The latest Managed Security Services (MSS)
24/7 사이버 위협 대응을 위한
지능형 통합 보안관제 서비스

Integrated and Intelligent SOC

I² SOC as a Service

IGLOO

Background

급격한 IT 지형 변화에 발맞춰, 조직의 보안 관리 전략도 변화해야 한다.

디지털 전환과 함께 지금까지 경험하지 못했던 복합적인 사이버 공격이 증가하고 있습니다.
공격자들은 다변화된 IT 환경 속 곳곳에 분산된 IT 인프라의 보안 취약점을 악용해
주요 정보를 빼돌리거나 시스템을 마비시켜 서비스 중단을 야기하는 등
비즈니스 활동에 악영향을 미치는 사이버 공격을 지속적으로 감행하고 있습니다.

이에 조직의 IT 인프라가 보안 위협에 노출되지 않도록 지켜보고, 위험 요소 발견 시 즉각 대처할 수 있도록
보안 환경에 대한 전문화된 운영·관리를 대행하는 서비스의 수요가 점점 높아지고 있습니다.

다만 보안 위협이 날로 고도화되는 만큼, 조직의 공격 방어 체계도 변화해야 합니다.
인공지능(AI), 보안 운영·위협 대응 자동화(SOAR) 등의 신기술을 적용한 한층 지능화된 보안 서비스가 필요한 시점입니다.

Overview

이글루코퍼레이션 I² SOCaaS는 전문화된 통합보안관리를 제공하는 서비스형 SOC(SOC as a Service)입니다.

고도화된 사이버 공격과 위협 요소에 대한 실시간 분석 및 대응을 통해, 고객의 정보 자산을 안전하게 보호하고 폭넓은 보안 요구 사항을 해결합니다.
고객은 정보 보안에 대한 확신을 토대로 핵심 비즈니스에 집중할 수 있습니다.

24x7x365 사이버 위협 대응

- 실시간 보안 이벤트 분석 및 보고
- 사이버 침해 대응/분석
- 홈페이지 위·변조 탐지
- 서비스 장애 관제
- 보안장비 운영/관리
- 보안정책 적용/관리
- 시스템 가용성 확인/관리

사전 침해 예방

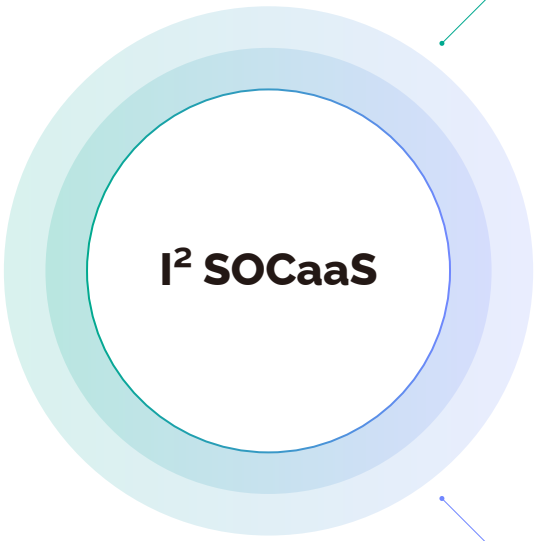
- 인프라 취약점 진단
- 모의 해킹
- 최신 보안 동향 제공
- 소스코드 진단
- 보안 실태 점검
- 보안 수준 진단
- 임직원 보안 인식 향상을 위한 모의 훈련 (악성메일 모의 훈련)

기타 정보 보안 업무 지원

- 각종 인증 준비 지원
- 지침/매뉴얼 개정 지원
- 정보 보안 법적 대응 지원
- 보안 교육 수행

Why
I² SOC as a Service

이글루코퍼레이션 I² SOCaaS는 급변하는 사이버 공격에 최적화된 현대적인 보안 운영 서비스입니다.
고객의 정보 자산에 대한 지능적인 보호를 통해 높은 효율성을 구현합니다.



