SANS Threat Hunting & IR Summit 2018
2018.09.06-09.07

\Orchestrating a brighter world NEC

Launching Threat Hunting from Almost Nothing

Takahiro Kakumaru, CISSP
NEC Corporation

Who am I

- Takahiro Kakumaru, CISSP
  Assistant Manager
  Cyber Security Strategy Division
  NEC Corporation
  <t-kakumaru@ap.jp.nec.com>

- Focus : Cyber Threat Intelligence, Threat Hunting, Cyber Threat Intelligence sharing & consumption

- Activities : OASIS CTI TC & OpenC2 TC member, Talk at FIRST2016

- Play & coach ice hockey

Disclaimer: "The opinions expressed in this presentation and on the following slides are solely those of the presenters and not necessarily those of their employers."

My favorite quote

"A good hockey player plays where the puck is. A great hockey player plays where the puck is going to be."

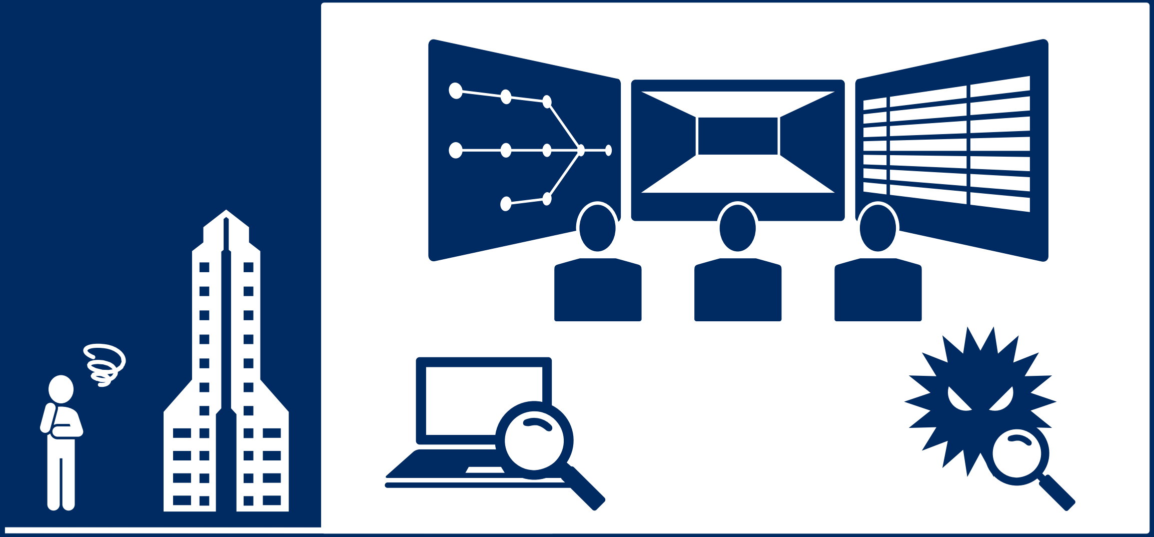
Wayne Gretzky "The Great One", the greatest hockey player ever

Today’s talk

“How can we incorporate threat hunting functions into the current security operations which don’t have a sophisticated hunter?”

Threat Hunting Techniques

Threat Hunter


Security Operations in the enterprise

Why I am here today

1. To share case study focusing on threat hunting operations in enterprise security operations.
2. To emphasize the importance of the process, communication, and culture.

Note: This presentation is going to be about operations, not specific hunting techniques.

Agenda

1. Introduction to Threat Hunting Operations
2. Let’s get quick win!
3. Building Threat Hunting Operations
4. Threat Hunting Case Study
5. Threat Hunting Operations At Scale
6. Threat Hunting Operations Framework

Introduction to Threat Hunting Operations

Threat Hunting is the PROCESS

"Cyber Threat Hunting is the <u>process</u> of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions."

https://sqrrl.com/media/Framework-for-Threat-Hunting-Whitepaper.pdf

Characteristics of a THREAT HUNTER

“Threat Hunter is a cybersecurity threat analyst who uses proactive methods to uncover security incidents that might otherwise go undetected.”

“Communicative”

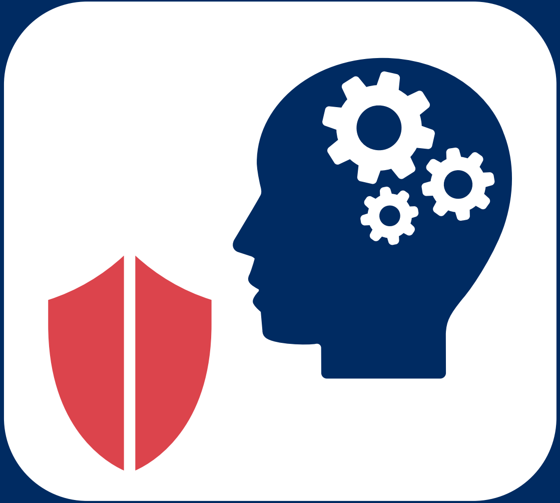
“Collaborative”

“Creative”

“Threat Awareness”

“Critical thinker”

“Business knowledge”

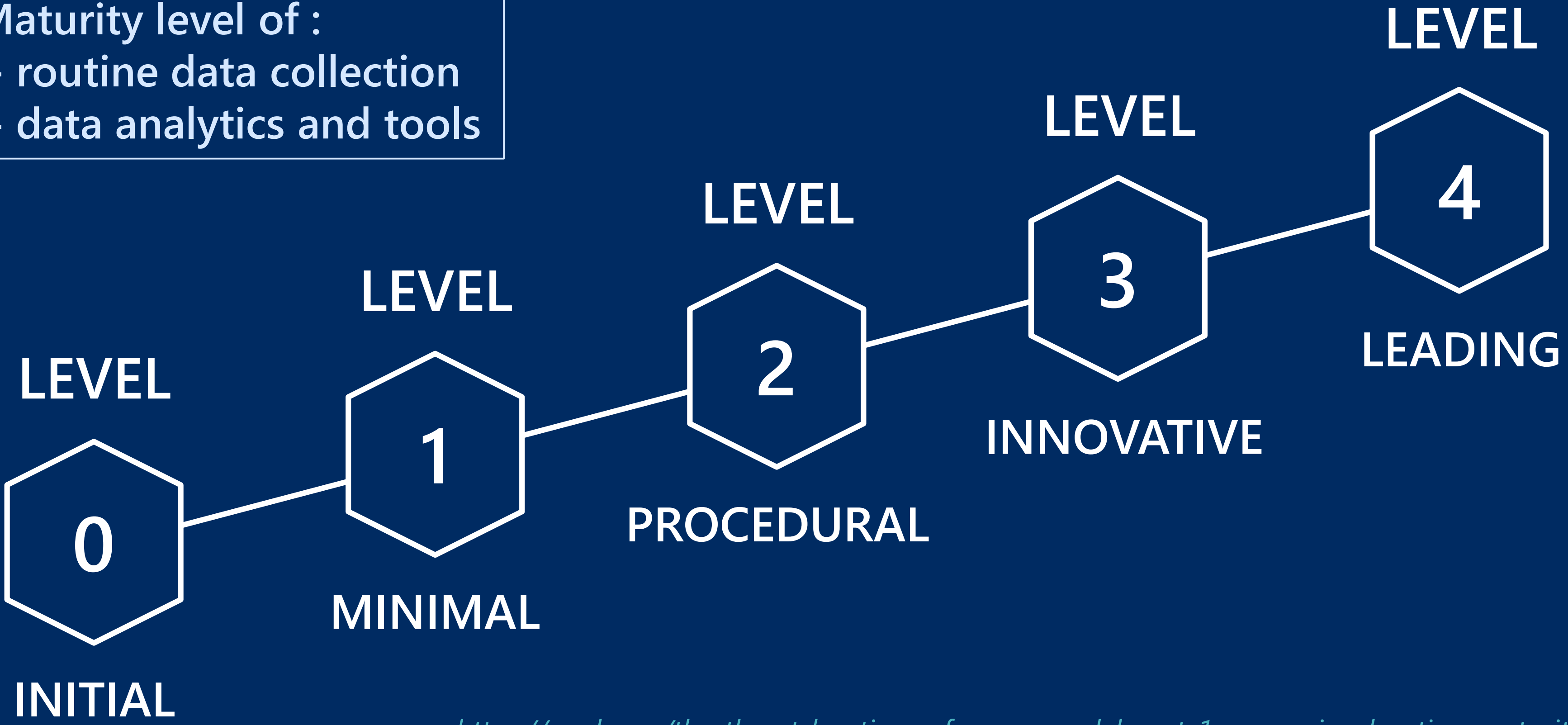


https://searchcio.techtarget.com/definition/threat-hunter-cybersecurity-threat-analyst

Threat Hunting Maturity Model (HMM)

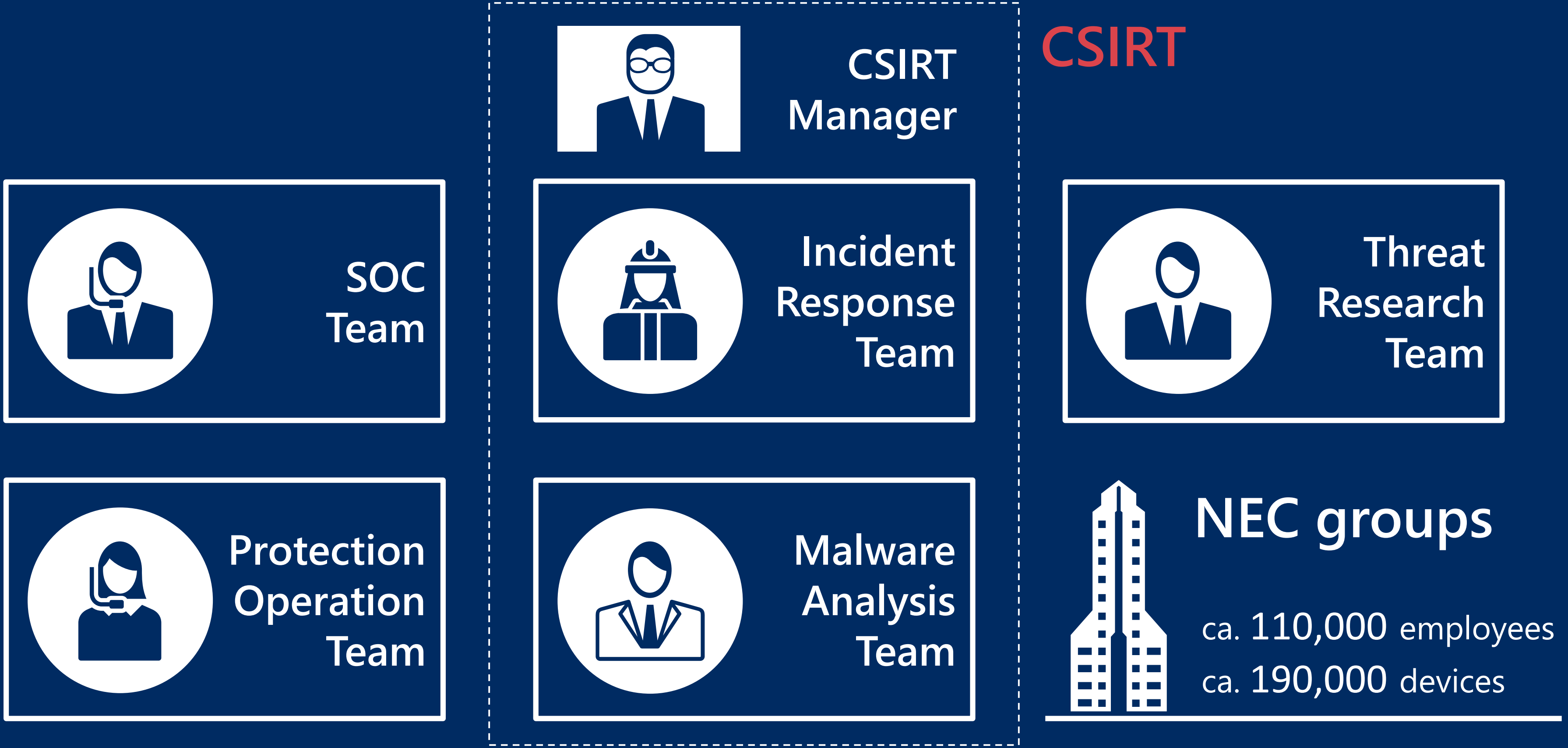
Maturity level of :

- routine data collection
- data analytics and tools



https://sqrrl.com/the-threat-hunting-reference-model-part-1-measuring-hunting-maturity/

Our Security Operations



CSIRT

CSIRT Manager

SOC Team

Incident Response Team

Threat Research Team

Protection Operation Team

Malware Analysis Team

NEC groups

ca. 110,000 employees

ca. 190,000 devices

Security Tools (1)

SOC Team

- Alerting System (IDS)
- Report from employee

Protection Operation Team

- Perimeter defense (Proxy, FW)
- Network Isolation (SDN)
- Patch Management System (NCSP)
- Information Sharing / Enlightenment

*NCSP: NEC Cyber Security Platform

Security Tools (2)

Incident Response Team

Forensic Tool

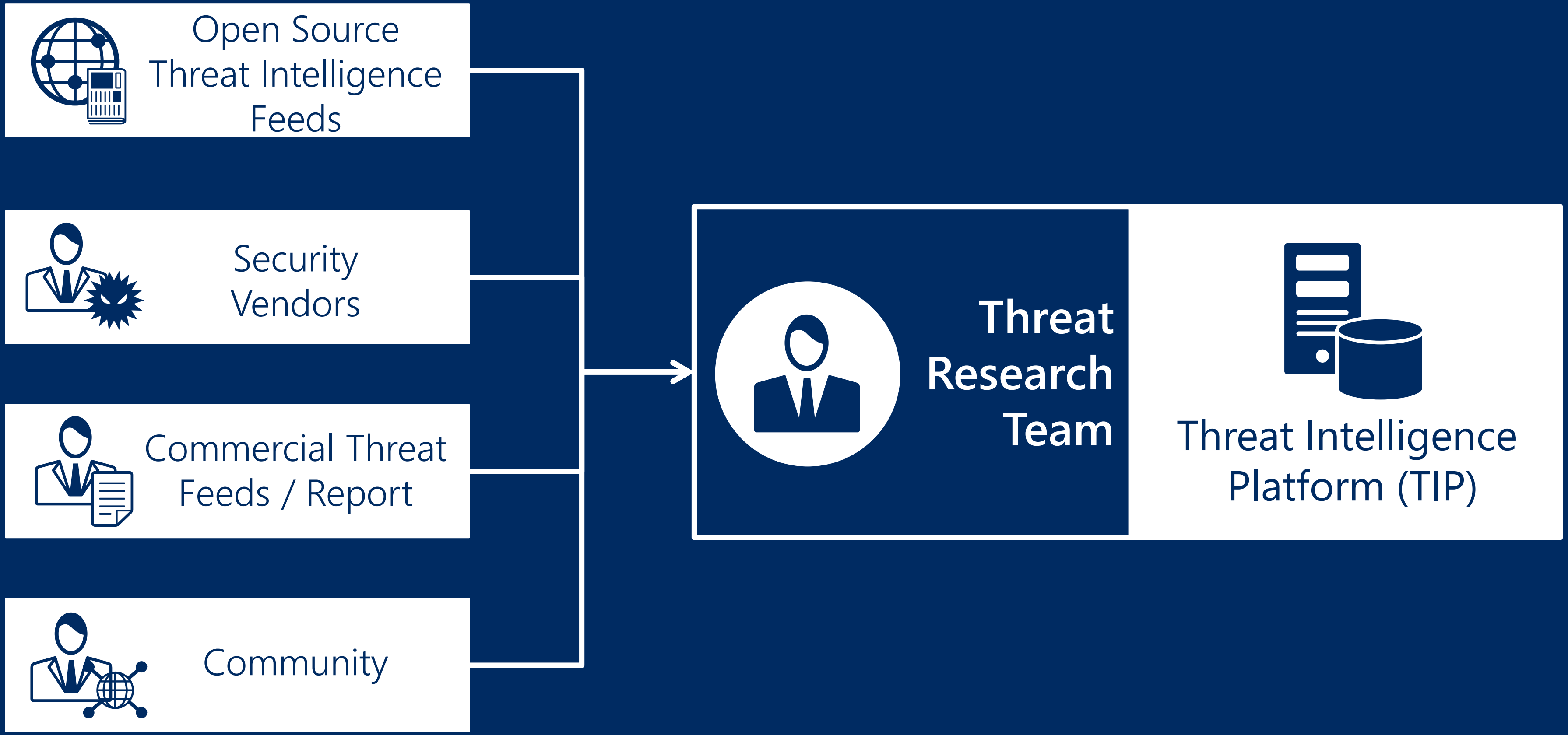
Log Management

Malware Analysis Team

Malware Analysis Tool

Malware DB

Security Tools (3)


Open Source Threat Intelligence Feeds
Security Vendors
Commercial Threat Feeds / Report
Community
Threat Research Team
Threat Intelligence Platform (TIP)

Let’s get quick win!

Let’s get quick win!

Primary Threat Hunting Techniques

- Searching
- Clustering
- Grouping
- Stack Counting

https://sqrrl.com/media/ebook-web.pdf

IOC searches

Indicators × Proxy log = ???

{IP address, URL} {IP address, URL}

Our First Threat Hunting Result

IOC searches finished!!!

0 (zero) matched.

Let’s confirm definition, again

“Threat Hunting is the PROCESS”

What we did

IOC searches

Indicators × Proxy log = ∅

{IP address, URL} {IP address, URL}

PROCESS or [✓ TECHNIQUE]

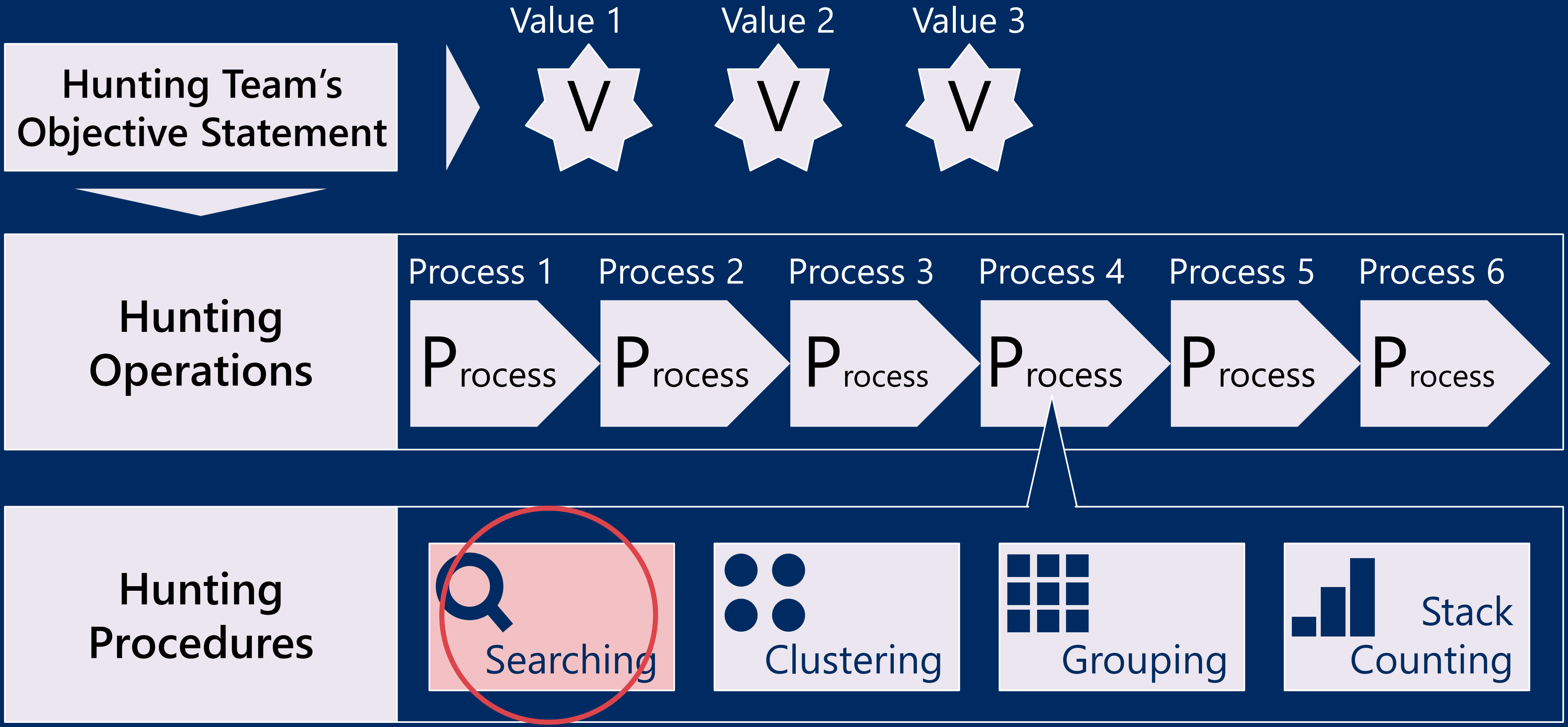
Building Threat Hunting Operations

KAIZEN

"The right process will produce the right results."

