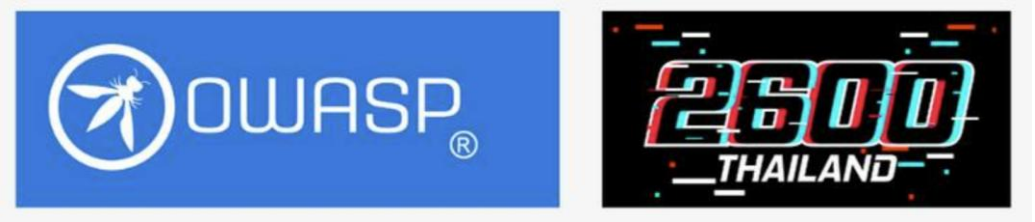


Incident Response Plan & Playbook

Setthawhut Saennam

MFEC

27 June 2025

Disclaimer

Any views or opinions presented in this presentation are solely those of the author and do not necessarily represent those of the employer.

About Me

- Information Security Consultant and CSOC Team Lead
- Experienced in DFIR, CTI, TH, ITSM, and ISMS
- Special lecturer, community contributor, and conference speaker

GIAC Certified Incident Handler (GCIH)

Global Information Assurance Certification...

GIAC Certified Forensic Analyst (GCFA)

Global Information Assurance Certification...

GIAC Certified Forensic Examiner (GCFE)

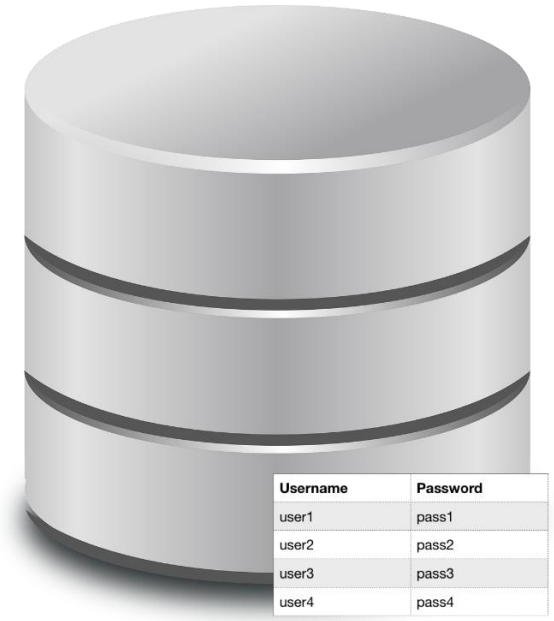
Global Information Assurance Certification...

Topics

- Incident Response Overview
- Developing Incident Response Plan
- Developing Incident Response Playbook
- Q&A

Incident Response Overview

Scenario #1



- A dump with username/password of users from your organization have been posted on “dark web”
- The leaked data also contains PIIs from your organisation staffs and customers
- Regulator asked for an incident report

- What can / should / must you do?
- What logs do you need for investigation?
- What legal issues arise?

Adapted from

TF-CSIRT TRANSITS

https://tf-csirt.org/transits/transits-materials/

Scenario #2

- You receive a complaint about illegal material on a website of your organization
- You've been asked to remove the content and prevent it from being republished
- The police ask for logs

- What can / should / must you do?
- What logs do you need for investigation?
- What legal issues arise?

Adapted from

TF-CSIRT TRANSITS

https://tf-csirt.org/transits/transits-materials/

What is Incident Response?

- An **event** is an innocuous action that happens frequently such as creating a file, deleting a folder, or opening an email. On its own an event typically isn't an indication of a breach but when paired with other events may signal a threat.
- An **alert** is a notification triggered by an event, which may or may not be a threat.
- An **incident** is a group of correlated alerts that humans or automation tools have deemed likely to be a genuine threat. On their own, each alert may not appear to be a major threat but when combined, they indicate a possible breach.

Incident response is the actions that an organization takes when it believes IT systems or data may have been breached. The goals of the response are to eliminate a cyberattack as quickly as possible, recover, notify any customers or government agencies as required by regional laws, and learn how to reduce the risk of a similar breach in the future.

https://www.microsoft.com/en-us/security/business/security-101/what-is-incident-response

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒”

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในพระราชบัญญัตินี้

“การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

“ไซเบอร์” หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

“หน่วยงานของรัฐ” หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์กรฝ่ายนิติบัญญัติ องค์กรฝ่ายตุลาการ องค์กรอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ

“ประมวลแนวทางปฏิบัติ” หมายความว่า ระเบียบหรือหลักเกณฑ์ที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์กำหนด

“เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์” หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

https://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF

Cyber Threat

Abbreviations / Acronyms / Synonyms:

threat show sources
Threat show sources

Definitions:

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.

Sources:

NIST SP 1800-15B under Threat from FIPS 200

https://csrc.nist.gov/glossary/term/cyber_threat

Computer Security Incident

Abbreviations / Acronyms / Synonyms:

incident show sources

Definitions:

An occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. See cyber incident. See also event, security-relevant, and intrusion.

Sources:

CNSSI 4009-2015 under incident from FIPS 200 - Adapted

Anomalous or unexpected event, set of events, condition, or situation at any time during the life cycle of a project, product, service, or system.

Sources:

NIST SP 800-160v1r1 under incident from ISO/IEC/IEEE 15288:2015

https://csrc.nist.rip/glossary/term/computer_security_incident

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ประกาศกำหนดรายละเอียดของลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ

อาศัยอำนาจตามความในมาตรา ๖๐ วรรคสอง แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๒/๒๕๖๔ ลงวันที่ ๔ ตุลาคม ๒๕๖๔ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

https://www.mdes.go.th/law/detail/5049

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์กำหนดหลักเกณฑ์และวิธีการรายงานเมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

อาศัยอำนาจตามความในมาตรา ๑๓ (๕) และมาตรา ๕๗ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ” หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

https://www.mdes.go.th/law/detail/6862

บทที่ ๔
แนวทางปฏิบัติในการรับมือเหตุภัยคุกคามทางไซเบอร์

กล่าวโดยทั่วไป

ภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นต่อ หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จนส่งผลกระทบต่อการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ สามารถจำแนกหมวดหมู่ตามประกาศ กมช. เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รายละเอียดตามผนวก ค สรุปได้ดังนี้

๑. เหตุการณ์จำลอง และ การฝึกจู่โจม ของหน่วยงานเอง (Training and Exercises)
๒. การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
๓. การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
๔. การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)
๕. การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
๖. การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
๗. การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
๘. การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
๙. เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
๑๐. เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)

https://dl.parliament.go.th/handle/20.500.13072/599337

https://www.facebook.com/NCSA.Thailand/posts/pfbid02oDV8Aysb91S4uD8n1kwCmhpAEWeimtc14n6BXgQfyefjqPC7WXVvwHJmy3VYHk3el

https://www.facebook.com/NCSA.Thailand/posts/pfbid02v7JZBiKQ4Qzg8GkuZedrhMtVMUfVttgnPDqeWnGy72KpYbhCQjvGubKqLfXE6VnHl

NCRAF

(Draft) Thailand National Cyber Risk Assessment framework

Identify → Protect → Detect → Respond → Recover

Step 1 ระบุชื่อและข้อมูลหน่วยงาน

Step 2 การระบุความเสี่ยง (Risk Identification)

Step 3 การประเมินช่องโหว่ (Vulnerability Assessment)

Step 4 มาตรการควบคุมความเสี่ยงที่ใช้ในปัจจุบัน (Existing Security Controls)

Step 5 แบบประเมิน Quantum Cyber Readiness

ประเภทภัยคุกคาม (Threat type) Incident Examples สำหรับจำแนกประเภทของเหตุการณ์ไซเบอร์ตามลักษณะและวิธีการโจมตีที่เกิดขึ้น

การจำแนกหมวดหมู่หลัก (Top-Level Categories ตาม eCSIRT.net Taxonomy ที่ใช้สำหรับจำแนกเหตุการณ์ความปลอดภัยไซเบอร์ (Cybersecurity Incident) โดยได้รับการสนับสนุนจาก ENISA และถูกใช้งานอย่างแพร่หลายในยุโรป ซึ่งช่วยให้หน่วยงานและ CSIRT (Computer Security Incident Response Team) สามารถรายงานและแลกเปลี่ยนข้อมูลเหตุการณ์ได้อย่างเป็นมาตรฐานเดียวกัน

INCIDENT CLASSIFICATION	INCIDENT EXAMPLES	DESCRIPTION
Abusive Content	Spam	or "Unsolicited Bulk Email", this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content
	Harmful Speech	Discreditation or discrimination of somebody (e.g. cyber stalking, racism and threats against one or more individuals)
	Child/Sexual/Violence/ ...	Child pornography, glorification of violence, ...
Malicious Code	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialler	
	Rootkit	
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This includes also some kind of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...), port scanning.
	Sniffing	Observing and recording of network traffic (wiretapping).
	Social engineering	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).
Intrusion Attempts	Exploiting known vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g. buffer overflow, backdoor, cross site scripting, etc.).
	Login attempts	Multiple login attempts (Guessing / cracking of passwords, brute force).
	New attack signature	An attempt using an unknown exploit.
Intrusions	Privileged account compromise	A successful compromise of a system or application (service). This can have been caused remotely by a known or new vulnerability, but also by an unauthorized local access. Also includes being part of a botnet.
	Unprivileged account compromise	
	Application compromise	
	Bot	
Availability	DoS	By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. DoS examples are ICMP and SYN floods, Teardrop attacks and mail-bombing. DDoS often is based on DoS attacks originating from botnets, but also other scenarios exist like DNS Amplification attacks. However, the availability also can be affected by local actions (destruction, disruption of power supply, etc.) – or by Act of God, spontaneous failures or human error, without malice or gross neglect being involved.
	DDoS	
	Sabotage	
	Outage (no malice)	
Information Content Security	Unauthorised access to information	Besides a local abuse of data and systems the information security can be endangered by a successful account or application compromise. Furthermore, attacks are possible that intercept and access information during transmission (wiretapping, spoofing or hijacking). Human/configuration/software error can also be the cause.
	Unauthorised modification of information	
Fraud	Unauthorized use of resources	Using resources for unauthorized purposes including profit-making ventures (E.g. the use of e-mail to participate in illegal profit chain letters or pyramid schemes).
	Copyright	Offering or installing copies of unlicensed commercial software or other copyright protected materials (Warez).
	Masquerade	Type of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it.
	Phishing	Masquerading as another entity in order to persuade the user to reveal a private credential.
Vulnerable	Open for abuse	Open resolvers, world readable printers, vulnerability apparent from Nessus etc scans, virus signatures not up-to-date, etc
Other	All incidents which do not fit in one of the given categories should be put into this class.	If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.
Test	Meant for testing	Meant for testing

Table 1: eCSIRT.net mkVI

ecsirt.net taxonomy.Reference Incident Classification Taxonomy. January 2018

เอกสาร	คำนิยามที่เกี่ยวข้องกับคำว่า “incident”
พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒	ภัยคุกคามทางไซเบอร์ เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
ประกาศ กกม. เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ฯ พ.ศ. ๒๕๖๔	ภัยคุกคามทางไซเบอร์
ประกาศ กกม. เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖	ภัยคุกคามทางไซเบอร์ เหตุภัยคุกคามทางไซเบอร์ เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ
(Draft) The National Cyber Incident Response Plan of Thailand 2022 Thailand’s National Cyber Exercise 2024	ภัยคุกคามทางไซเบอร์ เหตุการณ์ทางไซเบอร์ เหตุภัยคุกคามทางไซเบอร์
(Draft) Thailand National Cyber Risk Assessment Framework 2025 (เอกสารถูกลบออกไปแล้ว)	ภัยคุกคาม (Threat) เหตุการณ์ความปลอดภัยไซเบอร์ (Incident)

หมายเหตุ: ปัจจุบันทาง สกมช. อยู่ระหว่างการรับฟังความคิดเห็นในการปรับปรุงแก้ไข พรบ.ไซเบอร์ และกฎหมายลำดับรอง

Incident Response Plan

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Cybersecurity incident response planning: Practitioner guidance

First published: January 2022
Last updated: December 2024

Roles and responsibilities

Include details of the roles and responsibilities of core personnel and teams responsible for cybersecurity incident response and decision making. At a minimum, include the personnel responsible for receiving the initial notification, the operational level Cybersecurity Incident Response Team (CIRT) and the strategic level Senior Executive Management Team (SEMT).

All personnel listed should be familiar with their responsibilities in the CIRP and have practise their response.

Points of contact for reporting cybersecurity incidents

Include details about primary and secondary internal points of contact for personnel or stakeholders to report cybersecurity incidents to over a 24/7 period.

Name	Availability	Contact Details	Role/Title	Responsibilities
			on-call point of contact	▪ *Primary point of contact*

Cybersecurity Incident Response Team

Include details of the CIRT personnel responsible for managing responses to cybersecurity incidents. The composition of the CIRT will vary depending on the size of an organisation and available skills and resources.

Include details of any 3rd party vendors that provide or manage systems, services and/or networks. If applicable, include details of external cybersecurity incident response providers and the services they provide.

Name	Availability	Contact Details	Role/Title	Responsibilities
			cybersecurity incident manager	▪ *Response planning* ▪ *CIRT operations*
			deputy cybersecurity incident manager	▪ *Situational analysis* ▪ *Threat intelligence* ▪ *Technical advice*
			security manager	▪ *Investigation (if suspected malicious insider)* ▪ *Law enforcement liaison*
			cybersecurity incident responder	▪ *Technical investigation (collection and processing of network and host data)* ▪ *Containment, remediation and recovery efforts* ▪ *Investigation findings report*

Containment, evidence collection and remediation

Containment

Containment actions are implemented in order to minimise damage, prevent the cybersecurity incident from spreading or escalating, and prevent malicious actors from destroying evidence.

