Quad Miners

HUNT OR GET HUNTED

Network Blackbox Introduction

Felix Kim CTO
June 2025

Organization have been hacked.

Do you know who did it?

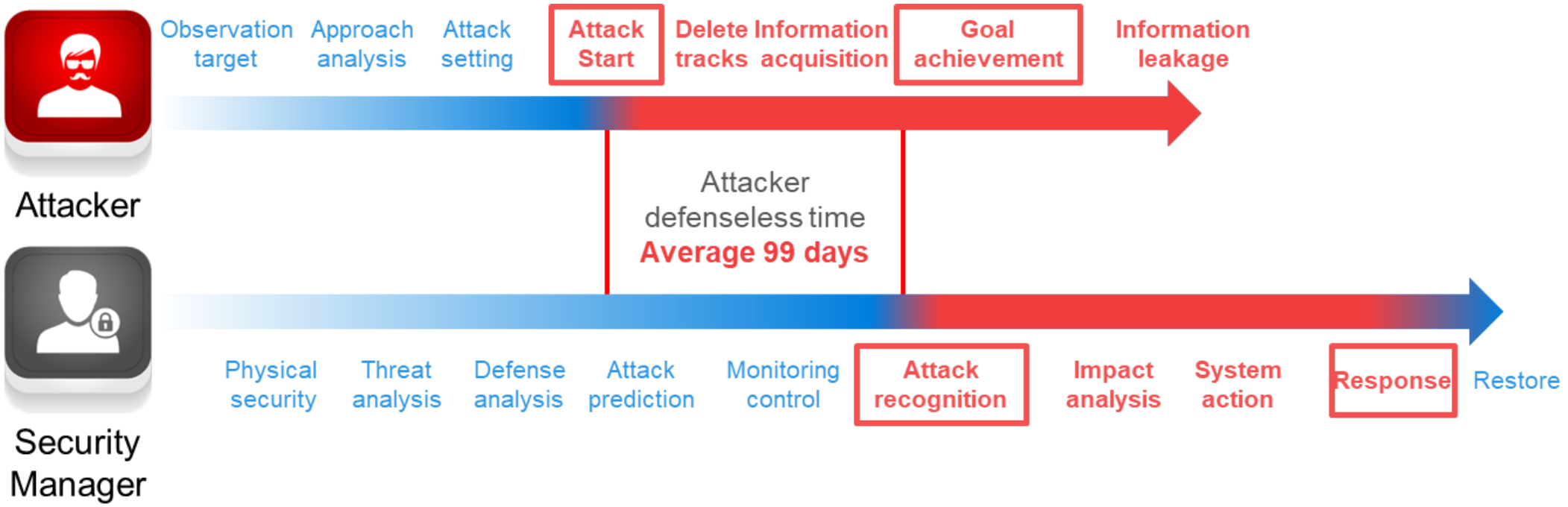
Do you know what was taken?

Do you know where they came from?

Ultimately, Can you stop the bleeding?

Quad Miners

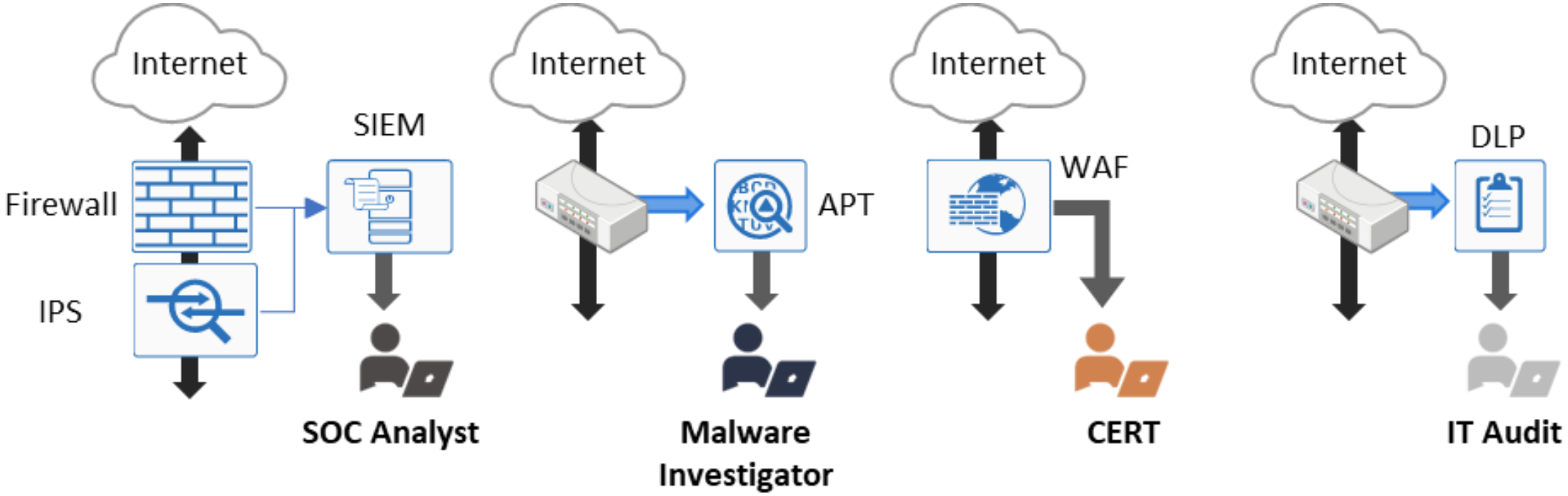
99% of hacking accidents caused damage within 3 days, and 85% of accidents leaked data.



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

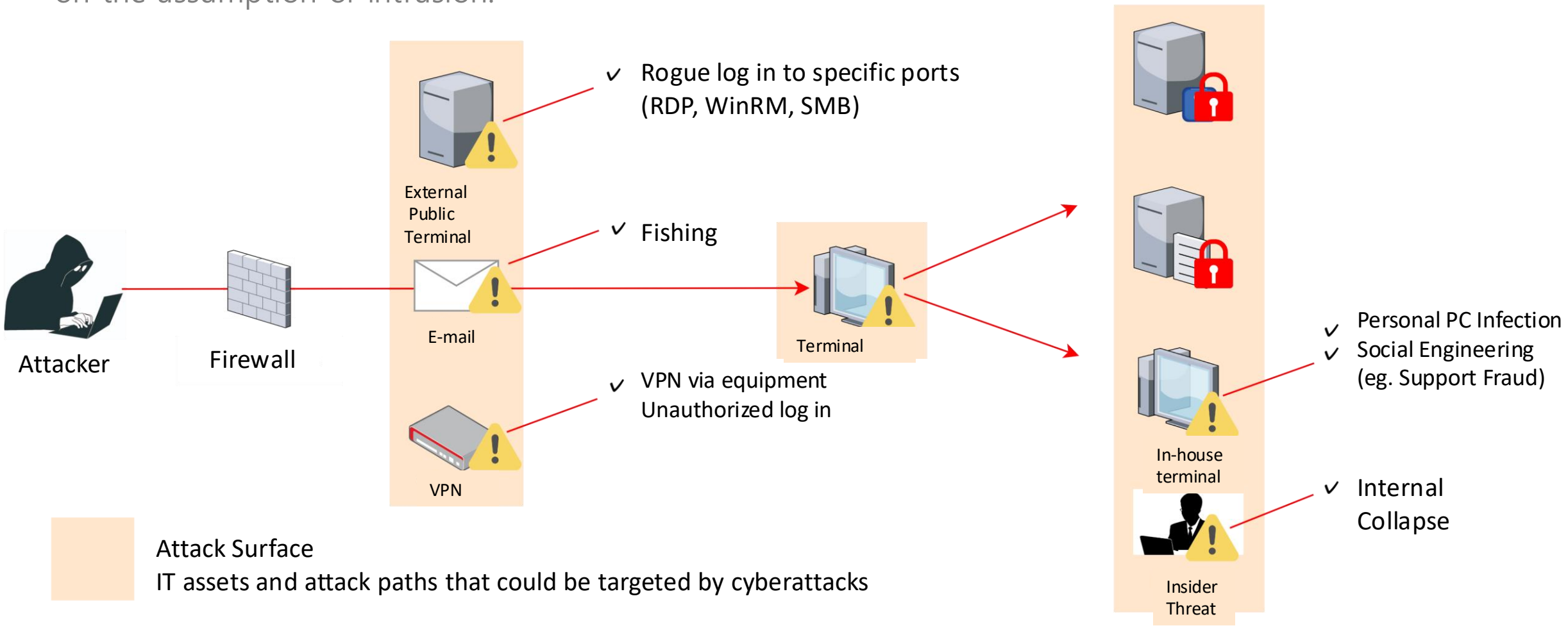
Problems and challenges with current security landscape

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



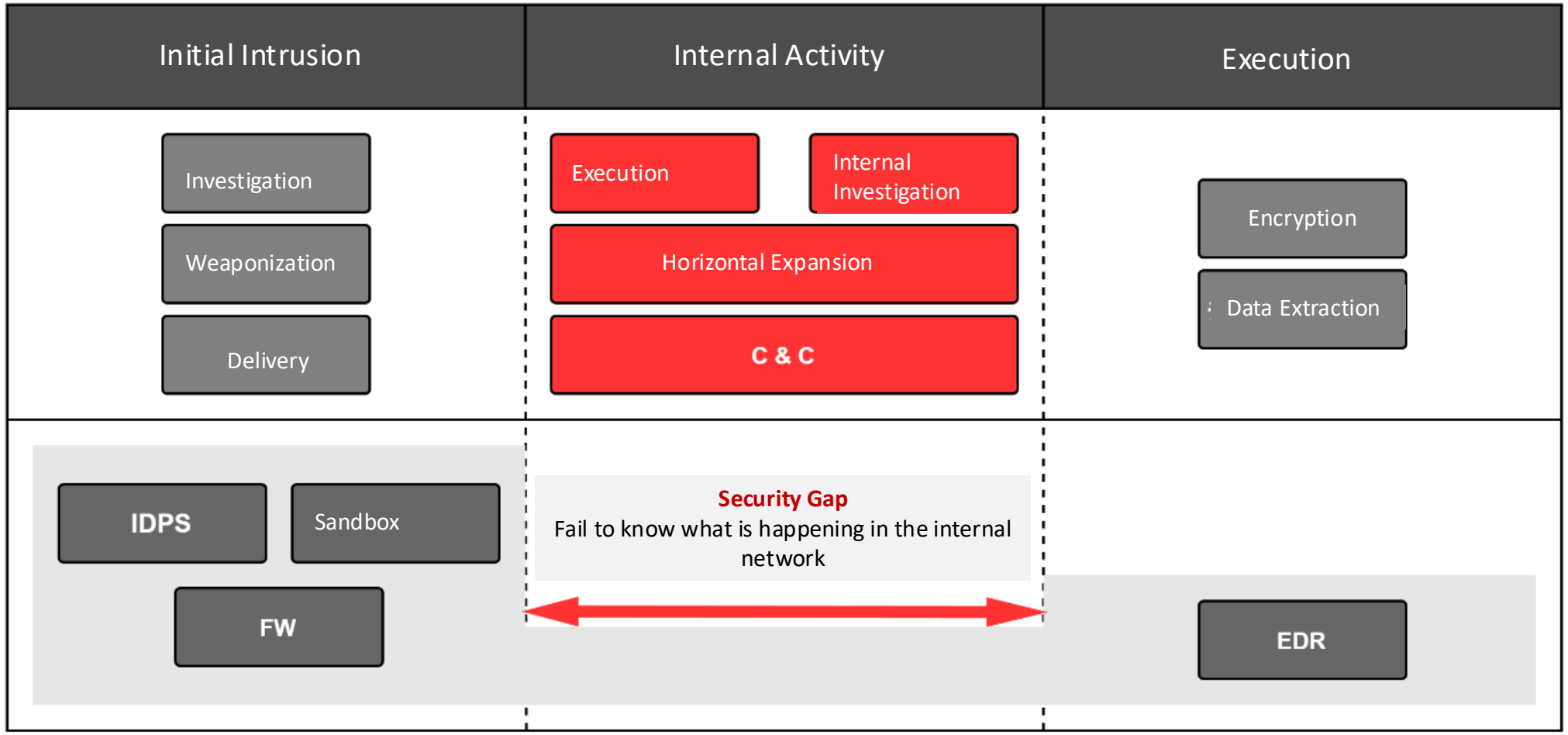
It is impossible to prevent attackers from intruding 100%.

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.



