2025 NSHC
보안교육 과정소개서

More Secure and Safe

NSHC SECURITY

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.

Cyber Threat Intelligence 전문가 교육

사이버상의 위협을 방어하기 위한 다양한 방법론

#MISP #악성코드 #Indicator
#MITRE ATT&CK #YARA\

Cyber Threat Intelligence 전문가 교육

교육 개요

- 사이버 위협으로부터 조직을 지키기 위한 전략
- CTI의 기본 개념과 단계별 접근 방식
- CTI를 위한 MISP 플랫폼 경험 및 구축
- 정적/동적 Indicator 추출 및 Pivoting
- Yara를 사용한 Threat Hunting
- MITRE ATT&CK

교육 대상

군/공공기관 및 기업 보안 담당자, 기업 보안 정책 담당자, 침해사고 대응 및 분석 담당자, 보안 관제 담당자, 악성코드 분석 담당자, 위협 인텔리전스 담당자 등 기타 사이버 보안 위협 관련 업무 담당자 등

선수 지식

- 컴퓨터 공학 및 소프트웨어 공학
- 정보보안 관련 도메인(Domain) 지식
- DFIR(Digital Forensic and Incident Response) 관련 지식과 경험
- 위협 헌팅 및 악성코드 헌팅 관련 지식과 경험
- 악성코드 분석 및 리버스 엔지니어링(Reversing Engineering) 관련 지식과 경험

Cyber Threat Intelligence 전문가 교육

	1일차	2일차	3일차
Session 1	[오리엔테이션] - 트레이닝 소개 및 학습 목표 - 강사 및 교육생 소개	[악성코드에서 Indicator 추출] - 정적 지표 소개 및 추출 기법 - 동적 지표 소개 및 추출 기법 - 네트워크 지표 소개 및 추출 기법 - 지표 추출 실습 진행	[Threat Hunting을 위한 Yara Rule] - Yara 기본 문법 - Yara 사용 사례 분석 및 실습 - Yara 사용 고급 사례 분석 및 실습 - Yara를 이용한 Threat Hunting 실습
Session 2	[사이버 위협 정보분석 개요] - CTI 개념과 3단계 레벨 - CTI를 위한 정보 출처 - CTI 기반의 보안 운영 - 악성코드 기반의 CTI 프로세스 - CTI를 이용한 위협 탐지/대응 개념		
Session 3	[MISP를 이용한 CTI 플랫폼 구축] - CTI를 위한 MISP 플랫폼 소개 - MISP 구축 실습	[Indicator를 이용한 Pivoting] - 네트워크 지표 기반의 Pivoting 기법 - 네트워크 지표를 이용한 Pivoting 실습	[MITRE ATT&CK] - ATT&CK Matrix 개념 - 분석 보고서와 ATT&CK Matrix 연결 사례 - Raw 데이터와 ATT&CK Matrix 연결 사례
Session 4		[Clustering & Correlation] - TLSH 활용 - Imphash 활용 - Rich Header Hash 활용 - .NET Module ID 활용 - 기타 Clustering 기법 활용	[Wrap Up] - 트레이닝 요약 및 마무리

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