

Kaspersky Threat Intelligence 를 이용한 APT / Ransomware 대응

강민석
kaspersky

kaspersky

Ransomware를 사용하는 APT Landscape

Advanced persistent threat landscape in 2020

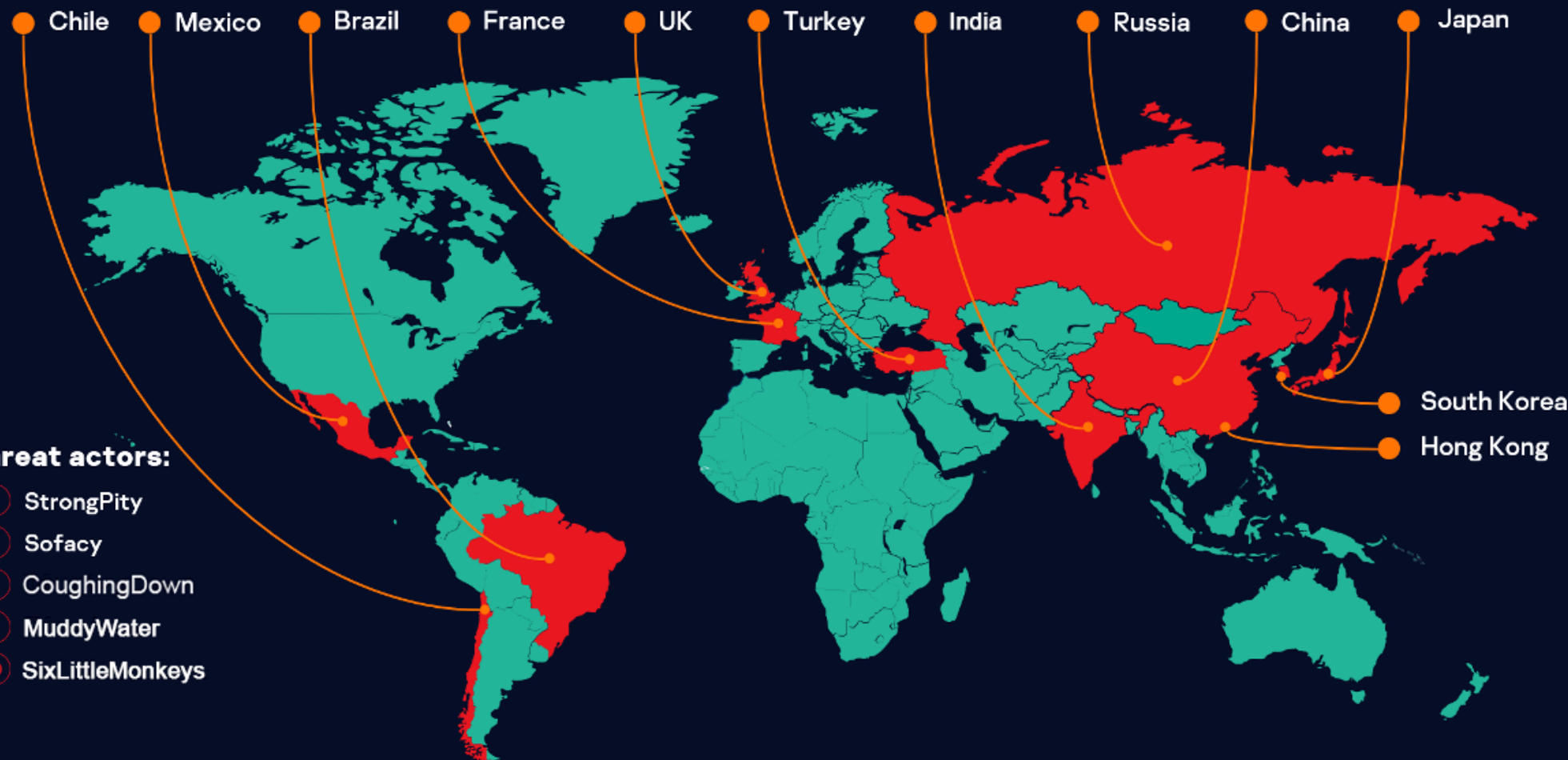
Kaspersky's Global Research and Analysis Team (GReAT) is well-known for the discovery and dissemination of the most advanced cyberthreats.

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

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 | 6 MuddyWater |
| 2 DarkHalo | 7 APT41 |
| 3 CloudComputing | 8 BlueNoroff |
| 4 Turla | 9 HoneyMyte |
| 5 SideCopy | 10 Gamaredon |

Advanced persistent threat landscape in 2022

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 2022 the top targets for advanced persistent threats (APT) were governments, and the most significant threat actor was Lazarus.

Top 10 targets

- | | |
|---|--|
|  Government |  Telecommunications |
|  Military Dipl |  Media |
|  Domestic |  Software Development |
|  IT companies |  Manufacturing |
|  Educational |  Logistics |

Top 10 significant threat actors

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



Top 12 targeted countries/territories



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.

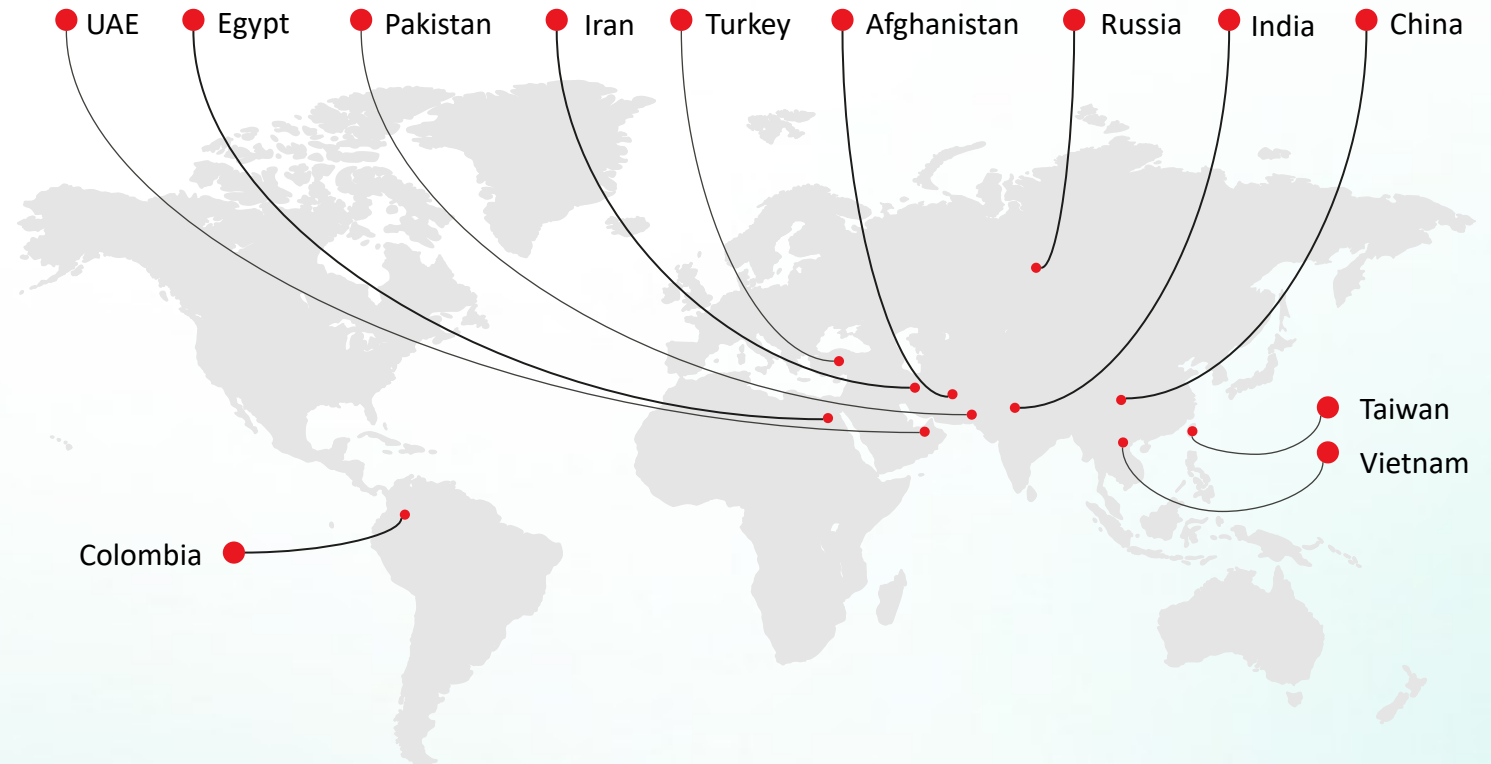
Top 10 targets

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

Top 10 significant threat actors











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

상위 12개 대상 국가 및 지역



카스퍼스키의 글로벌 연구 및 분석 팀(GReAT)은 가장 진보된 사이버 위협을 발견하고 분석하는 것으로 잘 알려져 있습니다. 2024년 지능형 지속 위협(APT)의 최대 표적은 정부, 통신, 금융이었으며 가장 중요한 위협 행위자는 5년 연속 Lazarus 였습니다.