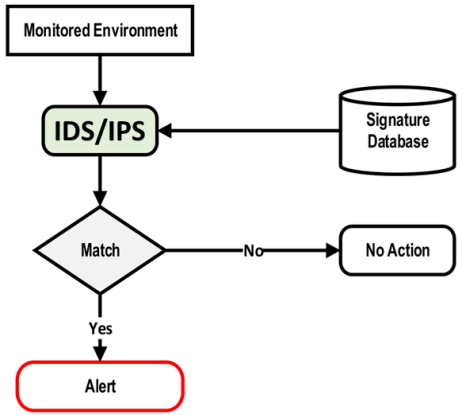
Differentiation with Full Packet Capture-based traffic total inspection

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

Evolution of technology

1

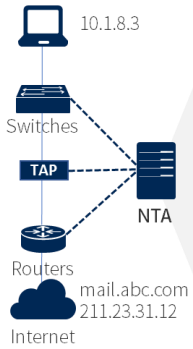
Intrusion Detection System
Intrusion Prevention System



- Known Attack Focused
- Over Detection and False Positive Issues

2

Network Traffic Analytics

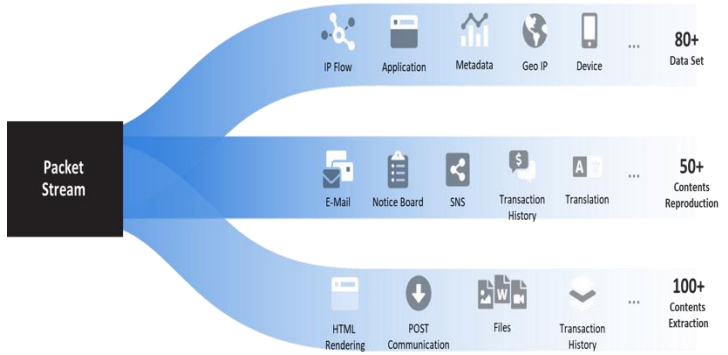


Information	Packets
SRC IP	10.1.8.3
DEST IP	211.23.31.12
SRC PORT	47321
DEST PORT	443
INTERFACE	Gi0/0/0
TOS	0x00
PROTOCOL	6
NEXT HOP	172.168.25.1
PACKETS/BYTES	23 / 1382
TIME STAMP	10:32:56.089
Meta Data	App Name HTTP
Meta Data	HTTP/1.1 200 OK
Meta Data	Host: mail.abc.com

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

3

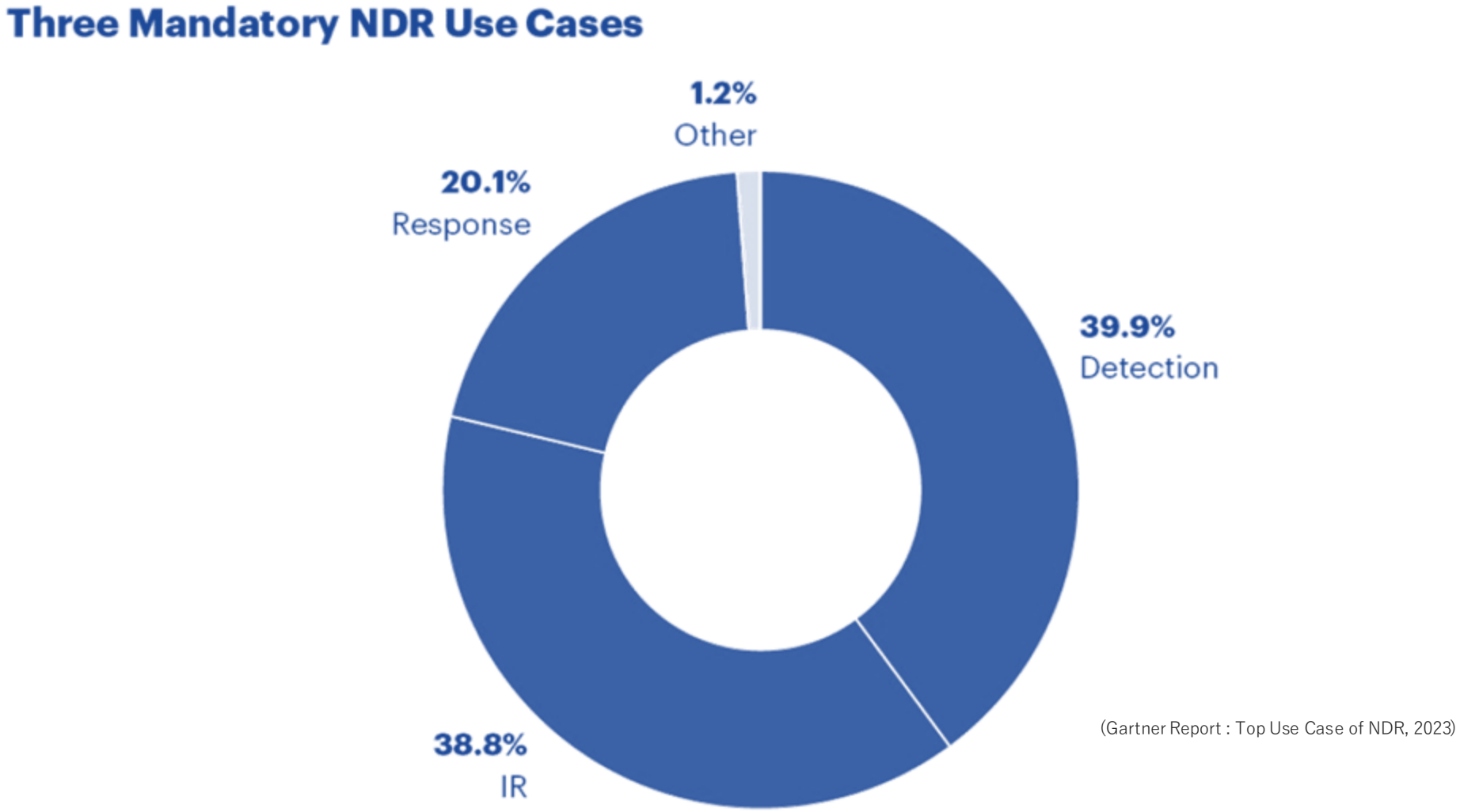
Network Detection and Response



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

Evolving Customer Adoption Trends in the NDR Market

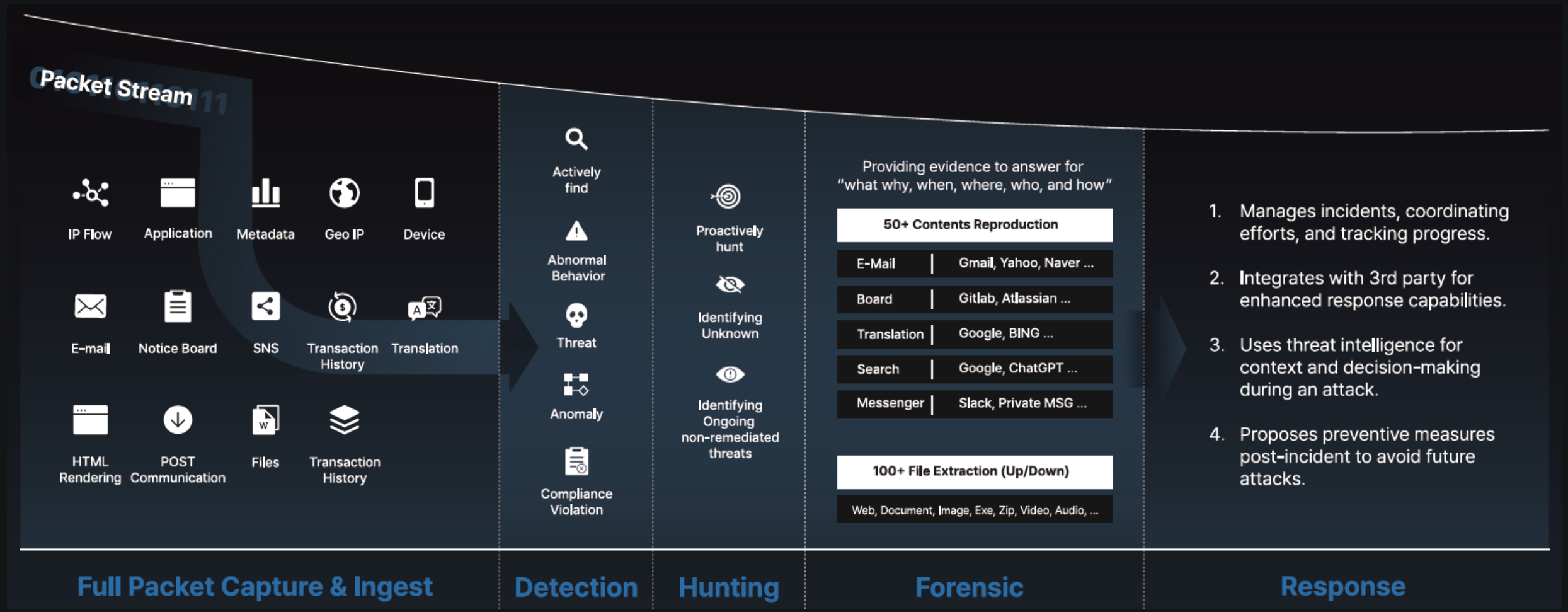
When buyers evaluate NDR, IR (Hunting & Forensic) functionality is where the time is spent.



