

실전에 강한 보안 팀, 위기에 강한 조직을 위한  
사이버 훈련 솔루션(Cyber Defense eExercise)

# PLOT CDX

## Background

### 공격의 발생 시점을 예측할 수는 없지만, 사이버 복원력 강화는 가능합니다.

기존의 방어 체계로는 예측하기 어려운 복합적인 사이버 공격이 증가하고 있습니다. 빠른 기술 발전과 함께 공격 표면이 확장되며 다양한 IT 자산과 인프라가 잠재적인 표적으로 떠올랐고, 공격 도구와 기법이 한층 지능화 되면서 공격의 빈도와 강도 역시 크게 높아졌습니다. 그에 비해 전문 인력의 수는 한정되어 있어 보안 조직의 업무 부담은 날로 커져만 가고 있습니다.

현대의 사이버 보안은 단순히 방어적 태세를 갖추는 것만으로 충분하지 않습니다. 공격자들이 끊임없이 진화하는 상황 속에서, 이에 한 수 앞선 '오펜시브 시큐리티(Offensive Security)' 전략 마련이 필요한 시점입니다.

사이버 공격은 항상 예상치 못한 순간에 발생합니다. 또한 시시각각 변화하고 진화합니다. 그렇기 때문에 지능화된 공격을 예방하고 적시 대응하며 피해를 최소화할 수 있는 역량이 필요합니다.

**이것이 바로 실제와 유사한 환경에서 다양한 침해 사고 시나리오를 수행하며, 실전 경험을 쌓을 수 있는 「사이버 훈련 솔루션」이 필요한 이유입니다.**



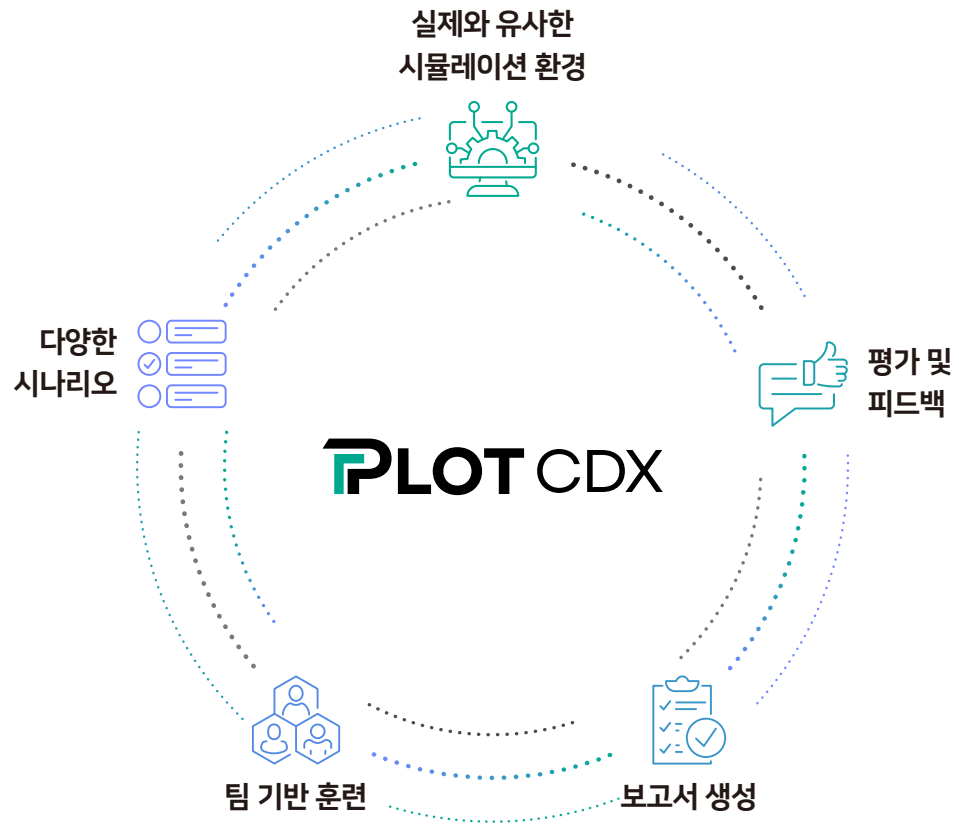
#### 오펜시브 시큐리티(Offensive Security)

해커 입장에서 시스템/서비스/인적 자원의 약점, 공격 경로를 찾고, 이에 대한 해결책을 모색하는 보안 분야

## Overview

플롯 시디엑스(PLOT CDX)는 실제 공격 시나리오에 기반한 대응 훈련을 지원하는 실전형 사이버 훈련 솔루션입니다.