TOYOTA WAY

Outline of Threat Hunting Operations Framework



Hunting Team's Objective Statement

Hunting Operations

Hunting Procedures

Challenges

Challenge 1:

“for what?” and “so what?”

Challenge 2:

“workable operations”

Challenge #1 “For what?” and “So what?”

“For what?”

Core values of threat hunting

- Threat Hunting Loop (cycle)

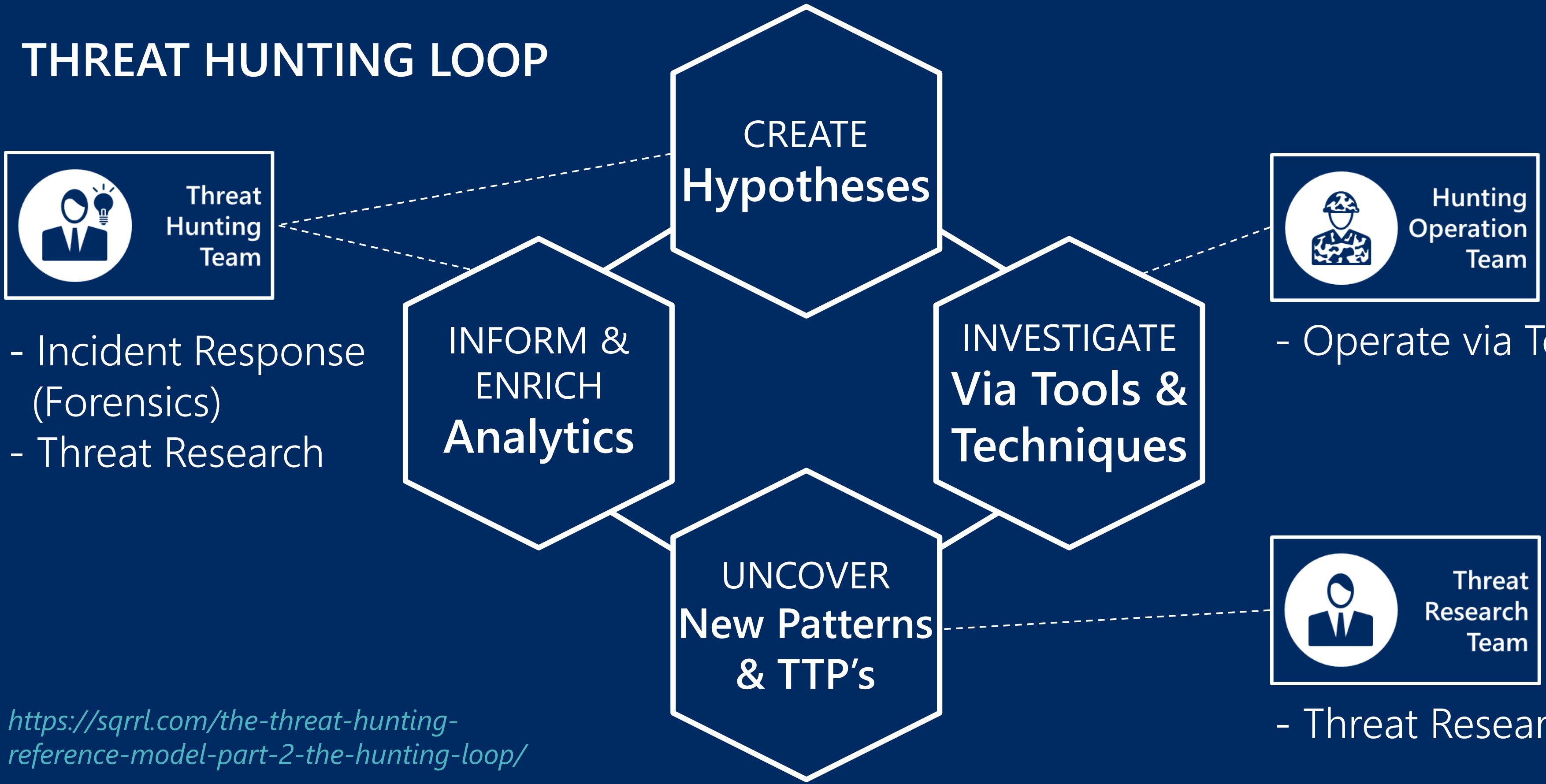
“So what?”

Actions after finding threat from hunting

- Remediation as quickly as possible
- Close detection gap (signatures, detection rules /algorithms)

Hunting Loop is "Core"

THREAT HUNTING LOOP



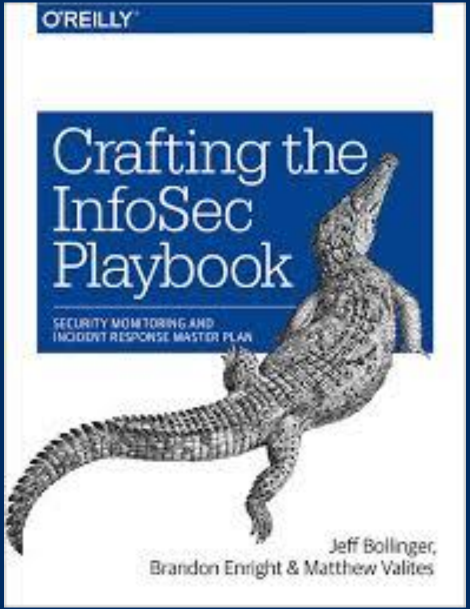
- Incident Response (Forensics)
- Threat Research

- Operate via Tools

- Threat Research

https://sqrrl.com/the-threat-hunting-reference-model-part-2-the-hunting-loop/

Actions lead to business goals



O'REILLY

Crafting the InfoSec Playbook

SECURITY MONITORING AND INCIDENT RESPONSE MASTER PLAN

Jeff Bollinger, Brandon Enright & Matthew Valites

"Crafting the InfoSec Playbook"

https://www.amazon.com/Crafting-InfoSec-Playbook-Security-Monitoring/dp/1491949406

"Understand business requirement enough before constructing the process."

Incident Response Team

Protection Operation Team

Define response policy in advance

- Escalation
- Precaution
- Mitigation
- Remediation

Challenges

Challenge 1:

"for what?" and "so what?"

Challenge 2:

"workable operations"

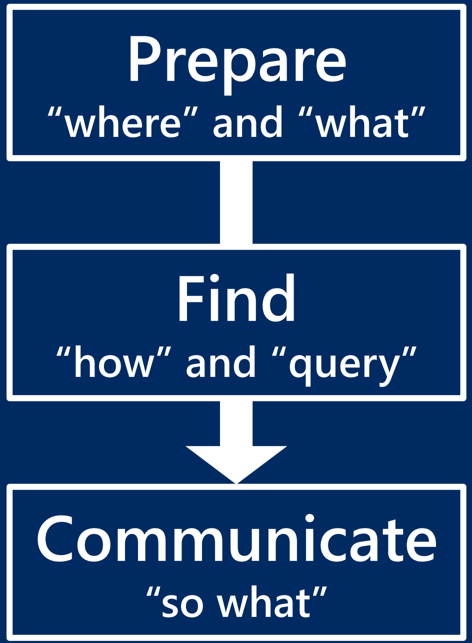
Challenge #2 : “workable operations”

High Process

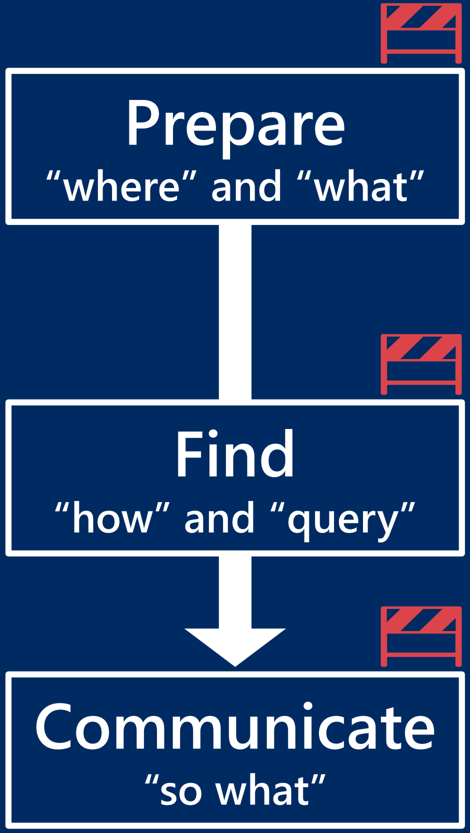
Prepare	- Ask a Question - Research - Hypothesis
Find	- Experiment - Working (Yes/No) - Troubleshoot
Commu-nicate	- Analyze and Draw Conclusions - Communicate All Results - Refactor include in Future Hunts

https://www.first.org/resources/papers/conf2017/Building-a-Threat-Hunting-Framework-for-the-Enterprise.pdf

Minimum Cycle



Jump the hurdle to getting the milestone



Prepare
"where" and "what"

Find
"how" and "query"

Communicate
"so what"

1. Simple first and collect from outside

a. Intelligence-driven
b. Situational awareness
c. Domain expertise

https://www.sans.org/reading-room/whitepapers/threats/generating-hypotheses-successful-threat-hunting-37172

