위협 인텔리전스 기반의 보안 운영 및 SIEM 연계 사례 소개

HangRo Lee (hangro.lee@kaspersky.com)
Distribution Partner Account Manager
Kaspersky Korea

kaspersky

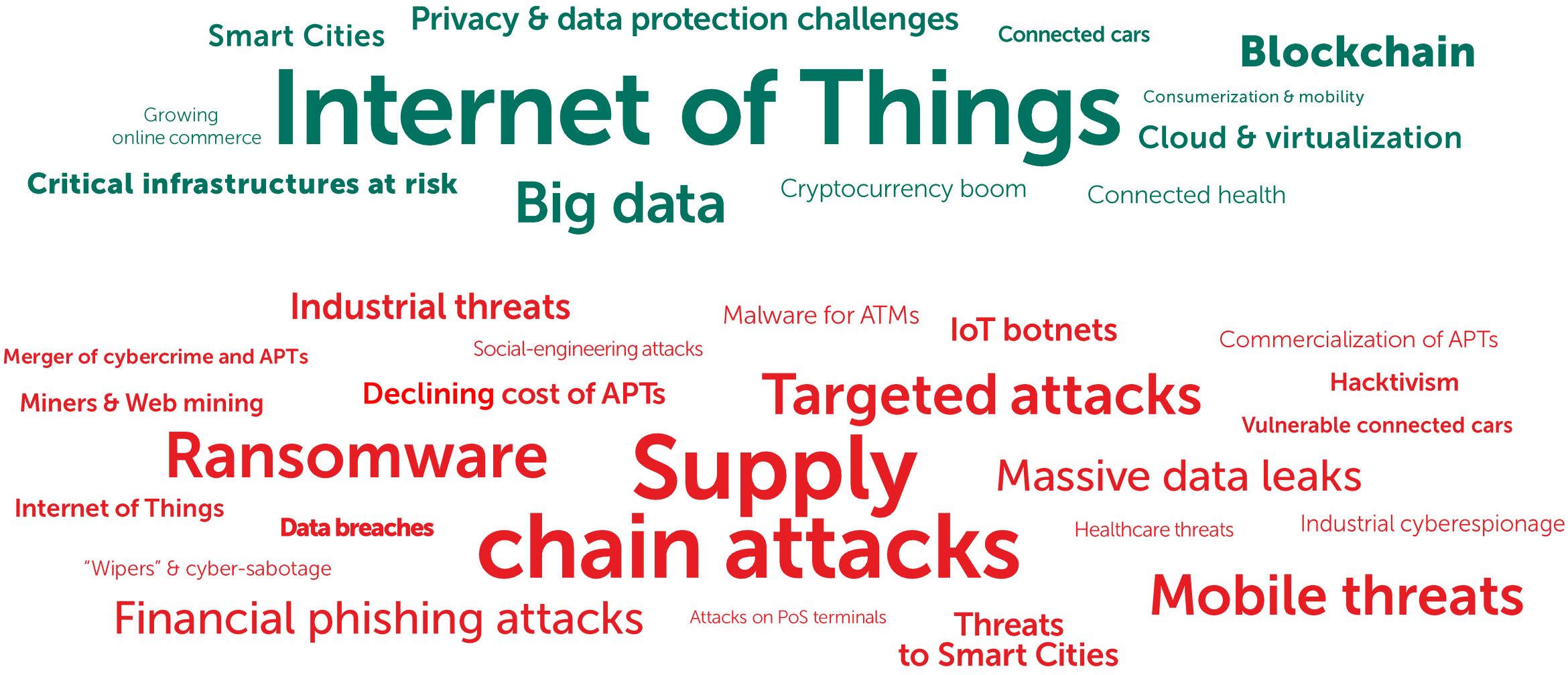
Agenda

- 최근 위협의 변화
- 위협 인텔리전스란?
- 카스퍼스키 위협 인텔리전스
  - 위협 데이터 피드
  - 사이버트레이스
  - 위협 룩업
  - 샌드박스 클라우드 & 리서치 샌드박스
  - 위협 인텔리전스 리포팅 (APT, 금융권)
  - 디지털 풋프린트, 오토모티브, ICS 인텔리전스
  - 위협 속성 엔진
- 카스퍼스키 위협 인텔리전스 Freemium
- SIEM 연계 사례
- 스플렁크와 연동 방법
- Q & A

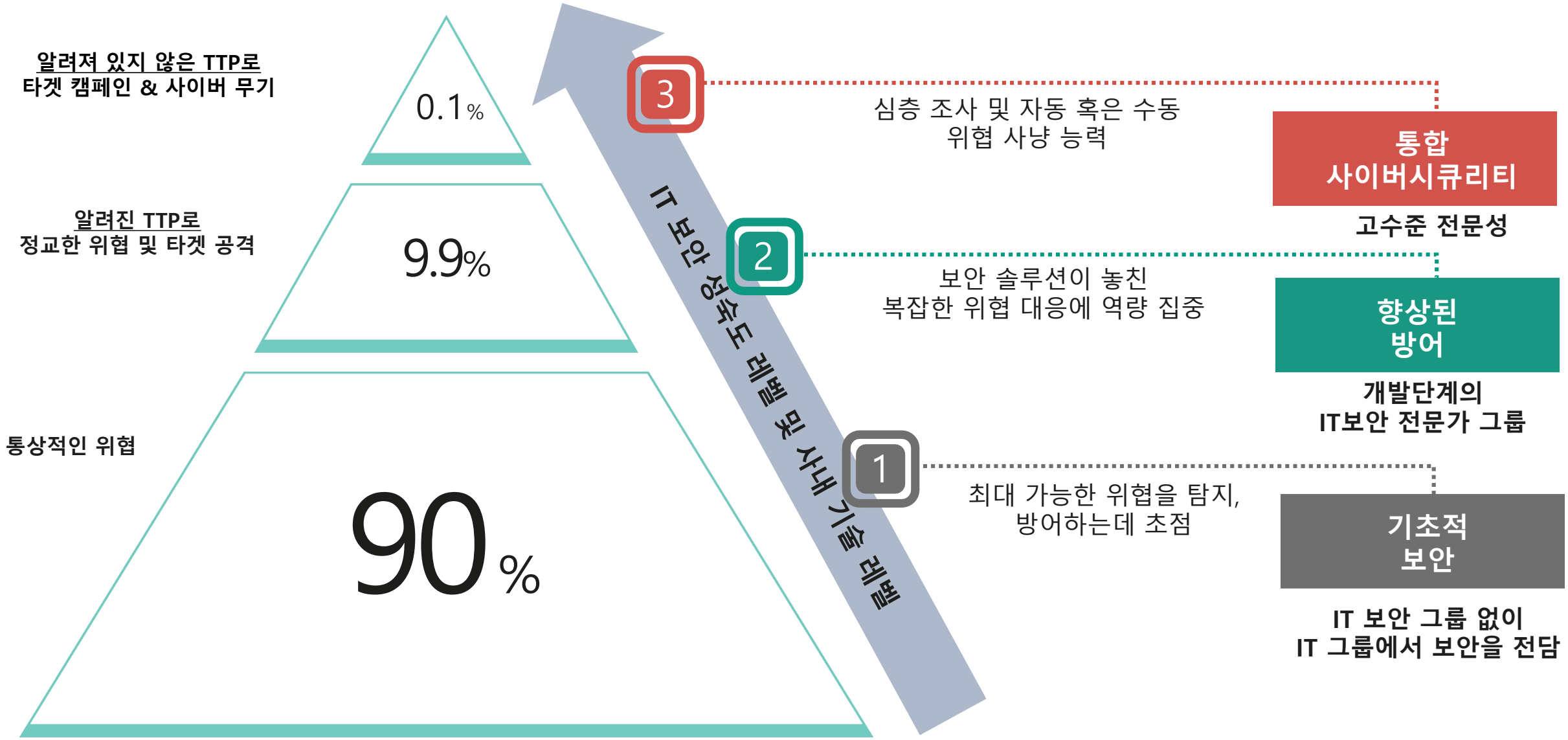
kaspersky

최근 위협의 변화

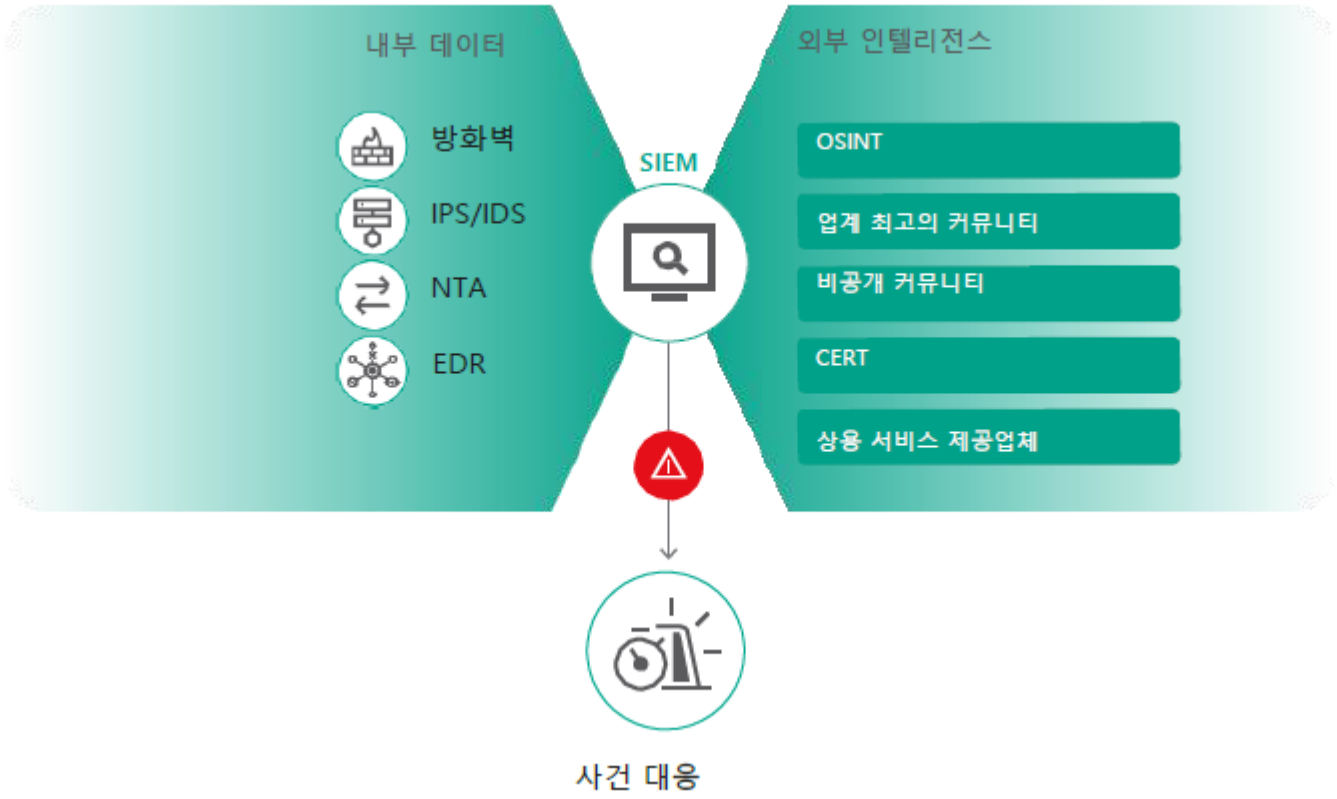
트렌드 및 위협


Smart Cities
Privacy & data protection challenges
Connected cars
Blockchain
Growing online commerce
Internet of Things
Consumerization & mobility
Cloud & virtualization
Critical infrastructures at risk
Big data
Cryptocurrency boom
Connected health
Industrial threats
Malware for ATMs
IoT botnets
Commercialization of APTs
Merger of cybercrime and APTs
Social-engineering attacks
Hacktivism
Miners & Web mining
Declining cost of APTs
Targeted attacks
Vulnerable connected cars
Ransomware
Supply chain attacks
Massive data leaks
Internet of Things
Data breaches
Healthcare threats
Industrial cyberespionage
"Wipers" & cyber-sabotage
Mobile threats
Financial phishing attacks
Attacks on PoS terminals
Threats to Smart Cities

위협 단계별 대응


알려져 있지 않은 TTP로
타겟 캠페인 & 사이버 무기
0.1%
알려진 TTP로
정교한 위협 및 타겟 공격
9.9%
통상적인 위협
90%
IT 보안 성숙도 레벨 및 사내 기술 레벨
3
심층 조사 및 자동 혹은 수동
위협 사냥 능력
통합
사이버시큐리티
고수준 전문성
2
보안 솔루션이 놓친
복잡한 위협 대응에 역량 집중
향상된
방어
개발단계의
IT보안 전문가 그룹
1
최대 가능한 위협을 탐지,
방어하는데 초점
기초적
보안
IT 보안 그룹 없이
IT 그룹에서 보안을 전담