Technology

보안업계를 선도하는 AI 기반 솔루션·서비스 개발 역량 확보

· 국내 최초로 보안 정보 및 이벤트 탐지 분석(SIEM) 솔루션과 인공지능(AI) 보안관제를 선보인 업계 리딩 기업
· 보안 운영·위협 대응 자동화(SOAR), 위협 인텔리전스(CTI), 생성형 AI 등 최신 기술의 지속적인 개발 및 적용을 통해 위협 탐지·대응 기법 고도화

People

핵심 전문가 집단 보유

· 공공·금융·서비스 등 다양한 환경의 수백 개 고객들의 보안을 운영한 경험과 노하우 보유
· 다년간의 보안 운영 경험과 축적된 위협 정보를 녹여내어 독자적인 '보안관제방법론'을 정립하고, 이를 토대로 한 검증된 서비스 제공

Process

높은 수준의 보안 운영 편의성 구현

· 업무 포털 'ISOC Insight'를 통해 사이버 공격 대응을 위한 핵심 정보 및 각종 보고서 등을 손쉽게 조회
· 공격 대응 현황, 공격 분석에 대한 자세한 내용을 실시간으로 제공하면서 직관적인 현황 파악 지원

Environment

통합된 보안 가시성 확보

· 고객의 요구 및 환경에 따라 파견 관제, 원격 관제, 하이브리드 관제, 클라우드 관제 등 다양한 레벨의 서비스 지원
· 온프레미스 환경과 클라우드 환경을 아우르는 통합된 보안 가시성 확보

Types of
I² SOC as a Service

다양한 레벨의 I² SOCaaS를 제공합니다.
조직 별 각기 다른 환경 및 보안 요구 사항에 유연하게 대응할 수 있습니다.

파견 관제 서비스
고객사 상주 인력에 의한 보안 운영 서비스

- 고객사에 특화된 프로세스 수립 및 서비스 제공
- 침해·장애 발생 시 즉각적인 조치 가능
- 보안 운영 연속성 및 효율성 증대

원격 관제 서비스
인터넷 망(VPN)을 통한 원격 보안 운영 서비스

- 보안 사고에 대한 인지 및 대응 강화
- 기존 보안 운영 프로세스 개선
- 파견 관제 대비 저렴한 단가 및 인력 관리 부담 해소

하이브리드 관제 서비스
파견 관제와 원격 관제의 장점을 융합한 보안 운영 서비스

- 상주 인력을 통한 원활한 의사소통 가능
- 침해·장애 발생 시 상주 인력의 신속한 선 조치 후,
  이글루코퍼레이션 I² SOC와의 공조를 통한 정확도 높은 대응 가능

Types of
I² SOC as a Service

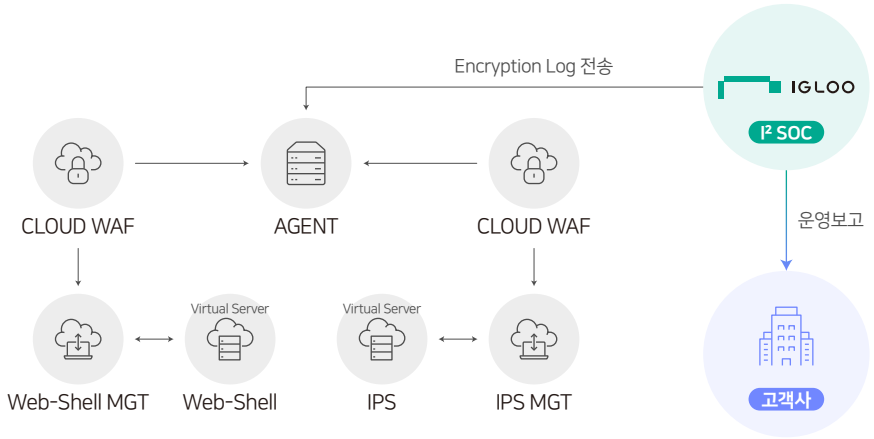
클라우드 환경에서도 온프레미스와 동일한 수준의 I² SOCaaS를 지원합니다.

