사이버 위협 정보공유를 위한 국내외 노력

위협정보공유센터 김정희

September , 2018

KISA

We Will be a **Global Leader** in the **Internet** & **Security Field**

01 사이버 위협 (Cyber Threats)

02 사이버 위협 정보공유(Cyber Threat Information Sharing)

03 사이버위협정보분석·공유(C-TAS) 시스템

1

사이버 위협(Cyber Threats)

1 사이버 위협 (Cyber Threats)

개념 (Concept)

Possibility of a malicious attempt to damage or disrupt a computer network or system

- 정보시스템, 통신망에 연결된 디바이스 또는 통신망 자체를 손상시키거나 파괴할 수 있는 잠재적 요인
- 악의적 시도, 공격 행위 등

① (협의) **정보시스템, 통신망에 대한 직접적인 공격 정보로 공격IP, 악성코드 등 기술적 침해사고지표(IoC)**

- 해킹·컴퓨터 바이러스·서비스방해·전자기파 등 전자적 수단을 이용하여 정보통신망과 정보통신기기를 침입·교란·마비·파괴 하거나 정보를 절취·훼손·왜곡 전파할 수 있는 행위

②(광의) **기술적 침해사고지표(IoC)뿐 아니라 전략적 분석(예측 트렌드), 상황인지(공격 실시간 정보), 취약점, 조치·대응 방안, 사고 분석결과 등**

- 사이버공격 방법에 관한 정보, 악성프로그램 및 이와 관련된 정보, 정보통신망·정보통신기기 및 S/W의 보안상 취약점에 관한 정보, 그 밖에 사이버공격의 예방을 위한 정보

1 사이버 위협 (Cyber Threats)

정보 유형 (Information Type)

사이버 위협 정보를 생산, 소비하는 이해관계자(CEO/CISO, 관리자, 기술자)에 따라 다양한 유형이 존재

- 사고 예방 및 사고 대응 측면

구분	유형	종류	이용자	활용 예	기한	Source
예방	전략	* **위협 글로벌 트렌드, 위협 전망** * **침해사고 News**	C-Level 의사결정권자	조직 보안 전략 수립	장기	외부
예방	관리	* **침해사고 조사결과** * 취약점 조치 방안, 사고 대응복구 방안 * 중앙관리 S/W	IoT 보안 가이드 * 시큐어코딩 지침	CISO, 보안관리자	보안 실행계획, 보안 조직운영	중기	외부
대응	기술	* **침해사고지표(IoC)** (공격IP, C&C IP, 악성URL, 악성코드 등) * 악성코드 상세분석서 (공격자 IP, 공격유형, 취약점, 악용기술, 조치절차 등)	사고대응팀	공격 방어, 공격증거 수집	즉시	내·외부

2

사이버 위협 정보공유
(Cyber Threat Information Sharing)

2 사이버 위협 정보 공유

KISA's Role

1. 침해사고 대응 조치 (Cyber Incident Response)

- **침해사고에 관한 정보의 수집 · 전파**, 침해사고의 예보 · 경보, 침해사고에 대한 긴급조치
- 주요정보통신서비스제공자, 집적정보통신시설 사업자와 **공동 대응**
- 소프트웨어 제작/배포자의 **보안취약점 수정 · 보완**
- 국가 정보통신망 안전에 필요한 경우 관계 기관에게 **침해사고 관련정보 제공**

2. 이용자 정보보호 (Information Protection)

- 이용자의 정보보호에 필요한 기준을 정하여 권고
- **침해사고 예방 및 확산 방지를 위한 취약점 점검, 기술 지원** 등 조치

3. 침해사고 대응 국제협력 (International Cooperation)

