

사이버 보안 실무자

○ 훈련목적 및 목표

- 기업의 정보 자산을 보호하기 위해 필수적인 기술적 사이버 보안의 기초를 다지고, 실무에서 발생하는 보안 위협에 즉각적으로 대응할 수 있는 인력의 역량 강화
- 기술적 보안의 주요 취약점을 이해하고, 오픈소스를 활용하여 보안 점검 및 분석을 수행할 수 있는 기술적 역량 함양

○ 프로그램 내용 요약

- 본 과정은 사이버 보안의 기술적 토대를 구축하는 데 중점을 둔 40시간 프로그램으로, 교육은 기본적인 네트워크 통신 원리(OSI 7계층, TCP/IP)에서 시작하여, 실제 데이터 패킷을 Wireshark로 분석하는 실습 진행
- 이후 서버(Windows, Linux)의 보안을 강화하는 하드닝(Hardening) 기술, 계정 관리, 로그 분석 방법을 학습하며, OWASP Top 10을 중심으로 한 웹 애플리케이션의 주요 취약점을 이해하고, OWASP ZAP과 같은 자동화 도구를 사용해 직접 취약점을 스캔하고 분석하는 실무 능력을 배양하고,
- 마지막으로 악성코드 분석의 기초와 침해사고 대응 절차를 학습하고, 가상의 랜섬웨어 감염 시나리오에 대한 원인 분석 및 대응 방안 보고서를 작성하는 종합평가를 통해 모든 기술을 통합적으로 적용하는 능력을 검증

○ 프로그램(모듈) 시간표

모듈명	세부내용	훈련시간
정보보호 개론 및 보안 법규	- 정보보호 3대 목표 (기밀성, 무결성, 가용성) - 최신 사이버 위협 동향 (랜섬웨어, APT, 공급망 공격 등) - 개인정보보호법 및 정보통신망법의 이해 - 비즈니스 환경에서의 컴플라이언스 준수 요건 [평가] 최신 보안 침해 사고 사례 분석	5
네트워크 통신과 프로토콜 보안	- OSI 7계층 모델과 TCP/IP 4계층 구조 이해 - 데이터 캡슐화 및 통신 과정 시뮬레이션 - HTTP/HTTPS, DNS, DHCP 프로토콜의 동작 원리 - 프로토콜 취약점을 이용한 공격 기법 이해 [평가] Wireshark를 활용한 HTTP/DNS 패킷 캡처 및 트래픽 분석	5
네트워크 보안 장비 활용	- 방화벽(Firewall), IDS/IPS, WAF, VPN의 역할과 기능 - 접근 제어 리스트(ACL) 설정 및 트래픽 제어 - 네트워크 보안 아키텍처 구성 사례 분석 [평가] 방화벽(Firewall) 인바운드/아웃바운드 보안 정책 설정	5
서버 운영체제(OS) 보안	- 서버 OS별 파일 시스템 및 계정 구조 - 불필요한 서비스 및 포트 비활성화 - 중요 파일/디렉토리 접근 권한(Permission) 설정 실습 [평가] 리눅스/윈도우 서버 보안 취약점 점검 및 조치	5
시스템 계정 관리 및 로그 분석	- 관리자/사용자 권한 분리 및 강력한 암호 정책 수립 - 시스템 이벤트 로그(Win) 및 Syslog(Linux) 구조 이해 - 로그 분석을 통한 비정상 행위 탐지 실습 [평가] Brute-Force 공격 시도 탐지 시스템 로그 분석	5
웹 인젝션 공격 및 인증 취약점 진단	- 웹 서비스 구조와 클라이언트-서버 통신 - Injection(SQL, Command) 공격 원리 및 실습 - 인증 및 세션 관리 취약점 분석 [평가] DVWA 활용 SQL Injection 공격 시연 및 방어 코드 적용	5
XSS/CSRF 취약 점 대응 및 시큐 어코딩	- XSS(Cross Site Scripting), CSRF 공격 및 대응 - 보안 설정 오류 및 민감 데이터 노출 사례 - 자동화 도구를 활용한 취약점 스캔 - 입력값 검증 등 시큐어코딩 적용 방안 [평가] Reflected XSS 취약점 공격 및 스크립트 필터링 적용	5
악성코드 분석 및 침해사고 대응	- 악성코드 유형(랜섬웨어, 트로이목마 등) 및 감염 경로 - 이메일 피싱 공격 식별 및 예방 훈련 - 사고 탐지 → 초기 대응 → 분석 → 복구 → 사후 조치 단계별 절차 - 침해사고 대응 모의 시나리오 워크숍 [평가] 피싱 메일 헤더 분석 및 악성 첨부파일 식별	5

