PASCON 2022

2022 공공 · 금융 · 기업 정보보안&개인정보보호 컨퍼런스

숨겨진 위협 헌팅으로 활용하는 CTI 현업 사례

강민석
Kaspersky Korea

kaspersky

kaspersky

진화하고 있는 위협

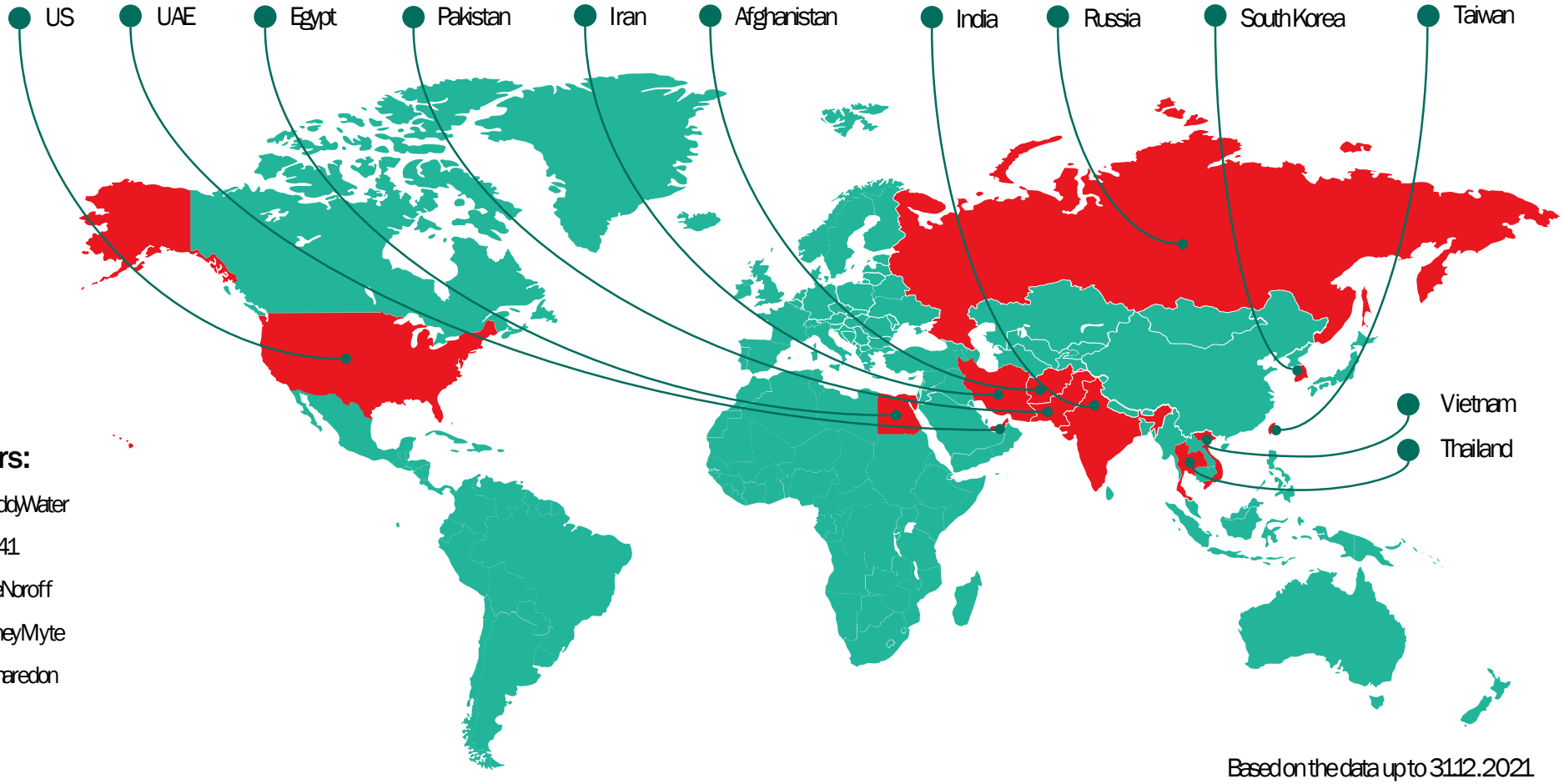
Advanced persistent threat landscape in 2021

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:



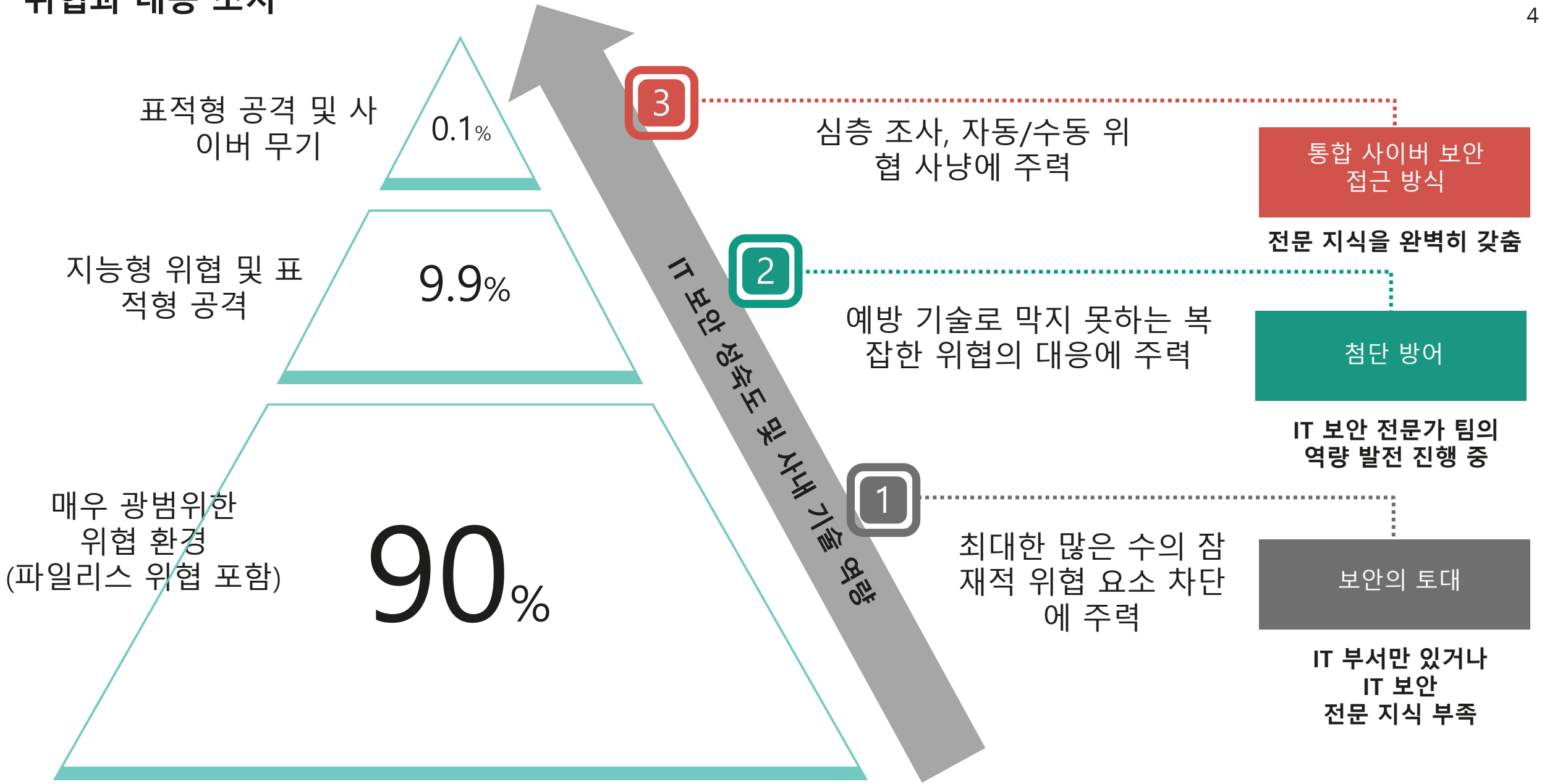
Top 10 significant threat actors:

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

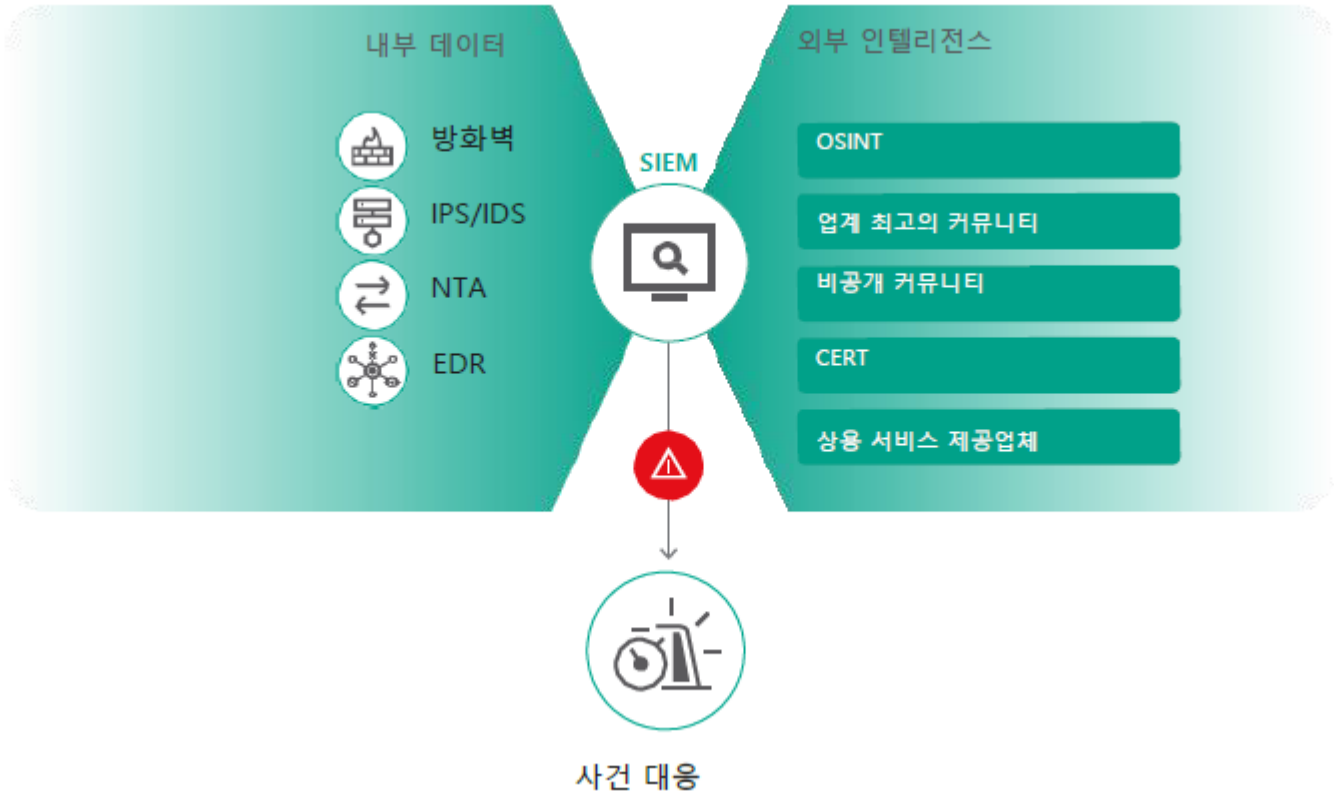
위협과 대응 조치


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

kaspersky

Threat Intelligence 란?

