PASCON 2024
2024 공공 · 금융 · 기업 정보보안&개인정보보호 컨퍼런스

Threat Intelligence를 이용한 Threat Hunting

강민석
kaspersky

kaspersky

진화하고 있는 위협

Advanced persistent threat landscape in 2020

Kaspersky's Global Research and Analysis Team (GReAT) is well-known for the discovery and dissemination of the most advanced cyberthreats.

According to their data, in 2020 the top targets for advanced persistent threats (APT) were governments, and the most significant threat actor was Lazarus.

Top 10 targets:

- Government
- Banks
- Financial Institutions
- Diplomatic
- Telecommunications
- Educational
- Defense
- Energy
- Military
- IT companies

Top 12 targeted countries:

Top 10 significant threat actors:

1. Lazarus
2. DeathStalker
3. CactusPete
4. IAmTheKing
5. TransparentTribe
6. StrongPity
7. Sofacy
8. CoughingDown
9. MuddyWater
10. SixLittleMonkeys

apt.securelist.com

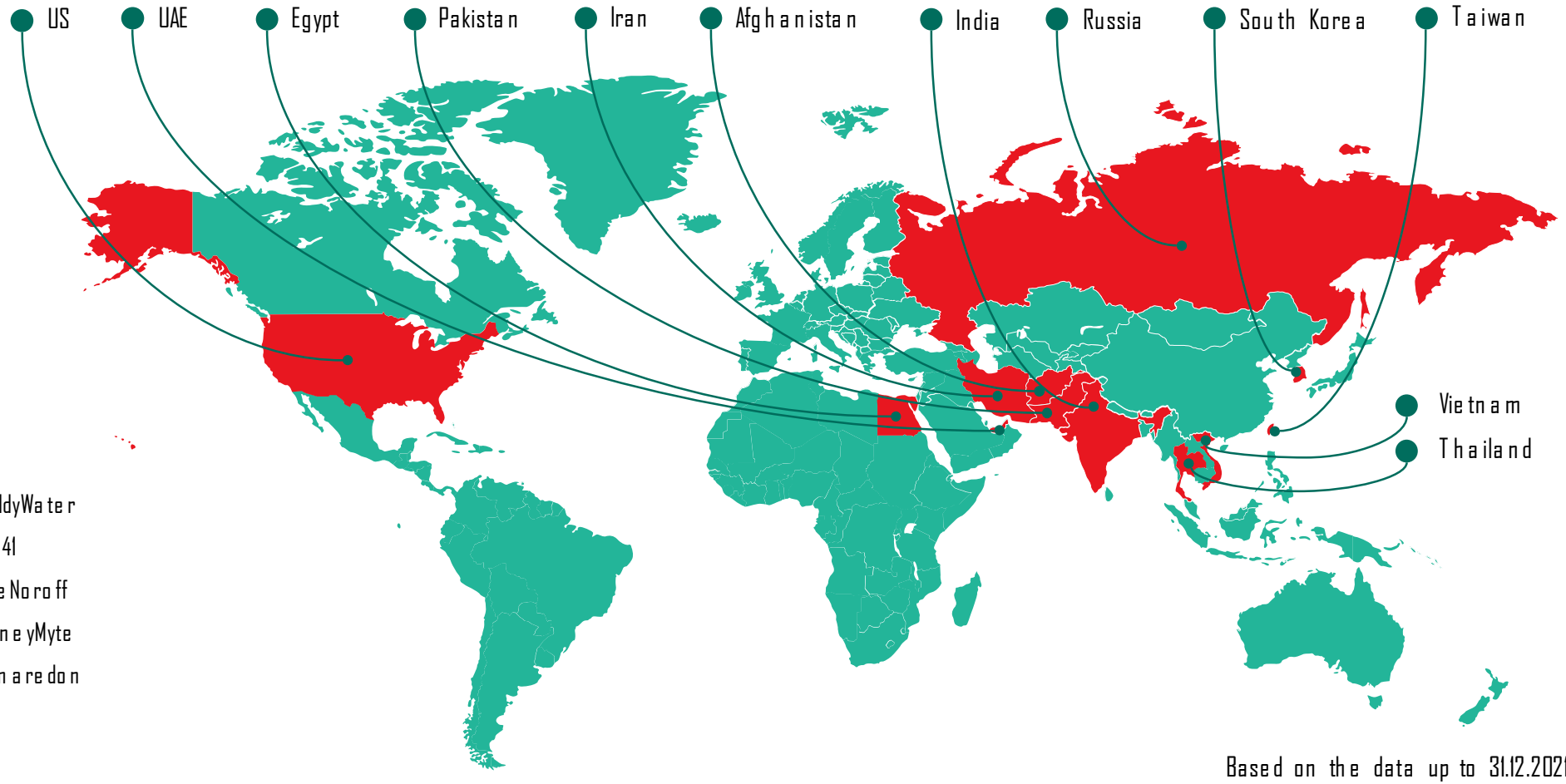
Advanced persistent threat landscape in 2021

Kaspersky's Global Research and Analysis Team (GReAT) is well-known for the discovery and dissemination of the most advanced cyberthreats.
According to their data, in 2021 the top targets for advanced persistent threats (APT) were governments, and the most significant threat actor was Lazarus.

Top 10 targets:

- Government
- Diplomatic
- Telecommunications
- Military
- Defense
- IT companies
- Educational
- Civil Aviation
- Logistics
- Pharmaceutical

Top 12 targeted countries:



Top 10 significant threat actors:

1. Lazarus
2. DarkHalo
3. CloudComputating
4. Turla
5. SideCopy
6. MuddyWater
7. APT41
8. BlueNoroff
9. HoneyMyte
10. Gamaredon

apt.securelist.com

Based on the data up to 31.12.2021

Advanced persistent threat landscape in 2022

Kaspersky's Global Research and Analysis Team (GReAT) is well-known for the discovery and dissemination of the mo st advanced cyberthreats.

According to their data, in 2022 the top targets for ad vanced persistent threats (APT) were governments, an d the most significant threat actor was Lazarus.

Top 10 targets

- Government
- Military Dipl
- omatic
- IT companies
- Educational
- Telecommunications
- Media
- Software Development
- Manufacturing Logistic
- s

Top 10 significant threat actors

1. Lazarus
2. APT10
3. Kimsuky
4. ZexCone
5. Tomiris
6. Ghostwriter
7. DeathStalker
8. BitterAPT
9. SideCopy
10. Gelsemium

Top 12 targeted countries/territories

Based on the data up to 31.12.2022

apt.securelist.com

Advanced persistent threat landscape in 2023

카스퍼스키의 글로벌 연구 및 분석 팀(GReAT)은 가장 진보된 사이버 위협을 발견하고 분석하는 것으로 잘 알려져 있습니다. 2023년 지능형 지속 위협(APT)의 최대 표적은 정부였으며 가장 중요한 위협 행위자는 Lazarus 였습니다.

