2025 NSHC
보안교육 과정소개서

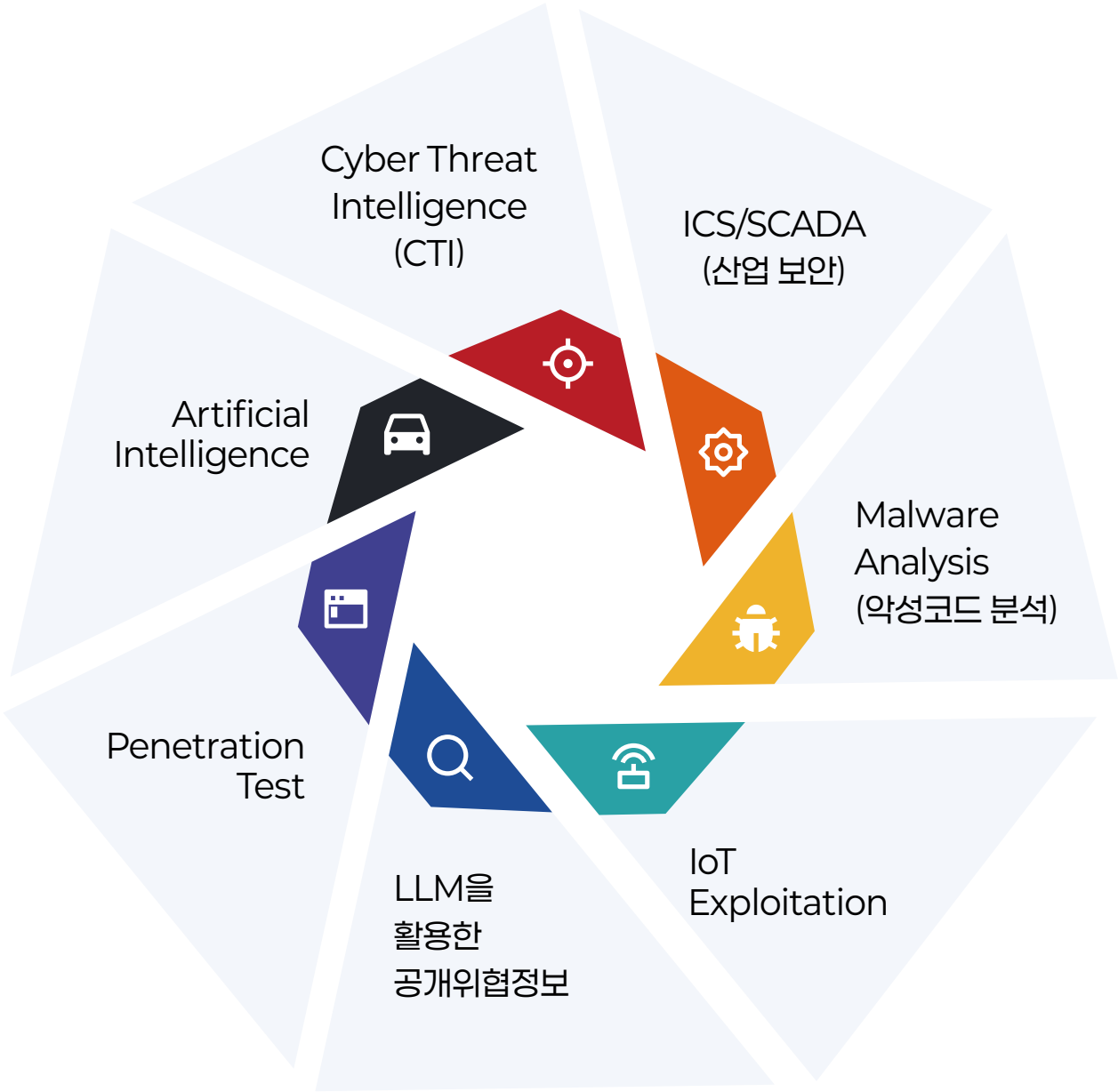
More Secure and Safe

NSHC SECURITY

NSHC Training

NSHC 보안교육은 보안 관리자 또는 실무자를 위한 Advanced 전문가 교육으로, 실제 사례를 통해 미래에 일어날 수 있는 보안 사고를 예방하거나 막는 데 도움이 되는 기술을 배울 수 있습니다.

NSHC 보안교육 둘러보기 [CLICK!]