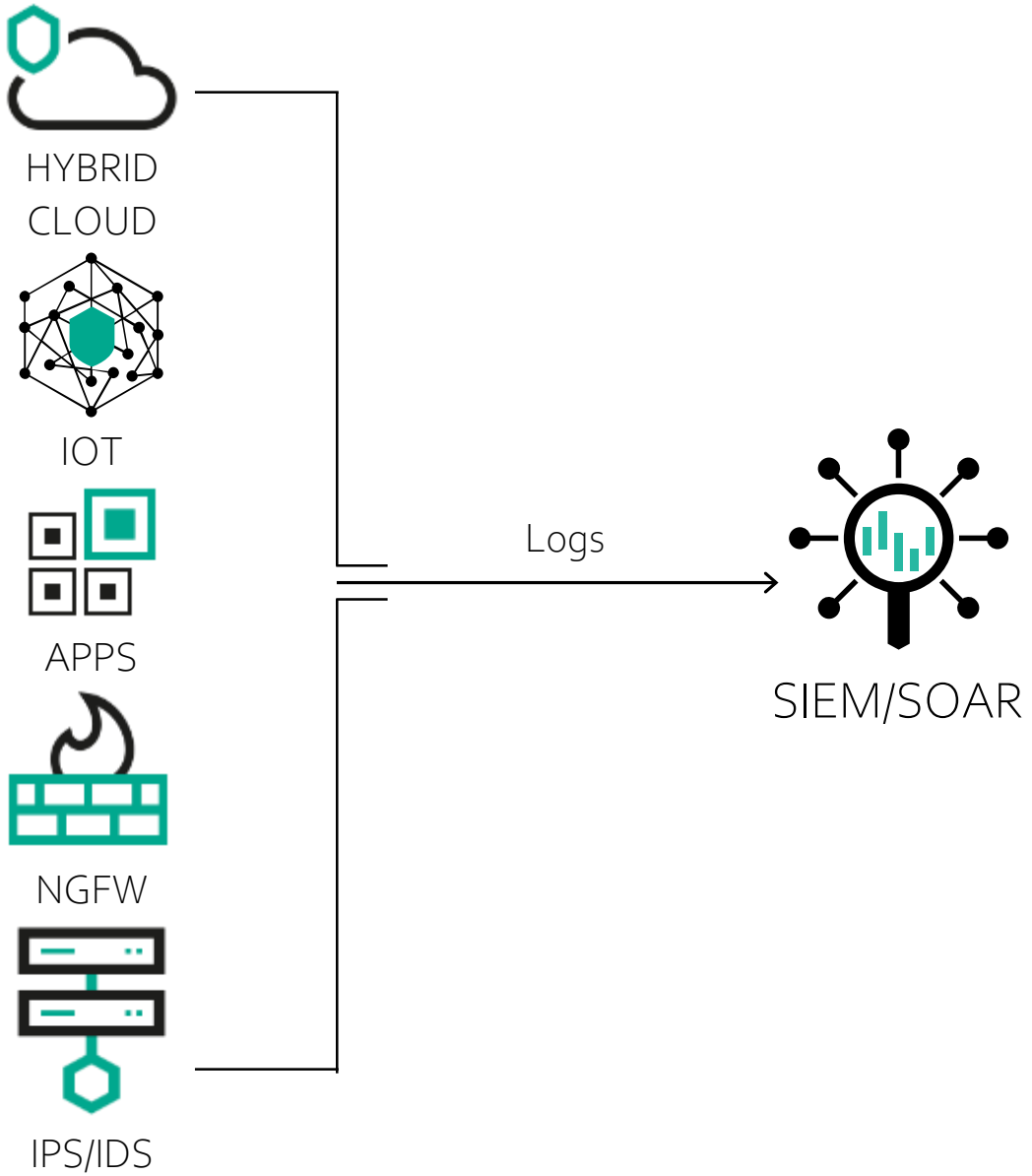
SOC & SIEM



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

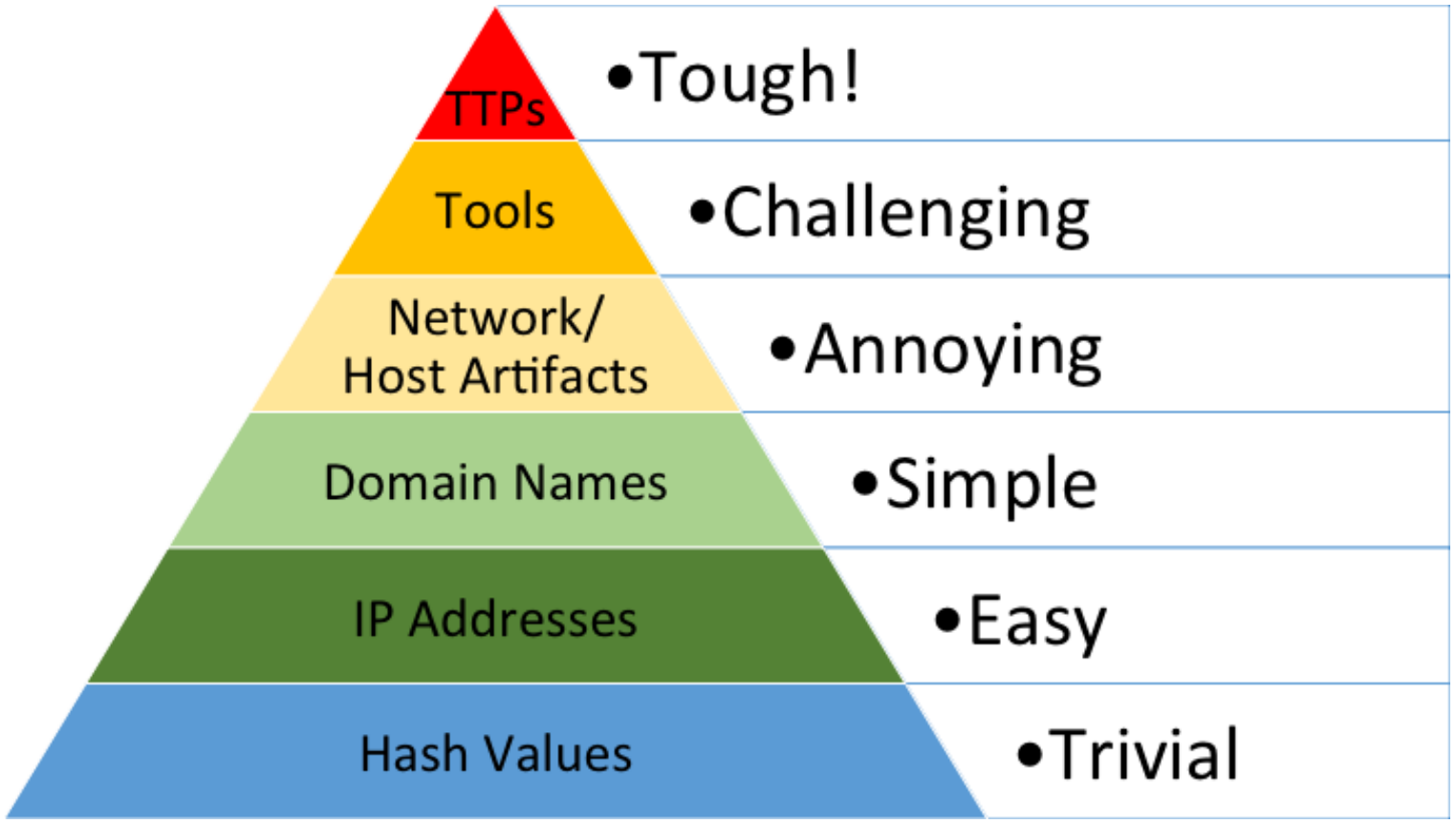
조직 내에 아직 발견되지 않은 위협이 존재

포괄적인 위협에 대한 개요 부족으로 인해
효과적인 보안 프로그램 개발 난항

kaspersky

위협 인텔리전스란?

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

Threat Intelligence 란 무엇인가?

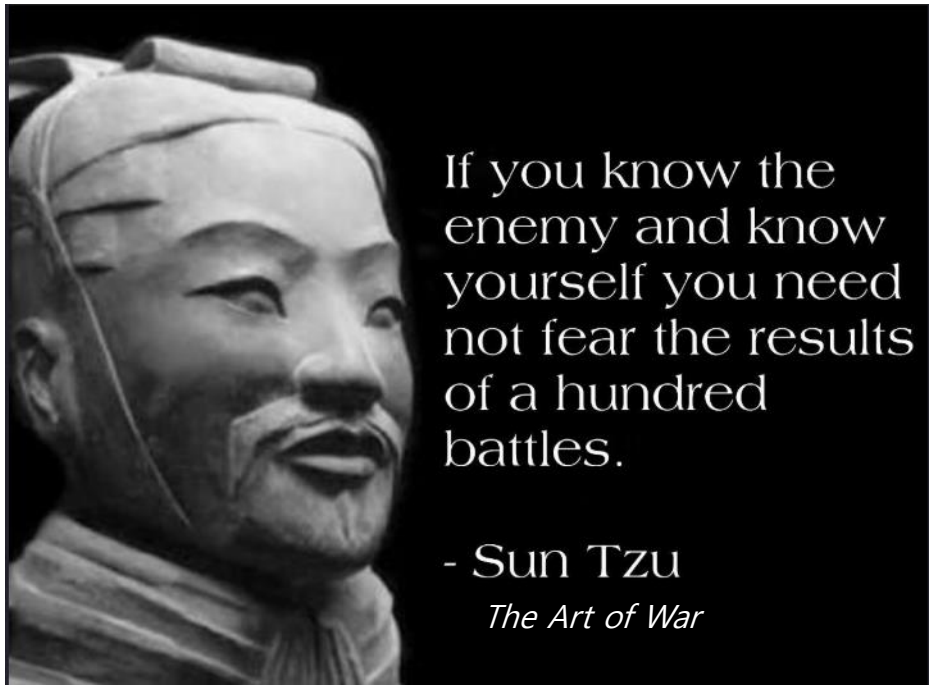
The analysis of an adversary's intent, opportunity, and capability to do harm is known as cyber threat intelligence. Intelligence is not a data feed, nor is it something that comes from a tool. Intelligence is actionable information that answers a key knowledge gap, pain point, or requirement of an organization – SANS.org

It identifies, analyzes and provides evidence-based knowledge, context, and actionable recommendations, regarding cyber threats aimed at your business. It is about shifting through piles of data
– Kaspersky

사이버보안 위험을 줄이기 위한 조직내 **의사결정 및 전달 과정,**
선제적 사이버 방어 체계를 구축하기 위한 **고급 정보**

Threat Intelligence 목표

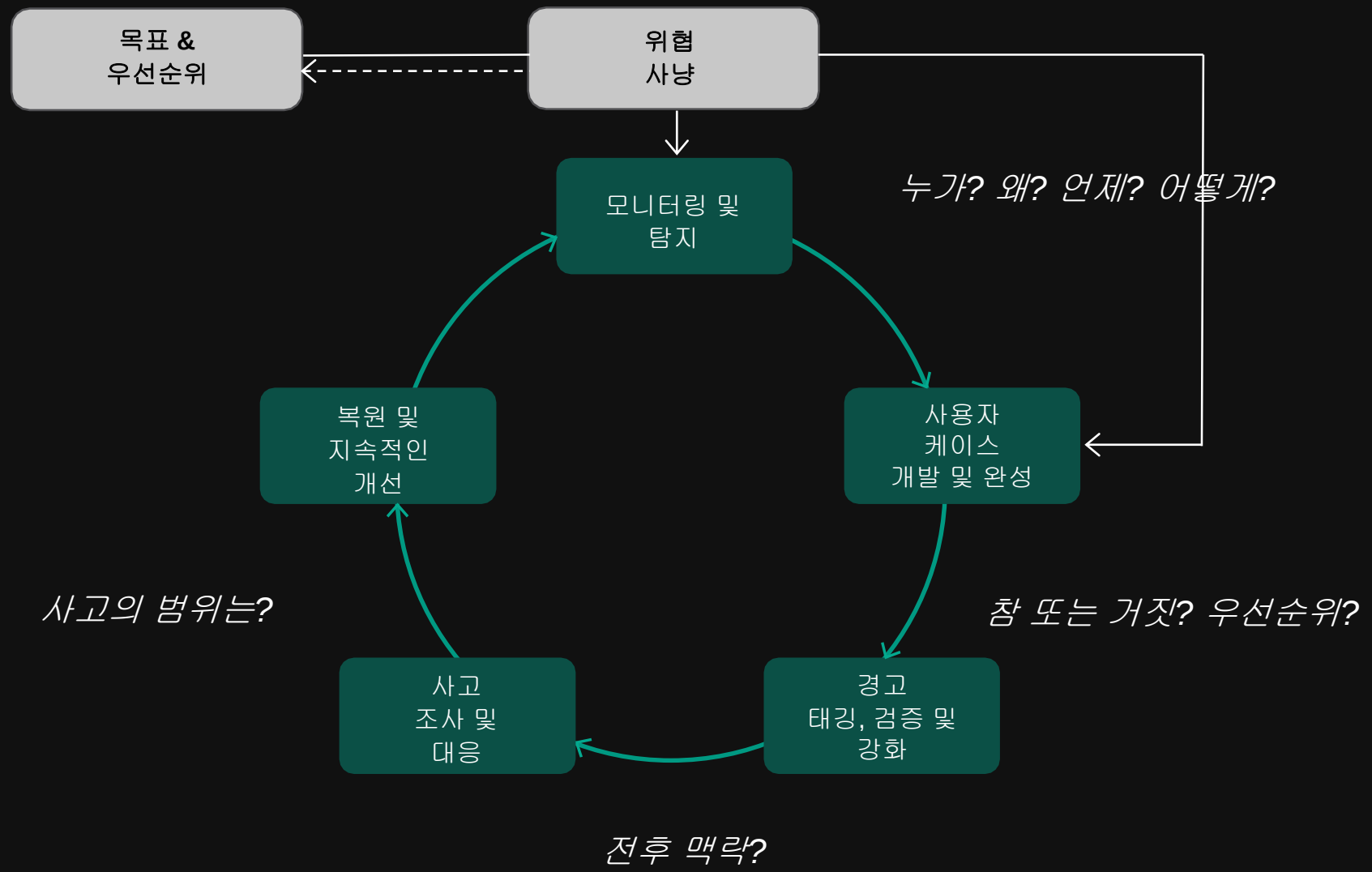
- **상대편의 행동**에 대한 정보 전환성
- 악의적 행동에 대한 **탐지 및 방어 체계** 구축
- 방어 수단에 대한 **중요도 지정**
- **사건 대응 및 위협 헌팅** 절차 최적화
- SOC 운영의 **조력자**