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

NETWORK BLACKBOX

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

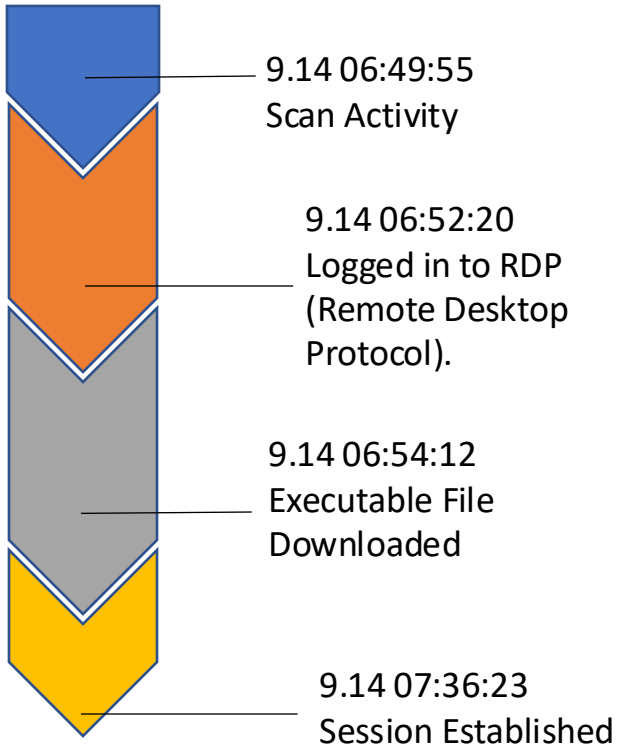


100% full packet capture

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

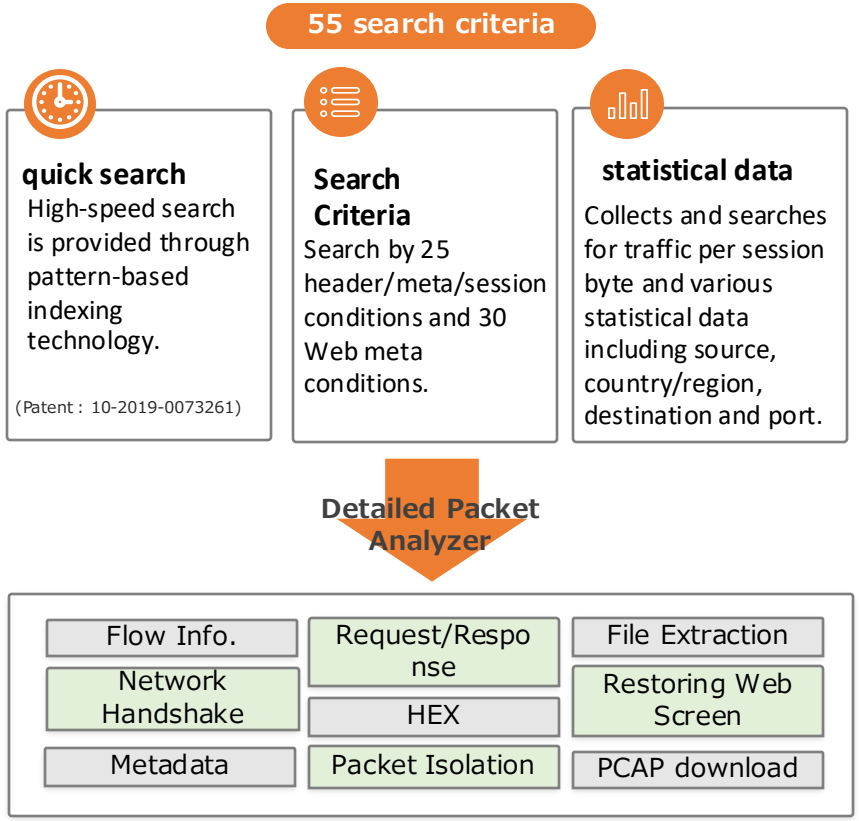
1. Threat Visualization

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



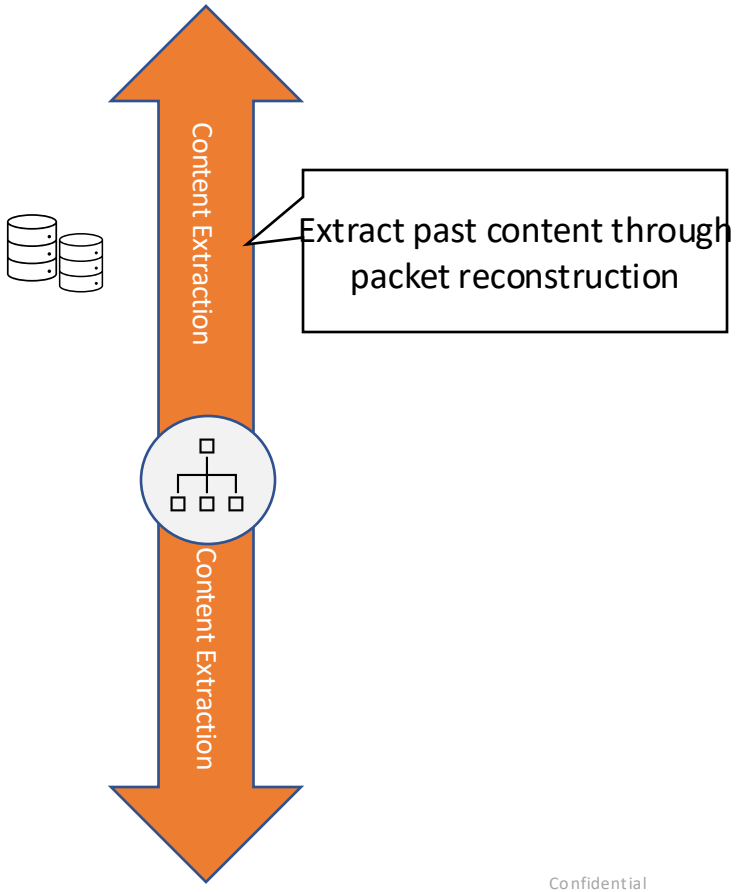
2. High Speed Analysis by Pattern

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

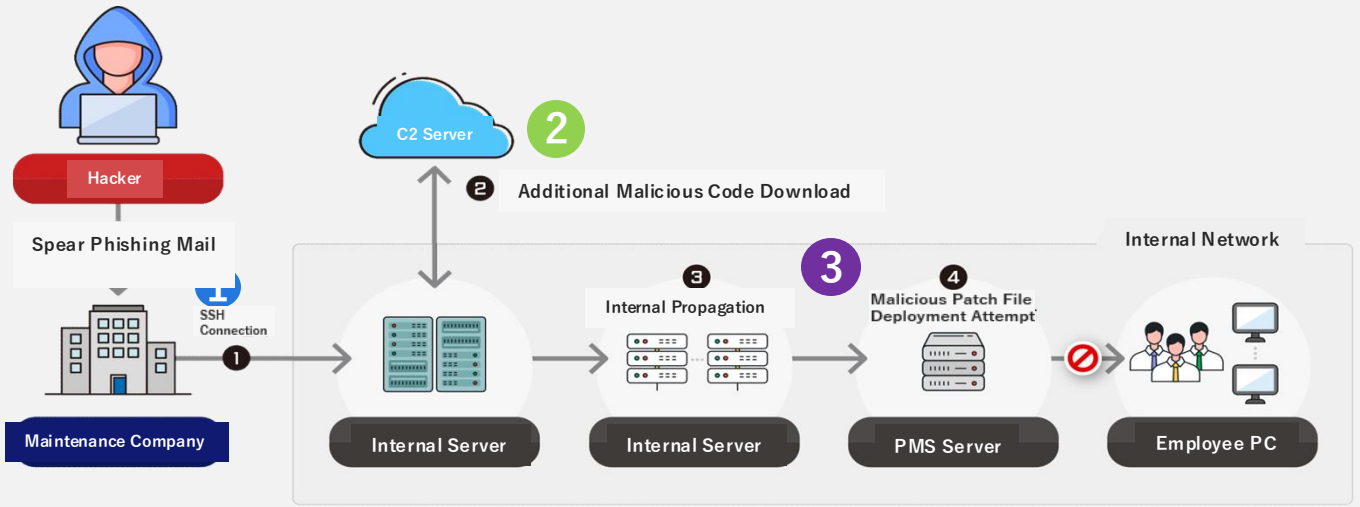


3. Packet Reconstruction

Reconstruct packets in full stream for conducting regression analysis



Network Blackbox Monitoring



1 Traffic Monitoring: Connection Pattern

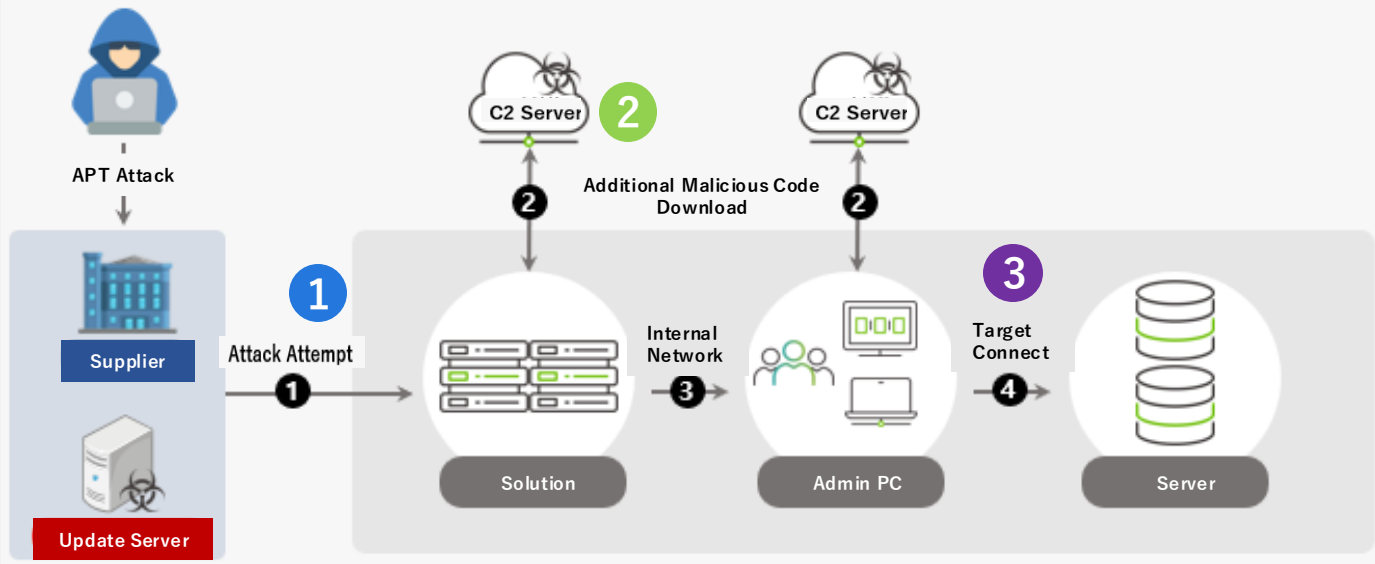
A. Pattern analysis of connections from maintenance contractors to servers:
-Existence of server connection time patterns
-Presence of connection history during work hours and after hours
-Presence of file uploads via SSH

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

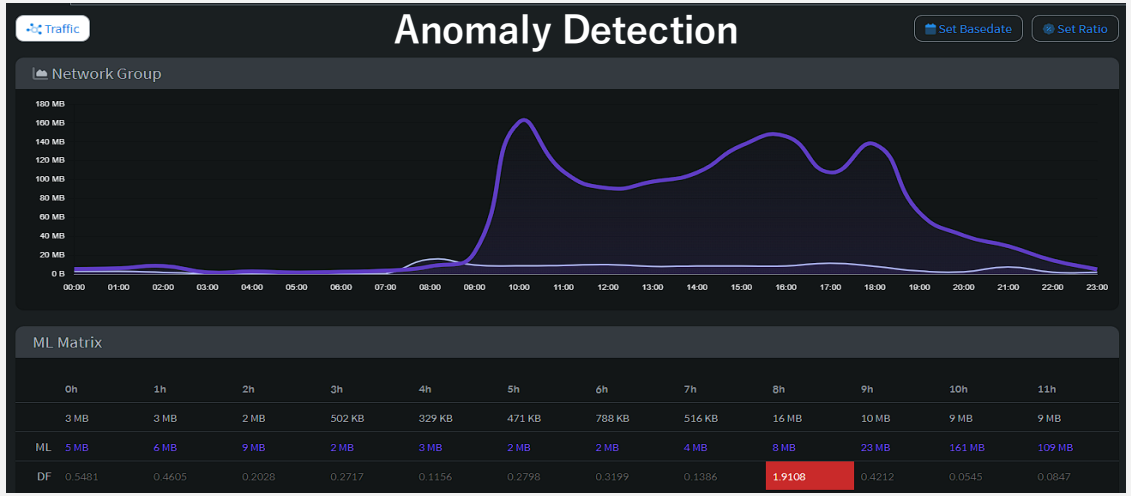
3 Traffic Monitoring: Connection Pattern

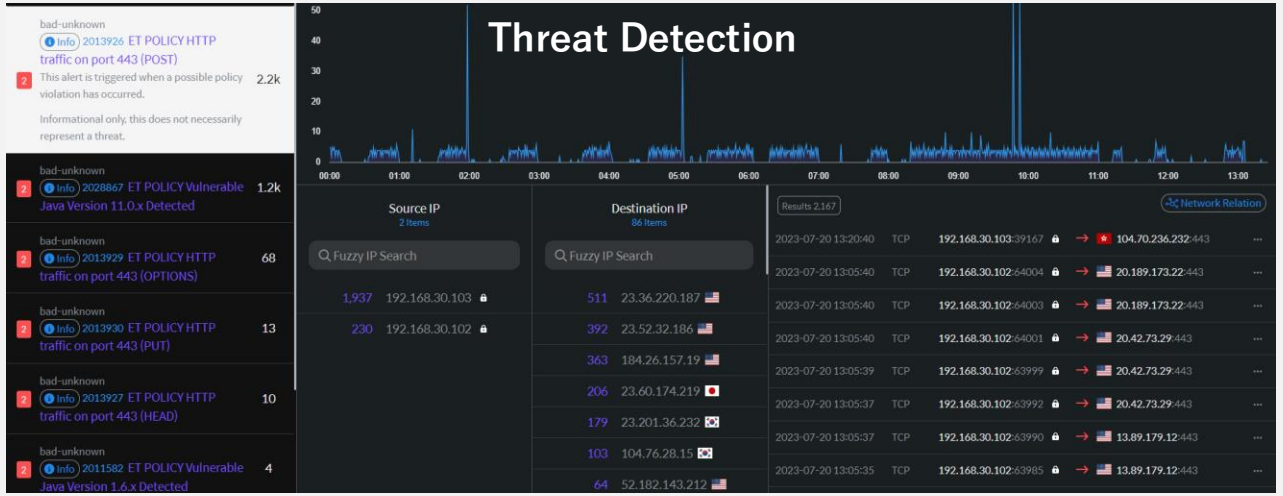
A. Analysis of connection patterns to servers:
-Monitoring of server-to-server session packets
-Presence of history indicating access to target servers from multiple PCs

