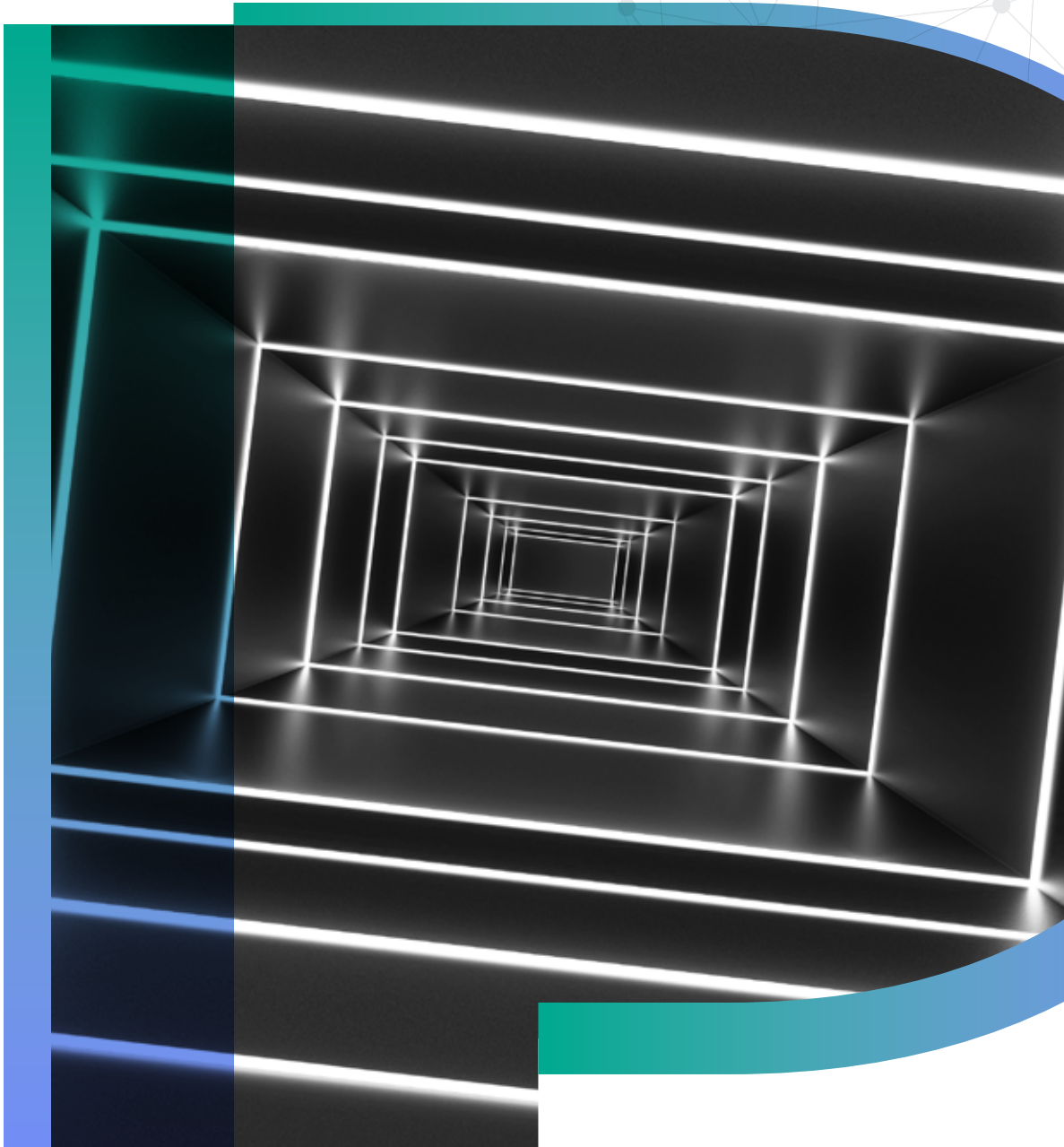
방어의 정석을 배우고 승리의 전략을 완성하다

AI 기반 오펜시브 시큐리티 플랫폼

PLOT



IGLOO

Background

공격자의 전술·기법·절차를 훈련해야 방어의 승률이 바뀝니다.

