신청방법

- **신청기간 :** 연중 수시
  ※ 보유한 프로그램 라이선스 수량 소진시까지
- **접수방법 :** 이메일 접수 ✉ monitor@kaits-info.or.kr
- **신청서류 :** 기술보호울타리 홈페이지에서 다운로드

접속경로: www.ultari.go.kr
▼
사전 예방
▼
기술지킴 서비스
▼
서비스 신청

- **제출 서류**

필수 신청서, 계약서 각 1부
필수 사업자등록증 1부
필수 정보 활용 동의서 1부
필수 중소기업확인서 또는 중견기업 확인서
선택 추가 지원 증빙자료(바우처, 방산기업 등)

문의처

가입문의

대·중소기업·농어업협력재단
02-368-8762
techkeeper@win-win.or.kr

한국산업기술보호협회
02-3489-7051~3
monitor@kaits-info.or.kr

기술지원

한국산업기술보호협회
02-3489-7060~4
security@kaits-info.or.kr

기술보호 통합상담·신고센터

02-368-8787
09:00~18:00
주말·공휴일 제외

중소기업 기술지킴서비스

대·중소기업·농어업협력재단 기술임치운영부
02-368-8762

한국산업기술보호협회 중소기업기술지킴센터
02-3489-7051~3

중소기업 기술보호울타리

국내 최초·최대 규모의 중소기업을 위한 보안 관제 센터

중소기업 기술지킴서비스



중소벤처기업부 | 대·중소기업 농어업협력재단 | 한국산업기술보호협회

중소기업
기술지킴서비스

사이버 해킹, 랜섬웨어 등을 통한 보안사고 예방
3년간 비용 부담 ZERO!

보안관제서비스를 제공하여 24시간 실시간 모니터링으로 해킹차단
내부유출방지(DLP)·악성코드·랜섬웨어 탐지 프로그램 3종 라이선스 제공

지원대상

- 「중소기업기본법」 제2조에 따른 중소기업 및 「중견기업법 시행령」 제9조의3에 따른 기술보호지원 특례 중견기업
  * 제외: 유흥·향락업, 숙박, 금융, 대부업 등 부적합 업종 및 휴·폐업 중인 기업



중소기업기술지킴서비스

24시간 × 365일 기술유출 방지 보안 서비스 **무상제공**
(중소기업기술보호법 제18조)

보안관제서비스

- 온라인 상 기술유출 시도 및 외부 공격에 대해 실시간 감시, 분석
- 신속·정확한 분석으로 정밀한 관제서비스 제공

기술지킴서비스 보안관제 프로세스

SCAM DDos XSS Zero-day
Scan SQL exploit Virus WebShell

1단계 위협발생
- 실시간 트래픽/이벤트 발생

2단계 자동화 분석 + 수동 정밀 분석
- 1차 AI 기술을 활용한 자동화 분석
- 2차 전문 인력의 정밀 검증

3단계 담당자 통보
- 위협 발생 후 평균 5분 이내 담당자 통보
- 분석 내용 및 대응 방안 제공

내부정보유출방지서비스

- 기업의 중요 문서가 내부 임직원에 의해 유출되는 것을 방지
- USB, E-mail, 출력물 등을 통한 내부 자료 유출 통제 및 이력 관리
- 기술유출 의심행위 발생 시 해당내역 담당자 통보
- 사용자가 사용하기 편리한 관리자 페이지 제공으로 IT비전문가라도 손쉽게 정책 설정 및 모니터링 가능
- 원격접속, 전화상담 등 기술 지원

출력물 이동식 매체 이메일 메신저

악성코드·랜섬웨어 탐지서비스

- 악성코드 랜섬웨어 탐지 및 복구 솔루션 무상제공
- 악성코드, 랜섬웨어 실시간 탐지 및 차단으로 정보자산 보호
- 지정 폴더에 주기적 자동 백업 및 폴더 보호
- 랜섬웨어 분석보고서 제공 및 조치방법 안내
- 메일을 통한 악성코드 수신 시 채증 및 분석지원

참여기업 혜택

- 기술지킴서비스 참여기업 대상으로 추가 서비스를 무상제공
  1. 방화벽, UTM 장비 교육 및 기술지원
  2. 악성메일 모의훈련
  3. 웹취약점 점검
  4. ASM(공격표면관리, Attack Surface Management)를 통한 인터넷에 노출된 자산, 취약점 등 식별 관리, 조치, 모니터링 제공

기술지킴서비스 사례

사례
대표이사 계정 탈취를 통한 내부 침투를 차단한 사례

01 문제 발생
- 고객사 메일 반송
- 불특정 다수 대량 메일 발송으로 계정 임시 차단
- 해킹이 의심되어 기술지킴센터에 분석요청

02 정밀 진단
- 새벽 시간대 불법 로그인 정황 확인
- 무단 생성된 계정 및 대표 계정 탈취 사실 확인

03 대응 및 성과
- 핵심기술 유출 사전 차단
- 취약 방화벽 재설정
- 맞춤형 재발방지책 제공