2. Practicable execution procedure

a. Minimum data collection
b. User-friendly tools

3. Actionable course of actions

a. Understandable
b. Evidence to lead actions

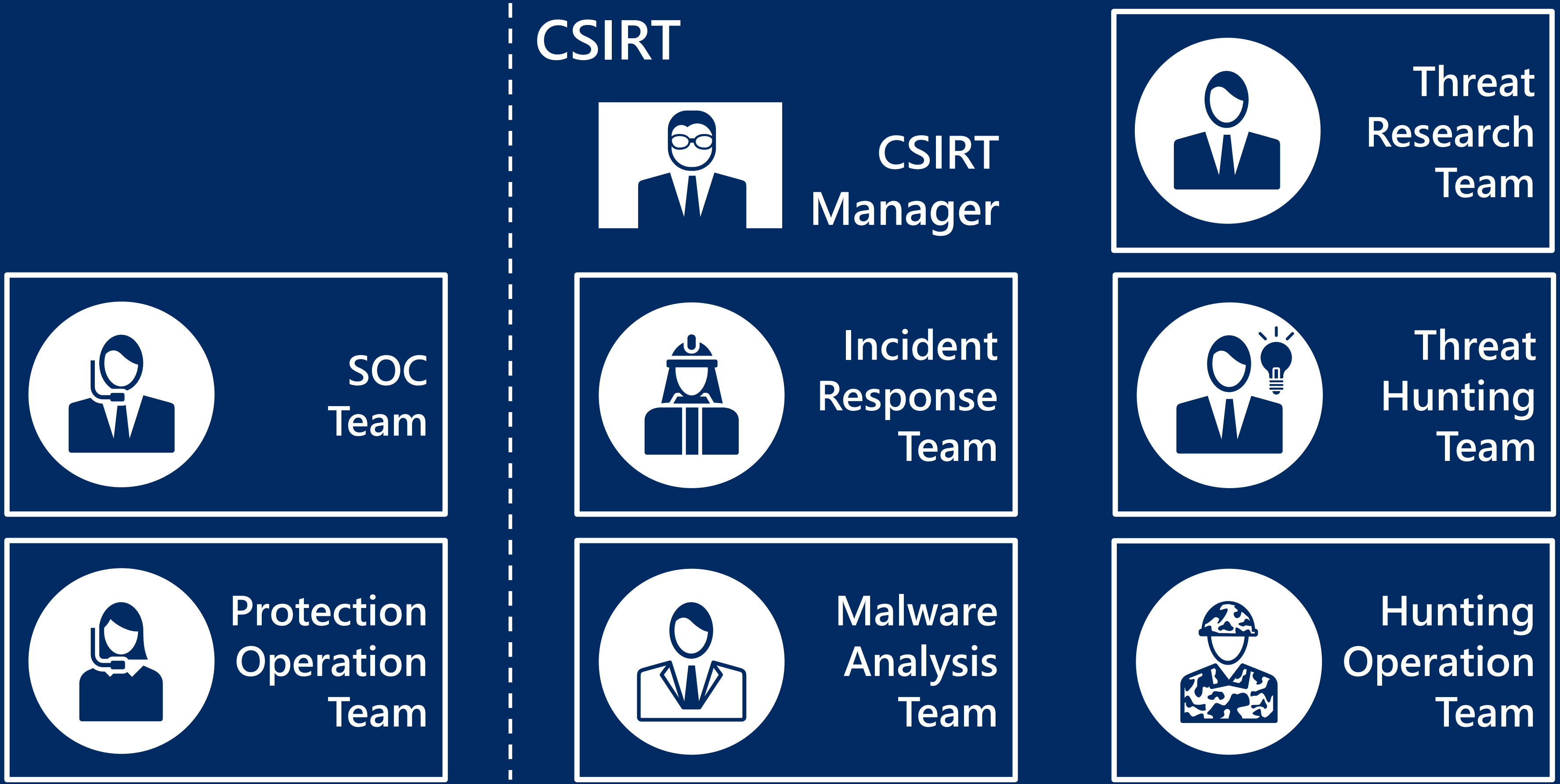
Threat Research Team

Threat Hunting Team

Hunting Operation Team

Incident Response Team

CSIRT with Threat Hunting Capabilities



CSIRT

CSIRT Manager

Threat Research Team

SOC Team

Incident Response Team

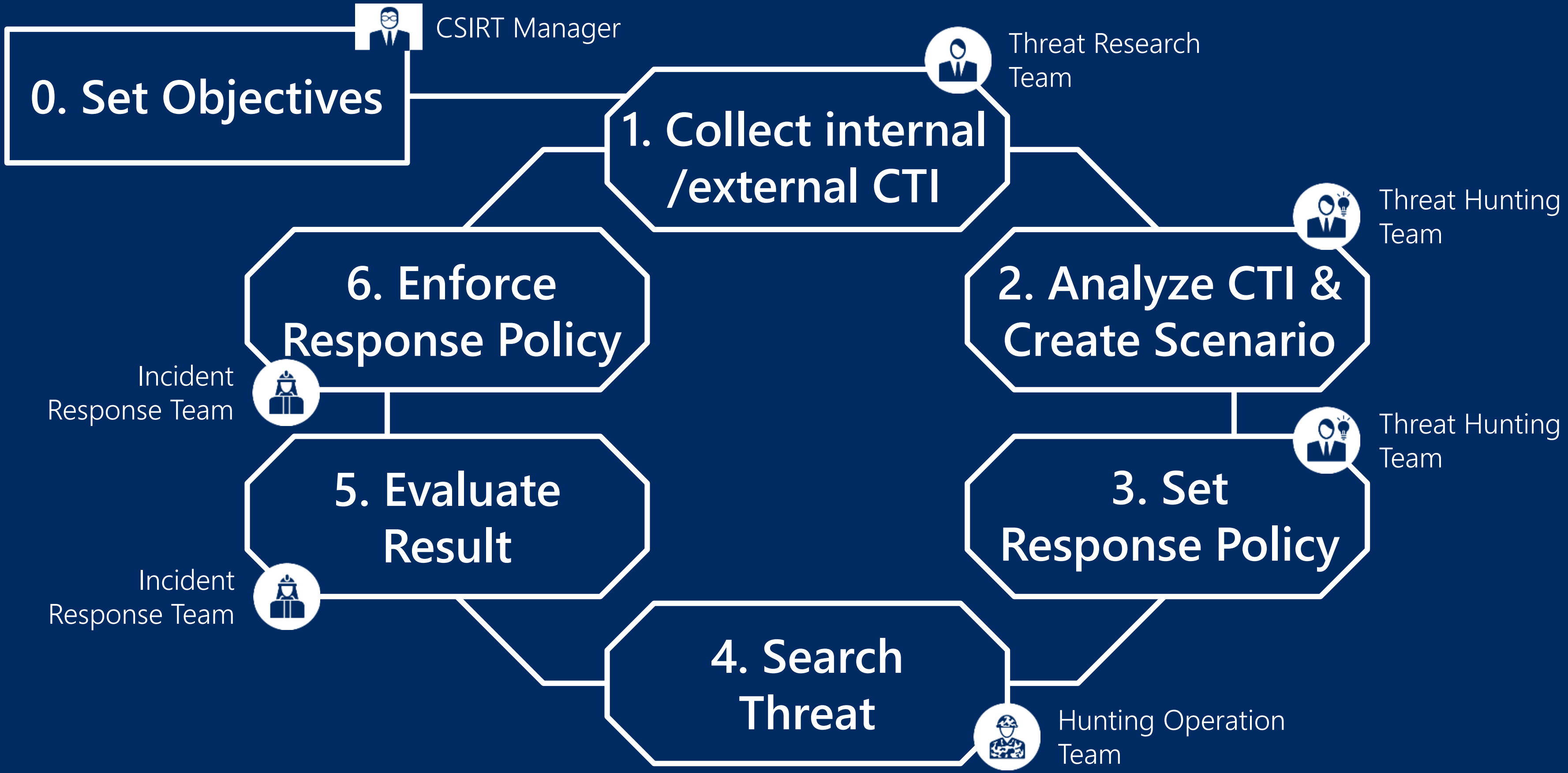
Threat Hunting Team

Protection Operation Team

Malware Analysis Team

Hunting Operation Team

Threat Hunting Operations



0. Set Objectives

CSIRT Manager

1. Collect internal /external CTI

Threat Research Team

2. Analyze CTI & Create Scenario

Threat Hunting Team

3. Set Response Policy

Threat Hunting Team

4. Search Threat

Hunting Operation Team

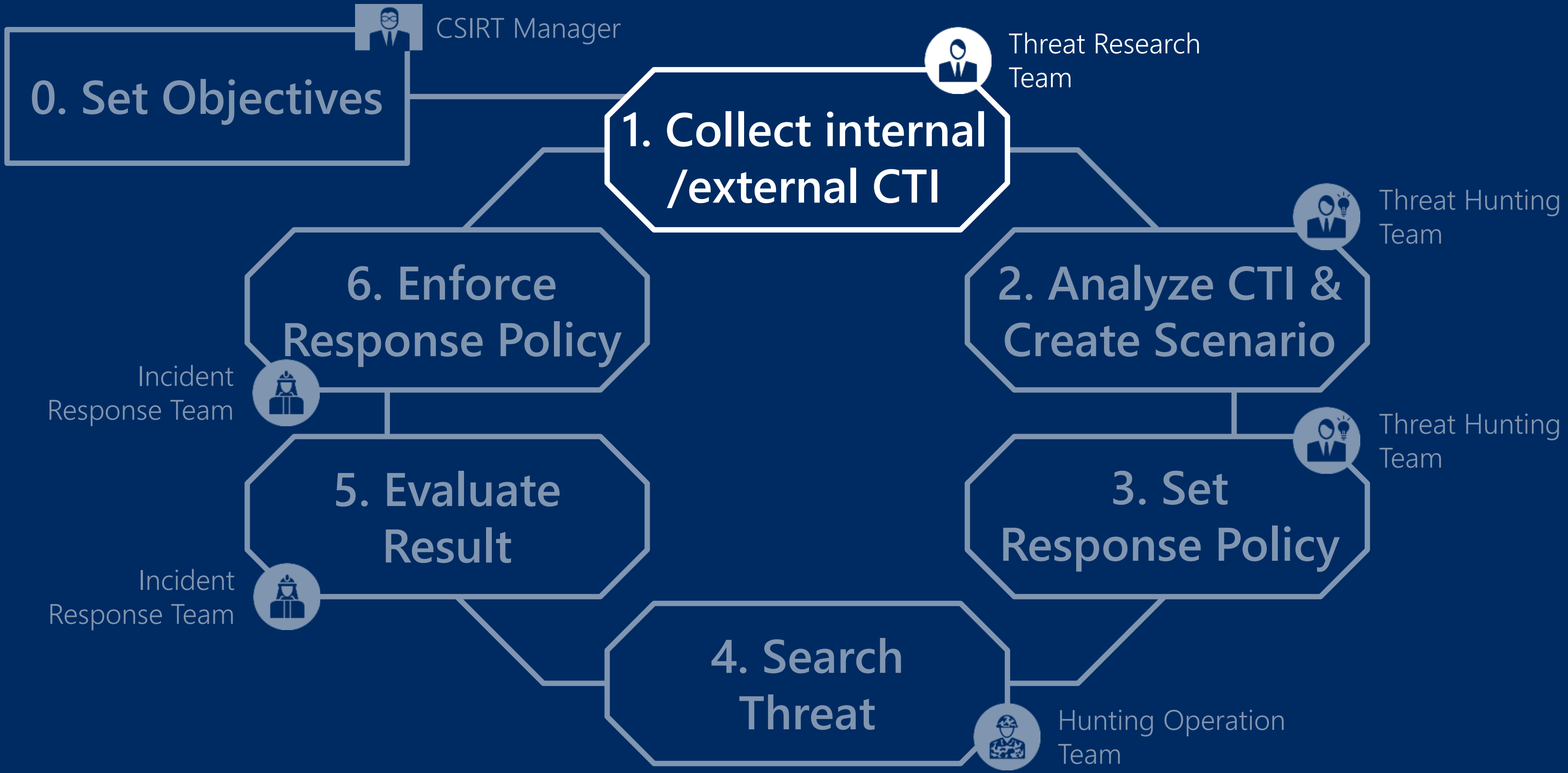
5. Evaluate Result

Incident Response Team

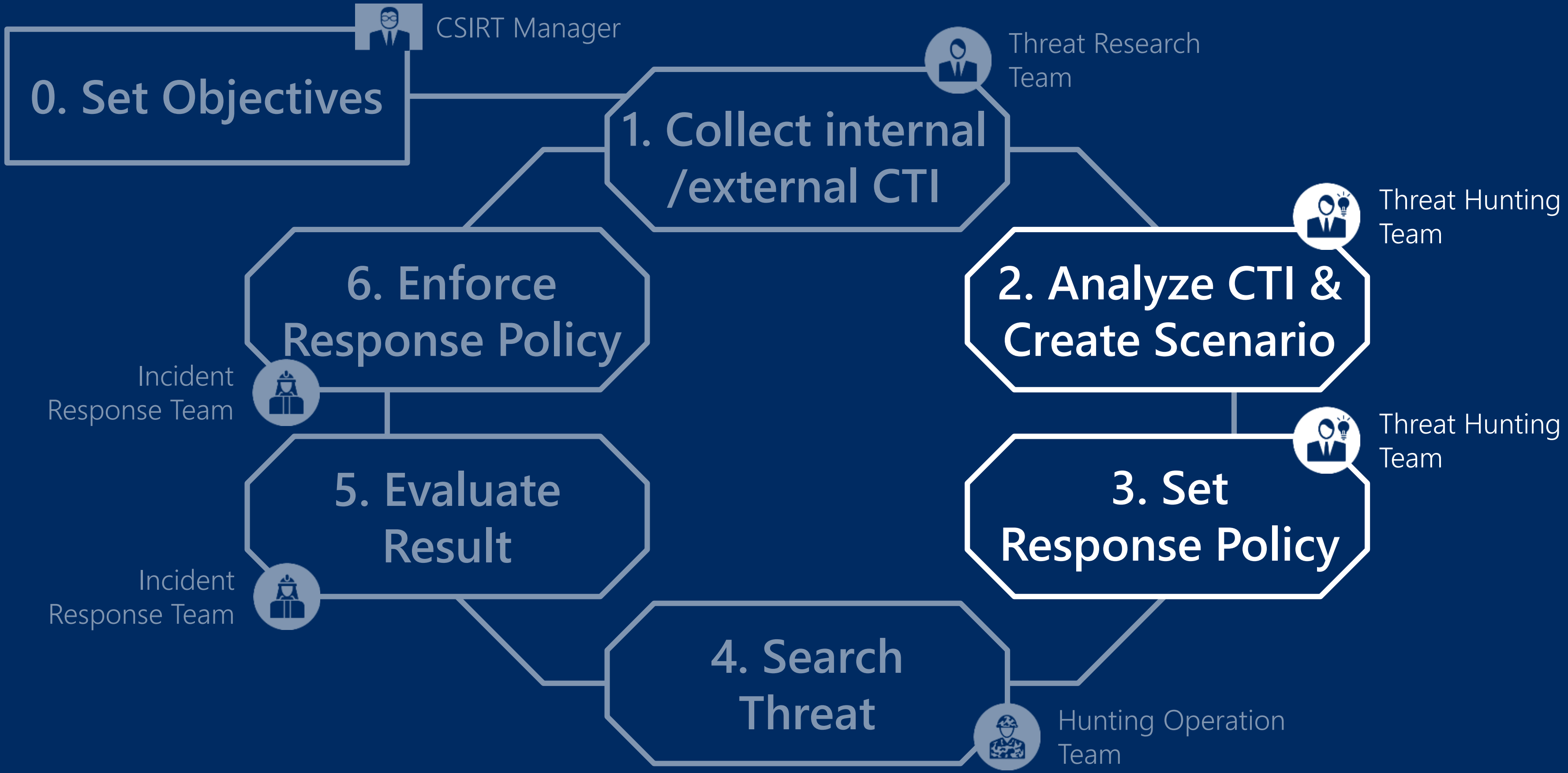
6. Enforce Response Policy

Incident Response Team

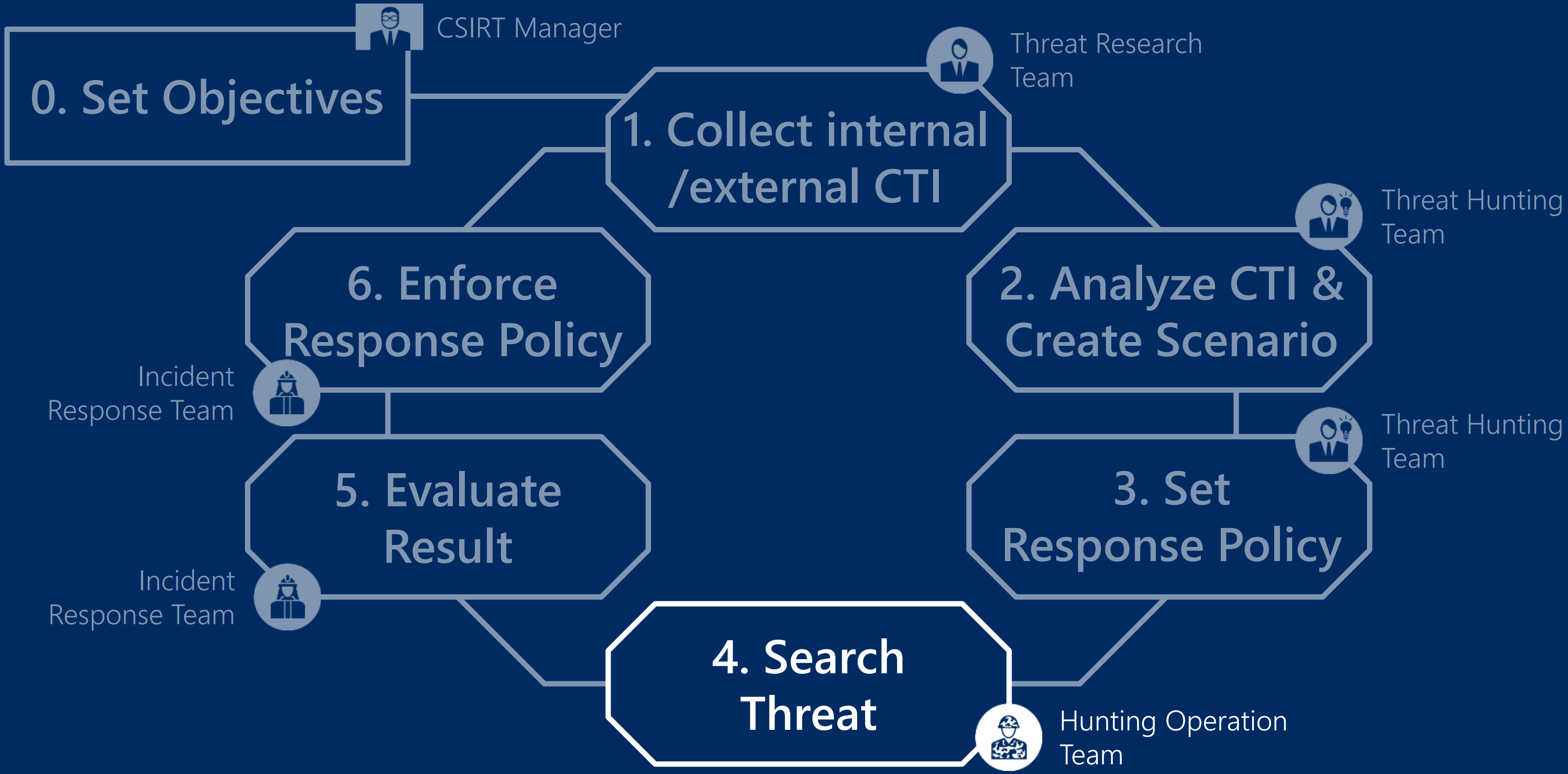
Threat Hunting Operations



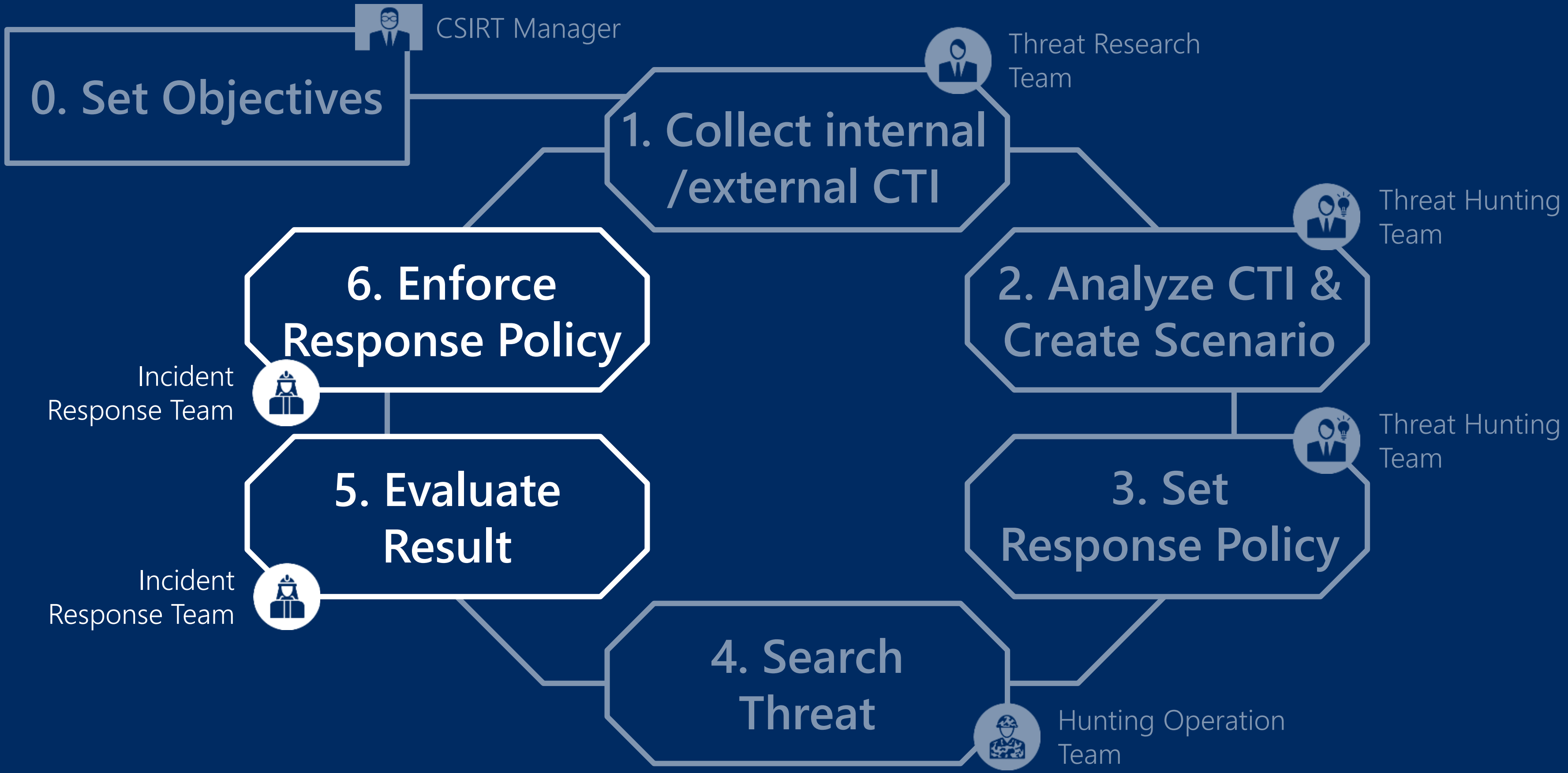
Threat Hunting Operations



Threat Hunting Operations



Threat Hunting Operations



0. Set Objectives

CSIRT Manager

1. Collect internal /external CTI

Threat Research Team

2. Analyze CTI & Create Scenario

Threat Hunting Team

3. Set Response Policy

Threat Hunting Team

4. Search Threat

Hunting Operation Team

5. Evaluate Result

Incident Response Team

6. Enforce Response Policy

Incident Response Team

Threat Hunting Case Study

Case Study #1 – Malicious email notification from employee

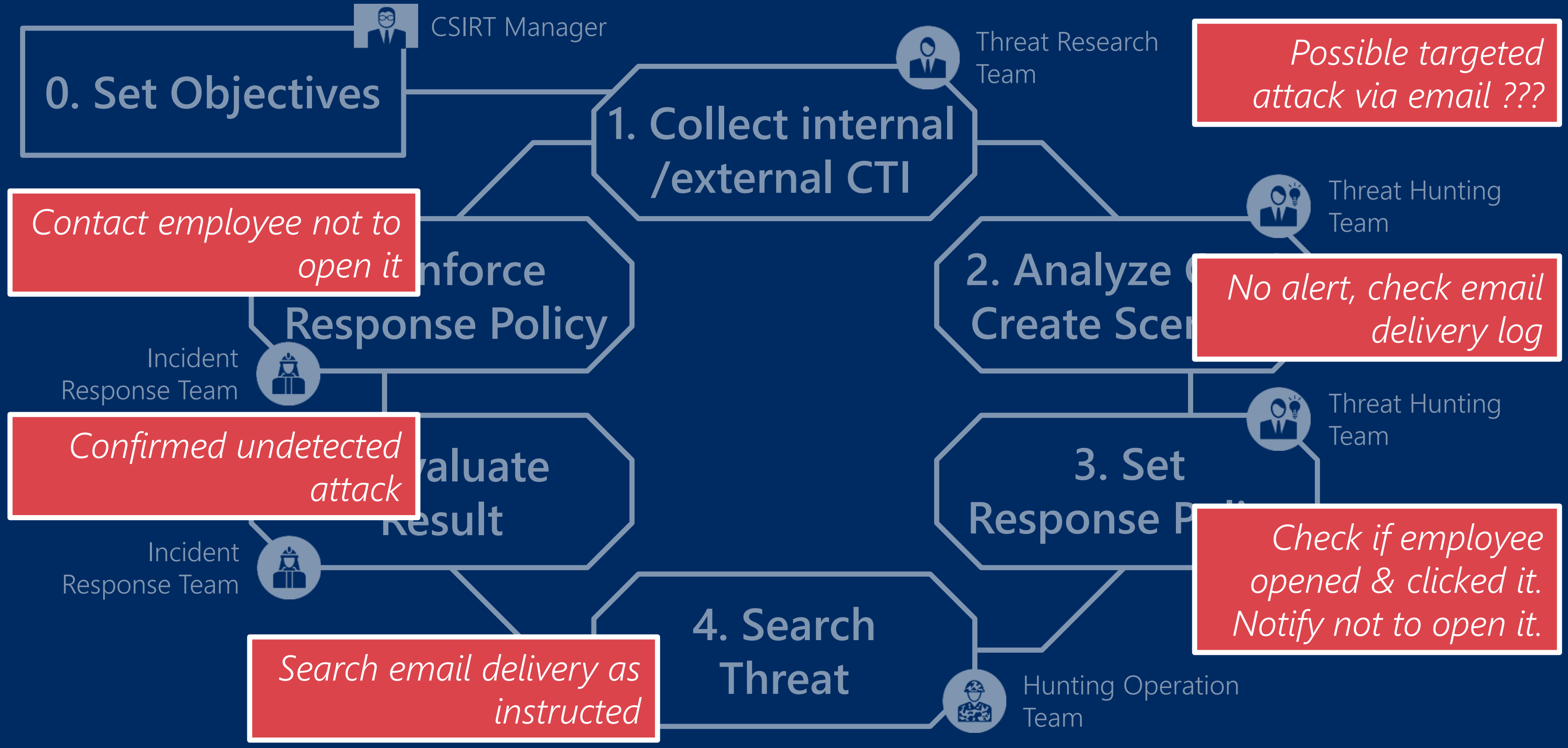
Sandbox email scanner didn’t detect spear phishing email.

Employee felt malicious email, and then notified security operation team of its.

Threat research and malware analysis team jointly analyzed it, and recognized possible targeted attack.

Let’s start hunting!

Case Study #1 – Process Overview



Possible targeted attack via email ???

No alert, check email delivery log

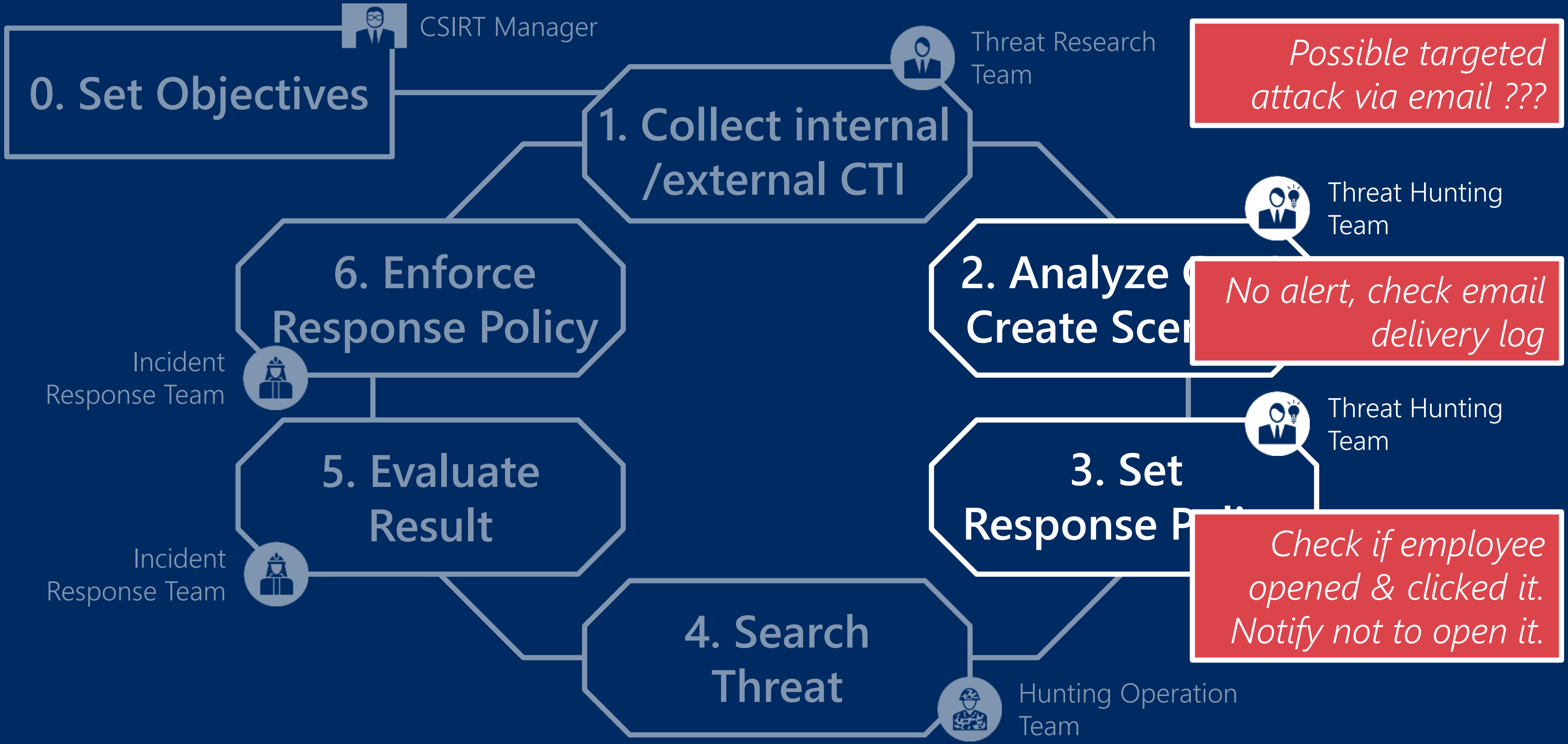
Check if employee opened & clicked it. Notify not to open it.