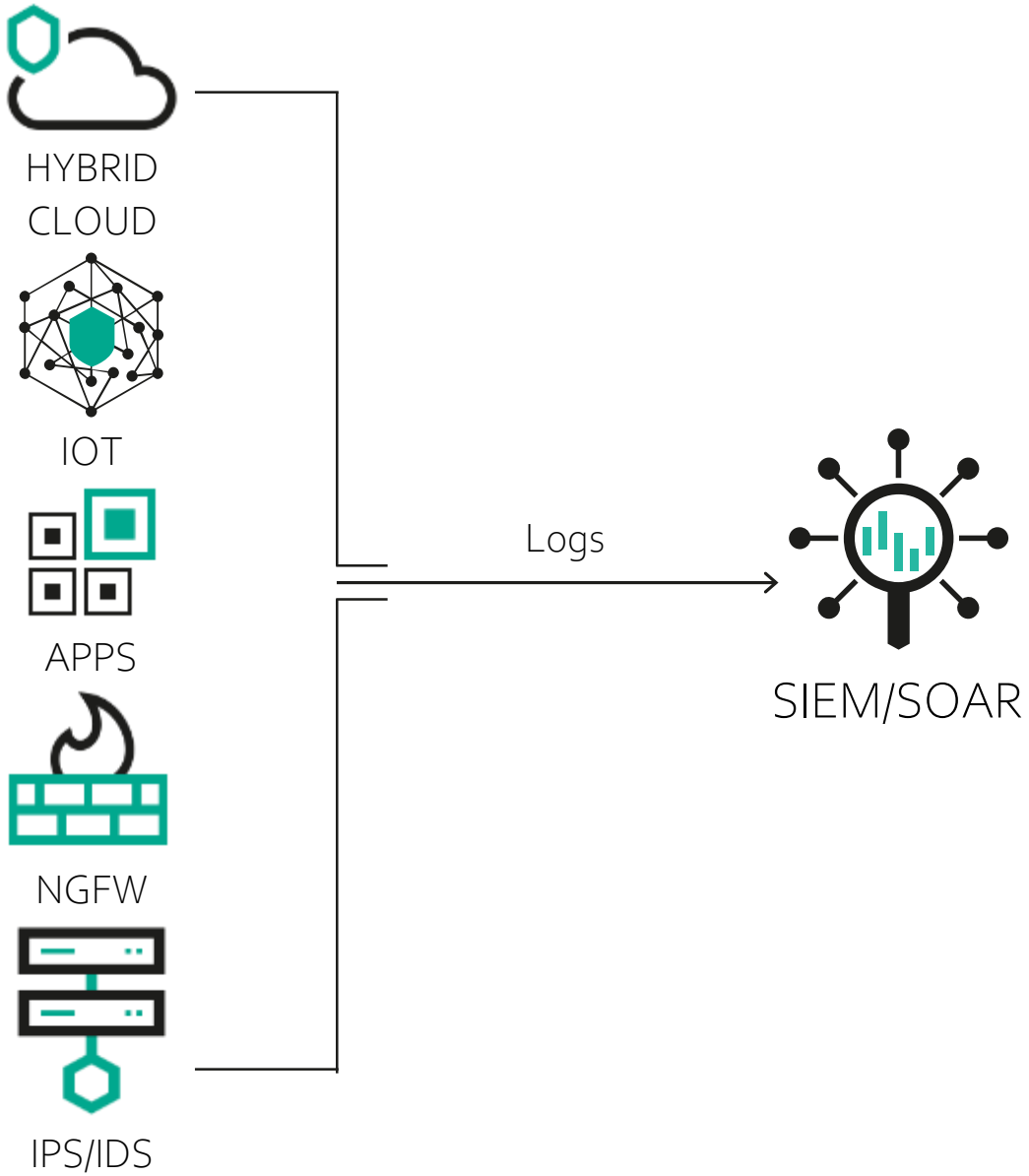
SOC & SIEM



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

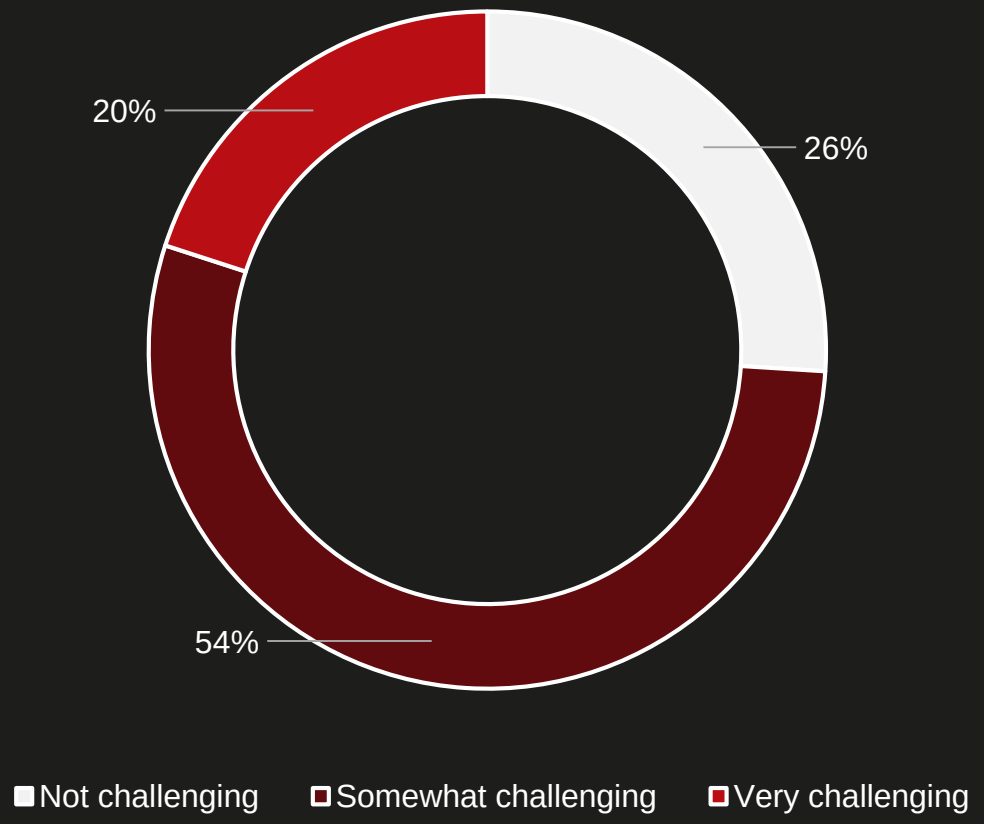
비효율적인 사고 대응으로 인해
높은 복구 비용 발생

조직 내에 아직 발견되지 않은 위협이 존재

포괄적인 위협에 대한 개요 부족으로 인해
효과적인 보안 프로그램 개발 난항

증가하는 보안 경고의 수

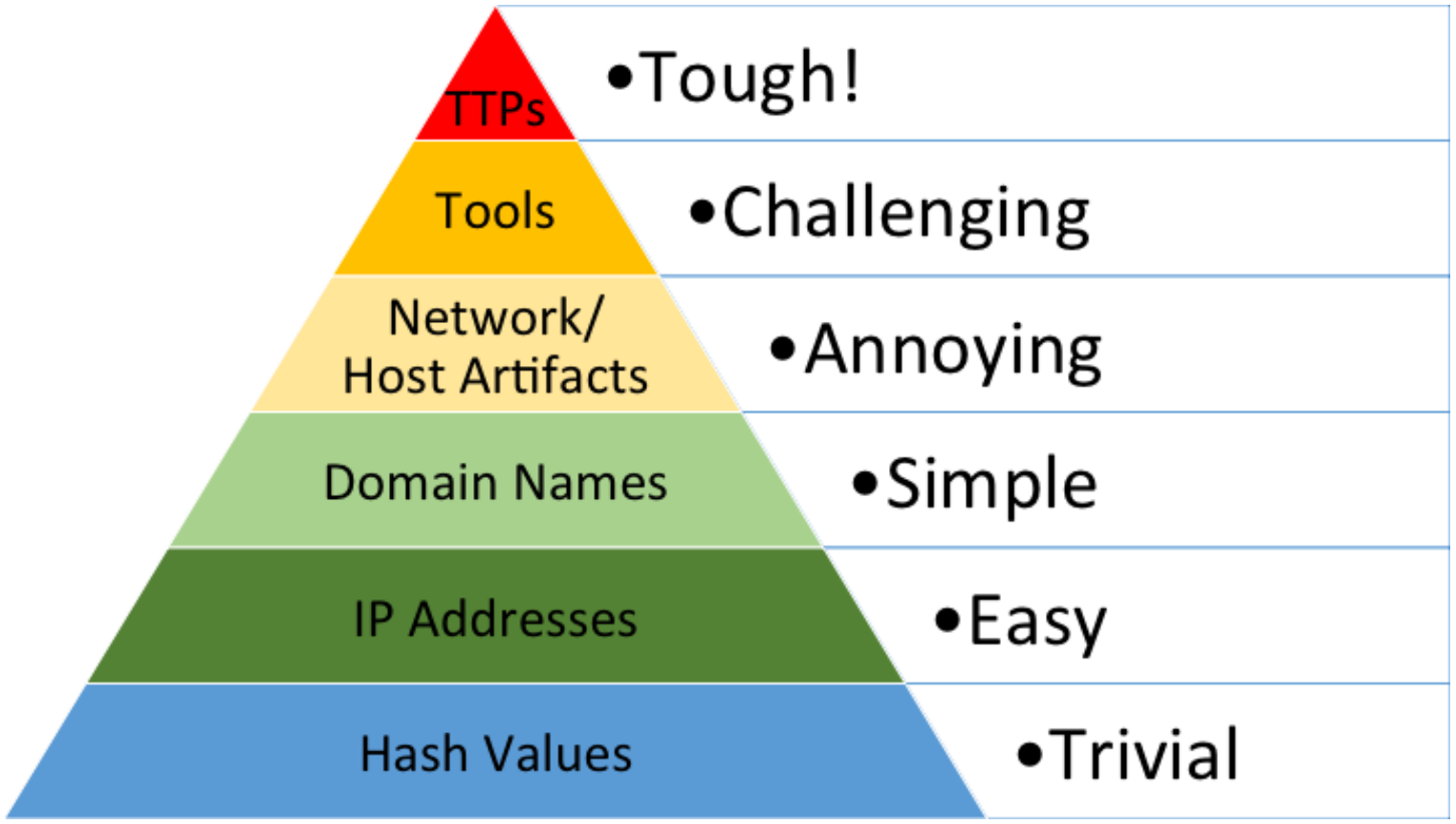
경고 조정의 당면 과제



많은 위협 경고가 조사되지 않거나 해결되지 않음

Source: Cisco 2018 Capabilities Benchmark Study

Information 과 Intelligence 의 차이



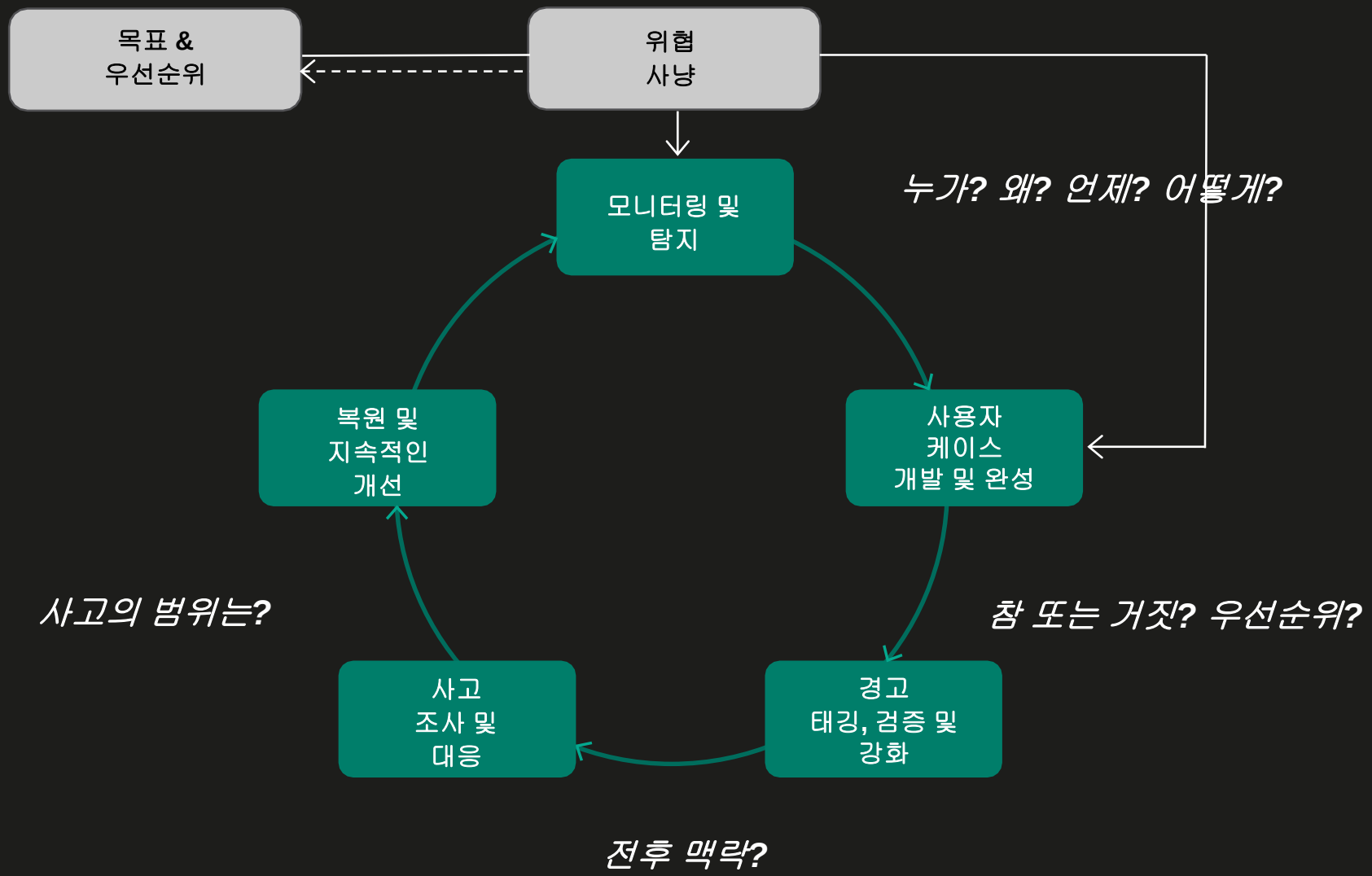
Threat **Intelligence**

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

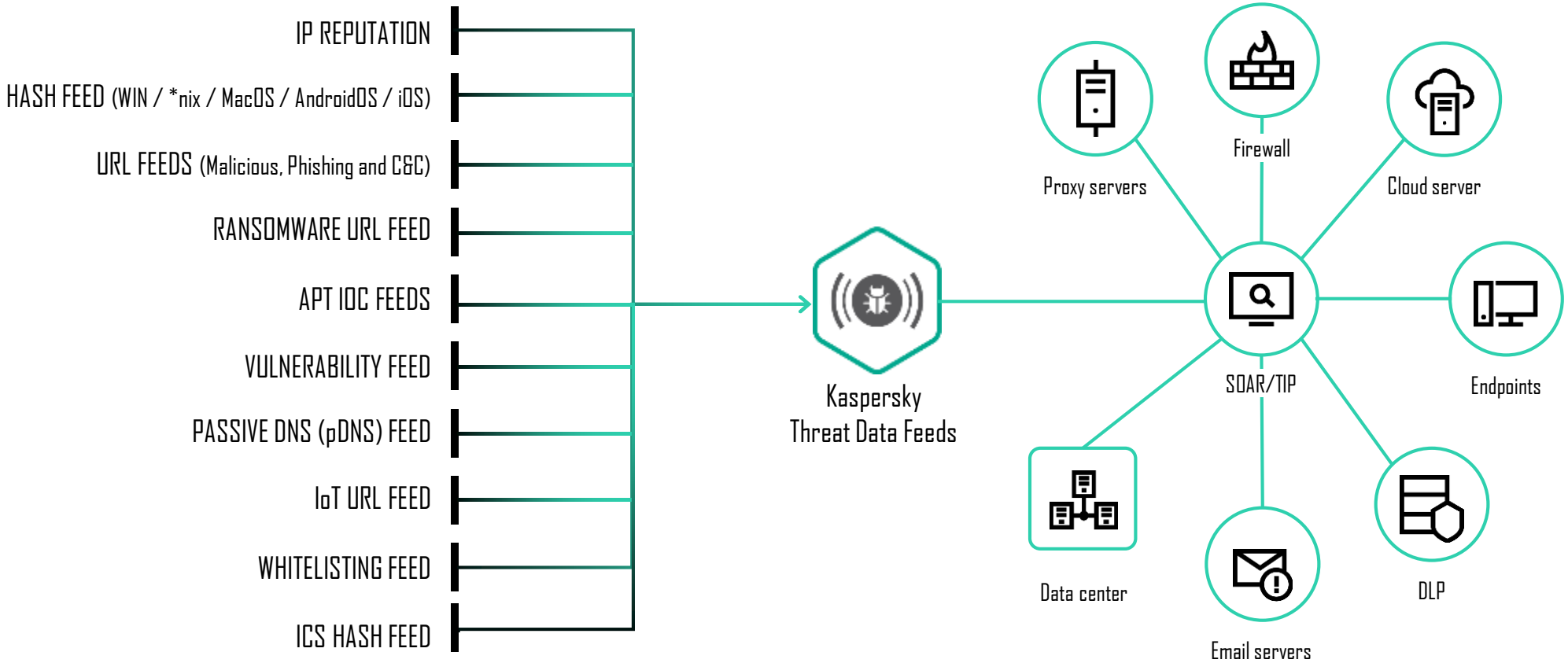
Threat Intelligence가 제공하여야 할 기능

Threat Data Feeds

오탐률이 0에 가깝고 지속적으로 업데이트 되는 위협 데이터

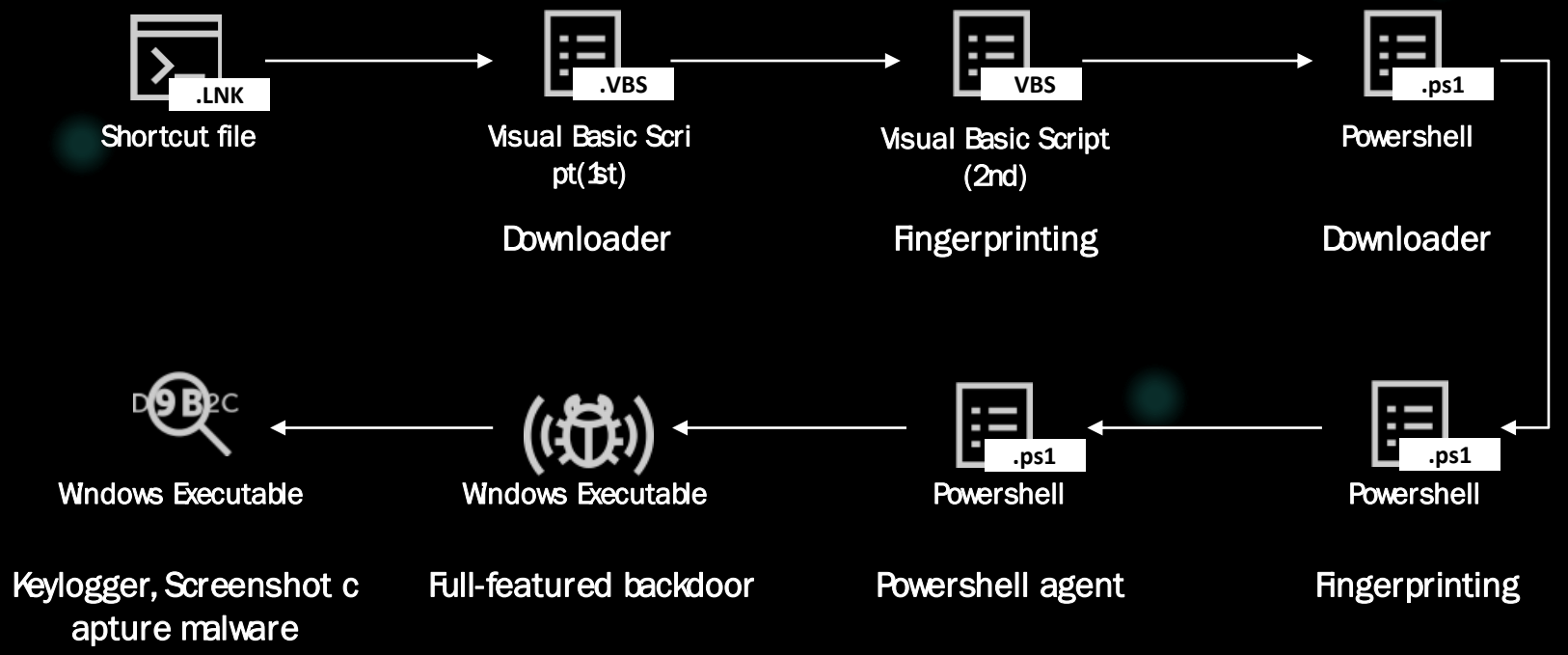
풍부하고 의미있는 전후사정 정보로 인해 인텔리전스를 즉시 실행

표준 전달 형식과 메커니즘을 통해 보안 제어에 쉽게 통합 가능



Latest Threat Landscape: Multi-stage infection