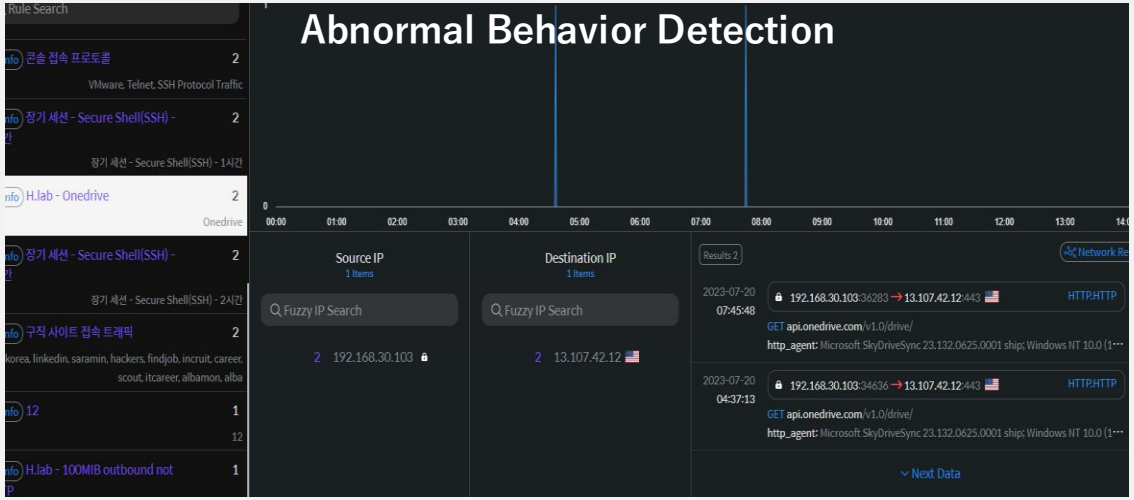


Network Blackbox- Detection

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

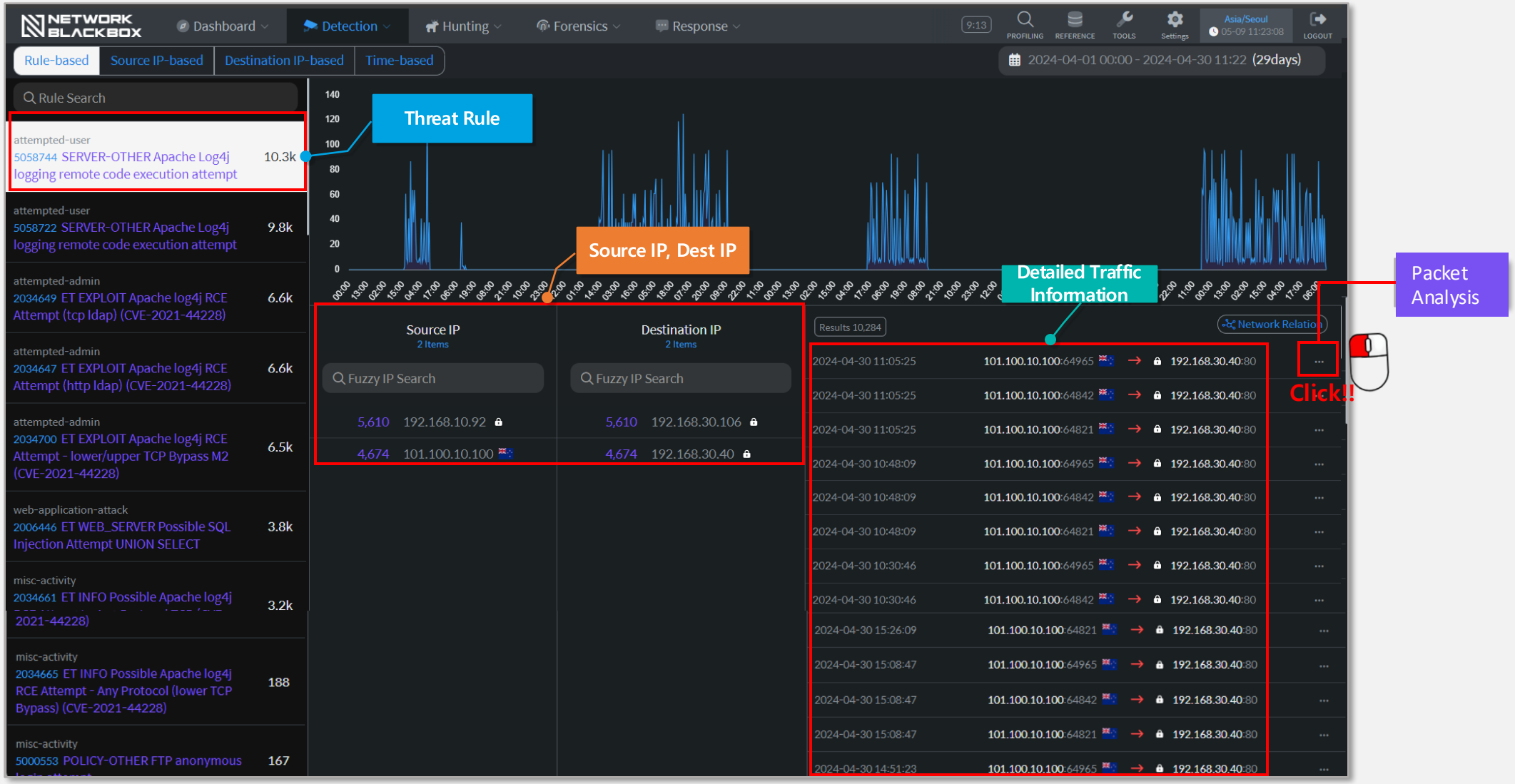






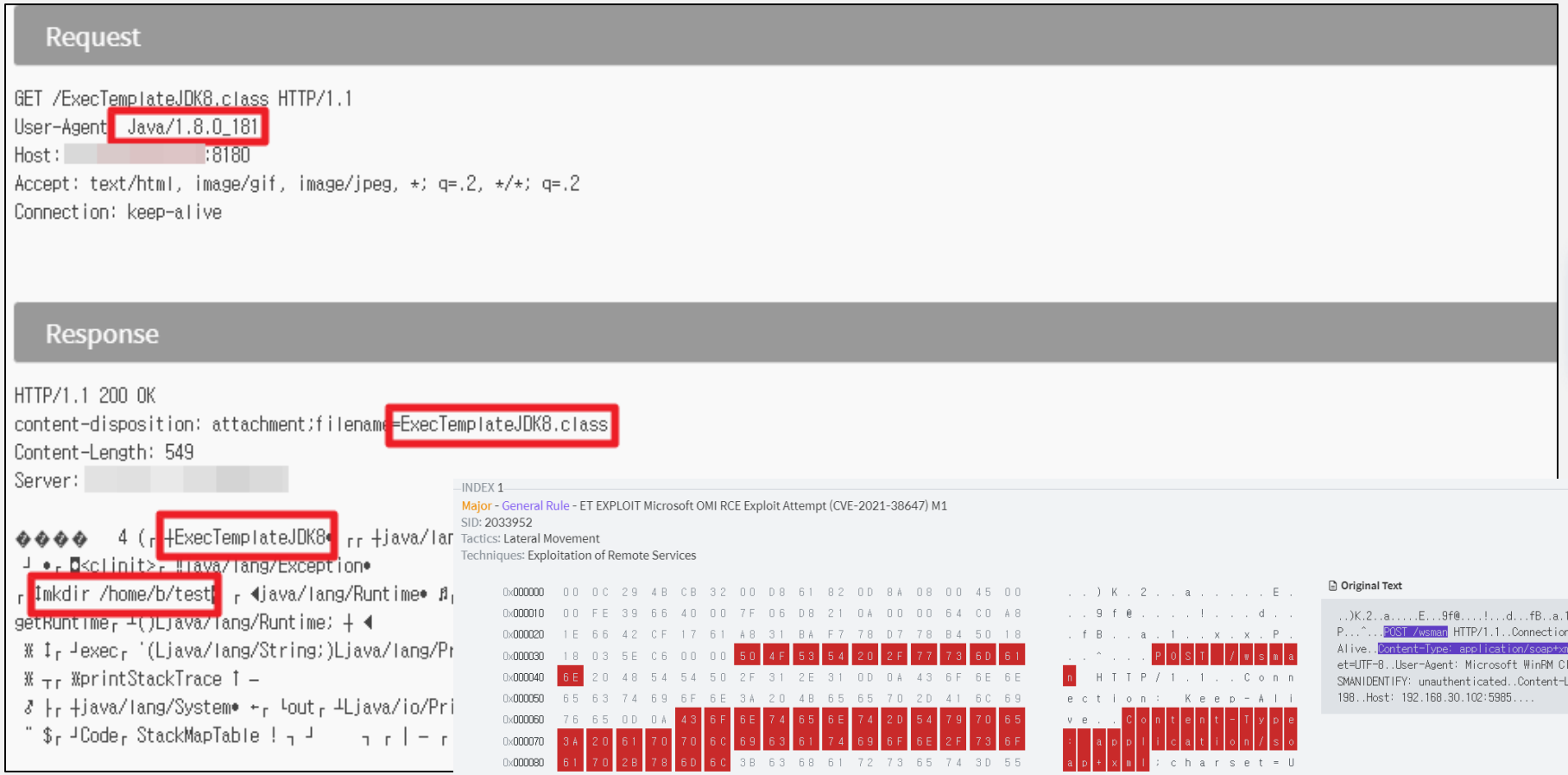
Network Blackbox- Detection

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



Network Blackbox- Detection

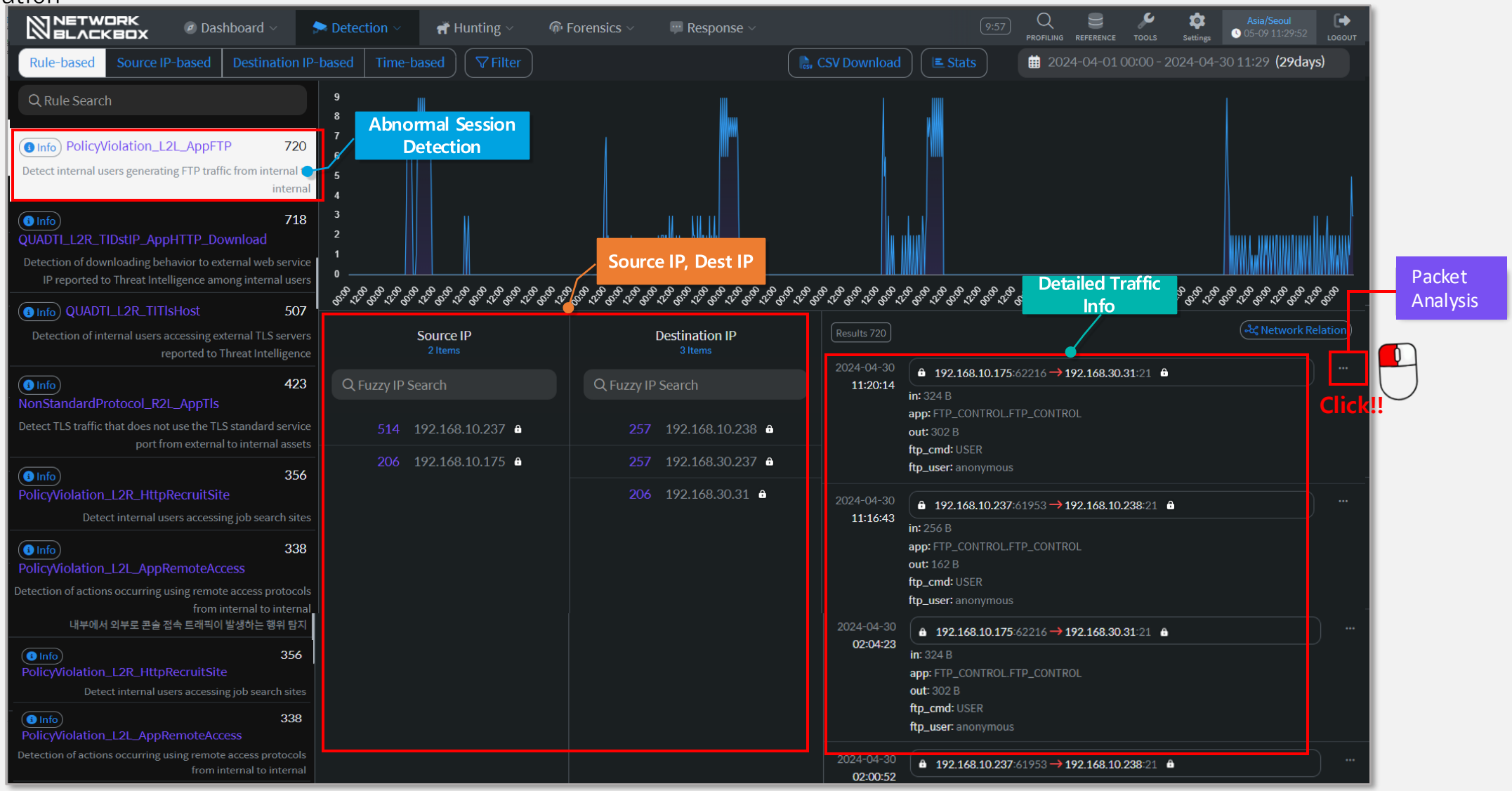
Menu : Detection → Threat Detection → Packet Analysis → VIEW



