื่อสารภายใน: สร้างความสัมพันธ์และวิธีการสื่อสารที่เหมาะสมกับกลุ่มภายในองค์กร

02

การสื่อสารภายนอก: ทำงานร่วมกับทีมตอบสนองเหตุการณ์อื่น ๆ และการบังคับใช้กฎหมาย

การทบทวนและประเมินผล

การทบทวนแผน:
ทบทวนแผนรับมือเหตุการณ์ภัยคุกคามอย่างสม่ำเสมอ

การประเมินประสิทธิภาพ:
ประเมินประสิทธิภาพของแผนและทีมตอบสนองเหตุการณ์เป็นระยะ ๆ เพื่อปรับปรุงกระบวนการให้ดียิ่งขึ้น