Search email delivery as instructed

Confirmed undetected attack

Contact employee not to open it

Case Study #1 – Process Overview (1)

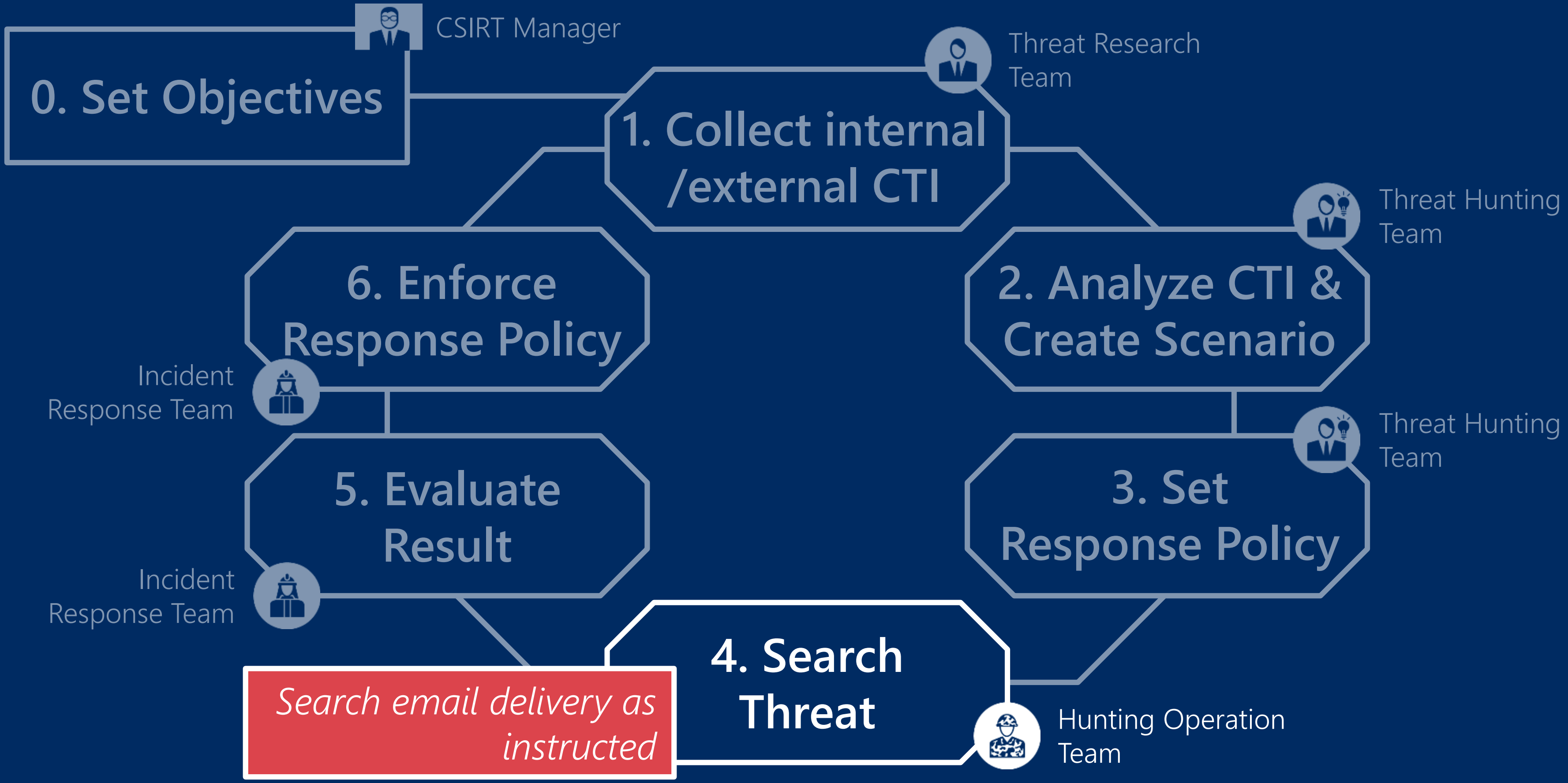


Possible targeted attack via email ???

No alert, check email delivery log

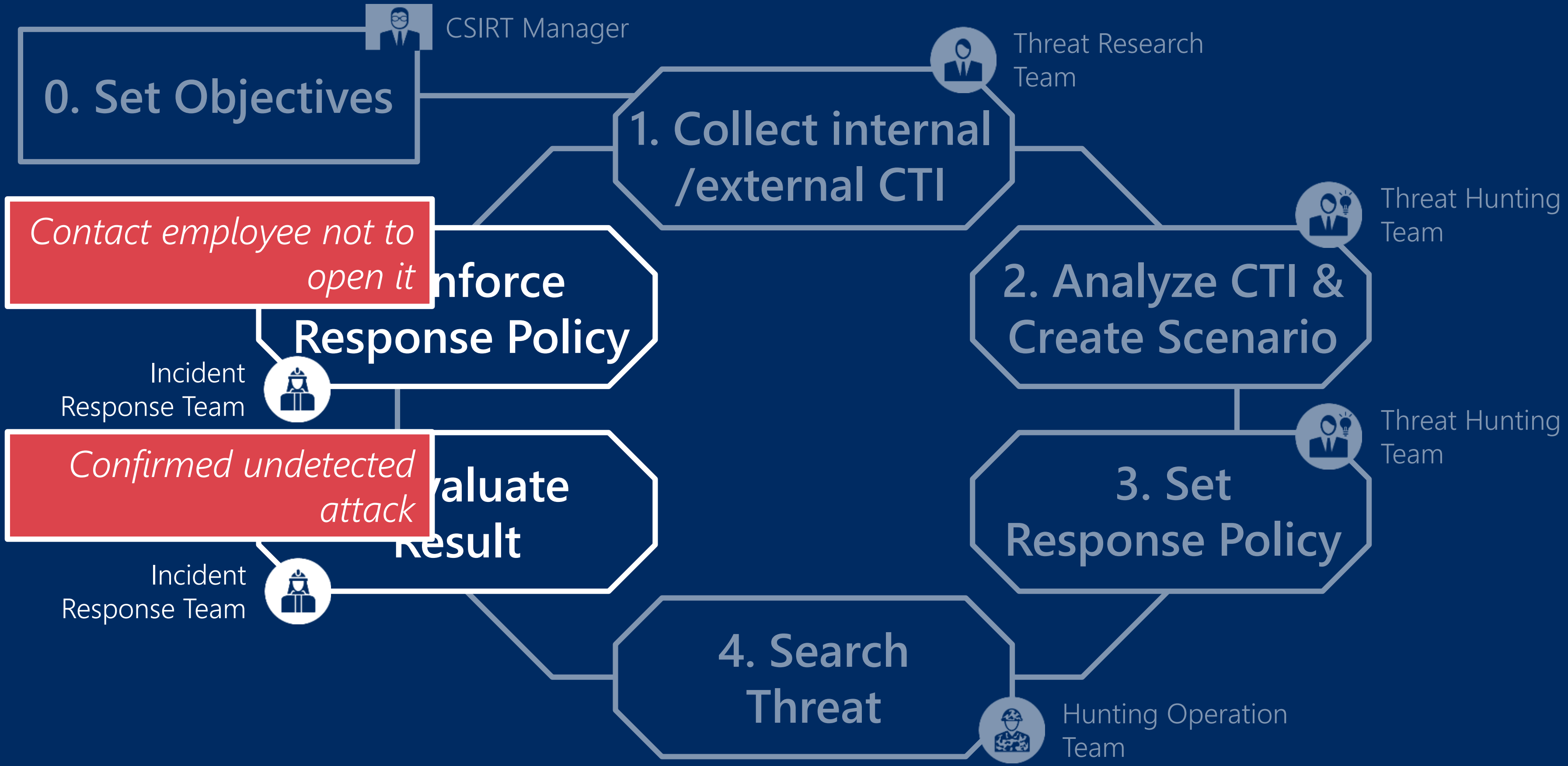
Check if employee opened & clicked it. Notify not to open it.

Case Study #1 – Process Overview (2)



Search email delivery as instructed

Case Study #1 – Process Overview (3)



CSIRT Manager

0. Set Objectives

Threat Research Team

1. Collect internal /external CTI

Threat Hunting Team

2. Analyze CTI & Create Scenario

Threat Hunting Team

3. Set Response Policy

4. Search Threat

Hunting Operation Team

nforce Response Policy

Incident Response Team

aluate Result

Incident Response Team

Contact employee not to open it

Confirmed undetected attack

Case Study #2 – Threat Report shows malicious indicators

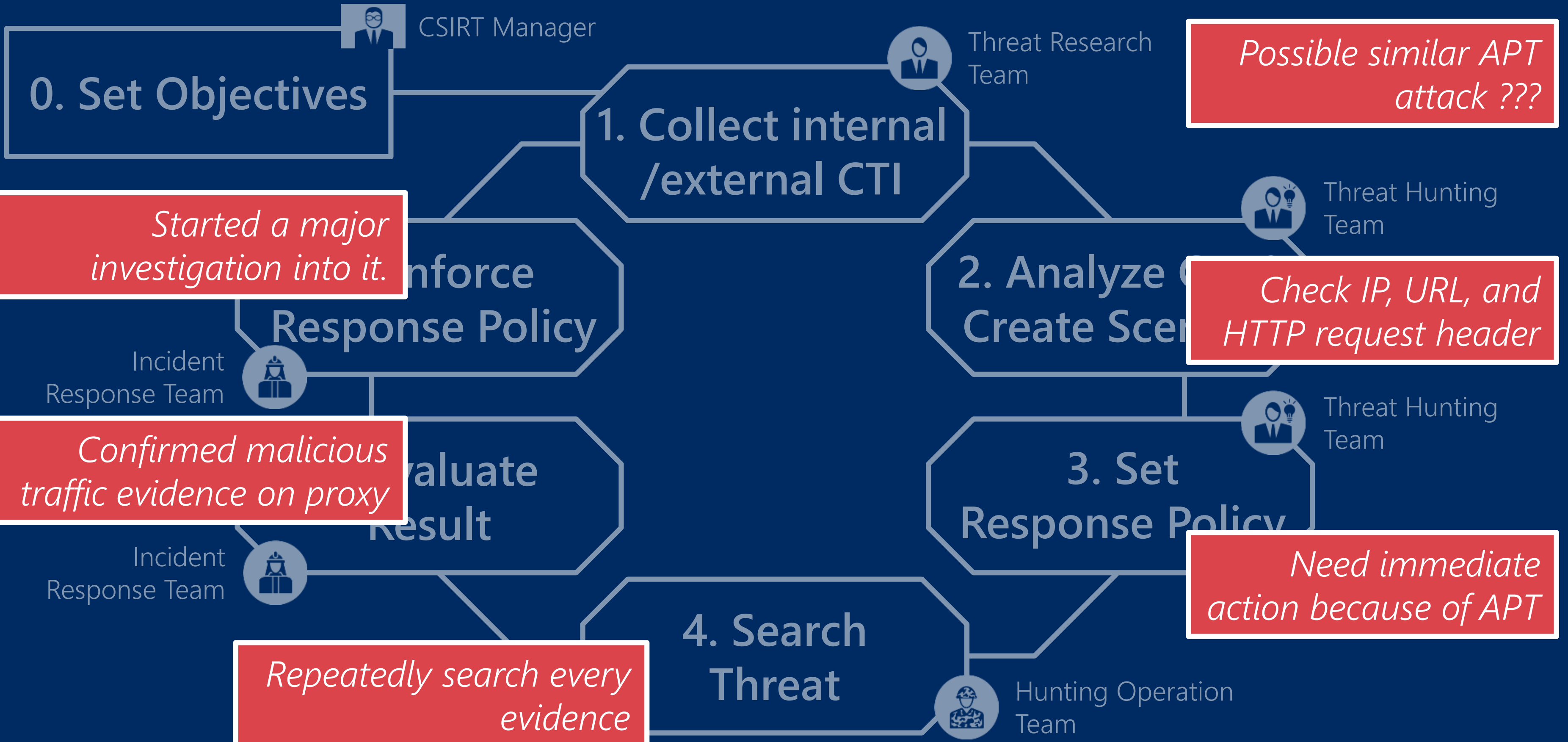
Threat research team recognized APT report shows several malicious indicators such as IP, URL, HTTP request, file path of malware, etc.

Threat hunting team wondered if same attack campaign has been happened to our organization because of intended country.

There were log collections to be verified.

Let's start hunting!

Case Study #2 – Process Overview (part 1)



Possible similar APT attack ???

Check IP, URL, and HTTP request header

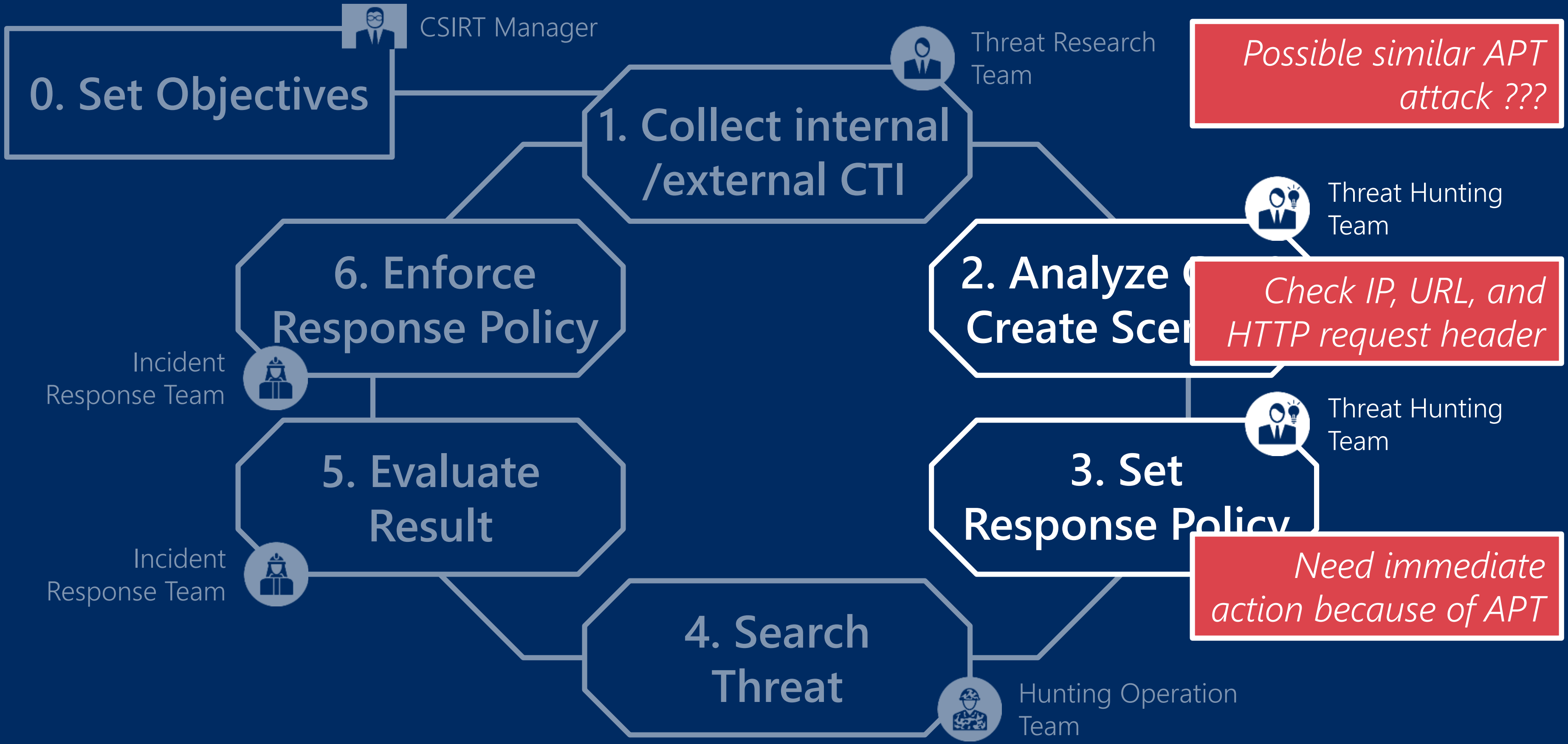
Need immediate action because of APT

Repeatedly search every evidence

Confirmed malicious traffic evidence on proxy

Started a major investigation into it.

Case Study #2 – Process Overview (part 1) (1)

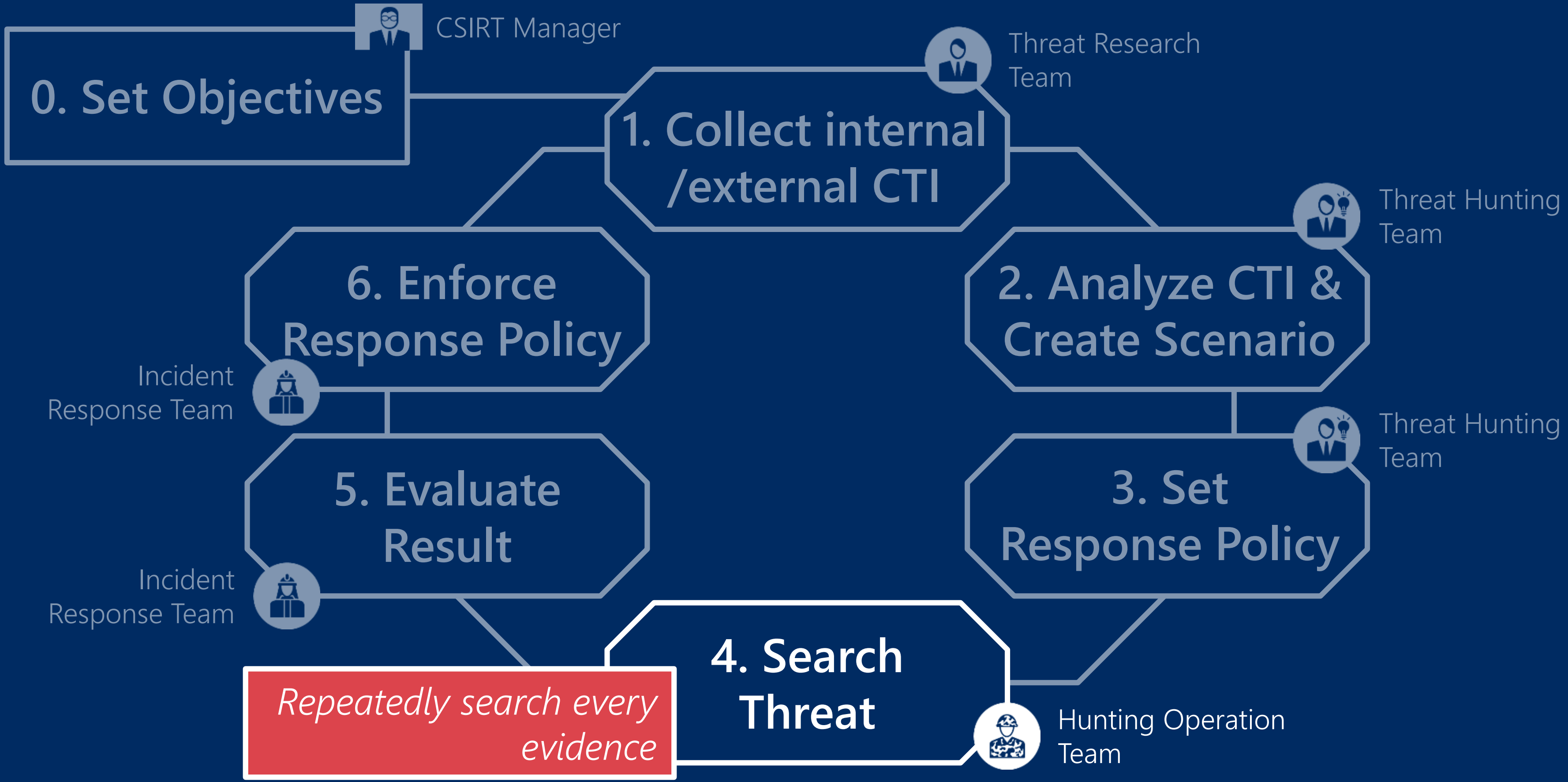


Possible similar APT attack ???