클라우드 관제 서비스

다양한 클라우드 환경에 대한 보안 운영 서비스

- 클라우드 보안 관리에 최적화된 서비스
- 고객사 클라우드 환경에 특화된 보안 정책 수립 후, 모니터링-분석-대응-보고 등 온프레미스 환경과 동일한 수준의 서비스 제공
- 서드파티(3rd Party), AWS 네이티브(AWS WAF, AWS 가드듀티) 시스템을 활용한 이벤트 분석 및 보고

서비스 구성도



서비스 범위

- 고객사 보안 솔루션 데이터
- 이상 트래픽 감지
- 보안 솔루션 운영

서비스 제공 내역

- 24/7 실시간 보안관제
- 침해사고 분석
- 리포팅

Features

A. ISOC Insight

업무 포털 서비스 ISOC Insight 를 통한 신속하고 투명한 정보 공유 체계 운영

- 실시간 고객사 보안 이슈 및 업무 보고 공유 지원
- 보안 운영 효율성을 높이는 직관적인 공격 현황·분석 시각화 대시보드 제공
- 즉각적인 공격 이력·히스토리 확인이 가능한 일원화된 커뮤니케이션 채널 지원

ISOC Insight 메인 페이지

ISOC Insight

Ticket
공격 이벤트에 대한
분석 결과 제공