Top 10 targeted industries

- | | |
|--|---|
|  Government |  Manufacturing |
|  Telecommunications |  Defense |
|  Financial Institutions |  IT companies |
|  Education |  Construction |
|  Energy |  Commercial |










Top 10 significant actors

- | | |
|--|---|
|  Lazarus |  Charming Kitten |
|  HoneyMyte |  Gamaredon |
|  Kimsuky |  SideWinder |
|  DeathStalker |  Awaken Likho |
|  BlindEagle |  Transparent Tribble |

Top 12 targeted countries and territories



Our major discoveries and research

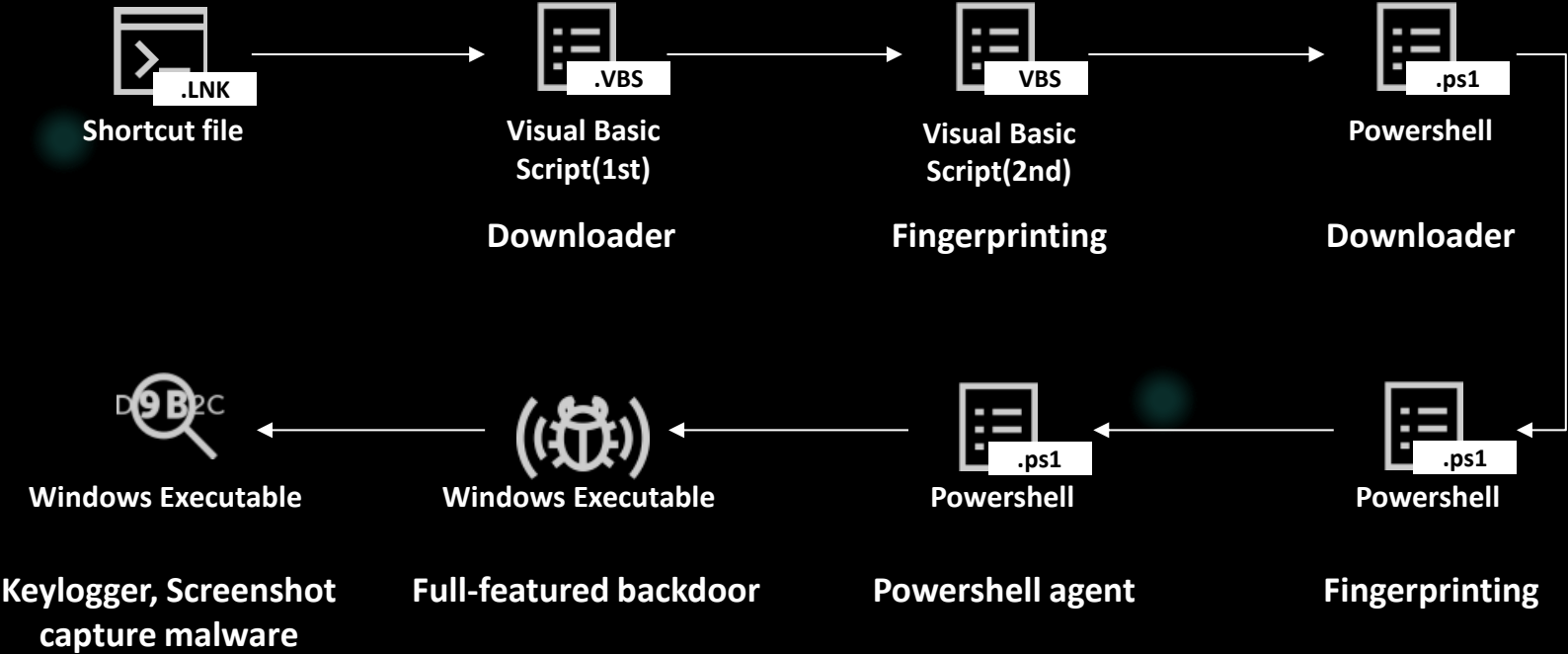
									
	Expetr/ Notpetya	Olympic destroyer	Shadow hammer	Tajmahal	Mosaicregressor	Ghostemperor	Moonbounce	Operation Triangulation	Grandoreiro
Detection	2017	2018	2018	2019	2020	2021	2022	2023	2024
Active since	2017	2017	2018	2013	2017	2020	2021	2019	2016
Classification	Data wiping campaign	Cyber-espionage malware	Cyber-espionage malware	Cyber-espionage platform	Cyber-espionage platform	Cyber-espionage platform	Cyber-espionage platform	APT campaign	Financial cybercrime
Description	A wiper pretending to be ransomware, using modified EternalBlue and EternalRomance exploits. Some observations point to a link between ExPetr and BlackEnergy APT	An advanced threat actor that hit organizers, suppliers and partners of the Winter Olympic Games in Pyeongchang, South Korea, with a destructive network worm. The deceptive behavior of this actor is an excessive use of various false flags	As a result of a sophisticated supply chain attack on the popular computer vendor's software update system, the malware disguised as a software update was distributed to about 1 million Windows computers and signed using legitimate certificate	Technically sophisticated APT framework designed for extensive cyberespionage. Features around 80 malicious modules and includes functionality never before seen in an advanced persistent threat, such as the ability to steal information from printer queues and to grab previously seen files from a USB device the next time it reconnects	A multi-stage, modular framework aimed at espionage and data gathering. It is leveraging a UEFI bootkit based on Hacking Team's leaked source code for persistence. Capable of communicating and fetching payloads over multiple, covert channels	A stealthy, sophisticated multi-stage malware framework incorporating Windows kernel mode rootkit. It's deployed via the ProxyLogon only days following the vulnerability disclosure	A highly sophisticated, complex UEFI firmware rootkit we attribute to APT41, which allows the attackers to persistently execute a malware stager on the operating system via a malicious driver	The targets are infected using zero-click exploits via the iMessage platform, and the malware runs with root privileges, gaining complete control over the device and user data. The targets are infected using zero-click exploits via the iMessage platform, and the malware runs with root privileges, gaining complete control over the device and user data	A sophisticated Brazilian banking trojan under the Tetrade malware family, enabling attackers to bypass banking security and commit fraud. Despite arrests in 2021 and 2024, it remains active, with recent lighter versions targeting 30 banks in Mexico. Responsible for 5% of global banking trojan attacks this year, Grandoreiro has targeted users of over 1,700 banks, making it one of the most persistent threats worldwide
Targets	Spread around the world, primarily targeting businesses in Ukraine, Russia and Western Europe. >50% of organizations attacked were industrial companies	Organizations related to Winter Olympic Games 2018; biological and chemical threat prevention organizations in EU, financial institutions in Russia	Banking and financial industry, software, media, energy and utilities, insurance, industrial and construction, manufacturing, and other industries	Special instructions in malware code were aimed at targeting only 600 systems, identified by specific MAC addresses	Diplomatic entities with possible affiliation to DPRK	Government organizations and Telecommunication companies	Holding companies and industrial suppliers	iOS devices	Financial institutions in more than 40 countries in North and Latin America, and Europe

Targeted attack research

2017	2018	2019	2020	2021	2022	2023	2024
 WannaCry	 Zebrocy	 Topinambour	 Cycldek	 GhostEmperor	 Tomiris	 PowerMagic	 CloudSourcerer
 Shamoon 2.0	 DarkTequila	 ShadowHammer	 SixLittleMonkeys (aka Microcin)	 ExCone	 ZexCone	 CommonMagic	 PipeMagic
 StoneDrill	 MuddyWater	 SneakyPastes	 CactusPete	 BlackShadow	 SilentMarten	 Trila	 Zanubis
 BlueNoroff	 Skygofree	 FinSpy	 DeathStalker	 BountyGlad	 MoonBounce	 LoneZerda	 SambaSpy
 ExPetr/NotPetya	 Olympic Destroyer	 DarkUniverse	 MATA	 EdwardsPheasant	 ToddyCat	 CloudWizard	 SideWinder
 Moonlight Maze	 ZooPark	 COMpfun	 TransparentTribe	 HotCousin	 MagicKarakurt	 Operation Triangulation	 BellaCPP
 ShadowPad	 Hades	 Titanium	 WellMess	 GoldenJackal	 CosmicStrand	 BlindEagle	 EastWind
 BlackOasis	 Octopus		 TwoSail Junk	 FerociousKitten	 SBZ	 Mysterious Elephant	 PassiveNeuron
 Silence	 AppleJeus		 MontysThree	 ReconHellcat	 StripedFly	 BadRory	 Awaken Likho
 WhiteBear			 MosaicRegressor	 CoughingDown	 DiceyF	 Dark Caracal	
			 VHD Ransomware	 MysterySnail	 MurenShark	 HrServ	
			 WildPressure	 CraneLand			
			 PhantomLance				

Latest Threat Landscape: Multi-stage infection

BlueNoroff's SnatchCrypto campaign



781a20f27b72c1c901164ce1d025f641
483e3eb01dceb4a5a13de65d3556c3fe
5e444ced6209e64254993beae92db0c93
c16977feafb825a5c67603db4ea3914
09bca3ddbc55f22577d2f3a7fda22d1c
0eb71e4d2978547bd96221548548e9f0
da599b0cde613b5512c13f299fec739e
0c9170a2584ceedd5b89e4c0f0a2353ed
5053103dd5057c1dc54edf1f8568098
536bae31c99a4d46f503c68595d4431
3078265f207fed66470436da07343732
15f1ae1fed1b2ea71fdb9661823663c6
56fe283ca3e1c1667191cc7764c260b6
850751de7b8e158d84669d22ad1c3101
1a8282f37b9656996107b6ec038dd5
2ea2ceab1588810961d2fc545e2f957e
561f70411449b327e3f19d811bb2cea08
3812cdc4225182326b1425c9f3c2d50b
5af886030204952ae243eedd25dd43c4

df21849756eca89ebfaa33ed3185d95
e18dd8e61c736cfc6ffff86b07a352c12
e546b851ac4fa5a111d10f40260b1466
e6e64c511f935d31a8859e9f3147fe24
ea7ed84f7936d4cbafa7cec51fe39cf7
fa1416569363037a6ec92a4d951bdf55
4e207d6e930db4293a6b720cf47858fc

ce09cdb7979fb9099f46dd33036b9001
f7f4aa55a2e4f38a6a3ea5a108baedf5

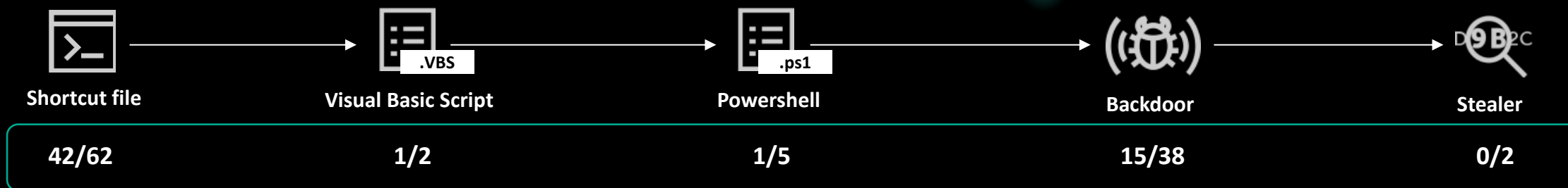
589f1bb4da89cfd4a2f7f3489aa426a9
ae52b28b360428829c4fcdc14e839f19
73572519159b0c27a18dbbaf25ef1cc0
8ae6aa90b5f648b3911430f14c92440b
ae12a668dd9f254c42fcd803c7645ed1