Check IP, URL, and HTTP request header

Need immediate action because of APT

Case Study #2 – Process Overview (part 1) (2)



0. Set Objectives

CSIRT Manager

1. Collect internal /external CTI

Threat Research Team

2. Analyze CTI & Create Scenario

Threat Hunting Team

3. Set Response Policy

Threat Hunting Team

4. Search Threat

Hunting Operation Team

5. Evaluate Result

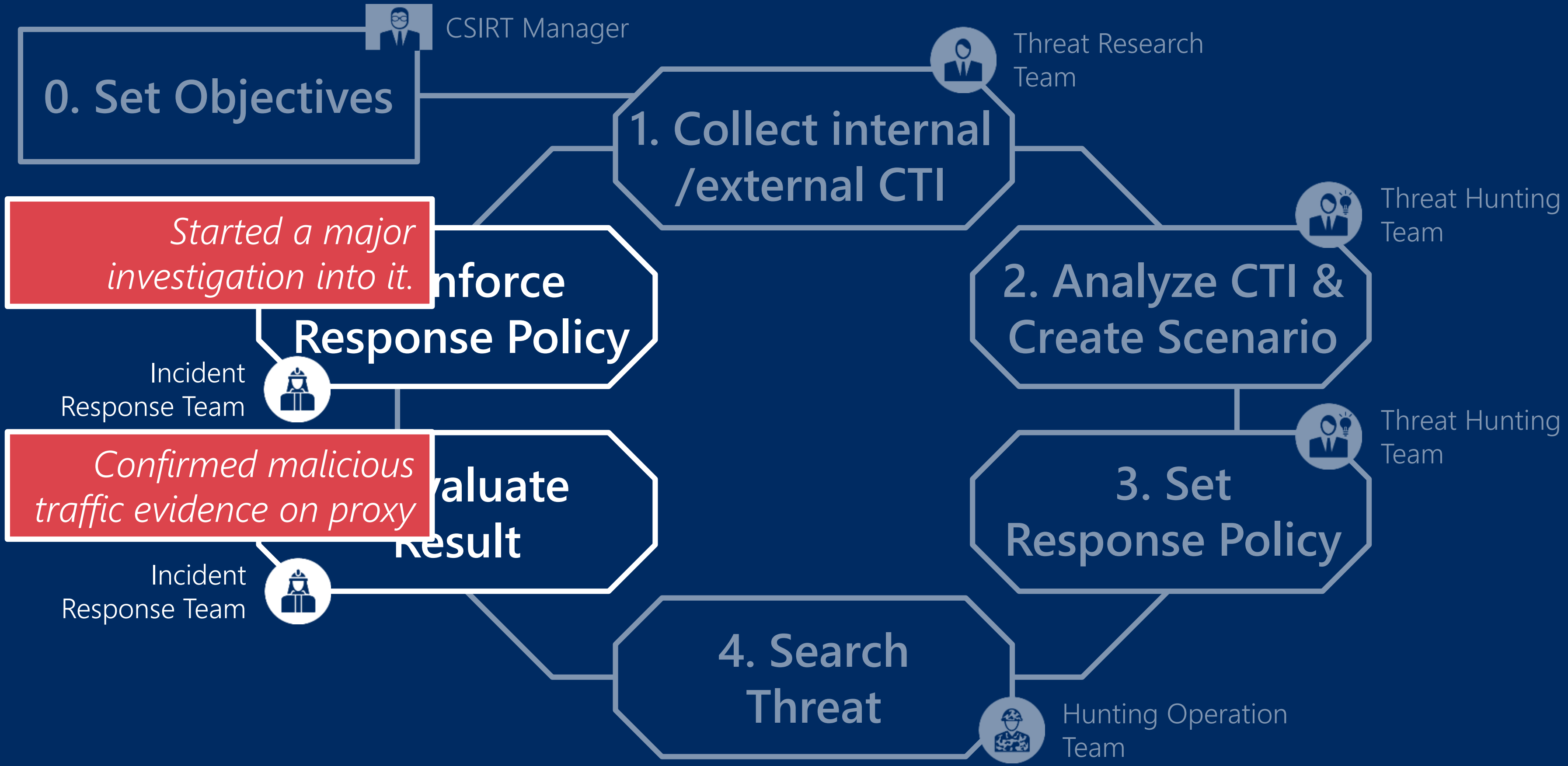
Incident Response Team

6. Enforce Response Policy

Incident Response Team

Repeatedly search every evidence

Case Study #2 – Process Overview (part 1) (3)



CSIRT Manager

0. Set Objectives

Threat Research Team

1. Collect internal /external CTI

Threat Hunting Team

2. Analyze CTI & Create Scenario

Threat Hunting Team

3. Set Response Policy

4. Search Threat

Hunting Operation Team

Confirmed malicious traffic evidence on proxy

valuate Result

Incident Response Team

Started a major investigation into it.

nforce Response Policy

Incident Response Team

Case Study #2 – Malware samples with characteristics

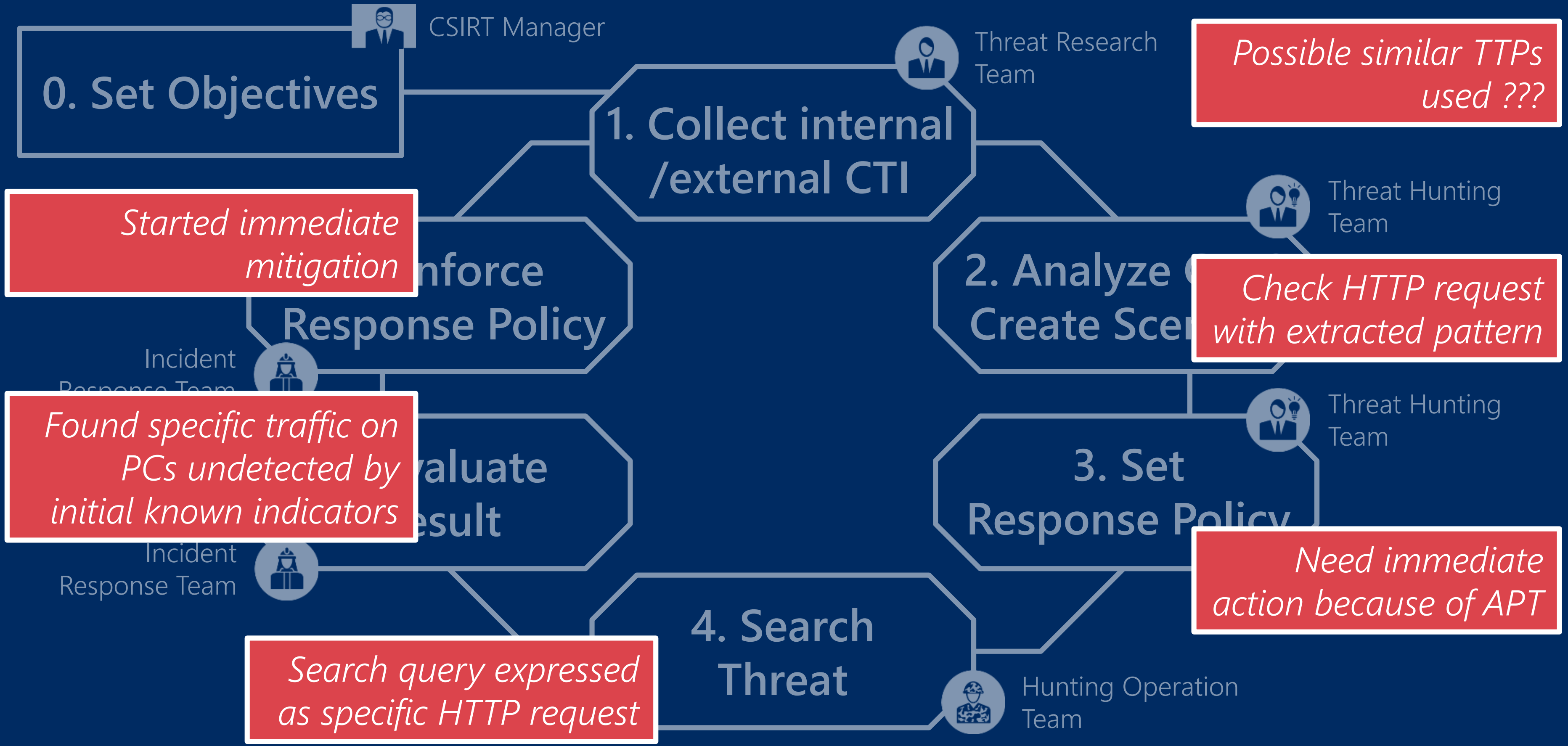
After investigation, IR team identified tens of PCs had been infected by this campaign.

Threat research team and malware analysis team looked at past attacks and TTPs attacker used.

Threat hunting team successfully generated extraction rule to this type of attack from samples.

Let's start hunting, again!

Case Study #2 – Process Overview (part 2)



Possible similar TTPs used ???

Check HTTP request with extracted pattern

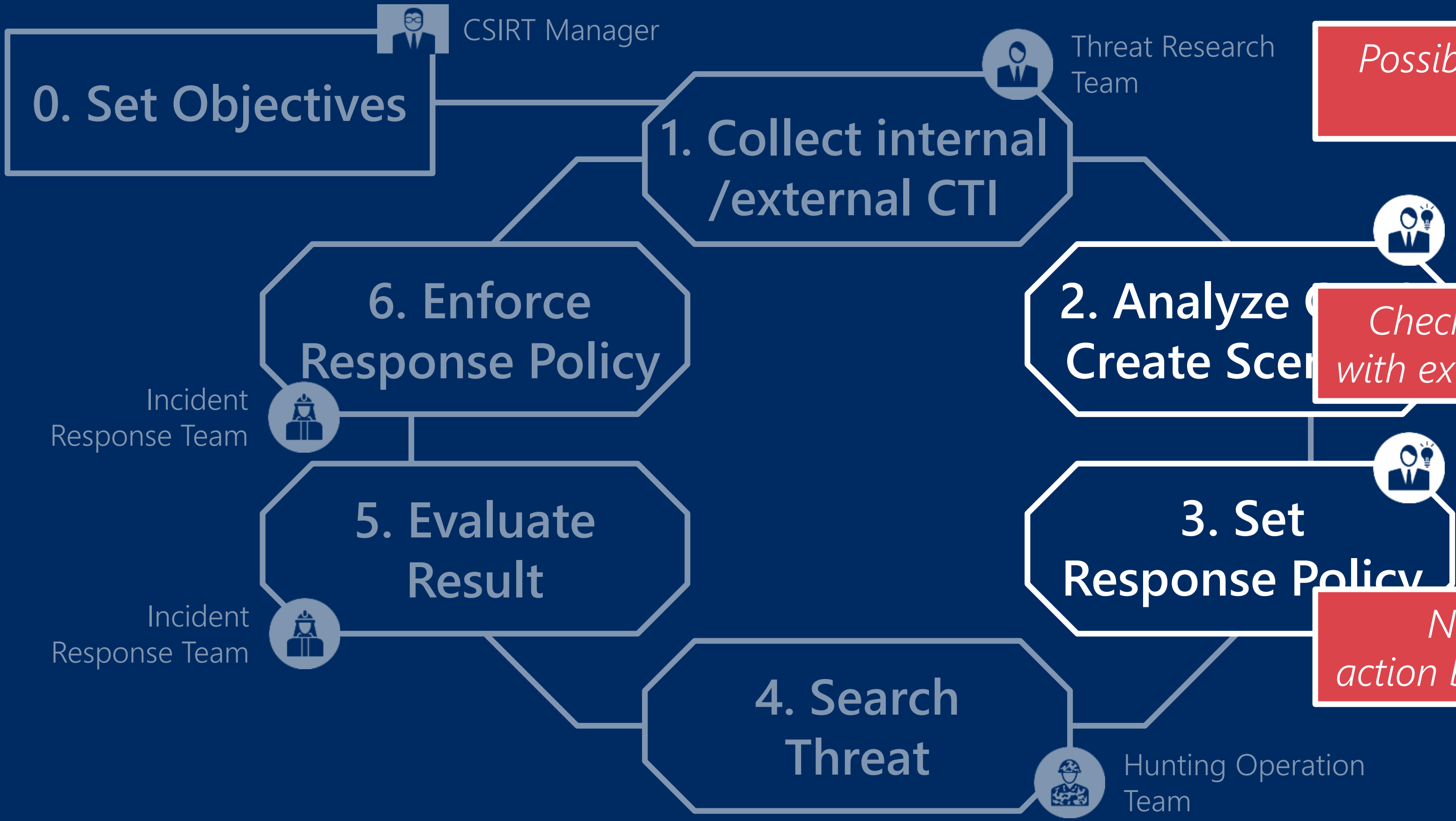
Need immediate action because of APT

Search query expressed as specific HTTP request

Found specific traffic on PCs undetected by initial known indicators

Started immediate mitigation

Case Study #2 – Process Overview (part 2) (1)

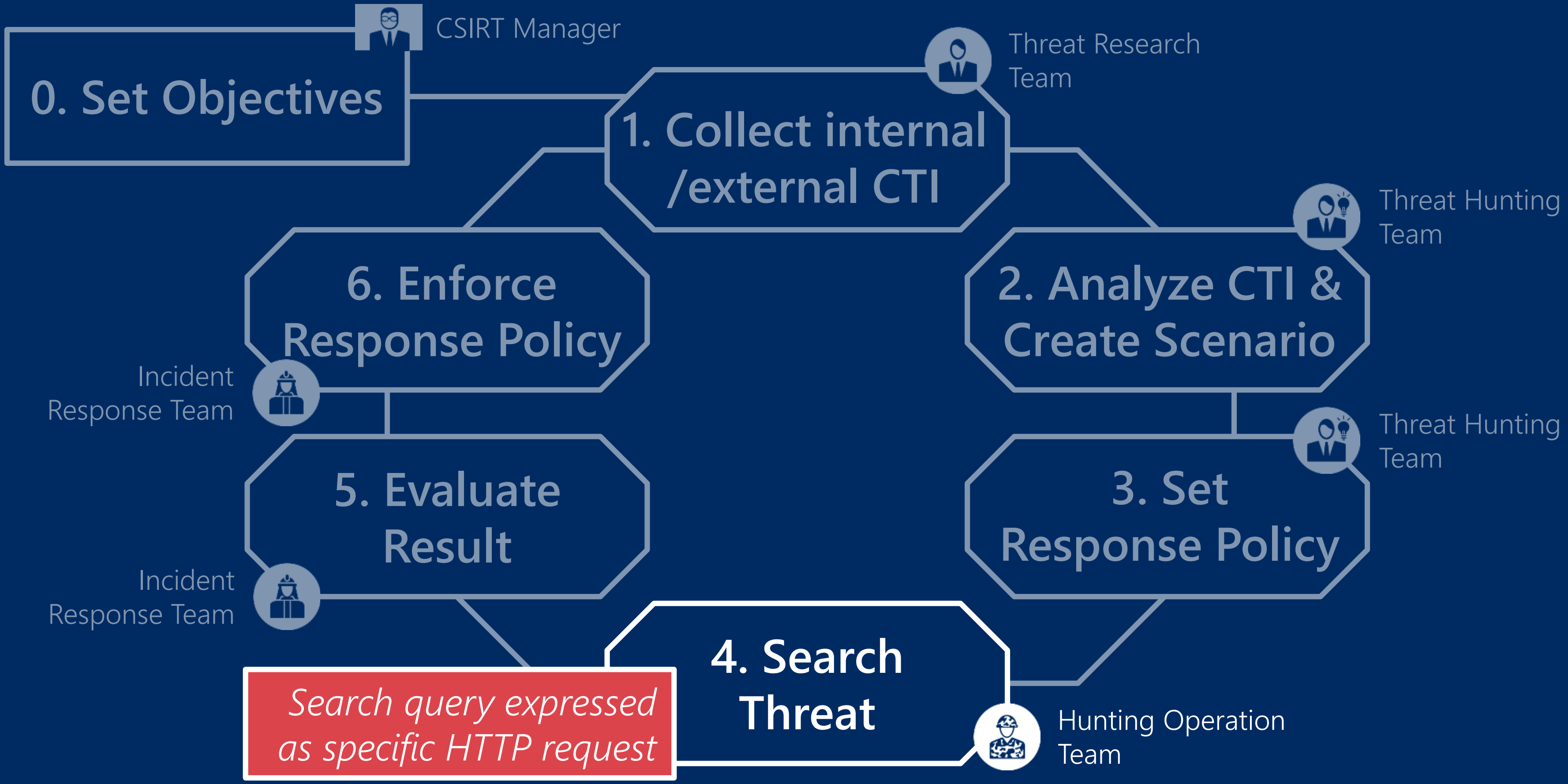


Possible similar TTPs used ???