AI 기술의 확산과 함께 사이버 공격은 더욱 정교해지고 있습니다.
공격은 더 이상 단일 기법이 아닌 전술과 흐름 단위로 설계·실행되는 복합적인 형태로 진화하고 있습니다.
그 결과 기존의 방어 체계만으로는 예측하기 어려운 공격이 빠르게 증가하고 있습니다.

그럼에도 많은 조직은 여전히 과거의 알려진 패턴과 사후 대응 중심의 보안에 머물러 있습니다.
실제 공격 상황을 전제로 한 대응 경험은 부족한 채, 수동적인 방어 체계에 의존하고 있는 것이 현실입니다.

공격자의 관점에서 보안을 바라보는 '**오펜시브 시큐리티(Offensive Security)**' 전략은,
이러한 한계를 극복하고 선제적 대응 체계를 구축하기 위한 필수 역량으로 부상하고 있습니다.

어제의 교육만으로는 내일의 공격을 막을 수 없습니다.
이것이 바로 공격자의 전술·기법·절차를 그대로 반영한『실전 훈련』이 필요한 이유입니다.

PLOT

공격자 관점의 플롯(TTPs)을 파고들다

Overview

플롯(PLOT)은 공격자 관점의 전술·기술·절차(TTPs)를 반영한 실전형 사이버 훈련을 제공하는 AI 기반 오펜시브 시큐리티 플랫폼입니다.

사이버 공격은 언제나 예측하기 어려운 순간에 발생하며, 시시각각 변화하고 진화합니다.
이에 대응하기 위해서는 지능화된 공격을 사전에 인지하고, 신속하게 대응하며, 피해를 최소화할 수 있는 역량이 필수적입니다.

PLOT은 실제 침해사고 시나리오 기반 방어 훈련 솔루션 '플롯 시디엑스(PLOT CDX)'와
팀 단위 공방 훈련 솔루션 '플롯 아레나(PLOT ARENA)'를 통해 개인과 조직이 고도화된 대응 역량을 내재화할 수 있도록 지원합니다.

시나리오 기반 실전형 사이버 훈련 솔루션

PLOT CDX

실제 침해사고 시나리오 기반 방어 훈련

(Live-Fire)

실전형 사이버 공방 훈련 솔루션

PLOT ARENA

공격팀-방어팀 대항 훈련

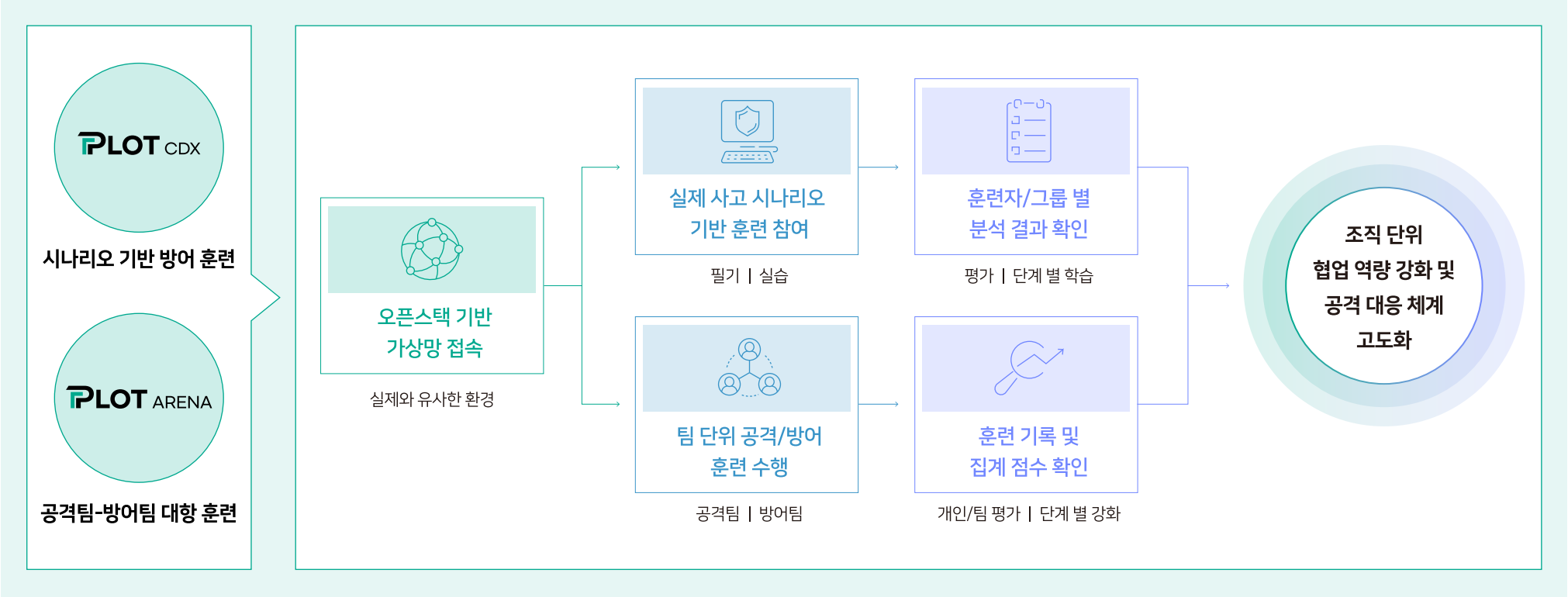
(Attack & Defense)