00a145e8f67a92b01ce4d85a0ed6bd77
ff28ec14ec926b9892c61b9b9f154a910
97e5c0f8e089da97665a22975ce2c86de
4fbff7f0f62b26963b56c0cf23486891
4bb579d598305279be9ead974a55001e
f1cfd14b030e6b5d75e777ace530dad9
1d0fc2f1a6eb2b2bfa166a13ca871f0
db91826bc9f2ad6edfed8d6bab5bef1f
c592a22acdfbf750c440fda31da4996c
2934a7a0dfa2f2ebc81b1f089277129c4

4fbff7f0f62b26963b56c0fc23486891
4bb579d59830579be9ead9f74a55001e
aafc80ff2afc71b0d5abd6c8d2809e65
9850b24f8d70d9d5f7328961170e2d40
58495a2083065b36040eea28ba9d5e17
f1cfd14b030e6b5d75e777ace530dad9
1fb25f72e4eb26b0df154de28dbff74c
1b1acc7f27717905e7094f338f81db9f
3776d4a24213972b54b9ed3360ac7883
c93f3bb447b19f5eb6f736f2659c4dae
908462be0219c035d6402b6395be1bf4cae

Files on Virustotal
Files not on Virustotal

f29be5c7e602e529339fda35ff91bd39
f194e074e7d73c544eebb70e2e2785a1

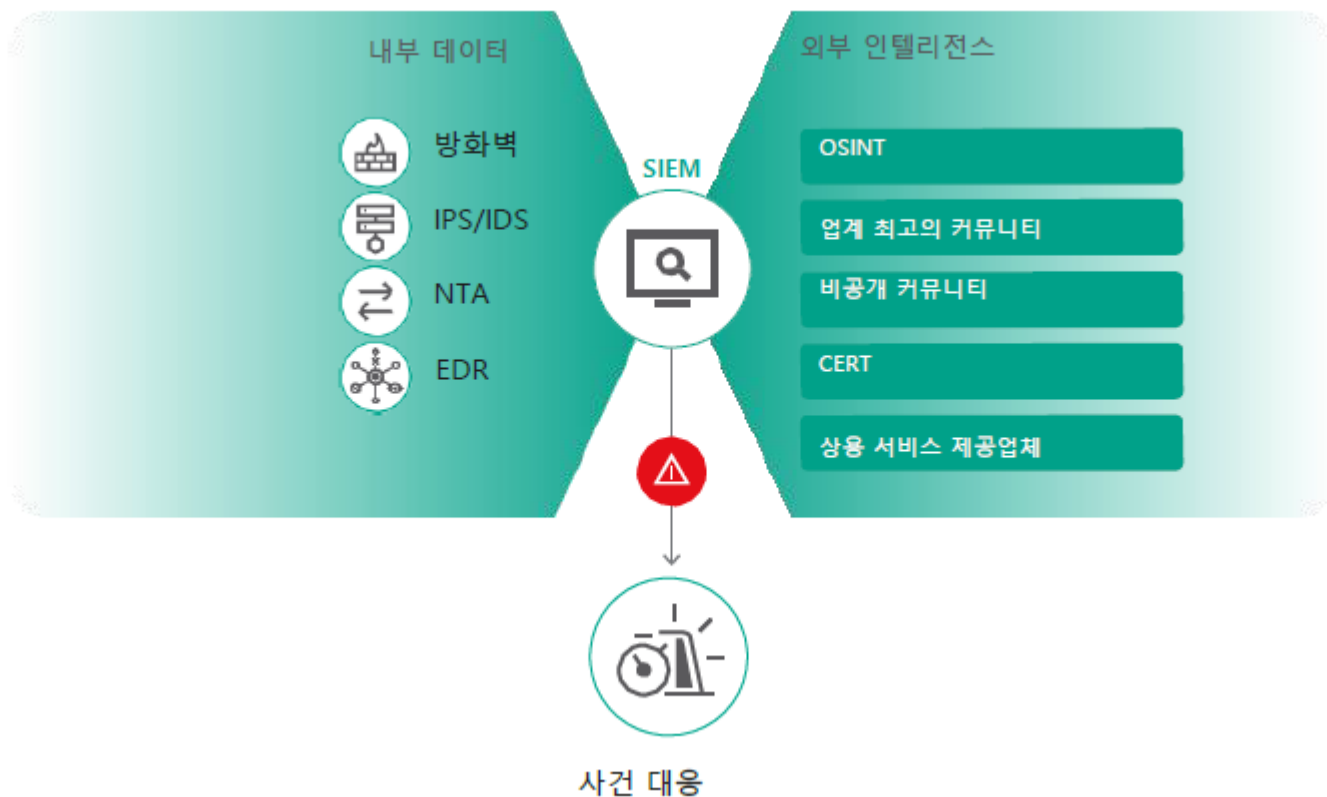


Important points we consider: Full-context understanding

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

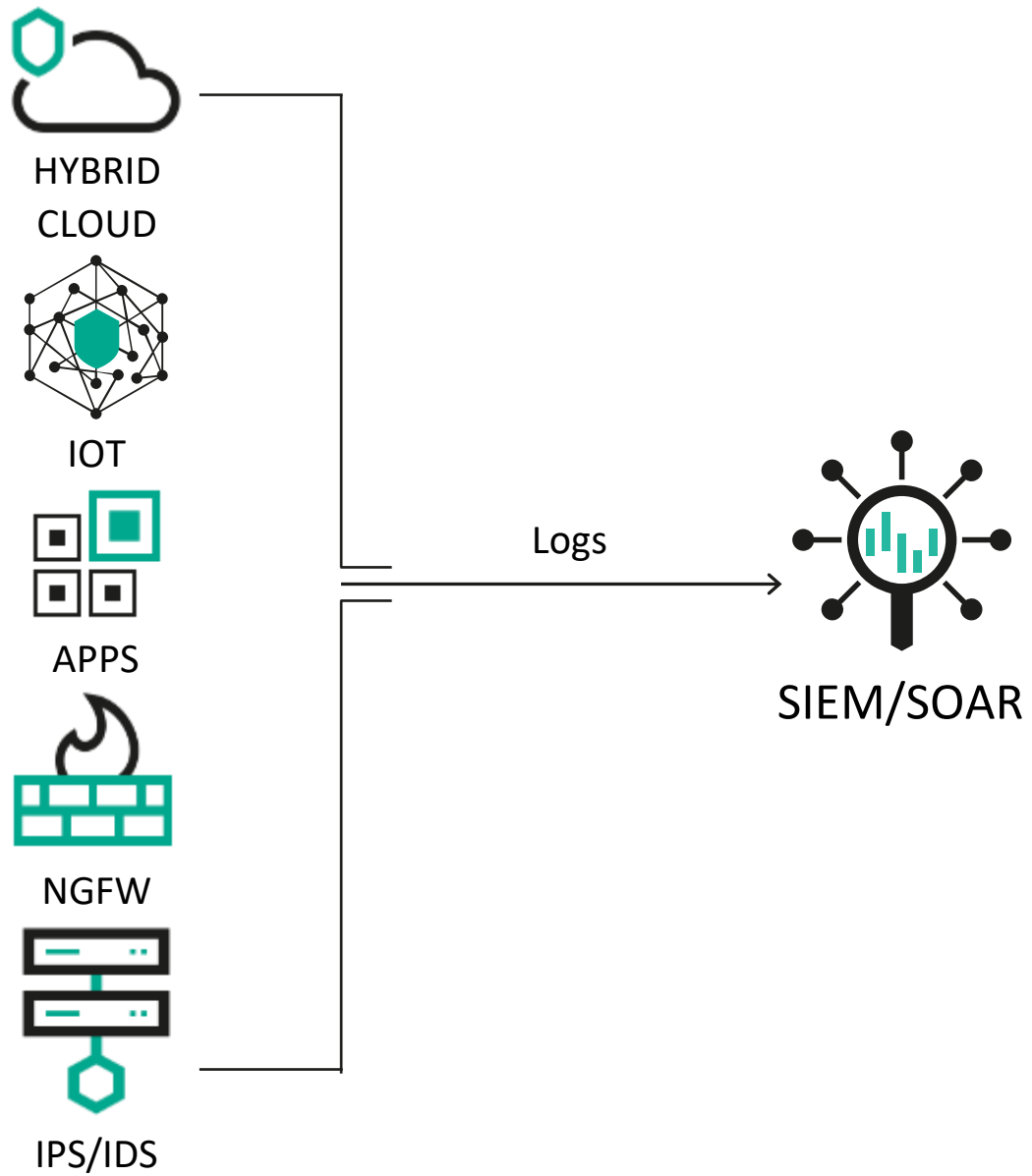
Threat Intelligence란?



