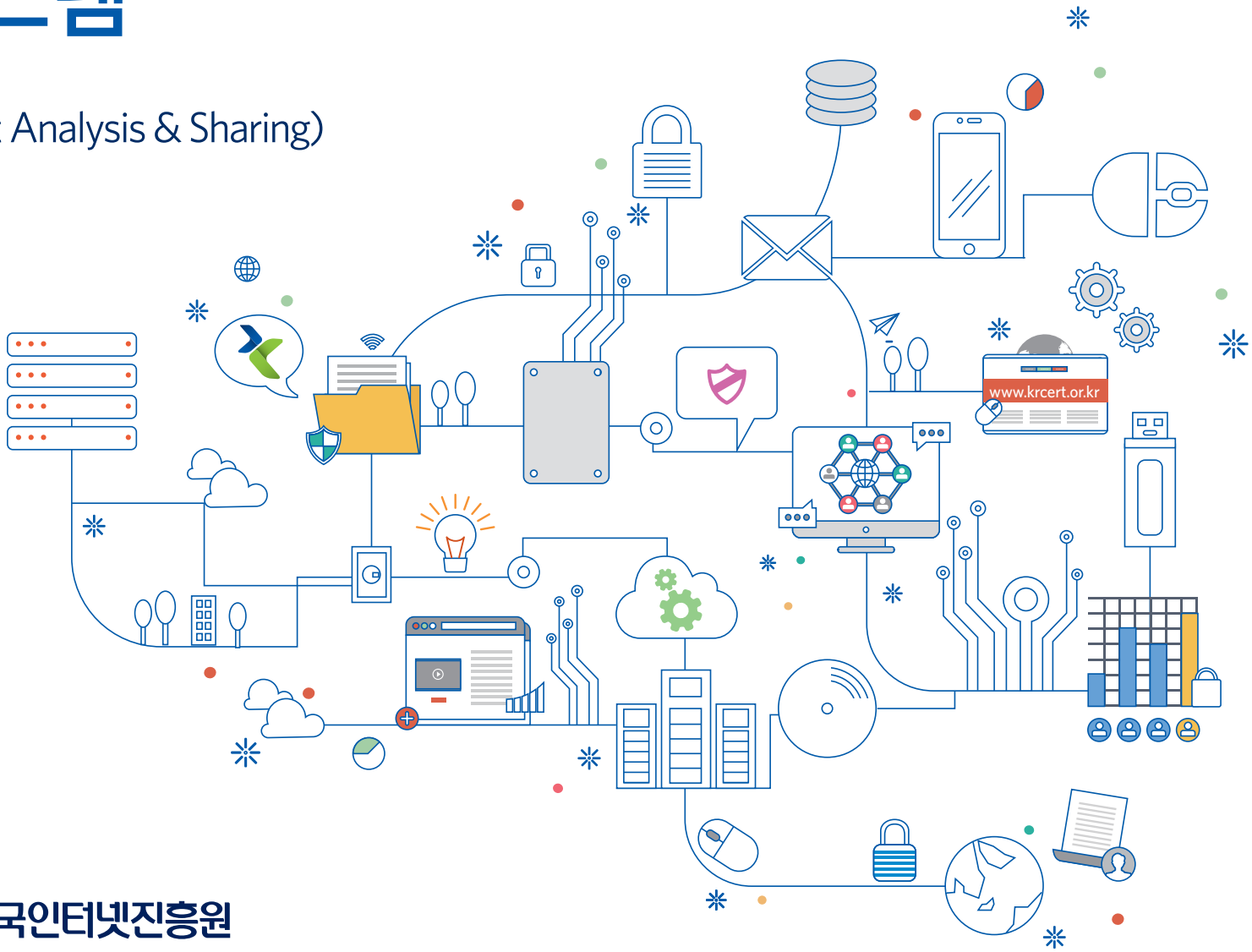
행복한 대한민국을 여는 정부 3.0

[개방 · 공유 · 소통 · 협력]

사이버위협정보 분석·공유시스템

C-TAS (Cyber Threat Analysis & Sharing)



미래창조과학부

KISA 한국인터넷진흥원

사이버 위협정보 분석·공유 시스템

C-TAS(Cyber Threat Analysis & Sharing) System

여러 산업분야에 걸쳐 광범위하게 발생하고 있는 침해사고에 대응하기 위한 사이버 위협정보 수집·분석·공유 시스템

위협 정보 공유 필요성

사이버 위협 증가

- 지속되는 APT위협
- 랜섬웨어 및 악성코드 증가
- IoT 기기 해킹과 DDoS 공격 증가

→ 사이버 위협의 지능화·고도화, 사이버 범죄집단의 전문화·조직화 →

사이버위협정보 공유를 통한 협력 및 신속한 사고 대응

C-TAS 위협정보 종합분석

- 수집된 위협 인텔리전스의 유효성 및 평판 검증
- 고위험 사이버 공격 징후 및 연관성 분석
- 위협 인텔리전스 유형별 수집 공유 현황 통계
- 인메모리 그래프 데이터베이스 기반 통계분석