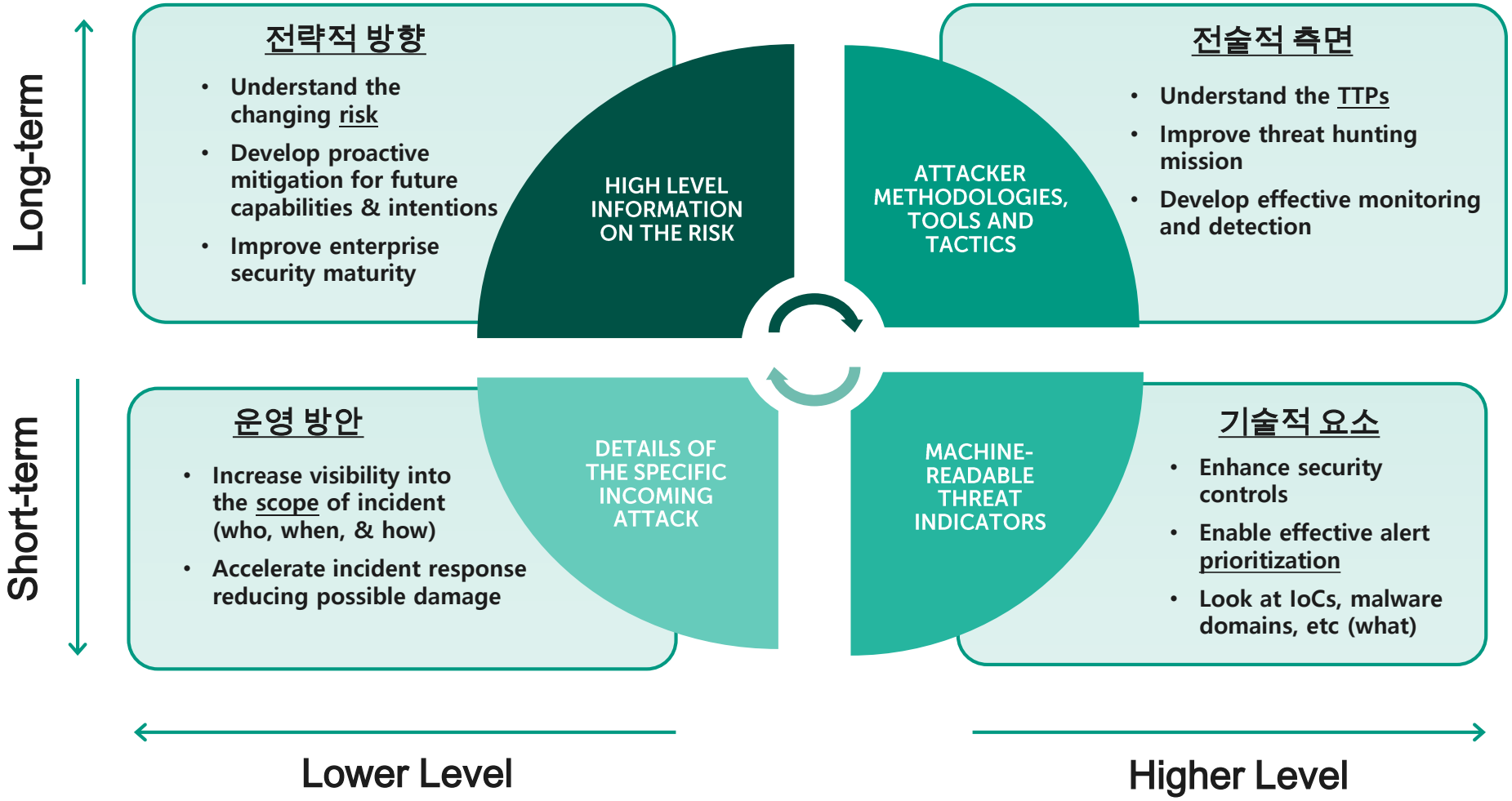
Threat Intelligence – SOC 운영의 조력자

Role	Description	Responsibilities
Tier-3 Security Expert	**Threat Intelligence** and Threat Hunting	• Threat Hunting • Use cases development • Security monitoring system improvements and development
Digital Forensics Expert	Digital Forensics	• Digital evidence collection and analysis • Incident investigation and root cause analysis • IOCs and TTPs acquisition
Malware Analyst	Malware Analysis	• Malware analysis and reverse-engineering • IOCs and TTPs acquisition
Threat Intelligence Analyst	**Threat Intelligence**	• Threat Intelligence collection, aggregation, filtering and analysis • Threat intelligence distribution and sharing • TTPs and IOCs database management • Threat Data Feeds management • Threat Intelligence analytic reports creation for various stakeholders • Produce relevant analytics for SOC team and external partners
Penetration tester	Security Assessment	• Security assessment • Red Teaming

인텔리전스 기반 보안 운영



위협 인텔리전스 적용


Long-term
Short-term
전략적 방향
Understand the changing risk
Develop proactive mitigation for future capabilities & intentions
Improve enterprise security maturity
HIGH LEVEL INFORMATION ON THE RISK
ATTACKER METHODOLOGIES, TOOLS AND TACTICS
전술적 측면
Understand the TTPs
Improve threat hunting mission
Develop effective monitoring and detection
운영 방안
Increase visibility into the scope of incident (who, when, & how)
Accelerate incident response reducing possible damage
DETAILS OF THE SPECIFIC INCOMING ATTACK
MACHINE-READABLE THREAT INDICATORS
기술적 요소
Enhance security controls
Enable effective alert prioritization
Look at IoCs, malware domains, etc (what)
Lower Level
Higher Level

Threat Intelligence - 프레임워크

kaspersky

위협 인텔리전스 선택 범주

가장 광범위한 공격 가시성을 제공하며, 전지구적 접근성을 가지는 인텔리전스

새로운 위협 요소를 일찍 발견하는 실적이 있는 공급자

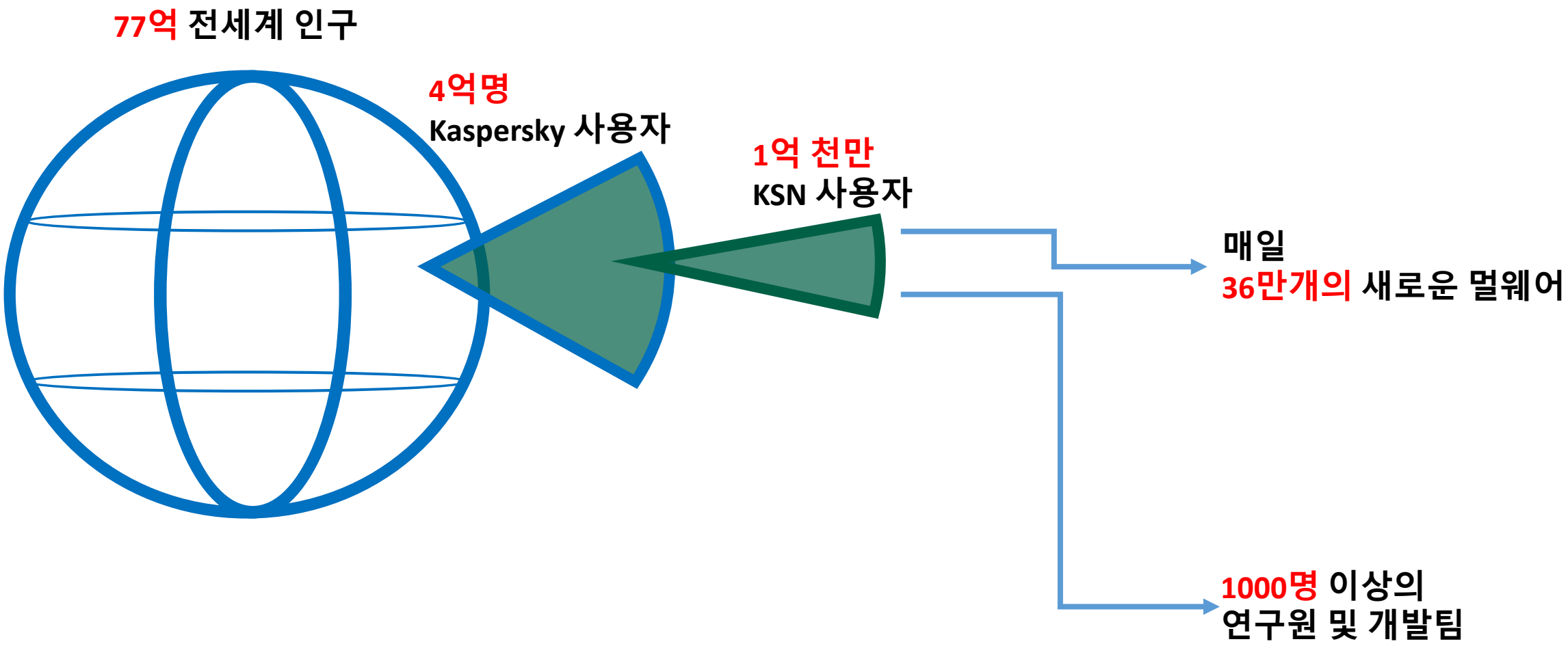
전후 사정이 풍부하고 즉각적으로 행동 가능한 인텔리전스

기존 보안 제어에 쉽게 통합할 수 있는 전달 형식 및 메커니즘 제공

kaspersky

카스퍼스키 위협 인텔리전스

글로벌 커버리지 및 영향력



GREAT

GLOBAL RESEARCH & ANALYSIS TEAM

Marco Preuss
Director of GReAT Europe
GReAT Europe

Vicente Diaz
Deputy Director of GReAT Europe
GReAT Europe

Christian Funk
Head of GReAT, Germany
GReAT Europe

David Emm
Principal Security Researcher
GReAT Europe

Dani Creus
Senior Security Researcher
GReAT Europe

David Jacoby
Senior Security Researcher
GReAT Europe

Jornt van der Wiel
Senior Security Researcher
GReAT Europe

Ido Naor
Senior Security Researcher
GReAT Europe

Ivan Kwiatkowski
Senior Security Researcher
GReAT Europe

Pierre Delcher
Senior Security Researcher
GReAT Europe

Giampaolo Dedola
Security Researcher
GReAT Europe

Félix Aime
Security Researcher
GReAT Europe

Ariel Jungheit
Security Researcher
GReAT Europe

Matthias Weckbecker
Security Researcher
GReAT Europe

Kurt Baumgartner
Principal Security Researcher
GReAT US

Brian Bartholomew
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

Thiago Marques
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

Sergey Novikov
Deputy Director
GReAT

Yury Namestnikov
Head of GReAT Russia
GReAT Russia

Igor Kuznetsov
Principal Security Researcher
GReAT Russia

Sergey Mineev
Principal Security Researcher
GReAT Russia

Sergey Belov
Principal Security Researcher
GReAT Russia

Konstantin Zykov
Senior Security Researcher
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

Maria S. Namestnikova
Project Manager
GReAT Russia

#Reverse Engineering #Security Intelligence #Digital Forensics #Mobile Security #User Security Education
#Underground Network Monitoring #Counteracting Cyber-Espionage #Internet of Things Research #Online Banking Security

kaspersky

Targeted attack research

What is so great about GReAT?

Coverage of threat actors regardless their origin

- Russian-speaking
- English-speaking
- Spanish-speaking
- Korean-speaking
- Chinese-speaking etc.

Actionable reporting on some of the most serious threats

- Public: 20+ per year
- …and even more in private: 140+ researches per year

Proprietary auto-attribution engine

- Incorporates several similarity algorithms
- Accumulated 12+ years of expertise in targeted attacks
- Knowledge about 800+ actors and campaigns
- Patent pending