SOC (Security Operation Center)
사이버상에서 발생하는 이상 현상을 사
전에 탐색하고 침해 사고를 대응하는
조직

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

진화하고 있는 사이버보안 과제



수많은 보안 기술로부터 오는 보안 알람들의
우선 순위 구분의 어려움

분석가들의 번아웃으로 인해 이직률 증가

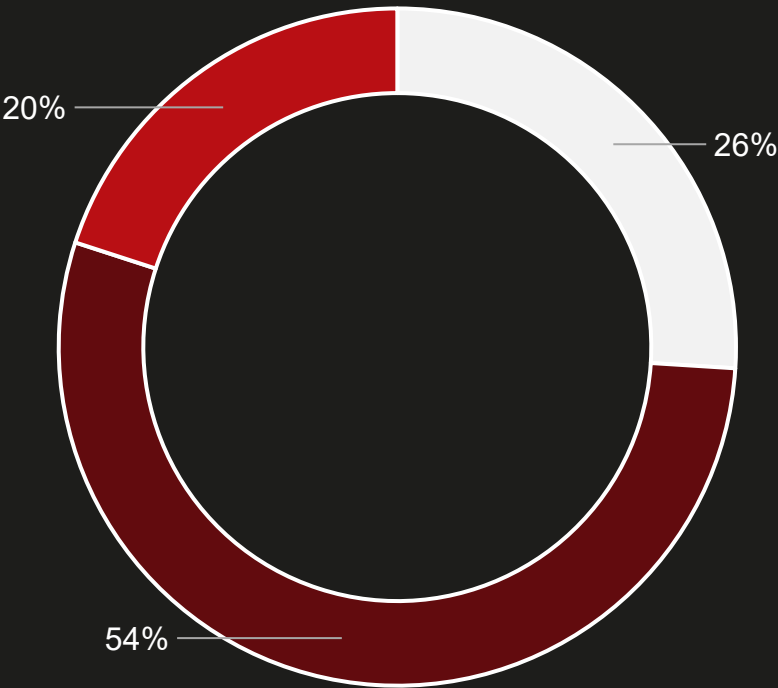
비효율적인 사고 대응으로 인해
높은 복구 비용 발생

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



■ Not challenging ■ Somewhat challenging ■ Very challenging

Source: Cisco 2018 Capabilities Benchmark Study

많은 위협 경고가 조사되지 않거나 해결되지 않음

34%의 경고가 유효함

51%의 유효한
경고가 해결됨

49%의 유효한
경고가
해결되지 않음

56%의 경고는 분석됩니다

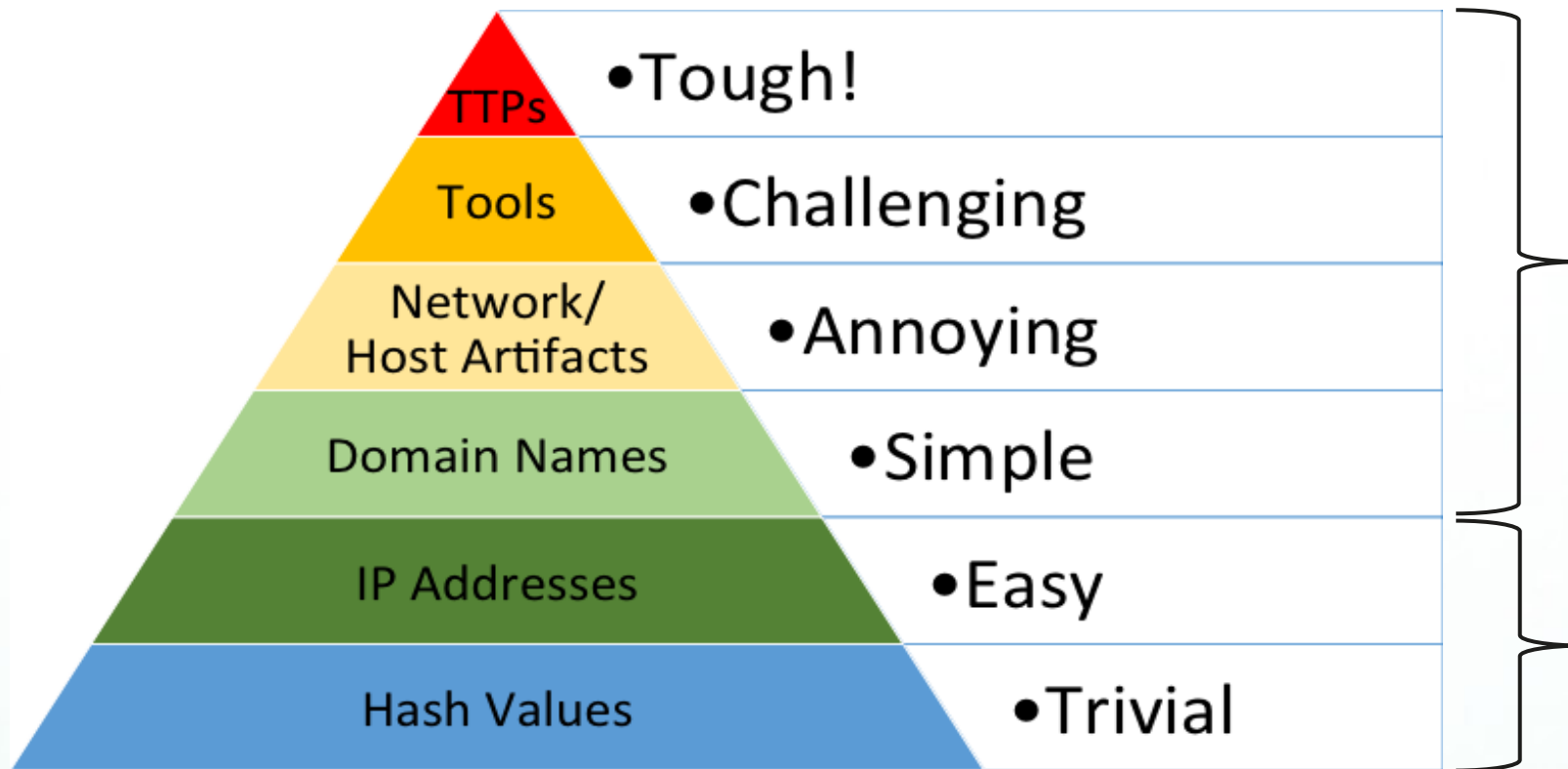


44%의 경고는
분석되지 않는다

8%
는 보안
경고를
경험하지
않는다

92%
는 보안 경고를
경험한다

- Information vs. **Intelligence**



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

Threat **Intelligence**

- > 네트워크/호스트 구조, 공격 툴, TTP 등 전술, 기술, 절차로 표현되는 침해지표들과 같이 정형화 될 수 없는 내용
- > 빠르게 탐지, 대응 및 공격자의 행위를 효과적으로 저지하기 위한 신속한 방어와 위협 헌팅 제공

Threat **Information**

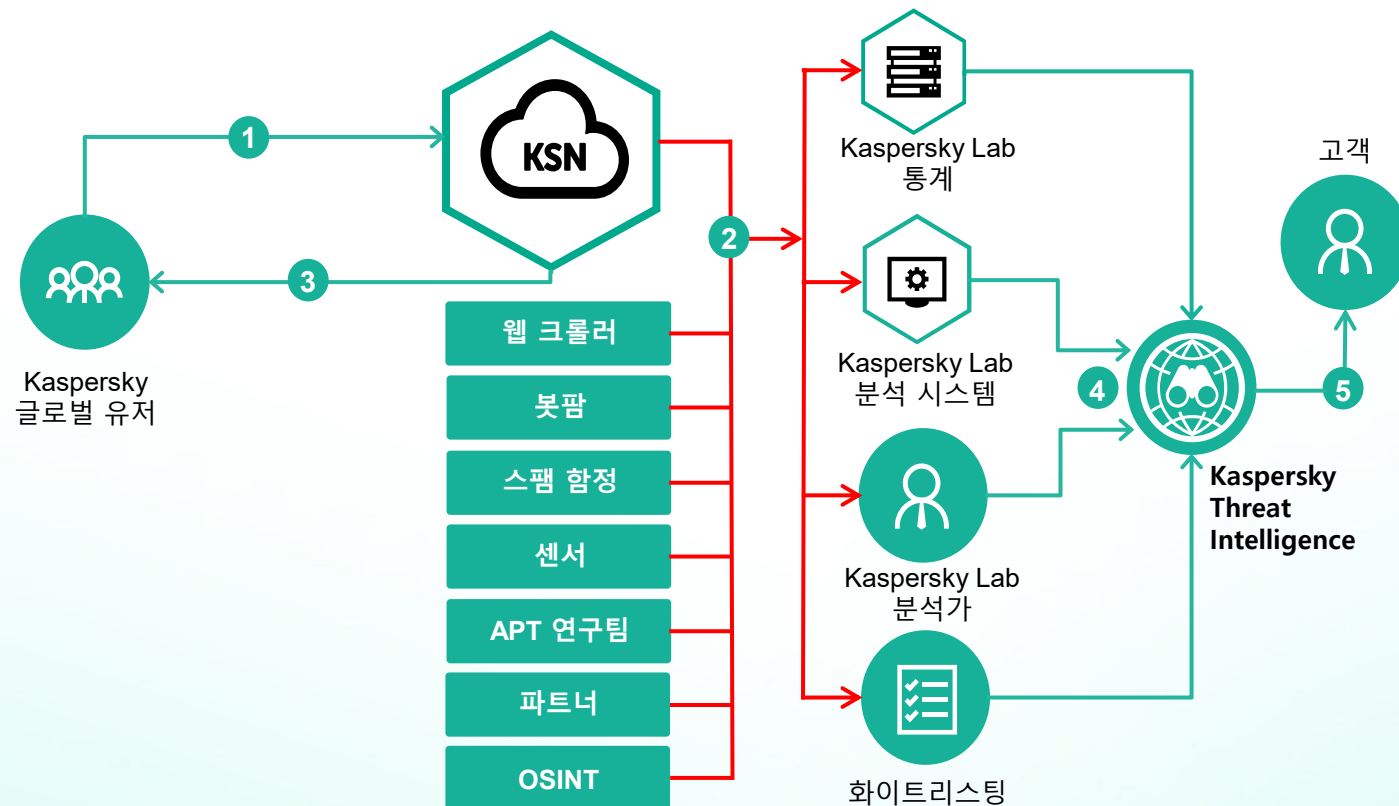
- > Hash값, IP 주소, 도메인 네임과 같이 정수나 문자로 표현될 수 있는 침해지표
- > 보안 장비 관점에서 보면, IDS, IPS, Anti-Virus, Firewall, URL Filtering System 등에 사용되는 시그니처