훈련 참가자는 개인 및 팀 단위로 침해 사고 시나리오 기반 시뮬레이션을 수행하며, 사이버 공격에 대한 실전 대응 역량을 강화할 수 있습니다. 보안 조직은 훈련 결과에 대한 상세 피드백/보고서를 토대로 개인과 조직의 약점을 개선하고, 조직의 보안 수준을 분석·관리할 수 있습니다.



## Why PLOT CDX

PLOT CDX로 사이버 복원력을 강화하고, 비즈니스 연속성을 확보하세요.

20년 이상 공격자와 맞서 싸워 온 실전 대응 경험과 방법론을 바탕으로, 조직이 상향된 수준의 대응 역량을 내재화할 수 있도록 지원합니다.

### 01 활용도 높은 훈련 콘텐츠·환경 구현

이글루코퍼레이션은 국내 보안 환경, SOC에 도입된 보안 장비 및 솔루션, 보안 조직을 노리는 공격 유형을 누구보다 가장 잘 아는 기업입니다. 국내 조직에 최적화된 활용도 높은 훈련 콘텐츠 및 시뮬레이션 환경 구현을 보장합니다.

### 02 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.

**PLOT CDX**

### 03 실시간 위협 정보를 반영한 콘텐츠 적용

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.

### 04 보안 장비 도입 및 설치 부담 해소

가상화된 서버와 네트워크 인프라를 통해 다양한 시나리오의 시뮬레이션 환경을 구현합니다. 보안 조직은 물리적 보안 장비 도입 및 설치의 부담 없이 실제와 같은 보안 훈련 환경을 체험할 수 있습니다.

## Features

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

### 01 대시보드 (일정/진행 상황 시각화)



- 실시간 훈련 일정 및 진행 상태 (예정, 진행, 완료) 확인 기능 제공

### 02 필기형/실습형 문제 생성 및 채점



- **필기형 문제** 객관식, 주관식, 스크립트 등 유형별 문제 생성과 배점, 풀이 제한, 오답 감점, 힌트, 해설 등 기능 제공
- **실습형 문제** 훈련 구성에 따라 사이버위경보, 보안 권고문, 일반 알림문 등록 및 스크립트 기반 VM 채점 기능 제공

### 03 시나리오 구성 및 훈련 생성 (개인/팀)



- 시나리오 기반 훈련 문제, VM 문제, 서비스 구성 기능 제공
- 소속 별, 팀 또는 개인 별 훈련 생성 및 참여 기능 제공

### 04 훈련 수행 및 통계



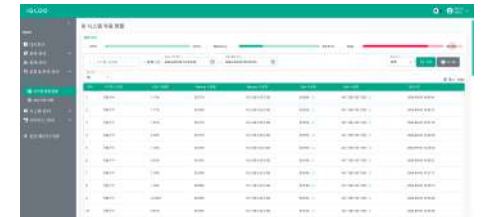
- 훈련 서비스 구성에 따른 문제 풀이와 VM 콘솔 접속을 통한 서비스 조치 기능 제공
- 개인/팀 별 참여 현황, 회사 별 과목 점수, 과목 별 참여 현황 등 정보 조회 기능 제공
- 훈련 수행 결과에 따른 통계 확인 기능 제공

### 05 설문/문의 관리



- 훈련 평가 설문 및 문제 풀이 문의 기능 제공
- 훈련 평가를 위한 설문지 제공 및 이력 관리 기능 제공
- 훈련 문제 풀이 관련 관리자 문의 기능 제공