When planning containment actions, consider:

- any additional impacts there could be to systems, services or networks
- time and resources required to contain the cybersecurity incident
- effectiveness of the containment solution (e.g. partial vs full containment)
- duration that the containment solution will remain in place (e.g. temporary vs permanent solution).

Documentation

Include processes and procedures for documenting the cybersecurity incident, including responsible personnel and timeframes. Refer to Appendix D for a situation report template and Appendix E for a cybersecurity incident log template.

Situation reports may contain the following information:

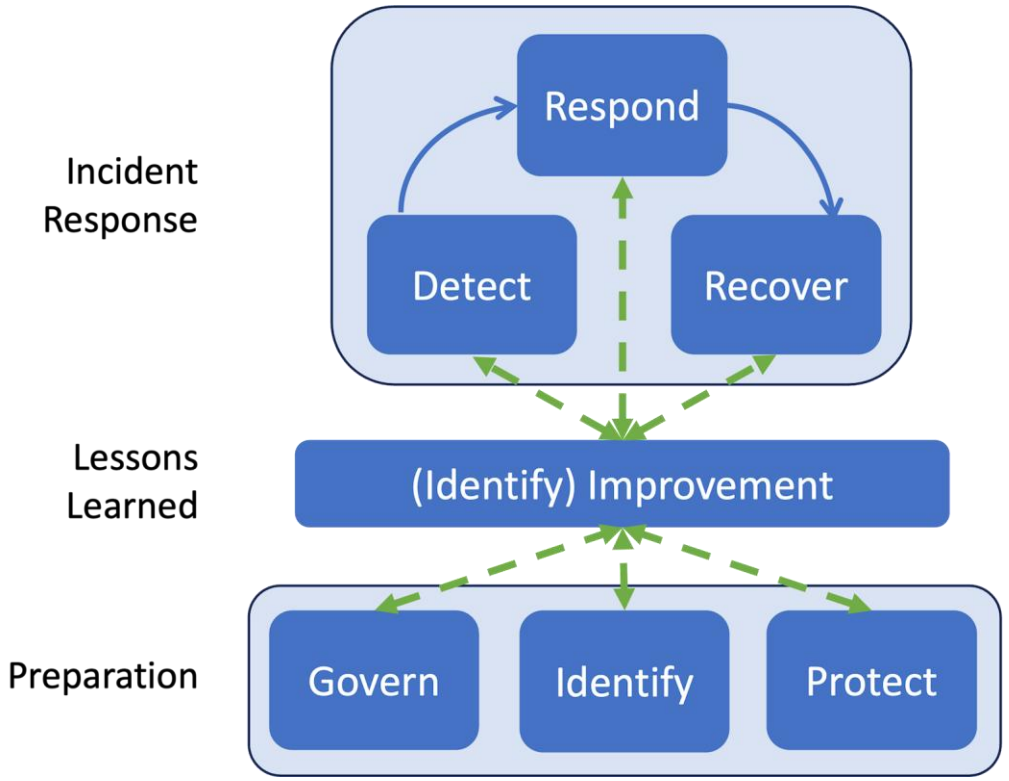
- cybersecurity incident date and time
- status of the cybersecurity incident
- cybersecurity incident type and classification
- cybersecurity incident scope and impact
- cybersecurity incident severity
- external assistance required
- actions taken to resolve the cybersecurity incident
- contact details for key CIRT personnel
- date and time of the next update.

Evidence collection and preservation

Include processes and procedures for collecting, preserving, handling and storing evidence, including responsible personnel and timeframes. As this can be complex, if necessary, seek advice from digital forensic professionals, legal advisors or law enforcement.

https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/incident-response/cybersecurity-incident-response-planning-practitioner-guidance

NIST SP 800-61r3 Incident Response Life Cycle



Previous Incident Response Life Cycle Model Phase	CSF 2.0 Functions
Preparation	Govern
	Identify (all Categories)
	Protect
Detection & Analysis	Detect
	Identify (Improvement Category)
Containment, Eradication & Recovery	Respond
	Recover
	Identify (Improvement Category)
Post-Incident Activity	Identify (Improvement Category)

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

Preparation Resources

The following are selected examples of additional resources supporting incident response preparation.

+ expand all

General Incident Response Programs, Policies, and Plans

Sector-Specific Incident Response Programs, Policies, and Plans

Incident Response Program Assessment and Improvement

Incident Response Training and Exercises

Life Cycle Resources

The following are selected examples of additional resources supporting the incident response life cycle.

+ expand all

Vulnerability and Threat Information

General Incident Reporting and Coordination

Reporting Incidents to US Federal Agencies

Digital Forensics

https://csrc.nist.gov/projects/incident-response

Incident Response Policies, Processes, and Procedures

Definition of computer security incidents and related terms

Who is responsible for responding to an event

Incident classification and severity

Incident response team communication

Documentation and reporting requirements

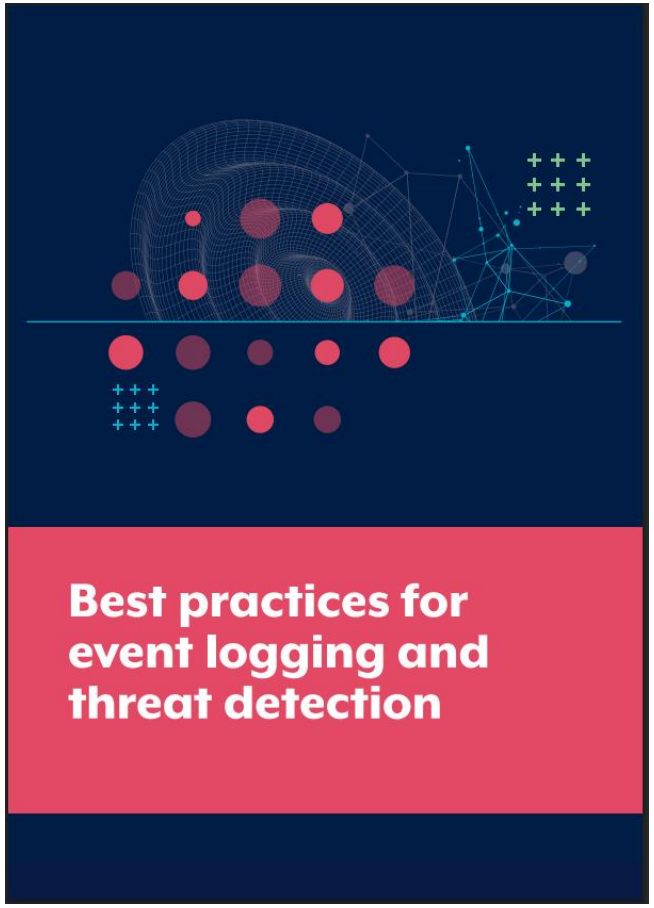
Awareness training and tabletop exercise

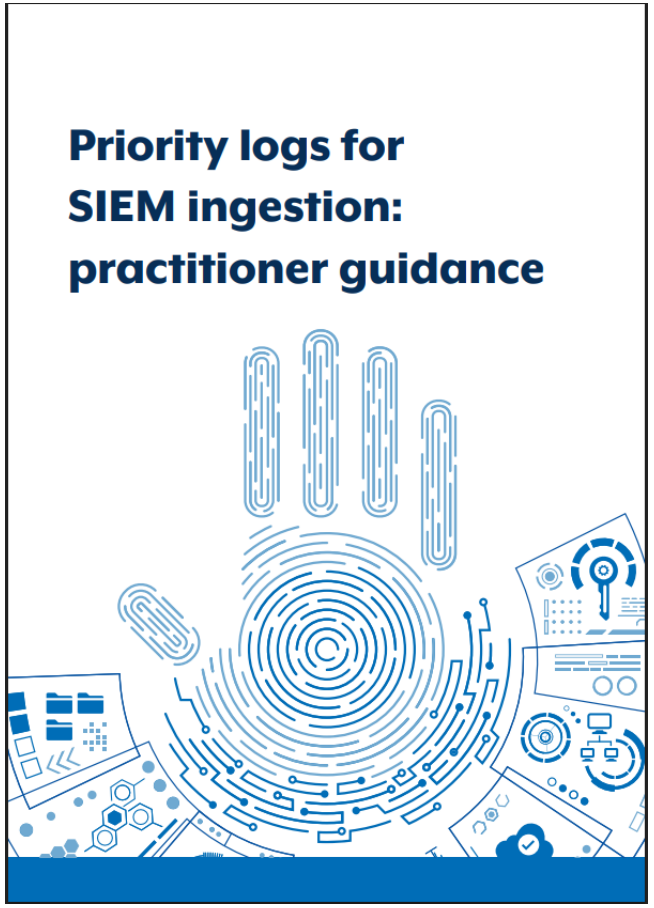
Roles and Responsibilities

Business leaders	Strategic choices: Top-level decisions on business continuity and reputation management.
	Clear communications: Approving what's shared with clients, regulators, and the press.
	Regulatory navigation: Initiating data breach notifications, if required (think GDPR, HIPAA).
	Coordination: Delegating outreach and support to affected customers and stakeholders.
Technical teams	Rapid containment: Isolating affected systems before threats spread.
	Root cause analysis: Assessing the depth and extent of damage.
	Restoration: Prioritizing restoring core systems safely and quickly.
	Ongoing vigilance: Auditing accounts, reviewing logs, rotating credentials, and ensuring all software and tech are updated.

https://www.huntress.com/blog/incident-response-planning-basics

Incident Detection – Log Sources





https://www.cisa.gov/resources-tools/resources/best-practices-event-logging-and-threat-detection

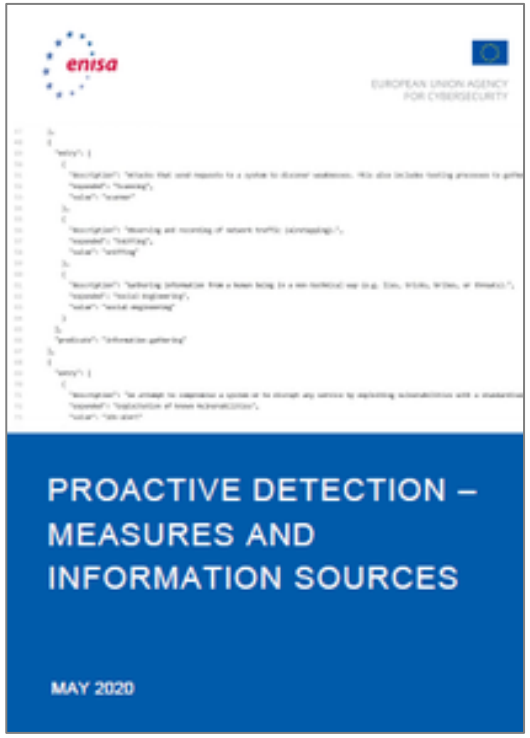
https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-monitoring/implementing-siem-and-soar-platforms

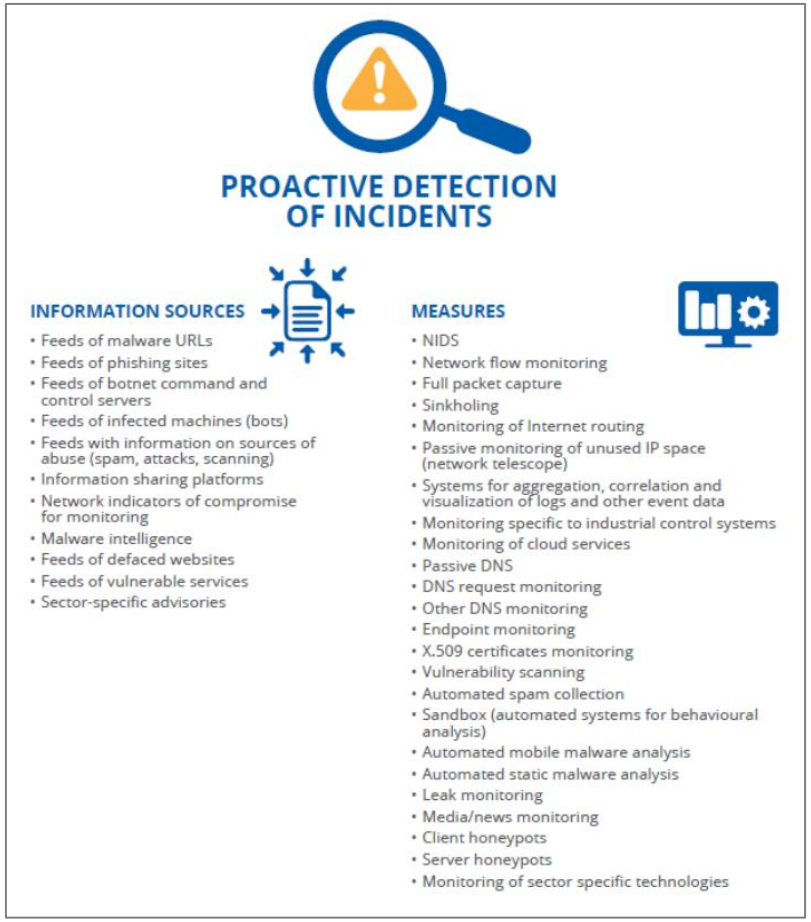
Incident Detection – Event Sources and Indicators

Tactic	Common Techniques	Log and Event Sources	Indicators
Initial Access	Phishing [T1566], Drive-by Compromise [T1189], Exploit Public Facing Application [T1190], External Remote Services [T1133]	Email, web proxy, server application logs, IDS/IPS	Phishing, redirect, and payload servers (domains and IP addresses), delivery mechanisms (lures, macros, downloaders, droppers, etc.), compromised credentials, web shells
Execution	Command and Script Interpreters [T1059], Exploitation for Client Execution [T1203]	Host event logs, Windows event logs, Sysmon, anti-malware, EDR, PowerShell logs	Invocation of command or scripting interpreter, exploitation, API calls, tools, malware, payloads
Persistence	Account Manipulation [T1098], Scheduled Task/Job [T1053], Valid Accounts [T1078]	Host event logs, Authentication logs, Registry	Scheduled Tasks, registry keys, autoruns, etc.
Lateral Movement	Exploitation of Remote Services [T1210], Remote Session Hijacking [T1563], Software Deployment Tools [T1072]	Internal network logs, host event logs, Application Logs	Mismatch of users and applications/credentials, workstation to workstation communication, beaconing from hosts not intended to be internet accessible, etc.
Credential Access	Brute Force [T1110], Modify Authentication Process [T1556], Man-in-the-Middle [T1557]	Authentication Logs, Domain Controller Logs, network traffic monitoring	LSASS reads, command or scripting interpreters accessing LSASS, etc.
C2	Application Layer Protocol [T1071], Protocol Tunneling [T1572]	Firewall, Web Proxy, DNS, Network Traffic, Cloud activity logs, IDS/IPS	C2 domains, IP addresses
Exfiltration	Exfiltration Over C2 Channel [T1041], Exfiltration Over Alternative Protocol [T1048]	Firewall, Web Proxy, DNS, Network Traffic, Cloud activity logs, IDS/IPS	Domains, URLs, IP addresses, IDS/IPS signatures

https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks

Incident Detection – Threat Information Sources





2.2.3 Feeds of botnet command and control servers[58]

Data on command and control servers used by malware, usually domains or IP addresses. This information is obtained by analysing individual malware samples or tracking the infrastructure used by threat actors. Addresses of command and control servers are very good network IoCs and can be used for real-time detection and blocking, but also for identification of infected machines by correlating them with network activity logs, for example netflow.