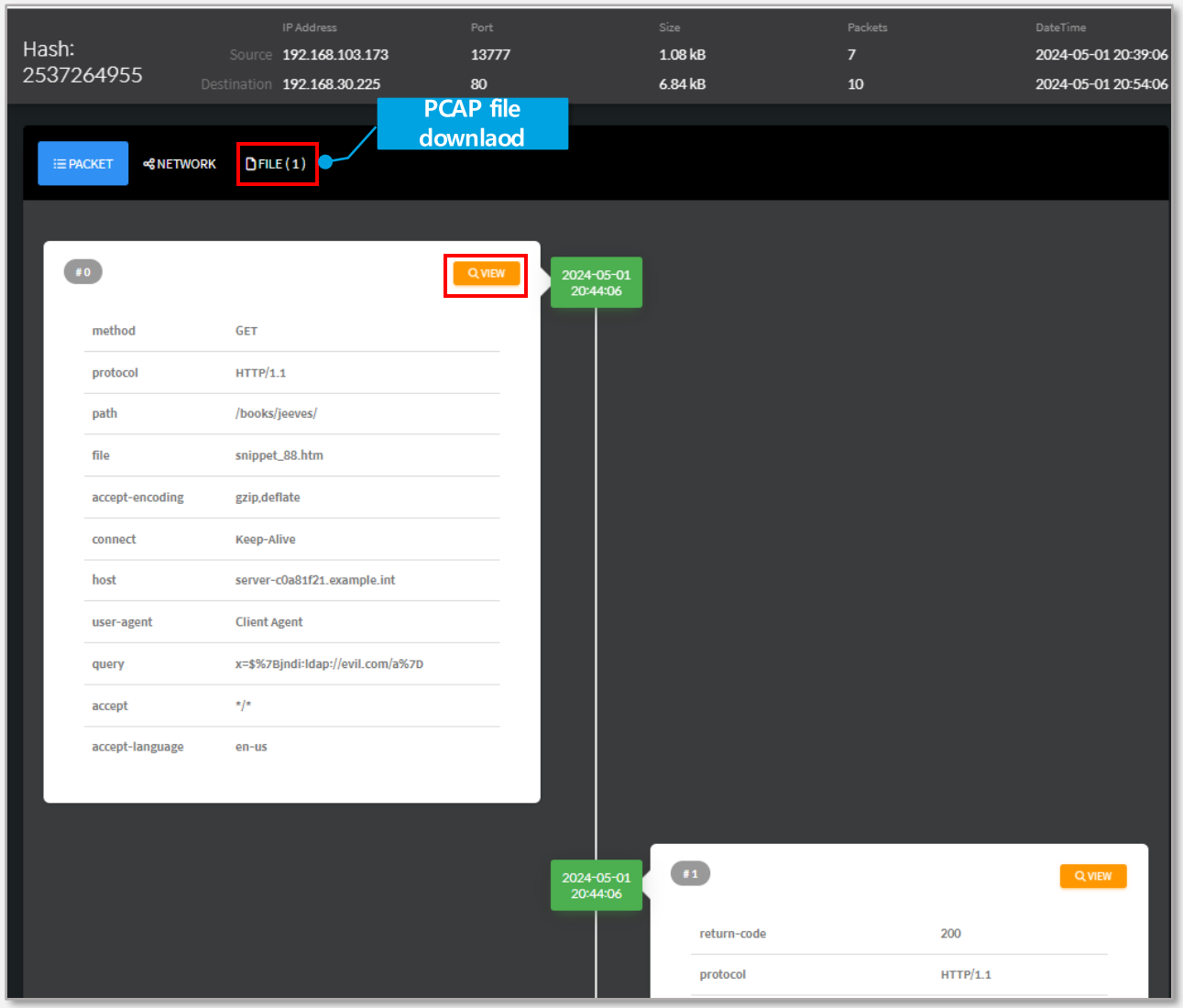
PCAP Download

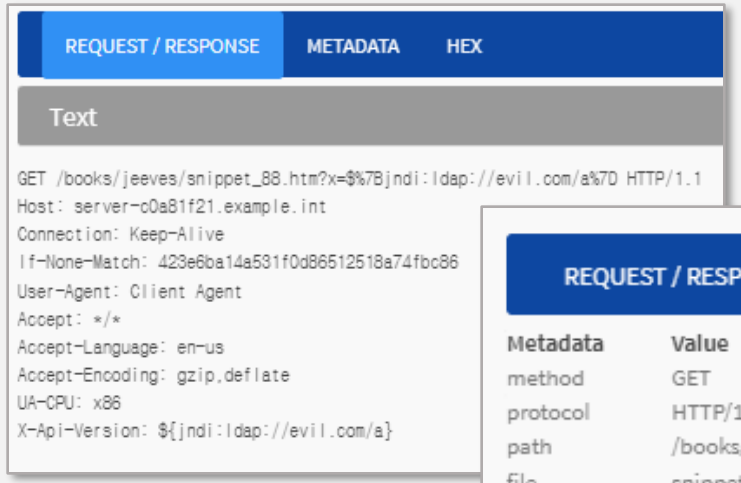
Network Blackbox- Detection

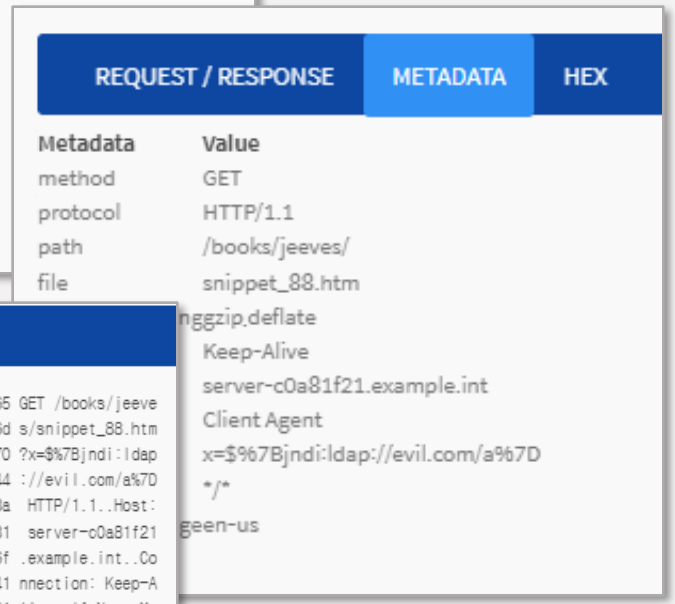
Abnormal Session Detection: Detects approximately 190 abnormal sessions and provides the ability to create custom rules tailored to the client's situation

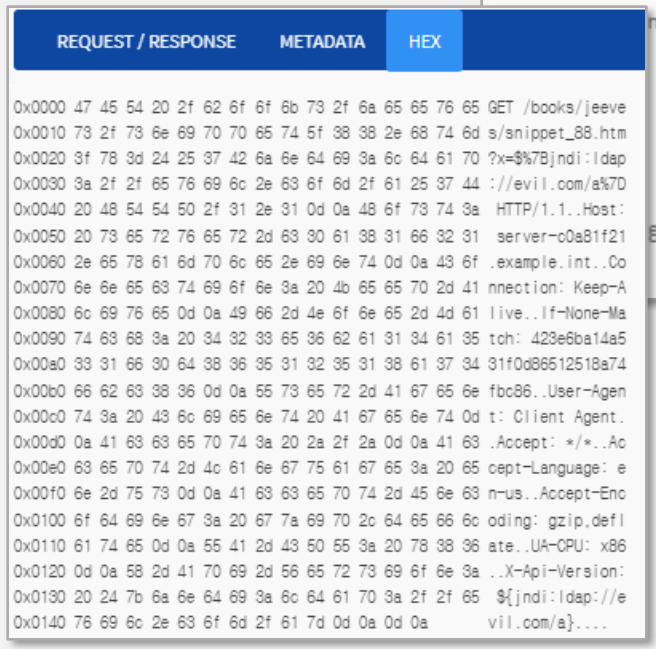


Network Blackbox- Detection



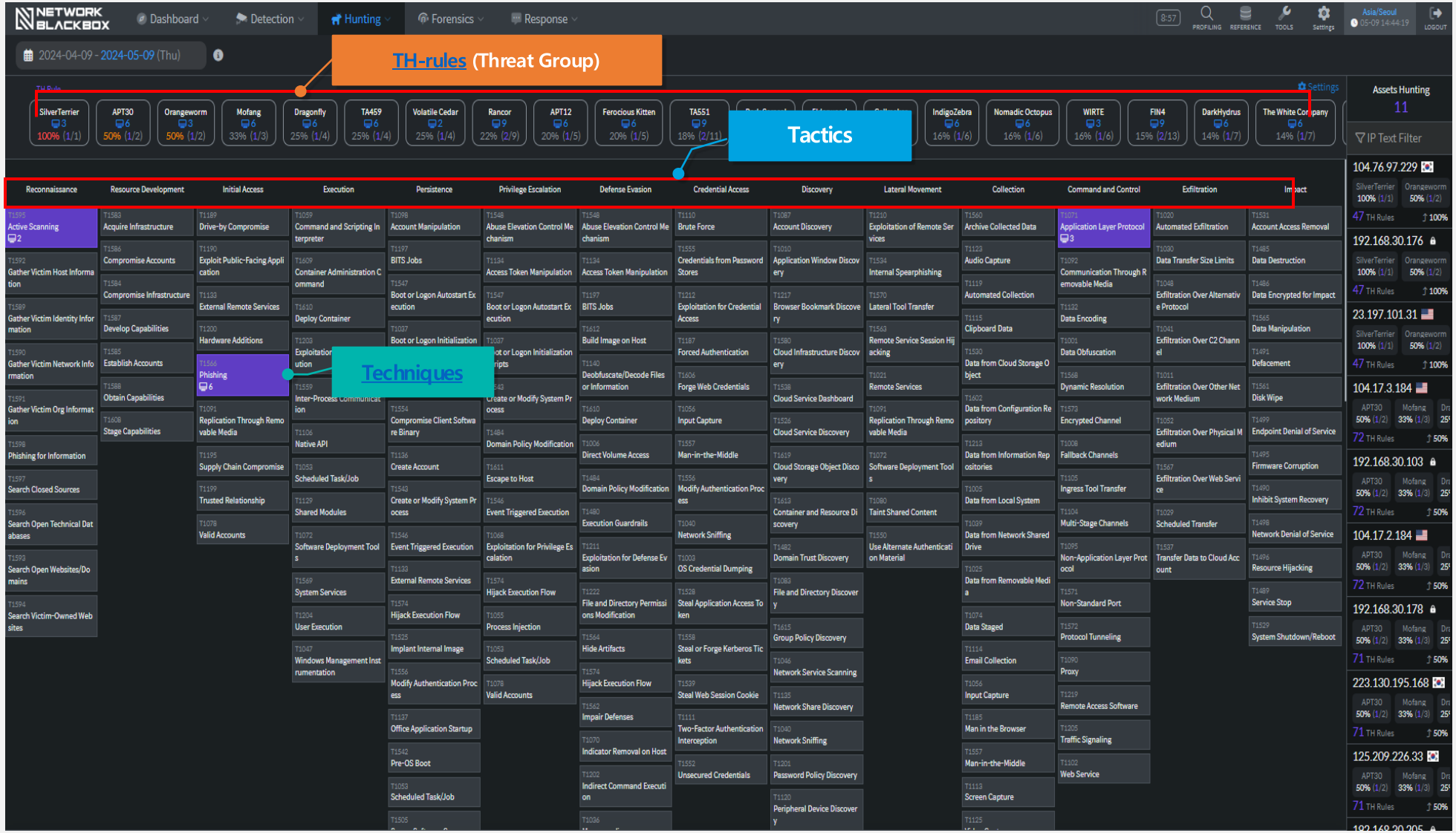






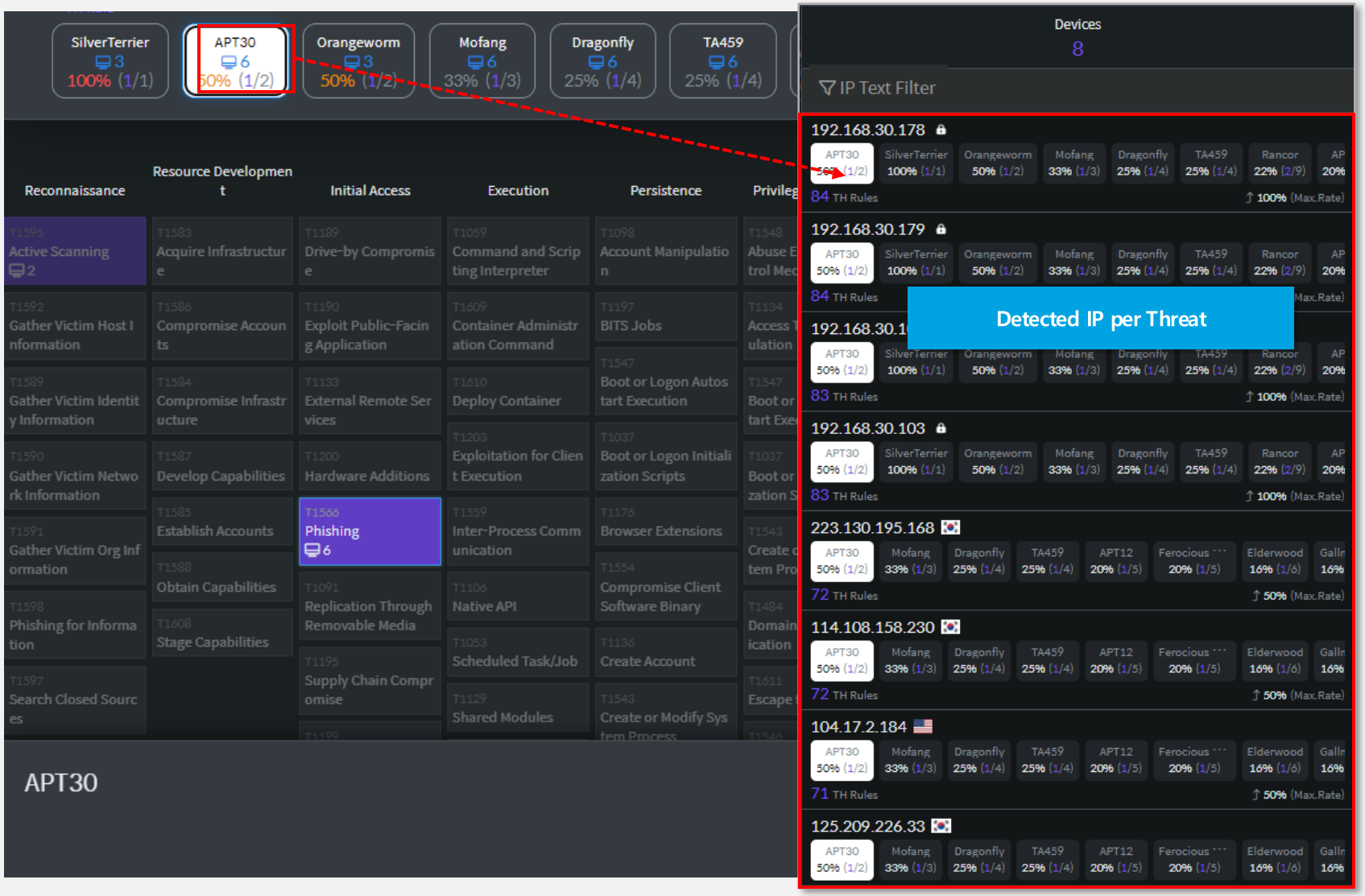
Network Blackbox- Hunting

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.