BlueNoroff's SnatchCrypto campaign



Important points we consider: Full-context understanding

781a20f27b72c1c901164ce1d025f641
483e3e0b1dceb4a5a13de65d3556c3fe
5e44deca6209e64f4093beae92db0c93
c16977fefbdc825a5c6760d2b4ea3914
09bca3ddbc55f22577d2f3a7fda22d1c
0eb71e4d2978547bd96221548548e9f0
da599b0cde613b5512c13f299fec739e
0c9170a2584ceeddb89e4c0f0a2353ed
5053103dd5d075c1dc54edf1f8568098
536bae311c99a4d46f503c68595d4431
3078265f207fed66470436da07343732
15f1ae1fed1b2ea71fdb966182363c6
56fe283ca3e1c166719icc7764c260b6
850751de7b8e158d86469d22ad1c3101
1a8282f73f393656996107b6ec038dd5
2ea2ceab158881096id2fc545e2f957e
561f7041l449b327e3f19d81bb2cea08
3812cdc4225182326b1425c9f3c2d50b
5af886030204952ae243eedd25dd43c4
....
dff21849756eca89ebfaa33ed3185d95
e18dd8e61c736cfc6fff86b07a352c12
e546b851ac4fa5a111d10f40260b1486
e6e64c511f935d31a8859e9f3147fe24
ea7ed84f7936d4cbafa7cec51fe39cf7
f414f6590636037a6ec92e4d951bdf55
4e207d6e930db4293a6d720cf47858fc

Hard to find a connection

00a145e8f67a92b01ce4d85a0ed6bd77
ff28ec14ec926b9892c61b9bf154a910
97e5c0fe8089da97665a22975e2c86de
4fbff7f0f62b26963b56c0fc23486891
4bb579d59830579be9ead9f74a55001e
fcfd14b030e6b5d75e777ace530dad9
1d0fc2fla6eb2b2bfa166a613ca871f0
db91826cb9f2ad6edfed8d6bab5beff
9c592a22acdfb750c440fda31da4996c
2934a7a0dfaf2ebc81b1f089277129c4
....
4fbff7f0f62b26963b56c0fc23486891
4bb579d59830579be9ead9f74a55001e
aafc80ff2afc71b0d5abd6c8d2809e65
9850b24f8d70ad957f328961170e2d40
58495a2083065b36040eea288a9d5e17
fcfd14b030e6b5d75e777ace530dad9
1fb25f72e4eb26b0df154de28dbff74c
1b1acc7f27717905e7094f338f81db9f
3776d4a24213972b54b9ed3360ac7883
c93f3bb4f7b19f5eb6f736f2659c4dae
9084620e0219c035d60d395be1bf4cae