2.2.3.1 Evaluation

Timeliness: Fair; new addresses are often added after manual analysis, which can take hours or days; some sources provide data from automated tracking of specific botnets, these information can be close to real-time.

Accuracy: Good; C&C servers are usually verified before being added to a blacklist.

Ease of use: Excellent; C&C addresses can be easily correlated with network logs using existing tools.

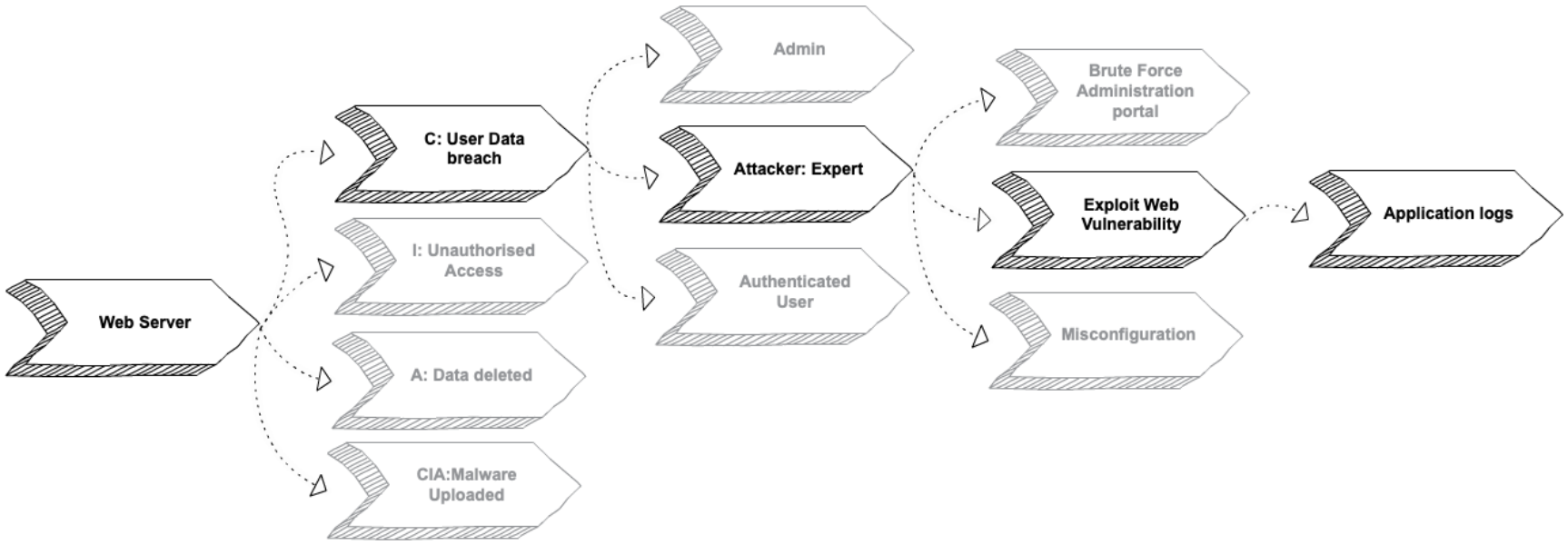
Data volume: Low, the number of C&C servers is much smaller than other types of malicious infrastructure.

Completeness: Fair; sufficient for detection and blocking: domains or IP addresses and malware name; some sources provide additional malware-specific details that can be used for in-depth investigations.

https://www.enisa.europa.eu/publications/proactive-detection-measures-and-information-sources

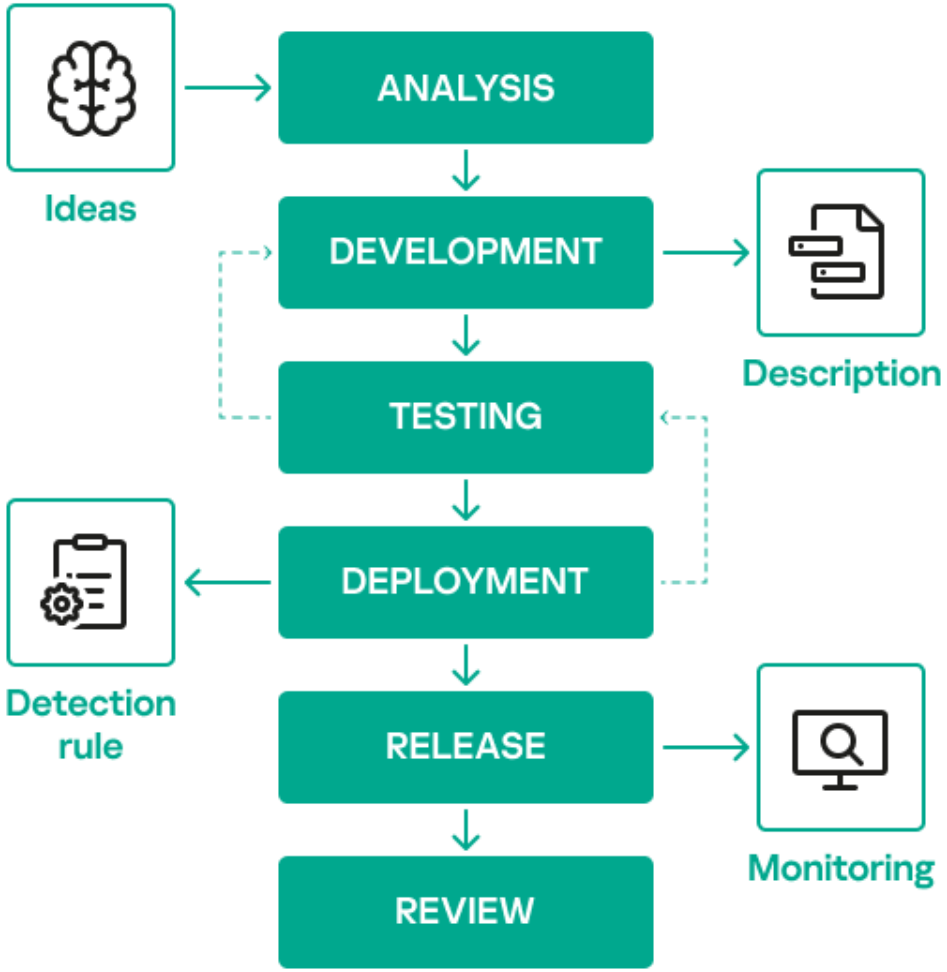
Incident Detection – Threat Modeling

Threat modeling is the process of identifying, analyzing, and prioritizing potential threats and vulnerabilities to a system or application.



https://www.ncsc.gov.uk/collection/building-a-security-operations-centre/onboarding-systems-and-log-sources/threat-modelling

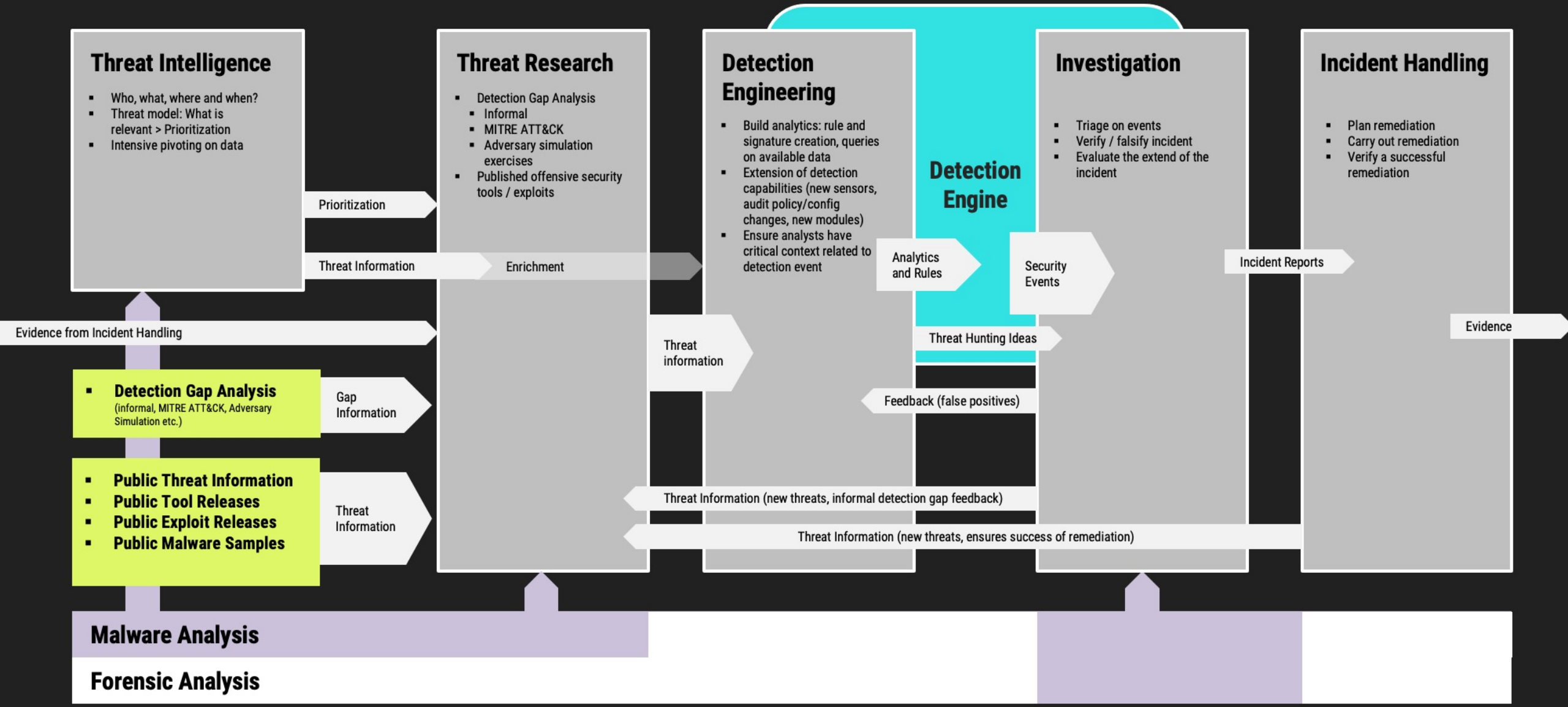
Detection Engineering Life Cycle



https://securelist.com/streamlining-detection-engineering/116186/

Detection and Response Roles Overview

https://cyb3rops.medium.com/about-detection-engineering-44d39e0755f0



Incident Classification

ภาคผนวก
ท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม
และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

ข้อ ๑ การจำแนกหมวดหมู่ของภัยคุกคามทางไซเบอร์

หมวดหมู่	คำอธิบาย
๐	เหตุการณ์จำลอง และ การฝึกจู่โจม ของหน่วยงานเอง (Training and Exercises)
๑	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)
๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)[๔4]
๙	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)

https://www.mdes.go.th/law/detail/5049

Category	Description
0	**Training and Exercises**—Operations performed for training purposes and support to CC/S/A/FA exercises.
1	**Root Level Intrusion (Incident)**—Unauthorized privileged access to an IS. Privileged access, often referred to as administrative or root access, provides unrestricted access to the IS. This category includes unauthorized access to information or unauthorized access to account credentials that could be used to perform administrative functions (e.g., domain administrator). If the IS is compromised with malicious code that provides remote interactive control, it will be reported in this category.
2	**User Level Intrusion (Incident)**—Unauthorized non-privileged access to an IS. Non-privileged access, often referred to as user-level access, provides restricted access to the IS based on the privileges granted to the user. This includes unauthorized access to information or unauthorized access to account credentials that could be used to perform user functions such as accessing Web applications, Web portals, or other similar information resources. If the IS is compromised with malicious code that provides remote interactive control, it will be reported in this category.
3	**Unsuccessful Activity Attempt (Event)**—Deliberate attempts to gain unauthorized access to an IS that are defeated by normal defensive mechanisms. Attacker fails to gain access to the IS (i.e., attacker attempts valid or potentially valid username and password combinations) and the activity cannot be characterized as exploratory scanning. Reporting of these events is critical for the gathering of useful effects-based metrics for commanders. Note the above CAT 3 explanation does not cover the "run-of-the-mill" virus that is defeated/deleted by AV software. "Run-of-the-mill" viruses that are defeated/deleted by AV software are not reportable events or incidents and should not be annotated in JIMS.
4	**Denial of Service (Incident)**—Activity that denies, degrades, or disrupts normal functionality of an IS or DoD information network.
5	**Non-Compliance Activity (Event)**—Activity that potentially exposes ISs to increased risk as a result of the action or inaction of authorized users. This includes administrative and user actions such as failure to apply security patches, connections across

	security domains, installation of vulnerable applications, and other breaches of existing DoD policy. Reporting of these events is critical for the gathering of useful effects-based metrics for commanders.
6	**Reconnaissance (Event)**—Activity that seeks to gather information used to characterize ISs, applications, DoD information networks, and users that may be useful in formulating an attack. This includes activity such as mapping DoD information networks, IS devices and applications, interconnectivity, and their users or reporting structure. This activity does not directly result in a compromise.
7	**Malicious Logic (Incident)**—Installation of software designed and/or deployed by adversaries with malicious intentions for the purpose of gaining access to resources or information without the consent or knowledge of the user. This **only** includes malicious code that does not provide remote interactive control of the compromised IS. Malicious code that has allowed interactive access should be categorized as Category 1 or Category 2 incidents, not Category 7. Interactive active access may include automated tools that establish an open channel of communications to and/or from an IS.
8	**Investigating (Event)**—Events that are potentially malicious or anomalous activity deemed suspicious and warrant, or are undergoing, further review. No event will be closed out as a Category 8. Category 8 will be recategorized to appropriate Category 1-7 or 9 prior to closure.
9	**Explained Anomaly (Event)**—Suspicious events that after further investigation are determined to be non-malicious activity and do not fit the criteria for any other categories. This includes events such as IS malfunctions and false alarms. When reporting these events, the reason for which it cannot be otherwise categorized must be clearly specified.