- 다른 국가/국제기구와 상호 협력
- **정보통신망의 안전성 침해행위 방지 업무, 정보통신서비스의 안전한 이용에 관한 업무**

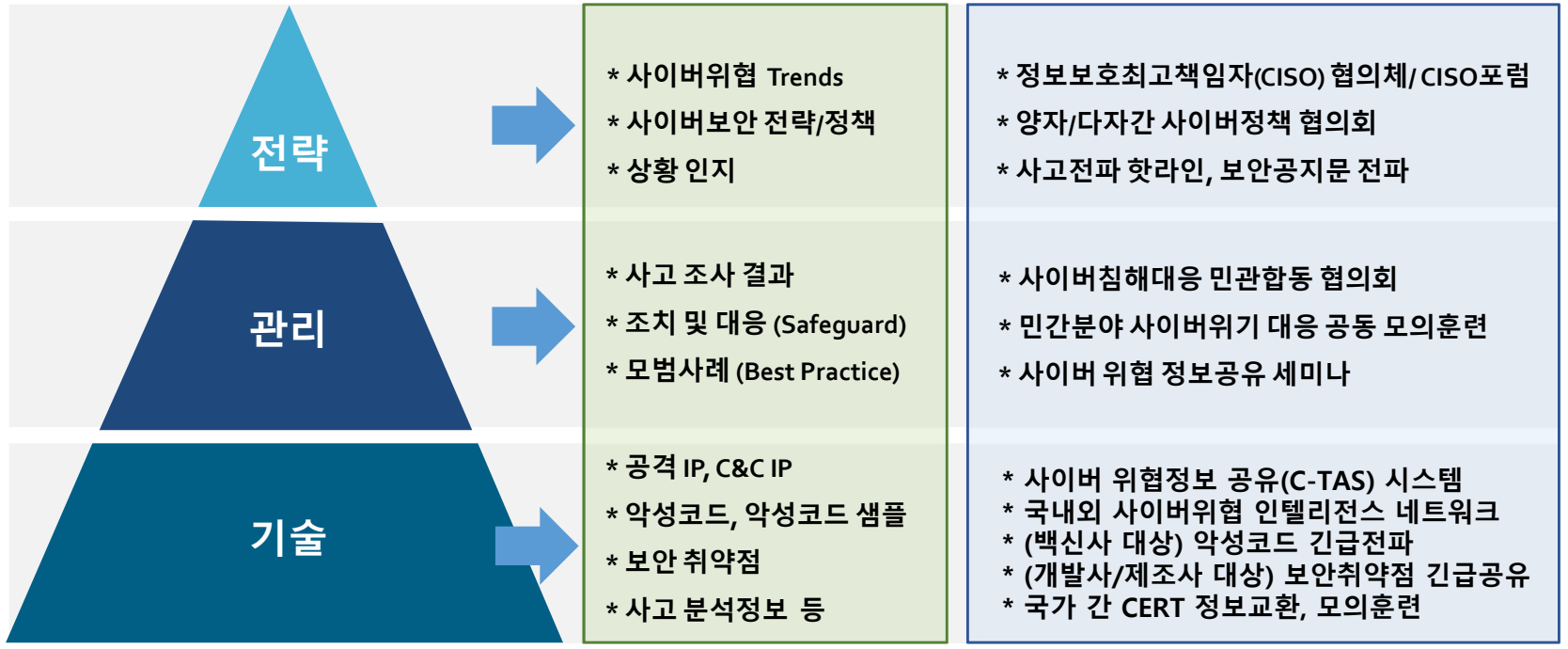
2 사이버 위협 정보 공유

KISA's Role

침해사고 예방/대응 협력 네트워크의 이해당사자

2 사이버 위협 정보 공유

KISA-정보공유/협의 활동



3

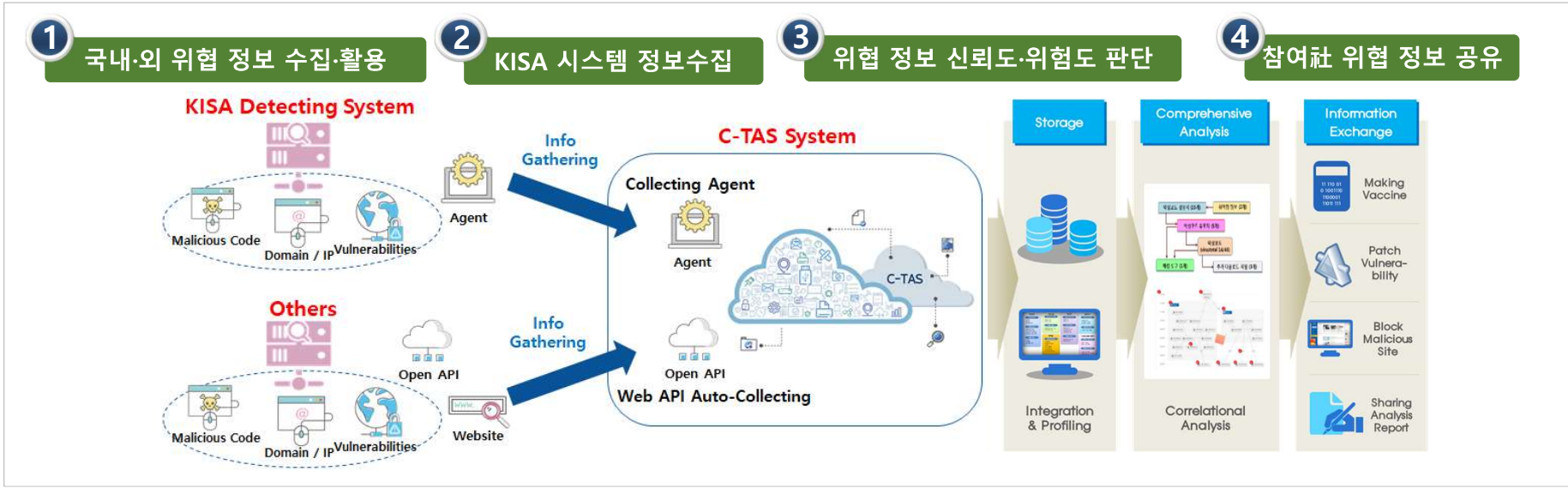
사이버위협정보 분석·공유(C-TAS) 시스템

3 사이버위협정보분석·공유(C-TAS) 시스템

Cyber Threat Analysis and Sharing(C-TAS) 시스템

민간분야 침해사고 확산 방지를 위하여 사이버 공격 시도 등을 수집분석하여 참여社와 함께 공유하는 플랫폼

- **악성도메인, 악성 IP, 악성코드** 등 KISA 자체 시스템(DDoS 사이버대피소, MC-Finder 등), 글로벌 공격 정보(타 국가 CERT), 참여社 공유 정보
- 통신, 보안관제/장비, 호스팅, 게임, 포털 등 분야의 **222개社** 참여 ('18.8)