01	**실제 침해사고 시나리오 기반 훈련**	실제 보안 현장에서 수집된 최신 공격 패턴이 반영된 공격·방어 훈련으로 실전 대응력 강화
02	**가상화/클라우드 환경의 유연한 훈련장**	별도의 장비 도입이나 물리적 제약 없이 손쉽게 구축·운영 가능한 훈련 환경 제공
03	**AI 기반 공격 시뮬레이션 자동화**	가상의 AI 해커가 지능형 공격을 재현하여 실제와 같은 방어 훈련 환경 구현
04	**국가정보원 사이버 보안 실태 평가지표 대응**	실전 역량 강화와 함께 국가정보원 사이버 보안 실태 평가지표 대응까지 해결 가능 [배점 상향 1→1.5점] 사이버 공격·재난 대응 훈련 [가산점 반영 1점] AI 기반 보안업무 도입 [가산점 반영 1점] 사이버공격방어대회 등 교육·훈련 참여

Why PLOT

PLOT을 통해 실전 경험을 쌓고, 공격자보다 한 수 앞선 대응 역량을 확보하세요.

사이버 공격을 미리 경험하고 대응해 보는 것은 조직이 급변하는 보안 위협에 신속하게 대응하고 피해를 최소화하는 데 중요한 역할을 합니다.
PLOT은 실제와 유사한 가상 환경에서 공격·방어 훈련을 수행하며, 개인과 조직의 실전 대응 경험을 체계적으로 축적할 수 있도록 지원합니다.
훈련 데이터 기반 분석과 피드백을 통해 대응 수준을 객관적으로 진단하고, 반복 학습을 통해 지속적인 역량 향상을 이끌어냅니다.
이를 통해 조직은 위기 대응 전략을 고도화하고, 변화하는 위협에도 흔들림 없는 보안 체계를 구축할 수 있습니다.



PLOT CDX

PLOT CDX를 통해 '방어의 정석'을 배우세요.

PLOT CDX는 실제 침해사고 시나리오를 기반으로 방어 훈련을 지원하는 실전형 사이버 훈련 솔루션입니다.
실제와 유사한 가상 환경에서 탐지부터 대응, 복구까지 사고 대응 전 주기를 단계적으로 학습할 수 있습니다.

훈련자들은 다양한 공격 시나리오를 기반으로 반복적인 대응 훈련을 수행하며,
실전과 같은 환경 속에서 대응 절차와 판단 기준을 자연스럽게 체득하게 됩니다.
이를 통해 개인의 실전 대응 역량을 강화하고, 조직의 보안 대응 수준을 체계적으로 향상시킬 수 있습니다.

Why PLOT CDX

PLOT CDX는 실제 운영 환경을 반영한 시나리오 기반 훈련을 통해 실무 중심의 대응 역량을 내재화할 수 있도록 설계되었습니다.