Threat intelligence sources

정보 보안 전략

리스크 이해
사전 예방적 완화조치 개발
예산과 인력 요구 사항 정당화

Digital Footprint Intelligence

위협 발견

기존의 보안 제어 강화

Threat Data Feeds
CyberTrace

우선순위 및 초기 대응

알람 분류, 검증 및 강화

CyberTrace
Threat Lookup

사고 분석

사고 대응 강화 및
가능한 피해 감소

Threat Lookup
Cloud Sandbox
Research Sandbox

위협 사냥

기존 보안 제어로 놓친 위협
찾기

APT, Financial and ICS Threat Intelligence Reporting
Threat Attribution Engine

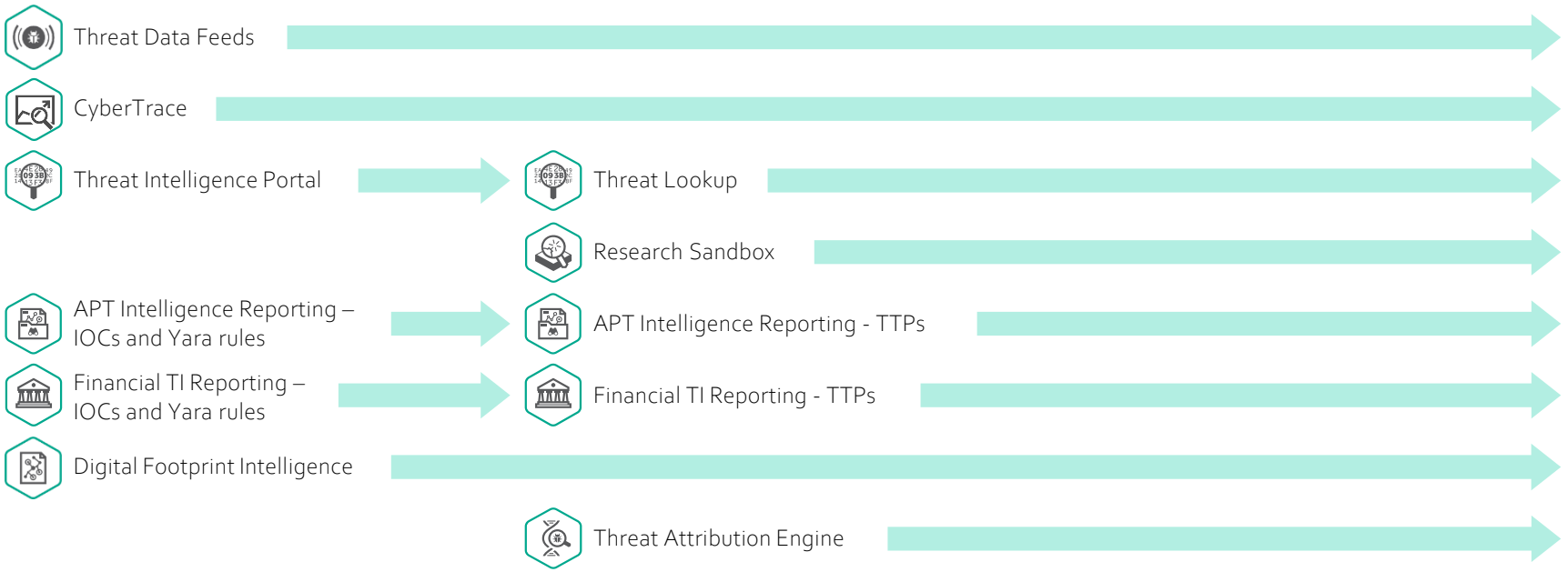
SOC 성숙도에 따른 매핑

기능 성숙도

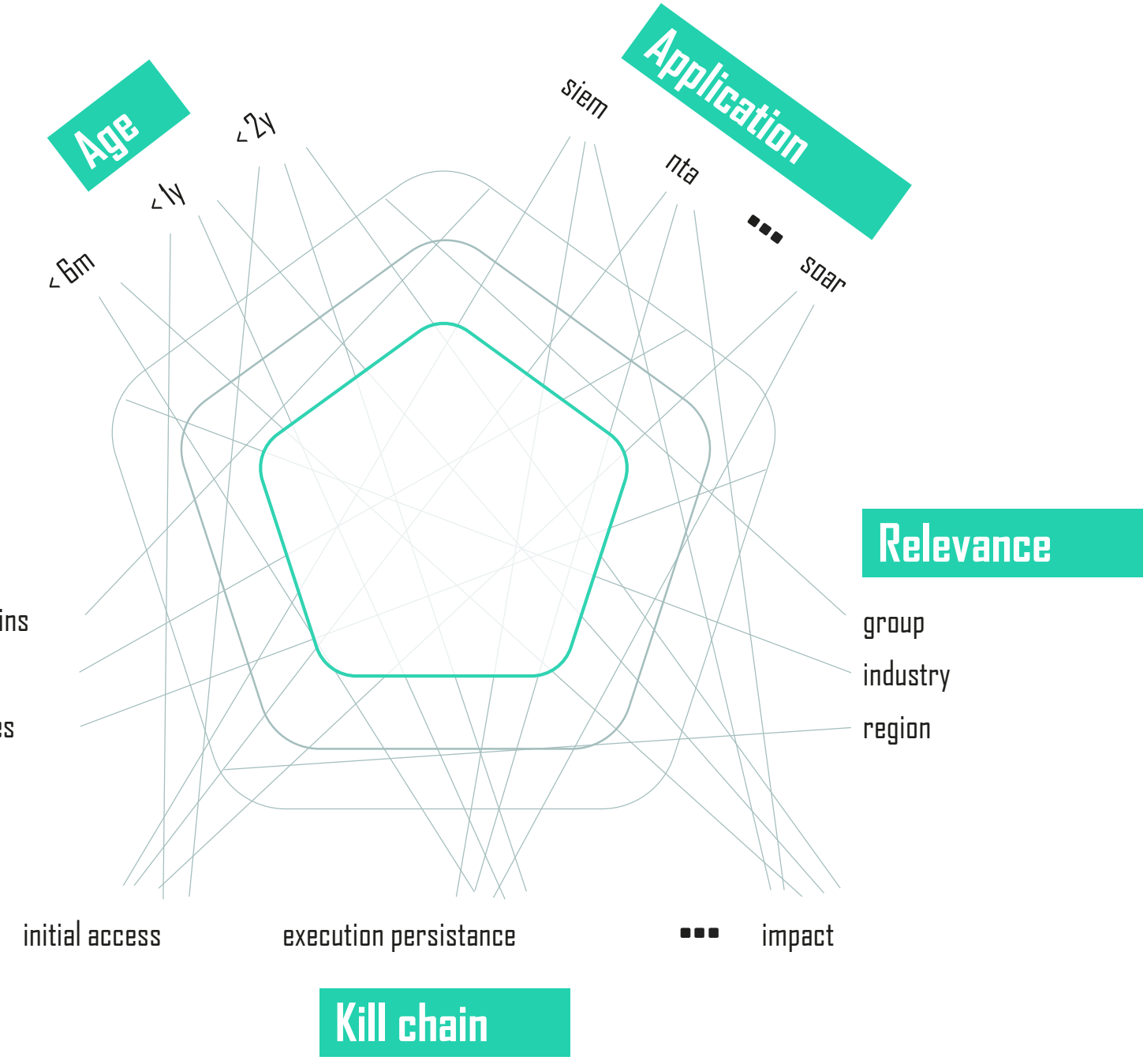
진화하는 IT 보안 기능 및 SOC

Tier 1 모니터링 & 분류	Tier 2 억제 및 수정	Tier 3 포렌식, 사냥 & 인텔리전스
• 모니터링 • 사고 식별 • 기본 분석 및 완화	• 더 깊은 분석 • 완화 • 추천 변화	• 악성코드 분석 • 디지털 포렌식 • 위협 인텔리전스 • 위협 사냥

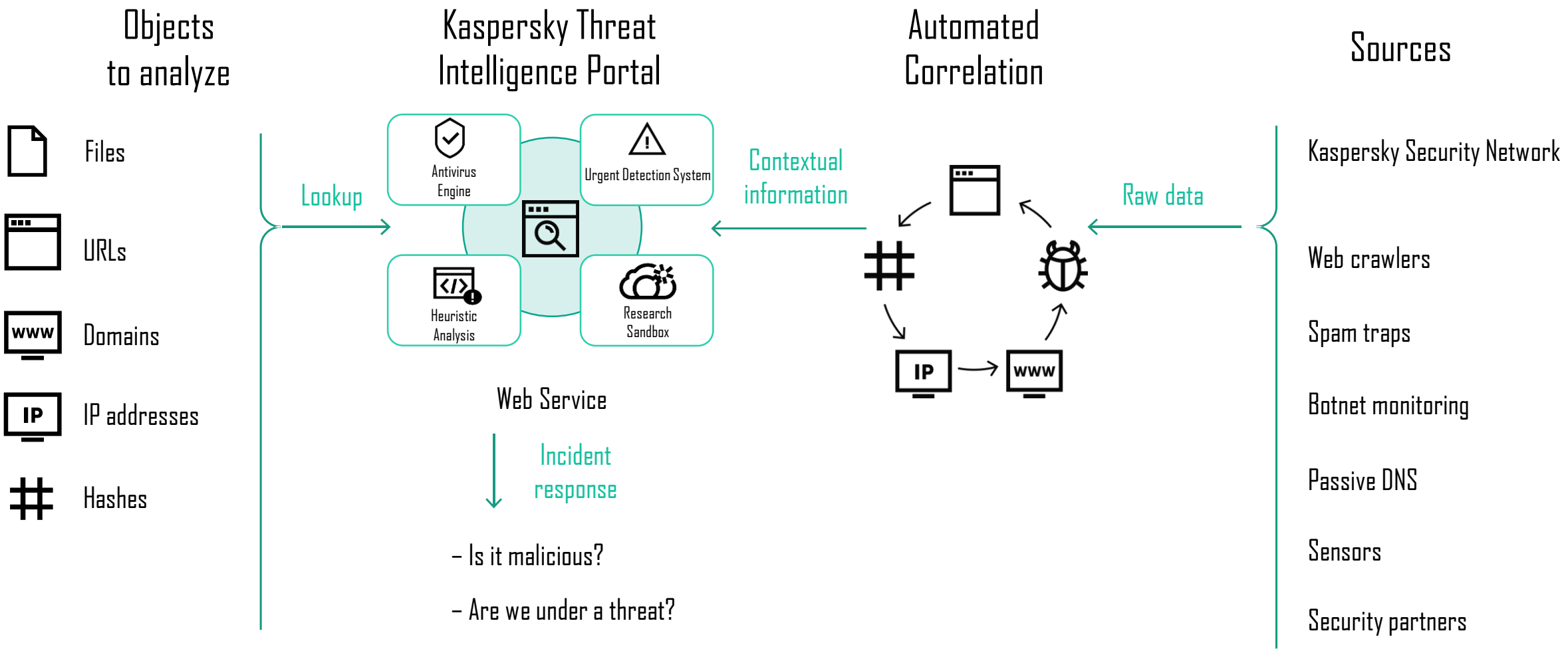
THREAT INTELLIGENCE SERVICES



Key TI characteristics



Threat Intelligence Portal



Kaspersky
Threat Intelligence Portal

Login

Hash, IP address, domain, or URL

Enter your request here

Look up

By requesting lookup data, you agree to our Terms of Use and Privacy Statement.

A375E3507978C4C0AFDC2FB9E85E74BD
Malware

< Public submissions

Report for hash: Malware

A375E3507978C4C0AFDC2FB9E85E74BD

Hits	≈ 1,000	Format	PE	MD5	A375E3507978C4C0AFDC2FB9E85E74BD
First seen	Feb 27, 2017 19:04	Size	248.24 MB	SHA-1	180CEF6E0BE51928DC004DAEC38F14E205A0E7D2
Last seen	Oct 17, 2019 04:11	Signed by	—	SHA-256	709ADA832565BD617A49B5BEFF9E2019DC4FB2C90C196F0B9881E069C131110F
		Packed by	—		

Detection names

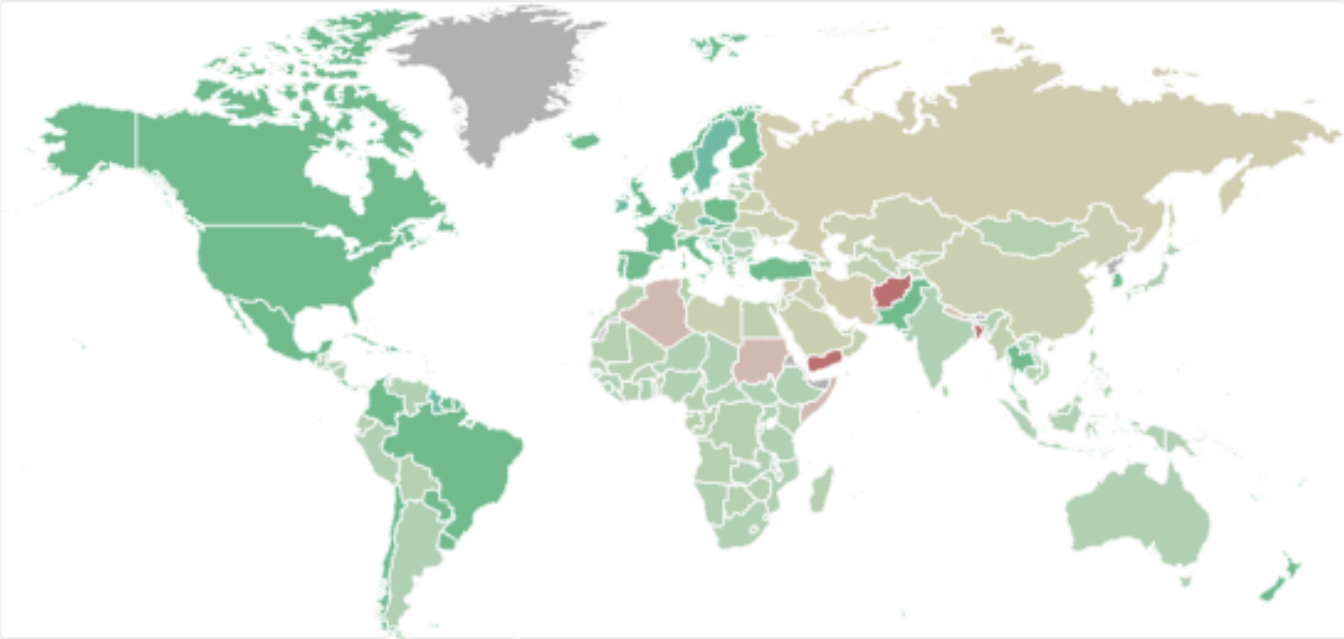
May 31, 2019 14:35

Oct 17, 2019 04:30

Worldwide

Period: Day | Week | Last month

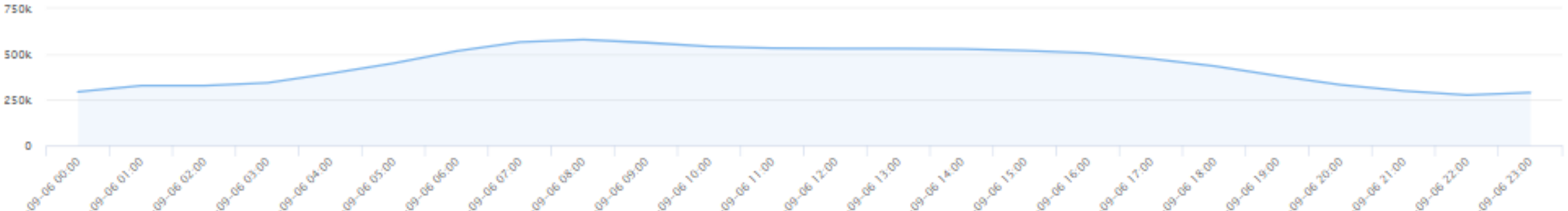
Type: OAS | WAV | MAV | ODS | IDS | KAS | VUL



TOP 10 Threats

1.	HackTool.Win32.KMSAuto.gen	12.89 %
2.	DangerousObject.Multi.Generic	9.33 %
3.	HackTool.MSIL.HackKMS.a	3.24 %
4.	HackTool.MSIL.KMSAuto.dh	2.99 %
5.	Hoax.Win32.Seguras.gen	2.61 %
6.	HackTool.MSIL.KMSAuto.di	2.32 %
7.	HackTool.MSIL.HackKMS.d	2.07 %
8.	HackTool.Win32.KMSAuto.ew	1.73 %
9.	HackTool.MSIL.HackKMS.h	1.69 %
10.	HackTool.Win64.HackKMS.b	1.45 %