Ticket Search
특정 조건에 따른 티켓 조회 및
파일 추출 서비스 제공

Trends & I-CERT
일일정보보호동향 및
상황전파문 제공

Report
정기/비정기 보고서 및
고객사 요청 자료 제공

발생한 공격 이벤트에 대한
정보를 즉각적으로 확인

I² SOCaaS를 통해 생성되는
각종 보고서 및 자료를 간편하게 조회

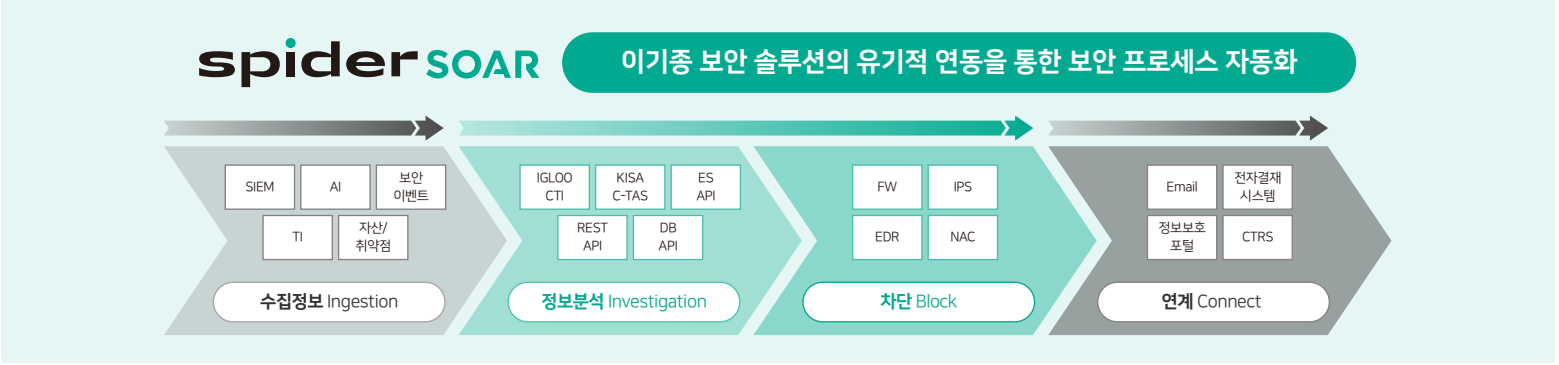
I-CERT가 제공하는 주요 보안
이슈에 대한 정보를 신속하게 공유

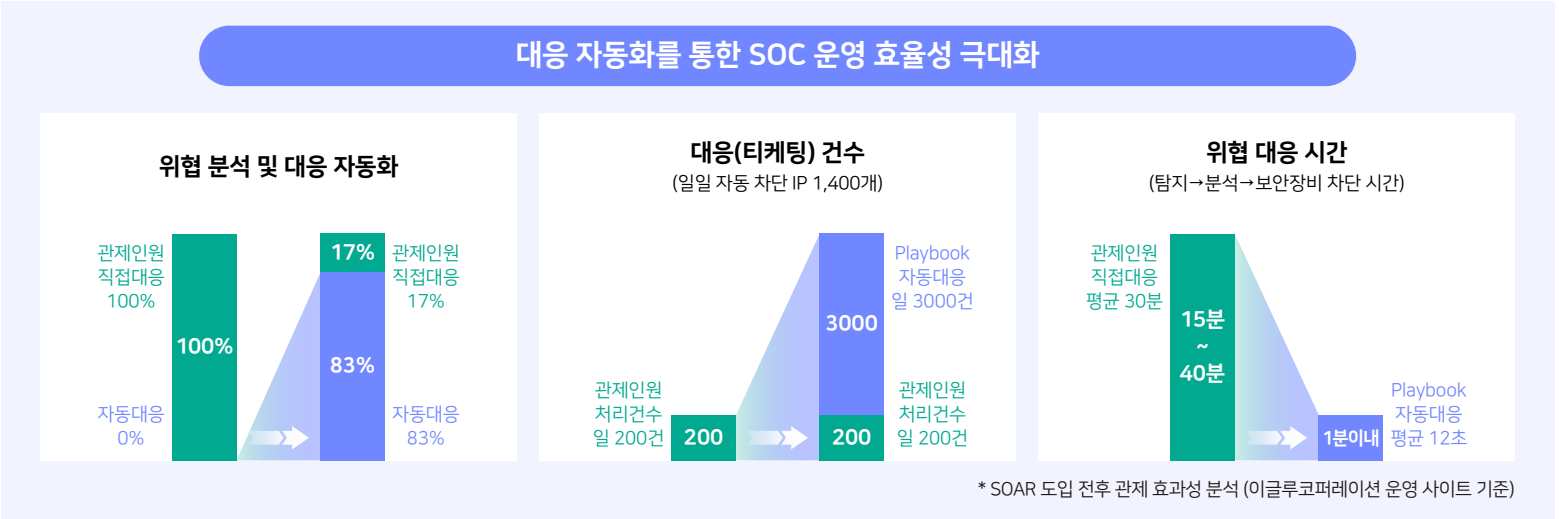
Features

B. SOAR

보안 운영·위협 대응 자동화(SOAR) 솔루션 SPiDER SOAR 를 통한 SOC 운영 자동화

· 플레이북(Playbook)을 바탕으로 탐지된 공격에 대한 자동 분석·대응을 지원하는 당사 SOAR 솔루션 SPiDER SOAR를 활용해 위협 대응 소요 시간 최소화
· 보안 전문가들은 단순 반복적인 업무 처리에서 벗어나 중요도 높은 분석 업무에 집중하게 되면서 보안 체질 개선 및 보안 운영 성숙도 제고