Table B-A-2. Cyber Incident and Reportable Cyber Event Categories

https://www.jcs.mil/Portals/36/Documents/Library/Manuals/m651001.pdf

CJCSM 6510.01B Incident Category

- หัวข้อ root level intrusion และ user level intrusion จะรวมถึงเหตุการณ์ประเภท unauthorized access to information และเหตุการณ์ malware ที่มีความสามารถในการทำ remote interactive control ด้วย ทำให้เหตุการณ์ประเภท web defacement หรือ backdoor จะถูกจัดเข้ามาอยู่ในหัวข้อนี้
- หัวข้อ unsuccessful activity attempt จะนับเฉพาะเหตุการณ์ที่เป็นการพยายามโจมตีระบบหรือโจมตีช่องโหว่ แต่ถูกป้องกันไว้ได้ รวมถึงการพยายาม brute force รหัสผ่านด้วย แต่ไม่นับเหตุการณ์ประเภท network scanning หรือ user enumeration (จัดไปอยู่ในหัวข้อ reconnaissance)
- หัวข้อ non-compliance activity นับรวมเหตุการณ์ที่เกิดทั้งจากผู้ใช้ทั่วไปและผู้ดูแลระบบ เช่น การติดตั้งแอปพลิเคชันที่ไม่ได้รับอนุญาต หรือการไม่อัปเดต security patch
- หัวข้อ reconnaissance เป็นเหตุการณ์ที่เกี่ยวข้องกับการพยายามรวบรวมข้อมูล แต่ไม่ได้เป็นการโจมตีเพื่อสร้างความเสียหาย (เช่น network scanning หรือ user enumeration)
- หัวข้อ malicious code ไม่รวมเหตุการณ์ประเภท backdoor (จัดไปอยู่ในหัวข้อ intrusion ตามระดับสิทธิ์ของ user ที่รัน malware นั้นๆ)

National Cyber Security Agency

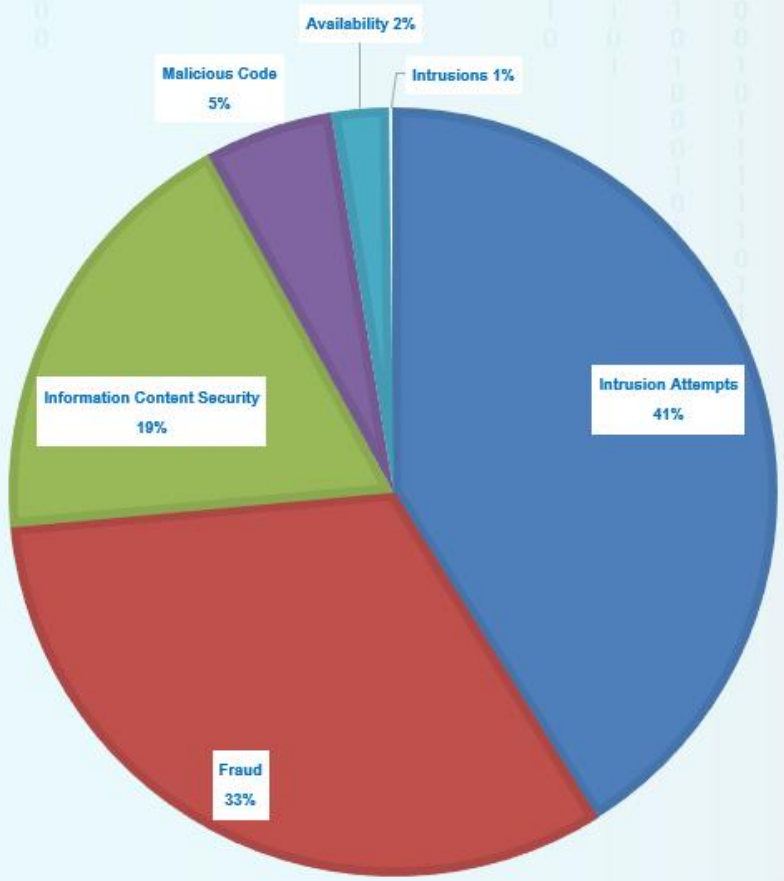
สถิติภัยคุกคามทางไซเบอร์ ประจำปี พ.ศ. 2568

NCSA สกมช

มกราคม – พฤษภาคม 2568

รวมทั้งสิ้น 1,002 เหตุการณ์

Intrusion Attempts	412
Fraud	325
Information Content Security	185
Malicious Code	54
Availability	24
Intrusions	2



ThaiCERT
Thailand Computer Emergency Response Team
By NCSA Thailand

หมายเหตุ – อ้างอิง Incident Class ตาม enisa

https://www.ncsa.or.th/policy/threat-statistics

สถิติภัยคุกคามทางไซเบอร์ แยกตามประเภทภัยคุกคาม ปีพ.ศ. 2566

ดาวน์โหลด | Visualization | Data API

URL: https://ncsa.gdcatalog.go.th/dataset/6673a096-ea64-4412-967b-74f30281a218/resource/a94bb6f6-77d2-46f2-b4f8-a20219b1ffe7/download/-new-microsoft-excel-worksheet...

สถิติภัยคุกคามทางไซเบอร์ แยกตามประเภทภัยคุกคาม ปีพ.ศ. 2566

Data Explorer

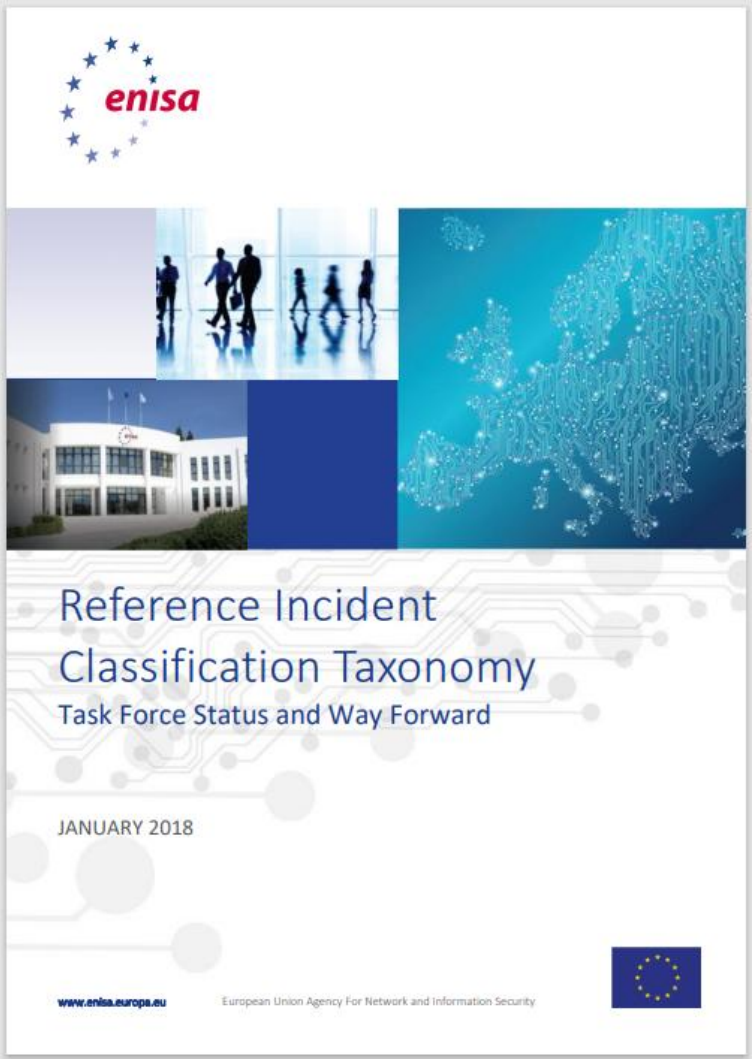
Fullscreen | ฝังตัว

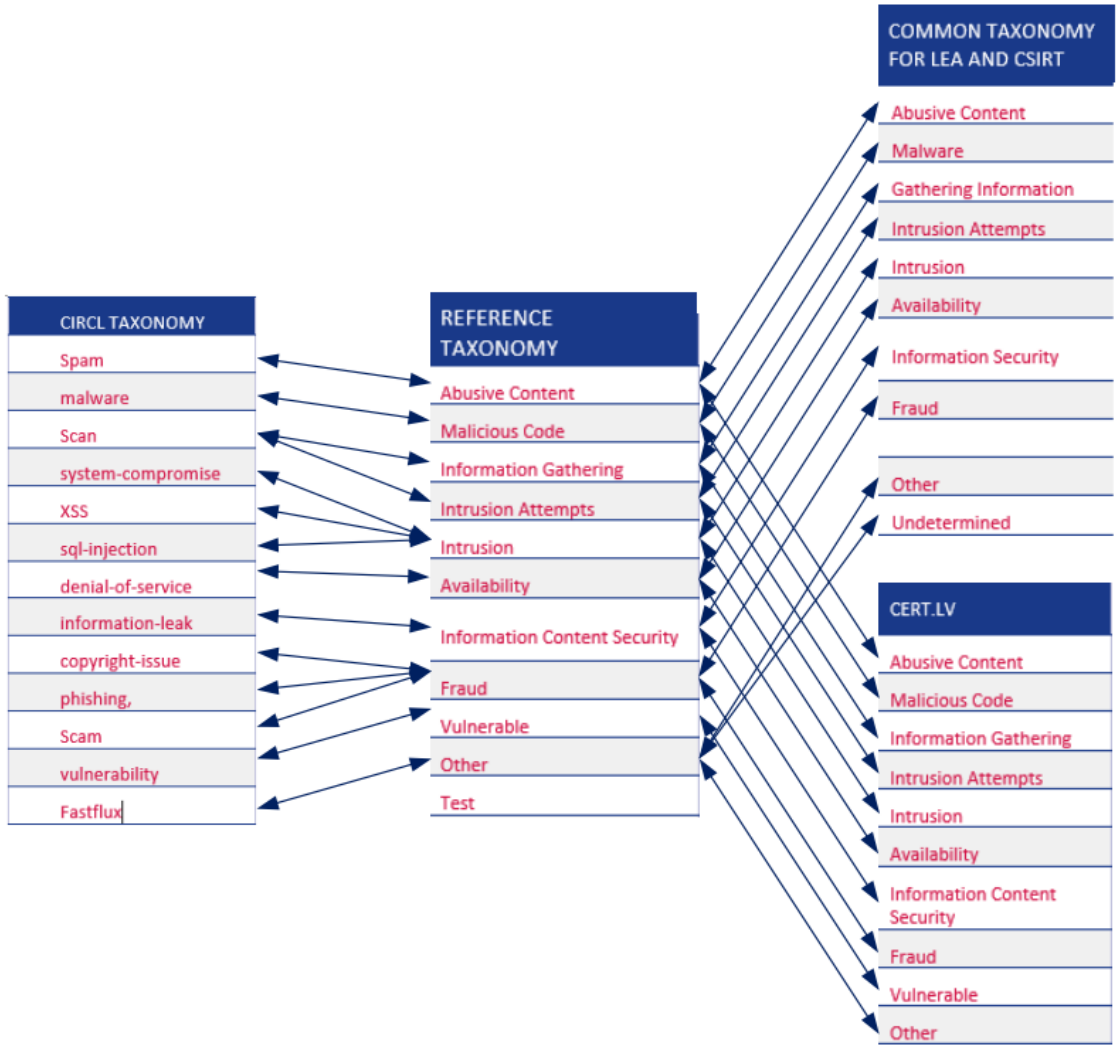
23 records « 1 – 23 » Search data ... Go » Filters