보안 담당자는 예방부터 탐지·대응, 사후 분석에 이르는 전 과정을 따라가며
실무에서 요구되는 대응 흐름과 판단 기준을 체계적으로 익힐 수 있습니다.
특히 취약점 진단, 엔드포인트 방어, 웹 서비스 보호 등 실제 업무를 반영한 다양한 실습 과제를 통해
현업에 즉시 적용 가능한 실전 대응 역량을 강화합니다.

1. 예방

취약점 진단 | 설정 오류 점검

계정 및 접근 통제 점검

네트워크 분리 방어선 점검

2. 탐지·대응

엔드포인트 방어
- 사용자 PC 내 악성코드 유입 대응
- 계정 탈취, 중요 데이터 유출 대응

웹 서비스 보호
- 취약점 공격, 침해 시도 식별
- 실시간 차단 → 서비스 가용성 확보

통합 대응 실무
- 보안 설정 점검/심층 로그 분석/조치 전 과정 수행
- 실제 사고 발생 시 대응 완결성 확보

3. 복구·사후분석

서비스 및 시스템 정상화를 위한 복구 절차 훈련

사고 긴급 대응부터 보고까지의 전 과정 훈련

현업에서 즉시 사용 가능한 포렌식 기법 훈련

재발 가능성을 원천 차단하는 대책 수립 훈련

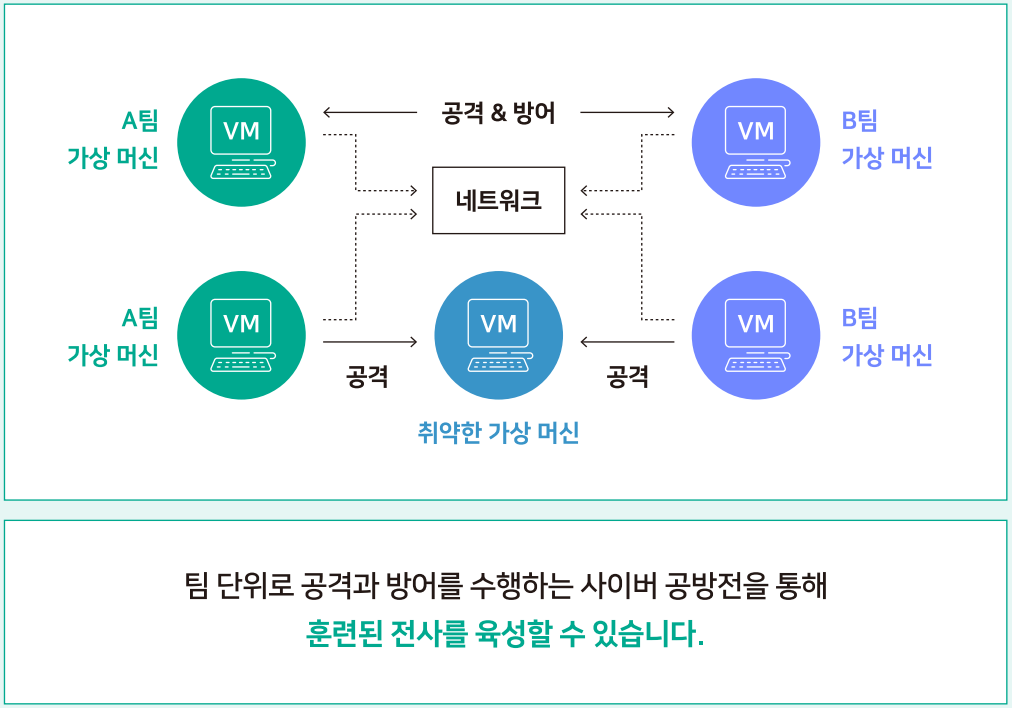
**실제 운영 환경을 이해할 수 있는 시나리오 기반 콘텐츠와 에이전트를 활용한 채점 스크립트를 통해
실습 콘텐츠의 수행 결과를 확인할 수 있는 기능을 제공합니다.**

PLOT ARENA

PLOT ARENA를 통해 '승리의 전략'을 완성하세요.

