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.”
“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 process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions.”

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”
“Threat Awareness”
“Creative”
“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

Our Security Operations

- SOC Team
- Incident Response Team
- Protection Operation Team
- Malware Analysis Team
- CSIRT Manager

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

IOC searches

Indicators \times Proxy log = ???

{IP address, URL} \times \{IP address, URL\} = ???

https://sqrrl.com/media/ebook-web.pdf
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 \{IP address, URL\} × Proxy log \{IP address, URL\} = \emptyset

PROCESS or TECHNIQUE
Building Threat Hunting Operations
"The right process will produce the right results."

TOYOTA WAY
Outline of Threat Hunting Operations Framework

Hunting Team’s Objective Statement

Value 1  Value 2  Value 3

Hunting Operations


Hunting Procedures

Searching  Clustering  Grouping  Stack Counting
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

CREATE Hypotheses

INFORM & ENRICH Analytics

UNCOVER New Patterns & TTP’s

INVESTIGATE Via Tools & Techniques

- Threat Hunting Team
  - Incident Response (Forensics)
  - Threat Research

- Hunting Operation Team
  - Operate via Tools

- Threat Research Team
  - Threat Research

Actions lead to business goals

“Understand business requirement enough before constructing the process.”

Define response policy in advance
- Escalation
- Precaution
- Mitigation
- Remediation

“Crafting the InfoSec Playbook”

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

Communicate
- Analyze and Draw Conclusions
- Communicate All Results
- Refactor include in Future Hunts

Minimum Cycle

Prepare
“where” and “what”

Find
“how” and “query”

Communicate
“so what”

Jump the hurdle to getting the milestone

1. Simple first and collect from outside
   a. Intelligence-driven
   b. Situational awareness
   c. Domain expertise
   
   [Link](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 Hunting Operations

0. Set Objectives

1. Collect internal/external CTI

2. Analyze CTI & Create Scenario

3. Set Response Policy

4. Search Threat

5. Evaluate Result

6. Enforce Response Policy

CSIRT Manager

Threat Research Team

Threat Hunting Team

Threat Hunting Team

Hunting Operation Team

Incident Response Team

Incident Response Team

Incident Response Team
Threat Hunting Operations

0. Set Objectives

1. Collect internal /external CTI

2. Analyze CTI & Create Scenario

3. Set Response Policy

4. Search Threat

5. Evaluate Result

6. Enforce Response Policy

CSIRT Manager

Threat Research Team

Threat Hunting Team

Incident Response Team

Hunting Operation Team
Threat Hunting Operations

0. Set Objectives

1. Collect internal/external CTI

2. Analyze CTI & Create Scenario

3. Set Response Policy

4. Search Threat

5. Evaluate Result

6. Enforce Response Policy

CSIRT Manager

Threat Research Team

Threat Hunting Team

Incident Response Team

Incident Response Team

Hunting Operation Team
Threat Hunting Operations

0. Set Objectives

1. Collect internal /external CTI

2. Analyze CTI & Create Scenario

3. Set Response Policy

4. Search Threat

5. Evaluate Result

6. Enforce Response Policy

- CSIRT Manager
- Threat Research Team
- Threat Hunting Team
- Threat Hunting Operation Team
- Incident Response Team
Threat Hunting Operations

0. Set Objectives

1. Collect internal /external CTI

2. Analyze CTI & Create Scenario

3. Set Response Policy

4. Search Threat

5. Evaluate Result

6. Enforce Response Policy

CSIRT Manager

Threat Research Team

Threat Hunting Team

Hunting Operation Team

Incident Response Team

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

0. Set Objectives

1. Collect internal/external CTI

2. Analyze CTI & Create Scenario

3. Set Response Policy

4. Search Threat

5. Evaluate Result

6. Enforce Response Policy

Possible targeted attack via email ???