ISMS 기반 정보보호 관리 실무자

○ 훈련목적 및 목표

- 단편적인 기술 대응을 넘어, 조직의 정보보호 및 개인정보보호 관리체계(ISMS-P)를 수립, 운영, 개선할 수 있는 전문 관리자로서의 역량 강화
- ISMS-P 인증 기준을 이해하고, 위험관리 방법론에 따라 조직의 정보 자산을 보호하기 위한 체계적인 정책과 절차를 수립할 수 있는 관리적 역량을 함양

○ 프로그램 내용 요약

- 본 과정은 기술적 보안을 넘어 조직의 정보보호 관리체계를 수립하고 운영하는 관리자 양성을 위한 40시간 전문 프로그램으로, 정보보호위원회를 구성하고 CISO/CPO를 지정하는 등 경영진의 참여를 확보하고 ISMS-P 인증 범위를 설정하는 '관리체계 기반 마련'부터 시작하여 조직의 모든 정보 자산을 식별하고, 자산-위험-취약점 기반의 정성적/정량적 '위험 평가'를 수행하여 보호 우선순위를 결정하는 핵심적인 위험관리 활동을 학습함
- 평가된 위험을 처리하기 위해 ISMS-P 인증 기준에 명시된 100여 개의 '보호대책 요구사항'을 인적, 물리, 기술적 영역에 걸쳐 구체적으로 학습하고 적용하는 방법을 익히며 특히, 개인정보보호법 준수를 위한 '개인정보 생명주기 관리'를 별도 모듈로 심도 있게 다루고 있음
- 마지막으로 실제적인 시나리오 기반의 모의 훈련을 통해, 침해사고 발생 시 수립된 관리체계가 어떻게 동작하는지 점검하고, 경영진에게 개선 방안을 보고하는 종합적인 실전 역량을 완성하고자 함