3 사이버위협정보분석·공유(C-TAS) 시스템

Cyber Threat Analysis and Sharing(C-TAS) 시스템 – 공유 정보

총 36개 종류의 위협 정보를 구분하여 C-TAS 시스템을 통해 공유

단일지표	악성코드, C&C, 감염IP, 공격시도IP, 유포지, 피싱, 파밍, 스미싱, 정보유출지 등	IoC (Indicator of Compromise)
분석보고	기술문서, 보안공지, 악성코드분석보고서, 악성모바일앱 분석보고서	-
추이정보	일간/주간/월간 추이	특정 관찰 기간 동안 전구간의 전체 지표와 비교하여 여러 수집처에서 발견한 정보, 해당 관찰시간에 재등장한 정보
지속정보	일간/주간/월간 지속	특정 관찰기간 동안 시간 기준으로 연속하여 등장하는 정보
중복정보	일간/주간/월간 중복	특정 관찰기간 동안 수집처 기준으로 여러 곳에서 등장하는 정보
동향정보	일간/주간/월간 동향	특정 관찰기간 동안 추이 또는 지속, 중복 등 다양한 속성의 최신경향 정보
핵심정보	일간/주간/월간 핵심	특정 관찰기간 동안 추이 및 지속, 중복성을 두루갖춘 고활동성 정보
중개지표	어뷰징IP, 상황전파/해제문, 원클릭서비스 등	-