_id	รูปแบบภัยคุกคาม	มกราคม	กุมภาพันธ์	มีนาคม	เมษายน	พฤษภาคม	มิถุนายน	กรกฎาคม	สิงหาคม	กันยายน
2	Hacked Website (Defacement)	83	60	79	17	13	20	8	5	19
3	Fake Website	20	28	50	49	26	26	13	50	13
4	จุดอ่อนช่องโหว่	1	1	4	6	4	10	45	6	1
5	Finance Scam - หลอกลวงการเงิน Online	0	10	7	12	19	17	15	24	5
6	Data Leak	0	0	2	31	3	0	4	60	0
7	DDos	0	0	1	0	0	3	20	9	0
8	Hacked Website (Phishing)	3	6	7	1	5	4	0	4	5
9	Data Breach	3	2	6	0	0	3	6	7	14
10	Ransomware	1	6	2	3	1	4	1	5	1
11	Hacked Website (Malware)	0	0	3	0	5	1	0	3	0
12	Privileged Account Compromise	0	0	0	1	0	1	1	6	3
13	Command and Control Server	1	0	0	0	0	0	2	2	0
14	Unauthorised access to information	0	0	2	0	3	0	0	0	0
15	Security Misconfiguration	0	0	0	0	1	0	1	0	0
16	Application Compromise	0	0	0	0	0	0	0	1	0
17	Mail Phishing	0	0	1	0	0	0	0	0	0
18	Malware	0	0	0	0	1	0	0	0	0
19	Unauthorised modification of information	0	0	1	0	0	0	0	0	0
20	Fraud	0	0	0	0	0	0	0	0	0
21	Broken access control	0	0	0	0	0	0	0	0	0
22	Website (Phishing)	0	0	0	0	0	0	0	0	0
23	อื่นๆ	0	1	0	0	0	0	0	0	0

https://gdcatalog.go.th/dataset/gdpublish-ro7irasuk/resource/b6a6217a-6088-4e11-a334-5cdb44a14439

ENISA Reference Incident Classification Taxonomy





https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

ENISA Reference Incident Classification Taxonomy

CLASSIFICATION (1ST COLUMN)	INCIDENT EXAMPLES (2ND COLUMN)	Description / Examples
Abusive Content	Spam	Or 'Unsolicited Bulk Email', this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content. This IOC refers to resources which make up spam infrastructure, for example, harvesters like address verification, URLs in spam emails, etc.
Abusive Content	Harmful Speech	Bullying, harassment or discrimination of somebody, e.g., cyber stalking, racism or threats against one or more individuals.
Abusive Content	(Child) Sexual Exploitation/Sexual/Violent Content	Child Sexual Exploitation (CSE), sexual content, glorification of violence, etc.
Malicious Code	Infected System	System infected with malware, e.g., a PC, smartphone or server infected with a rootkit. Most often this refers to a connection to a sinkholed command and control server.
Malicious Code	C2 Server	Command and control server contacted by malware on infected systems.
Malicious Code	Malware Distribution	URI used for malware distribution, e.g., a download URL included in fake invoice malware spam or exploit kits (on websites).
Malicious Code	Malware Configuration	URI hosting a malware configuration file, e.g., web injects for a banking trojan.
Information Gathering	Scanning	Attacks that send requests to a system to discover weaknesses. This also includes testing processes to gather information on hosts, services and accounts. This includes fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, etc) port scanning.
Information Gathering	Sniffing	Observing and recording of network traffic (i.e. wiretapping).
Information Gathering	Social Engineering	Gathering information from a human being in a non-technical way (e.g., using lies, tricks, bribes, or threats).

https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/working_copy/humanv1.md

Incident Classification Mapping (Example)

ENISA Classification	ENISA Incident Example	NCSA/CJCSM Category
Abusive Content	Spam	N/A
Abusive Content	Harmful Speech	N/A
Abusive Content	(Child) Sexual Exploitation/Sexual/Violent Content	N/A
Malicious Code	Infected System	Malicious Logic
Malicious Code	C2 Server	Malicious Logic
Malicious Code	Malware Distribution	ไม่เข้านิยามของ Malicious Logic น่าจะใกล้เคียงกับ Intrusion มากกว่า
Malicious Code	Malware Configuration	ไม่เข้านิยามของ Malicious Logic น่าจะใกล้เคียงกับ Intrusion มากกว่า
Information Gathering	Scanning	Reconnaissance
Information Gathering	Sniffing	N/A
Information Gathering	Social Engineering	N/A
Intrusion Attempts	Exploitation of Known Vulnerabilities	Unsuccessful Activity Attempt
Intrusion Attempts	Login Attempts	Unsuccessful Activity Attempt
Intrusion Attempts	New Attack Signature	ถ้าโจมตีสำเร็จน่าจะเป็น Intrusion แต่ถ้าไม่สำเร็จน่าจะเป็น Unsuccessful Activity Attempt
Intrusions	Privileged Account Compromise	Root Level Intrusion
Intrusions	Unprivileged Account Compromise	User Level Intrusion
Intrusions	Application Compromise	เป็นได้ทั้ง Root Level Intrusion และ User Level Intrusion
Intrusions	System Compromise	เป็นได้ทั้ง Root Level Intrusion และ User Level Intrusion

https://docs.google.com/document/d/14wTTgSBqMON4mXn0FD52q8gwh4-UT8JO-R5bhYl0Y4o/

Incident Type	Description	Event Criteria
Scanning	Send requests to a system to discover services or weak points	• IP/Port scanning • Vulnerability scanning
Host attack	Attempt to compromise service on host	• Web application attack • Exploiting known vulnerabilities
Credential attack	Attempt to compromise user account	• Multiple logon failures/Brute force • Suspicious logon activities
Malware	Malware found on endpoint or detected network connection to blacklisted IP/URL	• Malware detected • Connection to malware IP/URL
Availability	Attempt to delay or disrupt service	• DDoS • Service outage
Policy violation	Forbidden user activities	• Unauthorized access • Unauthorized network activity
Misconfiguration	Exposed service with known vulnerabilities or insecure public service	• Unpatched vulnerabilities • Insecure service configuration
Phishing	Phishing email received or phishing website visited	• Phishing
Data breach	Unauthorized data access/disclosure	• Data leaked • Data exposure
Anomaly	Suspicious activities	• Anomaly traffics • Anomaly account activities
Other	None of the above	• N/A

Incident Prioritization (Example)

Severity	Condition	Time to Notify (Example)
Critical	• Over 80% of staff (or several critical staff/teams) unable to work • Critical systems offline with no known resolution • High risk to / definite breach of sensitive client or personal data • Severe reputational damage - likely to impact business long term	• 30 Min • Call, Email
High	• 50% of staff unable to work • Risk of breach of personal or sensitive data • Noncritical systems affected, or critical systems affected with known (quick) resolution • Potential serious reputational damage	• 1 Hour • Call, Email
Medium	• 20% of staff unable to work • Possible breach of small amounts of non-sensitive data • Low risk to reputation • Small number of non-critical systems affected with known resolutions	• 12 Hour • Email
Low	• Minimal, if any, impact • One or two non-sensitive / non-critical machines affected • <10% of noncritical staff affected temporarily (short term)	• 24 Hour • Email

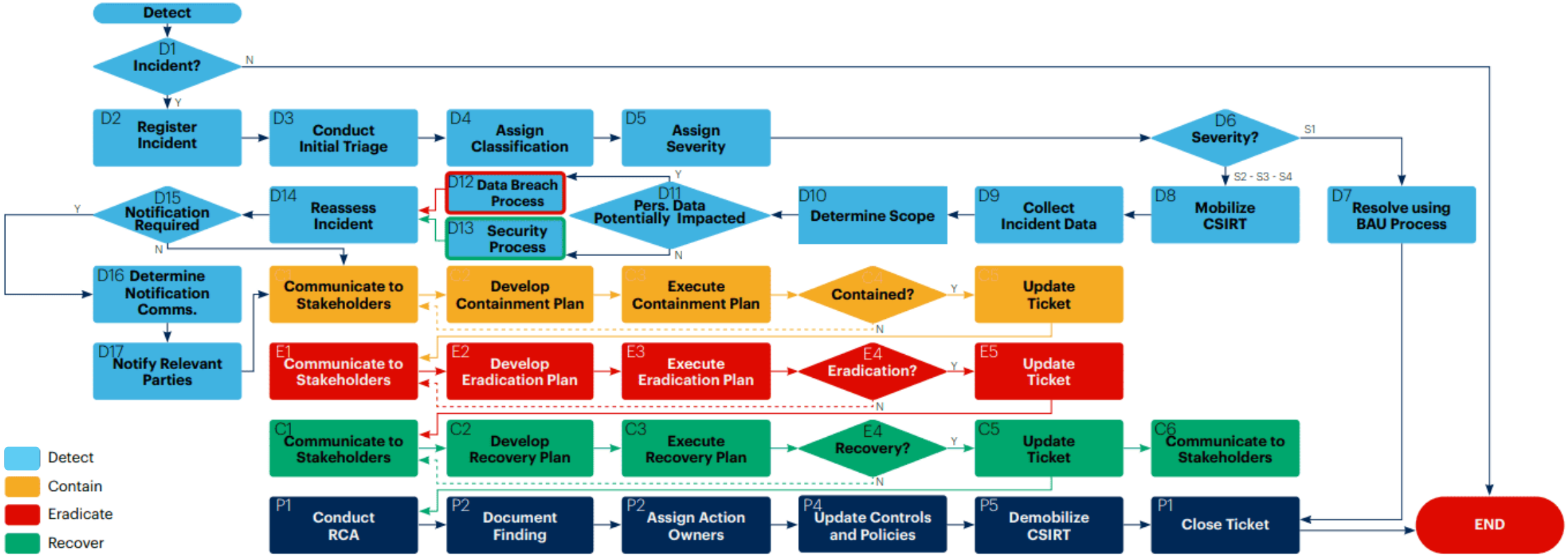
https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes

Incident type	Critical	High	Medium	Low
Scanning	• N/A	• Network scanning from server	• N/A	• Port scan • Vulnerability scan
Host attack	• Host compromised	• Application compromised	• N/A	• Unsuccessful exploit attempts
Credential Attack	• Privileged account compromised	• Unprivileged account compromised	• N/A	• Unsuccessful login attempts
Malware	• Ransomware infected	• Botnet or backdoor detected	• Crypto miner detected • Hacking tools detected • Suspicious script execution • Other malware detected	• N/A
Availability	• Critical service outage	• Critical service unresponsible for some users • SLA reached threashold	• DDoS attempt detected • Service malfunction	• Outage (no malice)
Policy violation	• Unauthorized access to classified information • Unauthorized modification of classified information	• Privilege account misuse • Unauthorized access to information • Unauthorized modification of information	• Access violation • Anomaly traffic/behavior/service • Installation or usage of unauthorized software	• N/A
Misconfiguration	• Unpatched critical vulnerabilities • Critical-level security misconfiguration	• Unpatched high vulnerabilities • High-level security misconfiguration	• Unpatched medium vulnerabilities • Medium-level security misconfiguration	• Unpatched low vulnerabilities • Low-level security misconfiguration
Phishing	• Spear-phishing clicked and credential/information leaked	• Spear-phishing detected	• User clicked phishing link but no credential leaked	• Spam • Phishing detected
Data breach	• Confidential information leaked • Exposed of PIIs information	• Exposed of classified information	• N/A	• N/A

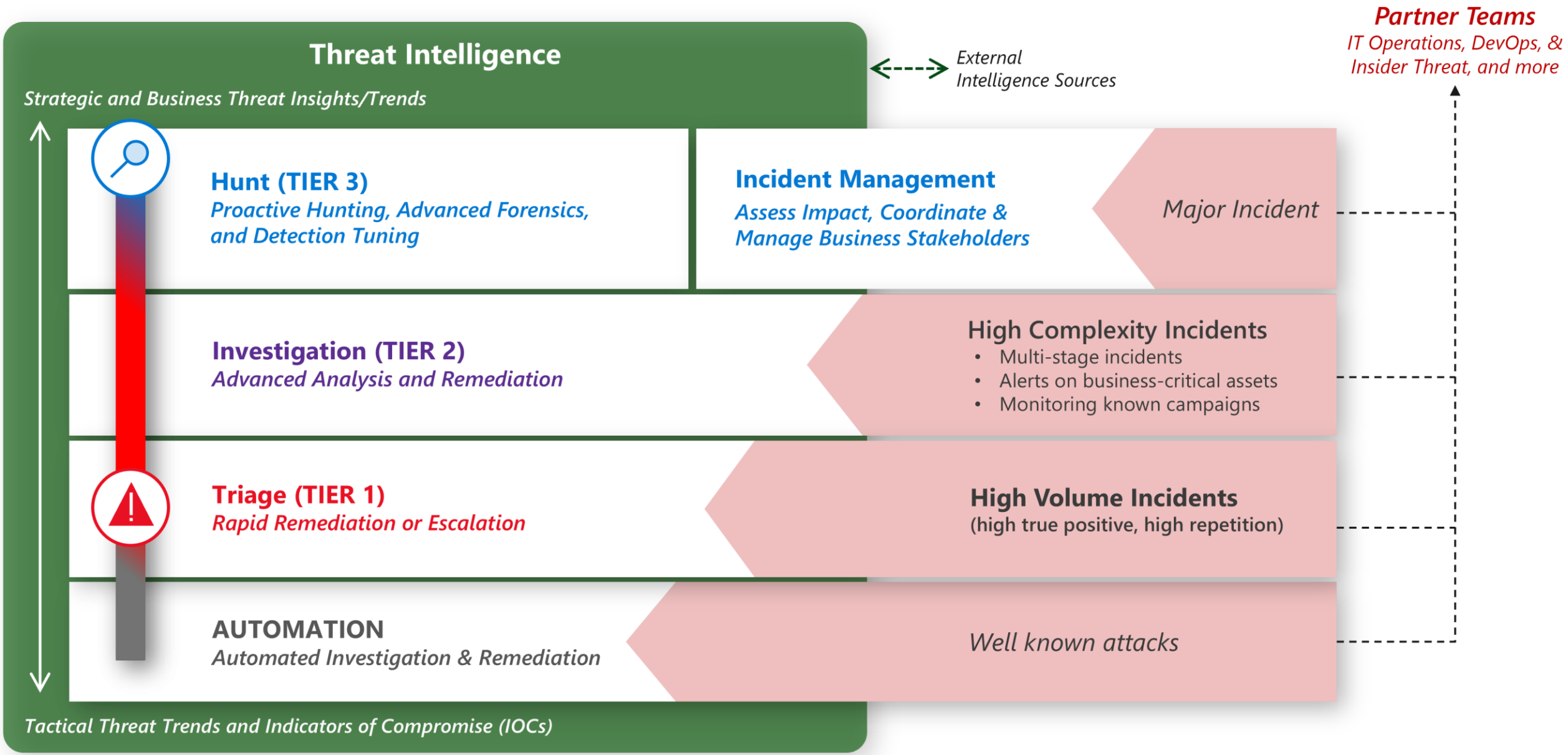
Incident Prioritization Matrix (Example)

