사이버 위협 인텔리전스

CTI & OSINT & 다크웹
정보 수집 / 분석 / 추적 / 모니터링
실무 과정

4일 교육과정 커리큘럼

INSEC security

사이버 위협 인텔리전스

CTI & OSINT & 다크웹 정보 수집 / 분석 / 추적 / 모니터링 실무 과정 (4일)

교육일정	교육내용	교육시간
1일차	**오픈소스 인텔리전스 [OSINT] 란?** – 데이터(Data) / 정보(Open Information) / 인텔리전스(Intelligence) – OSINT [Open Source Intelligence] 개요 – OSINT [Open Source Intelligence] 의 필요성 – Open Source Data의 분류 – Open Source Intelligence Cycle	10:00 ~ 10:25
	오픈소스 인텔리전스 [OSINT] 시작하기 – OSINT TECHNIQUES – OSINT FRAMEWORK – OSINT MAPS	10:25 ~ 10:50
	오픈소스 인텔리전스 [OSINT]와 사이버 보안 – 사이버 보안에서의 OSINT – 사이버 보안에서 OSINT 활용 방안 – OSINT를 활용한 사이버 범죄 조사 / 추적 사례 / 범죄 조사 / 추적 방안 – 공격 표면 관리(Attack Surface Management) – 사이버 보안에서 활용 가능한 OSINT TOOL 소개	11:00 ~ 11:50
	OSINT 정보 수집 및 분석 도구 – 쇼단(Shodan) – Shodan 개요 – Shodan 주요 기능 및 사용법 – Shodan을 활용한 정보 수집 및 분석 실습	13:00 ~ 13:50
	OSINT 정보 수집 및 분석 도구 – 센시스(Censys) – Censys 개요 – Censys 주요 기능 및 사용법 – Censys를 활용한 정보 수집 및 분석 실습	14:00 ~ 14:50
	OSINT 정보 수집 및 분석 도구 – 크리미널 아이피(Criminal IP) – Criminal IP 개요 – Criminal IP 주요 기능 및 사용법 – Criminal IP를 활용한 정보 수집 및 분석 실습	15:00 ~ 15:50
	OSINT 도구 활용 – [외부 노출 주요 자산 / 취약 자산] 정보 검색 실습 – 노출된 CCTV / CCTV Management 검색 실습 – 노출된 Database 검색 실습 – 노출된 터미널 서비스(FTP / TELNET / SSH / RDP 등) 검색 실습 – Heartbleed 취약점 검색 실습 – EternalBlue 취약점 검색 실습	16:00 ~ 16:50
	말테고 [Maltego] – 말테고 [Maltego] 개요 – Maltego 주요 특징 / 정보 수집 / 프로파일링 – Maltego 주요 기능 실습 / 활용	17:00 ~ 17:30
	OSINT 도구 활용 – [암호화폐 주소] 정보 검색 및 수집 실습 – 노출된 비트코인 주소 정보 수집 실습 – 노출된 이더리움 주소 정보 수집 실습 – 노출된 리플 주소 정보 수집 실습 – 기타 암호화폐 주소 정보 수집 실습	17:30 ~ 17:50
	질문 & Review	17:50 ~ 18:00

* 교육 시간 및 교육 내용은 사정에 따라 변동될 수 있으니 참고 바랍니다.

상담문의 : 02-851-5687

사이버 위협 인텔리전스

CTI & OSINT & 다크웹 정보 수집 / 분석 / 추적 / 모니터링 실무 과정 (4일)

