

// ROS2 · DDS · AI PIPELINE · CTF

로봇 특화 정보보호 교육 프로그램

4족 보행 로봇과 휴머노이드를 직접 다루며, 로봇 미들웨어의 통신 구조부터 AI 모델·데이터 보안까지 이들 만에 공격과 방어를 완결하는 실습 중심 과정입니다.

FREE 교육비 전액 무료

DAY 01 · UNITREE G01 AIR

DAY 02
UNITREE R1 EDU

신규인력 교육

TRACK A · 일반

1차 11.16 (월) - 17 (화)

2차 11.19 (목) - 20 (금)

재직자 교육

TRACK B · 심화

1차 12.07 (월) - 08 (화)

2차 12.10 (목) - 11 (금)

장소

영남대학교 학생회관 3층 CEL실
공학기술교육혁신센터

교육대상

로봇 AI 보안 관련 신규 인력 및 재직자

커리큘럼 · 2일 과정

09:30 - 17:30 · 이론 50 : 실습 50

01 DAY 01 · 과정 1 G01 AIR ROS2 및 로봇 미들웨어 보안

09:30 - 10:30 AI 로봇 보안 개요

이론

10:30 - 12:00 ROS2 기본 구조와 보안 이슈

이론

12:00 - 13:00 LUNCH

13:00 - 14:30 DDS 통신 구조 이해

이론 · 실습

14:30 - 16:00 ROS2 공격 표면 분석

실습

16:00 - 17:30 ROS2 보안 기능

실습

FOCUS 제어-상태 토픽 식별, 참가자 디스커버리, 전송 계층 인증·암호화, 보안 기능 적용 전후 비교

TRACK A · 일반

11월 · 신규인력

신규인력 트랙

공격과 방어 개념의 시각적 이해 중심

- 개념 → 시연 → 따라하기 순서의 단계별 실습
- 사전 구성된 VM 이미지로 진입 장벽 제거
- 입문 난이도 CTF로 성취 경험 먼저 제공

02 DAY 02 · 과정 2 R1 EDU AI 모델 및 로봇 데이터 보안

09:30 - 10:30 로봇 AI 파이프라인 이해

이론

10:30 - 12:00 AI 모델 공격 개요

이론

12:00 - 13:00 LUNCH

13:00 - 14:30 학습데이터 및 공급망 보안

이론 · 실습

14:30 - 15:30 Prompt Injection 및 LLM 로봇 보안

실습

15:30 - 17:00 로봇 데이터 보호

실습

FOCUS 양안 카메라 공간 정보 보호, 음성 입력 처리 경로, LLM 명령 주입 위험, SDK 제어 명령 검증

TRACK B · 심화

12월 · 재직자

재직자 트랙

실제 로봇 제품과 코드 대상 분석 중심

- 취약점 제로베이스 분석 직접 수행
- 시큐어 코딩과 보안 패치 적용까지 완결
- 미지의 대상을 스스로 분석하는 실전형 CTF

50%+ 실습·프로젝트 중심

두 트랙 모두 실습 및 프로젝트 비중 50% 이상

CTF 실무형 문제 풀이를 통한 평가

입문·응용·실전 3단계 문항으로 평가

3LV VM → 시뮬레이터 → 실물

폐쇄 네트워크에서 안전하게, 실제 로봇으로 검증

주관 KIRO 한국로봇융합연구원

교육진행



NSHC CIS 연구소

교육비

무료

관련문의

training@nshc.net

* 세부 시간은 현장 상황에 따라
일부 조정될 수 있습니다.

APPLY NOW

교육 신청

QR 코드를 스캔해
신청서를 작성하세요