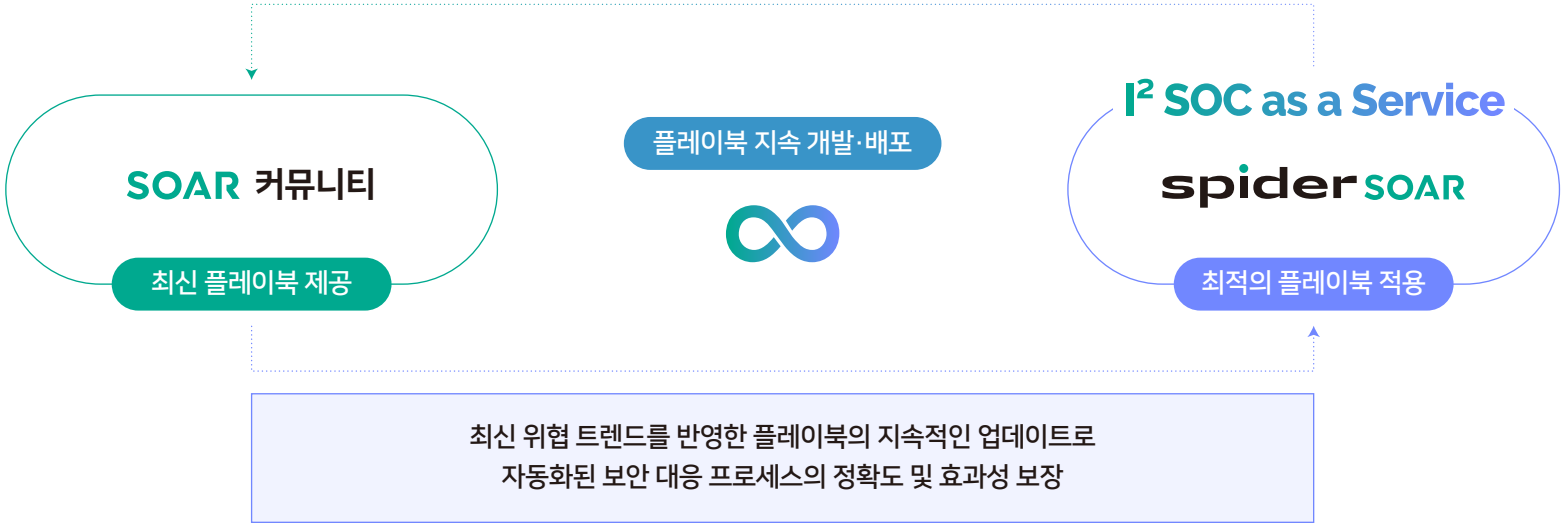
* SOAR 도입 전후 관제 효과성 분석 (이글루코퍼레이션 운영 사이트 기준)

Features

C. SOAR Community

위협 분석·대응 자동화의 기반이 되는 플레이북의 지속적인 개발 및 공유를 지원하는 SOAR Community 를 통한 보안 운영 효율성 극대화

· 이글루코퍼레이션 보안 전문가들이 검증한 플레이북 제공으로 높은 안정성과 활용성 보장
· 각 조직 상황에 부합하는 플레이북의 손쉬운 적용·활용을 통해 보안 운영에 실질적으로 도움이 되는 업무 자동화 구현



SOAR 커뮤니티 메인 페이지

SOAR 커뮤니티 Playbook Matrix 페이지

SOAR 커뮤니티 Playbook 상세 화면 페이지

Features

D. AI

분류형 AI, 설명 가능한 AI(eXplainable AI), 생성형 AI 등 인공지능(AI) 기술을 활용한 고도화된 위협 탐지 및 분석 지원

- 머신러닝 기반 지도/비지도 분석 기술의 적용을 통해, 보안 업무의 효율성을 높이고 위협에 대한 예측률 향상
- 하이브리드 AI 탐지 모델 서비스 'AiR' 연동을 통해, 데이터 분석의 정확도와 신뢰도를 높여 언제나 최상의 조치가 신속하게 실행될 수 있도록 지원

머신러닝 기반

지도/비지도 분석

위협 탐지 및 분석 정확도 향상

- 지도 학습 기반 스코어링 분석을 통해 우선 처리해야 할 고위험 이벤트 선별
- 비지도 학습을 통해 심각한 위협으로 발전할 수 있는 이상 행위를 판별하고 미탐 최소화