PLOT ARENA는 조직의 보안 성숙도와 목표에 맞춰 팀 단위 공방 훈련을 지원하는 지능형 사이버 훈련 솔루션입니다.
팀 단위 공격·방어 훈련을 통해 실전과 같은 협업 중심의 대응 환경을 구현합니다.

훈련자들은 다양한 전투 시나리오 속에서 공격자와 방어자의 역할을 수행하며, 상황 판단과 전략 수립, 팀 간 협업을 반복적으로 경험하게 됩니다.
이를 통해 개인의 기술 역량을 넘어, 조직 차원의 대응 전략을 수립하고 고도화하는 역량을 지속 강화할 수 있습니다.



팀 단위로 공격과 방어를 수행하는 사이버 공방전을 통해
훈련된 전사를 육성할 수 있습니다.

Why PLOT ARENA

PLOT ARENA는 팀 단위로 공격과 방어를 수행하는 실전형 사이버 공방 훈련 환경을 제공합니다.

여러 팀이 동일한 환경에서 동시에 공격과 방어를 수행하며, 실전과 같은 협업 상황에서 전략을 직접 실행하고 검증합니다.
경쟁, 대립, 점령, 미션 등 다양한 공방전 유형을 통해 상황에 따라 변화하는 전략을 반복적으로 경험하며,
팀 단위 협업과 전략 실행 역량을 실전 수준으로 끌어올립니다.

배틀 설정

- 네트워크 구성/타겟 미션 Flag
- 공통 미션 Flag
- 배틀 BOX/개인 미션 Flag
- 팀 정보/팀 미션 Flag
- 진행 시간/FAQ/규칙/보상

배틀 참여

- 공통 미션
- 팀 미션
- 개인 미션
- 타겟 미션

공방전 콘텐츠

경쟁 (Competition)

방식
Time Attack
(타임 어택)

목표
Flag First Capture
(선취)

대립 (Head-to-Head)

진행
무제한 자율 공방
(공격·방어 병행)

승리
타겟 시스템 플래그(Flag)
최종 획득

점령 (King of the Hill)

미션
자원(서버/서비스) 쟁탈 및
점수 확보

승리
지정 위치에 팀 코드 삽입
후 최장 시간 점유

미션 (Mission)

미션
주어진 시나리오 목표 달성
(팀 별 조건 상이)

승리조건
시나리오 별 미션 완수
(비대칭 대결 가능)

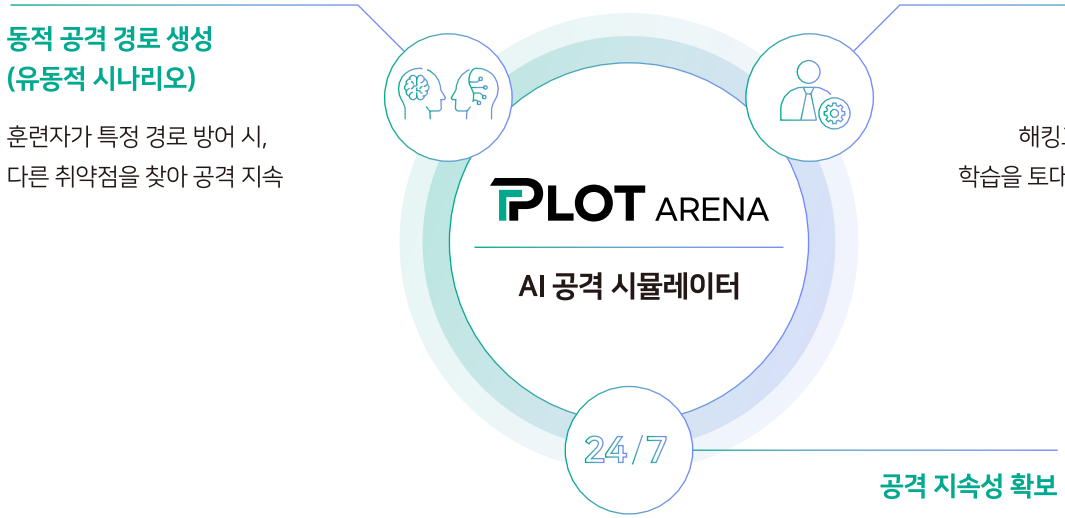
실제 인프라와 실시간 공격/방어 상황을 반영한 몰입형 훈련 환경 및 콘텐츠를 제공합니다.