kaspersky

Kaspersky Threat Intelligence

Kaspersky Threat Intelligence의 특징점

1. 전 세계 1억 2천만 명 사용자의 자발적 공유에 의해 개인정보를 제외한 보안 데이터들이 Kaspersky Security Network에 업로드
2. 이 데이터는 웹 크롤러, 봇팜과 같은 카스퍼스키 독점의 정보로 더욱 풍부
(봇팜은 알려진 모든 봇넷 제품군, 허니팟 등을 모니터링하는 카스퍼스키만의 특허 시스템)
3. 매일 40만개 이상의 새로운 위협을 탐지
4. 2,000명 이상의 연구원이 위협에 관련된 연구를 지속



Botnet C&C URL Feed

Description of fields

JSON format

```
{
  "id": "143348",
  "mask": "botnetccurl.com",
  "type": "1",
  "first_seen": "08.04.2014 16:45",
  "last_seen": "12.02.2015 13:56",
  "IP": "192.168.0.1",
  "popularity": "5",
  "threat": "CnC.Win32.ZBot",
  "geo": "EN,FR,RU,GE,CH",
  "files": [ { "MD5" :
    02d78d904db1d74f51f15
    53b05257060 } ]
  "urls": "urltohostbots.com" } ]
  "whois": { ... }
}
```

id – unique record identifier

mask – record covering malicious links or websites

type – record type (matching rules are different for different types)

first_seen – date when the record was created/detected

last_seen – date when the record was last encountered by Kaspersky users

IP – Top 10 IPs of the URL/mask within the last 3 months

popularity – index number defining how many users were affected by this record.
5 = most popular, 1 = least popular

threat – threat name (class, platform, family – i.e., verdict) according to Kaspersky classification

geo – Top 10 countries where Kaspersky users were most affected by this record

files – Top 10 hashes of bots that communicate with the C&C (about 50% of records have this field)

URLs – Top 10 URLs from where bots (of the C&C) were downloaded (about 1% of records have this field)

whois – domain and whois DNS data

Malware Hash Feed

JSON format

```
{
  "md5": "202cb962ac90...b4b0752d234b70",
  "sha1": "d471FEC3726b7b...24fc457b2",
  "sha256": "a665459422f9d...86f7f7a27ae3",
  "first_seen": "01.01.2013 12:00",
  "last_seen": "02.02.2014 22:00",
  "popularity": "3",
  "threat": "Net-Worm.Win32.Kido",
  "geo": "EN,FR,RU,GE,CH",
  "file_type": "DLL",
  "file_names": "1.exe, 2.exe, 3.exe",
  "file_size": "486",
  "IP": "11.111.111.111., 22.222.222.222",
  "urls": [ {...} ]
}
```

Description of fields

MD5 – MD5 hash of malicious object

SHA1 – SHA1 hash of malicious object

SHA256 – SHA256 hash of malicious object

first_seen – date when the object was first detected (UTC)

last_seen – date when the object was last met (UTC)

popularity – index number defining how many users were affected by this record.
5 = most popular, 1 = least popular

threat – threat name (class, platform, family – i.e., verdict) according to Kaspersky classification

geo – Top 10 countries where Kaspersky users were most affected by this object

file_type – malicious object's file format type

file_names – Top 10 file names

file_size – malicious object's file

IP – Top 10 IP addresses where the file was hosted

urls – Top 10 URLs from where the file was downloaded

Kaspersky Threat Intelligence 주요 기능 1- IoC와 Context

위협 탐지 DB와 분석 플랫폼을 이용한 다단계 킬체인 구축

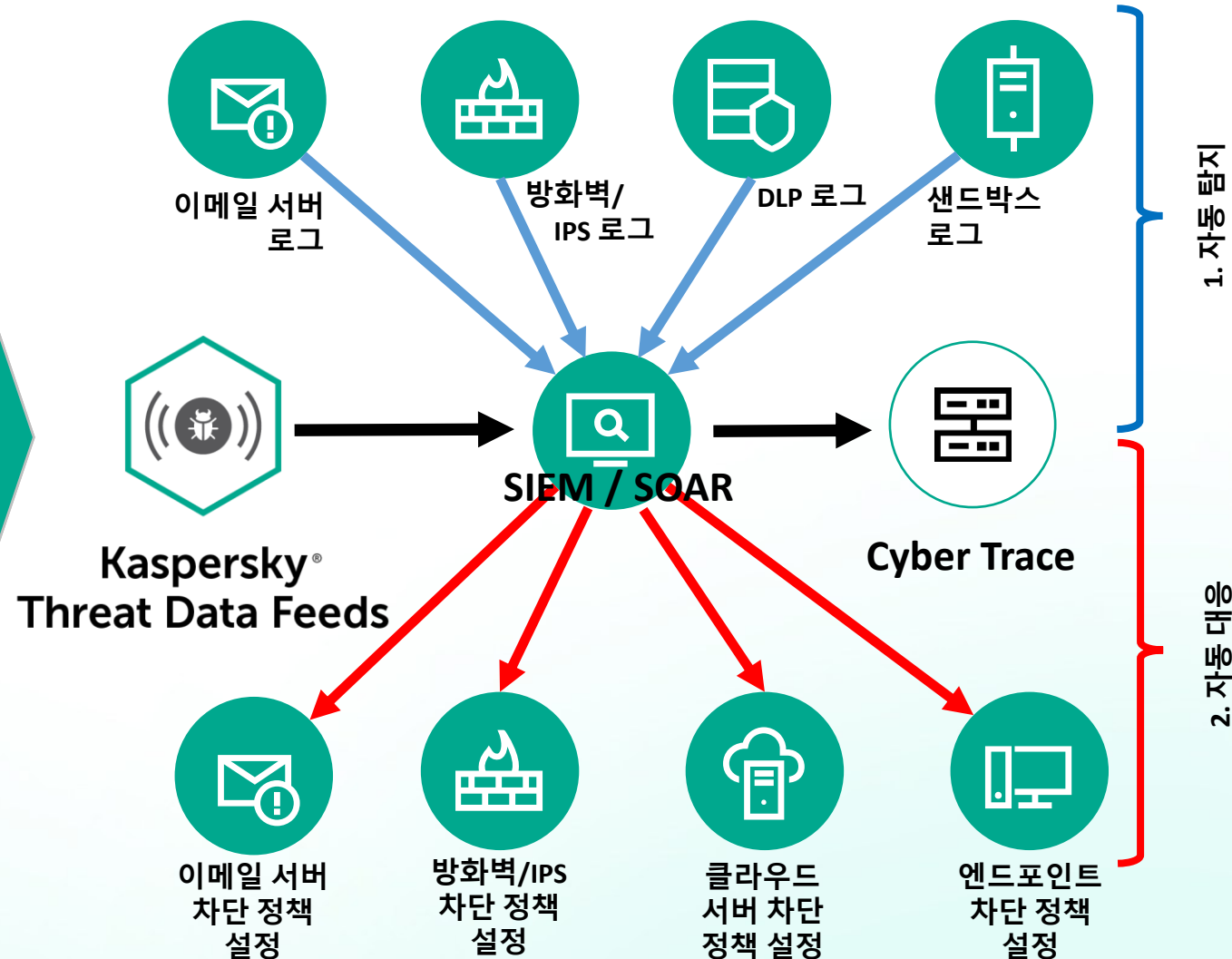
1. 자동 탐지

Kaspersky Threat Intelligence IOC Data Feeds를 SIEM / SOAR와 통합하여 위협 자동 탐지

- 1) 서버나 클라이언트에 심어져 있는 악성 Script가 공격용 트로이목마를 다운로드하는 행위 탐지.
- 2) 트로이목마가 공격자의 CnC 서버로 접속하여 데이터 유출, 파괴, 암호화를 위한 지령을 수신하는 행위 탐지.
- 3) 이메일 서버를 통한 공격 사전 단계의 악성 코드를 배포하는 행위 탐지.
- 4) 웹을 통한 공격 파일 다운로드 유인 행위 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