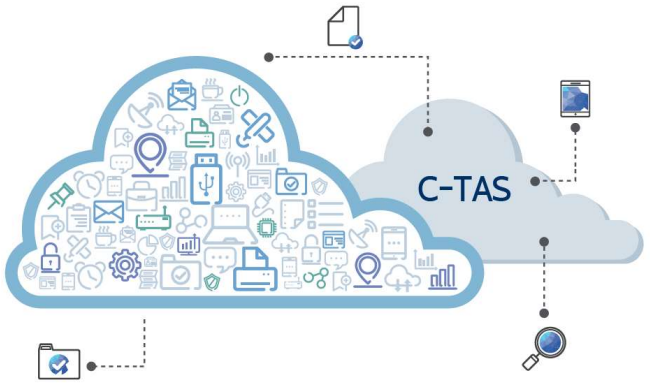
3 사이버위협정보분석·공유(C-TAS) 시스템

Cyber Threat Analysis and Sharing(C-TAS) 시스템 – 공유 방식

API(실시간 자동 공유 가능) 및 홈페이지를 통한 다운로드 방식

- API를 이용할 경우 실시간으로 자동 공유 가능
- 홈페이지의 경우, 이용자가 필요시 접속하여 정보 조회 및 다운로드 가능

Malicious Domain
…
Phishing Domain
Malicious IP
…
Malware
Web Shell
Vulnerability



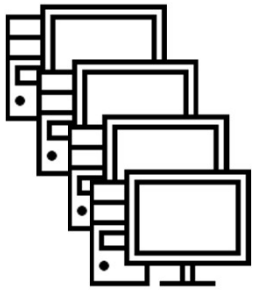
C-TEX & STIX 2.0 (2018)

The ways to disseminate are :

① Web API (export API) & TAXII (2018)

② Website (https://cshare.krcert.or.kr)