Files on Virustotal
Files not on Virustotal

f29be5c7e602e529339fda35ff91bd39
f194e074e7d73c544eebb70e2e2785a1

ce09cdb7979fb9099f46dd33036b9001
f7f4aa55a2e4f38a6a3ea5a108baedf5

589f1bb4da89cfd4a2f7f3489aa426a9
ae52b28b360428829c4fcdc14e839f19
735725191591b0c27af8dbbaf25ef1cc0
8ae6aa90b5f648b3911430ff4c92440b
aef2a668dd9f254c42fcd803c7645ed1


Shortcut file

Visual Basic Script

Powershell


Backdoor


Stealer

42/62	1/2	1/5	15/38	0/2

Low visibility

kaspersky

GREAT

Important points we consider: Full-context understanding

	Initial Access	Execution	Persistence	Priv	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

위협 관리 플랫폼

위협 탐지 DB와 분석 플랫폼을 이용한 다단계 킬체인 구축

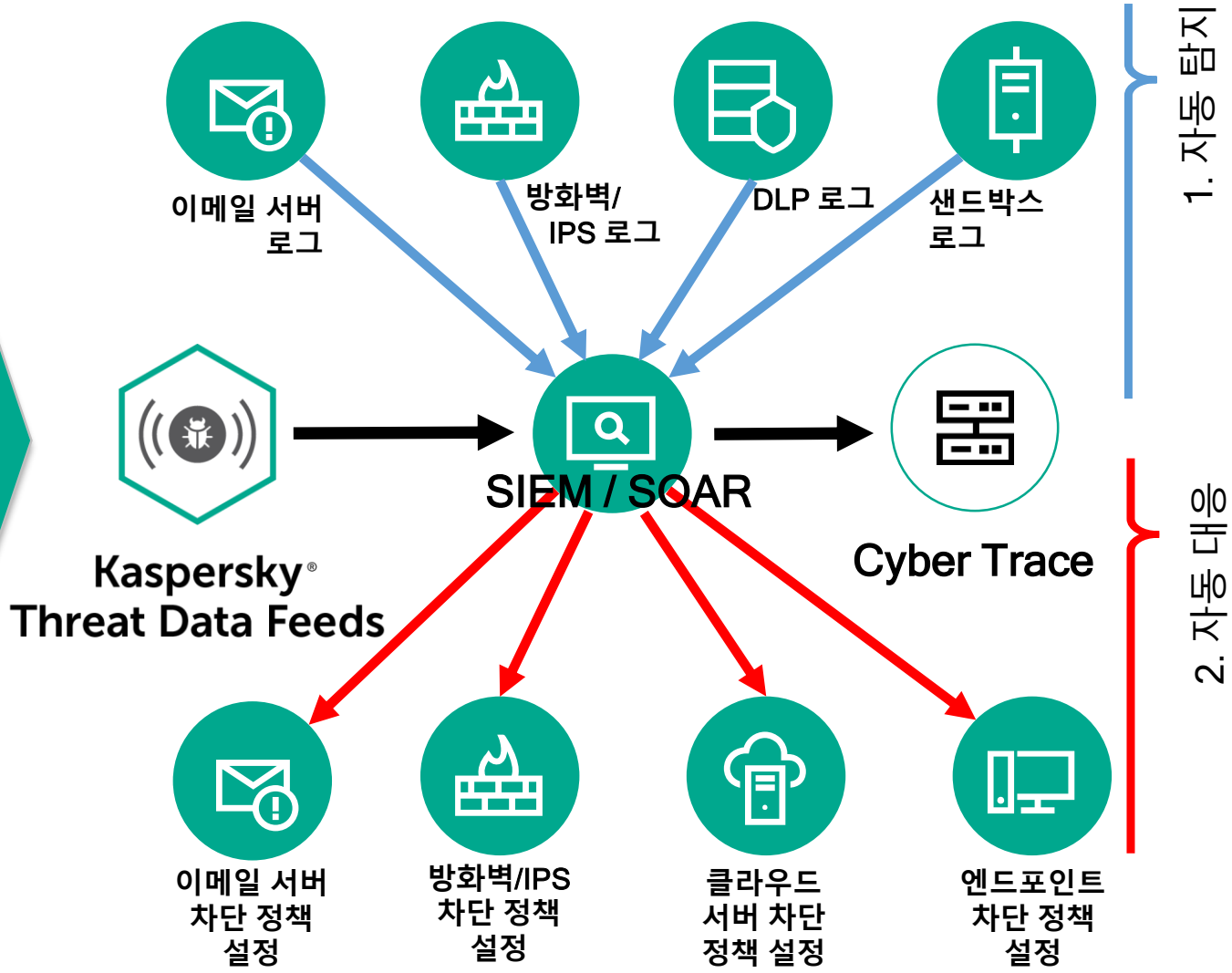
1. 자동 탐지

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.



