1 교육 커리큘럼

구분	과목명	대주제	소주제	강사명	교육 시수		
					계	이론	실습
공통과정	정보보호개론	정보보호 개요	• 정보보호 기본 개념, 3요소(CIA), 최신 사고·사례	이현호	2	2	0
		공격 및 방어 기법	• 네트워크, 웹, 시스템 공격의 이해 • 암호학 및 정보보호 장비에 대한 이해	이현호	2	2	0
		정보보호 법률	• 국내외 정보보호 관련 법률에 대한 이해	이현호	1	1	0
		직무 소개	• 보안관제 직무에 대한 소개 및 필요한 역량(이글루코퍼레이션 보안관제 센터 견학 및 직무소개 특강)	이규환	3	3	0
	시스템 보안	운영체제 기초	• 운영체제의 이해 • 윈도우 시스템, 리눅스 시스템의 이해	이현호	8	2	6
		시스템 공격 및 방어	• 취약점 및 Exploit의 이해 • 시스템 취약점 및 메모리 보호 기법	이현호	16	2	14
	네트워크 보안	네트워크 기초	• 네트워크 및 프로토콜의 이해 • TCP/IP 및 OSI 7 계층의 이해 • 네트워크 서비스의 이해	이현호	8	2	6
		네트워크 공격 및 방어	• 네트워크 스캐닝, 스니핑, 스푸핑 • 서비스거부공격 DoS(Denial of Service), DDoS(Distributed DoS)	이현호	16	2	14
	웹 보안	웹 기초	• 웹 개요 및 특징, 동작 방식 • 도메인 개요 및 체계, DNS(Domain Name Service), URL	이현호	8	2	6
		웹 공격 및 방어	• OWASP Top 10 취약점의 이해 • Client Side Attack(XSS, Session Fixation), Server Side Attack(SQL Injection, SSRF)	이현호	16	2	14
총 시수					80	20	60

AI보안관제 전문인력 양성교육

교육 커리큘럼

구분	과목명	대주제	소주제	강사명	교육 시수		
					계	이론	실습
실무과정	보안장비의 이해	침입차단시스템의 이해(F/W)	• 침입차단시스템의 구성 및 동작원리 • 침입차단시스템의 로그 분석/정책 관리	박종식	5	1	4
		침입탐지시스템의 이해(IDS/IPS)	• 침입탐지시스템의 구성 및 동작원리 • 침입탐지시스템의 로그 분석/정책 관리	박종식	5	1	4
		Snort 룰의 이해(Snort)	• Snort 룰의 정의 및 생성	황범석	5	1	4
		통합보안 시스템의 이해(SIEM/SOAR)	• 통합보안 시스템의 구성 및 동작원리 • 통합보안 시스템의 로그 검색 실습 • 통합보안 시스템의 탐지 정책 실습 • 통합보안 시스템의 경보이벤트 분석 실습 • 통합보안 시스템의 통계 생성 실습 • 공격유형별 시스템 운영 방안 실습	황범석	15	4	11
		네트워크 접근제어 시스템의 이해(NAC)	• 네트워크 접근제어 시스템의 구성 및 동작원리 • 네트워크 접근제어 시스템의 로그 분석/정책관리	박종식	5	1	4
	보안관제 실무	정보보호강화를 위한 보안관제 고도화 방안	• 사이버보안 트랜드 분석 및 보안전략 수립 시 고려사항 • 정보보호강화를 위한 보안관제 고도화 방안 • Introduction to Security Operations Center(SOC) • SOC Deployment Models와 Types에 따른 보안관제 역할	연준모	6	6	0
		통합보안관제시스템 운영방안	• 보안솔루션별 주요기능 및 운영 시 주의사항	연준모	6	2	4
		공격 시나리오 기반의 보안관제 고도화 방안	• 관제 이벤트 데이터 기반의 정오탐 판단 분석 훈련 시나리오	연준모	8	2	6
			• 관제 이벤트 데이터 기반의 정오탐 판단 분석 훈련 평가 및 개선	연준모	8	2	6
			• SOC Metrics과 SOC 고도화 방안	연준모	6	2	4
			• MITRE ATT&CK 기반의 SOC 구성요소 분석	연준모	7	3	4
			• SOC의 Event Monitoring과 Threat Hunting업무의 이해	김수영	6	2	4

AI보안관제 전문인력 양성교육

1 교육 커리큘럼

구분	과목명	대주제	소주제	강사명	교육 시수		
					계	이론	실습
실무과정	보안관제 실무	보안관제 운영시 침해사고 대응방안	• 침해사고 개요 및 필요성 • 침해사고 대응 준비 및 분석 절차 • 침해사고 유형별 분석방안 • 시나리오 기반 침해사고 대응 및 분석 훈련 • 침해사고 대응 평가 및 개선	김수영	8	5	3
		머신러닝 기반의 보안관제	• 기존의 보안관제 문제점	정일옥	2	2	0
			• 보안 데이터 수집하기 • 보안 데이터 분석하기(파이썬 등) • 보안 데이터에서 피처를 추출하기	정일옥	14	2	12
			• 보안에 적합한 알고리즘	정일옥	4	2	2
		생성형 AI를 이용한 보안관제	• 생성형 AI 개념 • 생성형 AI 활용하기 • 생성형 AI 를 활용한 보안관제 • 생성형 AI의 한계점	정일옥	10	2	8
총 시수					150	46	104