(주)코어시큐리티
Architecting Resilience for the Future

ShieldOn

AI 기반 실전형 사이버 공방훈련 플랫폼

" 보는 훈련이 아니라, 하는 훈련이 실력을 만든다 "

탐지부터 예방까지, AI가 자동화한 반복훈련 사이클로 조직이 즉시 투입 가능한 보안 인재를 양성합니다.
구축형 · 구독형으로 유연하게 도입하고, 차세대 협력형(Collaborative) 모델로 계속 진화합니다.

AGENDA

오늘 소개해 드릴 순서

지금의 ShieldOn 기술부터, 도입 방안, 그리고 다음 진화 모델까지 순서대로 안내드립니다.

(주)코어시큐리티
Architecting Resilience for the Future

교육훈련과 모의훈련은 다르다 - 그리고 하나로 이어진다

교육훈련(Training)과 모의훈련(Exercise)은 서로 다른 목적을 갖지만, 실전 대응력은 이 둘이 이어질 때 완성됩니다.

교육훈련 (Training)

개인의 지식 및 기술 습득 중심

보안 원리와 이론적 토대를 구축하는 과정. 본질 이해와 기술 실현 능력 배양이 목적입니다.

모의훈련 (Exercise)

절차 및 팀 숙련 중심

팀의 소통 및 업무 처리 숙련도를 높이는 과정. 위기 시 즉각적 행동 변화 및 팀내 절차수행 능력 배양이 목적입니다.

구분	CTF(Capture The Flag)	CDX(Cyber Defense Exercise)
목적	기술 역량 검증	절차 · 협력 숙달
환경	가상 단일 시스템	Cyber Range 전체
방식	개인 기술 연습	팀 기반 시나리오
평가	기술 점수	대응 완결성
산출물	취약점 리포트	대응 보고서 · SOP

ShieldOn 플랫폼은 교육훈련, 모의훈련, CTF, CDX 까지 모든 서비스를 하나의 통합 환경에서 지원합니다.

WHY NOW

지식이 아니라, 실전 경험이 격차를 만든다

사이버공격은 점점 더 자동화 · 국가화 · 다중화되고 있습니다. 단일 조직, 단일 인력의 능력만으로는 더 이상 막을 수 없습니다.

300%

국가 주도 공격 증가율

2020 → 2024 누적

SOURCE · MICROSOFT DIGITAL DEFENSE REPORT

$10.5T

연간 사이버 범죄 피해

2025 글로벌 추정 손실

SOURCE · CYBERSECURITY VENTURES

204일

평균 침해 탐지 소요

핵심 인프라 기준 MTTD

SOURCE · IBM COST OF A DATA BREACH

68%

복원력 훈련 부족 기관

주요 산업 설문 응답

SOURCE · WEF GLOBAL CYBER OUTLOOK 2025

INSIGHT

공격자는 이미 RaaS · IAB · 익스플로잇 거래소로 분업화된 공격 네트워크를 갖췄습니다. 막연한 지식이 아니라, 실전에서 검증된 대응 체계와 반복훈련만이 이 격차를 좁힐 수 있습니다.

(주)코어시큐리티
Architecting Resilience for the Future

ShieldOn 플랫폼 아키텍처

IT · OT를 통합한 하이브리드 가상환경 위에서 Red(공격)와 Blue(방어)가 실시간 교전하고, 결과는 즉시 훈련포탈에 가시화 됩니다.

Training Portal

훈련생 · 관리자 접점 - 훈련 일정 · 진행률을 대시보드로 실시간 확인

VIRTUALIZATION LAYER · IT · OT 하이브리드 가상환경 (디지털 트윈)

Opposing Force (AI Red)

MITRE ATT&CK 기반 AI 자동 공격 · 실시간 전술 변경 · 적응형 단계 확대

Defense Team (Blue)

탐지 → 분석 → 격리 → 복구, SOC/IR 절차 그대로 재현하는 방어 훈련

온프레미스 · 클라우드 · 이동형

IT / OT / ICS 통합

폐쇄망 지원

한국어 지원 · 국내 조달

System Administration & AI AAR

통합 관제 · 로그 · 사후강평 - 결과가 즉시 Training Portal로 환류됩니다

(주)코어시큐리티
Architecting Resilience for the Future

하나의 플랫폼 안에서 유기적으로 연결되는 6대 기능

Training Portal 부터 대항군 운영까지, ShieldOn은 사이버 공방훈련의 전 과정을 하나의 허브에서 지원합니다.