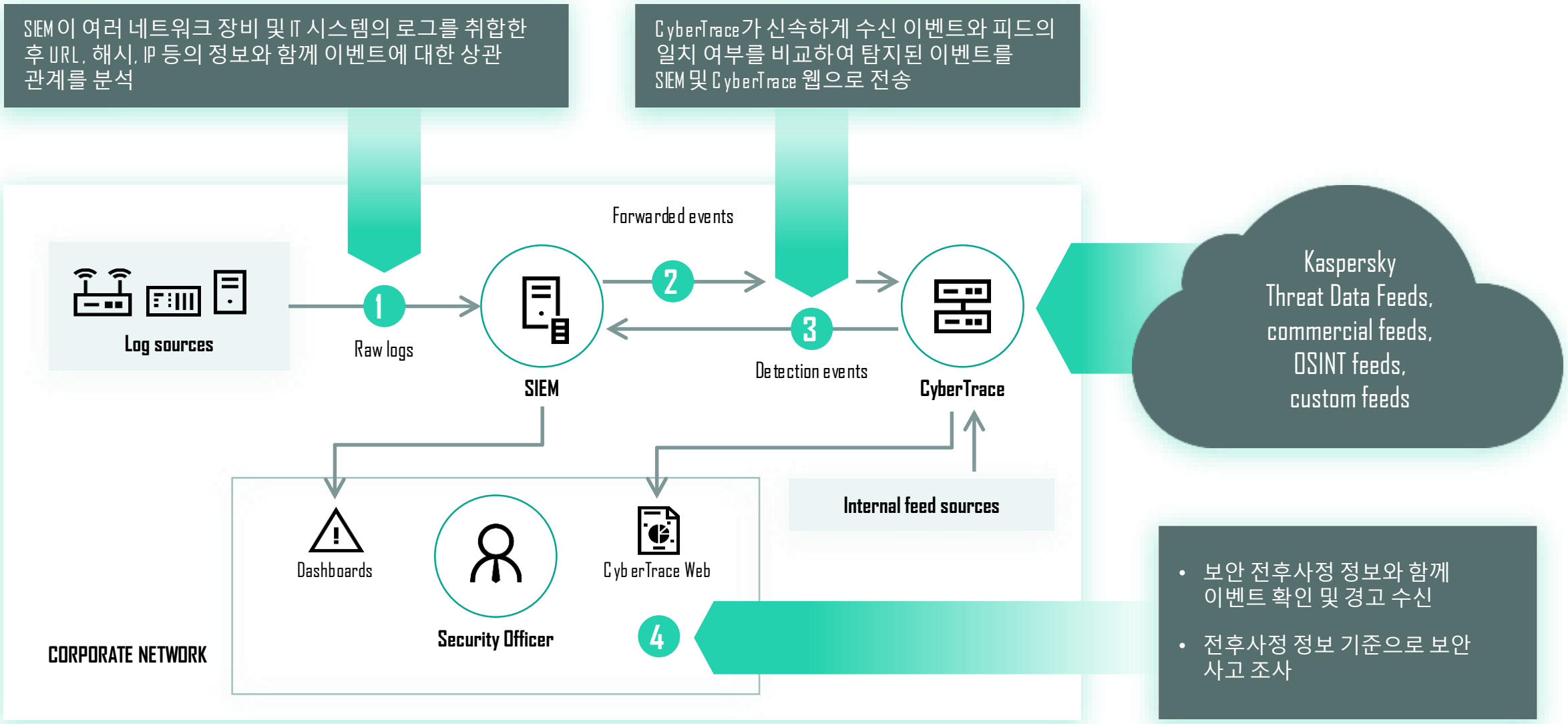
SIEM / SOAR와의 연동시 고려 사항

SIEM/SOAR/IRP

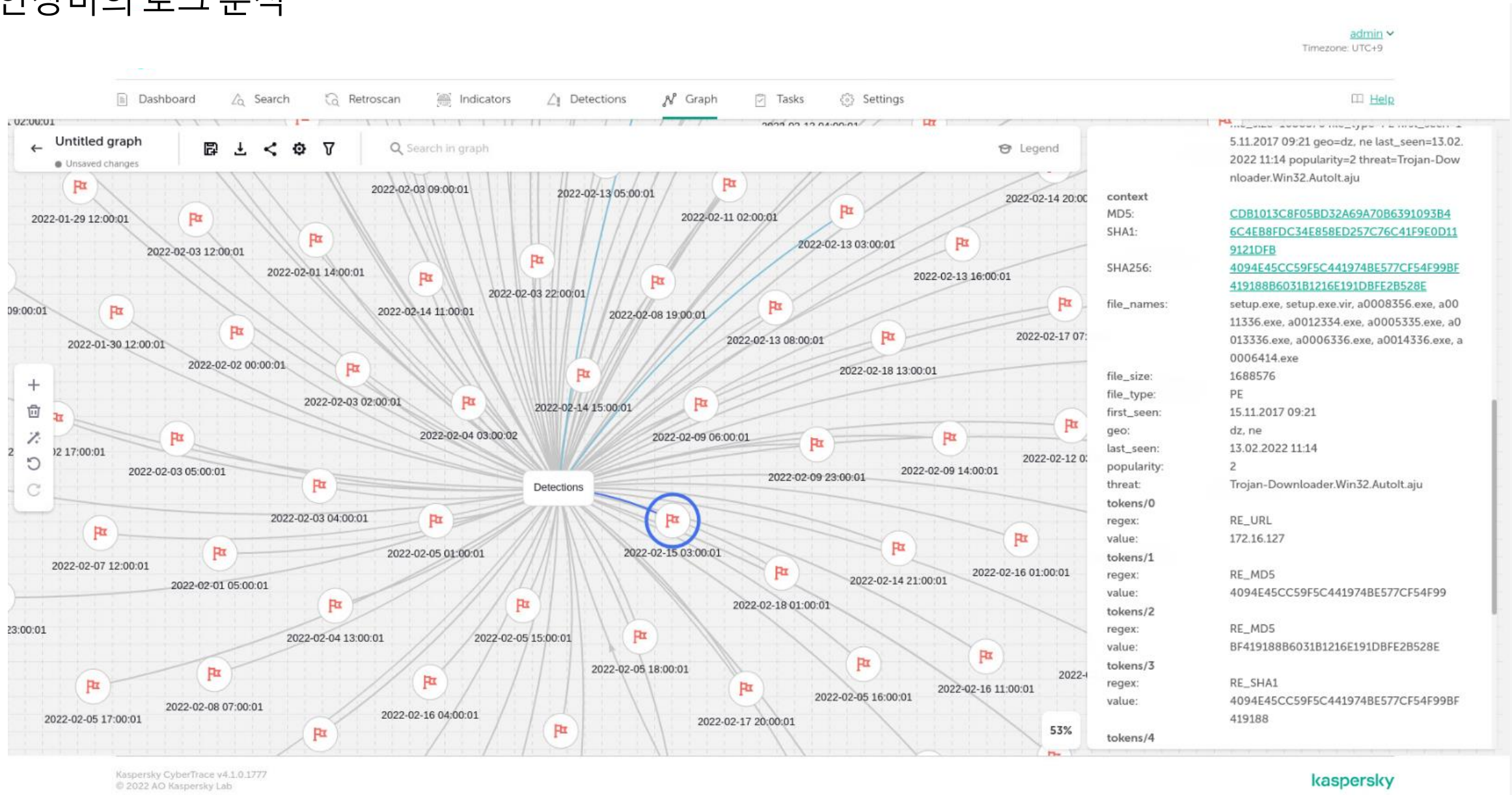
Threat Intelligence Platforms

Network security controls

보안장비의 로그 분석


SIEM이 여러 네트워크 장비 및 IT 시스템의 로그를 취합한 후 URL, 해시, IP 등의 정보와 함께 이벤트에 대한 상관 관계를 분석
CyberTrace가 신속하게 수신 이벤트와 피드의 일치 여부를 비교하여 탐지된 이벤트를 SIEM 및 CyberTrace 웹으로 전송
Forwarded events
Log sources
1
Raw logs
SIEM
2
3
Detection events
CyberTrace
Kaspersky Threat Data Feeds, commercial feeds, OSINT feeds, custom feeds
Internal feed sources
Dashboards
Security Officer
CyberTrace Web
CORPORATE NETWORK
4
• 보안 전후사정 정보와 함께 이벤트 확인 및 경고 수신
• 전후사정 정보 기준으로 보안 사고 조사

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
2022-02-17 07:
2022-01-30 12:00:01
2022-02-02 00:00:01
2022-02-13 08:00:01
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