정보 수집

❶ 침해사고 정보
❷ 공격시도IP
❸ 악성코드
⋮

종합 분석

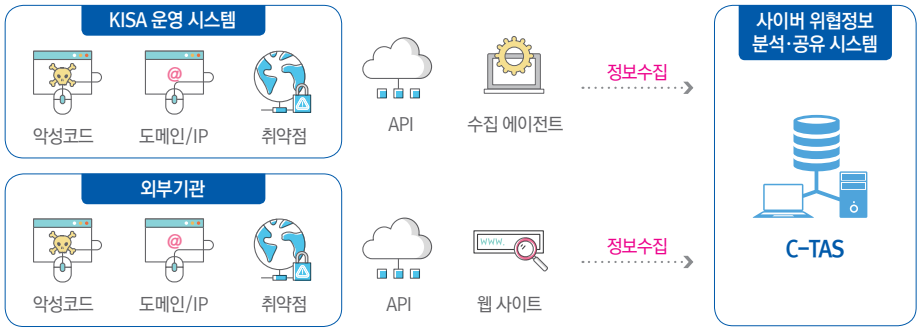
수집정보의 평판 검증 및
통계·연관성 분석

정보 공유

API, 홈페이지를
통한 공유

- 각종 사이버 위협정보의 빅데이터 기반 통합 저장·관리 체계 구축
- 저장된 대량의 정보 中 특정 위협 정보(도메인, IP, MD5 등)를 공유
- 단위 산업군별 정보 공유 희망 시 공유채널 제공 등 허브 역할 수행
- 위협정보 실시간 공유를 통한 침해사고 사전예방 및 피해 확산 최소화

C-TAS 위협정보 수집



- 한국인터넷진흥원 및 외부기관으로부터 위협정보 수집
- 수집된 위협정보를 유형별 분류 및 체계적 저장 관리

C-TAS 위협정보 공유

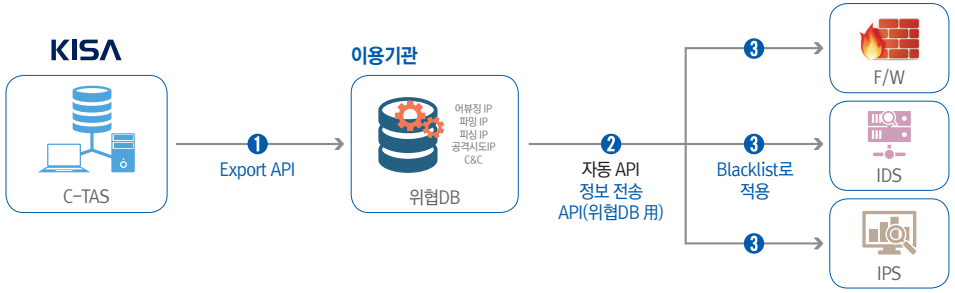
- **공유방법 :** API(실시간 자동 공유 가능) 및 홈페이지를 통한 다운로드 방식
- **공유정책 :** 양방향 정보공유, 권한관리를 통해 기관별 정보 공유 대상 및 범위 차등
- **공유정보 :** 8개 그룹, 36종 정보를 공유

No	구분	공유 정보 내역
1	단일지표	악성코드, C&C, 감염IP, 공격시도IP, 유포지, 피싱, 파밍, 스미싱, 정보유출지, 악성 이메일 등
2	분석보고	보안공지, 기술문서 등
3	추이정보	일간추이, 주간추이, 월간추이
4	지속정보	일간지속, 주간지속, 월간지속
5	중복정보	일간중복, 주간중복, 월간중복
6	동향정보	일간동향, 주간동향, 월간동향
7	핵심정보	일간핵심, 주간핵심, 월간핵심
8	중개지표	어뷰징IP 등

C-TAS 위협정보 활용 사례

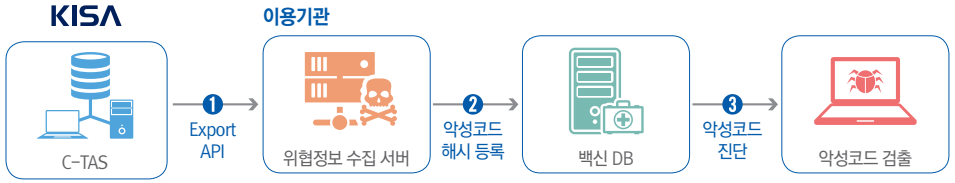
활용사례1 위협 IP 차단 Blacklist 적용

* **정보명** : 어뷰징IP, 파밍IP, 피싱IP, 공격시도IP, C&C
* 내부 DB에 저장 후 사내 IPS, IDS, F/W 등에 Blacklist로 적용