Threats dynamics

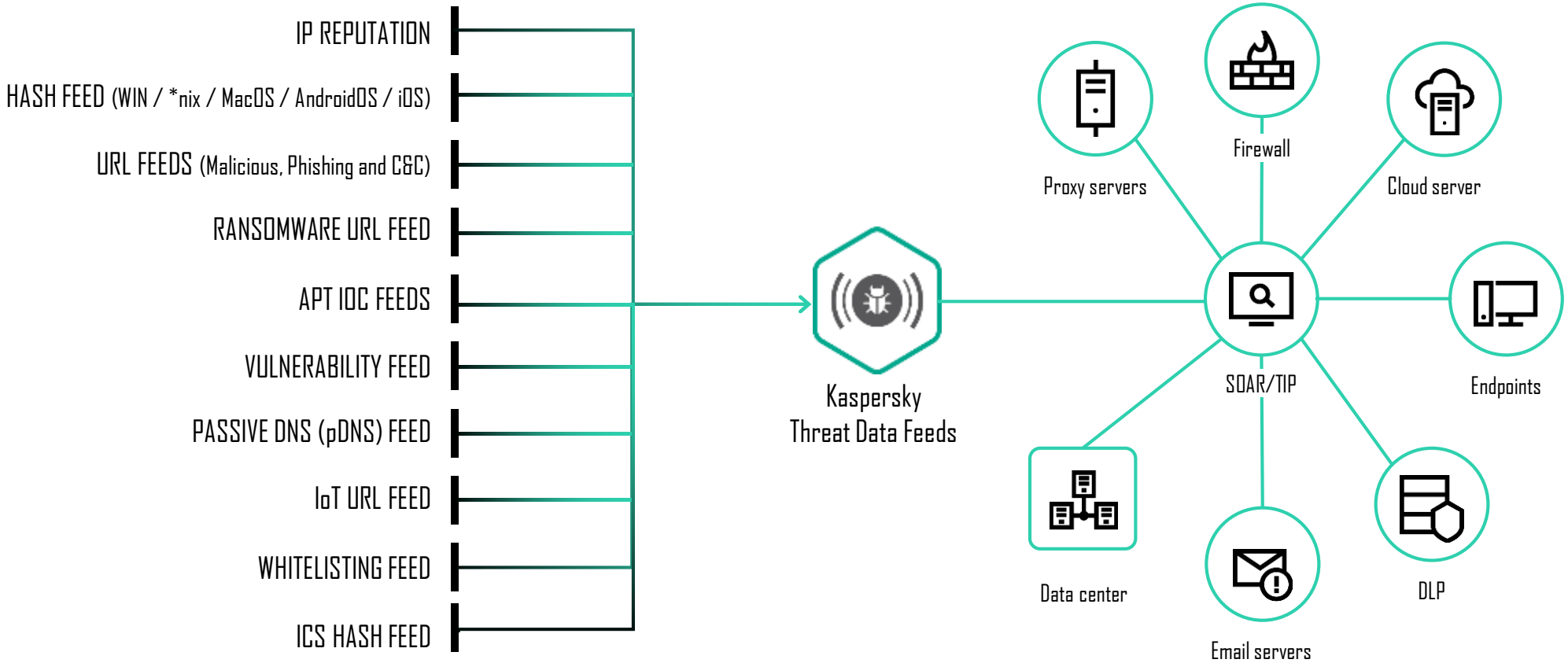


Threat Data Feeds

오탐률이 0에 가깝고 지속적으로 업데이트 되는 위협 데이터

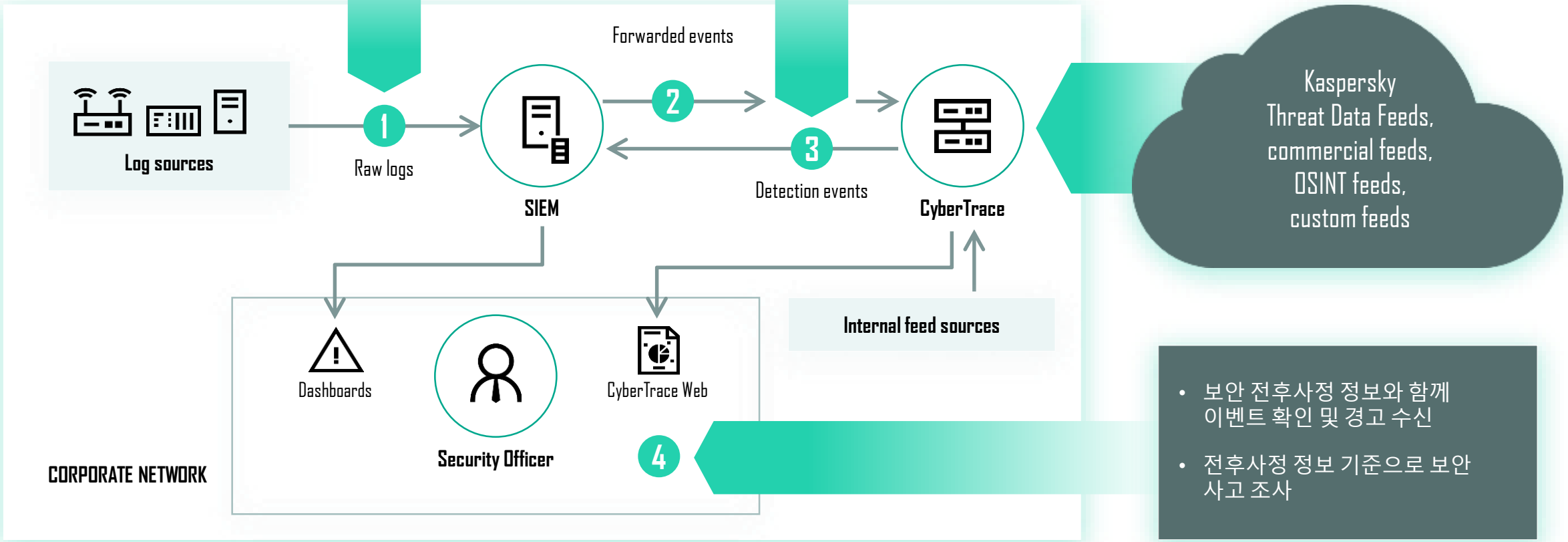
풍부하고 의미있는 전후사정 정보로 인해 인텔리전스를 즉시 실행

표준 전달 형식과 메커니즘을 통해 보안 제어에 쉽게 통합 가능



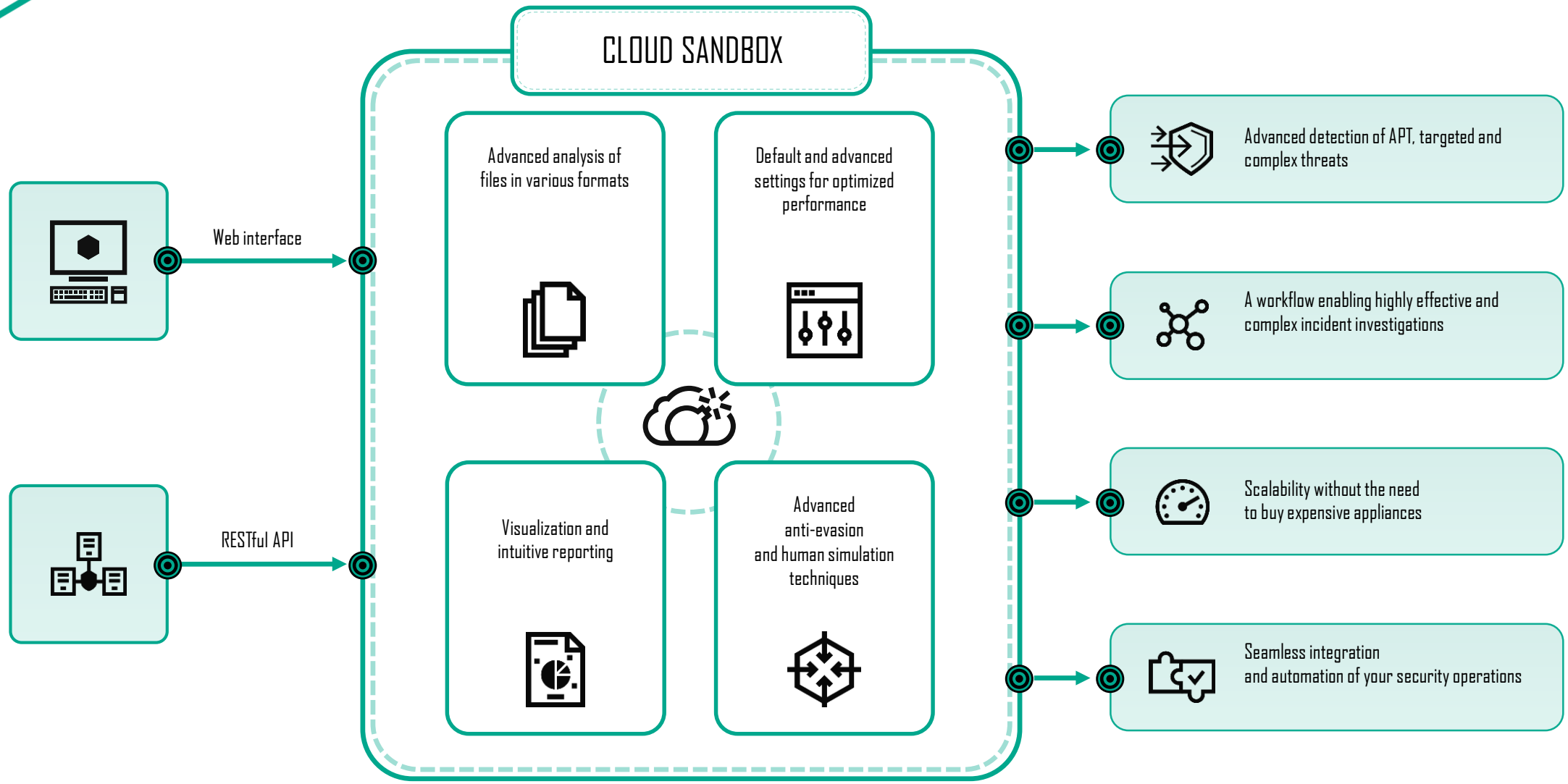
SIEM이 여러 네트워크 장피 및 IT 시스템의 로그를 취합한 후 URL, 해시, IP 등의 정보와 함께 이벤트에 대한 상관 관계를 분석

CyberTrace가 신속하게 수신 이벤트와 피드의 일치 여부를 비교하여 탐지된 이벤트를 SIEM 및 CyberTrace 웹으로 전송



- 보안 전후사정 정보와 함께 이벤트 확인 및 경고 수신
- 전후사정 정보 기준으로 보안 사고 조사

Kaspersky Cloud Sandbox



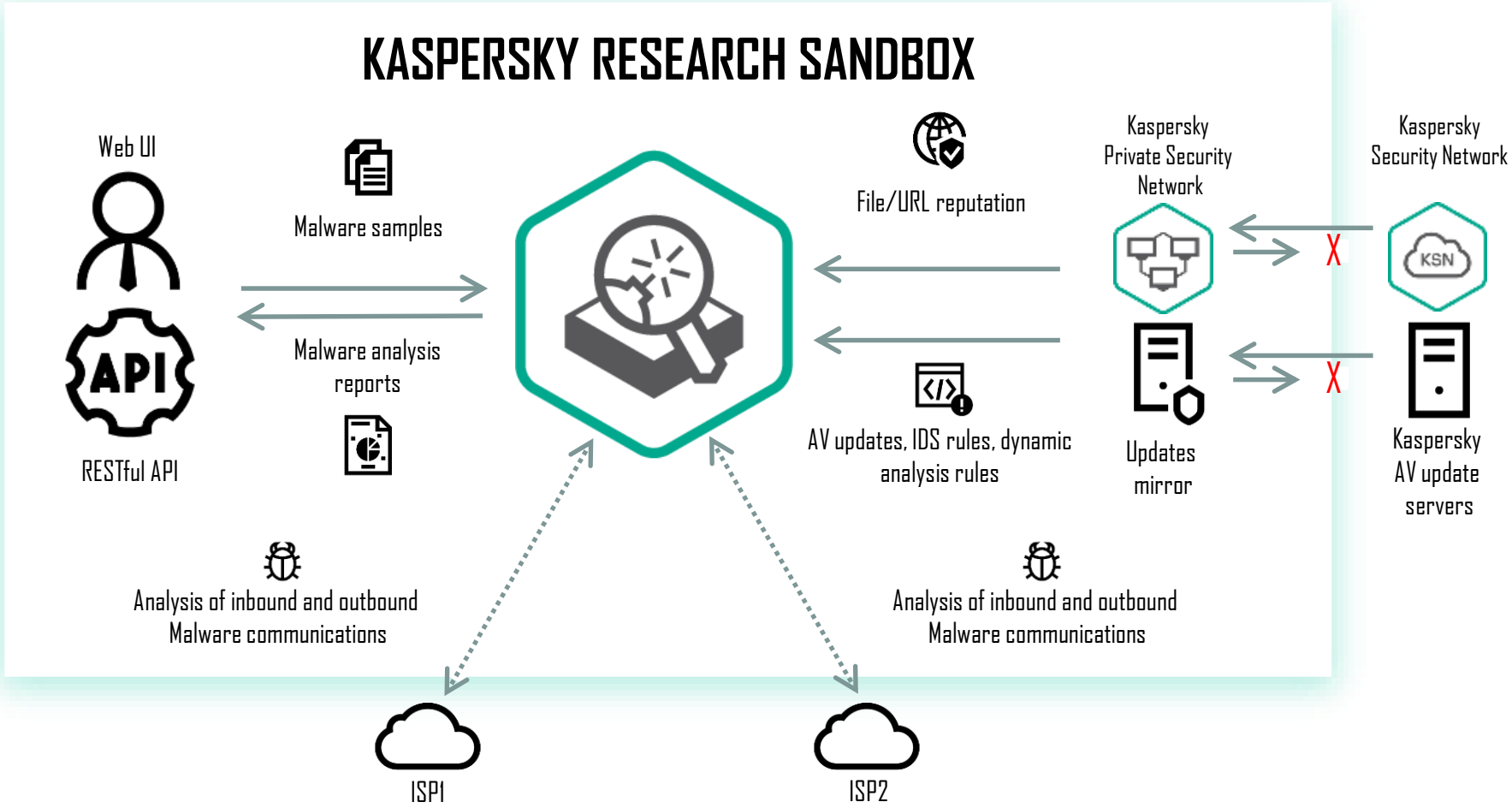
Research Sandbox

고급 탈취 방지 및 휴먼 시뮬레이팅 기술을 통해 특허받은 위협 에뮬레이션 기술을 제공합니다.

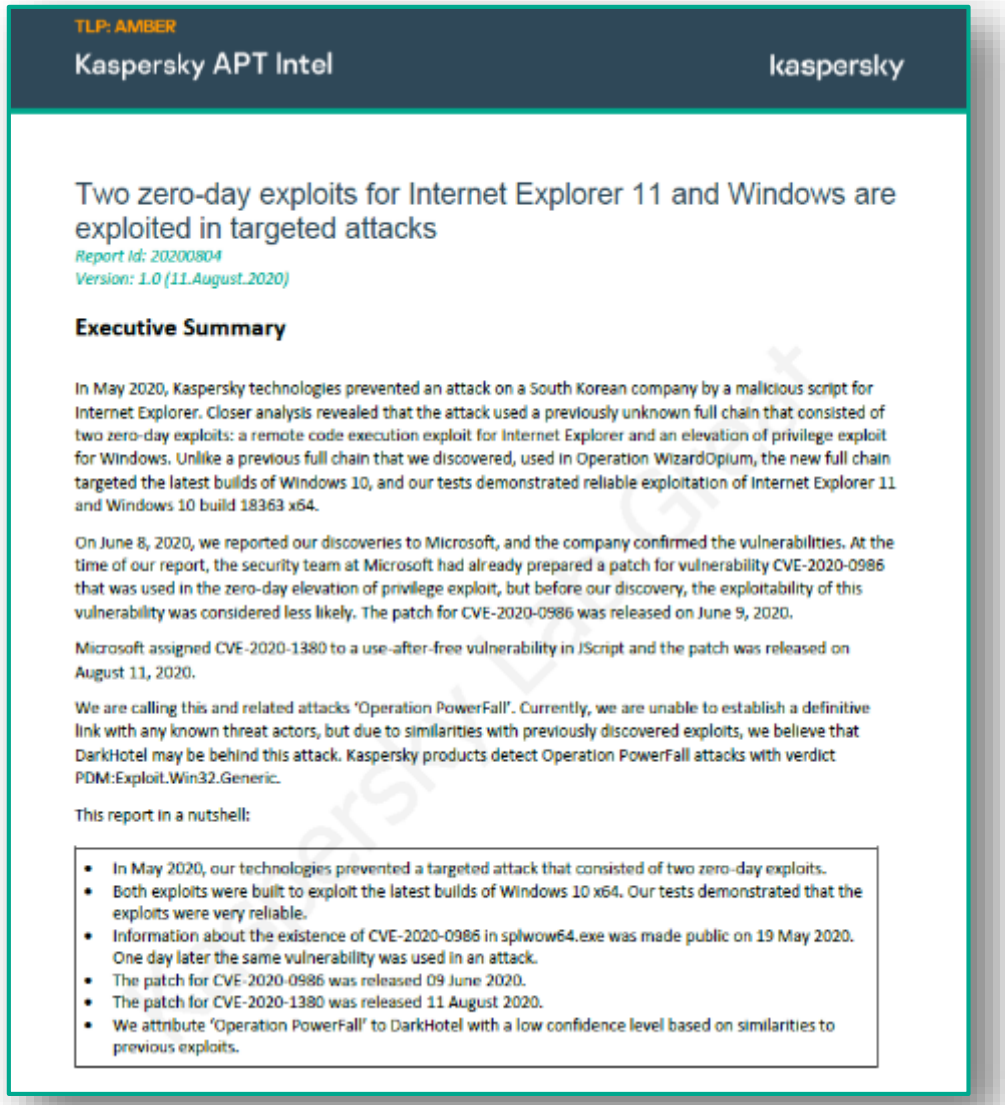
사용자 지정 이미지를 통해 실제 환경에 적용되는 OS 및 애플리케이션의 위협을 분석할 수 있습니다.