Check HTTP request with extracted pattern

Need immediate action because of APT

Case Study #2 – Process Overview (part 2) (2)



0. Set Objectives

CSIRT Manager

1. Collect internal /external CTI

Threat Research Team

2. Analyze CTI & Create Scenario

Threat Hunting Team

3. Set Response Policy

Threat Hunting Team

4. Search Threat

Hunting Operation Team

5. Evaluate Result

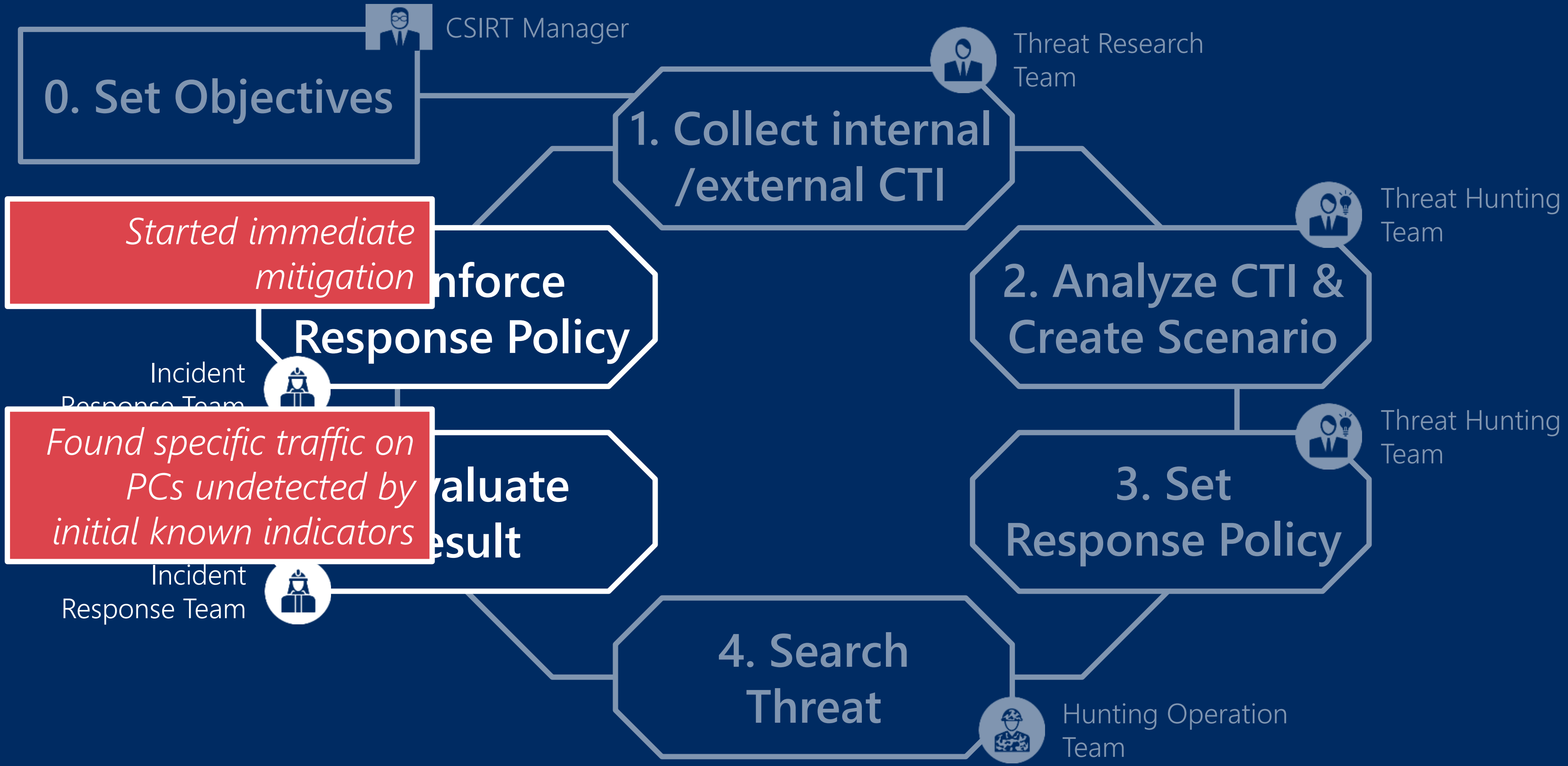
Incident Response Team

6. Enforce Response Policy

Incident Response Team

Search query expressed as specific HTTP request

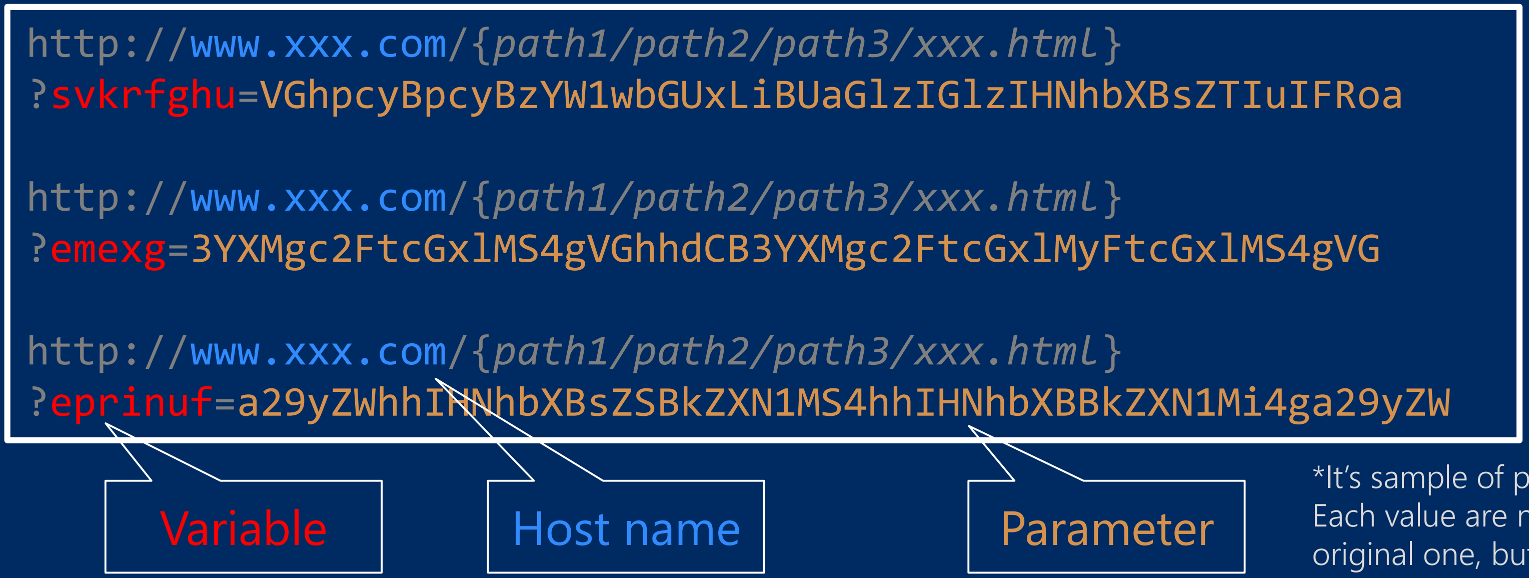
Case Study #2 – Process Overview (part 2) (3)



Started immediate mitigation

Found specific traffic on PCs undetected by initial known indicators

Case Study #2 – Found additional infected PCs by pattern



```
http://www.xxx.com/{path1/path2/path3/xxx.html}
?svkrfghu=VGhpcyBpcyBzYW1wbGUxLiBUaGlzIGlzIHNhbXBsZTIuIFRoa

http://www.xxx.com/{path1/path2/path3/xxx.html}
?emexg=3YXMgc2FtcGxlMS4gVGhhdCB3YXMgc2FtcGxlMyFtcGxlMS4gVG

http://www.xxx.com/{path1/path2/path3/xxx.html}
?eprinuf=a29yZWhhIHNhbXBsZSBkZXN1MS4hhIHNhbXBBkZXN1Mi4ga29yZW
```

*It's sample of patterning. Each value are not original one, but replaced.

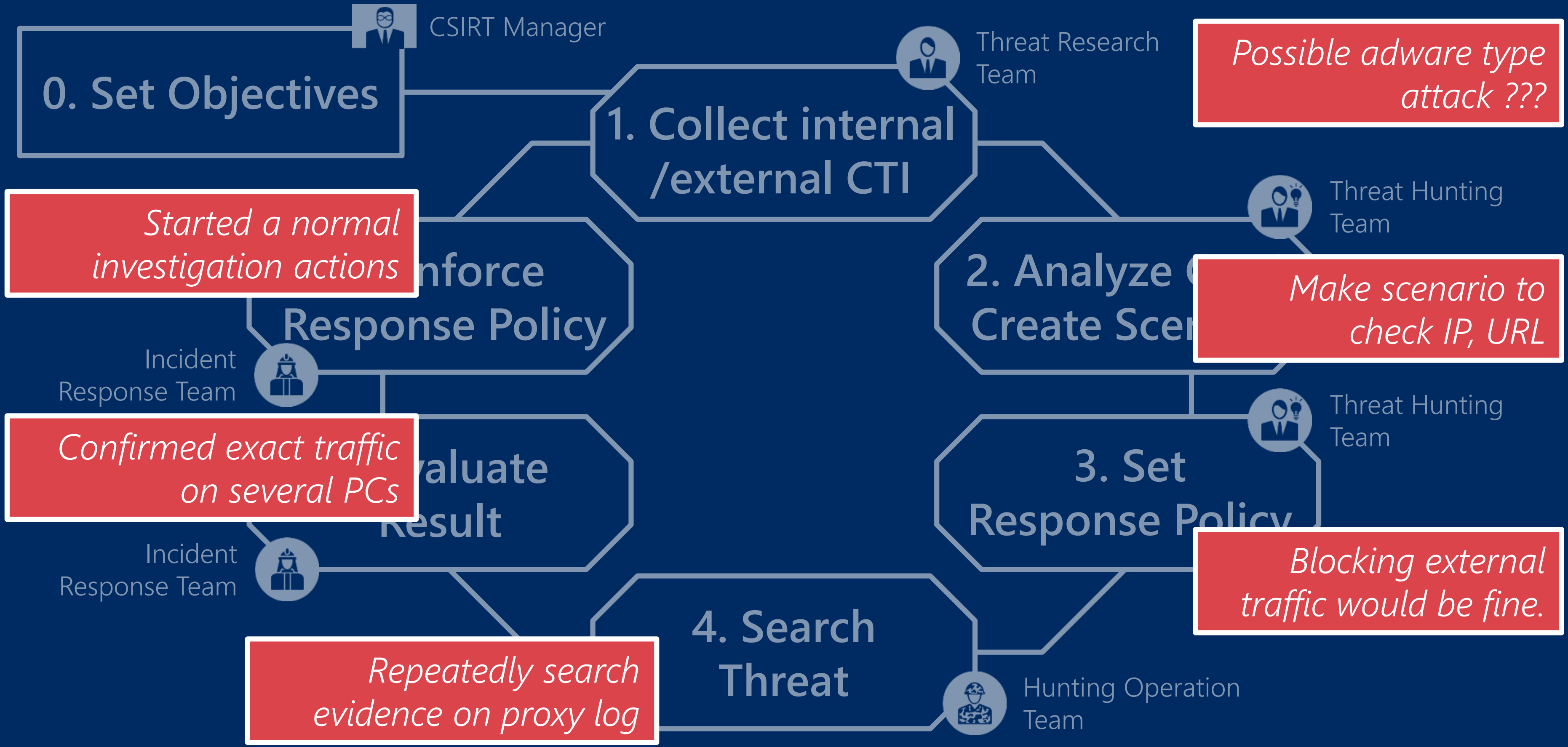
- Host name are same, and length > 100.
- Variable are almost different each other.
- Length of parameter > x0 byte

Case Study #3 – Adware, it's not Adware!?

Threat research team recognized that an unauthorized modification has been found on cleaner software, and notified it to hunting team. Threat hunting team started looking at it within several hours after first recognition.

Let's start hunting!

Case Study #3 – Process Overview (part 1)



Possible adware type attack ???

Make scenario to check IP, URL

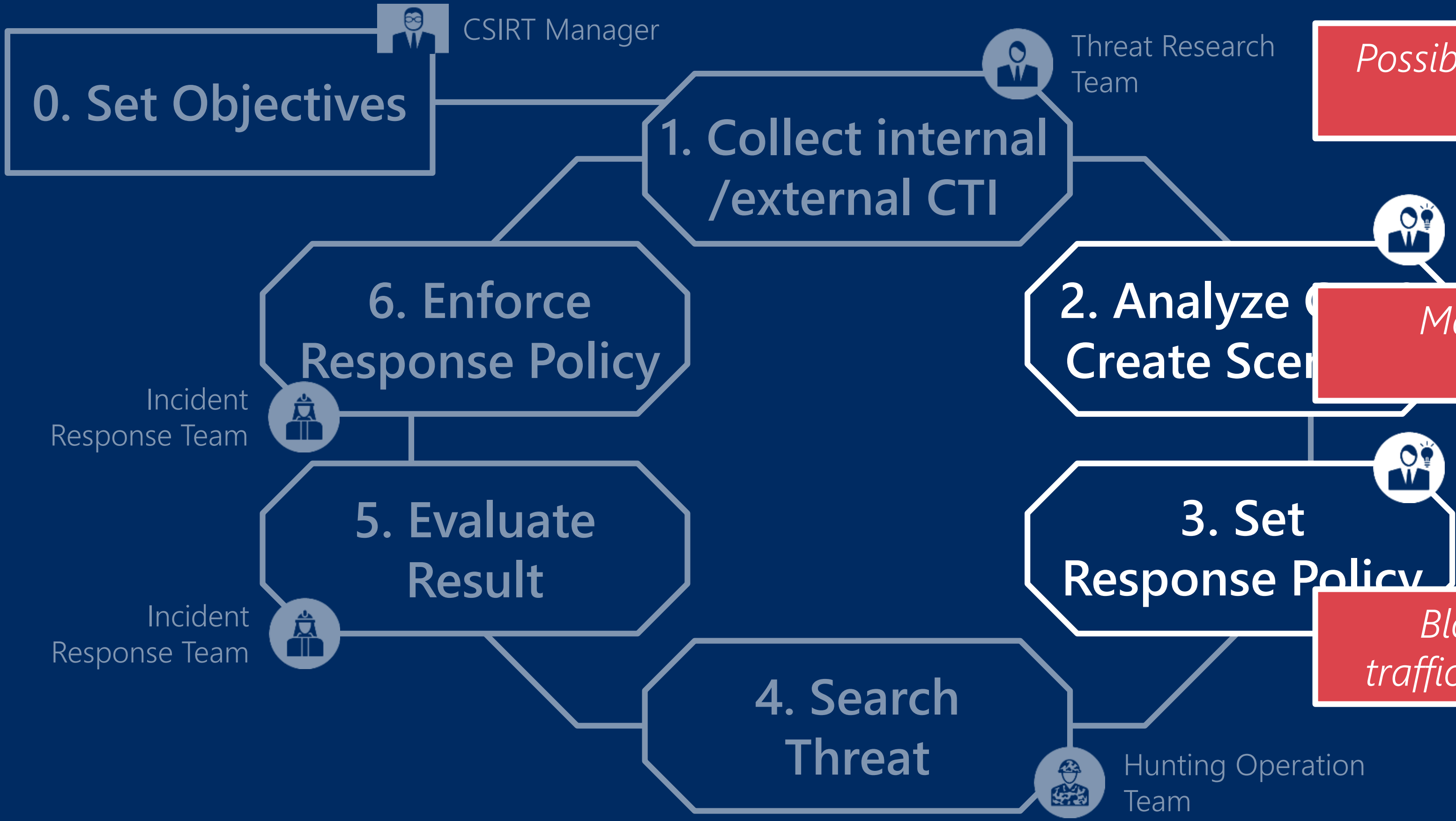
Blocking external traffic would be fine.

Repeatedly search evidence on proxy log

Confirmed exact traffic on several PCs

Started a normal investigation actions

Case Study #3 – Process Overview (part 1) (1)

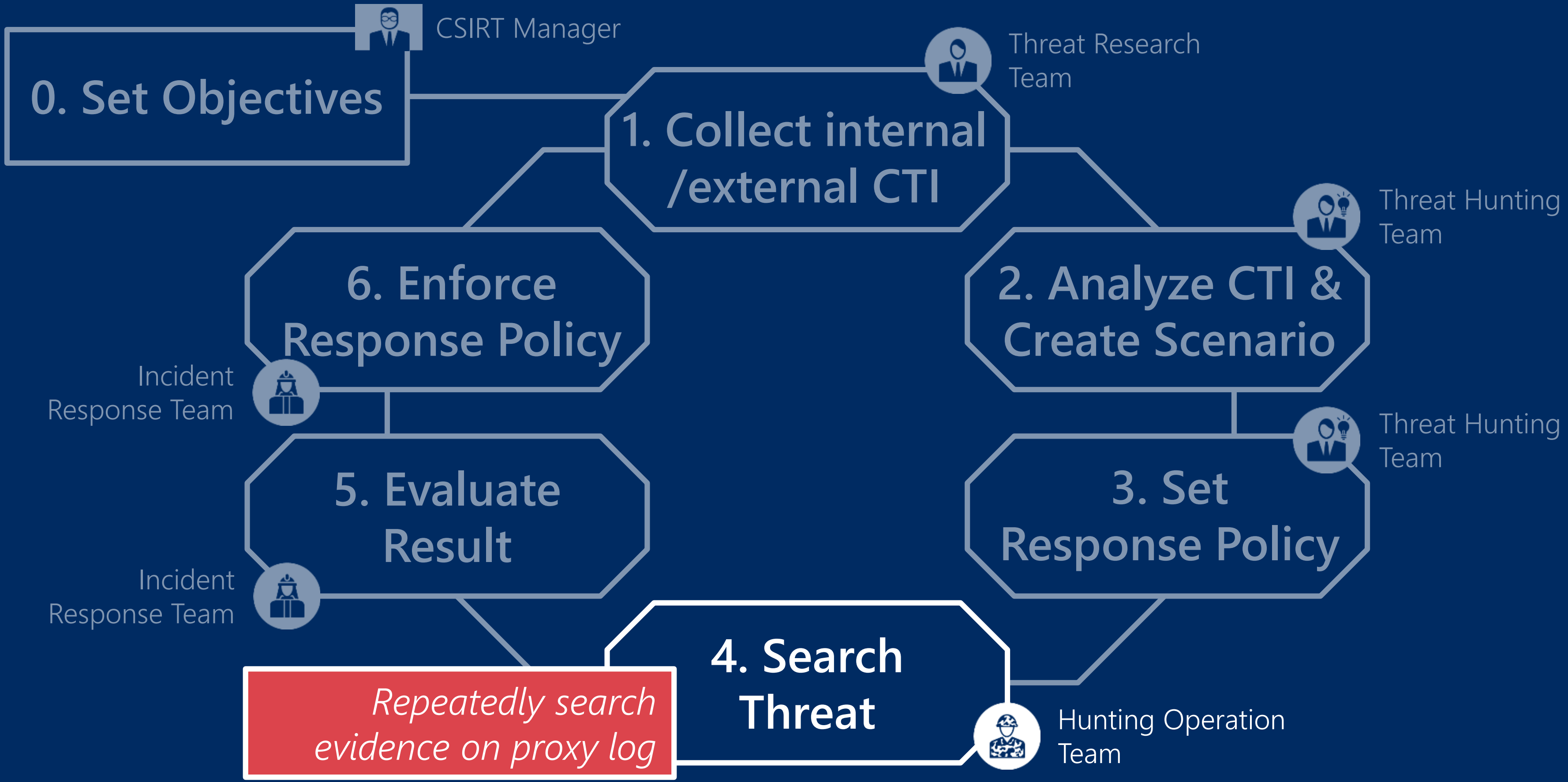


Possible adware type attack ???

Make scenario to check IP, URL

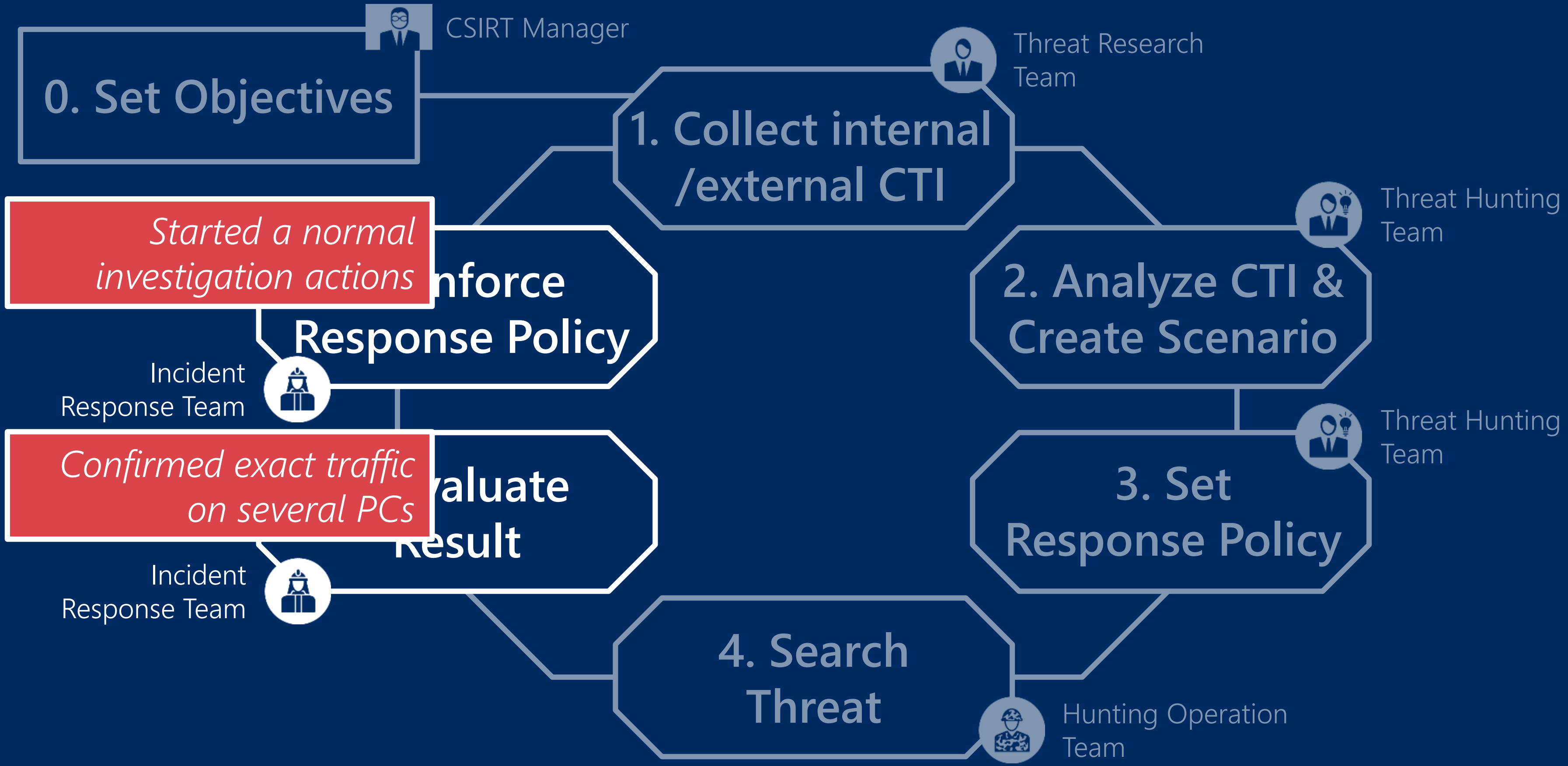
Blocking external traffic would be fine.

