사이버위협 공동대응 플랫폼 사업

참여 안내

01 | 참여기업에게는 무엇을 지원해 주나요?

- 통합로그수집(SIEM) 및 자동대응(SOAR) **최신 보안장비 무상 제공**
  - * 제공 장비는 KISA에서 임차형태로 제공(*매년 운영 결과 평가로 기간 연장 및 임차 종료)
  - * 단, 통신회선 및 상면은 참여사 마련
- 통합로그수집 및 자동대응 보안장비 **설치 지원 및 장비운영 교육 제공**
- **KISA-참여기업**간 위협정보 **공유 핫라인 운영** 및 **최신 위협정보 제공**

02 | 사업에 참여하면 참여기업은 무슨 혜택이 있나요?

- 침해위협 대응 **업무 자동화**로 **위협 탐지 시간 단축** 및 **정확도 향상**
- 참여사 상황에 적합한 **대응절차(플레이북) 제작** 및 **운영 가능**
- KISA가 보유한 **최신 위협인텔리전스(TI) 정보 연계**를 통한 **위협 대응 정보 수집가능**
- 참여사 **보안업무 담당자가 일을 쉽고, 빠르고, 정확히 처리 가능**

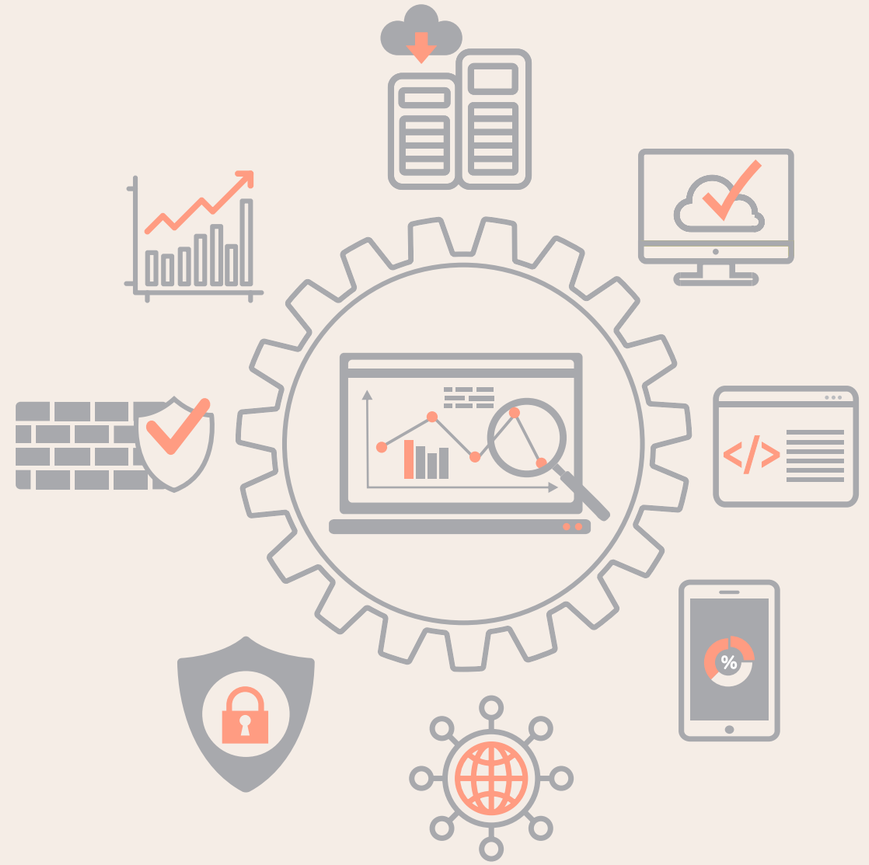
03 | 참여는 어떻게 할 수 있나요?