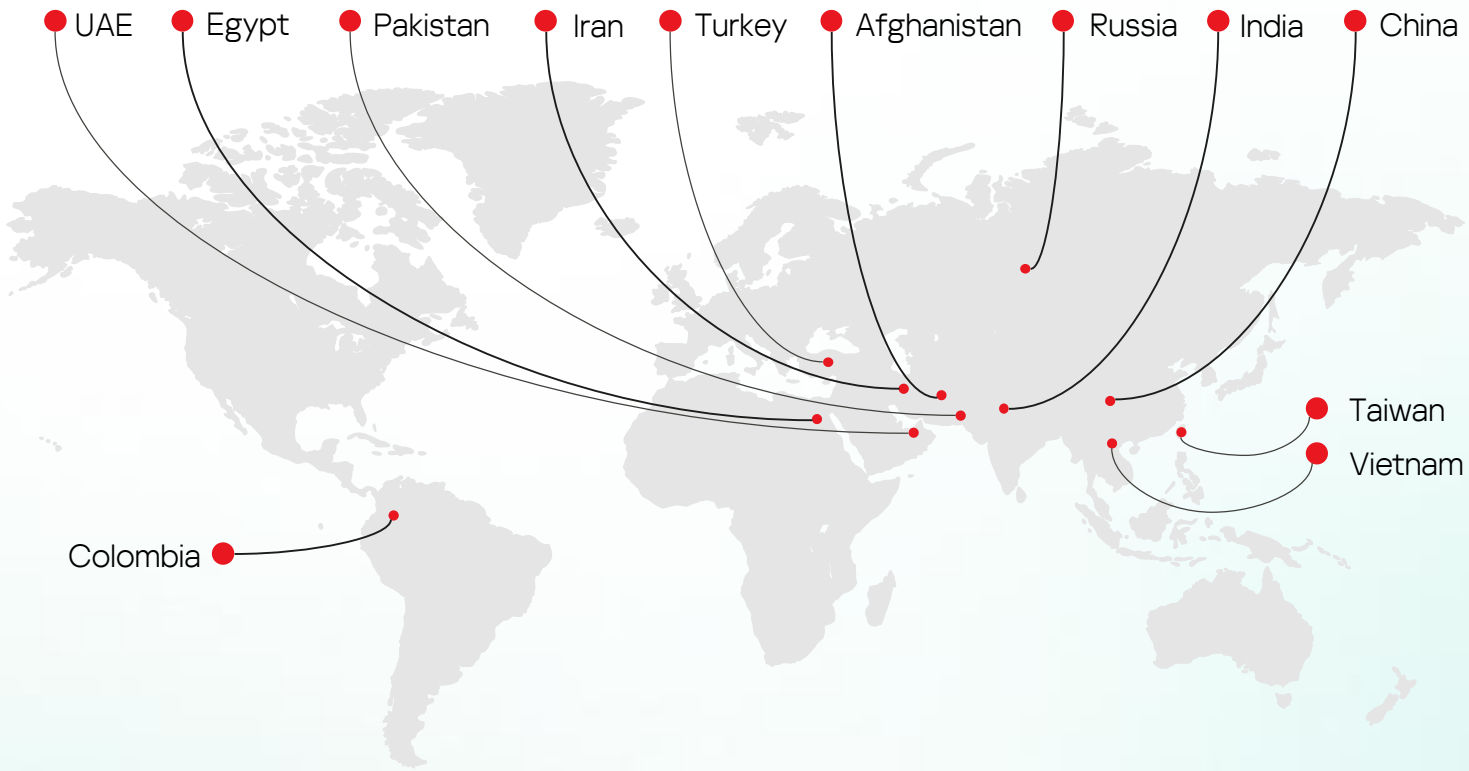
Top 10 targets

- Government
- Military
- Diplomatic
- IT companies
- Energy
- Telecommunications
- Cryptocurrency
- Industrial
- Manufacturing
- Technology Research

Top 10 significant threat actors

1. Lazarus
2. APT10
3. Kimsuky
4. ZexCone
5. Tomiris
6. Ghostwriter
7. DeathStalker
8. BitterAPT
9. SideCopy
10. Gelsemium