○ 프로그램(모듈) 시간표

모듈명	세부내용	훈련시간
관리체계 기반 및 거버넌스 수립	- ISMS-P 인증 제도의 이해 및 인증 의무 대상 - 경영진의 책임과 역할, 의사결정 체계 수립 - 정보보호 최고책임자(CISO/CPO) 지정 및 실무 조직 구성 [평가] 우리 조직에 맞는 정보보호 조직도 설계 및 R&R 정의서 작성	5
정책 수립 및 범위 설정	- 인증 범위(서비스, 자산, 조직, 물리적 위치) 식별 및 경계 설정 - 최상위 정책서 및 분야별 지침 수립 방법론 - 예산 및 인력 등 자원 할당 계획 수립 [평가] 정보보호 관리체계 인증 범위 설정 및 네트워크 경계 도출	5
정보자산 식별 및 관리	- 정보시스템, 데이터, 인력 등 자산 목록화 - 기밀성/무결성/가용성(CIA) 기반 자산 가치 평가 - 자산 분류 및 등급 산정 실습 [평가] 주요 정보자산 목록 작성 및 중요도 평가(CIA) 수행	5
위험관리	- 베이스라인법, 상세위험분석법 등 평가 기법 이해 - 위험 및 취약점 식별 실습 - DoA(수용가능 위험수준) 산정 및 위험 처리 전략(회피, 전가, 감소, 수용) - 정보보호 대책 명세서 작성 [평가] 위험 시나리오 작성 및 위험도 산정/조치 계획 수립	5
관리체계 운영 및 사후관리	- 보호대책 이행 및 운영 명세서 관리 - 법적 요구사항 준수 검토 프로세스 - 내부 감사 계획 수립 및 체크리스트 작성 - 결함 사항에 대한 시정 조치 및 경영진 보고 [평가] 내부 감사 체크리스트 개발 및 결함 보고서(NCR) 작성	5
물리 및 인적 보안 통제	- 보호구역(통제/제한/접견) 지정 및 출입 통제 절차 - 정보시스템 설비 보호 및 반출입 관리 - 입사/재직/퇴사 단계별 보안 서약 및 관리 절차 - 정보보호 교육 훈련 계획 및 시행 [평가] 물리적 보호구역 지정 및 출입통제 절차서 작성	5
기술적 접근통제 및 인증	- 네트워크, 서버, 응용프로그램 접근 권한 관리 - 특수 계정 및 원격 접근 통제 강화 방안 - 사용자 식별 및 인증(MFA 등) 적용 - 비밀번호 작성 규칙 및 주기적 변경 관리 [평가] 서버/시스템 접근제어 정책 수립 및 계정 권한 검토 리포트 작성	5
개발 보안 및 개인정보 생명주기	- 보안 요구사항 정의 및 시큐어코딩 적용 - 변경 관리 및 시스템 운영(백업, 장애 대응) 절차 - 수집/이용/제공/파기 단계별 법적 조치 사항 - 정보주체 권리 보장 및 개인정보 흐름표 작성 [평가] 개인정보 흐름표(Data Flow Chart) 작성 및 흐름 분석	5

AI 기반 지능형 위협 헌팅 및 제로트러스트 전문가

○ 훈련목적 및 목표

- AI 및 머신러닝 기술을 활용하여 고도화된 사이버 위협을 탐지하고 대응하는 전문 역량을 함양한다.
- 제로트러스트(Zero Trust) 보안 모델을 이해하고 실무 환경에 적용하여 보안 아키텍처를 고도화할 수 있다.
- 침해사고 발생 시 포렌식, 로그 분석, 위협 인텔리전스(CTI)를 활용하여 원인을 규명하고 재발 방지 대책을 수립한다.

○ 프로그램 내용 요약

- 본 과정은 제로트러스트 아키텍처의 핵심인 사용자 및 기기 인증, 접근 통제 정책 수립 방법을 학습하며, 네트워크 상에서 발생하는 정상 및 비정상 트래픽을 정밀하게 식별하고 분석하는 기초 체력을 다지고자 함
- 또한, 날로 지능화되는 사이버 공격에 대응하기 위해 인공지능(AI)과 머신러닝 기술을 보안에 접목하는 방법을 심도 있게 다루며, 머신러닝 알고리즘을 활용한 악성코드 탐지 모델링, ELK 스택을 활용한 대용량 로그 데이터 분석 및 시각화, 자동화된 대응(SOAR) 프로세스 설계 등의 학습을 통해 수동적인 보안 업무에서 벗어나 데이터 기반의 능동적인 위협 헌팅을 수행할 수 있는 역량을 갖추게 됨
- 나아가 클라우드 네이티브 환경(Docker, Kubernetes), 웹 애플리케이션의 최신 취약점(OWASP Top 10) 진단 및 대응 기술, 사이버 위협 인텔리전스(CTI)를 활용한 공격 그룹(APT) 프로파일링 등을 통해 단순한 기술 습득을 넘어 복합적인 보안 위협 상황에서 주도적으로 문제를 해결하고 협업할 수 있는 역량을 강화할 수 있음