### 06 시스템 관리

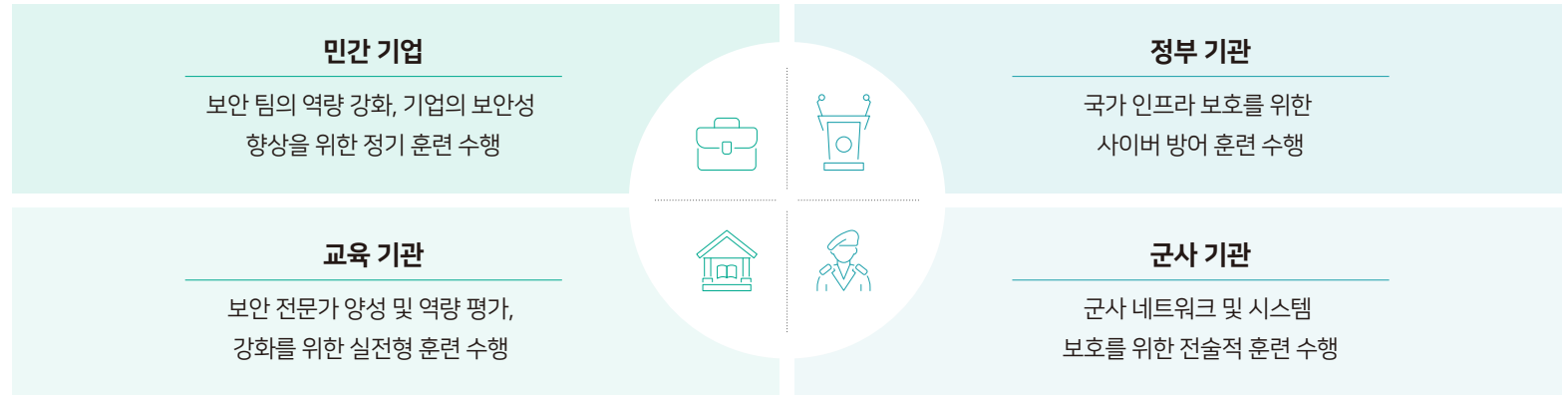


- 훈련 환경 조성을 위한 VM 및 연계 자원 관리 기능 제공
- 시스템 및 훈련 VM 자원(CPU, MEMORY, DISK) 관리 및 VM 제어를 위한 연계 관리 기능 제공

## Use cases

PLOT CDX는 민간·정부·군사·교육 기관 등 다양한 조직의 보안성 강화를 위한 핵심 요소로 기능합니다.

각 조직들은 핵심 정보 자산 및 인프라를 보호하고 사이버 전쟁에 대비한 전략 수립 및 대응 능력을 높이는 한편, 사이버 안보 수호의 핵심이 될 보안 전문가 양성·발굴에도 힘을 실을 수 있습니다.



## Service model

모든 보안 담당자 및 조직들이 보안 역량을 업스케일링할 수 있도록, 고객 상황에 부합하는 다각화된 서비스 모델을 제공합니다.

사이버 공격을 미리 경험하고 대응해 보는 것은 조직이 시시각각 변화하는 보안 위협에 신속하게 대응하고 피해를 최소화하는 데 중요한 역할을 합니다. PLOT CDX를 통해 실전 경험을 쌓고, 공격자 보다 한 수 앞선 대응 역량을 확보하세요.

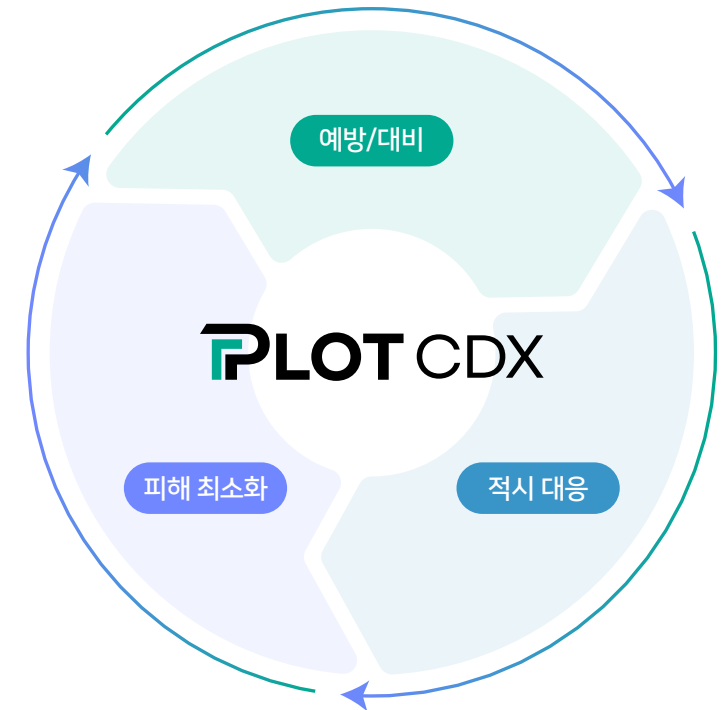
사용자	서비스 형태	비용
기관 및 기업	이론 및 실습 (오프라인)	유료 (협약: 교육 인원에 따라 금액 책정)
	구축형	유료 (협약)

(2024년 10월 기준)