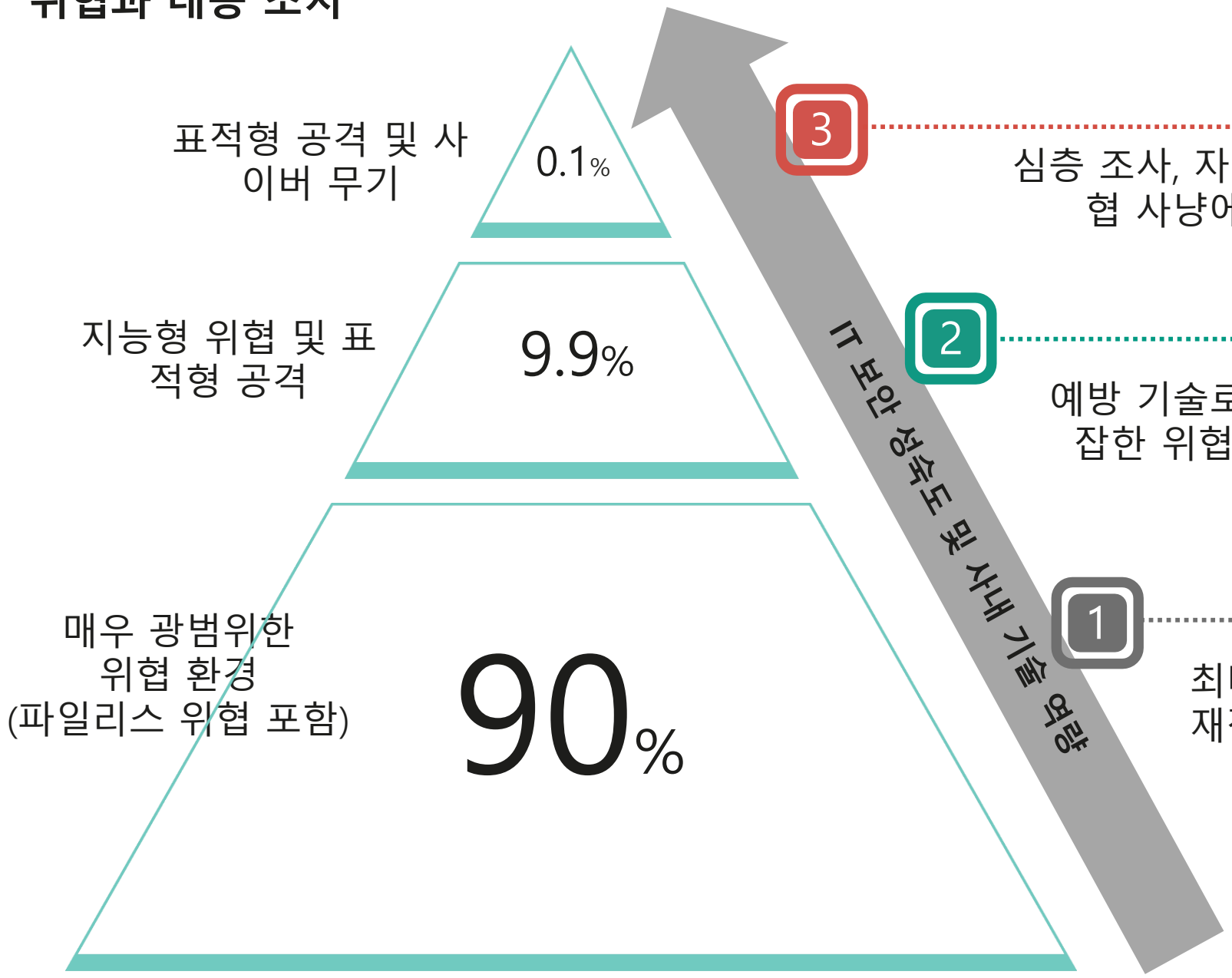
상위 12개 대상 국가 및 지역



apt.securelist.com

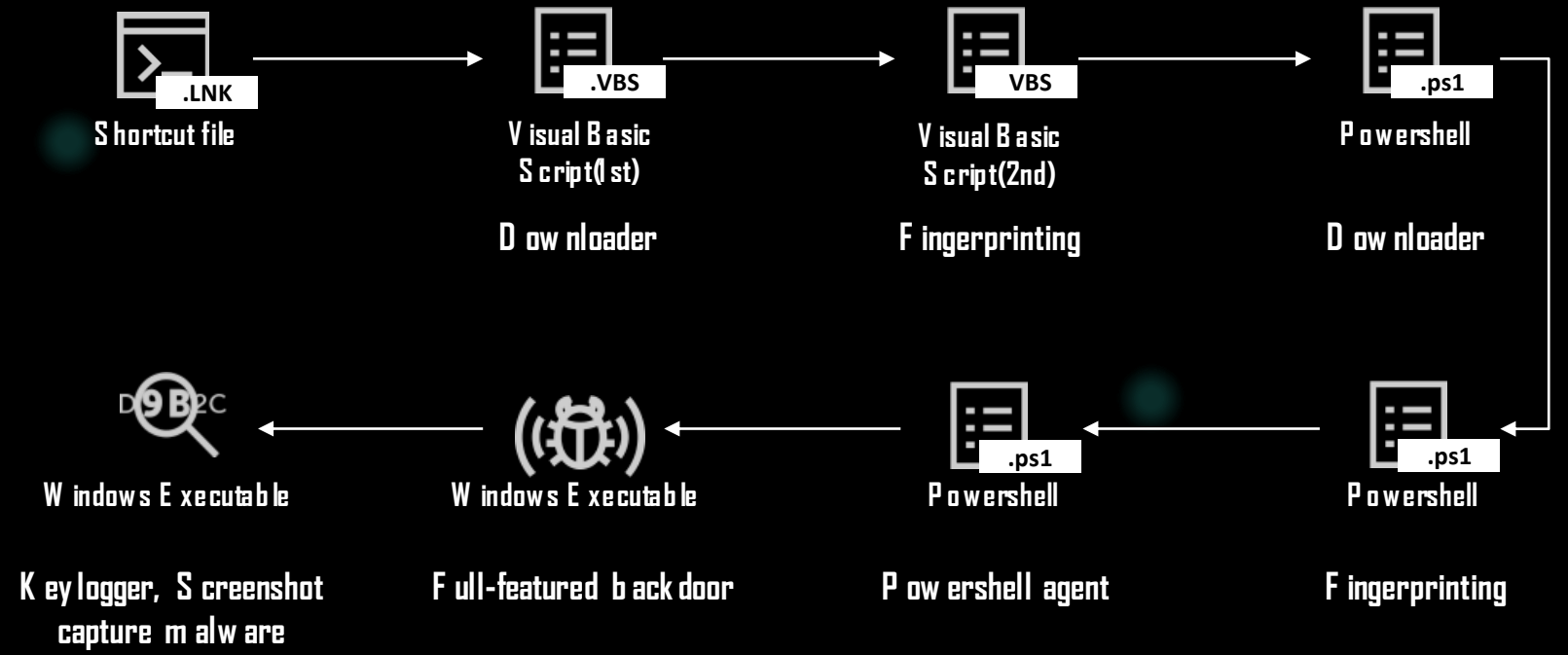
Based on the data up to 31.12.2023

위협과 대응 조치

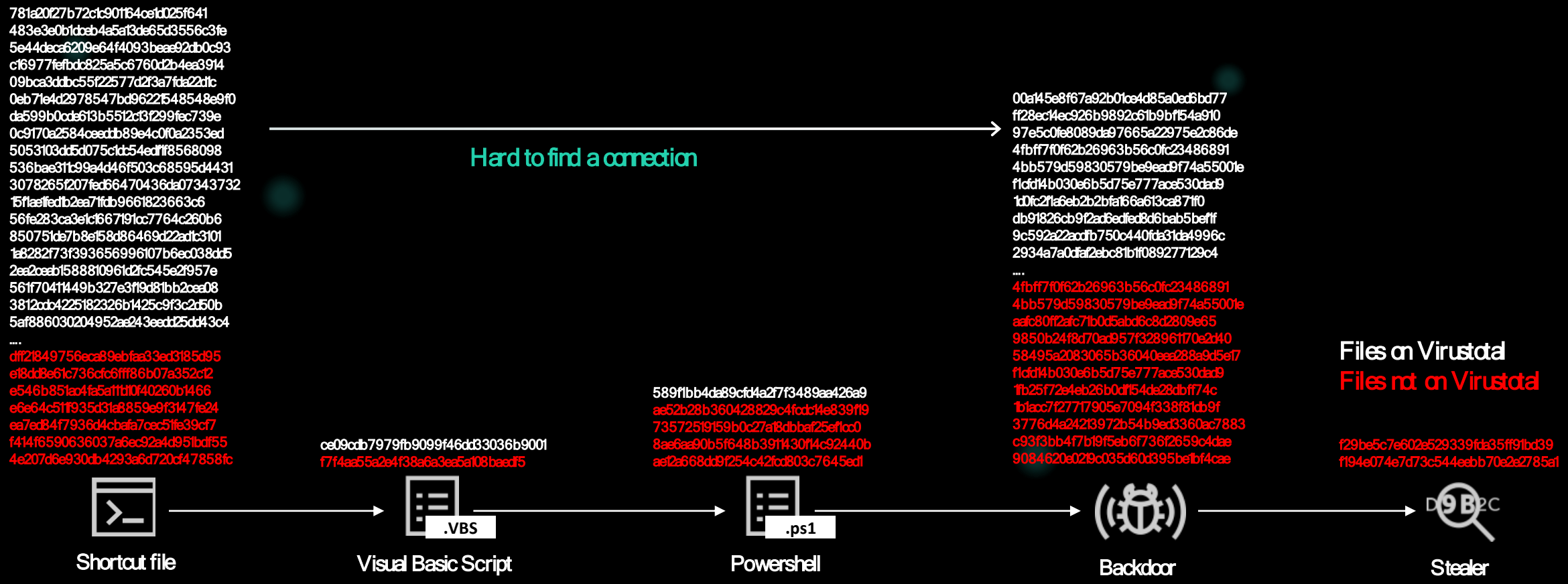

표적형 공격 및 사이버 무기
0.1%
지능형 위협 및 표적형 공격
9.9%
매우 광범위한 위협 환경 (파일리스 위협 포함)
90%
IT 보안 성숙도 및 사내 기술 역량
3
심층 조사, 자동/수동 위협 사냥에 주력
통합 사이버 보안 접근 방식
전문 지식을 완벽히 갖춤
2
예방 기술로 막지 못하는 복잡한 위협의 대응에 주력
첨단 방어
IT 보안 전문가 팀의 역량 발전 진행 중
1
최대한 많은 수의 잠재적 위협 요소 차단에 주력
보안의 토대
IT 부서만 있거나 IT 보안 전문 지식 부족

Latest Threat Landscape: Multi-stage infection

BlueNoroff's SnatchCrypto campaign



Important points we consider: Full-context understanding



Low visibility

kaspersky

GREAT

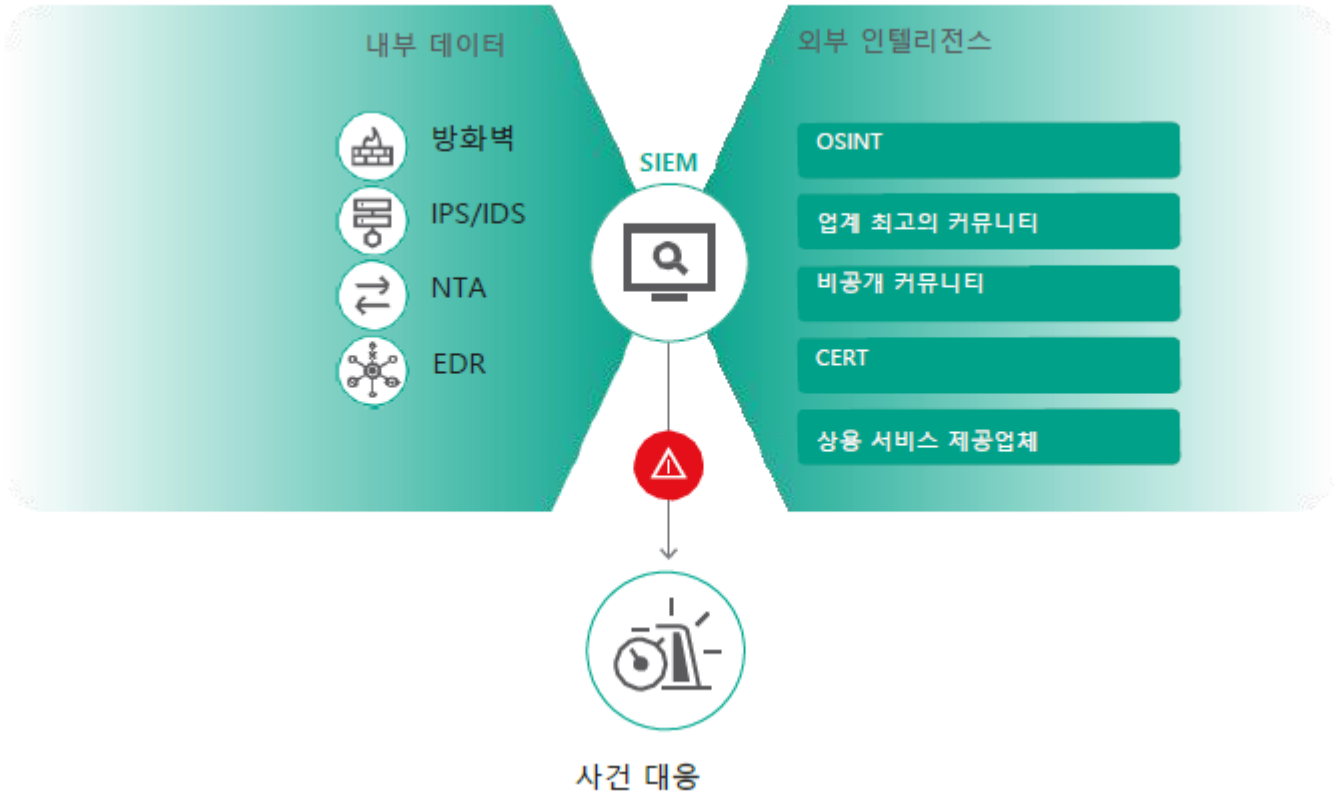
Important points we consider: Full-context understanding