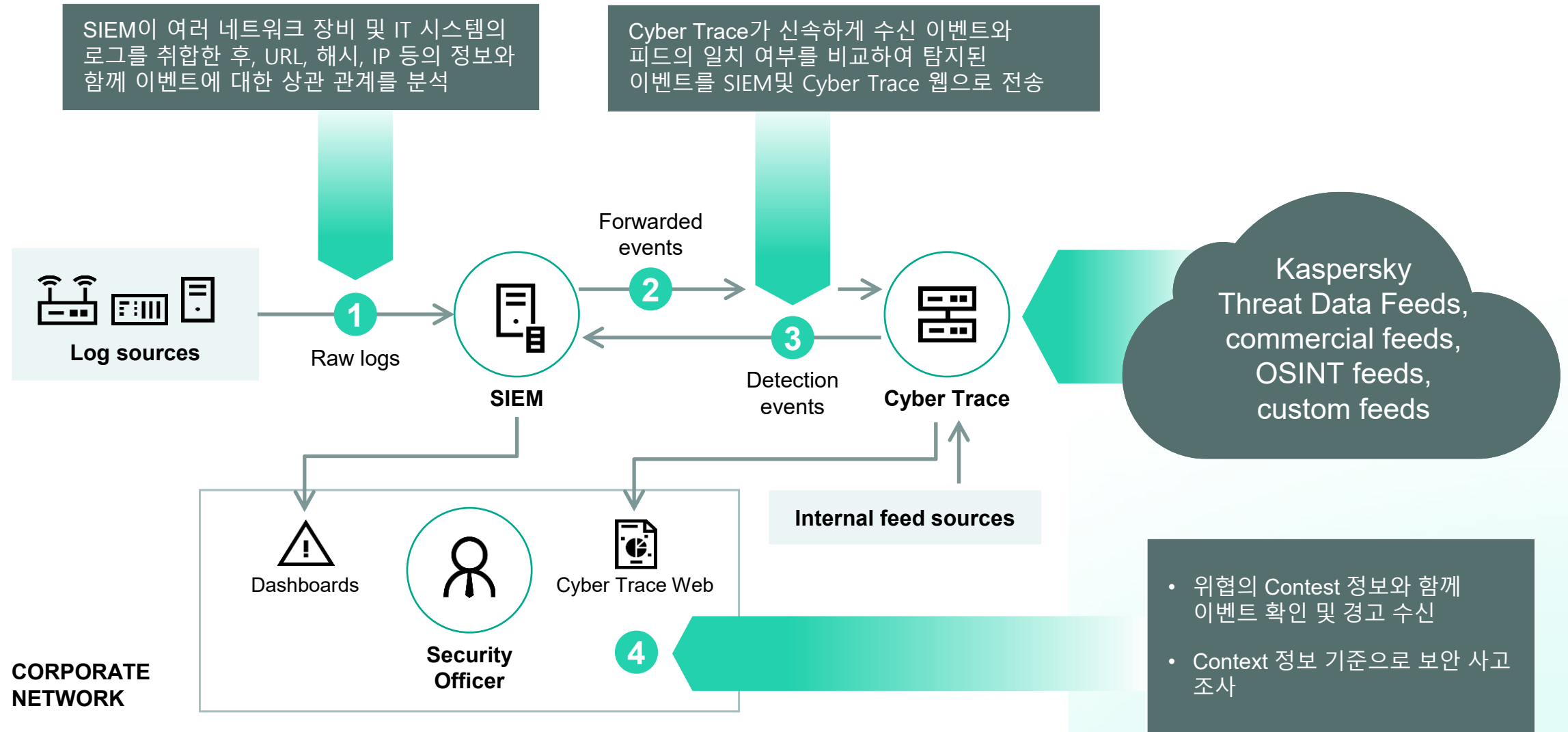


Network security controls



Kaspersky Threat Intelligence 주요 기능 2 - 위협 인텔리전스 플랫폼

보안 장비의 로그 실시간 분석

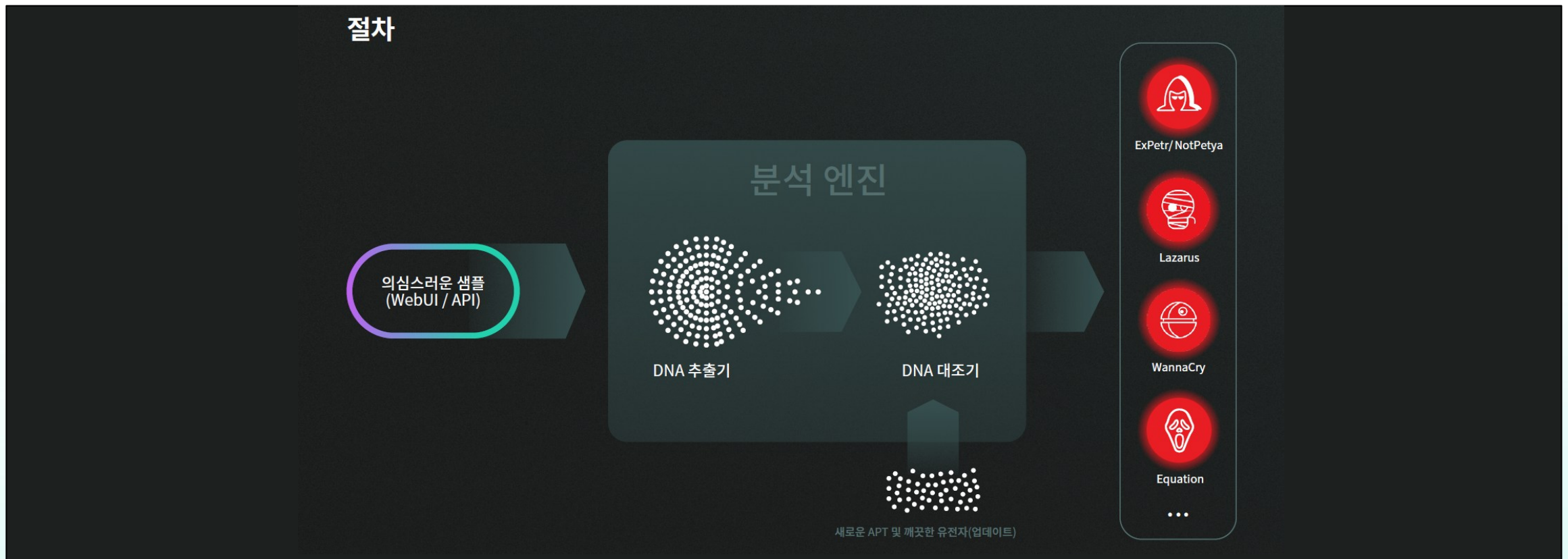


위협 분석 (Sandbox/Attribution Engine)

Kaspersky Threat Attribution Engine은 자동화된 방식으로

악성코드의 “유전자”를 분석하여 악성코드 기원, 위협 공격자, 알려진 APT 샘플과의 유사성에 대한 보고서 등 을 제공합니다. 또한 보안 팀이 자체적으로 보유하는 공격자 정보 및 샘플을 추가하는 기능을 통해 Kaspersky Threat Attribution Engine이 이를 학습하고 고객이 제공한 파일과 유사한 파일을 탐지할 수 있습니다.