분류형 AI, 설명 가능한 AI, 생성형 AI 기반

AI 탐지 모델 서비스 AiR

위협 분석 역량 및 대응 속도 향상

① 분류형 모델 결과: 특정 보안 데이터에 대한 자동 분석

② 설명형 모델 결과: 분석 결과에 영향을 미친 근거 제시

③ 생성형 모델 결과: 분석 결과에 대한 자연어 형태의 해석

Features

E. 이글루코퍼레이션 보안관제방법론

수많은 고객들의 보안을 책임지고 운영한 경험과 노하우가 담긴 이글루코퍼레이션 보안관제방법론을 토대로 체계적이고 전문적인 서비스 제공

- 미 국립표준기술연구소(NIST)의 Cyber Security Framework를 비롯한 주요 정보보호 프레임워크를 기반으로 고유의 보안관제방법론 개발
- '식별(Identify)-예방(Protect)-탐지(Detect)-대응(Respond)-복구(Recover)-관리(Manage)'의 6단계로 구성된 프레임워크 적용
- SOC 운영에 대한 체계화된 프로세스를 제공함으로써 SOC 운영 전문성 및 효율성 제고
- 실제 SOC 현장 적용 및 피드백을 통한 지속적인 검증, 개선 과정을 거치면서 최신화 진행

식별 Identify	예방 Protect	탐지 Detect	대응 Respond	복구 Recover	관리 Manage
ID.AM 자산 관리	PR.VA 취약점 진단	DE.EC 보안 이벤트 수집	RS.IA 침해사고 분석	RC.RP 복구 계획	MG.SL 서비스 수준 관리
ID.BE 비즈니스 환경 분석	PR.DT 모의 침투/인식 훈련	DE.DA 탐지 및 분석	RS.IP 침해사고 대응	RC.IM 개선	MG.MP 지침/절차 개정
ID.GV 법적 요건	PR.SH 보안 시스템 최적화	DE.RA 대응 및 조치	RS.CO 상황 전파	RC.CO 커뮤니케이션	MG.WS 근무 체계 관리
ID.RA 위험 식별 및 관리	PR.PP 대응 체계 수립	DE.PH 탐지 프로세스 관리 및 정책 최적화	RS.MI 확대 방지		MG.SE 평가
ID.SO 운영 관리	PR.IS 정보 공유		RS.IM 개선		MG.CE 인증
					MG.SP SOC 보호 및 시스템 운영

Benefits

다년간 축적된 경험과 전문 지식, 그리고 차별화된 기술력에 기반해
고객은 보안 관리의 복잡성을 해소하고, 흔들림 없는 비즈니스 연속성을 유지할 수 있게 됩니다.

이글루코퍼레이션은 1999년 창립 이래, 조직의 업무 환경 및 업무 수행 방식의 혁신을 앞당길 수 있는 핵심 기술 구현에 집중하여 왔습니다. 국내 최초의 보안 정보 및 이벤트 탐지 분석(SIEM) 솔루션 출시를 시작으로, 인공지능(AI), 보안 운영·위협 대응 자동화(SOAR), 위협 인텔리전스(CTI), 운영 기술 보안(OT), 전문 보안 서비스를 아우르는 다각화된 사업을 전개하며, 보안·인공지능·클라우드·빅데이터 분야를 아우르는 종합 IT 기업으로 성장했습니다. 이글루코퍼레이션은 고유의 AI 기반 보안 운영·분석 플랫폼을 바탕으로, 급변하는 비즈니스 환경에 최적화된 해결책을 제시하는 핵심 조력자 역할을 지속 수행하고자 합니다.

서울특별시 송파구 정의로8길 7 한스빌딩 6층 | TEL 02-3452-8814 | FAX 02-3452-8815 | www.igloo.co.kr

IGLOO