	Initial Access	Execution	Persistence	Priv Escalation	Defense Evasion	Credential Access	Discovery	Lateral movement	Command & control	Exfiltration
Conti	Phishing Exploit server Stolen RDP	Cobalt Strike Powershell Metasploit	Valid account	Cobalt strike	Legit tools AV remover	ProcDump Mimikatz NTDS.dit dump Ntdsutil	Windows cmd Adfind IP scanner	SMB PSExec RDP Anydesk	Anydesk Cobalt strike	Rcolne Mega.io
DarkSide	Phishing External remote access	PsExec Cobalt Strike SystemBC	GPO Schedule task		Legit tools (PCHunter, GMER)		ADRecon ADFind Netscan IP Scanner	PSExec RDP SSH	Plink Anydesk Cobalt strike	Mega.io Putty Rcolne 7zip
Ryuk		Cobalt Strike		Zerologon vulnerability		Rubeus	Adfind Windows cmd	SMB RDP		FTP

kaspersky

Threat Intelligence 란?

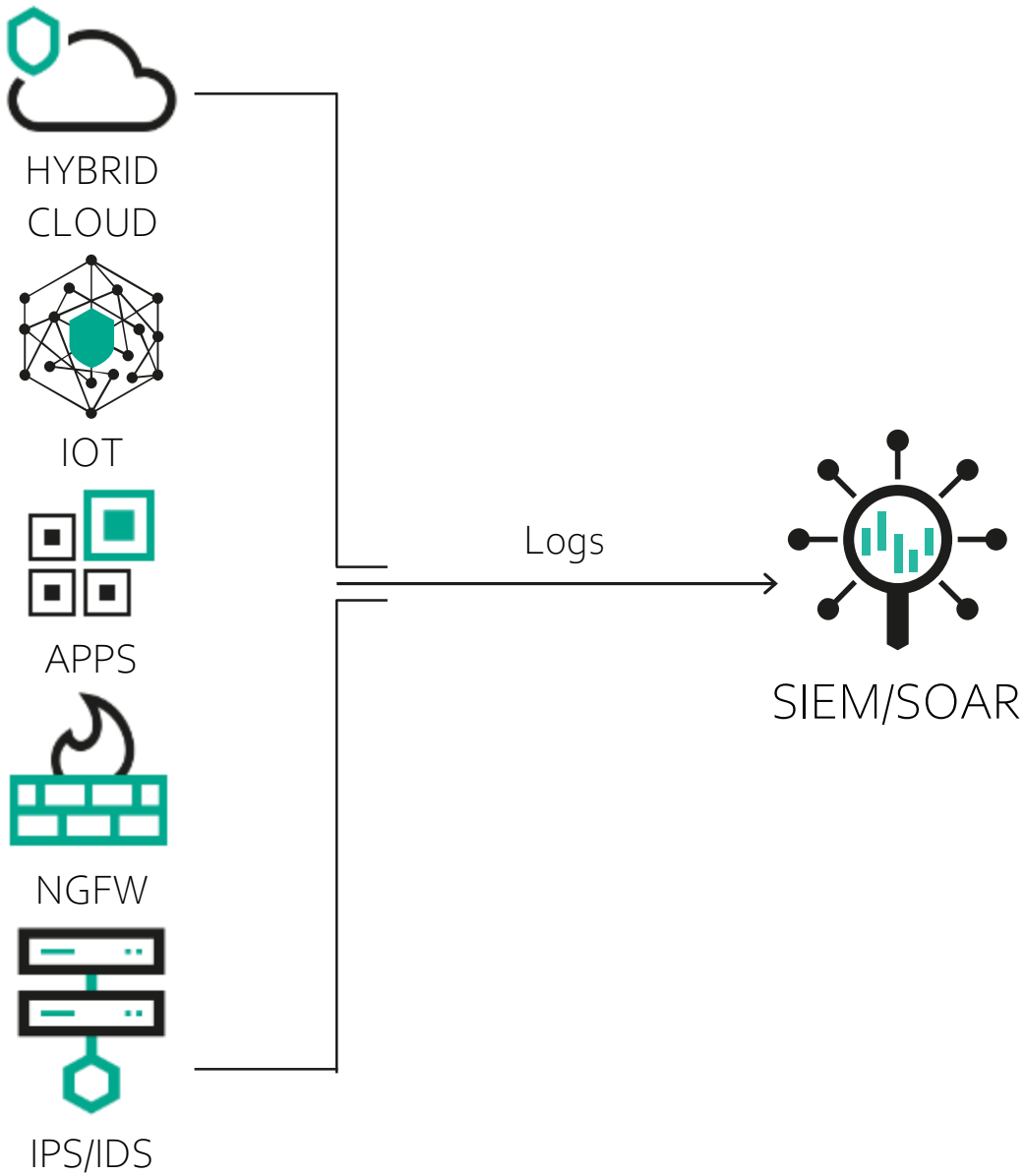
SOC & SIEM



SOC (Security Operation Center
사이버상에서 발생하는 이상 현상을 사전에 탐색하고 침해 사고를 대응하는 조직

SIEM(Security Information and Event Management)
보안 정보 및 이벤트 관리를 의미하며 조직에 차세대 탐지, 분석 및 대응 방안을 제공