- **(모집방법)** 다수 사업자에게 서비스를 제공하는 **실시간 위협 탐지/대응이 필요한 기업**을 대상으로 **모집공고 안내**
- **(선정방법)** 모집기간 내에 제출한 **신청서 평가를 통해 구축 기업 선정**
- **(추진일정)**
  - (상반기) **참여기업 모집 및 선정**
  - (하반기) **참여기업 장비 설치 지원 및 장비 활용**

문의 : ctap@kisa.or.kr

사이버위협 공동대응 플랫폼 구축 사업

민간 분야 실시간 사이버공격 탐지, 대응 및 공유 체계 구축을 위한 시스템 지원



과학기술정보통신부

KISA 한국인터넷진흥원

사이버위협 공동대응 플랫폼 구축 사업

추진 배경

- 민간 주요기업과 실시간 사이버공격 탐지 · 대응 체계 구축 및 침해사고 대응협력 강화

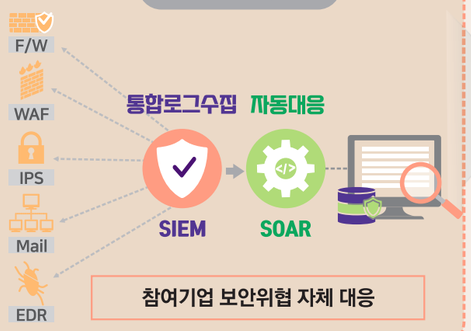
주요 내용

- 다중이용 서비스 제공 사업자(관제사, 호스팅, IDC등)와 실시간 위협정보 탐지, 대응 및 공유 체계를 구축하기 위해 기업에게 탐지된 위협 정보의 수집, 분석, 대응 및 공유를 위한 시스템 구축을 지원

플랫폼 체계도

통합로그수집 및 자동대응

참여기업



참여기업 보안위협 자체 대응

위협현황 통합 모니터링 및 대응

KISA

심층 분석 및 신규 위협 공유

이벤트 수집 및 탐지

↓

이벤트 분석 및 대응

- 다양한 사이버 위협 인텔리전스(CTI)와 실시간 연동 및 이벤트 분석
- 자동화 플레이북으로 보다 빠르고 효율적인 대응

추가 분석 이벤트 수집 및 분석

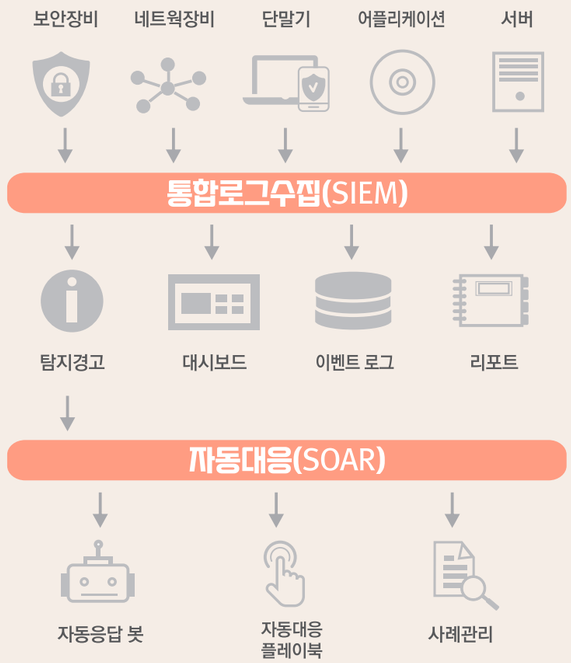
↓

신규 위협 정보 저장 및 공유

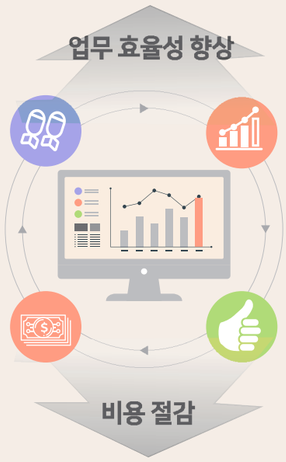
- KISA 보유 CTI를 활용하여 추가 분석
- 신규위협 정보 C-TAS 회원사 공유

사이버위협 공동대응 플랫폼 구축 사업

통합로그수집(SIEM) 및 자동대응(SOAR) 소개



통합로그수집(SIEM) 및 자동대응(SOAR) 도입효과



- **보안장비**에 대한 정책 연동 및 자동화 처리 가능
- 업무시간 절감 및 **반복적인 업무 리소스 낭비 최소화**

- 수많은 보안 장비의 **통합운영** 및 **이벤트 일원 관리** 가능
- **전체 위협 상황** 가시화

- **분석/대응 업무 프로세스 표준화** 및 자동화로 보다 중요한 업무에 집중 가능
- 위협발견 누락방지, 담당자 역량에 따른 **대응품질 편차 최소화**

민간 분야 실시간 사이버공격 탐지, 대응 및 공유 체계 구축을 위한 시스템 지원