2025 NSHC
보안교육 과정소개서

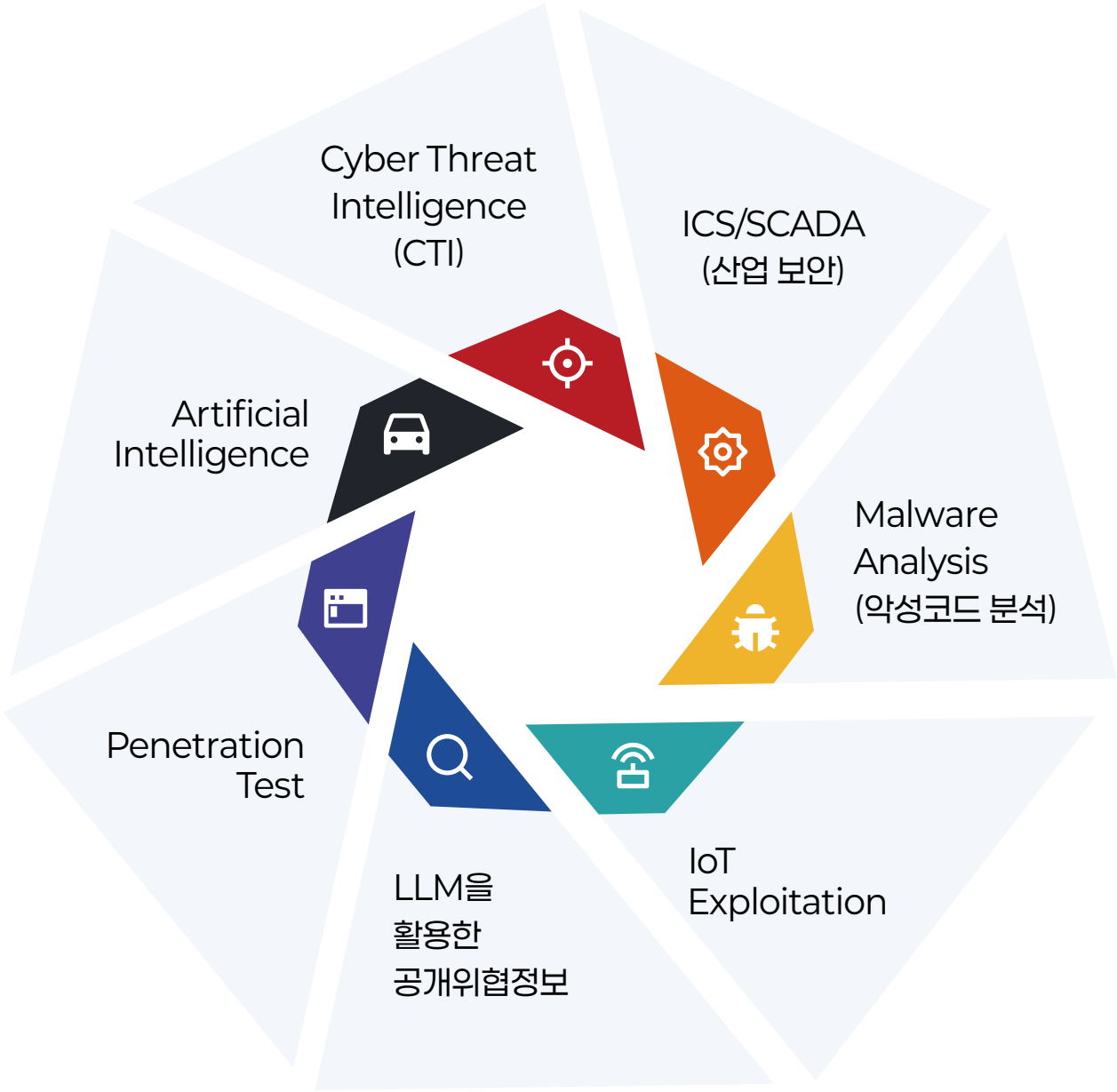
More Secure and Safe

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

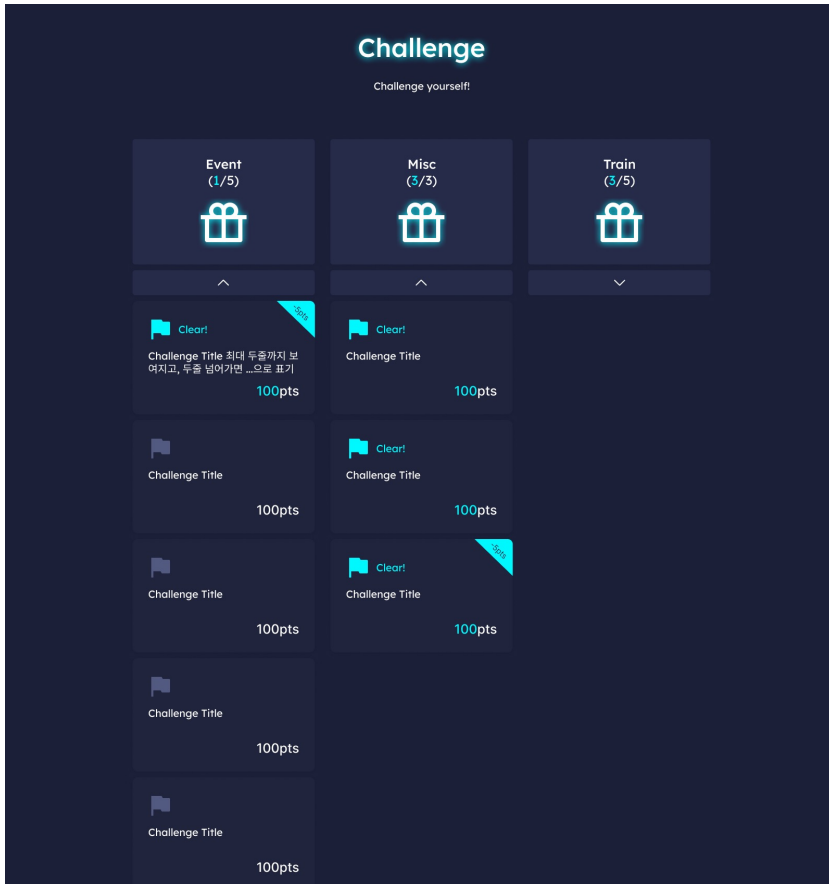
오프라인 교육 시 프리미엄급 교육장을 대관하여 교육이 쾌적하게 진행되도록 지원합니다. 온라인 교육을 진행할 경우 NSHC 온라인 교육센터인 RAT Studio에서 원격으로 실시간 교육 및 실습이 가능합니다.