Why PLOT ARENA

PLOT ARENA는 AI 기반 공격 시뮬레이션을 통해 고정된 시나리오를 넘어서는 지능형 사이버 공방 훈련 환경을 제공합니다.

AI 공격 시뮬레이터는 다양한 공격 시나리오를 현실감 있게 재현하는 데 그치지 않고,
훈련자의 대응에 따라 공격 경로와 전술을 실시간으로 변화시키며 예측을 뛰어넘는 공격 상황을 지속적으로 생성합니다.

이 과정에서 AI는 정해진 공격을 수행하는 도구를 넘어, 공격 전술을 스스로 생성하고 보완하며 새로운 경로를 탐색하는 '전략 참모'로 작동합니다.
이를 통해 조직은 예측이 어려운 위협 환경에서도 공격자보다 한 수 앞선 대응 우위를 확보할 수 있습니다.



스스로 판단하고 움직이는 가상의 AI 해커가 지능형 공격 시뮬레이션을 구현합니다.

Features

PLOT은 실전형 사이버 훈련을 위한 핵심 기능을 제공하며, 사용자 친화적인 메뉴 구성·구현으로 직관적인 사용이 가능합니다.

PLOT CDX | 시나리오 기반 방어 훈련

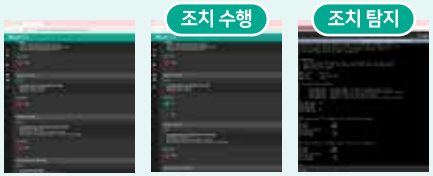
01 훈련 현황 대시보드

진행 중인 훈련의 위기 수준과 시나리오 상황을 실시간으로 확인하고, 발령된 위기 경보 단계와 공지에 따라 적절한 대응을 수행할 수 있습니다.

02 훈련 진행

필기형·실습형 문제 수행 현황과 점수 획득 상황을 실시간으로 확인하며, 다양한 유형의 문제를 통해 단계별 훈련을 진행할 수 있습니다.

03 에이전트 기반 자동 채점



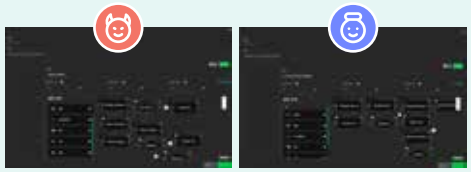
VM 내에서 패치나 보안 설정 변경 등 조치를 수행하면, 에이전트가 이를 실시간으로 감지해 성공 여부를 판정하고 그 결과를 점수로 자동 반영합니다.

PLOT ARENA | 공격팀-방어팀 대항 훈련

01 공방전 환경 생성

훈련 팀, 라우터, 네트워크 등 다양한 노드를 기반으로 공방전 환경을 설계하고, 클라우드에서 간편하게 구축해 훈련을 수행합니다.

02 AI 기반 VM 에이전트 설정



AI 기반 VM 에이전트를 통해 공격자 또는 보안 조력자 역할을 구성하고, 동적으로 변화하는 공격·대응 환경을 구현합니다.

03 훈련 진행

VM과 상호작용하며 공격·방어를 수행하고, 팀별·개인별 스코어 현황 및 훈련 정보를 실시간으로 확인할 수 있습니다.

Why IGLOO

PLOT을 통해 사이버 복원력을 강화하고, 비즈니스 연속성을 확보하세요.

이글루코퍼레이션은 20년 이상 공격자와 맞서 싸워 온 실전 대응 경험과 고유의 AI 원천기술을 바탕으로,
조직의 사이버 방어 역량을 지속해서 향상시킵니다.

어제 발생한 실제 공격이 오늘의 훈련 시나리오가 됩니다

01 실시간 위협 정보를 반영한 콘텐츠 적용

이글루코퍼레이션은 실제 보안 현장에서 수집된 공격 패턴과 대응 경험을 기반으로, 이론이 아닌 '현장에서 통하는 훈련'을 제공합니다. 공격 기법, 도구, 과정을 분석하고 유형별 최적의 대응 방안을 지속 개발할 수 있는 전문가 풀을 통해, 최신 위협 정보를 반영한 실시간 콘텐츠를 적용할 수 있습니다.