Develop a Response Process Map

The incident response plan should dictate detailed, sequential procedures to follow in the event of an incident. The incident coordinator (or similar role) should ensure that each step of the process is completed and that progress is tracked and communicated on a rolling basis.



https://www.resolutets.com/create-an-incident-response-plan/



https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/security-operations

Incident Analysis

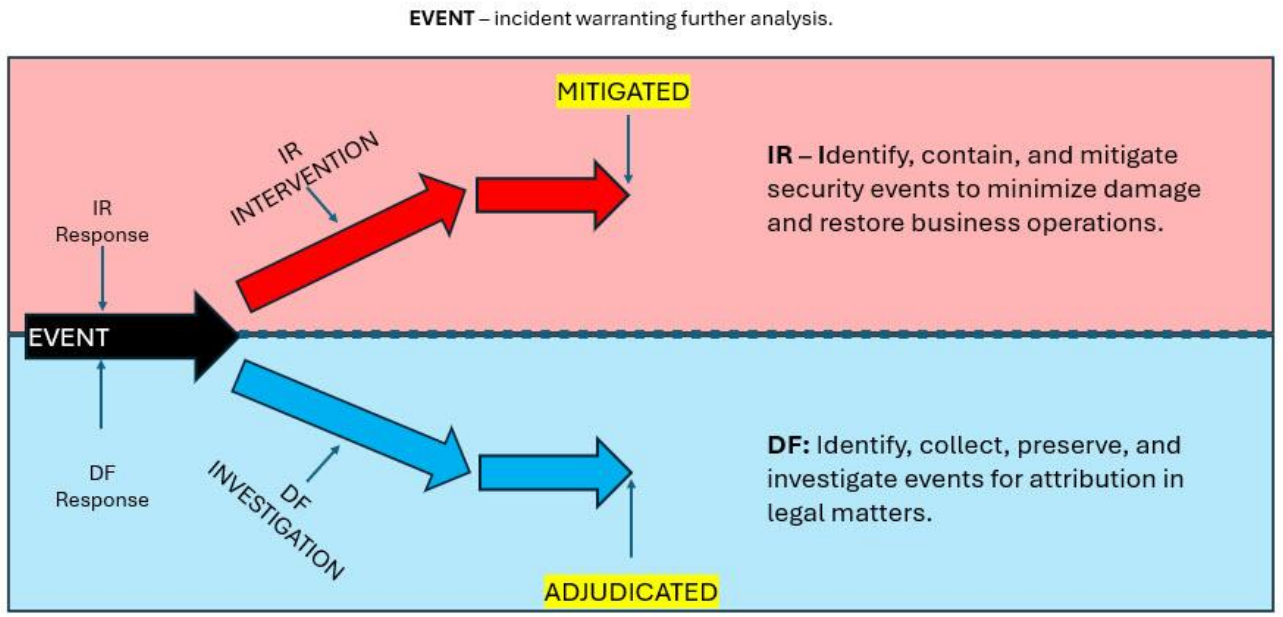
Key Questions to Answer

- What was the initial attack vector? (i.e., How did the adversary gain initial access to the network?)
- How is the adversary accessing the environment?
- Is the adversary exploiting vulnerabilities to achieve access or privilege?
- How is the adversary maintaining command and control?
- Does the actor have persistence on the network or device?
- What is the method of persistence (e.g., malware backdoor, webshell, legitimate credentials, remote tools, etc.)?
- What accounts have been compromised and what privilege level (e.g., domain admin, local admin, user account, etc.)?
- What method is being used for reconnaissance? (Discovering the reconnaissance method may provide an opportunity for detection and to determine possible intent.)
- Is lateral movement suspected or known? How is lateral movement conducted (e.g., RDP, network shares, malware, etc.)?
- Has data been exfiltrated and, if so, what kind and via what mechanism?

https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks

Incident Response vs Digital Forensics

- **Incident Response (IR)** is immediate and aimed at stopping threats and reducing impact during an incident to resume normal business operations.
- **Digital Forensics (DF)** is about precision—collecting, preserving, and analyzing evidence for legal or potential legal matters (civil or criminal).



https://brettshavers.com/brett-s-blog/entry/dfirs-degree-debate-do-degrees-deliver-or-does-direct-experience-dominate-in-digital-forensics

Incident Response vs Digital Forensics

Aspect	Incident Response (IR)	Digital Forensics (DF)
Primary Objective	Manage and mitigate security incidents	Collect, preserve, and analyze digital evidence
End Goal	Contain and recover from attacks quickly	Provide evidence for legal proceedings
Role Focus	Incident responder or analyst	Examiner or analyst
Evidence Handling	Focused on system recovery and containment	Strict chain of custody and preservation
Legal Standards	May not meet legal standards unless specified	Meets courtroom admissibility standards
Time Sensitivity	Highly time-sensitive for operational recovery	Not as time-sensitive unless court deadlines
Typical Context	Cybersecurity incidents, breaches, and intrusions	Criminal, civil, or regulatory investigations
Use of Tools	Uses similar tools for rapid analysis	Uses forensic tools for evidence extraction
Training Emphasis	Emphasizes quick action and recovery	Emphasizes legal procedures and evidence integrity
Mindset	Operational and urgent	Legal and methodical
Reporting	Reports focus on recovery steps and impact for business	Detailed and legally sound reports for legal proceedings

https://brettshavers.com/brett-s-blog/entry/should-df-be-separated-from-ir-1

Containment

- Isolating impacted systems and network segments from each other and/or from non-impacted systems and networks.
- Capturing forensic images to preserve evidence for legal use (if applicable) and further investigation of the incident.
- Updating firewall filtering.
- Blocking (and logging) of unauthorized accesses; blocking malware sources.
- Closing specific ports and mail servers or other relevant servers and services.
- Changing system admin passwords, rotating private keys, and service/application account secrets.
- Directing the adversary to a sandbox to monitor the actor's activity, gather additional evidence, and identify attack vectors.

https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks

Eradication

Remediating all infected IT environments.

Rebuilding systems from scratch.

Replacing compromised files with clean versions.

Installing patches.

Resetting passwords on compromised accounts.

Monitoring for any signs of activities.

https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks

Recovery

Reconnecting rebuilt/new systems to networks.

Tightening perimeter security and zero trust access rules.

Testing systems thoroughly—including security controls.

Monitoring operations for abnormal behaviors.

https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks

Lessons Learned

Ensuring root-cause has been eliminated or mitigated.

Identifying infrastructure problems to address.

Identifying organizational policy and procedural problems to address.

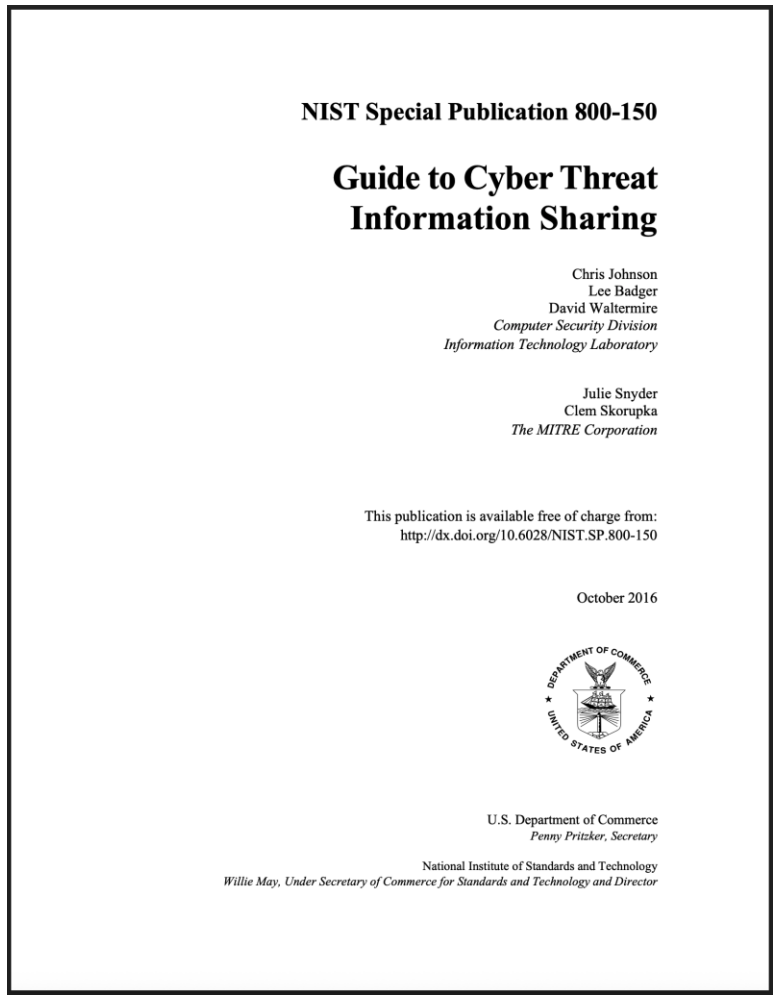
Reviewing and updating roles, responsibilities, interfaces, and authority to ensure clarity.

Identifying technical or operational training needs.

Improving tools required to perform protection, detection, analysis, or response actions.

https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks

Threat Information Sharing



NIST Special Publication 800-150

Guide to Cyber Threat Information Sharing

Chris Johnson
Lee Badger
David Waltermire
Computer Security Division
Information Technology Laboratory

Julie Snyder
Clem Skorupka
The MITRE Corporation

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-150

October 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

https://csrc.nist.gov/pubs/sp/800/150/final

Table 3-2: Handling Recommendations for Selected Types of Sensitive Data

Type of Threat Information	Examples of Sensitive Data Elements[9]	Recommendations
Network Indicators	Any single network indicator can be sensitive, but network indicators in the aggregate are often more sensitive because they can reveal relationships between network entities. By studying these relationships it may be possible to infer the identity of users, gather information about the posture of devices, perform network reconnaissance, and characterize the security safeguards and tools that an organization uses.	Focus on the exchange of network indicators such as destination IP addresses associated with an actor's command and control infrastructure, malicious URLs/domains, and staging servers. Before sharing, anonymize or sanitize network indicators that contain IP or MAC addresses of target systems or addresses registered to your organization. Also anonymize or sanitize indicators that may reveal the structure of internal networks, or ports or protocols that identify particular products.
Phishing Email Samples	Email headers may contain information such as: • Mail agent IP addresses, • Host or domain names, and • Email addresses. An email message body may also contain PII, CUI, or other types of sensitive information.	Organizations should anonymize email samples and remove any sensitive information that is not necessary for describing an incident or event of interest.
System, Network, and Application Logs	Log files may contain PII, CUI or other types of sensitive information. Log data may reveal IP addresses, ports, protocols, services, and URLs, as well as connection strings, logon credentials, portions of financial transactions, or other activities captured in URL parameters.	Organizations should perform IP address, timestamp, port, and protocol anonymization and remove any sensitive information that is not necessary for describing an incident or event of interest. Before sharing log data, it may also be necessary to sanitize URLs that contain identifying information such as session or user identifiers. Application logs may require redaction and anonymizing operations that are specific to particular application log formats.
Malware Indicators and Samples	Although organizations are unlikely to encounter sensitive information in malware indicators or samples, sensitive information may be present depending on how targeted the malware is and what collection methods were used to gather a sample.	Organizations should remove PII, CUI, and other types of sensitive information that is not necessary for describing an incident or event of interest.

Handling Mistakes

r/cybersecurity • 11 hr. ago
cautiously-excited

Handling Mistakes as Level 1 SOC Analyst

Starting Cybersecurity Career

I've been at my first legitimate cybersecurity job for almost 3 months. In that time I've handled about 1,024 security alerts but I screwed up today for I think the 3rd time. I improperly handled an incident bc I accidentally overlooked a log entry and my manager caught it pretty quick and brought me into a call to tell me it was gross negligence on my part (which I won't deny as I should have looked at more than just the last week of logs). As I said, this isn't the first time I've made a mistake and I'm really scared that they are going to fire me (idk why I have a mental image of three strikes and you're out). In all 3 mistakes I usually spend the next week going at about half the speed I usually do bc I'm so paranoid. So my question is how do yall handle alerts so quickly while minimizing mistakes and how do you handle the inevitable mistakes that DO happen?

https://www.reddit.com/r/cybersecurity/comments/1ldwx2y/comment/mybrlx8/

Kesshh • 11h ago

From someone who have managed multiple tech teams for 20+ years, my answer is always the same. I just spend $x (whatever the true cost of the mistake was) training you, why would I want to get rid of you?

But I'm not your boss, his disposition might differ.

Here's something to keep in mind.