Windows 및 Android OS를 지원하며 더블 클릭하여 실행할 수 있는 모든 파일 형식을 분석합니다.

온프레미스 또는 클라우드 구축 옵션을 통해 다양한 고객 프로파일을 해결 할 수 있습니다.



APT and Financial Threat Intelligence Reporting



TLP: AMBER

Kaspersky APT Intel — kaspersky

Two zero-day exploits for Internet Explorer 11 and Windows are exploited in targeted attacks

Report Id: 20200804
Version: 1.0 (11.August.2020)

Executive Summary

In May 2020, Kaspersky technologies prevented an attack on a South Korean company by a malicious script for Internet Explorer. Closer analysis revealed that the attack used a previously unknown full chain that consisted of two zero-day exploits: a remote code execution exploit for Internet Explorer and an elevation of privilege exploit for Windows. Unlike a previous full chain that we discovered, used in Operation WizardOpium, the new full chain targeted the latest builds of Windows 10, and our tests demonstrated reliable exploitation of Internet Explorer 11 and Windows 10 build 18363 x64.

On June 8, 2020, we reported our discoveries to Microsoft, and the company confirmed the vulnerabilities. At the time of our report, the security team at Microsoft had already prepared a patch for vulnerability CVE-2020-0986 that was used in the zero-day elevation of privilege exploit, but before our discovery, the exploitability of this vulnerability was considered less likely. The patch for CVE-2020-0986 was released on June 9, 2020.

Microsoft assigned CVE-2020-1380 to a use-after-free vulnerability in JScript and the patch was released on August 11, 2020.

We are calling this and related attacks 'Operation PowerFall'. Currently, we are unable to establish a definitive link with any known threat actors, but due to similarities with previously discovered exploits, we believe that DarkHotel may be behind this attack. Kaspersky products detect Operation PowerFall attacks with verdict PDM:Exploit.Win32.Generic.

This report in a nutshell:

- In May 2020, our technologies prevented a targeted attack that consisted of two zero-day exploits.
- Both exploits were built to exploit the latest builds of Windows 10 x64. Our tests demonstrated that the exploits were very reliable.
- Information about the existence of CVE-2020-0986 in splwow64.exe was made public on 19 May 2020. One day later the same vulnerability was used in an attack.
- The patch for CVE-2020-0986 was released 09 June 2020.
- The patch for CVE-2020-1380 was released 11 August 2020.
- We attribute 'Operation PowerFall' to DarkHotel with a low confidence level based on similarities to previous exploits.

- → Threat actor profiles
- → Mapping to ATT&CK
- → Executive summary
  - C-level oriented information
- → Deep technical analysis
  - Attack methods
  - Exploits used
  - Malware description
  - C&C infrastructure and protocols description
  - Victim analysis
  - Data exfiltration analysis
  - Attribution
- → Conclusions and recommendations
- → Indicators of Compromise and YARA rules

Digital Footprint Intelligence

네트워크 경계 인벤토리 (클라우드 포함)

- 사용가능한 서비스
- 서비스 지문인식
- 취약점 식별
- 익스플로잇 분석
- 스코어링 및 리스크 분석

Surface, deep, dark web

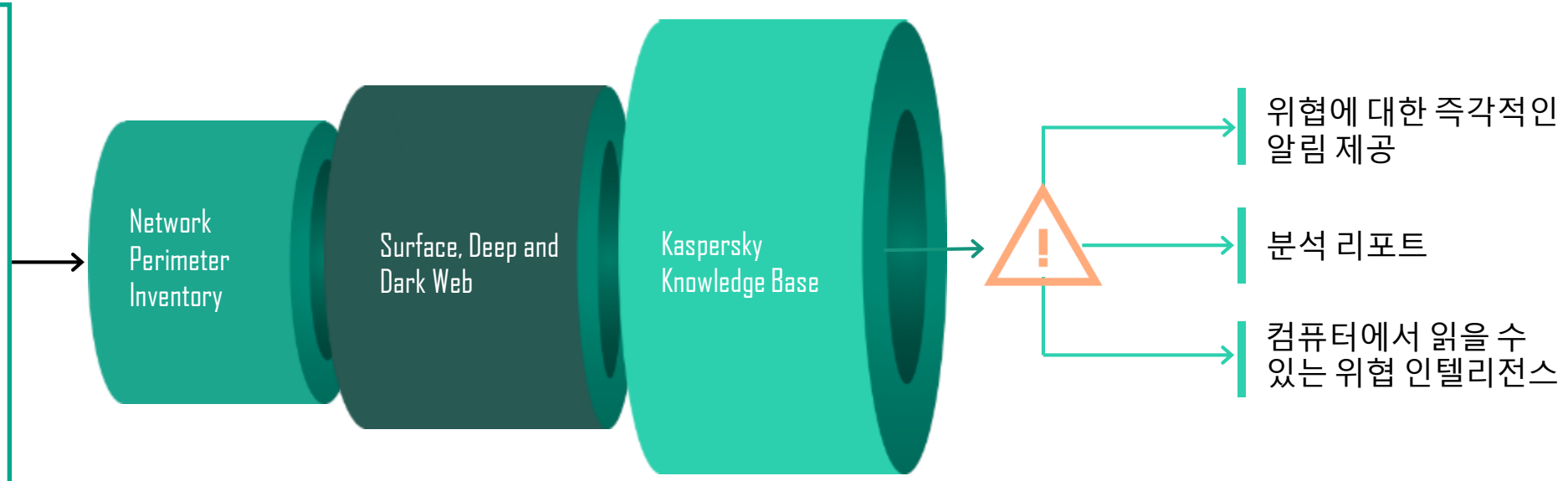
- 사이버범죄 활동
- 데이터 및 자격증명 누출
- 내부자 소행
- 소셜 미디어의 직원
- 메타데이터 누출

Kaspersky knowledge base

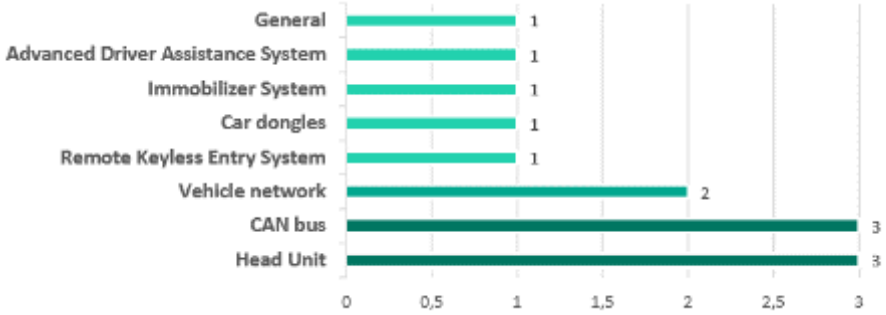
- 말웨어 샘플 분석
- 본넷 및 피싱 트래킹
- 싱크홀 및 악성코드 서버
- APT Intelligence Reporting
- Threat Data Feeds

고객의 비정형 데이터

- IP 주소
- 회사 도메인
- 브랜드 이름
- 키워드



Tailored reports on automotive specific threats



Overview on Trends in Automotive Cyber-security

100+ industry- and regional-specific forums and social networks

Tracking automotive-specific webinars, talks, videos, public software releases

30+ regulatory documents

780+ planned conferences in 2020

OEM Tailored Analysis

OEM-specific vulnerabilities and security threats, information related to fraud, data breaches, known exploits and abuses, OEM supply chain breakdown

ICS threat intelligence (TI) from Kaspersky ICS CERT

ICS Reporting on TIP

Subscription-based access via web portal to regular TI reports with ICS-specific information on attacks, threats and vulnerabilities

All ICS related threat intelligence research is done by a dedicated team – Kaspersky ICS CERT

- Established in 2016
- The first CERT team by a commercial organization
- Around 20 highly qualified experts on ICS threat and vulnerability research, incident response and security analysis

Types of reports available to subscribers

Vulnerability research

- Reports on vulnerability analysis results for the most popular products used in ICS, IIoT, and the infrastructure of various industries

APT reports

- Reports on new APT and high-volume attack campaigns targeting industrial organizations, and updates on active threats

Kaspersky ICS CERT has a dedicated vulnerability research team:

- 200+ zero-days reported
- Authorized to assign CVE IDs to vulnerabilities being a CVE Numbering Authority (CNA)
- Detailed actionable advisories
- Building a unique vulnerability database

ICS Reporting on Threat Intelligence Portal

Kaspersky Threat Intelligence Portal

Help | Support | Evgeny Goncharov

APT Reporting | Financial Reporting | ICS Reporting | Threat Lookup | Cloud Sandbox

Master YARA | Master IOC

Date	Report
Apr 20, 2020	Cyberthreats for the Logistics sector: TOP 3 Download Report (En)
Apr 6, 2020	Heap Overflow in Emerson OpenEnter Download Report (En)
Mar 27, 2020	Analysis of *CVE-2018-4843: Denial-of- Download Report (En)
Feb 15, 2020	Zebrocy Advances Social Engineering T Download YARA Rule IOC Report (En)
Dec 2, 2019	Biometric data processing and storage Download Report (En)
Nov 22, 2019	VNC vulnerability research Download Report (En)

ics-cert-query@kaspersky.com

ICS Reporting subscription:

- Threat landscape reports
- APT reports
- Vulnerability research
- Advisories

World-wide | Logistics

Sample advisory

Advisory KLCERT-18-001 Denial-of-Service Vulnerability via PROFINET DC... 2 / 21

Attack conditions

The attack must be launched from an adjacent to the targeted system network: specifically from the same ETHERNET segment.
No user interaction required.
No privileges required.

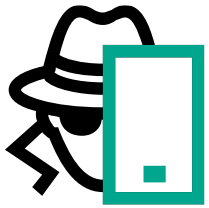
Impact

Vulnerability exploitation can severely affect availability of the targeted system.
Human interaction is required to recover the system.

Affected products

	CPU model	Firmware
1.	Siemens SIMATIC S7-300 CPU 314C-2 PN/DP (6ES7314-6EH04-0AB0)	All versions <V3.3.16
2.	Siemens SIMATIC S7-300 CPU 315-2 PN/DP (6ES7315-2EG10-0AB0)	All versions
3.	Siemens SIMATIC S7-300 CPU 315-2 PN/DP (6ES7315-2EH13-0AB0)	All versions
4.	Siemens SIMATIC S7-300 CPU 315-2 PN/DP (6ES7315-2EH14-0AB0)	All versions <V3.2.16
5.	Siemens SIMATIC S7-300 CPU 315F-2 PN/DP (6ES7315-2FH10-0AB0)	All versions

Attributing threats



Quickly identify the actor behind the attack

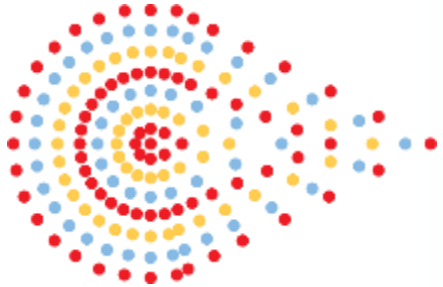
Detect and investigate based on available intelligence on the APT family

Act immediately and set up up proper containment procedures

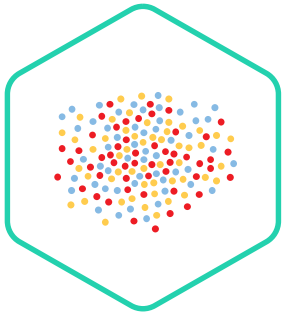
Kaspersky Threat Attribution Engine

SAMPLE

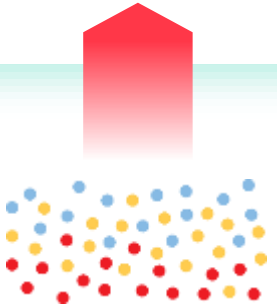
ATTRIBUTION ENGINE



DNA Extractor



DNA Matcher



New APT and clean files genotypes (updates)

ExPetr/NotPetya

Lazarus

WannaCry

Equation

Use cases for Attribution Engine and APT Intelligence Reporting

Use case	Key objective	Intelligence provided
Incident validation and prioritization	• Determine which incidents are likely to pose a risk, and prioritize them	• IoCs or malware samples linked to context and situational awareness
Incident analysis	• Answer who/what/why/when/how questions about attacks • Determine if attacks are still in progress and identify the impact	• IoCs or malware samples with links to 'context' about campaigns, threat actors and targets • Knowledge base with detailed information about APT profiles, attack histories and techniques
Containment and remediation	• Disrupt attacker communications • Remove malware and reverse changes • Eliminate vulnerabilities	• Knowledge base with detailed information about APT profiles, attack histories and techniques • IoCs or malware samples linked to known APT actors to take effective countermeasures
Hunt missions	• Uncover previously undiscovered attacks related to current incidents or to threats targeting the specific industry, geolocation, etc.	• IoCs or malware samples with links to 'context' about related attacks

Partnerships

SIEM/SOAR/IRP

Threat Intelligence Platforms


Network security controls

kaspersky

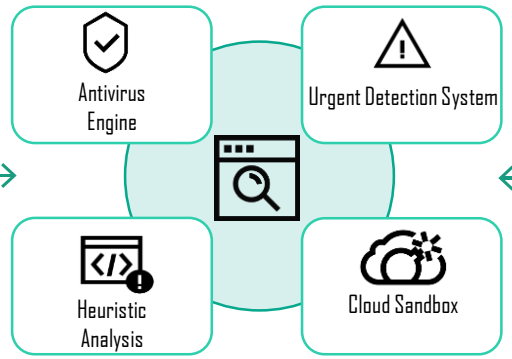
카스퍼스키 위협 인텔리전스 포탈 Freemium

Kaspersky Threat Intelligence Portal (freemium) (opentip.kaspersky.com)

Objects to analyze

- Files
- URLs
- Domains
- IP addresses
- Hashes

Kaspersky Threat Intelligence Portal



Lookup

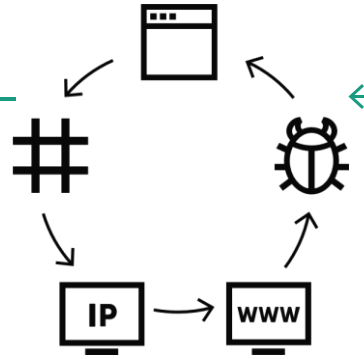
Web Service

Incident Response

- Is it malicious?
- Are we vulnerable?