## Benefits

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

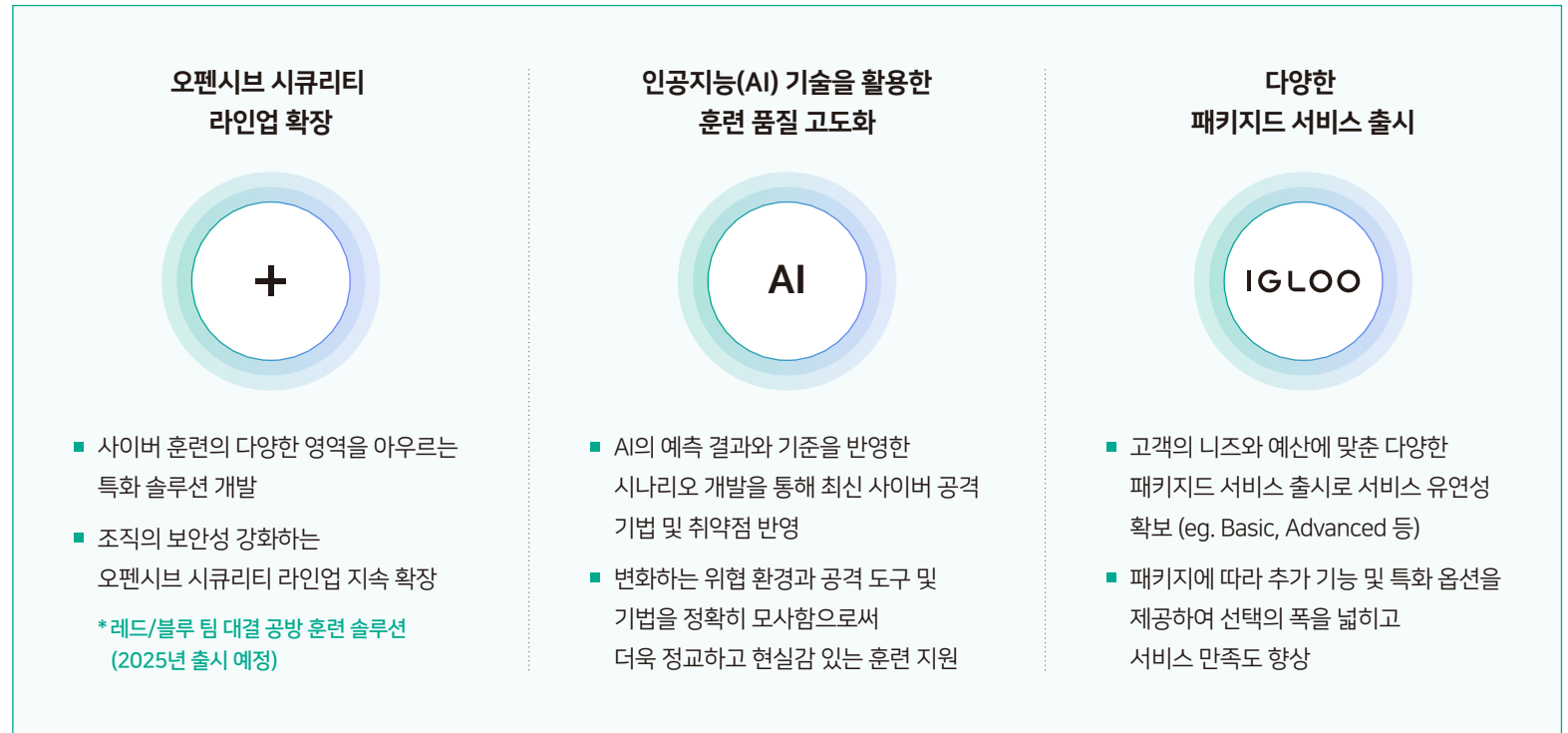
PLOT CDX를 통해 보안 담당자는 사이버 공격 탐지·대응·분석 역량을 강화하고, 조직은 상황에 부합하는 위기 대응 전략을 개발·점검·평가함으로써, 미래 공격에 대한 안정적인 보안 태세를 유지할 수 있습니다.



## Roadmap

제품 라인업 확장·적용 기술 고도화·서비스 모델 다양화를 통해, 더 많은 조직이 PLOT CDX를 활용할 수 있도록 지원할 예정입니다.

이글루코퍼레이션이 제공하는 오픈시브 시큐리티 제품을 통해 조직의 보안 태세를 점검하고, 비즈니스 운영에 영향을 미칠 수 있는 잠재적 취약성을 파악하면서 진화하는 위협에 앞서가세요.



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 관리(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.