PLATFORM

(주)코어시큐리티
Architecting Resilience for the Future

ShieldOn 6대 핵심 기능

ICDX부터 실전훈련까지 단일 플랫폼으로 통합 운영합니다. 시나리오 저작 · 대항군 운용 · 사후강평 3개 기능에 AI를 적용해 정교한 실전 훈련 환경을 제공합니다.

Training Portal

훈련 포털

훈련 일정 · 인원 · 진행률을 대시보드로 실시간 확인, 관리자/훈련생 역할별 맞춤 뷰

Virtualization

가상 · 모사

서버 · 네트워크 · 보안장비를 가상으로 완벽 재현한 디지털 트윈 전장

Scenario Authoring

AI

AI 시나리오 저작

MITRE ATT&CK 기반으로 AI가 공격 시나리오를 자동 생성 · 난이도 조절. 최신 CVE 즉시 반영

Opposing Force

AI

AI 대항군 운용

AI 기반 공격자가 실시간 전술 변경 · 우회 공격 수행, 방어자 수준에 맞춰 적응형 단계 확대

After Action Review

AI

사후강평 (AAR)

탐지 · 대응 시간 · 정확도 등 핵심 KPI를 AI가 자동 분석, 취약 영역별 개선안 제시

System Administration

훈련체계 관리

사용자 권한 · 가상장비 · 훈련 이력 · 로그를 단일 콘솔에서 통합 관제

AI AUTOMATION

(주)코어시큐리티
Architecting Resilience for the Future

준비 → 공격 → 평가까지, AI가 자동화합니다

AI 3종 세트(시나리오 생성 · 레드팀 · 사후강평)의 통합 운영이 ShieldOn의 핵심 경쟁력입니다. 사람은 「판단」에 집중합니다.

STAGE 01

AI 시나리오 준비

- 최신 CTI 자동 수집 · 위협 인텔 매핑
- TTP ↔ 시나리오 자동 변환
- 분야별(국방 · 금융 · OT) 캠페인 생성
- 난이도 · 유형 동적 조정

STAGE 02

AI 공격 실행

- AI 자율 레드팀이 다중 벡터 동시 공격
- 방어 대응에 따라 적응형 단계 확대
- 무제한 반복 · 별도 공격 인력 불필요
- OT/ICS · 공급망 벡터 포함

STAGE 03

방어 모니터링

- 실시간 공방 대시보드
- 자동 채증 · 로그 수집
- 다중 시나리오 병렬 운영
- 훈련생 · 관전자 실시간 가시화

STAGE 04

AI 사후강평 (AAR)

- 행동 · 결과 자동 채점
- AI 디브리핑 리포트 자동 생성
- 취약점 · 재훈련 영역 도출
- 맞춤 교육 경로 제안

TRAINING CYCLE

(주)코어시큐리티
Architecting Resilience for the Future

탐지 → 예방, 반복훈련 5단계 사이클

피해를 최소화하고 회복력을 강화하는 5단계 사이클. 사람은 훈련에 더 오래 머무르고, AI는 반복 비용을 낮춥니다.

01
DETECT
탐 지
실시간 탐지 · 이상 징후 포착. EDR · SIEM · NDR 룰 트리거

→

02
INVESTIGATE
조 사
로그 · 패킷 상세 조사, 타임라인 재구성

→

03
ANALYZE
분 석
공격 경로 · 영향도 분석, TTP 매핑 · 행위자 추정

→

04
RESPOND
조 치
차단 · 격리 신속 대응, 자원 동원 · 의사결정

→

05
PREVENT
예 방
취약점 개선 · 재발 방지, 정책 갱신 · 룰 튜닝

FEEDBACK LOOP · 5단계의 결과는 즉시 1단계에 반영되어 다음 시나리오의 난이도와 벡터를 결정합니다. REPEAT ↻

-72%
평균 탐지 시간(MTTD) 단축

3.4×
사고 대응 정확도 향상 (재훈련 1기수 대비)

무제한
AI 대항군 상대 반복훈련 · 별도 공격인력 불필요

(주)코어시큐리티
Architecting Resilience for the Future

두 갈래로 나뉘는 보안 인프라 흐름, ShieldOn은 모두 대응합니다

망분리 규제가 강화되는 공공 · 국방 영역과, 클라우드 전환이 가속화되는 민간 영역 - 두 흐름에 맞춰 구축형과 구독형을 함께 제공합니다.

B2G · 규제 대응

구축형 (On-Premise)

플랫폼을 고객 내부 서버에 설치합니다. 망분리 · 보안 규정에 완벽 대응하며, B2G 공공 · 국방 · 에너지 영역에 주력합니다.