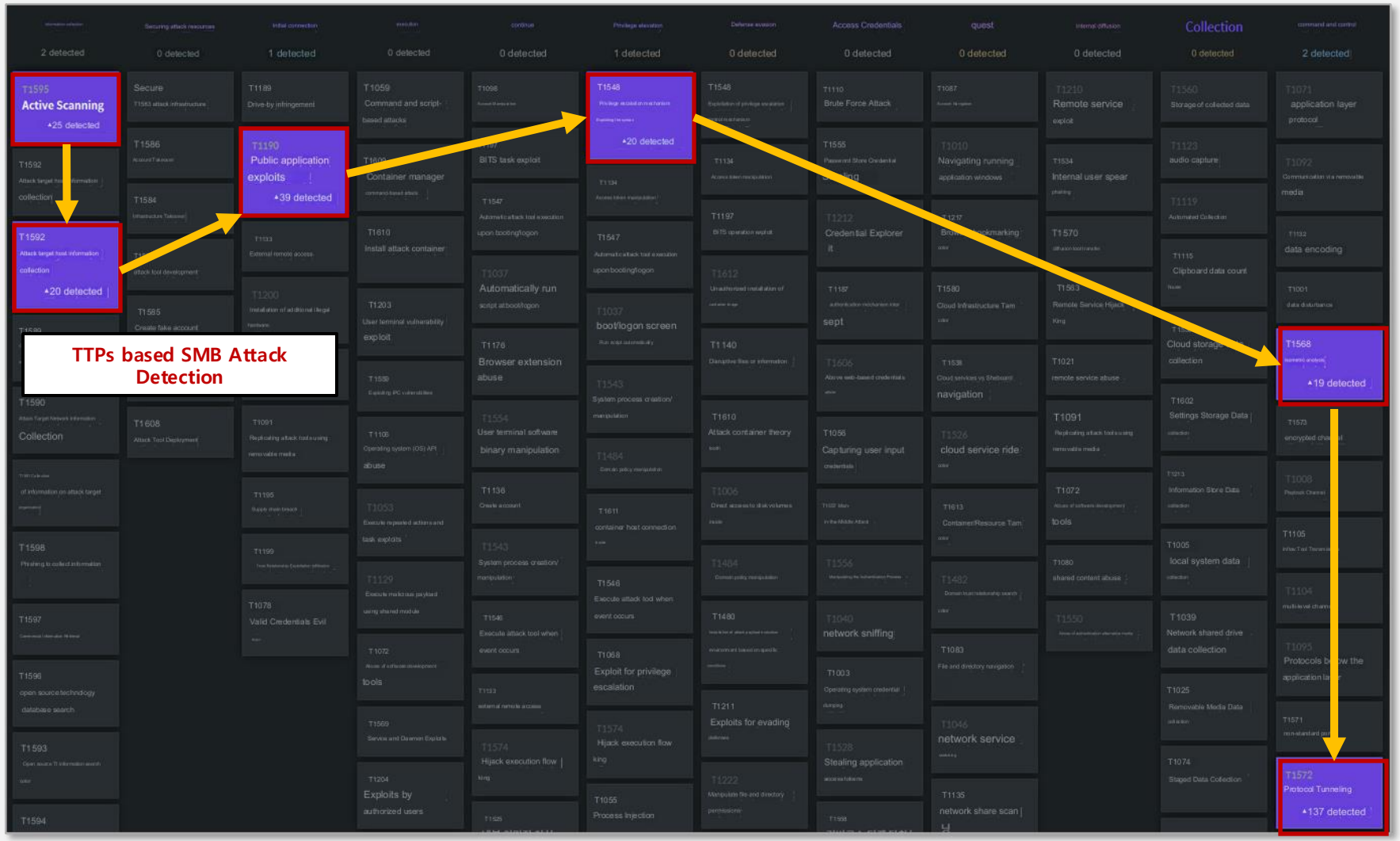
Network Blackbox- Hunting

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

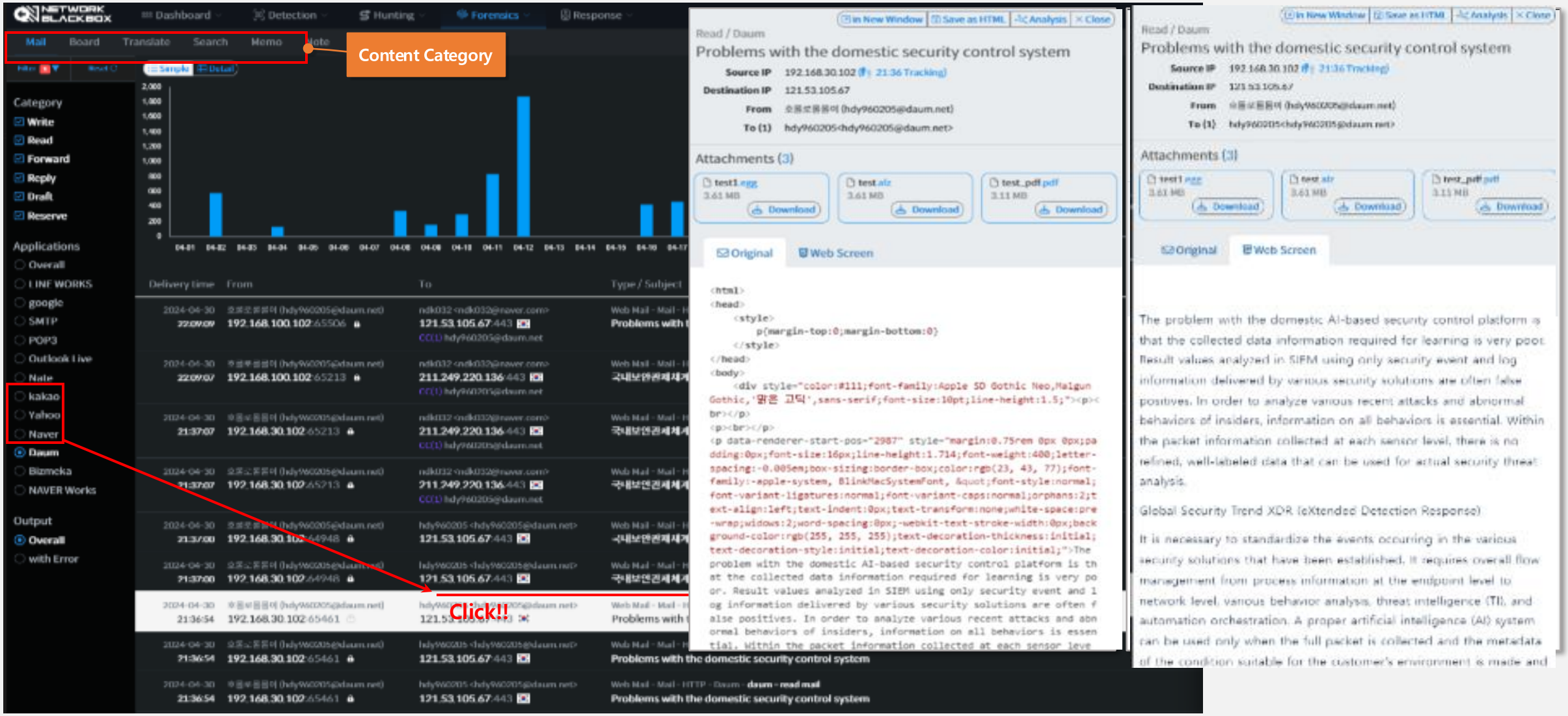
After observing real cyber attack cases, analyze the attack methods and techniques used by attackers from a malicious behavior and technical perspective.



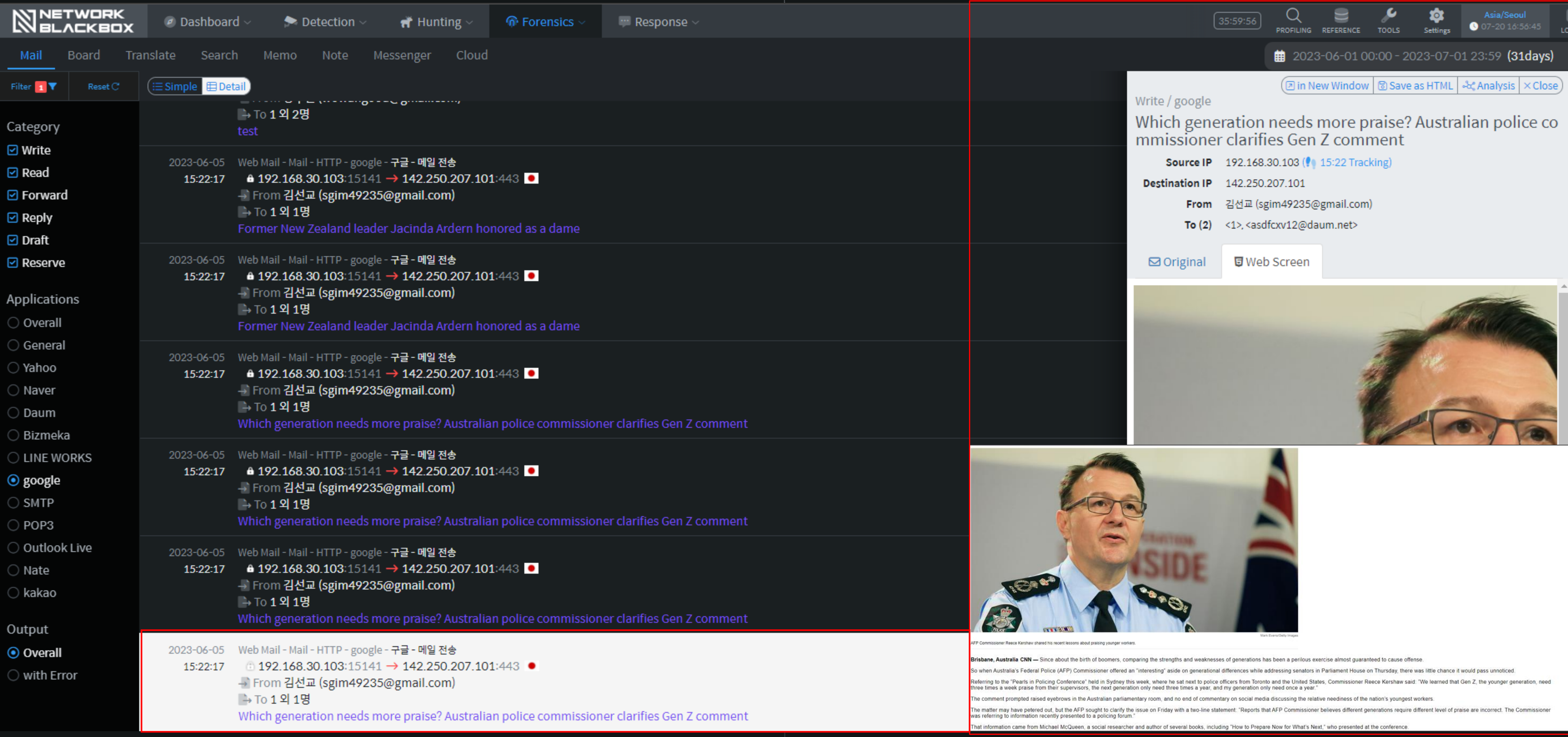
- Through the MITRE ATT&CK analysis feature, security personnel analyze what tools and tactics, techniques, and procedures (TTPs) attackers used.
- Using the MITRE ATT&CK Matrix, security personnel can accurately understand the threats that have occurred and provide faster responses than before.
- This 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.