Case Study #3 – Process Overview (part 1) (2)



Repeatedly search evidence on proxy log

Case Study #3 – Process Overview (part 1) (3)



CSIRT Manager

0. Set Objectives

Threat Research Team

1. Collect internal /external CTI

Threat Hunting Team

2. Analyze CTI & Create Scenario

Threat Hunting Team

3. Set Response Policy

4. Search Threat

Hunting Operation Team

Started a normal investigation actions

nforce Response Policy

Incident Response Team

Confirmed exact traffic on several PCs

valuate Result

Incident Response Team

Case Study #3 – No Adware!? Software Supply Chain Attack

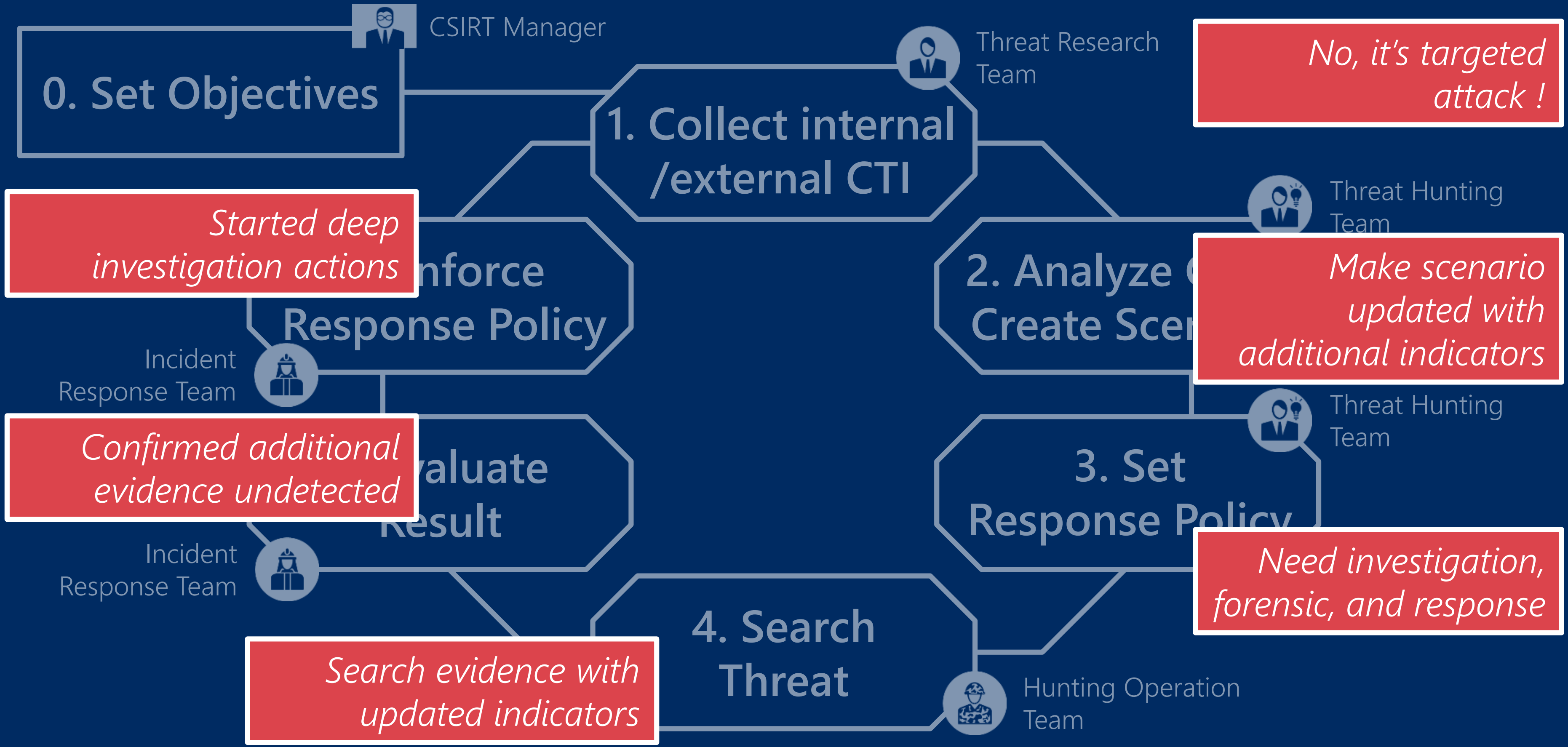
A few days later, software developer notified IR team as it's watering hole attack and we are one of them!?

Threat research team started analyzing threat report from the developer and looking for more information.

Threat hunting team changed response policy from adware policy to targeted attack policy immediately.

Let's start hunting, again, and rapidly!

Case Study #3 – Process Overview (part 2)



No, it's targeted attack !

Make scenario updated with additional indicators

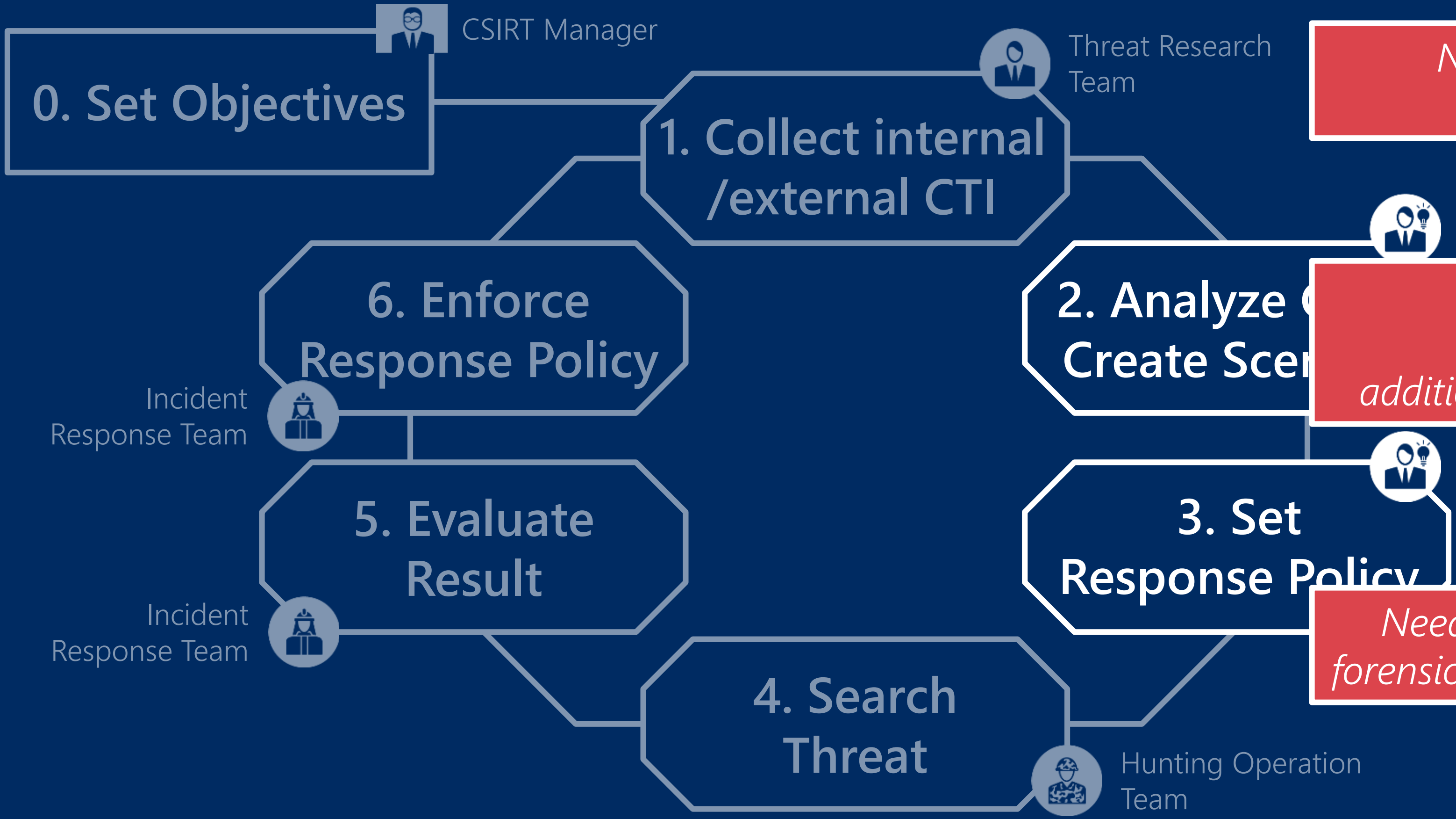
Need investigation, forensic, and response

Search evidence with updated indicators

Confirmed additional evidence undetected

Started deep investigation actions

Case Study #3 – Process Overview (part 2) (1)

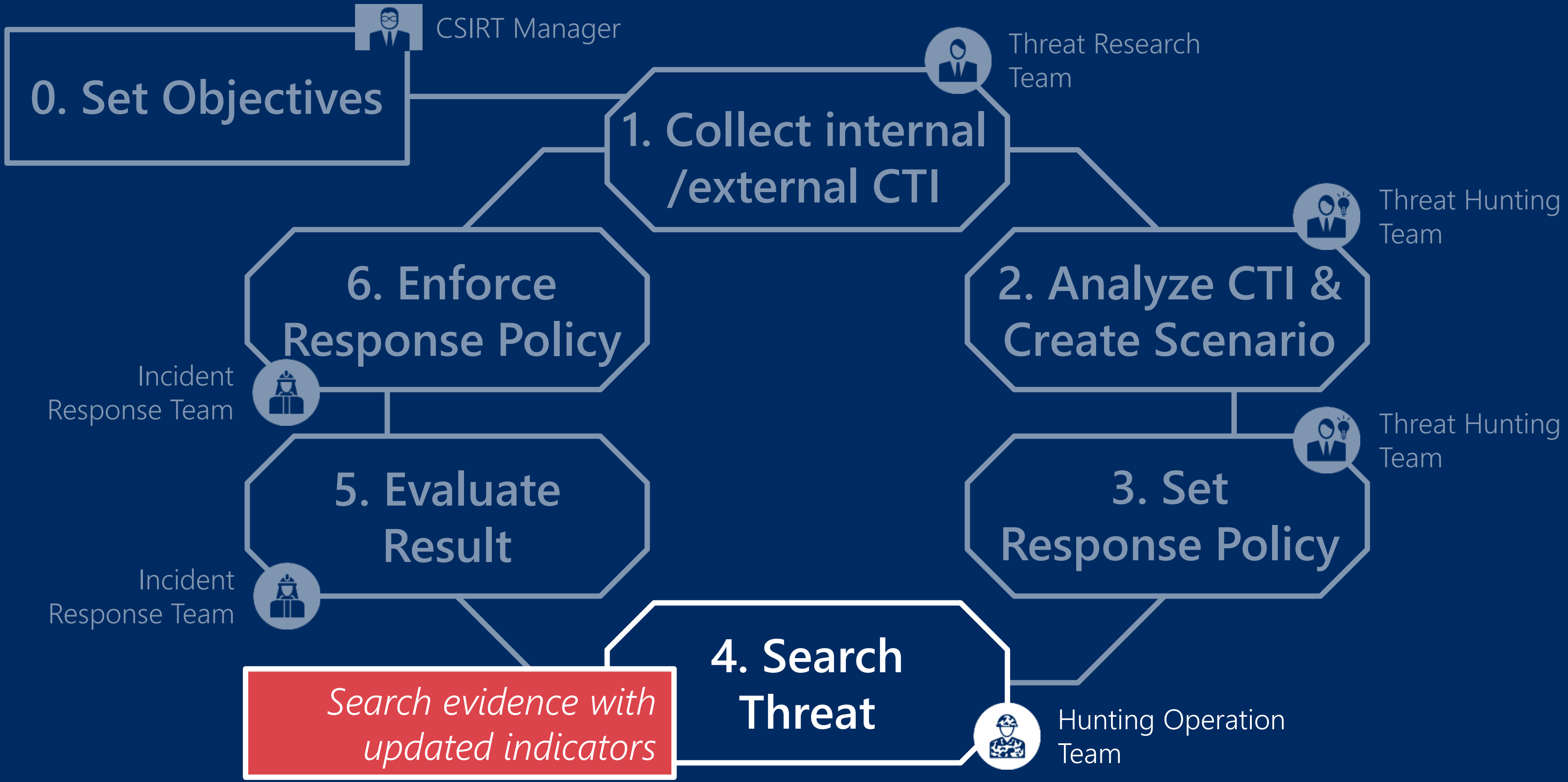


No, it's targeted attack !

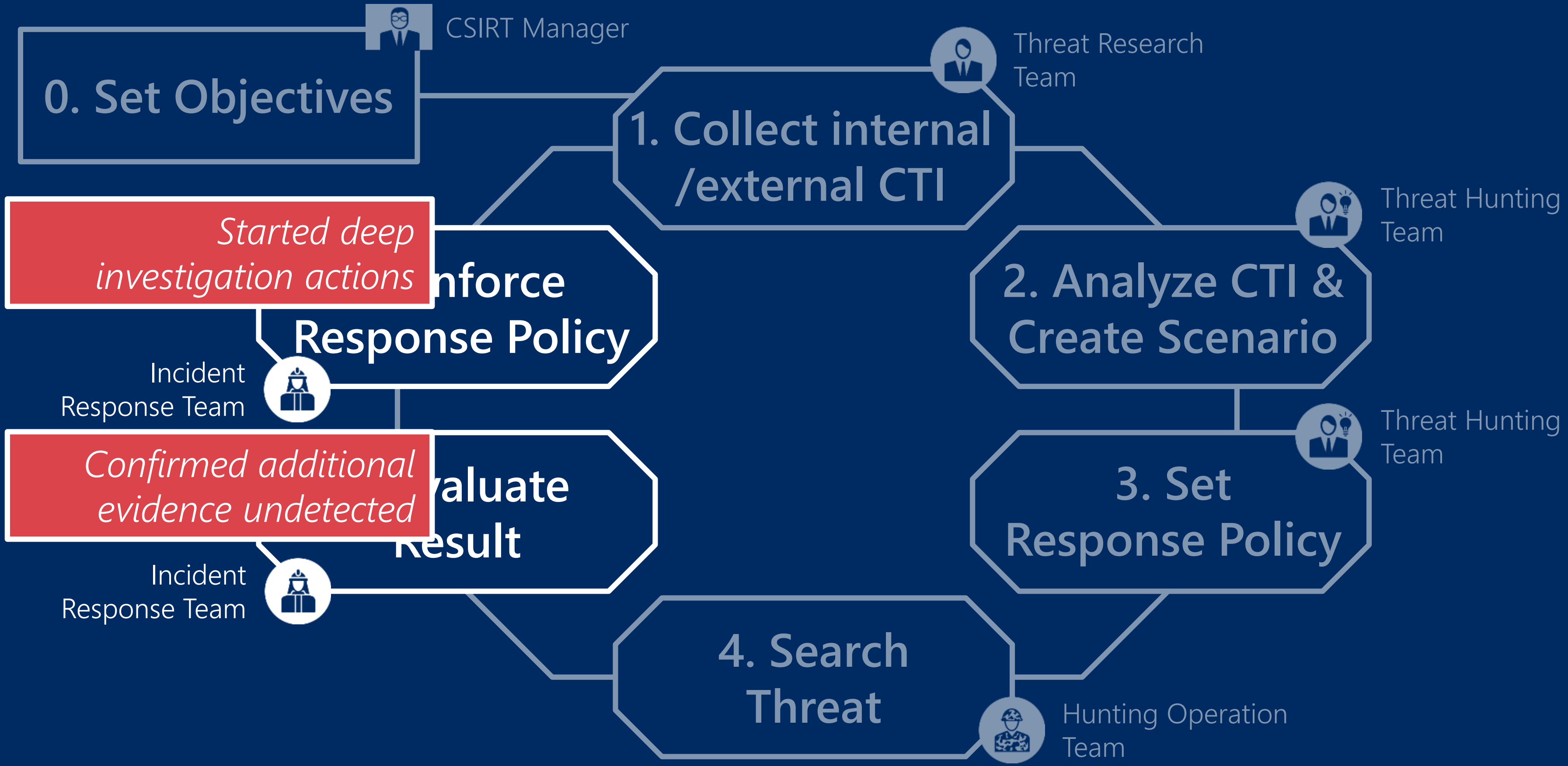
Make scenario updated with additional indicators

Need investigation, forensic, and response

Case Study #3 – Process Overview (part 2) (2)



Case Study #3 – Process Overview (part 2) (3)



CSIRT Manager

0. Set Objectives

Threat Research Team

1. Collect internal /external CTI

Threat Hunting Team

2. Analyze CTI & Create Scenario

Threat Hunting Team

3. Set Response Policy

4. Search Threat

Hunting Operation Team

Started deep investigation actions

nforce Response Policy

Incident Response Team

Confirmed additional evidence undetected

valuate Result

Incident Response Team

Lessons learned from case study

1. It’s not always have to rely on difficult hunting techniques to identity undetected threat, but build the process.

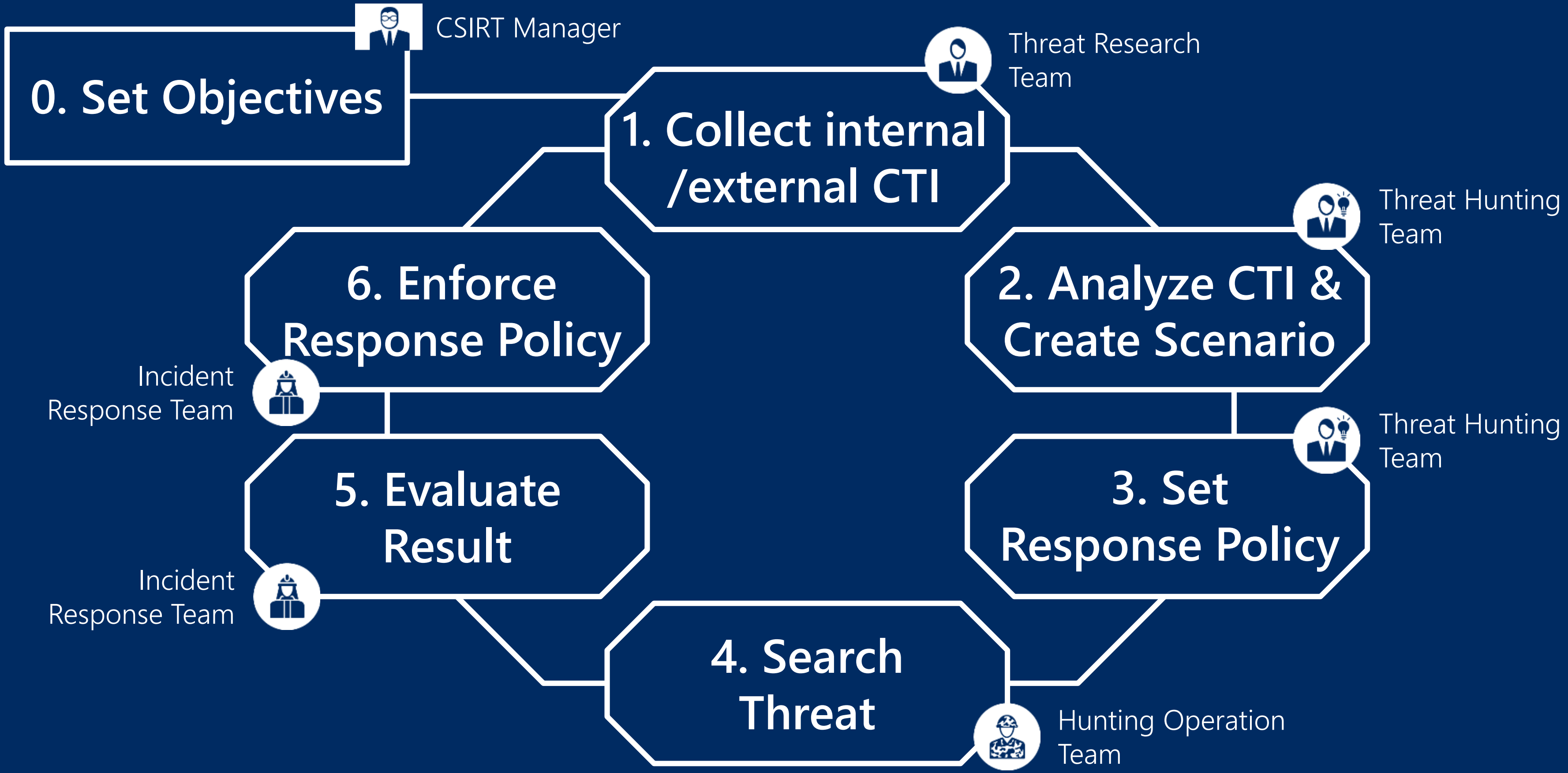
2. It’s much worth if we can find security breach by ourselves before being notified from outside.