진화하고 있는 사이버보안 과제



수많은 보안 기술로부터 오는 보안 알람들의
우선 순위 구분의 어려움

분석가들의 번아웃으로 인해 이직률 증가

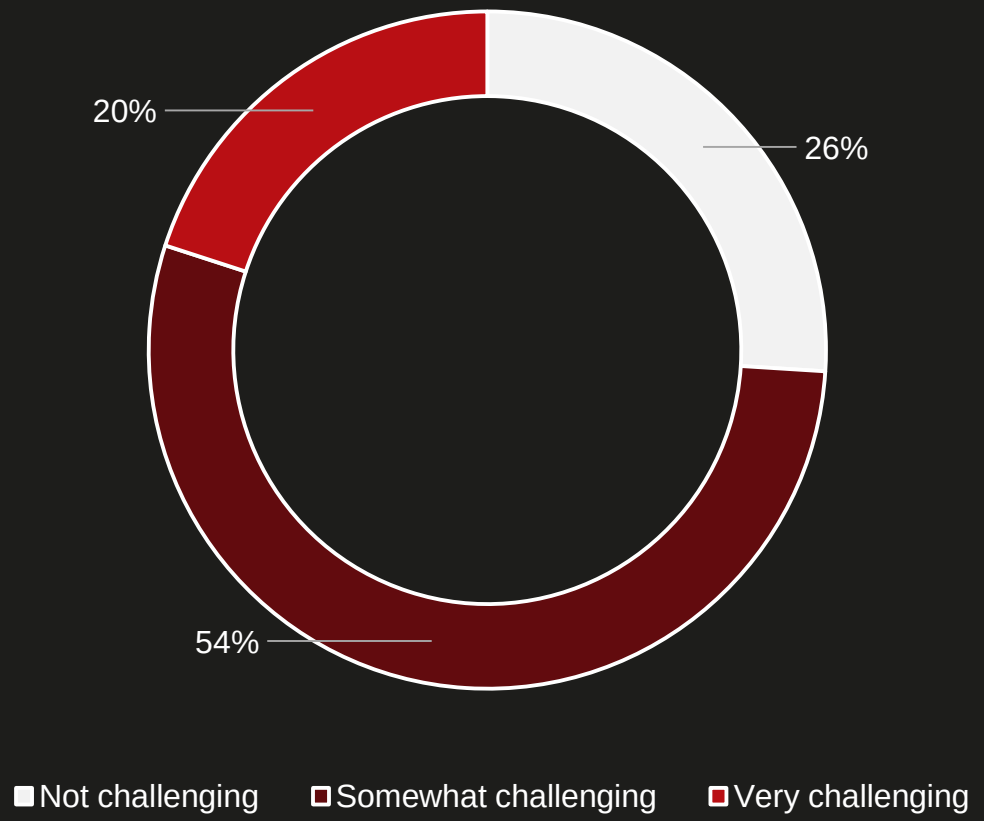
비효율적인 사고 대응으로 인해
높은 복구 비용 발생

조직 내에 아직 발견되지 않은 위협이 존재

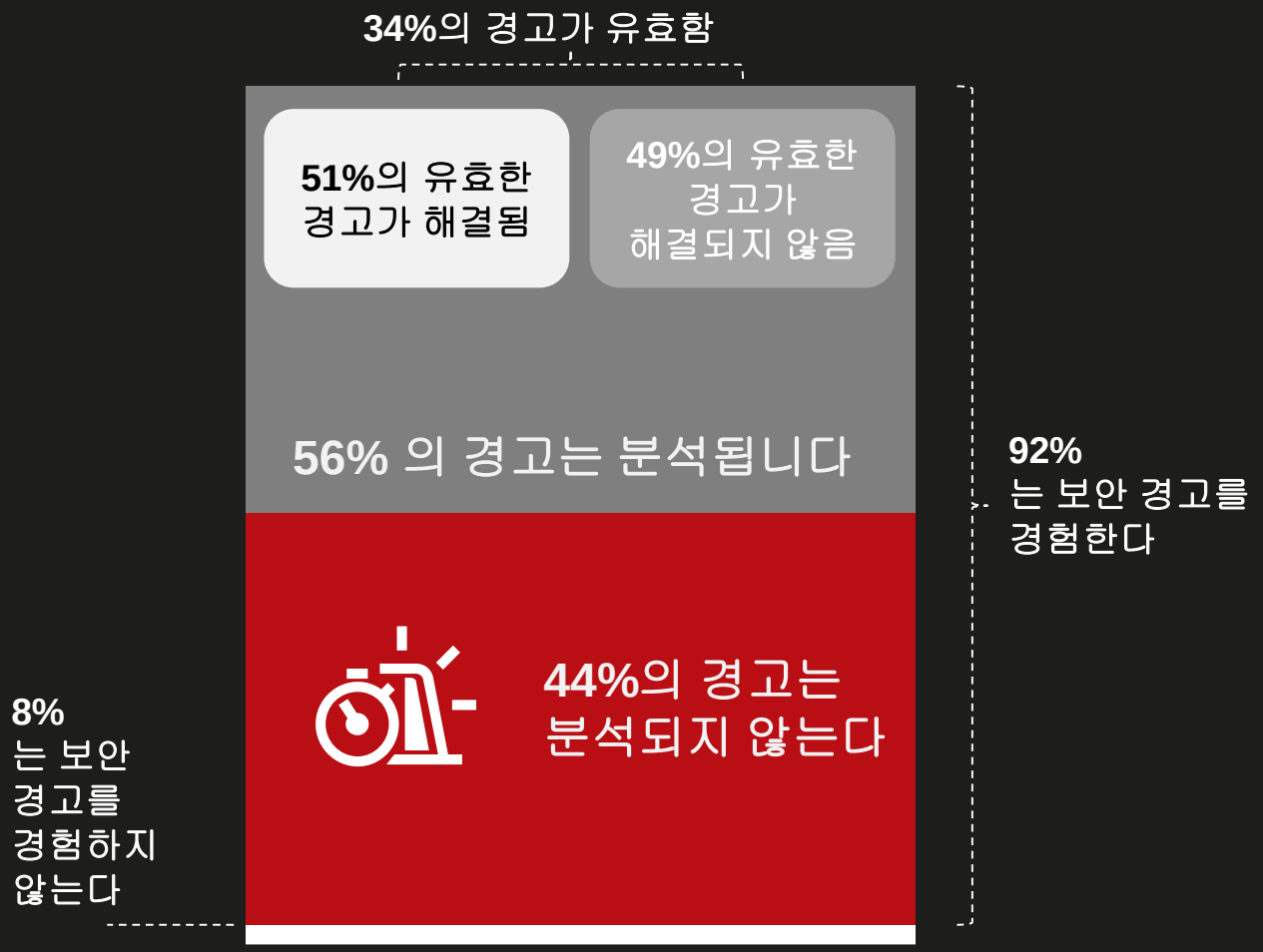
포괄적인 위협에 대한 개요 부족으로 인해
효과적인 보안 프로그램 개발 난항