C-TAS Participants

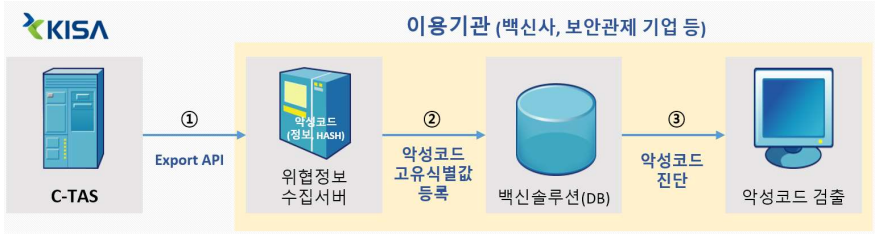


3 사이버위협정보분석·공유(C-TAS) 시스템

Cyber Threat Analysis and Sharing(C-TAS) 시스템 – 활용사례

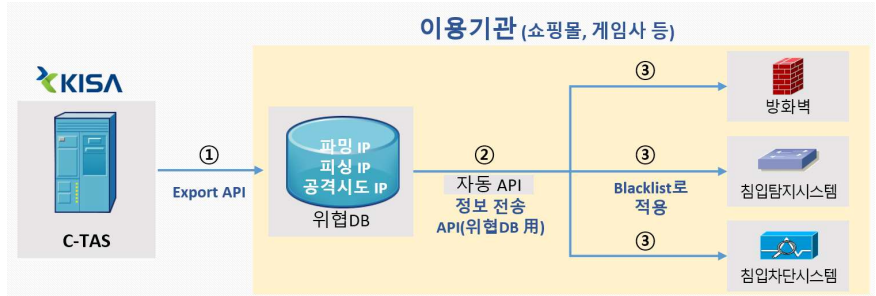
① 악성코드 차단

- 악성코드의 고유 식별값을 자사 백신 솔루션의 탐지룰에 업데이트 하여 악성코드 차단



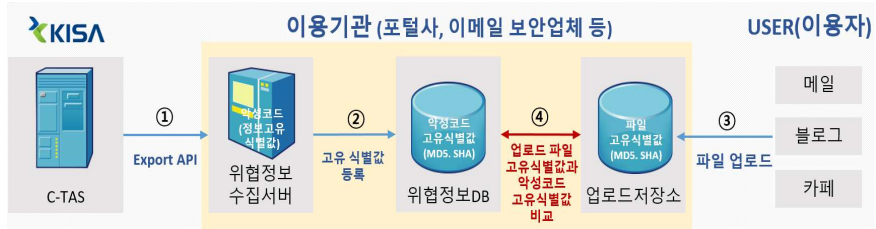
② 악성 IP 차단

- 악성 IP(파밍IP, 피싱IP, 공격시도IP 등)를 보안장비(방화벽, 침입탐지시스템 등) 블랙리스트에 추가하여 공격 차단



③ 악성파일 업로드 탐지·차단

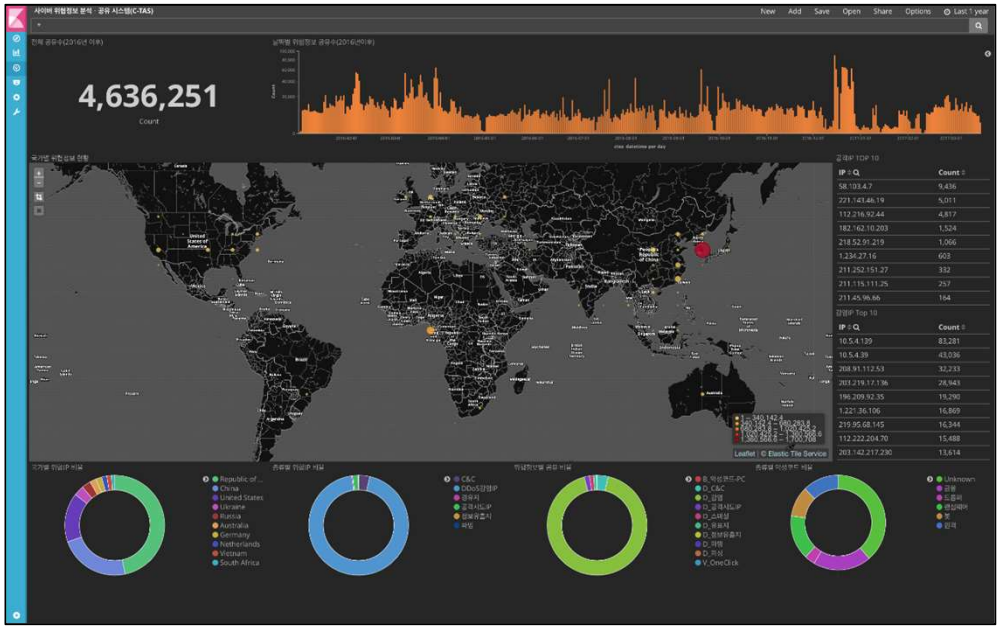
- 웹서비스를 통해 업로드 되는 파일과 고유식별값을 비교하여 악성파일 차단