NSHC 보안교육 소개

교육생들의 역량 강화를 위해 실무에 경험이 풍부한 연구진이 직접 강의를 진행하여 수준 높은 강의 콘텐츠를 제공합니다.

실습 위주의 교육

단순 이론 교육이 아닌 실제 상황 및 사건을 바탕으로 구성된 실습 교육을 통해 실제 위협에 대응할 수 있는 방법을 알려드립니다.

맞춤형 교육

기관 및 회사에서 필요로 하는 교육 과정을 제공합니다. 교육 대상 및 기관 요청에 따라 커리큘럼을 수정할 수 있고, 기본 3일 교육을 2~5일로 유연하게 조정 가능합니다. 또한, 교육생 관리를 위해 평가기준에 따른 이론 및 실습평가를 선택적으로 진행합니다.

온/오프라인 교육 가능

오프라인 교육 시 프리미엄급 교육장을 대관하여 교육이 쾌적하게 진행되도록 지원합니다. 온라인 교육을 진행할 경우 NSHC 온라인 교육센터인 RAT Studio에서 원격으로 실시간 교육 및 실습이 가능합니다.

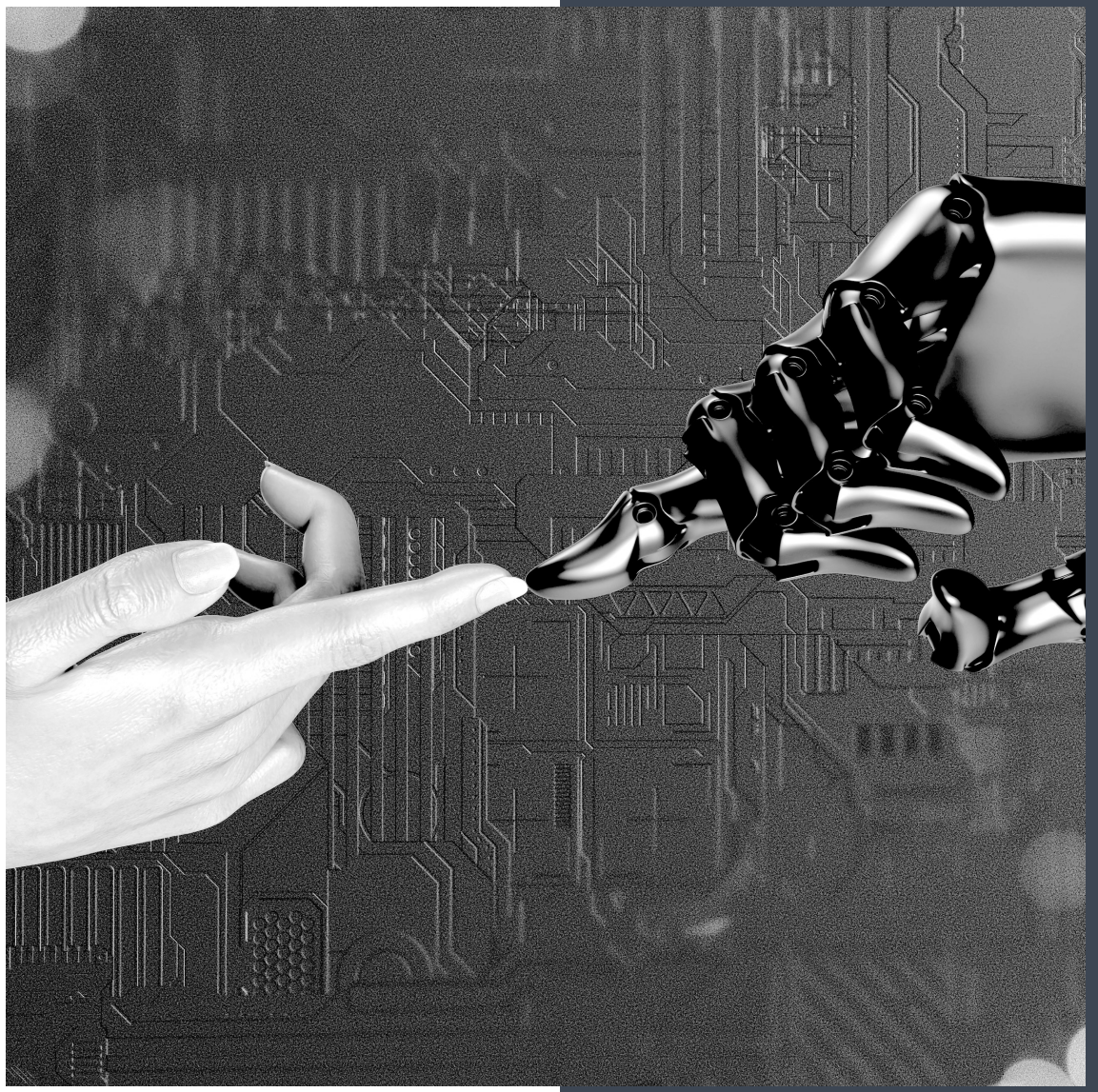
보조강사 지원

매 교육마다 3~4명의 현업 연구원들이 보조강사로서 직접 교육을 지원하여 교육생의 실습이 원활하게 진행되도록 도와드립니다.

AI Red Teaming
전문가 교육

AI 보안을 Red teaming 관점에서 심도 있게 다룬 보안 교육

#LLM 및 AI 활용 개요 #AI 보안 위협 이해 #AI 기반 보안 기술 활용



NSHC SECURITY

AI Red Teaming 전문가 교육

교육 개요

- LLM 및 AI 활용 개요
- AI 보안 위협 이해
- AI 기반 보안 기술 활용
- 프롬프트 인젝션
- AI Redteaming
- AI 인프라 보안

교육 대상

보안 담당자 (정보보호팀, 보안관제, 침해대응), 개발자 (웹/서비스/AI 서비스 개발), 보안 컨설턴트 및 감사 담당자
클라우드/AI 인프라 운영자, AI 서비스 기획자 및 PM

선수 지식

- 기본적인 웹 보안 개념 (XSS, SQLi 등) 이해
- 리눅스/CLI 환경 사용 경험
- API 및 웹 서비스 구조에 대한 기초 지식
- AI/머신러닝 기본 개념에 대한 이해

AI Red Teaming 전문가 교육

시간	Day 1 – Security for AI	Day 2 – AI for Security	Day 3 – AI Red Teaming