증가하는 보안 경고의 수

경고 조정의 당면 과제

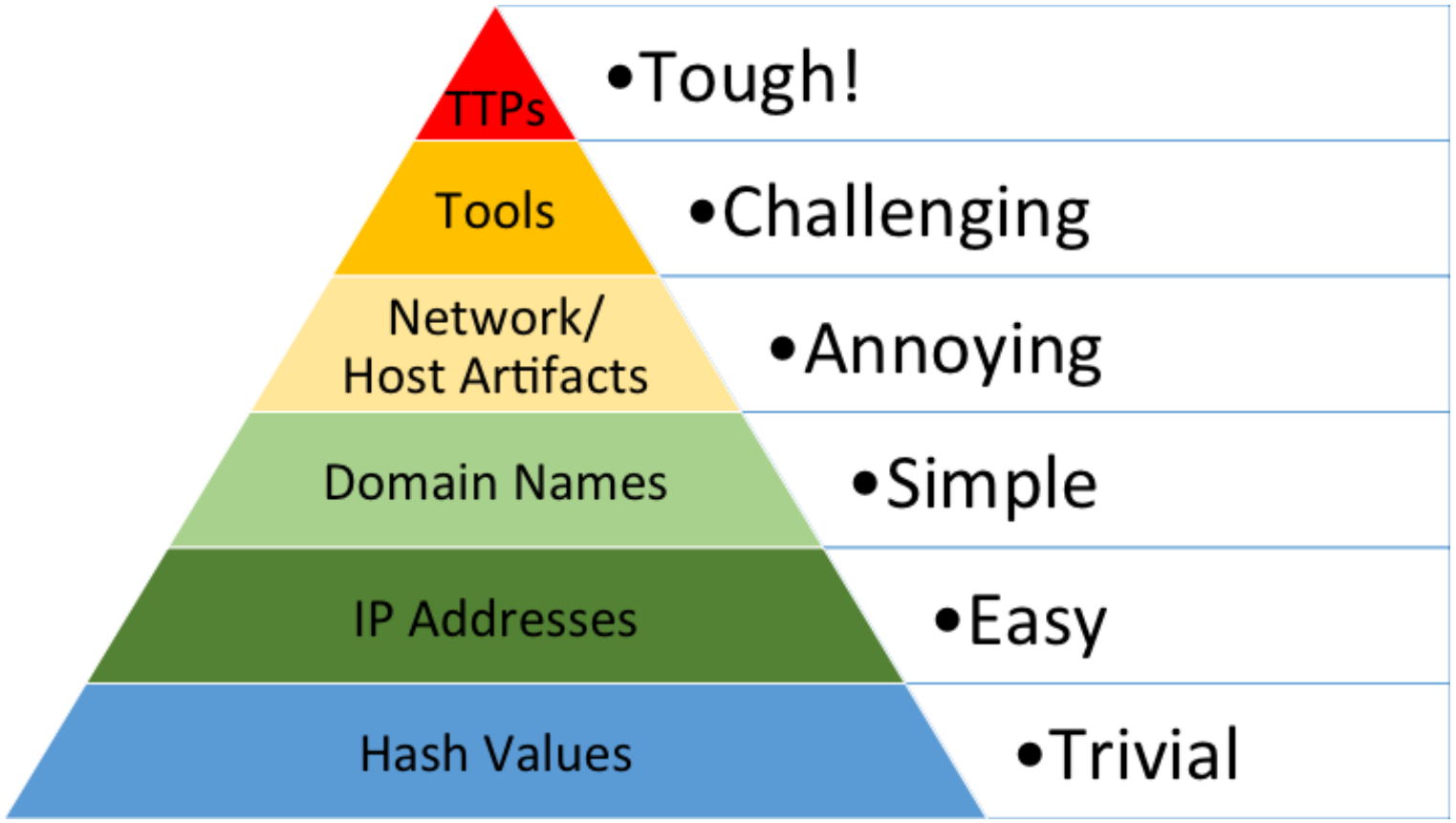


많은 위협 경고가 조사되지 않거나 해결되지 않음



Source: Cisco 2018 Capabilities Benchmark Study

Information 과 Intelligence 의 차이



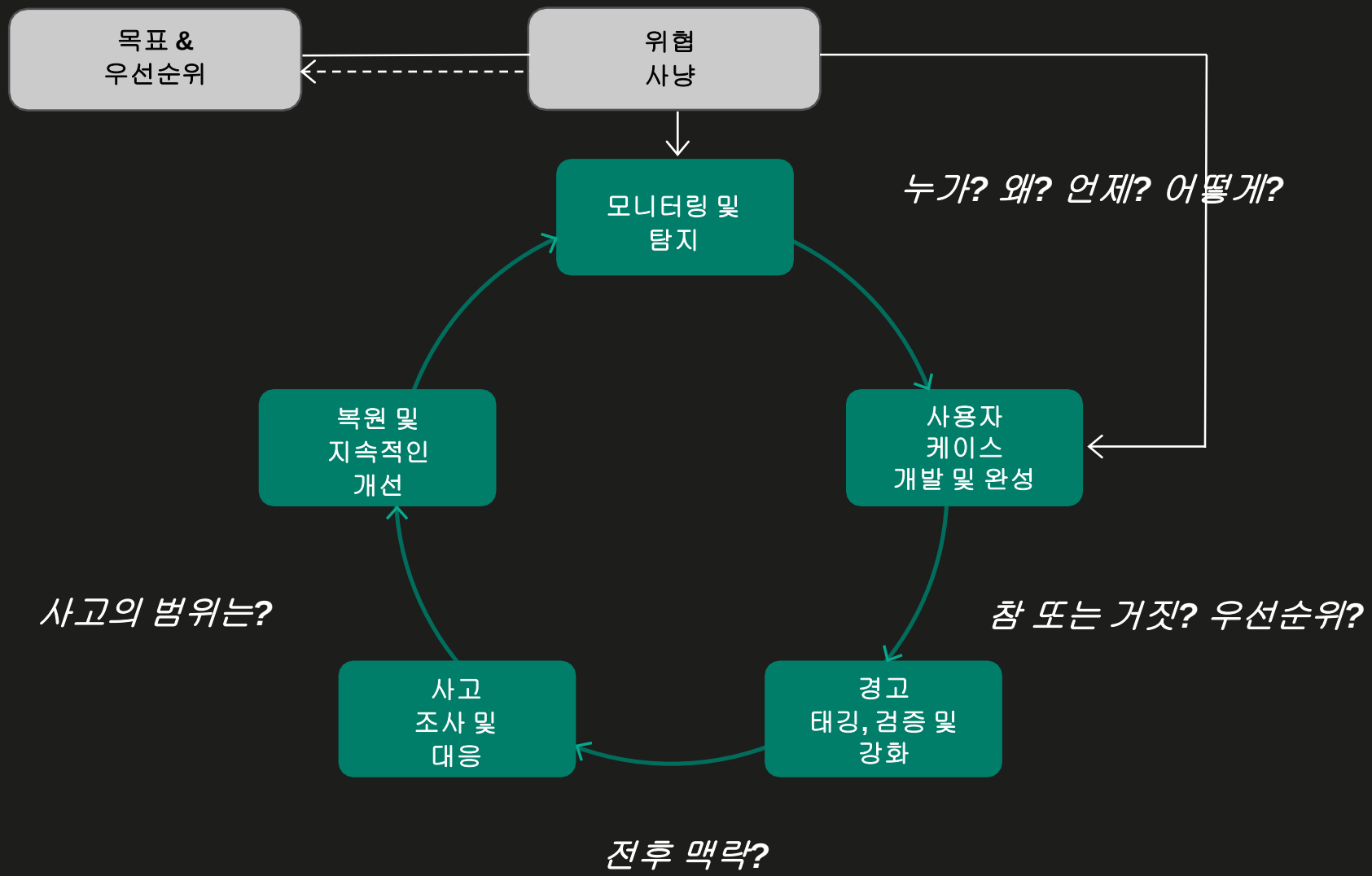
Threat **Intelligence**

빠르게 탐지, 대응하고
상대방의 행동을 효과적으로
저지하였을 때, 방어를 넘어
공격 행위가 된다.

Threat **Information**

Source: Pyramid of Pain - David Bianco
https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