교육일정	교육내용	교육시간
2일차	**OSINT 도구 활용 – [악성코드 & 랜섬웨어] 정보 수집** – 악성코드 정보 수집/분석 방법 및 도구소개 – 바이러스토탈 [VirusTotal] – 애니런 [AnyRun] – 메타디펜더 [MetaDefender] – 조샌드박스 [Joe Sandbox] – MISP [Malware Intelligence Sharing Platform] – 에얼리언 볼트 [AlienVault OTX]	10:00 ~ 10:25
	OSINT 정보 수집 자동화 – 스파이더 풋 [SpiderFoot]를 통한 수집 자동화 실습 – 에스노인트 [Sn0int]를 통한 수집 자동화 실습 – Python을 통한 여러 서비스 통합 및 자동화 실습	10:25 ~ 10:50
	사이버 위협 인텔리전스 [CTI : Cyber Threat Intelligence] – 사이버 위협 인텔리전스 개요 – 사이버 위협 인텔리전스 목적 / 유형 / 활용 사례 – 사이버 위협 인텔리전스 주요 기능 / 프로세스 / 위협 탐지 및 대응 – 사이버 위협 인텔리전스 정보 수집 및 분석 도구 소개 – 사이버 위협 인텔리전스를 활용한 사이버 범죄 조사 / 추적 사례 / 추적 방안	11:00 ~ 11:50
	CTI/OSINT 도구 활용 – [악성코드 & 랜섬웨어] 정보 분석 실습 – 랜섬웨어 / 암호화폐 채굴 악성코드 분석 – 분석에서 엔티티 추출 (HASH / IP / Domain / URL / JA3 / CryptoCurrency Address 등) – Hash 엔티티를 통한 연관 샘플 수집	13:00 ~ 13:50
	CTI/OSINT 도구 활용 – [네트워크 엔티티] 정보 분석 실습 – 추출된 네트워크 엔티티 분류 – CTI/OSINT를 통한 IP 분석 – CTI/OSINT를 통한 Domain 분석 – CTI/OSINT를 통한 URL 분석 – CTI/OSINT를 통한 JA3 분석	14:00 ~ 14:50
	CTI/OSINT 도구 활용 – [암호화폐 주소 엔티티] 정보 분석 실습 – 추출된 암호화폐 주소 분류 – CTI/OSINT를 통한 트랜잭션 데이터 추출 – CTI/OSINT를 통한 거래 대상 식별 – CTI/OSINT를 통한 암호화폐 주소 내 자금 흐름 추적	15:00 ~ 15:50
	CTI/OSINT 수집 / 분석 통합 실습 – 악성코드 샘플 분석 실습 – 악성코드 내 주요 엔티티 추출 실습 – 추출된 파일 엔티티를 통한 유사 샘플 분석/식별 실습 – 추출된 네트워크 엔티티를 통한 C2 / 유포지 등 분석/식별 실습 – 추출된 암호화폐 주소 추적 및 자금 도착지 분석/식별 실습	16:00 ~ 16:50
	다크웹 인텔리전스 [Darkweb Intelligence] – 다크웹(Darkweb) 개요 – 다크웹(Darkweb) 검색 서비스 – 다크웹 인텔리전스(Darkweb Intelligence) 서비스 – OSINT & CTI & Darkweb Intelligence 연동 활용 방안	17:00 ~ 17:50
	질문 & Review	17:50 ~ 18:00

* 교육 시간 및 교육 내용은 사정에 따라 변동될 수 있으니 참고 바랍니다.

상담문의 : 02-851-5687

사이버 위협 인텔리전스

CTI & OSINT & 다크웹 정보 수집 / 분석 / 추적 / 모니터링 실무 과정 (4일)

교육일정	교육내용	교육시간
3일차	**다크웹 [Darkweb]** - 다크웹 이란? - 다크웹 주요 특징 - 다크웹 거래 및 범죄 유형 / 범죄 사례	10:00 ~ 10:25
	다크웹 접속 및 검색 - 토르 브라우저(Tor Browser) 개요 - 토르 브라우저 설치 및 다크웹 접속 - 다크웹 블랙마켓 / 범죄 관련 주요 사이트 - 다크웹 검색 엔진 및 서비스 유형	10:25 ~ 10:50
	다크웹 접속을 위한 VPN 도구 - 다크웹 VPN 접속 개요 및 필요성 - 다크웹 접속용 유명 VPN 종류 설명	11:00 ~ 11:25
	다크웹 접속을 위한 VPN 도구 - Anonymous VPN 특징 및 주요 기능 - Anonymous VPN 도구를 이용한 VPN 연결 실습 - ExpressVPN 특징 및 주요 기능 - ExpressVPN 도구를 이용한 VPN 연결 실습	11:25 ~ 11:50
	다크웹 접속을 위한 VPN 도구 - CyberGhost VPN 특징 및 주요 기능 - CyberGhost VPN 도구를 이용한 VPN 연결 실습	13:00 ~ 13:50
	다크웹 익명 서비스 - 히든 위키(Hidden Wiki) / 히든 웰렛(Hidden Wallet) - 다크웹 익명 이메일 서비스 - 다크웹 파일 공유 [파일 업로드 / 다운로드] 서비스 - 기타 다크웹 익명 서비스	14:00 – 14:50
	다크웹 정보 수집 / 분석 – 랜섬웨어 유형 [Ransomware] - 최신 랜섬웨어 동향 및 피해사례 - RaaS (Ransomware as a Service) 특징 이해 - 랜섬웨어 비트코인 요구 방식 이해 - AnChain.AI를 활용한 랜섬웨어 비트코인 거래 내역 추적 실습 - Criminal IP 인텔리전스 솔루션을 이용한 랜섬웨어 다크웹 실제 IP 탐색	15:00 – 15:50
	다크웹 정보 수집 / 분석 – 마약 / 블랙마켓 유형 [Drug Store] - 다크웹 상의 블랙마켓을 통한 거래 특징 - 다크웹 마약 거래 블랙 마켓 및 사이트 - 다크웹 마약 거래 검색 방법 - AnChain.AI를 활용한 마약 거래 관련 분석 실습 (마약거래 조직 및 SilkRoad 사례 분석)	16:00 – 16:50
	다크웹 정보 수집 / 분석 – 성착취물 [Sexual Abuse Material] - 다크웹 성착취물 거래 특징 - 다크웹 성착취물 거래 블랙 마켓 및 사이트 - 다크웹 성착취물 거래 검색 - AnChain.AI를 활용한 성착취물 거래 관련 가상화폐 주소 트랜잭션 분석	17:00 – 17:20
	다크웹 정보 수집 / 분석 – 위조, 무기, 테러, 기타 범죄 정보 - 다크웹 위조, 무기, 테러, 기타 범죄 정보 거래 특징 - 다크웹 위조, 무기, 테러, 기타 범죄 정보 거래 블랙 마켓 및 사이트 - 다크웹 위조, 무기, 테러, 기타 범죄 정보 거래 검색 - AnChain.AI를 활용한 무기, 테러 등 거래 관련 가상화폐 주소 트랜잭션 분석	17:20 – 17:40
	질문 & Review	18:00 ~

* 교육 시간 및 교육 내용은 사정에 따라 변동될 수 있으니 참고 바랍니다.