No alert, check email delivery log

Confirmed undetected attack

Contact employee not to open it

Search email delivery as instructed

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

Confirmed undetected attack

Contact employee not to open it

Search email delivery as instructed

Check if employee opened & clicked it. Notify not to open it.
Case Study #1 – Process Overview (1)

0. Set Objectives

1. Collect internal /external CTI

2. Analyze CTI & Create Scenario

3. Set Response Policy

4. Search Threat

5. Evaluate Result

6. Enforce Response Policy

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)

0. Set Objectives

1. Collect internal /external CTI

2. Analyze CTI & Create Scenario

3. Set Response Policy

4. Search Threat

5. Evaluate Result

6. Enforce Response Policy

- Search email delivery as instructed

Threat Research Team

CSIRT Manager

Incident Response Team

Threat Hunting Team

Incident Response Team

Threat Hunting Team

Hunting Operation Team

Threat Hunting Operation Team
Case Study #1 – Process Overview (3)

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

Contact employee not to open it

Confirmed undetected attack

Incident Response Team
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)

0. Set Objectives

1. Collect internal/external CTI

2. Analyze CTI & Create Scenario

3. Set Response Policy

4. Search Threat

5. Evaluate Result

6. Enforce Response Policy

Possible similar APT attack ???

Check IP, URL, and HTTP request header

Need immediate action because of APT

Confirmed malicious traffic evidence on proxy

Repeatedly search every evidence

Started a major investigation into it.
Case Study #2 – Process Overview (part 1)

0. Set Objectives

1. Collect internal/external CTI

2. Analyze CTI, Create Scenario

3. Set Response Policy

4. Search Threat

5. Evaluate Result

6. Enforce Response Policy

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

1. Collect internal/external CTI

2. Analyze CTI & Create Scenario

3. Set Response Policy

4. Search Threat

5. Evaluate Result

6. Enforce Response Policy

Repeatedly search every evidence

CSIRT Manager

Threat Research Team

Threat Hunting Team

Threat Hunting Team

Incident Response Team

Incident Response Team

Hunting Operation Team
Case Study #2 – Process Overview (part 1)

0. Set Objectives

1. Collect internal / external CTI

2. Analyze CTI & Create Scenario

3. Set Response Policy

4. Search Threat

5. Evaluate Result

6. Enforce Response Policy

Confirmed malicious traffic evidence on proxy

Started a major investigation into it.

CSIRT Manager

Threat Research Team

Threat Hunting Team

Threat Hunting Team

Hunting Operation Team

Incident Response Team

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)

0. Set Objectives

1. Collect internal/external CTI

2. Analyze CTI & Create Scenario

3. Set Response Policy

4. Search Threat

5. Evaluate Result

6. Enforce Response Policy

- **CSIRT Manager**
- **Threat Research Team**
- **Threat Hunting Team**
- **Incident Response Team**

**Found specific traffic on PCs undetected by initial known indicators**

**Search query expressed as specific HTTP request**

**Started immediate mitigation**

- **Threat Research Team**
- **Incident Response Team**

**Check HTTP request with extracted pattern**

**Possible similar TTPs used ???**

**Need immediate action because of APT**
Case Study #2 – Process Overview (part 2)

0. Set Objectives

1. Collect internal/external CTI
   - Threat Research Team
   - Hunting Operation 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