인텔리전스 기반 보안 운영



kaspersky

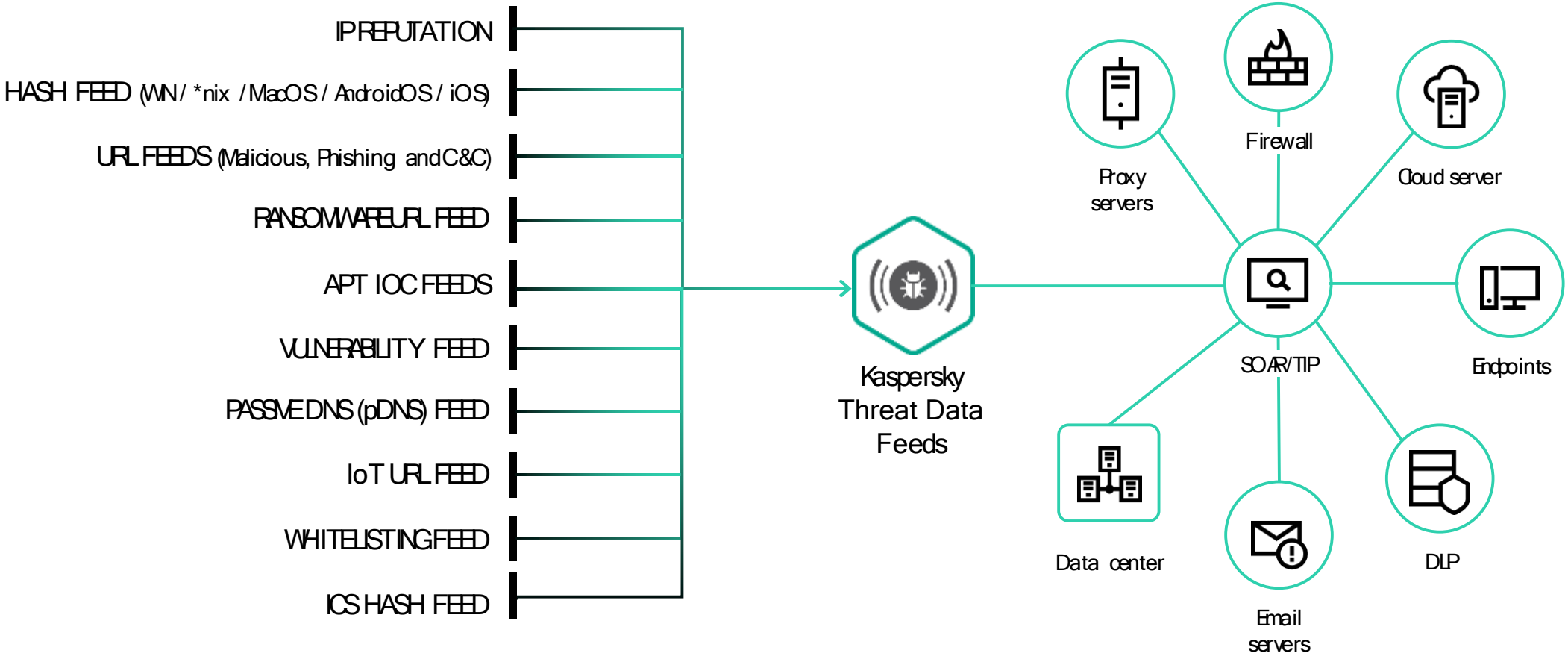
Threat Intelligence가 제공하여야 할 기능

Threat Data Feeds

오탐률이 0에 가깝고 지속적으로 업데이트 되는 위협 데이터

풍부하고 의미있는 전후사정 정보로 인해 인텔리전스를 즉시 실행

표준 전달 형식과 메커니즘을 통해 보안 제어에 쉽게 통합 가능



위협 관리 플랫폼

위협 탐지 DB와 분석 플랫폼을 이용한 다단계 킬체인 구축

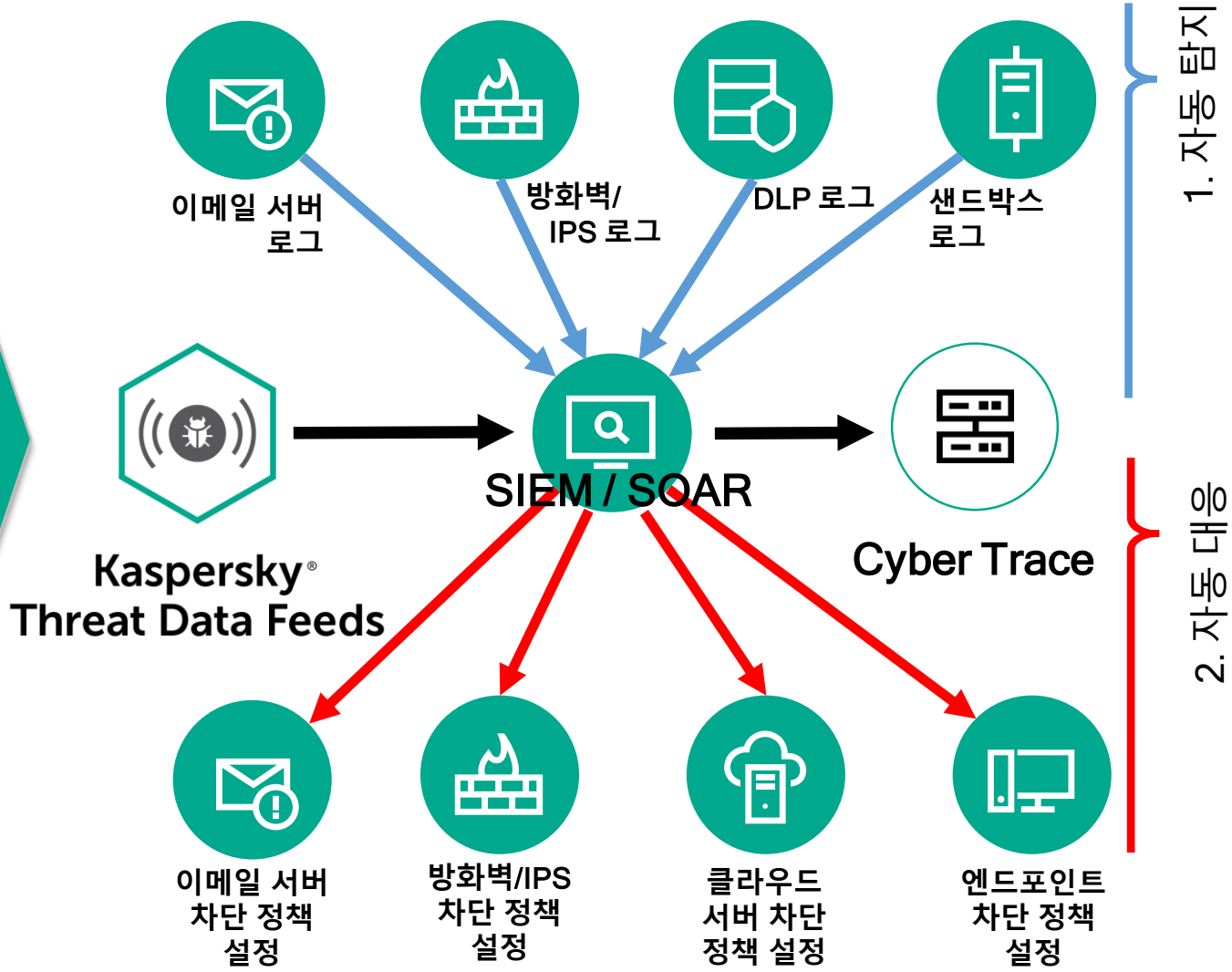
1. 자동 탐지

카스퍼스키 위협 인텔리전스 IOC Data Feeds를 SIEM / SOAR와 통합하여 위협 자동 탐지.

1. 서버나 클라이언트에 심어져 있는 악성 Script가 공격용 트로이목마 다운로드 탐지.
2. 트로이목마가 공격자의 CnC 서버로 접속하여 데이터 유출, 파괴, 암호화를 위한 지령 수신 탐지.
3. 이메일 서버를 통한 공격 전단계의 악성 코드 배포 탐지.
4. 웹을 통한 공격 파일 다운로드 유인 탐지.

2. 자동 대응

1. 공격을 위한 사전 징후 탐지시 CnC 서버로의 접속 차단정책을 방화벽에 자동 등록.
2. 공격을 위한 악성코드 배포 탐지시 해당 URL로의 접속 차단정책을 IPS에 자동 등록.
3. 공격을 위한 공격도구의 파일 Hash 값을 Email 서버에 실시간 업데이트 하여 차단.
4. 각종 공격 탐지 시 클라우드 서버와 엔드포인트 중앙관리 서버에 차단정책 등록.