Automated Correlation

Contextual Intelligence

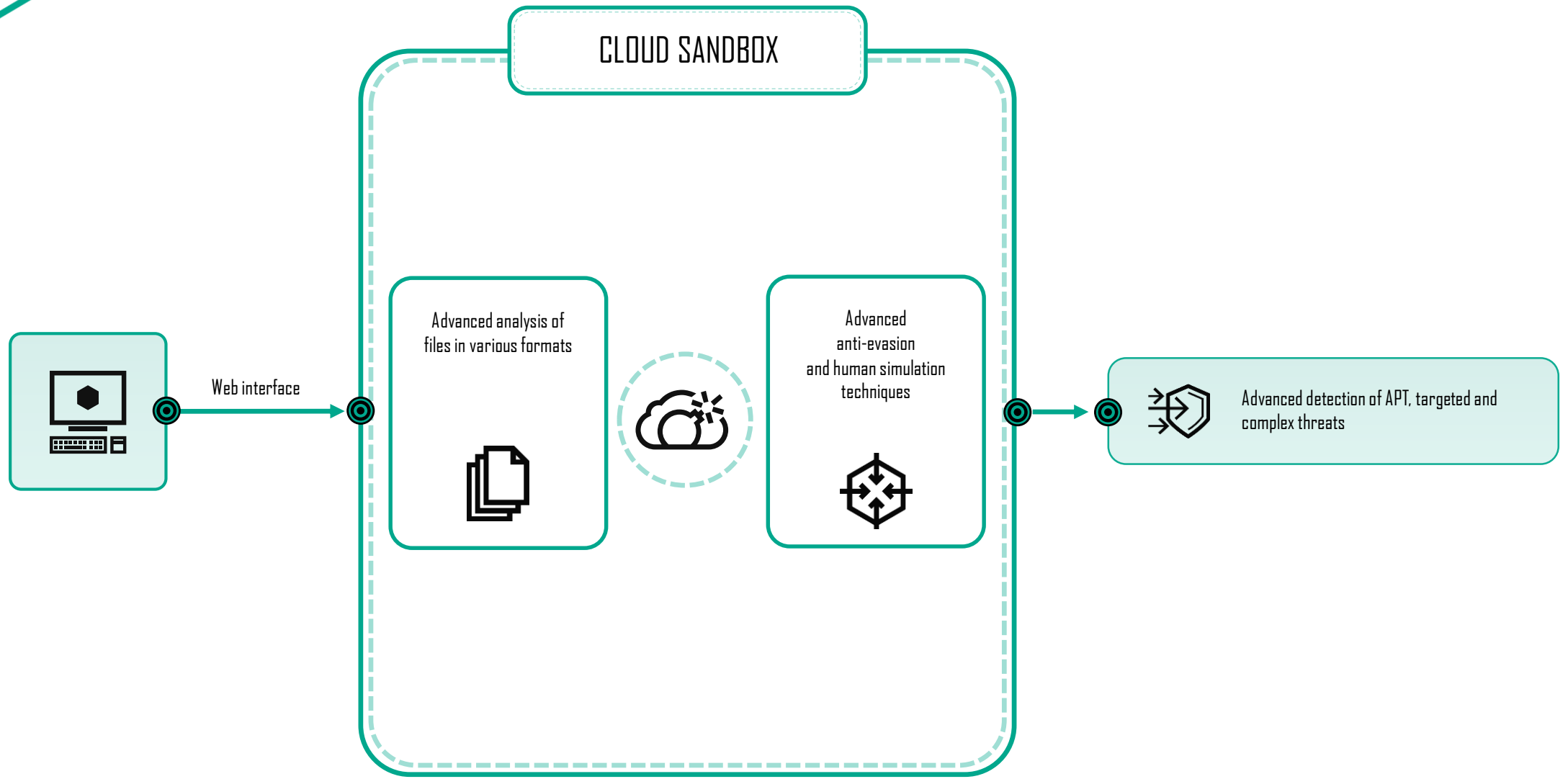


Intelligence

Sources

- Kaspersky Security Network
- Security partners
- Spam traps
- Networks of sensors
- Web crawlers
- Botnet monitoring

Kaspersky Cloud Sandbox (freemium)



Kaspersky
Threat Intelligence Portal

EN | Login

Analyze files

Drag and drop file here to start analysis

Browse...

File size up to 256 MB

Hash, IP address, domain, or URL

Enter your request here

Look up

By submitting a file or requesting lookup data, you agree to our Terms of Use and Privacy Statement.

Public submissions

kaspersky

Kaspersky
Threat Intelligence Portal

Login

Hash, IP address, domain, or URL

Enter your request here

Look up

By requesting lookup data, you agree to our Terms of Use and Privacy Statement.

A375E3507978C4C0AFDC2FB9E85E74BD
Malware

‹ Public submissions

Report for hash: Malware

A375E3507978C4C0AFDC2FB9E85E74BD

Hits	≈ 1,000	Format	PE	MD5	A375E3507978C4C0AFDC2FB9E85E74BD
First seen	Feb 27, 2017 19:04	Size	248.24 MB	SHA-1	180CEF6E0BE51928DC004DAEC38F14E205A0E7D2
Last seen	Oct 17, 2019 04:11	Signed by	—	SHA-256	709ADA832565BD617A49B5BEFF9E2019DC4FB2C90C196F0B9881E069C131110F
		Packed by	—		

Detection names

May 31, 2019 14:35
HEUR:Trojan.Win32.Generic

Oct 17, 2019 04:30
UDS:DangerousObject.Multi.Generic

Dynamic analysis summary

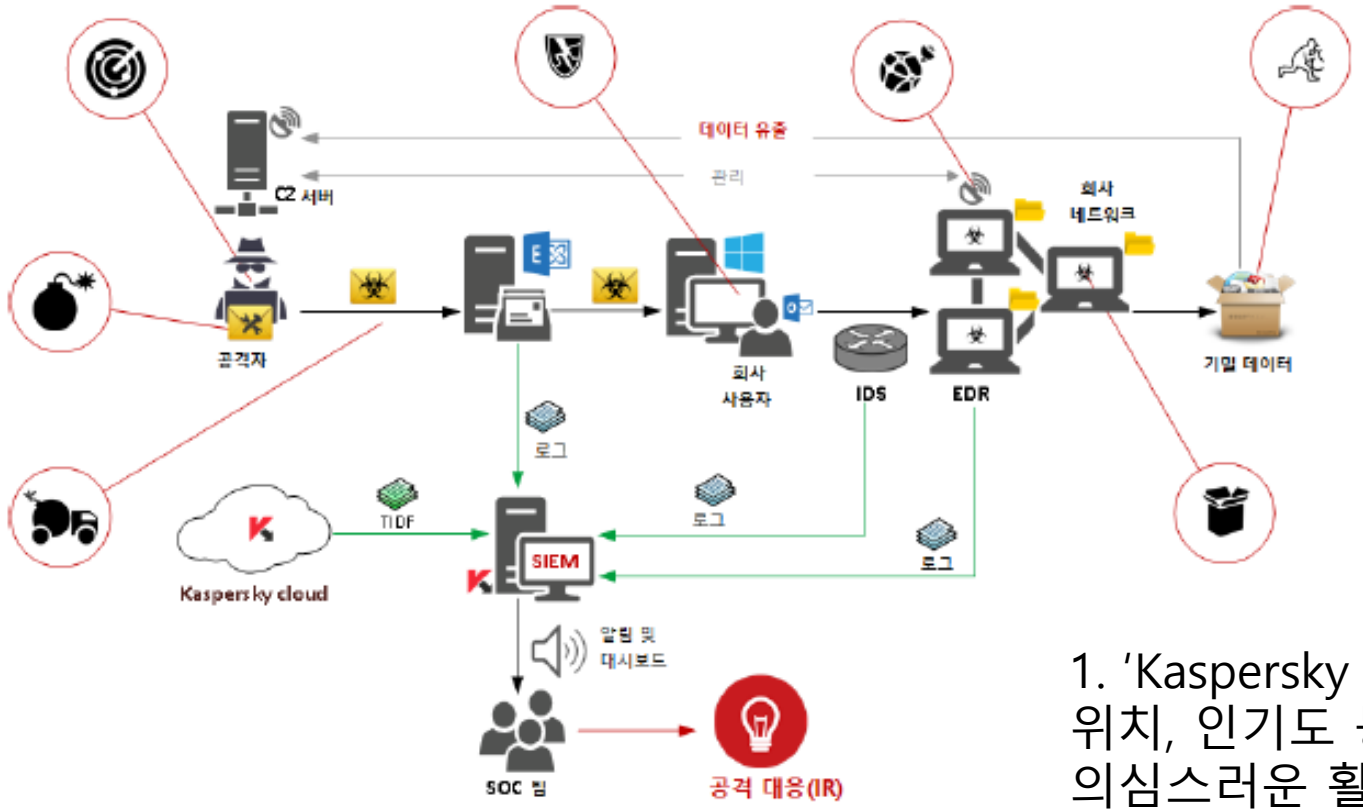
Premium Access to Kaspersky Threat Intelligence Portal is required to view a detailed Kaspersky Cloud Sandbox report.

Last scan performed at Wed, Oct 16, 2019 with anti-virus databases updated at Wed, Oct 16, 2019

kaspersky

SIEM 연계 사례

기밀 정보 침해 방지



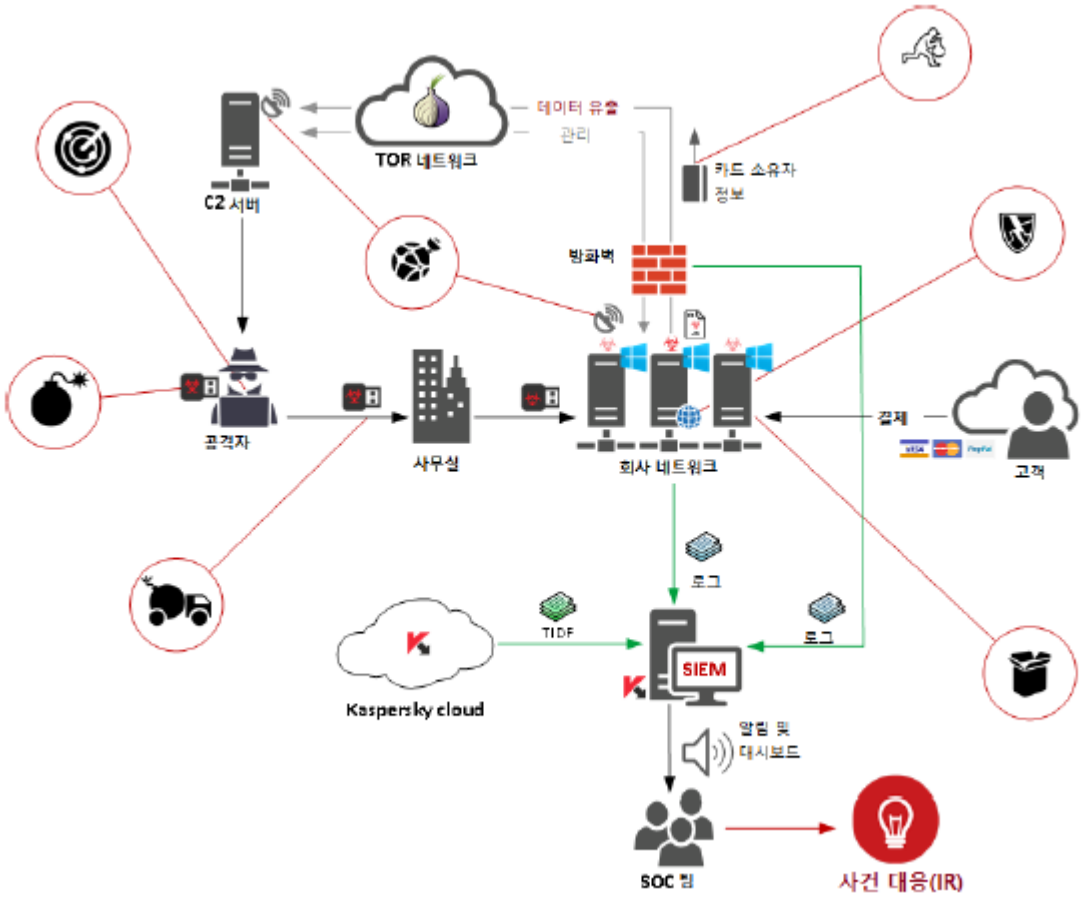
비즈니스 피해:
- 평판 하락 위험
- 지적 재산권 손실
- 수익 하락

적용 피드:
- Kaspersky IP Reputation Feed
- Kaspersky Malicious Hash Feed

1. 'Kaspersky IP Reputation Feed'를 통해 특정 IP 평판, 지리적 위치, 인기도 등에 대한 최신 정보를 제공받은 덕분에 SOC 팀이 의심스러운 활동 수행에 대해 위험성을 판단하고 선제적 방어 장치 통합을 통해 데이터 침해를 방지할 수 있었습니다.