3 사이버위협정보분석·공유(C-TAS) 시스템

Cyber Threat Analysis and Sharing(C-TAS) 시스템 –시각화 도구

기업에서 활용 가능한 위협정보 시각화 도구 제공



▪ Dashboard

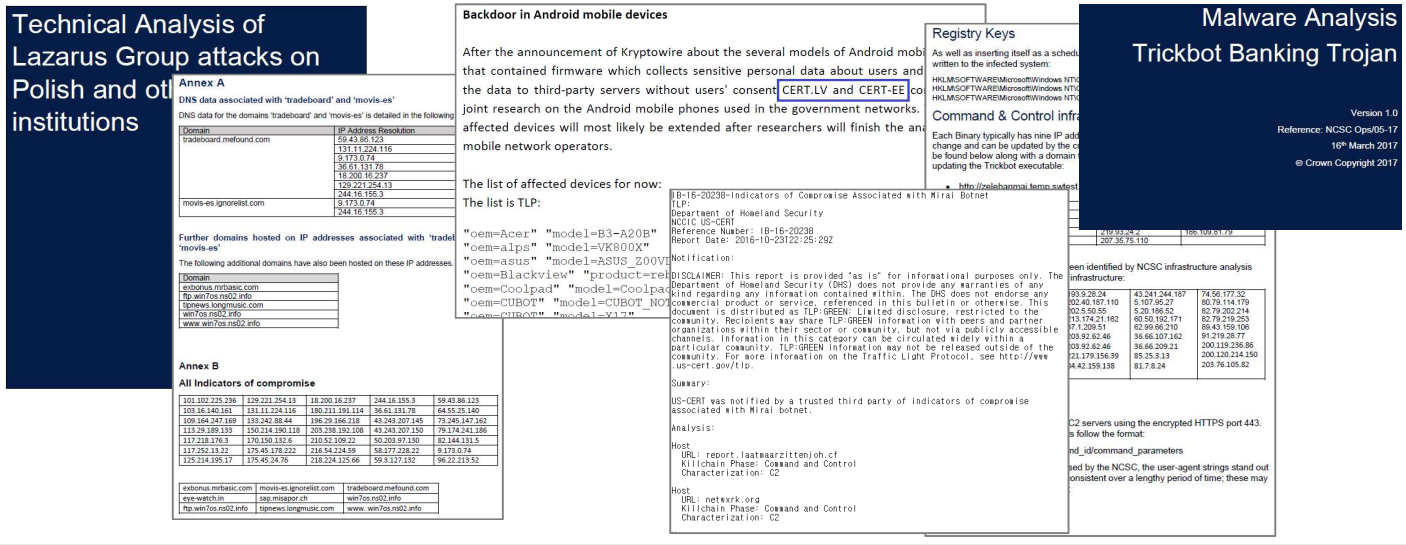
▪ Search

3 사이버위협정보분석·공유(C-TAS) 시스템

위협 정보수집 강화 – Incident Response with National CERTs

국가 간 CERT 협업(美,中,日,英 등) – 침해사고 中心

- 국가 CERT 연락망을 통해 침해사고 중심의 정보를 TLP 규약에 따라 정보공유
- 사이버공격 비상대응 핫라인을 통해 단순 사고정보 뿐 아니라 사고 연관성 정보(공격분석보고서, 악성코드 등) 등 고품질 위협 정보 확보 (TLP 규약 준수)



3 사이버위협정보분석·공유(C-TAS) 시스템

위협 정보수집 강화 – Incident Response with National CERTs

국가 간 CERT 협업 – 중점 협력국 확대

- 유럽(영국, 에스토니아, ENISA), 아시아(대만, 홍콩) 권역에 사이버 위협정보 공유를 위한 협력 파트너 확보
- (다국적) 국제사고침해대응협의회(FIRST), 아태침해사고대응협의체(APCERT) 공동모의훈련 등