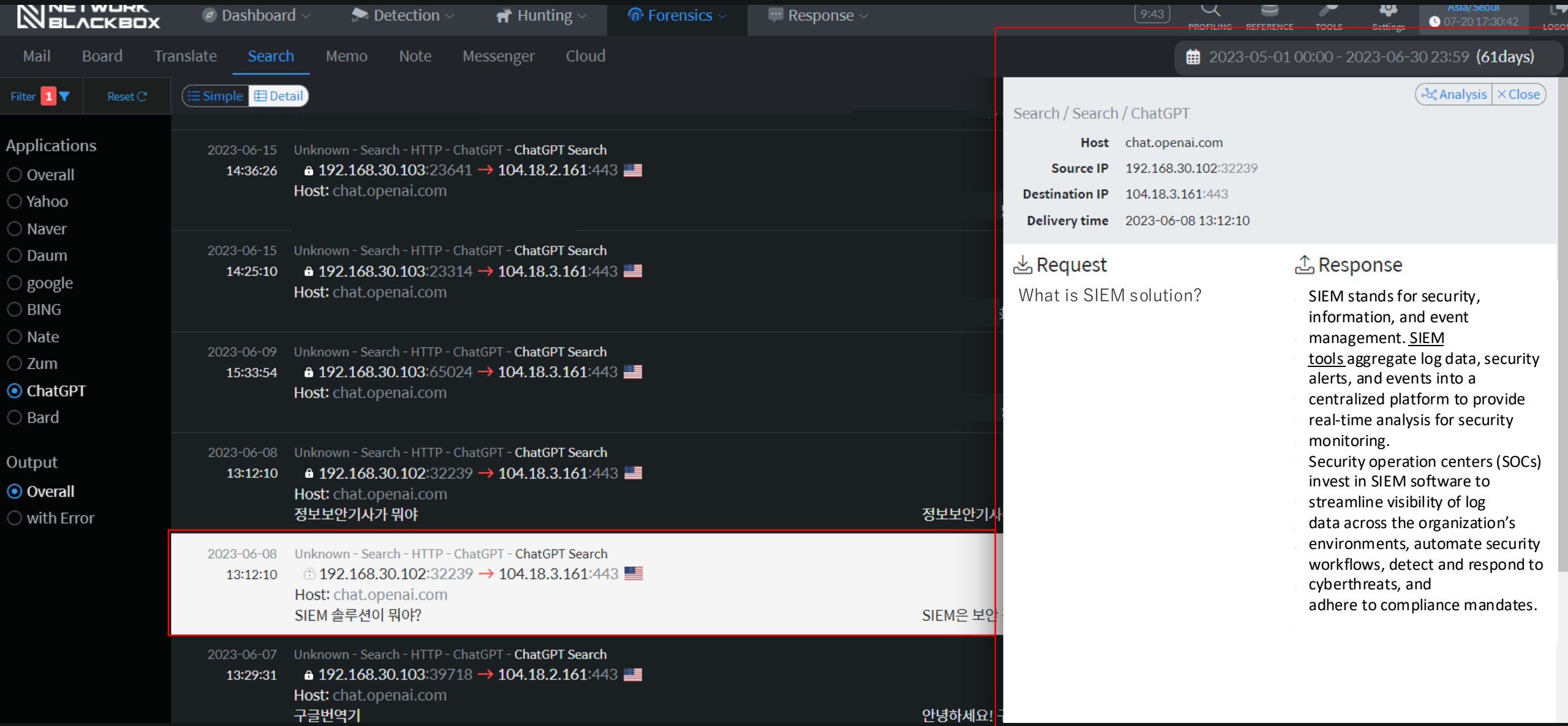


Forensic : Contents Search - Gmail



Network Blackbox- Forensic

Network Blackbox- Forensic



Forensic : File Extraction

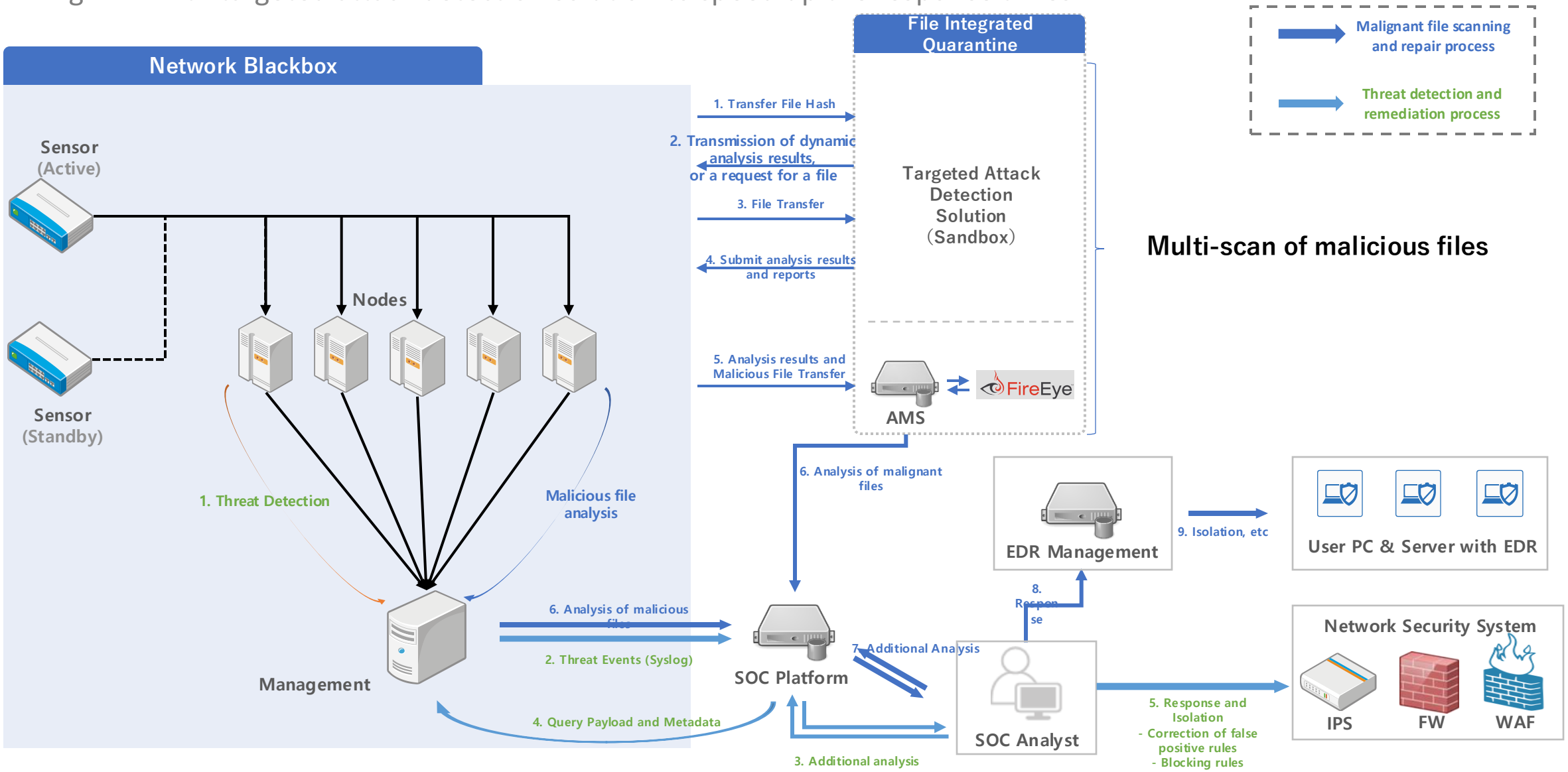
Simple | Detail

Results 152

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

Network Blackbox- Response (3rd-party Integration)