1. Everyone makes mistakes. Sometimes they are big, sometimes they are small. But everyone does.
2. Making mistakes is part of learning. The impression of making those mistakes cannot be replicated by any other methods.
3. Recognized there are mistakes, negligence, and gross negligence. They are not the same things. Negligence and gross negligence has an element of not caring. Not caring and not careful are different. If it is an honest mistake, you should recognize that. Other people's judgment might be oriented differently.

To your specific question, not making silly mistakes has to do with having and following procedures. In cyber, this is especially important because you need to collect not just data and information, but also your steps/procedures so you can prove your (and in context your department's) due diligence with evidence. Ask yourself, if you have procedures, did you follow them? If you have check lists, did you check them off? If what you missed wasn't on the list, maybe a more detailed list or procedure is warranted. If what you missed was on the list, did you check them off in error? How would you minimize the same error next time?

With our craft, it isn't about "being more careful next time". That's not a control. Think about the controls you need to ensure that would be a good exercise.

After all that, in the end, don't beat yourself up too badly. If no one died, if no customers lost money, if your shop didn't lose money, you can recover.

73 Reply 2 Share

Wellbeing for Incident Responders

These should be embedded in cyber-readiness activities and (where relevant) documented in cyber incident response plans and playbooks.

1. **Acknowledgment:** openly acknowledge the mental health and wellbeing challenges confronting cyber defence and incident response teams and key decision-makers (including senior executives and directors) with those stakeholders as part of incident response planning.
2. **Preparation and training:** proactively train staff on what to expect during a cyber incident (including evolving threat actor tactics) and incorporate relevant challenges into cyber simulations—this helps reduce fear and uncertainty, which can be significant stressors during such an event. Training for leaders should address how best to manage and support staff during a major incident. Training for the broader executive, cyber defence and incident response teams should include coping strategies for stress management and a focus on building resilience. Organisations like Cybermindz can also help provide proactive support for cyber professionals.
3. **Mental health first aid officers:** establish a team of trained mental health first aid officers who can provide initial support and guidance to those experiencing mental health difficulties during a crisis.
4. **Employee Assistance Programs (EAP):** EAPs offer confidential counselling services to employees dealing with personal or work-related problems that might impact their job performance, health and wellbeing. Ensure these services are well-advertised and easily accessible. Most EAPs can also provide proactive 'check-in' calls or onsite support to ensure staff at high risk are provided with support and coping strategies during the incident, rather than after.
5. **Regular communication:** keep lines of communication open before, during and after an incident. Regular updates (even where there is no new information) can help alleviate some of the stress that comes with uncertainty.
6. **Monitoring and check-ins:** working hours should be monitored, with time off scheduled during peak periods. Wellbeing check-ins should also be conducted. If leaders are going to be involved in high-stress activities with reduced sleep, ensure they have someone (either a leader not doing long hours or EAP/similar) undertaking regular check-ins.
7. **Flexible work arrangements:** during high-stress periods, allow flexible work arrangements to help staff balance their workload with other life responsibilities.
8. **Resourcing:** consider the potential for additional resourcing to assist through the crisis period to help manage high workload and demands.
9. **Post-incident support:** after the immediate threat has passed, continue providing resources for staff to cope with any lingering stress or trauma related to the incident—this could involve debriefing sessions or continued access to counselling services.

3 Andrew Reeves, Malcolm Pattinson and Marcus Butavicius, 'Is Your CISO Burnt Out Yet? Examining Demographic Differences in Workplace Burnout amongst Cyber Security Professionals' (2023) *Human Aspects of Information Security and Assurance* 11.

WHS regulatory activity and the management of psychosocial risks

Organisations have had a general safety obligation to manage psychological risks to their workforce for some time now. However, the risk of psychological injury arising out of factors present in the work environment has received significantly more focus in the past few years, particularly with the introduction of WHS regulations (in all states except Victoria) that specifically address psychosocial risk.

Under safety legislation, businesses must proactively identify psychosocial hazards arising from the workplace environment and put in place measures to control those hazards as far as is reasonably practicable.

Regulatory activity arising out of psychosocial risk factors has also increased. In some states, specialist psychosocial inspectors have been appointed and enforcement action arising out of alleged failures to manage psychosocial risk are becoming more common.

A recent example was the prosecution of the Court Services Victoria (CSV) following the death by suicide of one worker and numerous others taking stress leave. CSV, which is the independent statutory body that administers Victoria's court system, was sentenced in the Melbourne Magistrates' Court last year and fined $379,157 after earlier pleading guilty to failing to provide and maintain a safe workplace. The court heard that, from December 2015 to September 2018, workers at the Coroner's Court were at risk from exposure to traumatic materials, role conflict, high workloads and work demands, poor workplace relationships and inappropriate workplace behaviours.

The decision reflects the importance of organisations ensuring that, as far as is reasonably practicable, they identify risks inherent in the work their employees do every day, and implement effective control measures to prevent harm from arising. This obligation extends to the foreseeable stressors that could arise for staff in the event of a cyber incident.

https://www.allens.com.au/insights-news/insights/2024/03/why-organisations-must-embed-mental-health-and-wellbeing-support-into-cyber-incident-response-planning/

Incident Response Playbook

SANS DFIR

Ransomware and Cyber Extortion

POSTER

digital-forensics.sans.org

Poster was created by Kathryn Hedley and Ryan Chapman based on the research and knowledge of Ryan Chapman in authoring FOR528.

DFIR_FOR528_0124

Overview: Ransomware and Cyber Extortion

The term "ransomware" was originally used to reference the malware itself. We now call this the "payload" or "encryptor." The general term "ransomware" is now used to reference the overall attack campaign, which includes all stages of the attack. Some ransomware attacks include the deployment of a payload/encryptor, whereas others do not. These latter attacks may alternatively be referred to as "cyber extortion."

RaaS Business Model – Roles and Participation

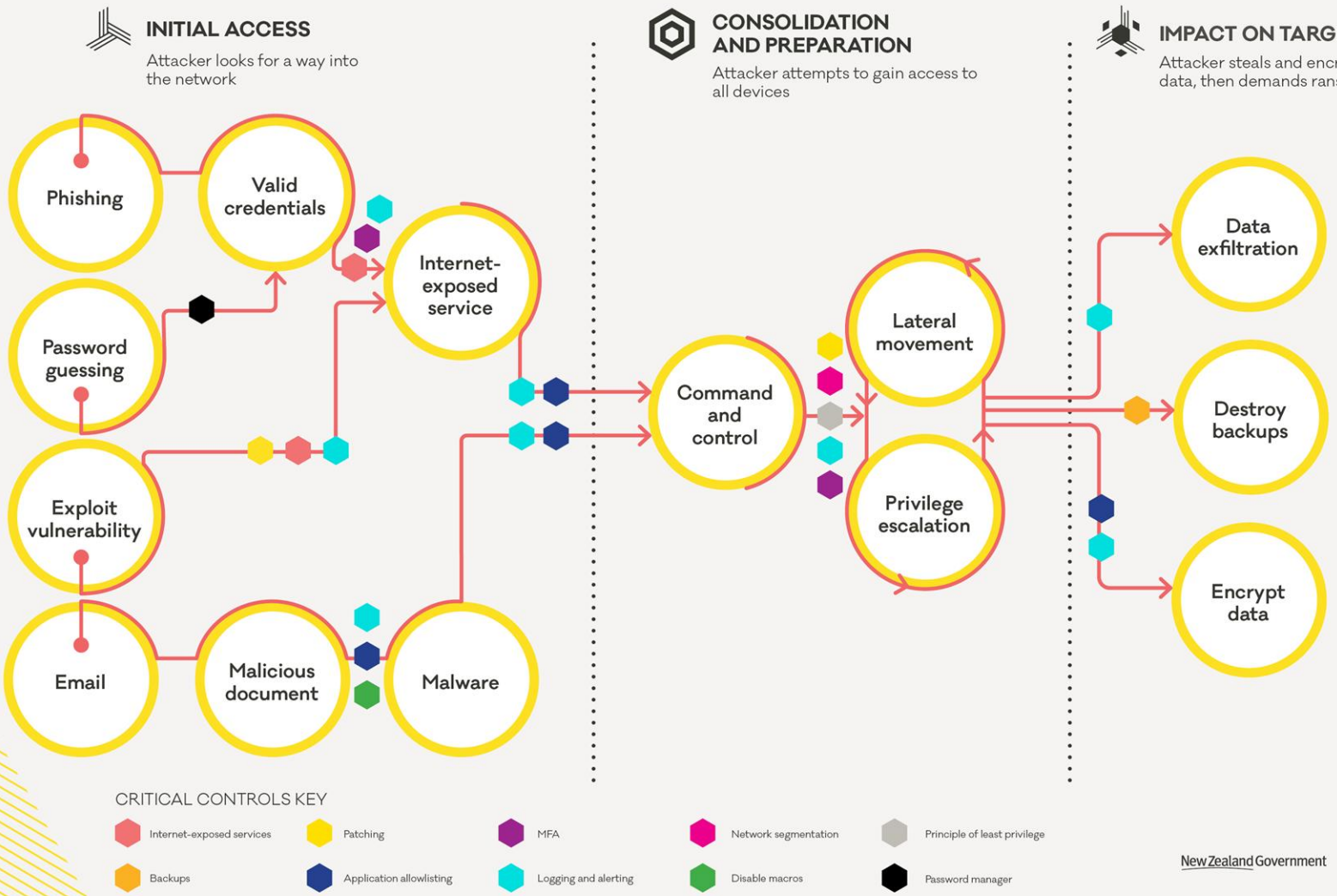
Each role is critical to the success of the ransomware campaign.