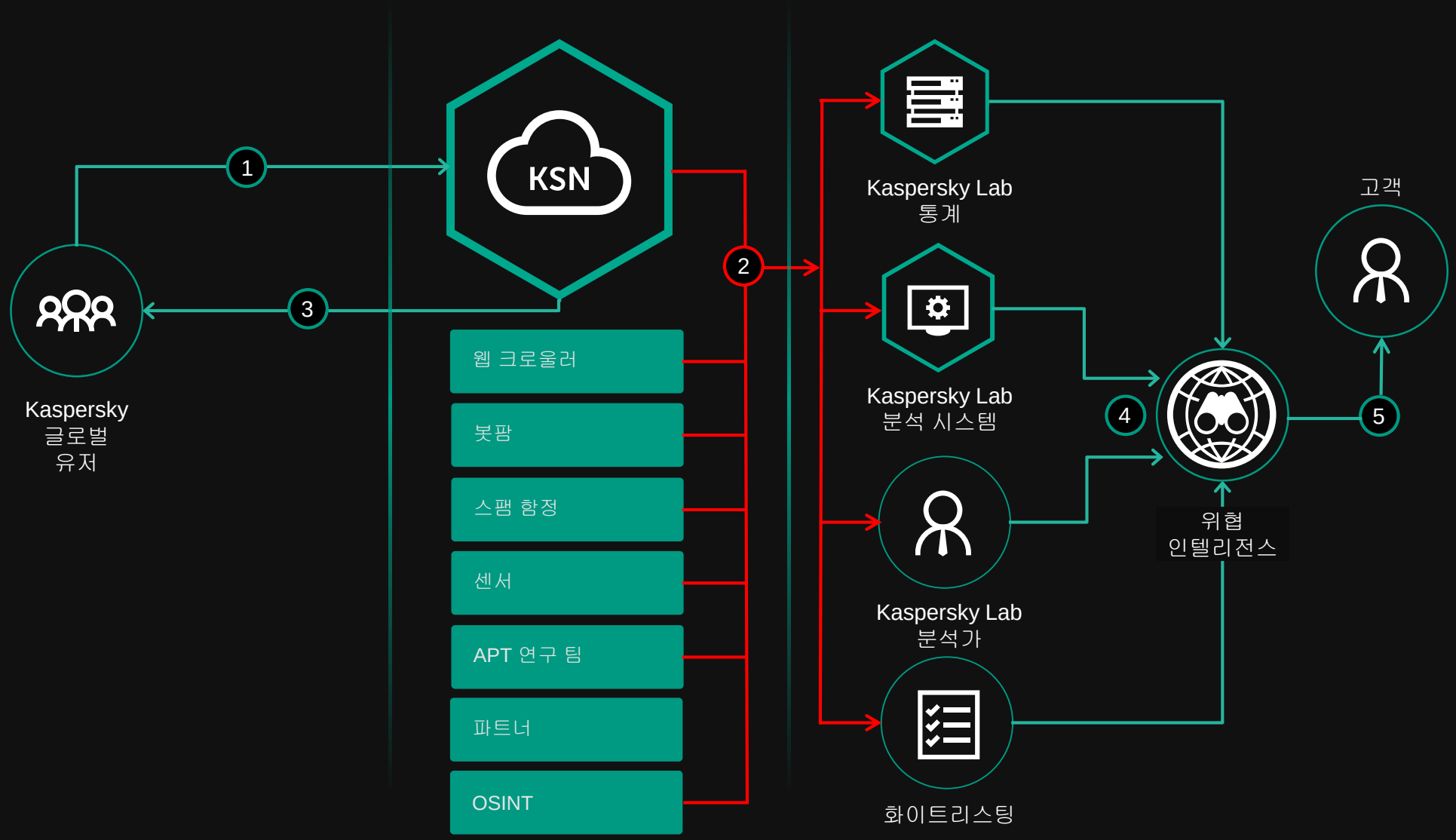
kaspersky

Demo
로그분석 실무

kaspersky

Kaspersky Threat Intelligence

Kaspersky 위협 인텔리전스의 정보 출처



Threat intelligence sources

GREAT
GLOBAL RESEARCH & ANALYSIS TEAM


Christian Funk
Head of GReAT, Germany
GReAT Europe


Marco Preuss
Director of GReAT Europe
GReAT Europe

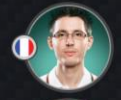

David Emm
Principal Security Researcher
GReAT Europe


Dani Creus
Senior Security Researcher
GReAT Europe


Marc Rivero
Senior Security Researcher
GReAT Europe


David Jacoby
Senior Security Researcher
GReAT Europe

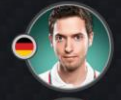

Jornt van der Wiel
Senior Security Researcher
GReAT Europe


Ivan Kwiatkowski
Senior Security Researcher
GReAT Europe


Pierre Delcher
Senior Security Researcher
GReAT Europe


Paul Rascagneres
Senior Security Researcher
GReAT Europe


Mark Lechtik
Senior Security Researcher
GReAT Europe


Ariel Jungheit
Senior Security Researcher
GReAT Europe


Giampaolo Dedola
Security Researcher
GReAT Europe

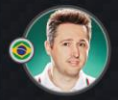

Matthias Weckbecker
Security Researcher
GReAT Europe

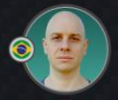

Aseel Kayal
Security Researcher
GReAT Europe


Kurt Baumgartner
Principal Security Researcher
GReAT US


Dmitry Bestuzhev
Director of GReAT LatAm
GReAT LatAm


Roberto Martinez
Senior Security Researcher
GReAT LatAm


Fabio Assolini
Senior Security Researcher
GReAT LatAm


Fabio Marenghi
Senior Security Researcher
GReAT LatAm


Santiago Pontiroli
Security Researcher
GReAT LatAm

APAC

Europe

Eastern Europe

Middle East & Africa

North America

Russia

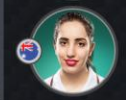
LatAm


Costin Raiu
Director
GReAT


Dan Demeter
Security Researcher
GReAT EEMEA


Vitaly Kamluk
Director of GReAT APAC
GReAT APAC


Seongsu Park
Senior Security Researcher
GReAT APAC


Noushin Shabab
Senior Security Researcher
GReAT APAC

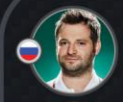

Saurabh Sharma
Senior Security Researcher
GReAT APAC

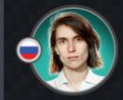

Suguru Ishimaru
Security Researcher
GReAT APAC

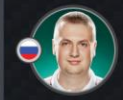

Mohamad Amin Hasbini
Director of GReAT META
GReAT META

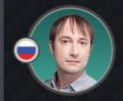

Maher Yamout
Senior Security Researcher
GReAT META

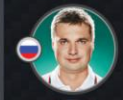

Abdessabour Arous
Security Researcher
GReAT META

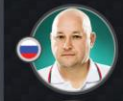

Sergey Novikov
Deputy Director
GReAT

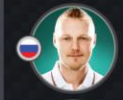

Maria Namestnikova
Head of Research Center
GReAT Russia

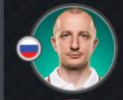

Igor Kuznetsov
Chief Security Researcher
GReAT Russia

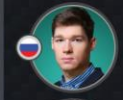

Victor Chebyshev
Lead Security Researcher
GReAT Russia


Sergey Mineev
Principal Security Researcher
GReAT Russia


Sergey Belov
Principal Security Researcher
GReAT Russia


Konstantin Zykov
Senior Research Developer
GReAT Russia


Denis Legezo
Senior Security Researcher
GReAT Russia


Boris Larin
Senior Security Researcher
GReAT Russia

Dmitry Galov
Security Researcher
GReAT Russia

Alexey Firsh
Security Researcher
GReAT Russia

Leonid Bezvershenko
Junior Security Researcher
GReAT Russia

Georgy Kucherin
Intern
GReAT Russia

GReAT팀을 주축으로 ICS Cert 및 멀웨어 대응팀까지 모두 1000명 이상의 연구팀이 Threat Intelligence에 기여합니다.

kaspersky

kaspersky

감사합니다.