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

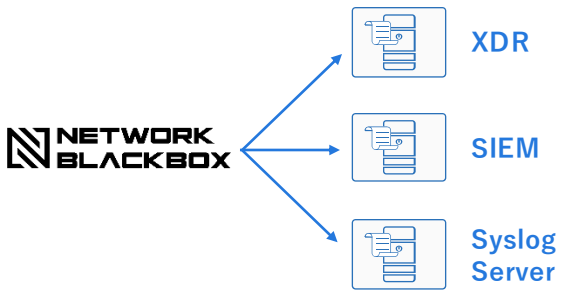


Response : Actionable Response

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

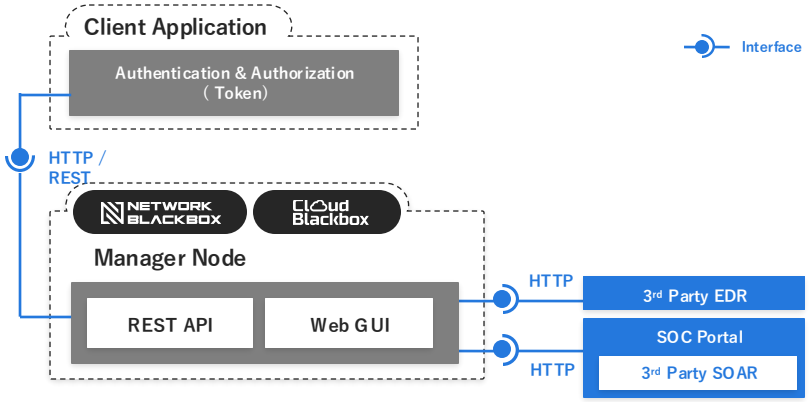
1 Network Blackbox Syslog

- 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



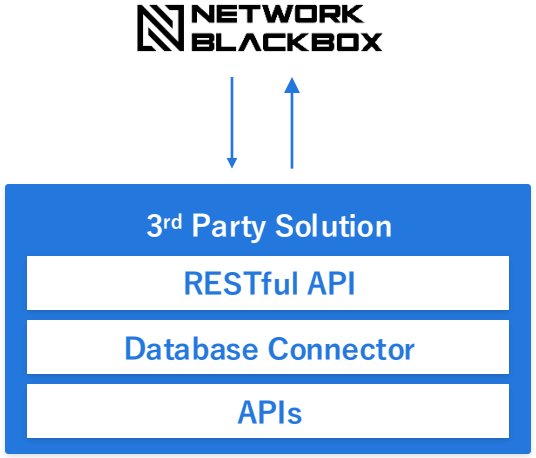
2 Network Blackbox RESTful API

- 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

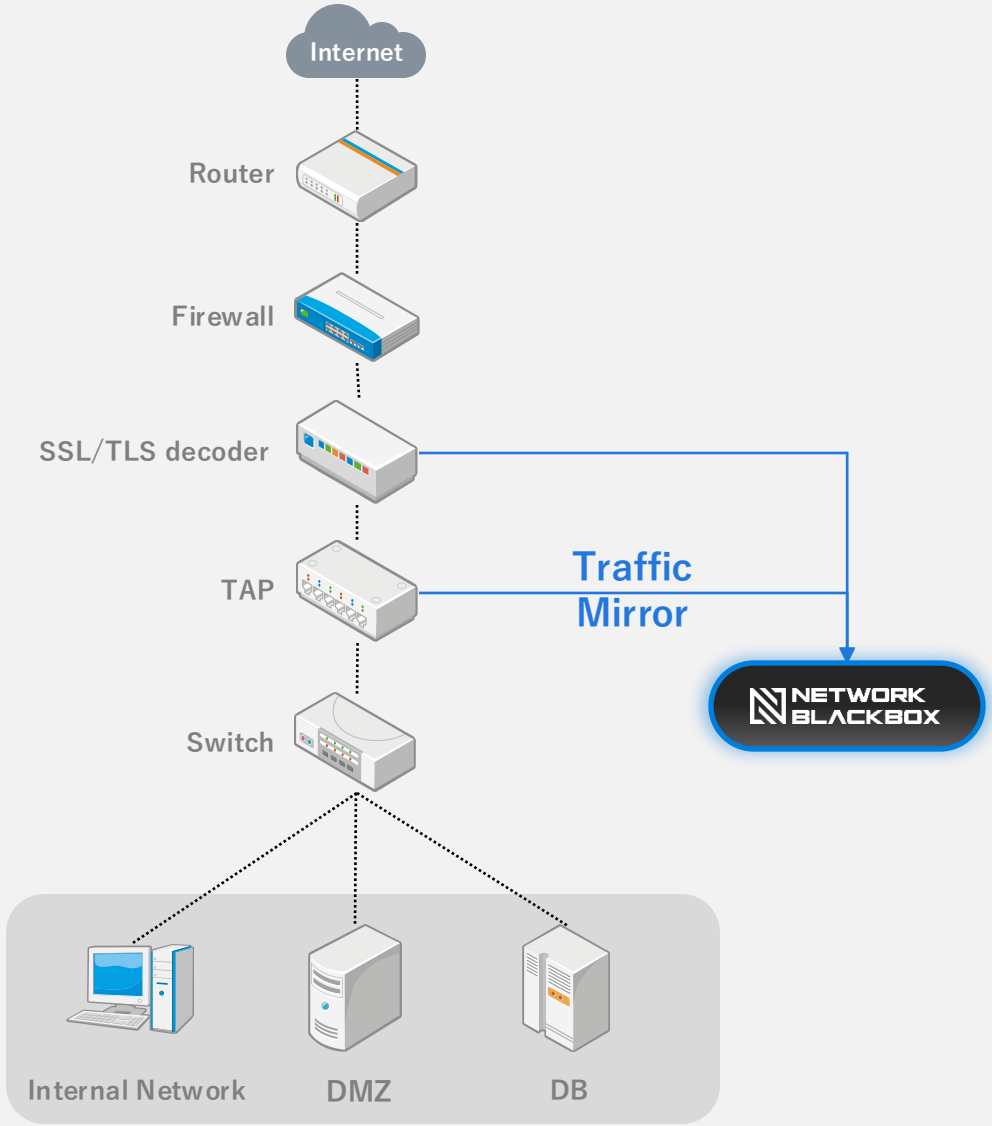


3 3rd party RESTful API

- 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



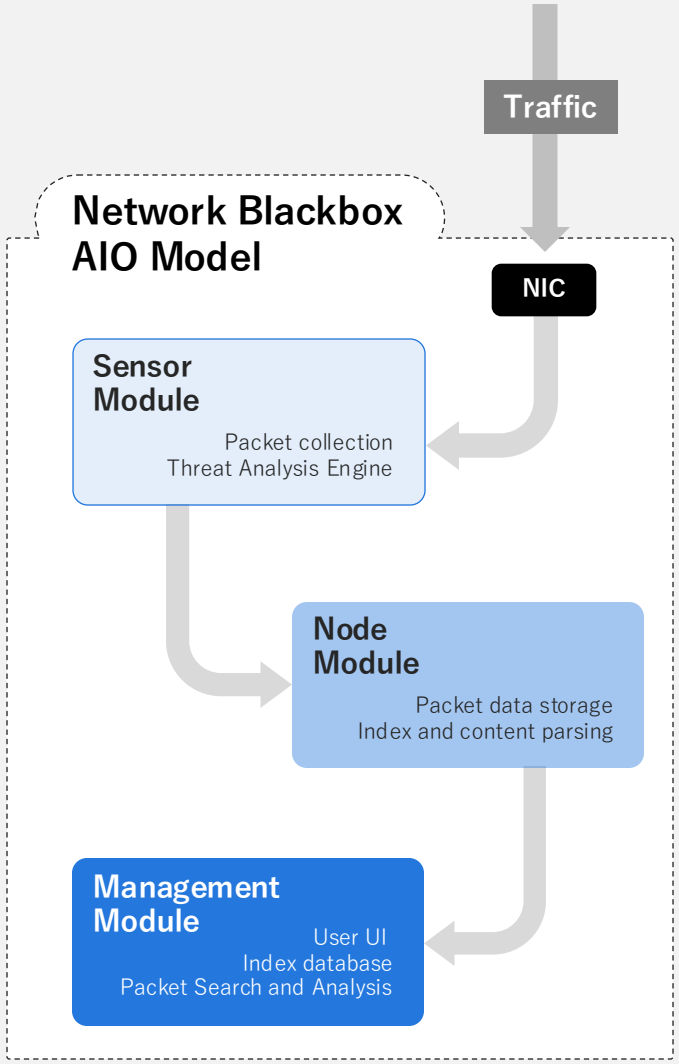
Quick deployment / No effect on system

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

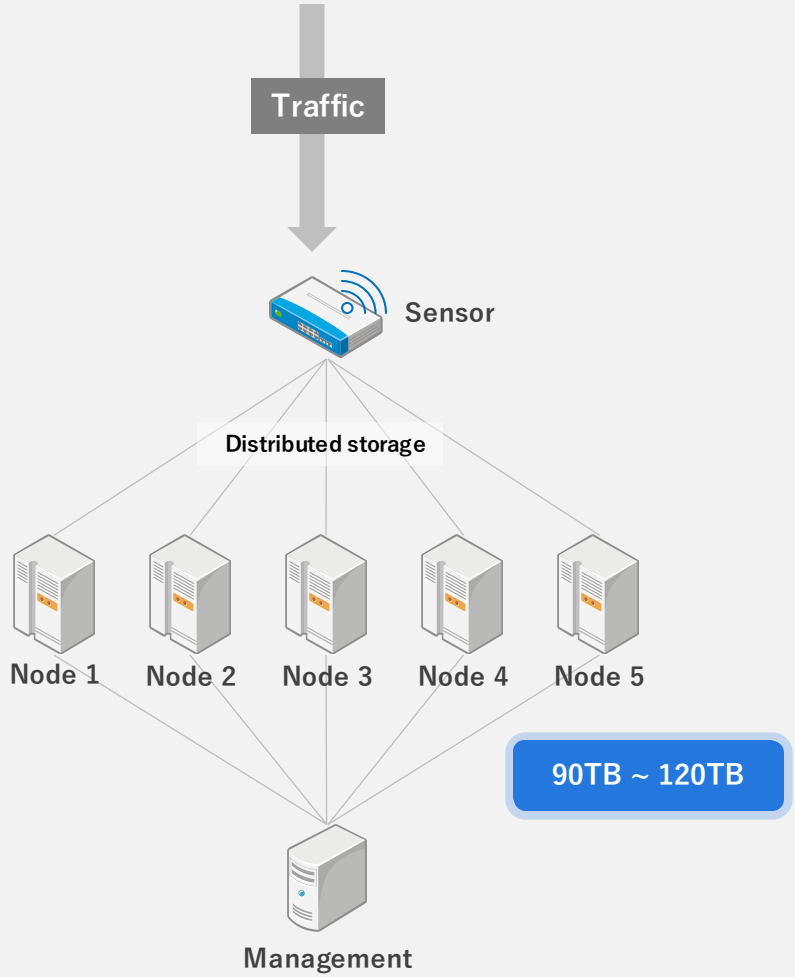
Decryption Proxy Device Integration

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

Architecture



All In One

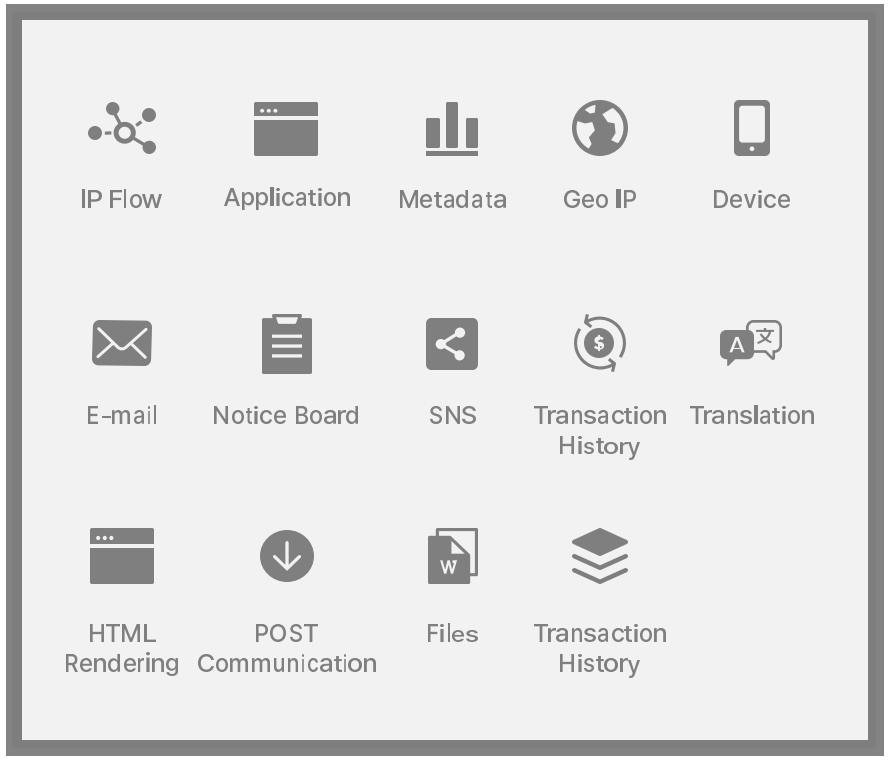


Expanded

Quad Miners vs Other NDRs

Why Quad Miners use Full Packet for its NDR

Quad Miners



Full Packet (Flow data & Metadata + Payload)

VS

Other NDRs

Flow data & Metadata

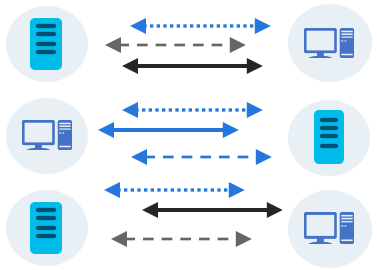
The need for next-generation AI network security technology

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

Collection & Analysis of Full Packet Data



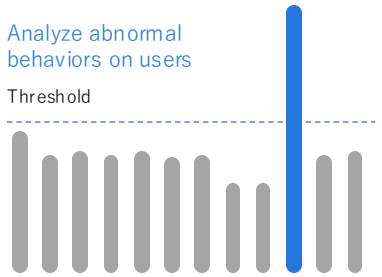
Full Packet

Create a Baseline for Normal Behavior

~100 Security Events		
Number of concurrent flows	New flows created	Number of SYNs received
Packet per second	Number of SYNs sent	Rate of connection resets
Bits per second	Time of day	Duration of the flow

Improvement of learning accuracy based on supervised learning and generation of criteria suitable for customer environment

Alerts for Abnormal Signs and Behavior Changes



Internal -> External Behavior

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	SIEM	Flow-based NTA
Generate events	Limited Correlation Analysis	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

NETWORK BLACKBOX

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 fine 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)

- Ministry of National Defense
- Army
- Air Force
- ROKMC
- Navy
- Defense Acquisition Program Administration
- 정보사령부
- 777사령부
- 사이버사령부
- 군인공제회
- 국방과학연구소 Agency for Defense Development
- 작전사령부

Financial Group (16)

- NongHyup Bank
- NATIONAL AGRICULTURAL COOPERATIVE FEDERATION
- Shinhan Bank
- MG Korean Federation of Community Credit Cooperatives
- KDB Bank
- KB Kookmin Card
- KB Securities
- Hana Financial Group
- KEB Hana Bank
- KEB Hana Card
- Hana Securities
- Hana Capital
- ana Life
- Hana Insurance
- Hanna Savings Bank

Public (19)

- KNPA KOREAN NATIONAL POLICE AGENCY
- GYEONGGI NAMBU POLICE AGENCY
- GRAC Game Rating and Administration Committee
- 문화체육관광부 Ministry of Culture, Sports and Tourism
- GYEONGGI-DO
- 경기도소방재난본부 GYEONGGI-DO FIRE SERVICES
- 중앙선거관리위원회
- KFE 한국핵융합에너지연구원 KOREA INSTITUTE OF FUSION ENERGY
- NRC 경제·인문사회연구회 National Research Council for Economics, Humanities and Social Sciences
- 서울호서직업전문학교 SEOUL HOSEO OCCUPATIONAL COLLEGE
- KRICT Korea Research Institute of Chemical Technology
- HF KOREA HOUSING-FINANCE CORPORATION
- KSD 한국예탁결제원
- 한국생명공학연구원 Korea Research Institute of Bioscience and Biotechnology
- 영남이공대학교 Yeungnam University College
- ULLEUNG-GUN
- KAC KOREA AIRPORTS CORPORATION
- KOICA
- K water

Global / Enterprise (22)

- SAMSUNG
- kakao
- STARBUCKS
- coupang
- neople
- coway
- GS Caltex
- GOLFZON
- ASIANA IDT
- LG Energy Solution
- DONGSUH
- 금호석유화학
- XLGAMES
- korbit
- 연세대학교 의료원
- MALAYSIA
- S-1
- INDONESIA
- SK telecom
- SK hynix
- SK C&C
- Homeplus

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.	**Metadata** provides information about the structure and flow of network traffic but **doesn't include the actual content within the packets.**
Payload Analysis	Examining the actual data within the packets, such as application-layer content (e.g., HTTP requests, email contents, file transfers).	**Metadata doesn't contain the application data being transmitted.** 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.	**Metadata** can show when and where communication occurred, but it **can't provide the specific content of the communication.**
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).	**Metadata** lacks the actual data content, so it **cannot filter or scan for specific words or patterns within the transmitted data.**