B2B · 신속 도입

구독형 (Cloud SaaS)

클라우드로 설치 없이 바로 사용합니다. B2B 기업 · 교육기관 · 클라우드 허용 기관에 적합합니다.

해외 수출용

국가별 단기 · 중장기 파이프라인을 분리 관리하며, 한국어 · 현지어를 병행 지원합니다.

(주)코어시큐리티
Architecting Resilience for the Future

구축형 도입 기대효과

망분리 의무기관 · 공공 · 국방 · 에너지 영역에 최적화된 도입 방식입니다.

적합 대상

- 정부 · 공공기관
- 국방 · 안보기관
- 에너지 · 기간산업
- 금융보안 특화기관

2016년 금융보안원 최초 구축 이후, KISA · 한국전력 · 해군 등 국내 폐쇄망 환경에서 실전 운영을 검증했습니다.

완전한 망분리 · 데이터 주권

폐쇄망 환경에서 100% 자체 운영, 외부 데이터 유출 리스크를 원천 차단합니다.

보안규정 · 조달요건 충족

국가 조달 및 보안적합성 검증 등 공공 · 국방 규정에 그대로 대응합니다.

기밀 시나리오 완전 통제

기관 고유 자산과 시나리오를 외부 노출 없이 커스텀 설계할 수 있습니다.

기존 인프라 연동

내부 SIEM · EDR · 자산관리시스템과 직접 연동해 운영 효율을 높입니다.

대규모 반복훈련 시 TCO 절감

장기적으로 대량 훈련 횟수 대비 총소유비용(TCO)이 구독형보다 유리해집니다.

(주)코어시큐리티
Architecting Resilience for the Future

구독형 도입 기대효과

설치 없이 즉시 시작하는 기업 · 교육기관을 위한 도입 방식입니다.

- ✔ 즉시 시작 (Time-to-Value)
- ✔ 초기투자 최소화
- ✔ 사용량 기반 유연 확장
- ✔ 최신 AI 시나리오 자동 반영
- ✔ 원격 · 다지점 동시 훈련

Starter

1회 훈련

- ✔ 클라우드 플랫폼 접근
- ✔ 훈련 1회 포함 (0.5 or 1일)
- ✔ 기본 시나리오 라이브러리
- ✔ 자동 AAR 리포트

Professional

추 천

연간 훈련 구독

- ✔ 클라우드 플랫폼 연간 이용
- ✔ 훈련 연 4회 포함 (볼륨 선택)
- ✔ 업종별 환경 템플릿
- ✔ 팀 성과 대시보드

Enterprise

맞춤 계약

- ✔ 전용 클라우드 테넌트
- ✔ 훈련 횟수 약정 · 무제한
- ✔ 커스텀 시나리오 제작 포함
- ✔ CISO 보고서 브리핑 포함

(주)코어시큐리티
Architecting Resilience for the Future

SHIELDON NEXT · 예고

차세대 협력형(Collaborative) ShieldOn

지금의 ShieldOn 위에 「협력」을 훈련하고 측정하는 레이어를 더한, 코어시큐리티의 다음 진화 모델입니다.

협력형이란, 사이버 위협 대응의 각 단계에서 개인 · 기관 · 국가 간 부족한 부분을 상호 보완하며 함께 대응해 나가는 전(全) 과정을 훈련하는 모델입니다.

사이버레인지는 어떻게 진화해 왔는가

2016 – 2020

1세대

기술습득형

고정 시나리오 · 단일 사용자, 정답 매칭 기반 채점

2021 – 2025 현 재

2세대 · CURRENT

가상화 통합형

AI 자동화 · IT/OT 하이브리드 가상환경,
ShieldOn이 지금 제공하는 모델

2026 –

차세대 · NEXT

AI 기반 협력형

AI 자동 시나리오·공격·평가 + 조직·국가 간
단계별 협력을 정량 측정

(주)코어시큐리티
Architecting Resilience for the Future

SHIELDON NEXT · 예고

협력형(Collaborative) 모델은 세 계층을 함께 다룹니다

공격은 한 사람, 한 조직만 잘 막아서 끝나지 않습니다. 차세대 ShieldOn은 세 계층의 협력을 모두 훈련 대상으로 설계하고 있습니다.