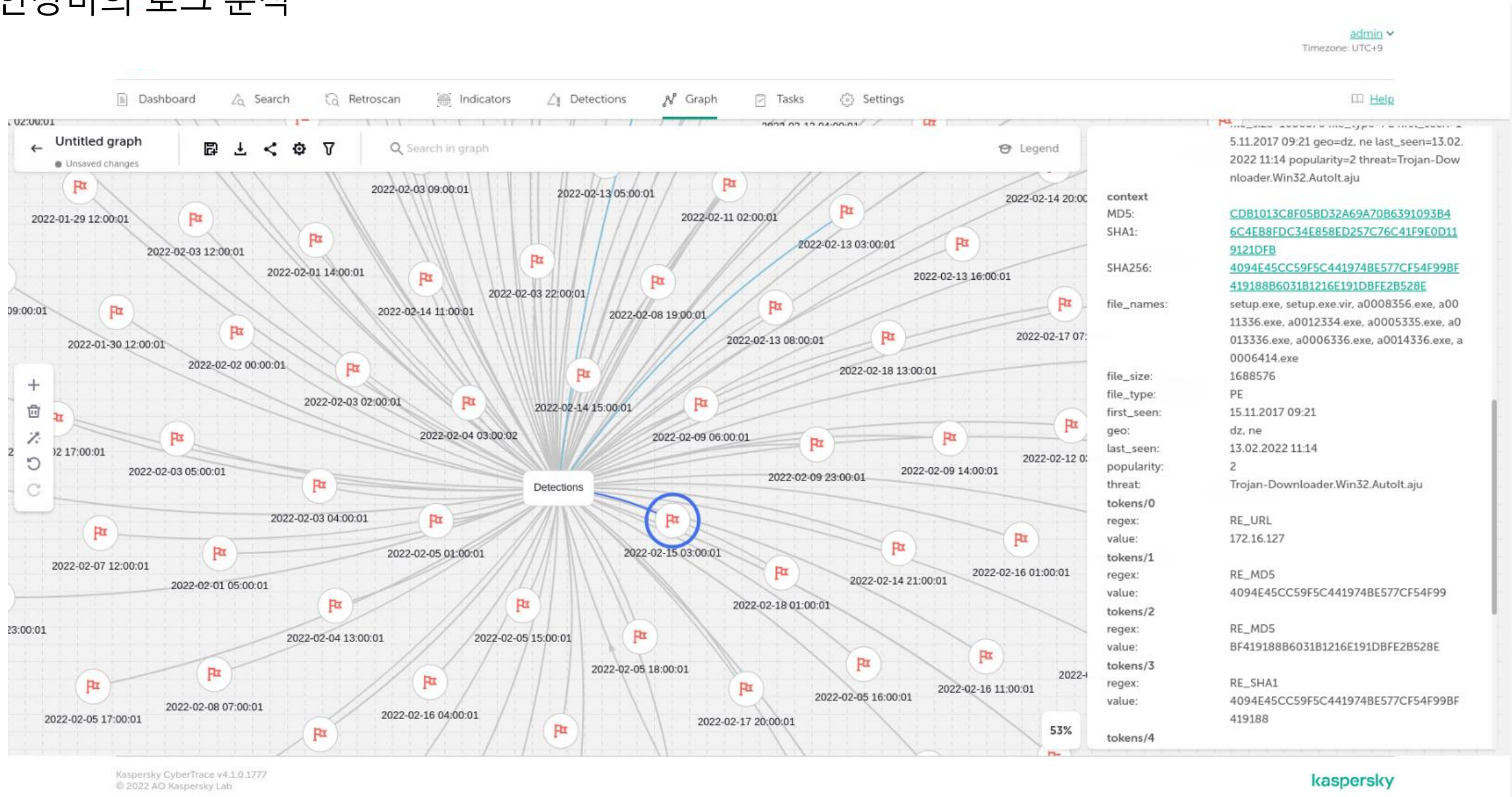
SIEM/SOAR와의 연동시 고려 사항

SIEM/SOAR/IRP

Threat Intelligence Platforms

Network security controls

보안장비의 로그 분석


admin
Timezone: UTC+9
Dashboard
Search
Retroscan
Indicators
Detections
Graph
Tasks
Settings
Help
Untitled graph
Unsaved changes
Search in graph
Legend
Detections
2022-02-03 09:00:01
2022-02-13 05:00:01
2022-02-11 02:00:01
2022-02-14 20:00
2022-01-29 12:00:01
2022-02-03 12:00:01
2022-02-01 14:00:01
2022-02-13 03:00:01
2022-02-13 16:00:01
2022-02-03 22:00:01
2022-02-14 11:00:01
2022-02-08 19:00:01
2022-01-30 12:00:01
2022-02-02 00:00:01
2022-02-13 08:00:01
2022-02-17 07:
2022-02-18 13:00:01
2022-02-03 02:00:01
2022-02-14 15:00:01
2022-02-04 03:00:02
2022-02-09 06:00:01
2022-02-12 0
2022-02-03 05:00:01
2022-02-09 23:00:01
2022-02-09 14:00:01
2022-02-03 04:00:01
2022-02-05 01:00:01
2022-02-15 03:00:01
2022-02-07 12:00:01
2022-02-01 05:00:01
2022-02-14 21:00:01
2022-02-16 01:00:01
2022-02-18 01:00:01
2022-02-04 13:00:01
2022-02-05 15:00:01
2022-02-05 18:00:01
2022-02-05 16:00:01
2022-02-16 11:00:01
2022-02-05 17:00:01
2022-02-08 07:00:01
2022-02-16 04:00:01
2022-02-17 20:00:01
53%
5.11.2017 09:21 geo=dz, ne last_seen=13.02.2022 11:14 popularity=2 threat=Trojan-Downloader.Win32.AutoIt.aju
context
MD5: CDB1013C8F05BD32A69A70B6391093B4
SHA1: 6C4EB8FDC34E858ED257C76C41F9E0D119121DFB
SHA256: 4094E45CC59F5C441974BE577CF54F99BF419188B6031B1216E191DBFE2B528E
file_names: setup.exe, setup.exe.vir, a0008356.exe, a0011336.exe, a0012334.exe, a0005335.exe, a0013336.exe, a0006336.exe, a0014336.exe, a0006414.exe
file_size: 1688576
file_type: PE
first_seen: 15.11.2017 09:21
geo: dz, ne
last_seen: 13.02.2022 11:14
popularity: 2
threat: Trojan-Downloader.Win32.AutoIt.aju
tokens/0
regex: RE_URL
value: 172.16.127
tokens/1
regex: RE_MD5
value: 4094E45CC59F5C441974BE577CF54F99
tokens/2
regex: RE_MD5
value: BF419188B6031B1216E191DBFE2B528E
tokens/3
regex: RE_SHA1
value: 4094E45CC59F5C441974BE577CF54F99BF419188
tokens/4
Kaspersky CyberTrace v4.1.0.1777
© 2022 AO Kaspersky Lab
kaspersky

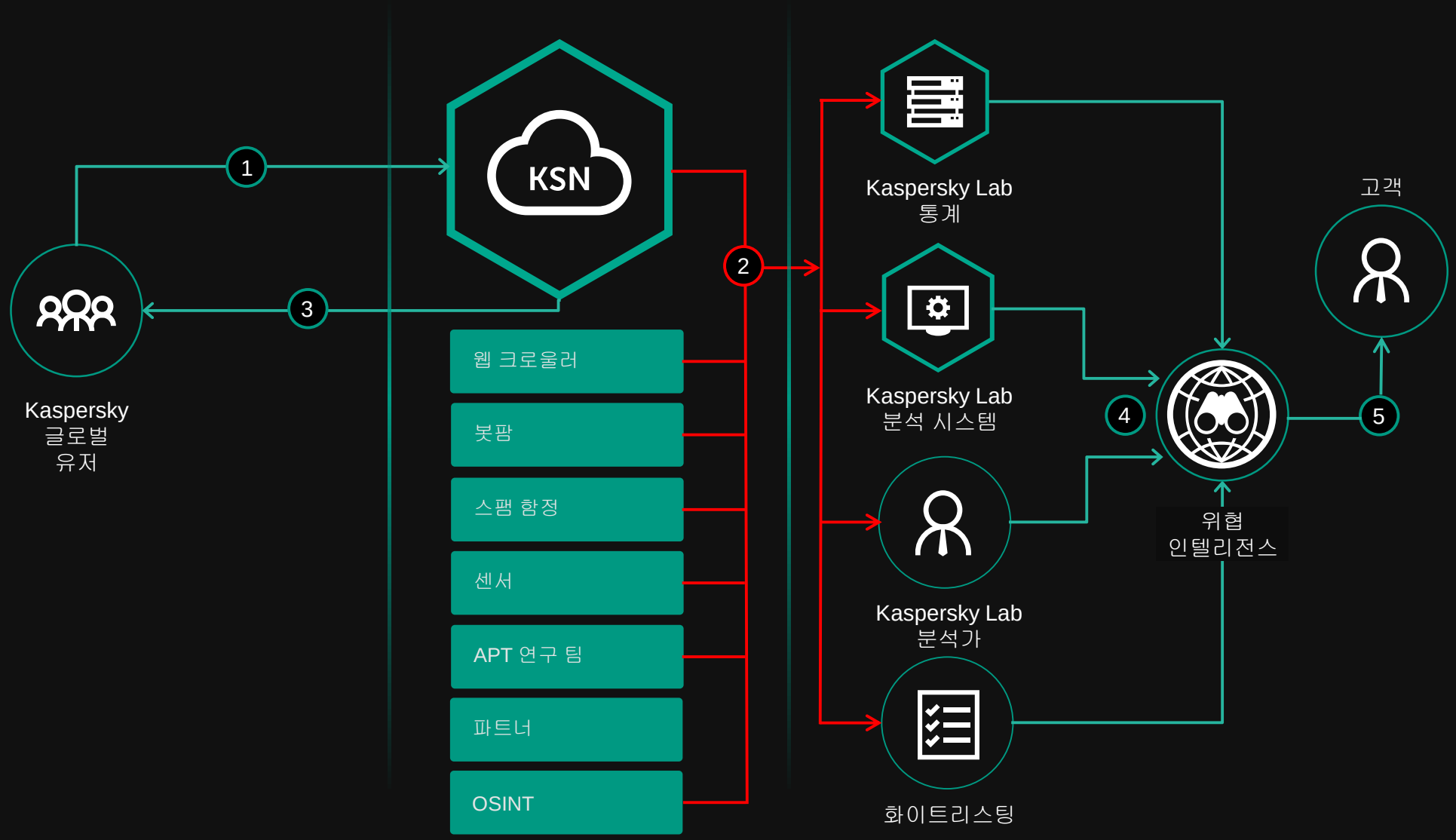
kaspersky

Demo
Threat Hunting 실무

kaspersky

Kaspersky Threat Intelligence

Kaspersky 위협 인텔리전스의 정보 출처



저희의 미션은 간단합니다.
바로 보다 안전한 세상을 만드는 것 입니다.

그 미션을 이루기 위하여 저희는 사이버시큐리티 분야의
글로벌 리더로 거듭나는것을 목표로 하고 있으며,
저희 각자와 모두에게 기회가 되는 가능성을 가져다 줄
기술력 확보를 위하여 최선을 다하고 있습니다.

끝없는 가능성을 위하여,
보다 안전한 내일을 위하여.

Eugene Kaspersky, CEO