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

1. Collect internal/external CTI

2. Analyze CTI & Create Scenario

3. Set Response Policy

4. Search Threat

5. Evaluate Result

6. Enforce Response Policy

Search query expressed as specific HTTP request
0. Set Objectives

- Found specific traffic on PCs undetected by initial known indicators

1. Collect internal/external CTI

- Started immediate mitigation

2. Analyze CTI & Create Scenario

3. Set Response Policy

4. Search Threat

5. Evaluate Result

- Reinforce Response Policy

6. Enforce Response Policy

- Incident Response Team

- Threat Research Team

- Threat Hunting Team

- Threat Hunting Operation Team

- CSIRT Manager
Case Study #2 – Found additional infected PCs by pattern

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Host name</th>
<th>Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.xxx.com/%7Bpath1/path2/path3/xxx.html%7D">http://www.xxx.com/{path1/path2/path3/xxx.html}</a></td>
<td>?svkrfghu=VGhpcyBpcyBzYW1wbGUxLiBUaGlzIGlzIHNhbXBsZTIuIFRo</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.xxx.com/%7Bpath1/path2/path3/xxx.html%7D">http://www.xxx.com/{path1/path2/path3/xxx.html}</a></td>
<td>?emexg=3YXMgc2FtcGx1MS4gVGhhdCB3YXMgc2FtcGx1MyFtcGx1MS4gVG</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.xxx.com/%7Bpath1/path2/path3/xxx.html%7D">http://www.xxx.com/{path1/path2/path3/xxx.html}</a></td>
<td>?eprinuf=a29yZWhhIHNhbXBsZSBkZXN1MS4hhIHNhbXBBkZXN1Mi4ga29yZW</td>
<td></td>
</tr>
</tbody>
</table>

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

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

0. Set Objectives
- Start a normal investigation action.

1. Collect internal/external CTI

2. Analyze CTI, Create Scenario
- Make a scenario to check IP, URL.

3. Set Response Policy
- Blocking external traffic would be fine.

4. Search Threat
- Repeatedly search evidence on proxy log.

5. Evaluate Result
- Confirmed exact traffic on several PCs.

6. Enforce Response Policy
- Possible adware type attack ???

Threat Hunting Team
Threat Research Team
Incident Response Team
CSIRT Manager
Hunting Operation Team
Case Study #3 – Process Overview (part 1) (1)

1. Collect internal/external CTI

2. Analyze CTI & Create Scenario

3. Set Response Policy

4. Search Threat

5. Evaluate Result

6. Enforce Response Policy

0. Set Objectives

Possible adware type attack???

Make scenario to check IP, URL

Blocking external traffic would be fine.
Case Study #3 – Process Overview (part 1) (2)

0. Set Objectives

1. Collect internal /external CTI

2. Analyze CTI & Create Scenario

3. Set Response Policy

4. Search Threat
   - Repeatedly search evidence on proxy log

5. Evaluate Result

6. Enforce Response Policy

CSIRT Manager

Threat Research Team

Incident Response Team

Threat Hunting Team

Threat Hunting Operation Team
Case Study #3 – Process Overview (part 1) (3)

0. Set Objectives

1. Collect internal/external CTI

2. Analyze CTI & Create Scenario

3. Set Response Policy

4. Search Threat

5. Evaluate Result

6. Enforce Response Policy

- Confirmed exact traffic on several PCs
- Started a normal investigation actions

CSIRT Manager

Threat Research Team

Incident Response Team

Hunting Operation Team

Threat Hunting Team
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)

0. Set Objectives

1. Collect internal /external CTI

2. Analyze CTI & Create Scenario

3. Set Response Policy

4. Search Threat

5. Evaluate Result

6. Enforce Response Policy

CSIRT Manager

Threat Research Team

Threat Hunting Team

Incident Response Team

Hunting Operation Team

No, it’s targeted attack!

Make scenario updated with additional indicators

Search evidence with updated indicators

Confirmed additional evidence undetected

Started deep investigation actions

Need investigation, forensic, and response

Confirmed additional evidence undetected

Search evidence with updated indicators

No, it’s targeted attack!
Case Study #3 – Process Overview (part 2)

1. Collect internal/external CTI

2. Analyze CTI & Create Scenario

3. Set Response Policy

4. Search Threat

5. Evaluate Result

6. Enforce Response Policy

- Set Objectives
- Collect internal/external CTI
- Analyze CTI & Create Scenario
- Set Response Policy
- Search Threat
- Evaluate Result
- Enforce Response Policy

No, it’s targeted attack!