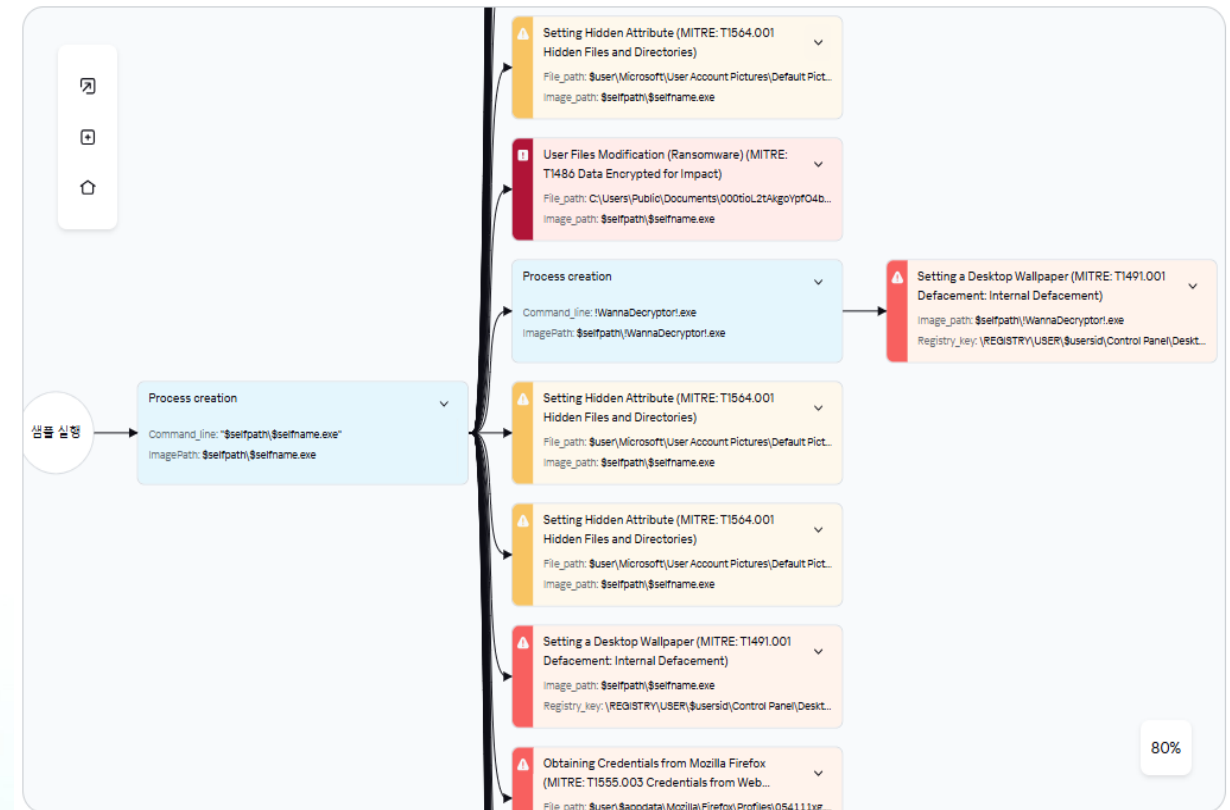
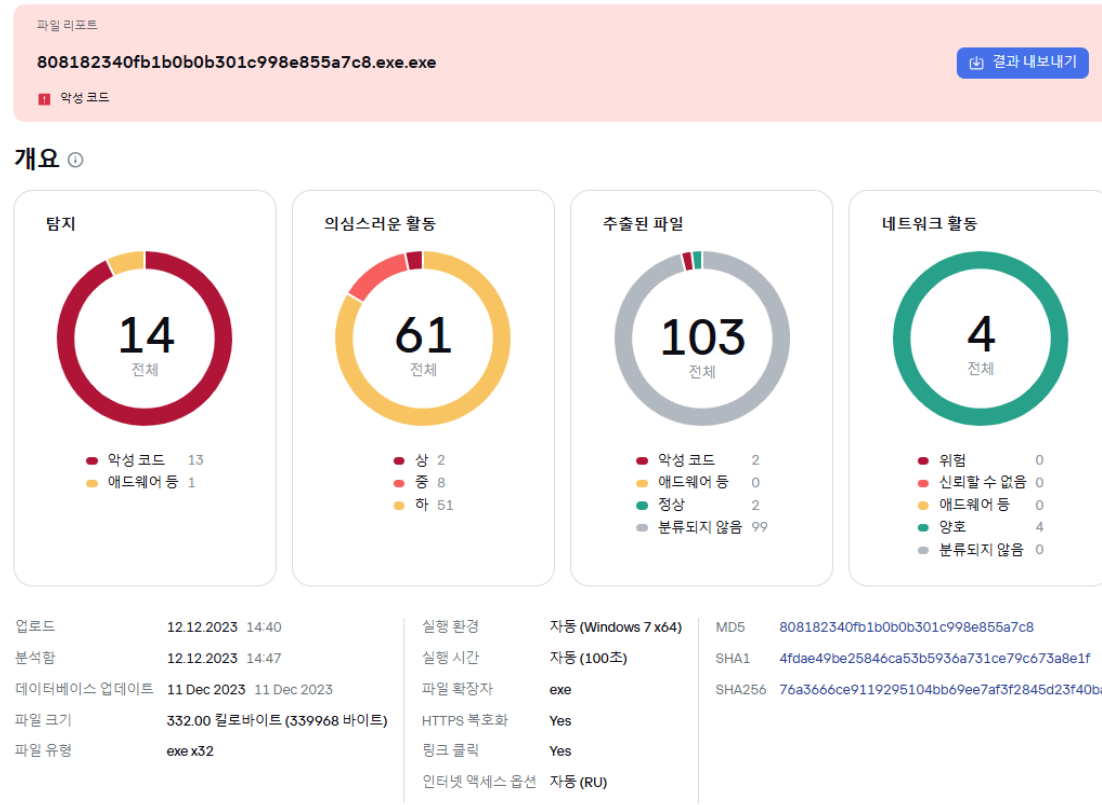
Threat Attribution Engine을 사용하면 과거에는 수년이 걸리던 추적 프로세스를 단 몇 초만에 완료할 수 있습니다.



위협 분석 (Sandbox/Attribution Engine)

Attribution Engine은 Kaspersky만의 독자적인 솔루션

1. Kaspersky는 지난 수년 간 Kaspersky Security Network으로부터 추출한 방대한 악성코드의 DNA를 분석하여 게놈 지도를 완성하였고, 이 게놈 지도로부터 유전자(Gene)를 분리하여 각각의 악성 코드의 유전체(Genome)를 완성
2. 이 유전체 정보와 분석 대상 파일에서 추출한 유전자형(Genotype)을 비교/분석하여 공격자와 그 배후 정보를 찾아 제공
3. Kaspersky는 매일 40만 개의 신규 악성코드를 발견하며, 실시간으로 게놈 지도를 업데이트



kaspersky

Demo

Threat Hunting 실무

• Facts about us

- > 25년 이상의 보안 사업
- > 5,000명의 전문가 보유
- > 전세계 **400,000,000**명의 사용자 보유
- > 전세계 **220,000**개의 기업 고객 보유

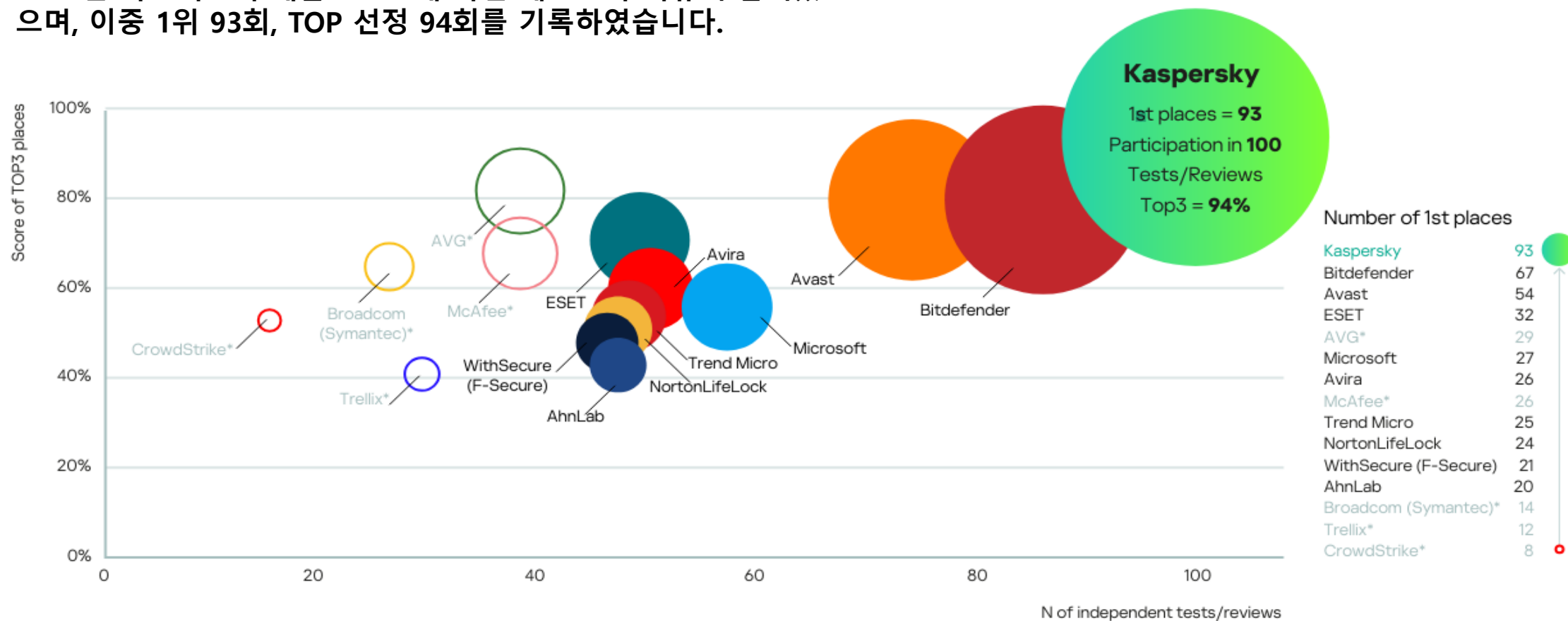


Why Kaspersky ?

최다 테스트 참여, 최다 상위권 선정

2023년 카스퍼스키 제품은 100개 독립 테스트와 리뷰에 참여했으며, 이중 1위 93회, TOP 선정 94회를 기록하였습니다.

1



MOST TESTED*
MOST AWARDED*
KASPERSKY PROTECTION

*[kaspersky.com/top3](https://www.kaspersky.com/top3)

- 기업용, 소비자용, 모바일용 제품에 대한 2023년 독립 테스트 요약 결과에 따르면.
- 요약에는 AV-Comparatives, AV-TEST, MRG Effitas, SE Labs, Testing Ground Labs, Virus Bulletin이 수행한 독립적인 테스트가 포함됩니다.
- 이러한 프로그램에서 수행되는 테스트는 알려진 위협, 알려지지 않은 위협 및 고급 위협에 대해 모든 보호 기술을 평가합니다.
- 원의 크기는 1위 달성 횟수를 반영합니다.
- 2013년부터 2023년까지 대부분 테스트를 거쳤습니다.
- *로 표시된 공급업체는 전체 테스트 횟수의 35% 미만에 참여했기 때문에 차트에 보완적으로 추가되었습니다.

카스퍼스키 글로벌 투명성 이니셔티브 (Global Transparency Initiative)



사이버 위협 관련 사용자 데이터 저장 및 처리

유럽, 북미 및 라틴 아메리카, 중동 및 아시아 태평양 지역의 국가에 있는 카스퍼스키 제품 사용자로부터 수신된 악성 및 의심스러운 파일은 스위스에서 처리 및 저장됩니다.



투명성 센터

고객, 파트너 및 정부 이해관계자가 회사의 코드, 소프트웨어 업데이트 및 위험 탐지 규칙과 기타 활동을 검토할 수 있는 시설입니다.