3 사이버위협정보분석·공유(C-TAS) 시스템

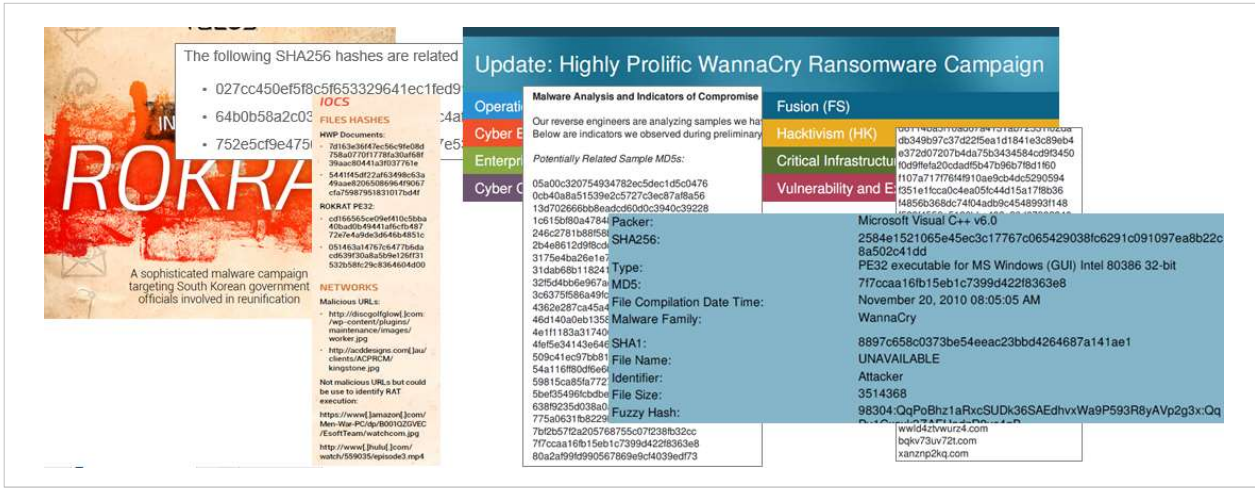
위협 정보수집 강화 – 글로벌 사업자

플랫폼 사업자

- **(Google)** Safe browsing을 통한 악성코드 탐지 협력
- **(Microsoft)** Government Security Program(GSP), Cloud Security, Cyber Security Framework(vulnerability information, malicious code, and mitigation guide)
- **(Facebook)** Threat Exchange 위협정보교환 협력

글로벌 보안 기업

- FireEye, Fortinet, McAfee, Microsoft, Palo Alto Networks, Symantec, CISCO 등

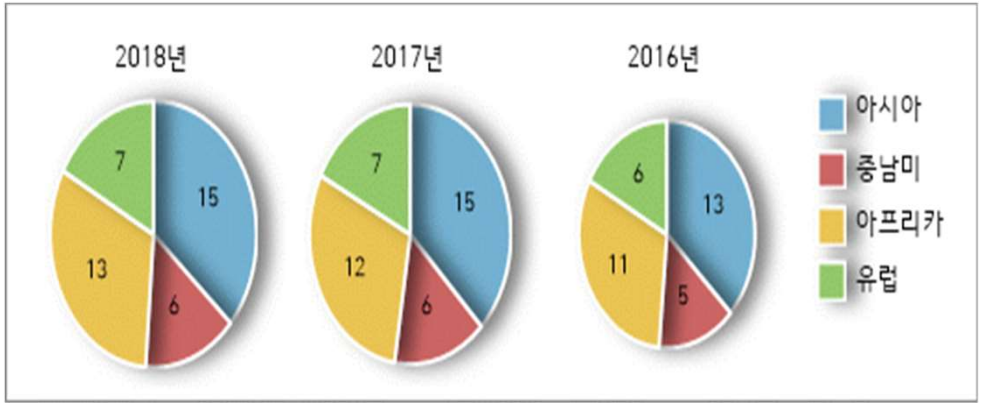


3 사이버위협정보분석·공유(C-TAS) 시스템

위협 정보수집 강화 – GCCD와 CAMP

글로벌 사이버보안 협력 네트워크 (CAMP, Cybersecurity Alliance for Mutual Progress)

- 국경없이 발생하는 고도화, 지능화된 사이버위협에 공동 대응하고, 사이버 보안 협력 사안을 함께 논의, 발전시켜 나가기 위한 협의체
- 다양한 침해사고 대응 경험과 정보보호 노하우, 사이버보안 전략과 경험을 국제사회에 공유·전파
- 정보공유, 사고 공동대응, 역량강화 등 사이버보안 발전을 서로 돕는 글로벌 사이버보안 허브 기능



< CAMP 플랫폼을 통한 사이버보안협력 >

구분	사이버보안 기술	사이버보안 정책	사이버보안 역량강화
정보 공유	· 신규 위협정보 · IoT 등 융합환경 보안기술 · CERT 구성·운영 가이드	· 사이버보안전략·표준 · 사이버보안 법령/체계 · 회원국 시장 트렌드 등	· 전문가 교육(K-Shield) · 자격인증(정보보안기사 등) · 인식제고 캠페인
공동 활동	· 침해사고 모의훈련 · **취약점 컨설팅 (GCCD)** · **PKI, CSIRT 등 F/S**	· 사이버보안 공통보안수칙 · **공동세미나 (GCCD)** · **정책 컨설팅 (외부기관)**	· **APISC CSIRT 교육** · **역량진단 (WB-OXF-GCCD)** · **초청연수**

CAMP(Cyber security Alliance for Mutual Progress) 플랫폼

KISA

안전한 사이버 세상을
만들기 위해 노력하겠습니다

국민 안심, 국가 안전

한국인터넷진흥원이 함께 합니다 !