https://www.sans.org/posters/ransomware-and-cyber-extortion/

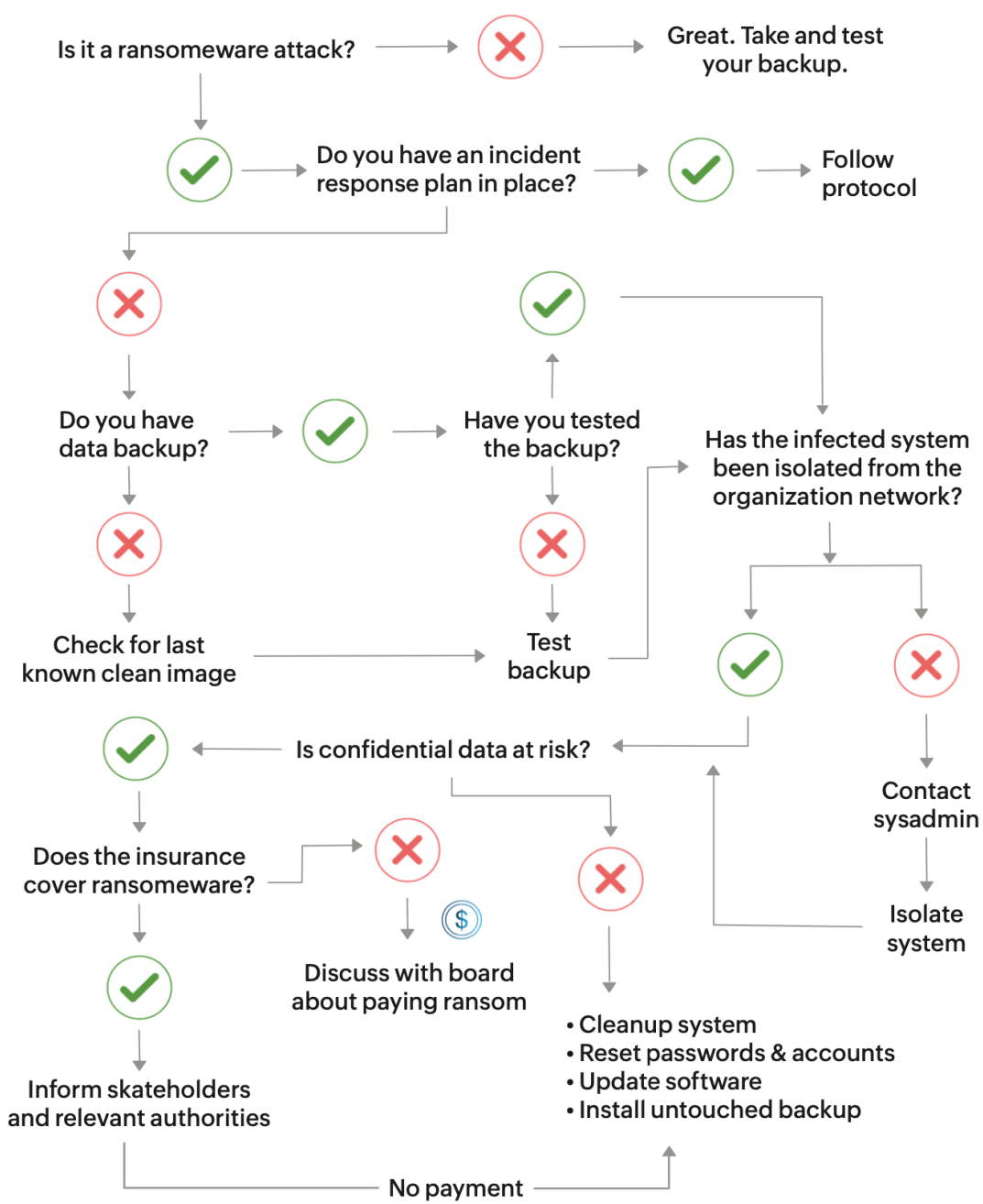
LIFECYCLE OF A RANSOMWARE INCIDENT

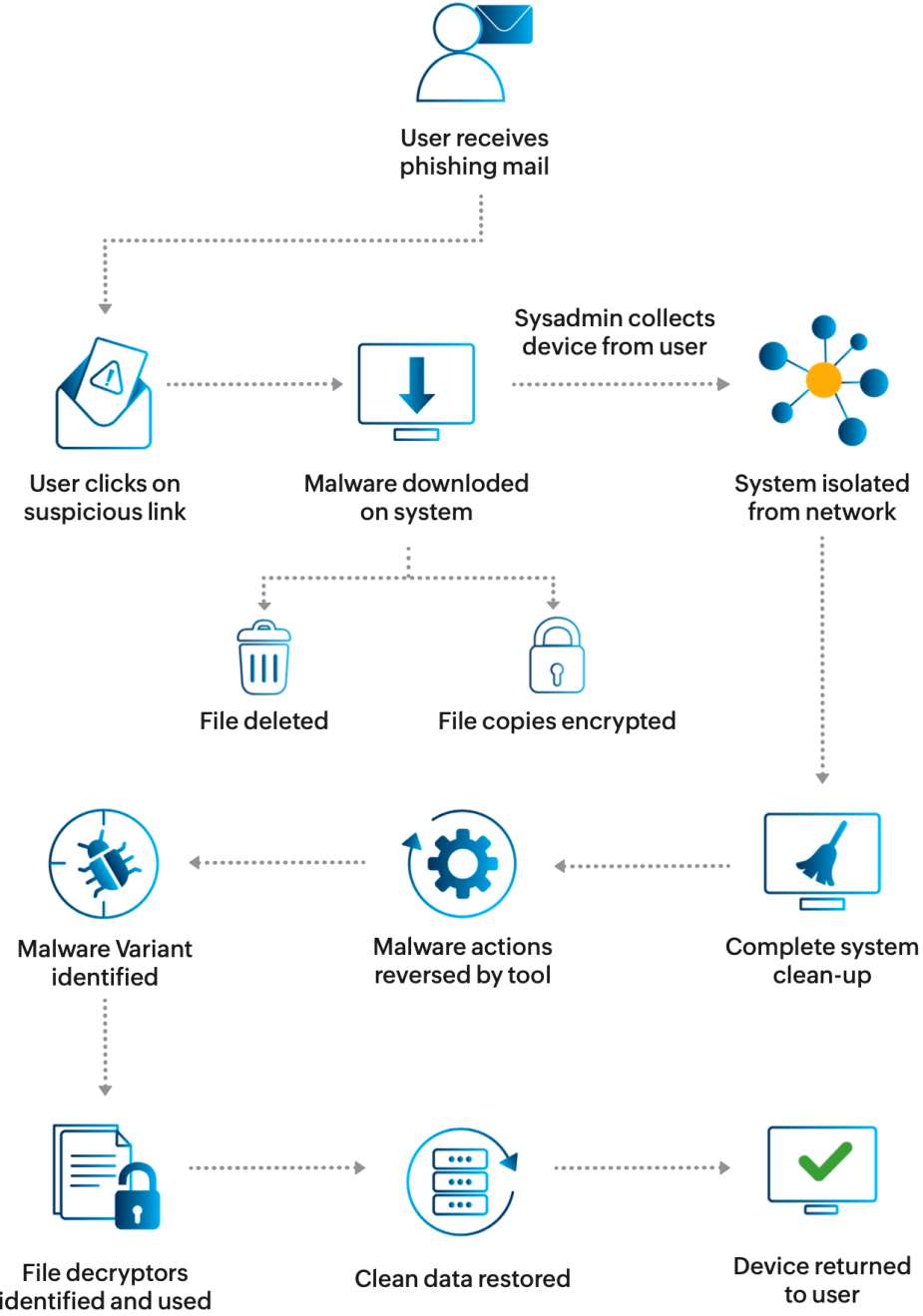
certnz

How the CERT NZ Critical Controls can help you stop a ransomware attack in its tracks.



https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/





https://www.manageengine.com/academy/ransomware-response-plan.html

Ransomware IR Playbook

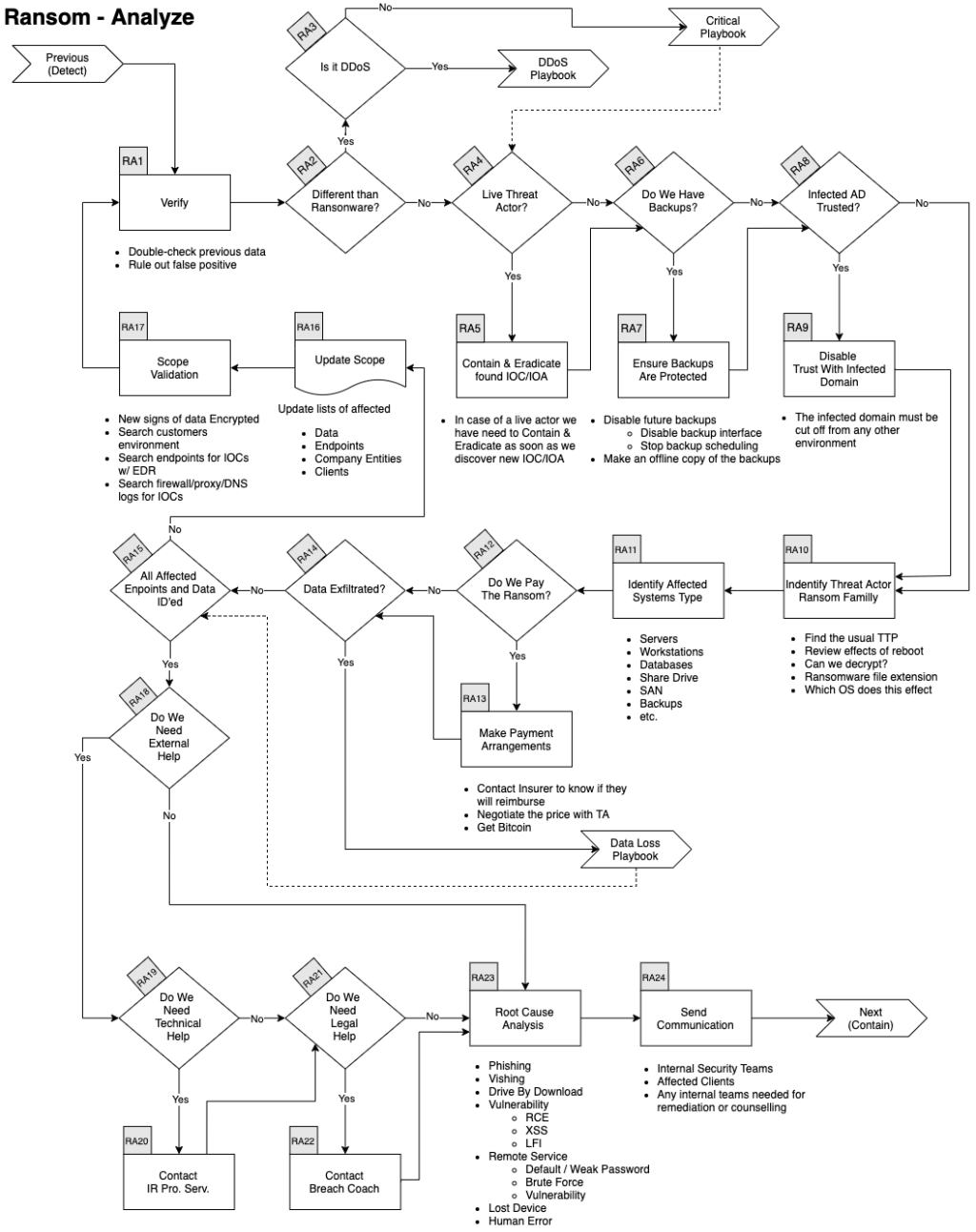
Public Playbooks

main ▾ playbooks — Find file — Code ▾

Initial Commit
@Scoubi authored Jul 23, 2021 — 797ef4cf — History

Name	Last commit	Last update
Customers	Initial Commit	3 years ago
IRP-AccountCompromised	Initial Commit	3 years ago
IRP-Critical	Initial Commit	3 years ago
IRP-DataLoss	Initial Commit	3 years ago
IRP-Malware	Initial Commit	3 years ago
IRP-Phishing	Initial Commit	3 years ago
IRP-Ransom	Initial Commit	3 years ago
Products	Initial Commit	3 years ago
Tools	Initial Commit	3 years ago
.gitignore	Initial Commit	3 years ago
IRP-TEMPLATE.md	Initial Commit	3 years ago
README.md	Initial Commit	3 years ago
TEMPLATE-Incident_EventLog.xlsx	Initial Commit	3 years ago

https://gitlab.com/syntax-ir/playbooks



TLP:CLEAR

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

#StopRansomware Guide

Publication: October 2023

Disclaimer: *This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp/.*

TLP:CLEAR

Part 1: Ransomware and Data Extortion Preparation, Prevention, and Mitigation Best Practices

These recommended best practices align with the CPGs developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. For more information on the CPGs and recommended baseline protections, visit CISA's Cross-Sector Cybersecurity Performance Goals.

Preparing for Ransomware and Data Extortion Incidents

Refer to the best practices and references listed in this section to help manage the risks posed by ransomware and to drive a coordinated and efficient response for your organization in the event of an incident. Apply these practices to the greatest extent possible pending the availability of organizational resources.

- **Maintain offline, encrypted backups of critical data**, and regularly test the availability and integrity of backups in a disaster recovery scenario [CPG 2.R]. Test backup procedures on a regular basis. It is important that backups are maintained offline, as most ransomware actors attempt to find and subsequently delete or encrypt accessible backups to make restoration impossible unless the ransom is paid. Ransomware actors often hunt for and collect credentials stored in the targeted environment and use those credentials to attempt to access backup solutions; they also use publicly available exploits to target unpatched backup solutions.

  Automated cloud backups may not be sufficient because if local files are encrypted by an attacker, these files will be synced to the cloud, possibly overwriting unaffected data.

  - Maintain and regularly update "golden images" of critical systems. This includes maintaining image "templates" that have a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server [CPG 2.O].
    - Use infrastructure-as-code (IaC) to deploy and update cloud resources and keep backups of template files offline to quickly redeploy resources. IaC code should be version controlled and changes to the templates should be audited.
    - Store applicable source code or executables with offline backups (as well as escrowed and license agreements). Rebuilding from system images is more efficient, but some images will not install on different hardware or platforms correctly; having separate access to software helps in these cases.

Part 2: Ransomware and Data Extortion Response Checklist

Should your organization be a victim of ransomware, follow your approved IRP. The authoring organizations strongly recommend responding by using the following checklist. Be sure to move through the **first three steps in sequence.**

The authoring organizations do not recommend paying ransom. Paying ransom will not ensure your data is decrypted, that your systems or data will no longer be compromised, or that your data will not be leaked.

Additionally, paying ransoms may pose sanctions risks. For information on potential sanctions risks, see U.S. Department of the Treasury Office of Foreign Assets Control (OFAC) memorandum from September 2021, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments. The updated advisory states that Treasury's Office of Foreign Assets Control (OFAC) would consider 'mitigating factors' in related enforcement actions. Contact your local FBI field office, in consultation with OFAC, for guidance on mitigating penalty factors after an attack.

Detection and Analysis

Refer to the best practices and references below to help manage the risk posed by ransomware and support your organization's coordinated and efficient response to a ransomware incident. Apply these practices to the greatest extent possible based on availability of organizational resources.

- ☐ **1. Determine which systems were impacted, and immediately isolate them.**
  - ☐ If several systems or subnets appear impacted, take the network offline at the switch level. It may not be feasible to disconnect individual systems during an incident.
  - ☐ Prioritize isolating critical systems that are essential to daily operations.
  - ☐ If taking the network temporarily offline is not immediately possible, locate the network cable (e.g., ethernet) and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.
  - ☐ For cloud resources, take a snapshot of volumes to get a point in time copy for reviewing later for forensic investigation.
  - ☐ After an initial compromise, malicious actors may monitor your organization's activity or communications to understand if their actions have been detected. Isolate systems in a coordinated manner and use out-of-band communication methods such as phone calls to avoid tipping off actors that they have been discovered and that mitigation actions are being undertaken. Not doing so could cause actors to move laterally to preserve their access or deploy ransomware widely prior to networks being taken offline.
- ☐ **2. Power down devices if you are unable to disconnect them from the network to avoid further spread of the ransomware infection.**

  Note: This step will prevent your organization from maintaining ransomware infection artifacts and potential evidence stored in volatile memory. **It should be carried out only if it is not possible to temporarily shut down the network or disconnect affected hosts from the network** using other means.

https://www.cisa.gov/resources-tools/resources/stopransomware-guide

OFF THE BEATEN PATH

Feed Me Seymour

After a ransomware attack there are going to be a lot of people working very long hours, often around the clock, to get your organization up and running again.

Feed them.

Not just warmed-over pizza once a day. Include food planning in your IR plan. Plan for breakfast, lunch, and dinner, as well as enough beverages to keep everyone fully engaged. You lose precious time every time someone, or more likely, some group, goes out to eat together. Feeding everyone, ultimately, saves money.

Also consider the responders' mental health. These are long days filled with tedious work, so encourage everyone to take a break, stretch, and get some exercise. If there are walking/running paths nearby, let the team know. If your building has a gym, arrange for everyone doing IR to have 24-hour access to it. Keeping everyone mentally and physically fit is going to make the incident response go more smoothly and finish up more quickly.

https://go.recordedfuture.com/ransomware-understand-prevent-recover-third-edition

Recommended Materials

- NCSC – Incident Management (https://www.ncsc.gov.uk/collection/incident-management)
- CISA – Cybersecurity Incident & Vulnerability Response Playbooks (https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf)
- CISA – Technical Approaches to Uncovering and Remediating Malicious Activity (https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-245a)
- HHS – Cyber Security Incident Response Plan (https://www.hhs.gov/sites/default/files/cybersecurity-incident-response-plans.pdf)
- Microsoft – Navigating the Maze of Incident Response (https://www.microsoft.com/en-us/security/blog/2023/12/11/new-microsoft-incident-response-team-guide-shares-best-practices-for-security-teams-and-leaders/)

Questions?