2. 'Kaspersky Malicious Hash Feed'를 통해 가장 보편적으로 사용되는 위험한 악성 개체에 대한 최신 정보를 제공받은 덕분에 SOC 팀에서 기업 데이터 내부의 악성 코드를 탐지할 수 있었습니다.

사기 방지



비즈니스 피해:
- 평판 하락 위험
- 수익 하락

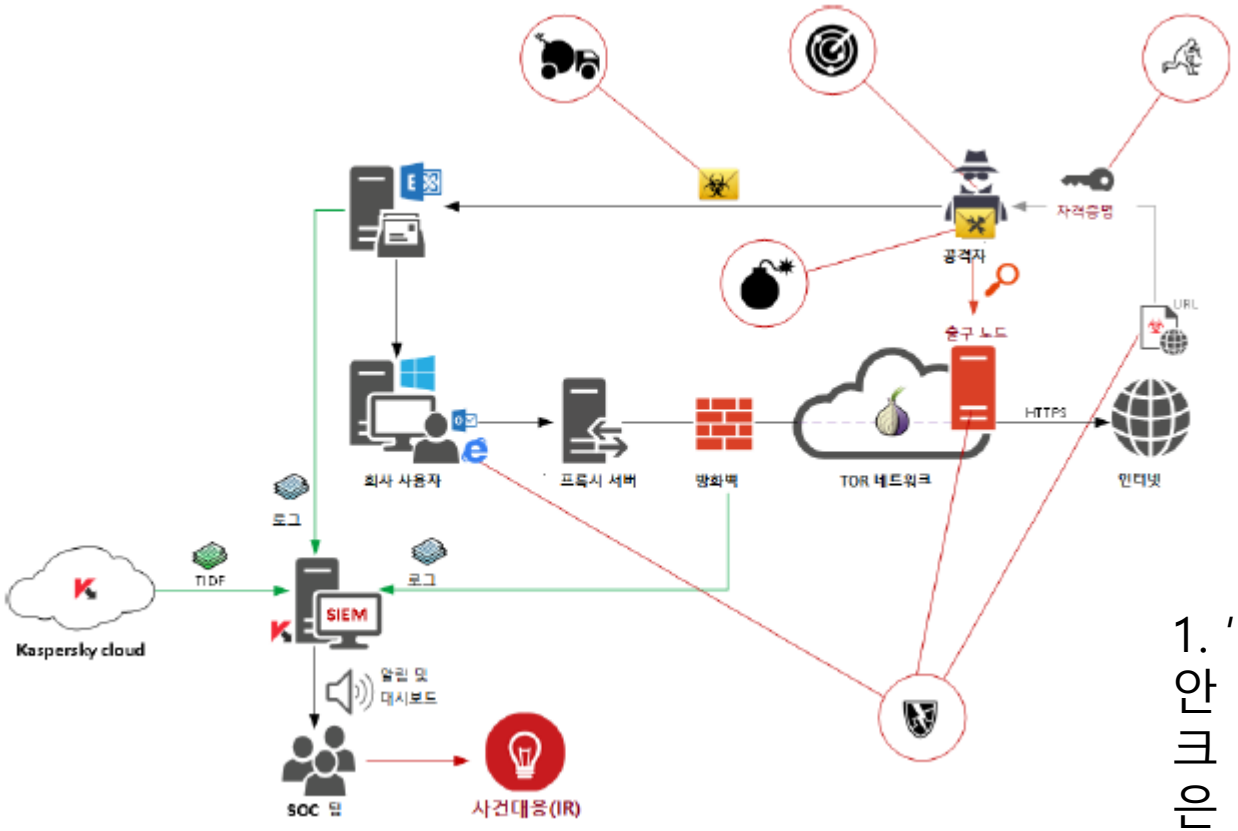
적용 피드:
- Kaspersky Botnet C&C URL Feed
- Kaspersky IP Reputation Feed
- Kaspersky Malicious Hash Feed

1. 'Kaspersky Botnet C&C URL Feed'를 통해 SOC 팀은 다음과 같은 최신 정보를 제공받았습니다.
- C2 서버 IP, 지리적 위치, 인기도 등, SOC 팀이 봇넷 활동을 파악할 수 있는 정보
- 해당 봇넷과 관련된 악성 파일 해시

2. SOC 팀은 'Kaspersky IP Reputation Feed' 덕분에 Tor 출구 노드에서 웹 서버로 전송된 의심스러운 트래픽을 파악할 수 있었습니다.

3. SOC 팀은 'Kaspersky Malicious Hash Feed' 덕분에 기업 네트워크 내의 감염된 호스트에 대해 실제로 활용할 수 있는 정보를 제공받았습니다.

내부자 위협 방지

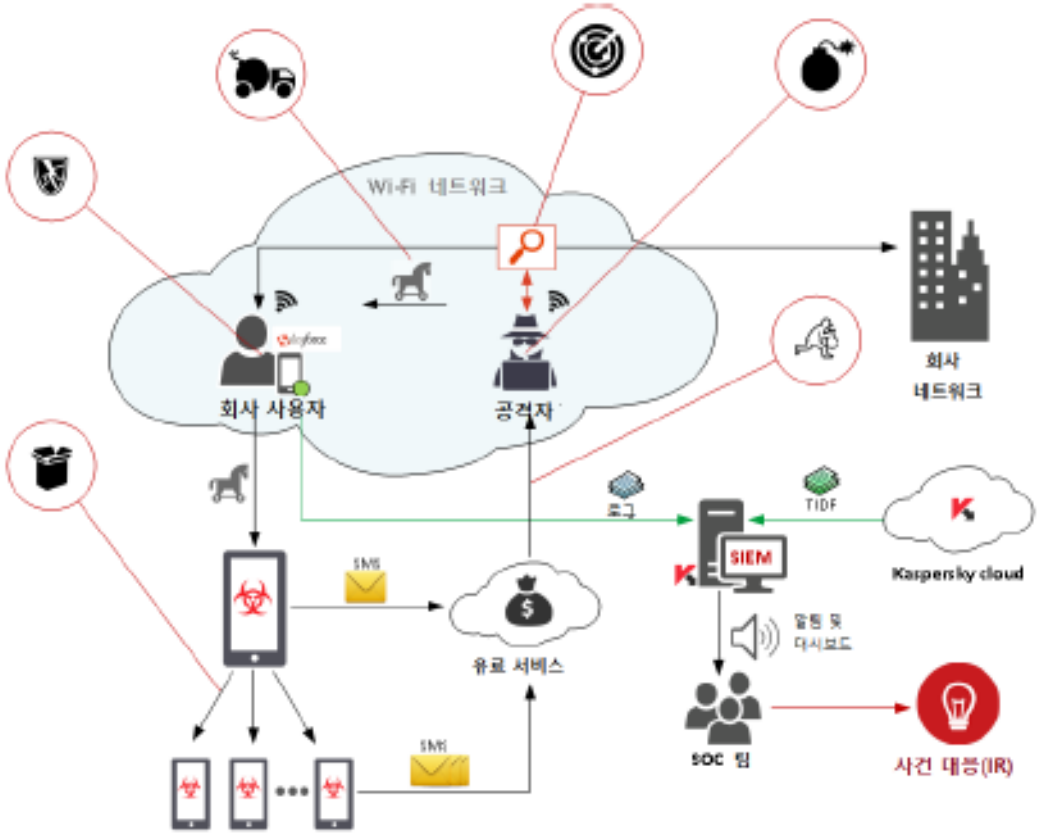


비즈니스 피해:
기밀 정보 유출
비즈니스 연속성 중단
수익 하락

적용 피드:
Kaspersky Malicious URL Feed
Kaspersky Phishing URL Feed

1. 'Kaspersky Malicious URL FEED'는 모든 악성 URL의 보안 배경 정보(인기도, 호스팅된 IP 주소, 지리적 위치, 마스크 등)와 관련된 최신 정보를 제공합니다. 덕분에 SOC 팀은 공격의 근본 원인을 찾아내고 적절한 대응 조치를 취할 수 있었습니다.
2. SOC 팀은 'Kaspersky Phishing URL FEED' 덕분에 일반적으로 피싱 공격과 관련 있는 신뢰할 수 없는 IP 주소를 통해 직원의 인증 정보가 탈취된 사실을 파악할 수 있었습니다.

SMS 피싱 방지



비즈니스 피해:
평판 하락
항의 및 법무 비용 발생
수익 하락

적용 피드:
Kaspersky Mobile Malicious Hash 피드
Kaspersky Malicious URL 피드

1. SOC 팀은 'Kaspersky Mobile Malicious Hash 피드' 덕분에 회사 모바일 장치를 모두 검사하고 전체적으로 악성 코드를 제거할 수 있었습니다.
2. SOC 팀은 'Kaspersky Malicious URL 피드'를 통해 악성 코드 유포 출처였던 악성 URL 관련 최신 정보를 제공받았습니다.

kaspersky

스플렁크와 연동 방법

Kaspersky CyberTrace App for Splunk

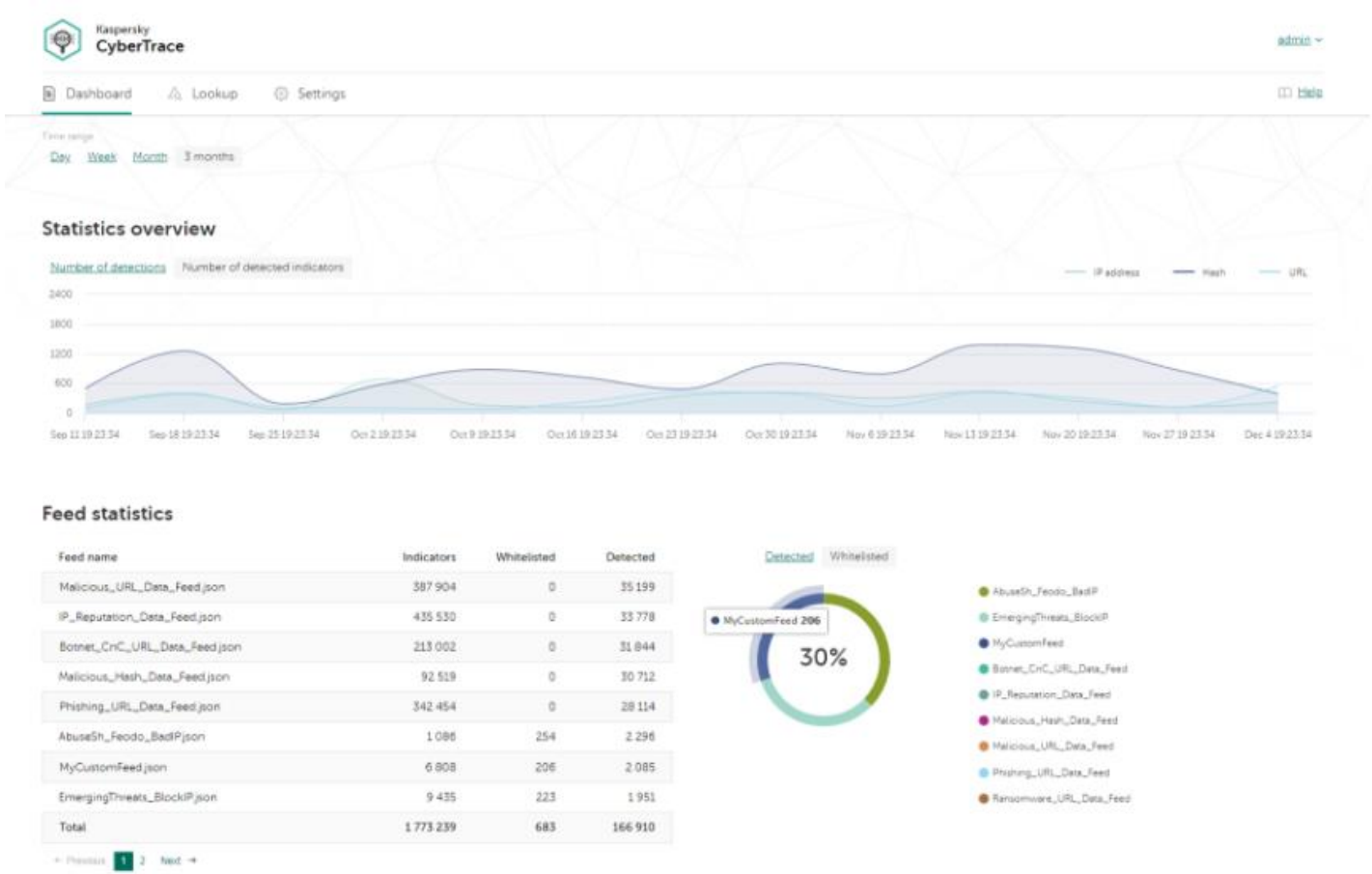
★★★★★ 3 ratings Splunk AppInspect Passed

Kaspersky Threat Intelligence Portal for Splunk

★★★★★ 4 ratings

Kaspersky Threat Feed App for Splunk

★★★★★ 1 rating Splunk AppInspect Passed



Kaspersky 위협 인텔리전스 서비스

위협 정보를 받아서 회사에 구축한 SIEM 시스템과 연동하여
효과적인 관제 시스템을 만들 경우 –

위협 데이터 피드, 사이버트레이스

위협 범죄 조직들의 지능형 공격 동향, 수법, 동기, 배후 등에 대한 광범위한
리포트 및 장기 보안 계획에 대한 정보를 얻어야 할 경우 –

APT 위협 인텔리전스 리포팅

금융권에 관련된 위협 범죄 조직들에 대한 리포트 및 복합적인 위협에 대한
장기 보안 계획에 대한 정보를 얻어야 할 경우 –

금융권 위협 인텔리전스 리포팅

오토모티브, ICS 등의 위협에 대한 지능형 공격 동향, 수법, 동기, 배후 등에 대한 광범위한
리포트 및 장기 보안 계획에 대한 정보를 얻어야 할 경우 –

오토모티브, ICS 인텔리전스 리포팅

위협 공격을 받을 때 드웰 타임 (dwell time)을 최소화 하기 위해 카스퍼스키 랩이
가지고 있는 위협 데이터의 상관 관계들을 룩업으로 사용하려는 경우 –

위협 상세 검색 서비스

악성 코드나 위협으로 의심되는 파일을 클라우드에서 샌드박스로 분석하려는 경우 –

클라우드 샌드박스, 리서치 샌드박스

APT 그룹의 공격 흔적을 빠르게 알고 싶은 경우 –

위협 흔적 (Attribute) 서비스

kaspersky

Q & A