보조강사 지원

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

모의 해킹 방어 대회 (CTF)

교육 기간 동안에는 모의 해킹 방어 대회를 진행합니다. 시나리오 기반의 CTF(Capture the Flag) 방식을 통해 학습한 내용을 실전에 바로 적용할 수 있습니다.
모의 해킹 방어 대회는 ICS/SCADA, OSINT, IoT 교육에서 실시합니다.



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)

ICS/SCADA
정보 보안 전문가 교육

산업 기반 시설을 안전히 지키기 위한 보안교육

#ICS취약점 #OT위협 #PLC&HMI #RF #BadUSB #BadDNS

NSHC SECURITY

ICS/SCADA 정보 보안 전문가 교육

교육 개요

- ICS/SCADA 기반 시설 대상 사이버 공격 증가
- 산업시설 안전/보안설계의 중요성 증가
- 기반 시설 시스템/소프트웨어의 보안 취약점 이해
- 해커 및 비인가 사용자의 공격 경로 파악
- 공격으로 인한 자동화장비 오작동과 이로 인한 피해 예방
- 기반시설 IT 및 OT 보안 강화

교육 대상

OT 엔지니어, 산업제어장비 보안 관제 엔지니어, 산업제어장비 시스템 관리자/네트워크 관리자, 보안 연구원, IT 기술팀 등

선수 지식

- 정보보안 관련 도메인(Domain) 지식
- 리눅스 OS 기본 사용법 (Kali Linux 사용법)
- 파이썬 기초
- Network 취약점 분석 기초

교육 장비

자체 제작한 시뮬레이션 장비를 실제 PLC와 HMI로 구성하여 기반시설 취약점 진단 및 모의 해킹을 해볼 수 있는 환경을 제공합니다.

Runway

공항관리 시뮬레이션

사이버 공격을 통해 공항 활주로의 유도등을 소등 시켜 항공기를 추락시키는 공격 시뮬레이션

SFPCS

원자로 냉각수 공격 시뮬레이션 시스템

PLC 프로토콜 사이버 공격을 통해 밸브를 제어하고 열교환기가 제기능을 하지 못하도록 하는 시뮬레이션

Smart City

스마트 시티

철도 시스템, 발전소, 공항의 취약점을 이용해 사이버 공격 침해사고를 시각화한 시뮬레이션

Crane

산업용 크레인 공격 시뮬레이션

리모트 제어기 RF 신호를 조작하여 골리앗 크레인을 조작하는 공격 시뮬레이션

PPS

인증우회 시스템

지문인식, RFID, Card, 키패드를 활용한 지능형 폐쇄회로와 인증우회 시뮬레이션

ICS/SCADA 정보 보안 전문가 교육

	1일차	2일차	3일차
Session 1	[ICS/SCADA 개요] OT/ICS 보안에 대한 전반적 동향 ICS/SCADA 구성과 공격 시나리오 Purdue 모델 소개 IT 보안과의 차이점	[ICS 취약점 공격 심화] - Part 1 Fuzzing 기술 & Exploit 개발 개요 실 공격 사례 Case Study	[Radio Frequency Attack] - Part 1 RF 공격 개요 무선신호 감지 RF 공격도구 사용
	[IEC 62443 표준] O.T 보안을 위한 국가 및 국제 표준 소개 IEC 62443 개요 IEC 62443 3-3 규격 상세 소개	[ICS 취약점 공격 심화] - Part 2 Fuzzing 기술 & Exploit 개발 개요 실 공격 사례 Case Study	[Radio Frequency Attack] - Part 2 Crane 시뮬레이션 대상 실습 Replay Attack 실습
Session 2	[PLC 기초] - Part 1 PLC 시뮬레이션 개요 활주로 제어 시스템(Runway) 레더로직 실습 - 1	[PLC 공격 심화] - Part 1 통신 프로토콜 개요 ICS 네트워크 기초 PLC ↔ HMI 패킷 분석	[ICS 취약점 공격 심화] - Part 3 Mini CTF 교육 요약 및 마무리
	[PLC 기초] - Part 2 HMI Simulation 생성 및 PLC 연결 활주로 제어 시스템(Runway) 작화 실습	[PLC 공격 심화] - Part 2 제어전용 프로토콜 분석 제어 프로토콜 변조공격 실습 Malware Injection	
	[PLC 기초] - Part 3 활주로 제어 시스템(Runway) 레더로직 실습 - 2 제어전용 프로토콜 분석 (Modbus, OPC, UA)	[망분리 우회기술] Bad USB 소개와 실습	

감사합니다

More Secure and Safe

NSHC SECURITY

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

E-mail | training@nshc.net

2025.1