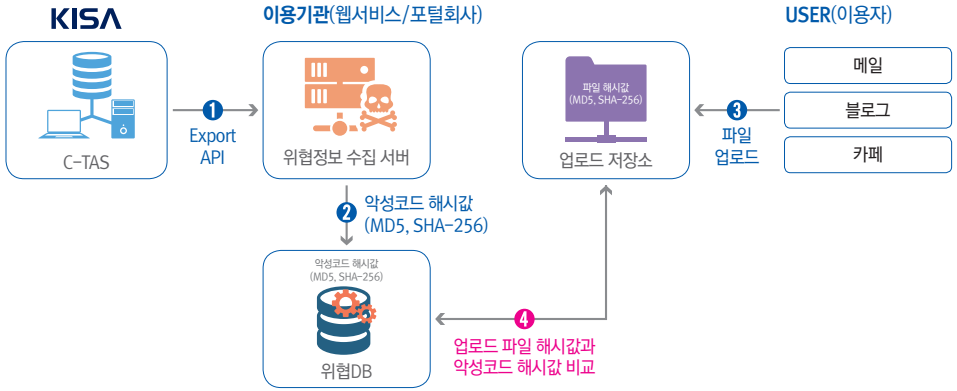
활용사례2 악성코드 대응 및 차단

* **정보명** : 악성코드
* DB(내부 위협 DB)에 저장 후 사내 백신 솔루션에 악성코드 해시(Hash)값 등록



활용사례3 악성파일 업로드 탐지 및 차단

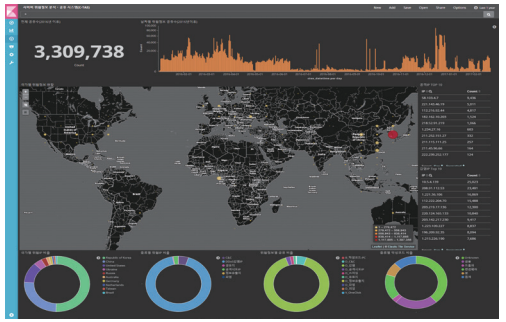
* **정보명** : 악성코드, 악성이메일
* 구축 DB(내부 위협 DB)에 저장 후 웹서비스를 통해 업로드 되는 파일과 해시값 비교



C-TAS 위협정보 활용 가이드 지원

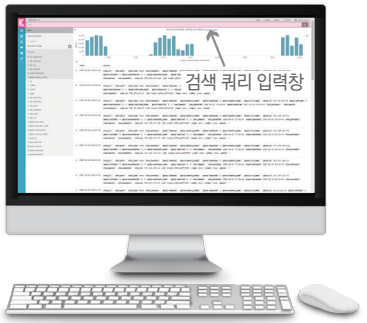
기업에서 활용 가능한 위협정보 시각화 도구 제공

* C-TAS 공유위협 정보를 사용자가 원하는 형태로 시각화해서 표현 가능



※ 사용자 커스터마이징을 통한 맞춤형 대시보드 구성 가능

* 검색 엔진을 통해 원하는 정보 검색 가능



C-TAS 가입 절차 안내

협의 단계 진행 후 정보공유사이트를 통한 가입 및 공유 단계 진행

협의 요청
사이버 위협정보에 대한 공유를 주제로 회원사와 협의를 요청하거나 진행하는 단계로
C-TAS 설명 및 취지, 활용 시 이점, 공유정책, 상호 관심정보를 논의

회원 신청
C-TAS에 회원 가입을 신청하는 단계로 '회원가입 신청서' 및 '보안서약서' 작성

정보 신청
C-TAS와 회원사간 공유할 정보에 대한 요청사항을 기록

API 활성
공유정보에 대한 자동 수집 및 제공을 위하여 API를 활성화하는 단계
회원사가 위협정보 표현 규격에 맞추어 C-TAS로 정보를 송부하고 공유 받음

정보 승인
C-TAS와 회원사간 공유할 정보에 대하여 최종 승인 처리

※ 각 단계를 종료할 때마다, 현재 진행현황 및 향후 단계를 시스템 이메일을 통해 자동 알림

협의 요청 및 기타 문의 ✉ help@cshare.krcert.or.kr (**자세한 내용은** www.krcert.or.kr**를 참고하여주시기 바랍니다**)