TIER 1 · OPERATOR-LEVEL

개인 ↔ 개인

분석가 · 운영자 간 인계와 의사소통, 야간/주간 교대 시 상황 인수인계, 역할 교차 협업 (Red↔Blue 학습)

TIER 2 · ORGANIZATION-LEVEL

기관 ↔ 기관

정보공유(CTI · IoC · TTP) · 공동대응(CSIRT · ISAC · MSP) · 공급망 · 협력사 · 자회사 간 합동 훈련

TIER 3 · NATIONAL-LEVEL

국가 ↔ 국가

동맹 · 우방국 간 연합 사이버 훈련 · 국가 사이버 안보센터 연계 · 국제 규범 · 법집행 공조

(주)코어시큐리티
Architecting Resilience for the Future

SHIELDON NEXT · 예고

개인 기술을 넘어, 협력 능력까지 측정할 계획입니다

현재 ShieldOn은 Skill · Performance를 평가합니다. 차세대 ShieldOn은 여기에 「협력」을 더해 3축으로 평가하는 체계를 준비하고 있습니다.

S Skill · 개인 기술 역량

탐지 · 분석 · 격리 · 복구의 절차 정확도 (현재 제공 중)

P Performance · 팀 대응 성과

침해 차단 시간(RTO) · 오탐률 · 피해 확산 차단 시점 (현재 제공 중)

C Cooperation · 협력 지표 ★

정보공유 적시성 · 역할분담 명확성 · 인계 정확도, 차세대 ShieldOn에서 추가될 평가축입니다.

협력지표 세부 설계 (안) - 예시 코호트 데이터

① 정보공유 적시성

IoC 공유까지 걸린 시간 ≤ 3분

88%

② 역할분담 명확성

중복 · 공백 없이 역할이 배분됐는가

76%

③ 공동의사결정 품질

팀 합의 결정이 최적 대응과 일치

92%

④ 교대인계 정확도

인계 시 누락 없이 상황 전달

71%

설계 방향 수료 = Skill ∩ Performance ∩ Cooperation · 협력지표 70% 미달 시 재훈련 부여 (안)

(주)코어시큐리티
Architecting Resilience for the Future

SHIELDON NEXT · 예고

협력형 훈련이 기대하는 인재상

차세대 ShieldOn의 협력형 훈련을 거친 인재는 다음과 같은 역량을 갖출 것으로 기대합니다.

01 · REACTION
실전 반응속도

AI 적응형 공격을 반복 경험하여, 처음 보는 공격에도 우선순위 판단이 빠릅니다

02 · COOPERATION
협력 역량

정보공유 · 인계 · 공동의사결정 등 「사람과 일하는 능력」이 행동으로 체화됩니다

03 · THREAT MODEL
위협 사고 모델

Red↔Blue 양방향 학습으로 「공격자 관점에서의 방어 설계」가 가능해집니다

04 · DATA-DRIVEN
데이터 기반 개선

AAR과 협력지표를 토대로 본인 · 팀의 약점을 정량적으로 인식하고 보완합니다

05 · SYSTEM-LEVEL
체계 설계 시야

단일 도구가 아닌 「훈련체계」 자체를 이해 - 조직의 보안 체계 설계가 가능합니다

06 · GLOBAL
국제 호환 역량

글로벌 표준 시나리오 · 평가에 맞춰 훈련 - 연합훈련 · 해외협력에 즉시 투입 가능

ONBOARDING

4단계 표준 도입 절차

사전 진단부터 운영 안정화까지, 구축형 · 구독형 공통의 표준화된 절차로 빠르고 안전하게 도입합니다.

사전 진단
1주

환경 · 요구 분석, 직무 현황 파악, 도입 목표 설정

도입 타당성 보고서

→

PoC
2주

시범 운영, 핵심 기능 검증, 효과 측정

PoC 결과 · 권고안

→

본 도입

전체 온보딩, 콘텐츠 · 역량 모델 설정, 시스템 연동

운영 가능 상태

→

운영 안정화

정기 점검 · 콘텐츠 업데이트 · 신규 직무 추가

월간 운영 보고

(주)코어시큐리티
Architecting Resilience for the Future

CLOSING

실전과 같은 훈련이, 실전에서 통하는 사람을 만듭니다

ShieldOn - 지금은 실전형 AI 공방훈련, 다음은 협력형 사이버레인지

NOW

지금, ShieldOn

AI 기반 실전 공방훈련을 구축형 · 구독형으로 유연하게 도입할 수 있습니다.

NEXT

다음, ShieldOn NEXT

협력을 훈련하고 측정하는 차세대 협력형 모델을 준비하고 있습니다.

CORE

변하지 않는 것

2011년부터 15년, 실전 운영 경험과 7만+명 양성 실적입니다.

발표자

주한익 기술이사 · (주)코어시큐리티 사이버교육훈련사업본부

THANK YOU.

웹사이트

www.coresec.co.kr

문의

02-3453-6630 · 사이버보안교육훈련사업본부