상담문의 : 02-851-5687

사이버 위협 인텔리전스

CTI & OSINT & 다크웹 정보 수집 / 분석 / 추적 / 모니터링 실무 과정 (4일)

교육일정	교육내용	교육시간
4일차	**다크웹 정보 수집 / 분석 – 기업정보 및 개인정보 유형** – 다크웹 기업정보 및 개인정보 거래 특징 – 유명 포럼을 통한 개인정보 거래 사례 – 기업 보안 담당자 입장에서의 대응 방안 – S2W Quaxar 다크웹 모니터링 솔루션을 이용한 기업정보 유출 모니터링 방법 설명	10:00 ~ 10:25
	사이버 위협 인텔리전스 도구 활용 방안 – 다크웹 인텔리전스 분석 도구 (S2W Quaxar) 주요 기능 설명 – 기업 정보 모니터링을 위한 Attack Surface Monitoring 기능 이해	10:25 ~ 10:50
	사이버 위협 인텔리전스 도구 활용 – 기업 정보 유출 사례 분석 – 다크웹 기업 핵심 자산 및 정보 유출 – 국내 기업 및 기관 피해 사례 [계정 정보, 이메일 정보, 재무 및 회계 정보 등] – 다크웹 기업 핵심 자산 및 정보 유출 – 국내 기업 및 기관 관련 검색	11:00 ~ 11:25
	사이버 위협 인텔리전스 도구 활용 – 기업 정보 유출 사례 분석 – 사이버 위협 인텔리전스 전문 도구 활용 및 사용법 실습 – S2W Quaxar를 활용한 주요 키워드 및 기업 도메인을 이용한 모니터링 방법	11:25 ~ 11:50
	사이버 위협 인텔리전스 도구 활용 – 기업 사칭(Brand Abuse) 사례 분석 – 기업 사칭 (Brand Abuse) 피해 사례 – 공격자들의 기업 사칭 패턴 이해 – S2W Quaxar를 활용한 기업 사칭 사례 분석 실습 – Phishing 및 Fake 웹 사이트 탐지	13:00 ~ 13:50
	사이버 위협 인텔리전스 도구 활용 – 랜섬웨어 피해 사이트 검색 – 랜섬웨어 범죄 조직 특징 이해 – S2W Quaxar를 활용한 국내 및 해외 기업 랜섬웨어 피해 사례 검색 실습 – 기업 보안 담당자 관점에서의 랜섬웨어 공격 모니터링 및 대응 방안	14:00 – 14:50
	사이버 위협 인텔리전스 도구 활용– 텔레그램 관련 범죄 [Tellegram] – 텔레그램 주요 특징 – 범죄 관련 텔레그램 정보 수집 및 분석 방법 – 텔레그램 관련 가상화폐 주소 트랜잭션 분석 – S2W Quaxar를 활용한 텔레그램 모니터링 실습 (Telegram Monitoring)	15:00 – 15:50
	사이버 위협 인텔리전스 도구 활용 – 해킹 그룹 / 각종 범죄자 검색 – 유명 해킹 그룹 및 범죄자 (Threat Actor)로 인한 국내 기업 피해 사례 – S2W Quaxar를 활용한 국내 기업 피해 사례 검색 실습 – Threat Actor 정보 수집을 통한 공격자 유형 파악	16:00 – 16:50
	선제적 대응을 위한 인텔리전스 정보 수집 – IoC 공격 패턴 활용 방법 – Threat Actor 정보 수집을 통한 공격자 유형 파악 – S2W Quaxar 인텔리전스 보고서 정보를 기반으로 한 악성코드/랜섬웨어 공격 대응	17:00 – 17:20
	선제적 대응을 위한 보안 솔루션 연계 방안 – SoC API 연동 방안 – SIEM API 연동 방안 – 각종 보안솔루션 API 연동 – 야라룰(Yara rules) 설정	17:20 – 17:40
	질문 & Review	18:00 ~

* 교육 시간 및 교육 내용은 사정에 따라 변동될 수 있으니 참고 바랍니다.

상담문의 : 02-851-5687

(주)인섹시큐리티 공인 교육센터

교육센터 지점별 안내 [서울 독산 / 제주 함덕] 바로가기

2023년도 교육일정 안내 바로가기

교육문의 : 02-851-5687

INSEC security