3. Let's start from what we can do, and we should do what we can do.

4. Hypothesis generation would be still difficult part for us.

Threat Hunting Operations At Scale

Threat Hunting Operations



0. Set Objectives

CSIRT Manager

1. Collect internal /external CTI

Threat Research Team

2. Analyze CTI & Create Scenario

Threat Hunting Team

3. Set Response Policy

Threat Hunting Team

4. Search Threat

Hunting Operation Team

5. Evaluate Result

Incident Response Team

6. Enforce Response Policy

Incident Response Team

Tools for Support Threat Hunting Operations

Threat Hunting Team

- Asset, Internal System, Directory DB
- Internal CTI (Observed & Analysis) DB
- Hunting Scenario System (STIX)

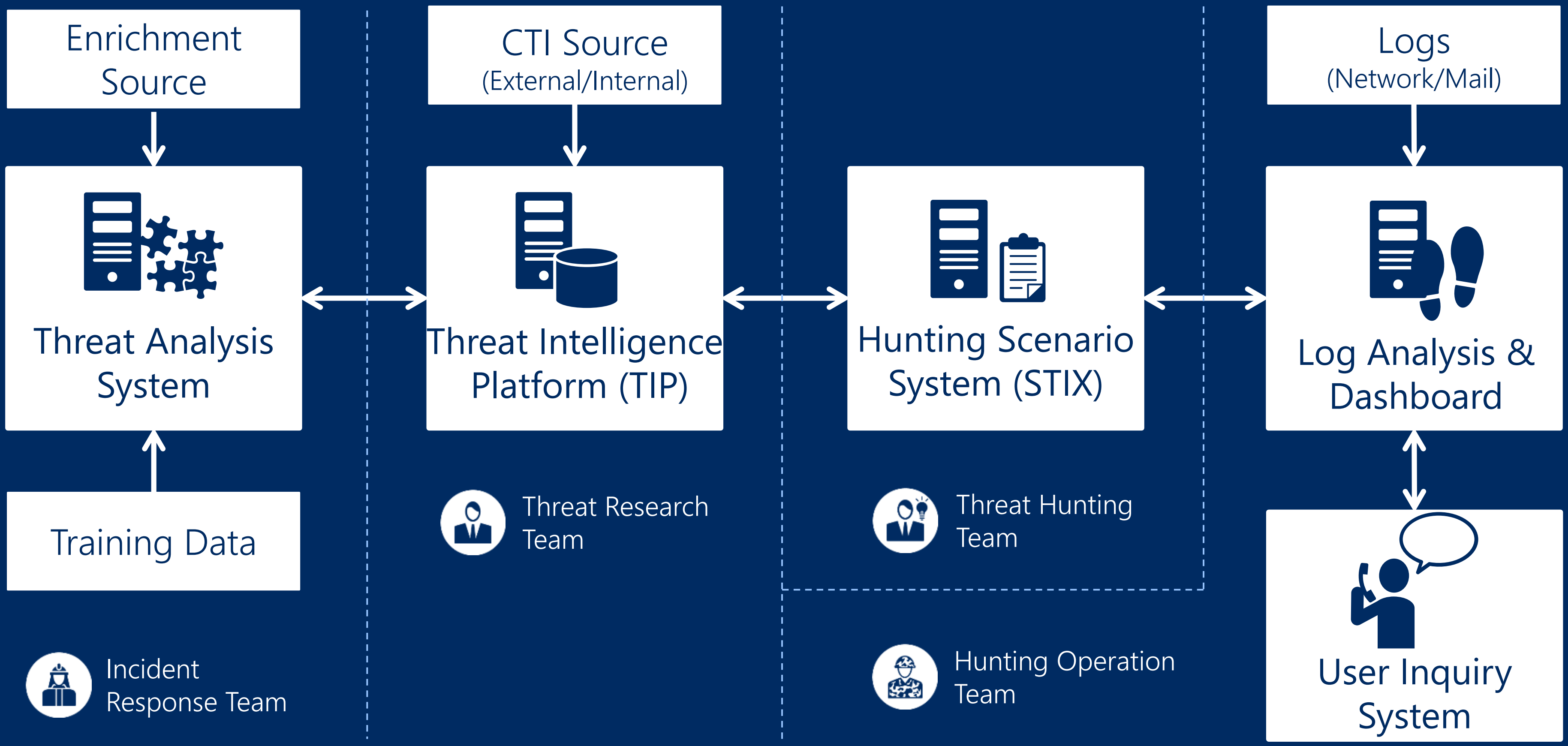
Hunting Operation Team

- Log Analysis & Dashboard
- EDR / NCSP
- User Inquiry System

Incident Response Team

- Forensic Tool
- Log Management
- Threat Intelligence Platform (TIP)
- Threat Analysis System

Threat Hunting System Architecture Overview



Enrichment Source

Threat Analysis System

Training Data

Incident Response Team

CTI Source (External/Internal)

Threat Intelligence Platform (TIP)

Threat Research Team

Hunting Scenario System (STIX)

Threat Hunting Team

Hunting Operation Team

Logs (Network/Mail)

Log Analysis & Dashboard

User Inquiry System

Threat Hunting Operations Framework

Values of Hunting Operations

1

Look for uncovered threat or ongoing threat that evade existing security solutions, and mitigate and remediate it as soon as possible.

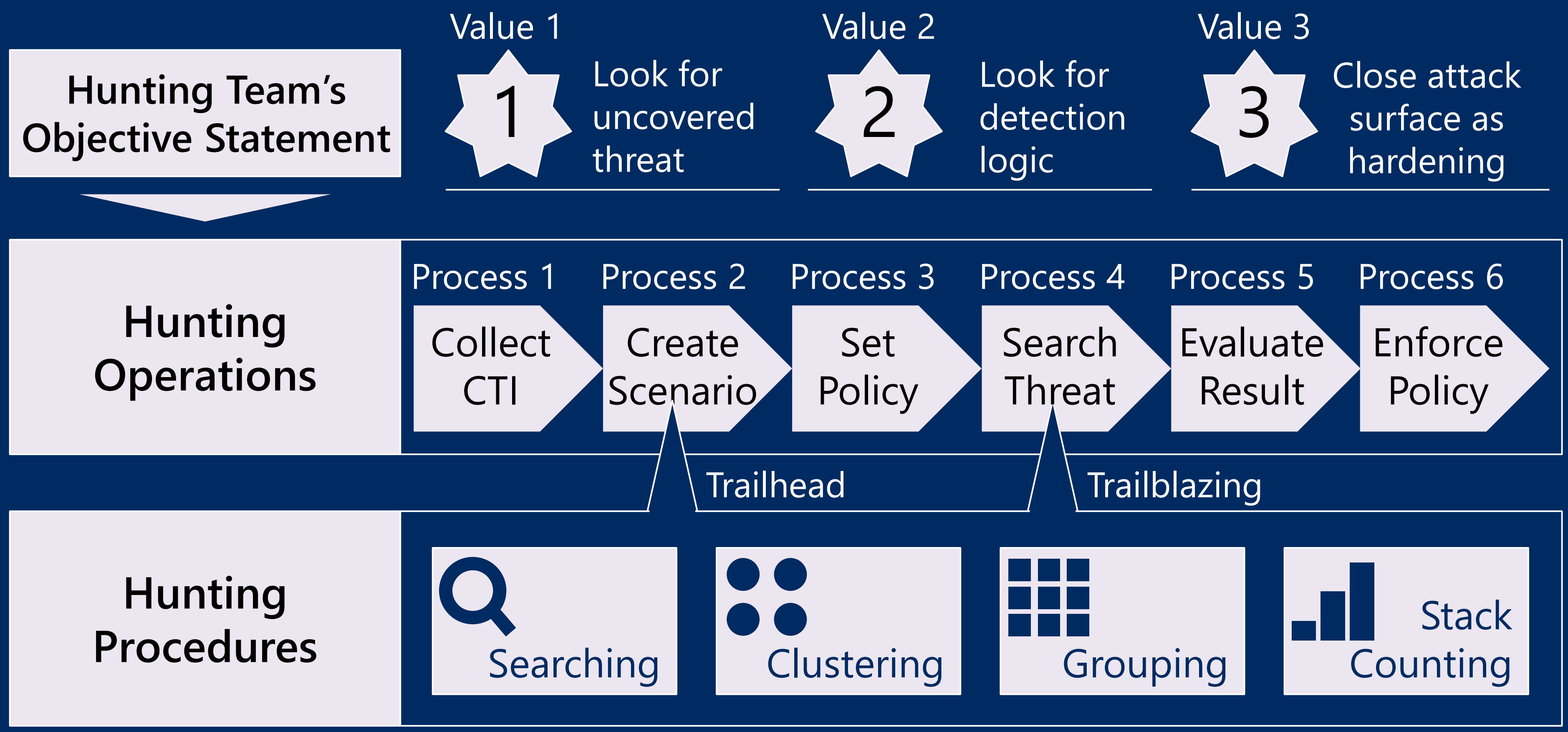
2

Look for logic such as signature, detection rule to detect uncovered threat, and apply to existing security solutions to close detection gaps.

3

Close attack surface as part of hardening activities to enhance current security posture together with Red team.

Threat Hunting Operations Framework



Hunting Team's Objective Statement

Value 1 — 1 — Look for uncovered threat

Value 2 — 2 — Look for detection logic

Value 3 — 3 — Close attack surface as hardening

Hunting Operations

Process 1: Collect CTI

Process 2: Create Scenario

Process 3: Set Policy

Process 4: Search Threat

Process 5: Evaluate Result

Process 6: Enforce Policy

Trailhead

Trailblazing

Hunting Procedures

Searching

Clustering

Grouping

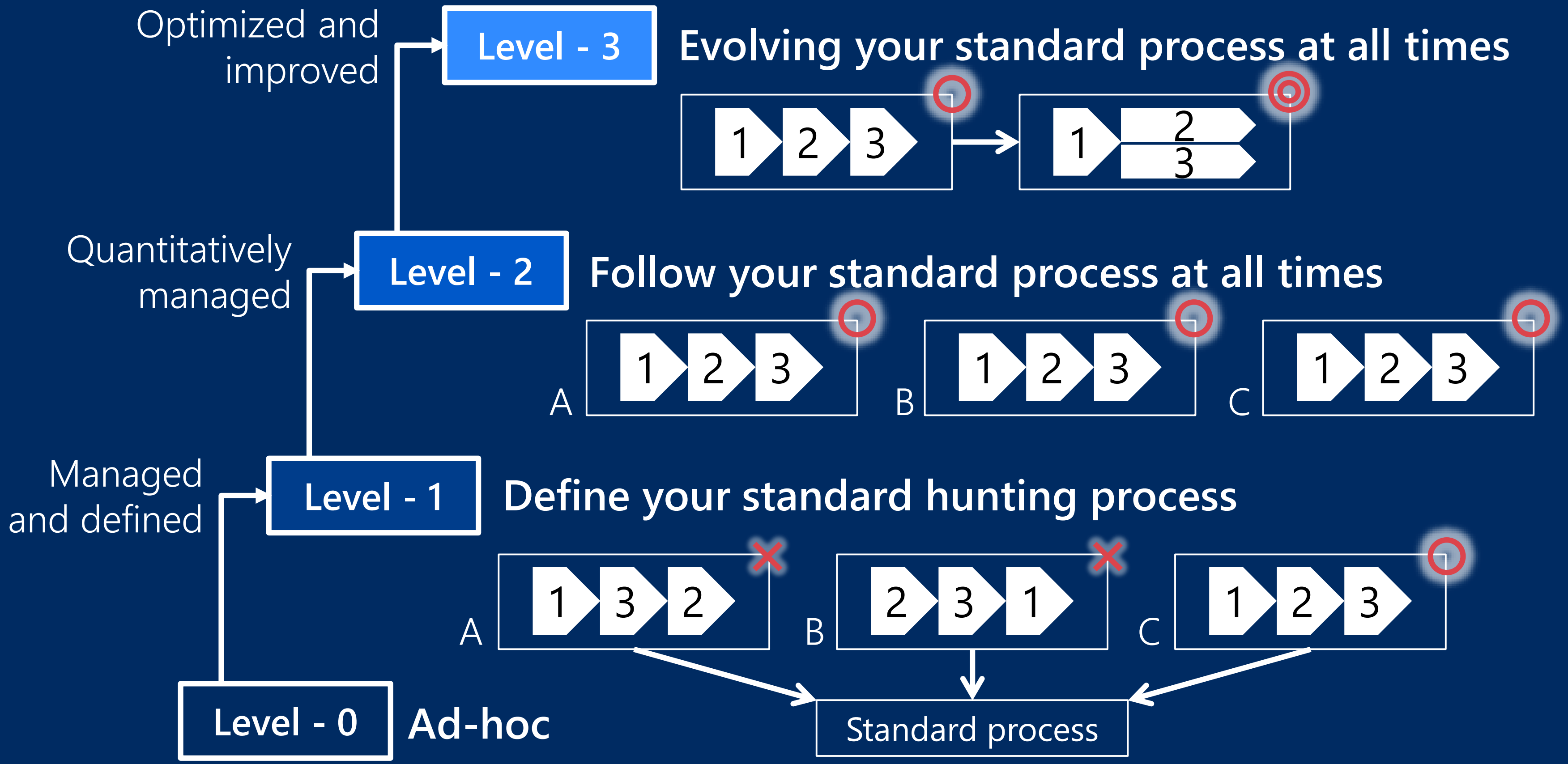
Stack Counting

KAIZEN, again

"The right process will produce the right results."

TOYOTA WAY

Hunting Process KAIZEN Model



Optimized and improved

Level - 3

Evolving your standard process at all times

Quantitatively managed

Level - 2

Follow your standard process at all times

Managed and defined

Level - 1

Define your standard hunting process

Standard process

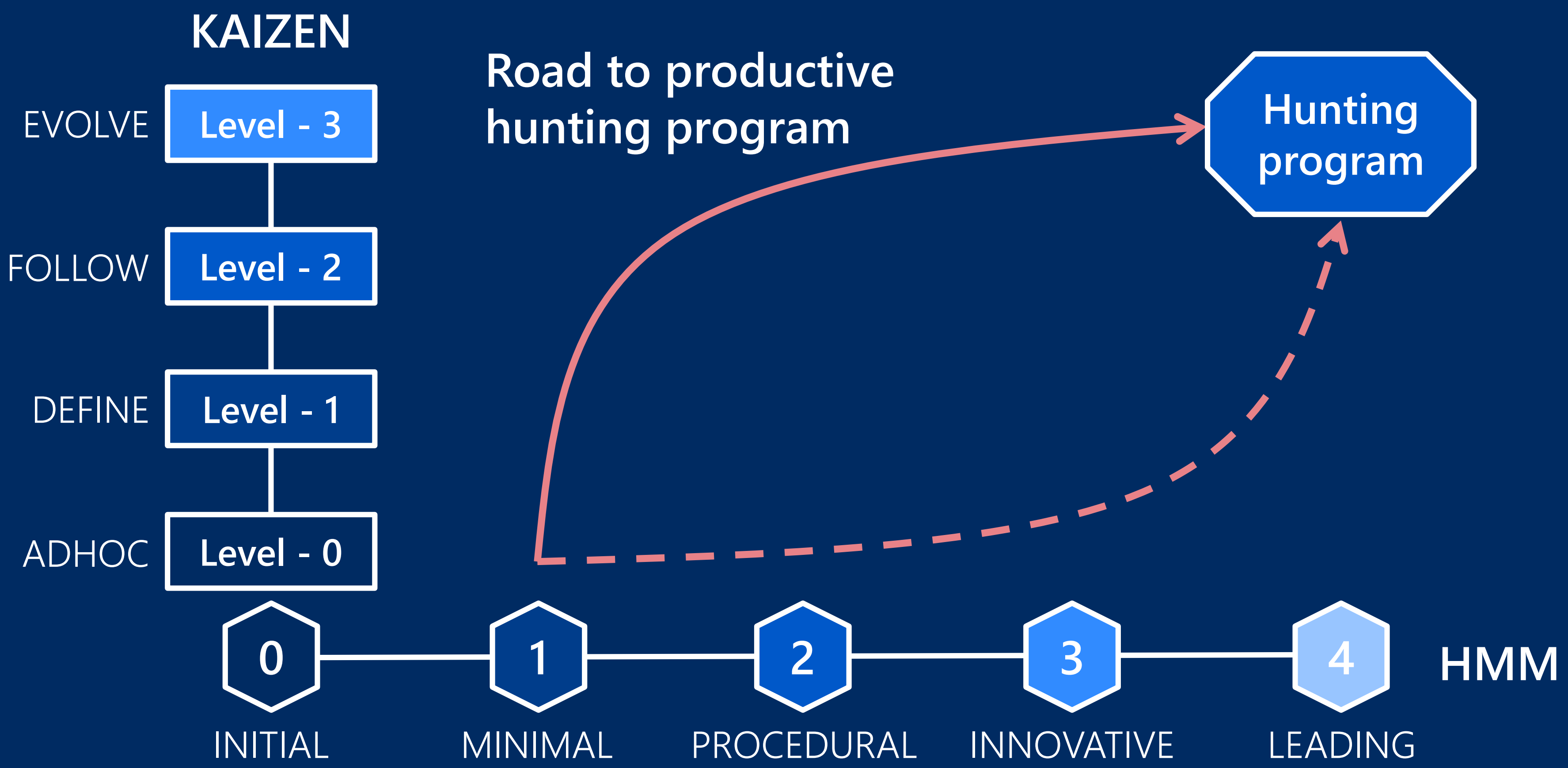
Level - 0

Ad-hoc

To improve productivity of hunting program

1. **Define your hunting process according to objectives where hunting team would produce the right results.**
   - Give priority to accomplish the process than making use of difficult hunting techniques you cannot handle.
   - Choose hunting techniques and tools which support the hunting process.
2. **Improve the process first based on KAIZEN**
   - Communication and KAIZEN culture are key to success.

HMM and KAIZEN



Conclusion

“A good hunter plays where the threat is. A great hunter plays where the threat is going to be.”

Thanks to

- Naoki Sasamura (NEC-CSIRT)
- Takeo Tagami (NEC-CSIRT)
- Yoshihiro Oshibuchi (NEC)

\Orchestrating a brighter world

NEC

References

"A Framework for Cyber Threat Hunting"
https://sqrrl.com/media/Framework-for-Threat-Hunting-Whitepaper.pdf

"threat hunter (cybersecurity threat analyst)"
https://searchcio.techtarget.com/definition/threat-hunter-cybersecurity-threat-analyst

"THE THREAT HUNTING REFERENCE MODEL PART 1: MEASURING HUNTING MATURITY"
https://sqrrl.com/the-threat-hunting-reference-model-part-1-measuring-hunting-maturity/

"Hunt Evil - Your Practical Guide to Threat Hunting"
https://sqrrl.com/media/ebook-web.pdf

"THE THREAT HUNTING REFERENCE MODEL PART 2: THE HUNTING LOOP"
https://sqrrl.com/the-threat-hunting-reference-model-part-2-the-hunting-loop/

"Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan"
https://www.amazon.com/Crafting-InfoSec-Playbook-Security-Monitoring/dp/1491949406

"Hunting Update, Joe Ten Eyck"
https://www.first.org/resources/papers/conf2017/Building-a-Threat-Hunting-Framework-for-the-Enterprise.pdf

"Generating Hypotheses for Successful Threat Hunting"
https://www.sans.org/reading-room/whitepapers/threats/generating-hypotheses-successful-threat-hunting-37172

"Threat Hunting in Security Operation - SANS Threat Hunting Summit 2017"
https://www.youtube.com/watch?v=pDY639JsT7I

"TOYOTA KAIZEN practice in management"
https://www.amazon.co.jp/o/ASIN/4046019603