Session 1	**AI Red Teaming 및 LLM 개요** White / Black box Red Teaming against AI	**LLM 탈옥(Jailbreak) 자동화 에이전트 제작** LLM 탈옥 개념, 전략 설명 및 실습 LLM 탈옥 자동화 에이전트 제작 실습 교육 참가자의 LLM 탈옥 자동화 에이전트 커스터마이징 및 테스트	**Red Teaming SOTA Models with Blackbox Approach** GPT 5에서 Claude 4.5까지 가장 안전한 모델에 대한 Red Teaming 전략
Session 2	**AI Red Teaming 및 LLM 개요** Emerging Threats in Agentic AI	**Google Dorking 자동화 에이전트 제작** Google Dorking 개념 설명 및 예제 실습 AI 에이전트 및 멀티 에이전트 개념 설명 Google Dorking 자동화 에이전트 제작 실습	**Red Teaming ML~AI Models with Whitebox Approach** White box 방법론을 통해 다양한 모달리티의 ML Model에 대한 적대적 공격부터 모델 추출 공격까지
Session 3	**LLM 위협 모델링** OWASP Top 10 for LLM 2025 위협별 개념 설명 및 예제 실습 **실습 예시** - Direct/Indirect Prompt Injection 실습 예제 - RAG 아키텍처에서의 개인정보 노출 실습 예제 - LLM SSRF 혹은 SQLi 실습 예제	**정찰 자동화 에이전트 제작** 정찰 개념 설명 다양한 정찰 기법(URL 아카이브 분석, Dorking, 기술 스택 핑거프린팅, Javascript 분석) 실습 정찰 자동화 에이전트 제작 실습	**Red Teaming AI Agents & Wrap-Up** Agentic AI 시스템에 대해서 zero-day 들과 이를 악용하는 공격 전략

NSHC 보안교육 이력

다년간 Advanced Security Training을 통해 약 100여 회의 교육을 진행하였고, 3,000여 명이 넘는 교육생을 배출하였습니다.

- ICS/SCADA Training (2014~현재) 총 56회
- OSINT Training (2017~현재) 총 23회
- Cyber Threat Intelligence Training (2020~현재) 총 7회
- IoT Exploitation Training (2017~현재) 총 8회
- Malware Analysis Training (2014~현재) 총 10회

(2025.1. 기준)

감사합니다

More Secure and Safe

NSHC SECURITY

Homepage | https://st.nshc.net/

E-mail | training@nshc.net

2025.1