공격은 계속 진화합니다. 훈련은 그보다 더 빠르게 진화합니다

02 AI 기반 오펜시브 시큐리티 경쟁력 강화

이글루코퍼레이션은 고유의 AI 원천 기술을 기반으로 시나리오, 난이도, 훈련 방식까지 지속적으로 고도화하며 도입 이후에도 훈련의 효과와 가치를 끊임없이 높입니다. 이글루코퍼레이션의 선도적인 AI 기술이 플랫폼의 완성도를 더하며, 훈련 콘텐츠의 신선도와 실전성을 극대화합니다.

국내 최대의 보안 노하우가 곧 최강의 시나리오가 됩니다

03 활용도 높은 훈련 콘텐츠·환경 구현

수많은 공격과 대응을 통해 축적된 노하우는 그 자체로 가장 현실적인 훈련 자산이 됩니다. 이글루코퍼레이션은 국내 보안 환경과 SOC에 대한 깊은 이해를 바탕으로, 조직에 최적화된 훈련 콘텐츠와 시뮬레이션 환경을 제공합니다. PLOT의 모든 시나리오는 실제 보안 현장에서 검증된 공격 패턴을 기반으로 구성됩니다.

훈련은 결과로 끝나지 않고, 개선으로 이어집니다

04 평가·개선 리포트 및 상세 가이드 제공

보안 담당자, 인사 담당자, CISO를 아우르는 다양한 사용자가 훈련 결과를 손쉽게 이해하고 목적에 따라 활용할 수 있도록, 평가 결과 및 개선 방안 등을 담은 리포트와 테스트 내용 및 결과에 대한 상세 답변을 알려주는 전문가 서비스를 지원합니다.

Benefits

조직의 사이버 위기 대응 프로세스를 최적화하고, 실제 위기 상황 발생 시 대응력을 극대화할 수 있습니다.

보안 담당자는 실전 대응 역량을 강화하고, 조직은 상황에 부합하는 위기 대응 전략을 개발·점검·평가함으로써
미래 공격에도 흔들림 없는 보안 태세를 구축할 수 있습니다.

신변종 위협에 대한 대응 역량 극대화

AI 공격을 비롯한 다양한 공격 시나리오를 경험함으로써 진화하는 보안 위협에 대한 실전 대응력 강화

지속적 관리를 통한 보안 성숙도 개선

평가와 피드백을 통해 훈련 성과를 효율적으로 분석 및 관리하고, 조직의 보안성에 대한 지속적인 개선

보안 조직 내 유기적 협업 체계 구현

팀 기반 훈련을 통해 조직 내 문제 해결 능력 향상 및 대응 역량 상향 평준화

전문 인재 선별의 효율성 극대화

객관적인 훈련 결과를 역량 평가와 인력 채용 도구로 활용하여 효율적인 보안 인재 유치 및 유지에 기여

Roadmap

더 많은 조직이 상향평준화된 사이버 방어 체계를 구축하고 성숙한 실전 대응력을 확보할 수 있도록 지원할 예정입니다.

AI 기반 오펜시브 시큐리티 플랫폼을 통해 조직의 보안 태세를 점검하고,
비즈니스 운영에 영향을 미칠 수 있는 잠재적 취약성을 파악하면서 진화하는 위협에 앞서가세요.

콘텐츠 자동 생성

훈련 목적과 환경에 맞는 시나리오를 자동으로 구성하여, 훈련 설계의 속도와 유연성을 동시에 확보합니다.

공격 패턴 학습

훈련 데이터를 기반으로 AI가 공격 패턴을 학습하고, 지속적으로 진화하는 시나리오를 생성합니다.

디지털 트윈 기반 훈련 환경

실제 조직 환경을 반영한 디지털 트윈 기반으로, 현실과 동일한 수준의 대응 시뮬레이션을 구현합니다.

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
COPYRIGHT 2026. IGLOO Corp. ALL RIGHTS RESERVED.

IGLOO