Make scenario updated with additional indicators

Need investigation, forensic, and response
Case Study #3 – Process Overview (part 2) (2)

0. Set Objectives

1. Collect internal /external CTI

2. Analyze CTI & Create Scenario

3. Set Response Policy

4. Search Threat

5. Evaluate Result

6. Enforce Response Policy

Search evidence with updated indicators

CSIRT Manager

Threat Research Team

Incident Response Team

Threat Hunting Team

Incident Response Team

Threat Hunting Team

Hunting Operation Team

SANS Threat Hunting & IR Summit 2018
Case Study #3 – Process Overview (part 2) (3)

0. Set Objectives

1. Collect internal/external CTI

2. Analyze CTI & Create Scenario

3. Set Response Policy

4. Search Threat

5. Evaluate Result

6. Enforce Response Policy

- Started deep investigation actions
- Confirmed additional evidence undetected

Threat Research Team

Threat Hunting Team

Incident Response Team

Hunting Operation Team

CSIRT Manager
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

1. Collect internal/external CTI

2. Analyze CTI & Create Scenario

3. Set Response Policy

4. Search Threat

5. Evaluate Result

6. Enforce Response Policy
<table>
<thead>
<tr>
<th>Threat Hunting Team</th>
<th>Hunting Operation Team</th>
<th>Incident Response Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset, Internal System, Directory DB</td>
<td>Log Analysis &amp; Dashboard</td>
<td>Forensic Tool</td>
</tr>
<tr>
<td>Internal CTI (Observed &amp; Analysis) DB</td>
<td>EDR / NCSP</td>
<td>Log Management</td>
</tr>
<tr>
<td>Hunting Scenario System (STIX)</td>
<td>User Inquiry System</td>
<td>Threat Intelligence Platform (TIP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Threat Analysis System</td>
</tr>
</tbody>
</table>
Threat Hunting System Architecture Overview

1. **Enrichment Source**
2. **CTI Source (External/Internal)**
3. **Threat Analysis System**
4. **Threat Intelligence Platform (TIP)**
5. **Hunting Scenario System (STIX)**
6. **Logs (Network/Mail)**
7. **Training Data**
8. **Threat Research Team**
9. **Threat Hunting Team**
10. **Hunting Operation Team**
11. **Incident Response Team**
12. **Log Analysis & Dashboard**
13. **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

<table>
<thead>
<tr>
<th>Value 1</th>
<th>Value 2</th>
<th>Value 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Look for uncovered threat</td>
<td>Look for detection logic</td>
<td>Close attack surface as hardening</td>
</tr>
</tbody>
</table>

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

Hunting Procedures

- Searching
- Clustering
- Grouping
- Stack Counting

Trailhead

Trailblazing
KAIZEN, again

"The right process will produce the right results."

TOYOTA WAY
Hunting Process KAIZEN Model

Level - 0: Ad-hoc
- Managed and defined
- Quantitatively managed
- Optimized and improved

Level - 1: Define your standard hunting process
- A: 1 → 2 → 3
- B: 2 → 3 → 1
- C: 1 → 2 → 3

Level - 2: Follow your standard process at all times
- A: 1 → 2 → 3
- B: 1 → 2 → 3
- C: 1 → 2 → 3

Level - 3: Evolving your standard process at all times
- A: 1 → 2 → 3
- B: 1 → 2 → 3
- C: 1 → 2 → 3
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

Road to productive hunting program

KAIZEN

EVOLVE - Level - 3
FOLLOW - Level - 2
DEFINE - Level - 1
ADHOC - Level - 0

0 - INITIAL
1 - MINIMAL
2 - PROCEDURAL
3 - INNOVATIVE
4 - LEADING

HMM

Hunting program

Level - 0

Level - 1

Level - 2

Level - 3
“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)
“A Framework for Cyber Threat Hunting”

“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”

“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”

“Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan”

“Hunting Update, Joe Ten Eyck”

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

https://www.youtube.com/watch?v=pDY639JsT7I

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