독립 리뷰

내부 프로세스에 대한 정기적인 타사 평가를 통해 카스퍼스키 프로세스 및 시스템의 보안을 확인합니다:

- 정기 SOC 2 감사
- 회사의 데이터 시스템에 대한 ISO 27001 인증



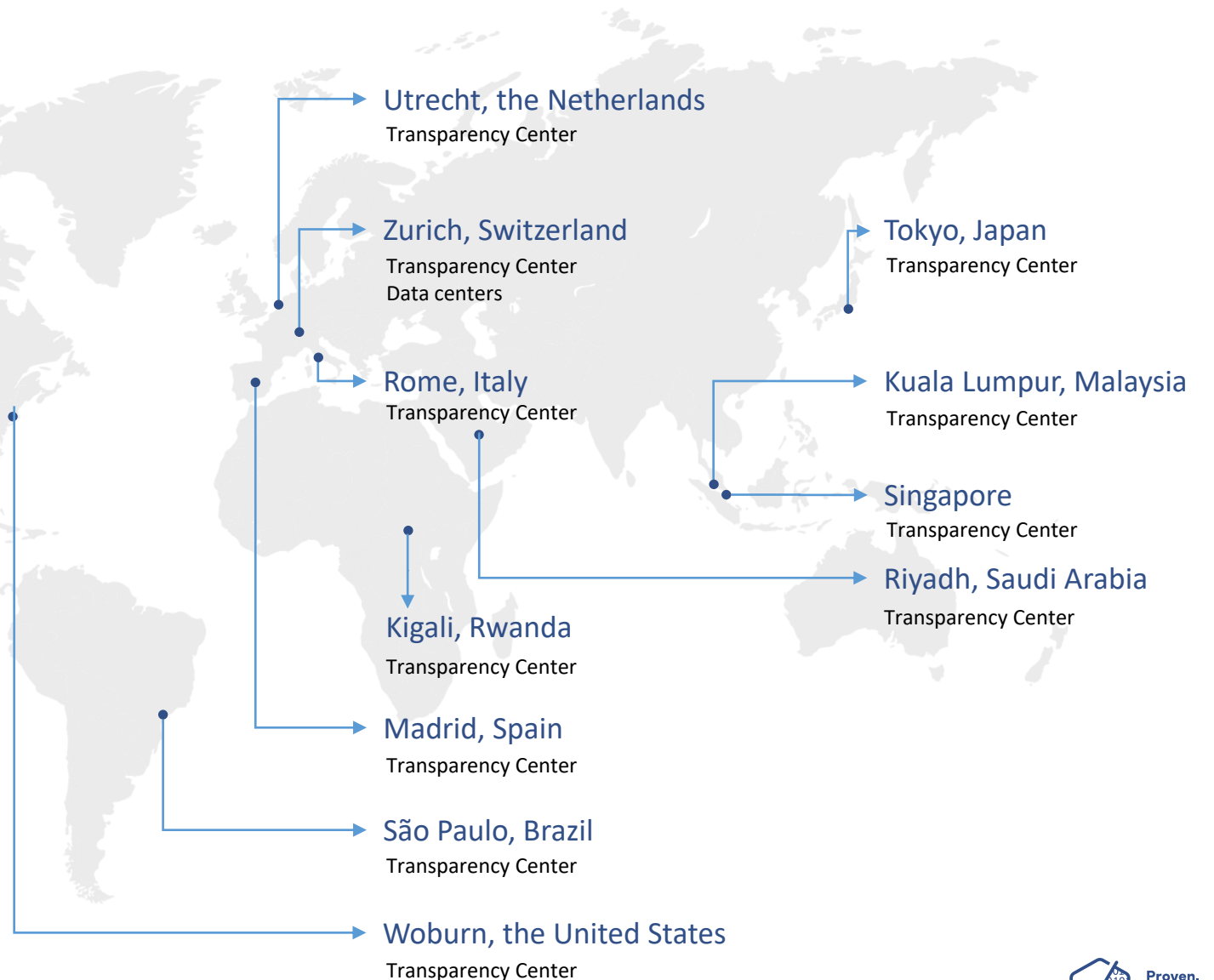
버그 바운티 프로그램

가장 중요한 취약점에 대한 버그 포상금을 최대 10만 달러로 인상하여 보안 연구원들이 솔루션의 보안을 보장하기 위해 자체적으로 수행하는 작업을 보완할 수 있도록 했습니다.



투명성 보고서

카스퍼스키가 정부 및 법 집행 기관의 요청과 자체 사용자의 개인 데이터 관련 요청에 어떻게 대응하는지에 대한 정기적인 업데이트를 제공합니다.

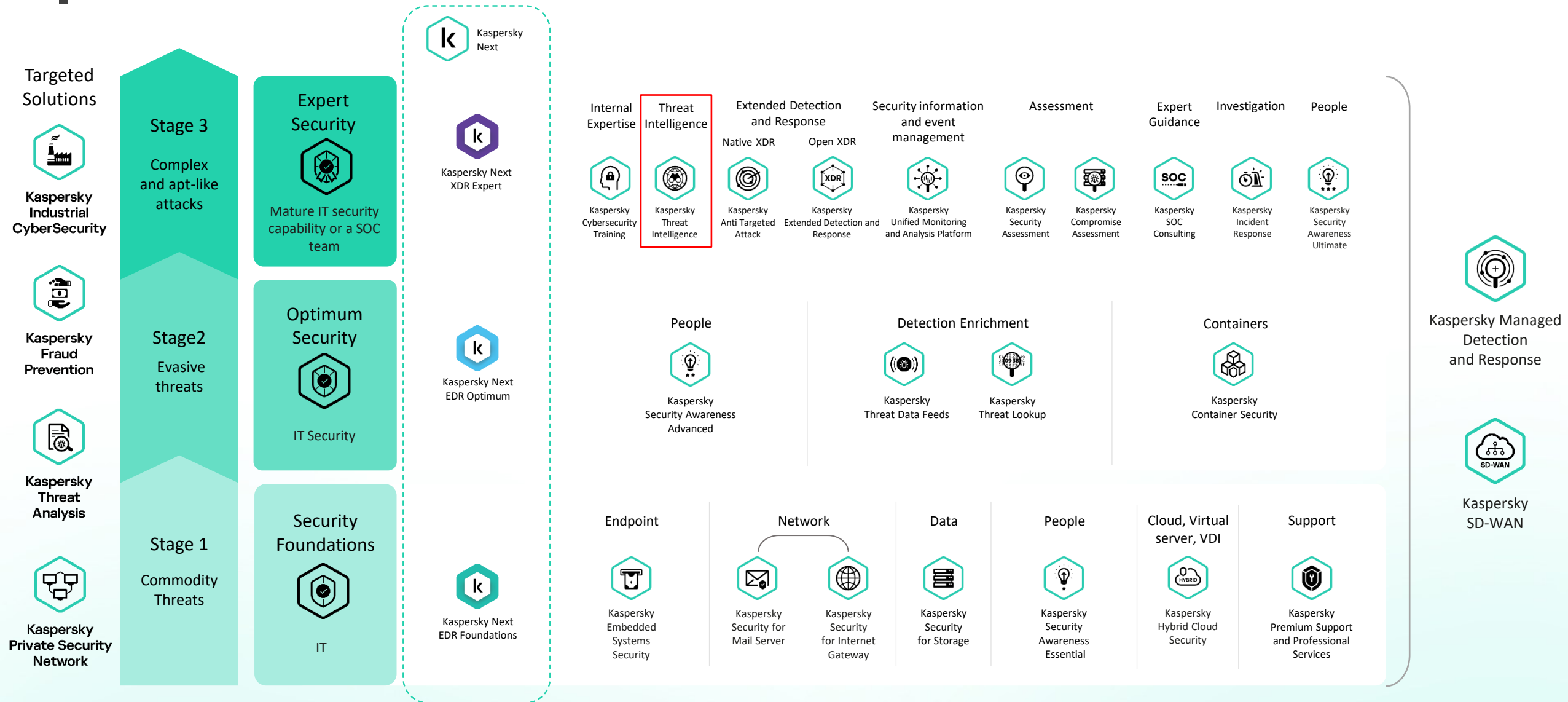


글로벌 IT 보안 커뮤니티에서의 역할

당사는 글로벌 IT 보안 커뮤니티, 인터폴과 같은 국제기구, 전 세계 법 집행 기관 및 CERT와 함께 공동 작전 및 사이버 범죄 조사에 참여하고 있습니다.

[Learn more](#)[Learn more](#)[Learn more](#)[Learn more](#)

카스퍼스키 엔터프라이즈 솔루션



Why Kaspersky Threat Intelligence?

No	Kaspersky 특징점
1	위협 인포메이션을 넘어 각각의 IoC에 대한 Context까지 제공하는 진정한 위협 인텔리전스
2	전 세계 1억 2천만 명의 자발적인 고객 참여 Network로부터 실시간으로 정확하고 풍부한 위협 정보 수집
3	카스퍼스키만의 특허 시스템인 봇팜(알려진 모든 봇넷 제품군, 허니팟 등을 모니터링)에 의한 풍부한 위협 정보
4	매일 40만개의 신규 악성 코드를 탐지하고 있는 기술력과 조직(2,000명 이상의 관련 연구원)
5	폐쇄망에서도 완벽 운영 가능한 유연한 솔루션 설계
6	조직 내부에서 독자적으로 구축 가능한 Private CTIP(Cyber Threat Intelligence Platform) 제공
7	특허받은 Kaspersky만의 독자 솔루션인 공격툴의 DNA를 분석한 게놈지도에 의한 악성코드 유전체 분석 도구
8	업계 유일의 OT에 대한 위협 인텔리전스 제공
9	Microsoft MAAP (Microsoft Active Protection Program)의 최고 기여자



저희의 **미션**은 간단합니다.
바로 보다 **안전한 세상**을 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