○ 프로그램(모듈) 시간표

모듈명	세부내용	훈련시간
최신 보안 트렌드와 제로트러스트 아키텍처	- 전통적 경계 보안의 한계와 제로트러스트(ZTA) 도입 전략 - AI/ML을 활용한 사이버 보안 동향 및 공격/방어 사례 [평가] 제로트러스트 정책 수립 및 접근 통제 시나리오 설계	5
심층 패킷 분석 및 네트워크 포렌식	- Wireshark/Tcpdump 활용 고급 패킷 분석 - 비정상 트래픽 식별 및 프로토콜(HTTP/2, QUIC 등) 분석 [평가] 실제 공격 패킷(PCAP) 분석을 통한 공격 경로 역추적	5
AI 활용 악성코드 탐지 및 분석	- 머신러닝 기반의 이상 징후 탐지 모델 이해 - 샌드박스 환경 구축 및 자동화 분석 도구 활용 [평가] 오픈소스 AI 도구를 활용한 악성 파일 분류 및 분석	5
웹/애플리케이션 취약점 심화 대응	- OWASP Top 10(API Security 포함) 심층 분석 - 시큐어 코딩 및 소스코드 진단 자동화 [평가] Burp Suite Pro 활용 모의해킹 및 API 취약점 진단	5
로그 데이터 분석 및 ELK 스택 활용	- 대용량 보안 로그의 통합 및 상관관계 분석 기법 - ELK(Elasticsearch, Logstash, Kibana) 스택 구축 및 시각화 [평가] 보안 관제 대시보드 구축 및 위협 탐지 룰(Rule) 제작	5
클라우드 네이티브 보안 및 컨테이너 위협 대응	- Docker/Kubernetes 환경의 보안 위협 및 대응 방안 - 클라우드 워크로드 보호 플랫폼(CWPP) 이해 [평가] 컨테이너 취약점 점검 및 침해사고 대응 훈련	5
사이버 위협 인텔리전스(CTI) 활용	- 사이버 위협 인텔리전스(CTI) 플랫폼 활용 및 공유 체계 - MITRE ATT&CK 프레임워크 기반 공격 전술 분석 [평가] CTI 정보를 활용한 공격 그룹(APT) 프로파일링	5
AI 기반 침해사고 대응 시나리오	- 랜섬웨어/APT 공격 시나리오 기반 팀 프로젝트 - AI 자동 대응(SOAR) 프로세스 설계 및 모의 훈련 [평가] 팀별 대응 보고서 작성 및 발표 (강사 피드백 포함)	5

클라우드 보안 컴플라이언스(CSAP/ISMS-P) 전문가

○ 훈련목적 및 목표

- 클라우드 환경에서의 보안 컴플라이언스(CSAP, ISMS-P) 요구사항을 이해하고 실무에 적용하는 능력을 배양한다.
- 클라우드 인프라의 기술적 취약점을 진단하고 조치하여 안전한 클라우드 운영 환경을 구축한다.
- 모의 감사 및 컨설팅 실무를 통해 보안 거버넌스 수립 및 리스크 관리 전문가를 양성한다.

○ 프로그램 내용 요약

- 본 과정은 급변하는 클라우드 규제 환경에 발맞춰 기업이 필수적으로 준수해야 할 보안 거버넌스와 컴플라이언스를 체계적으로 학습하는 과정으로, 개인정보보호법, 정보통신망법 등 최신 정보보호 관련 법규를 이해하고, 국내 클라우드 보안인증(CSAP) 및 정보보호 관리체계(ISMS-P) 인증 기준 심층 분석을 통해 기업의 상황에 맞는 보안 정책을 수립하고, 법적 리스크를 최소화할 수 있는 관리적 보안 역량을 강화하고자 함
- 단순한 법규 이해를 넘어, 실제 클라우드 인프라(AWS 등) 환경에서의 기술적 진단 실습을 병행하여 이론과 실무의 균형을 맞추고 있으며, 클라우드 계정 관리(IAM), 가상 네트워크(VPC) 설정, 스토리지 암호화 및 로깅 등 핵심 인프라 요소에 대한 보안 설정 방법을 학습하고, CSPM(클라우드 보안 형상 관리) 도구를 활용하여 취약점을 자동으로 탐지하고 조치하는 기술적 역량을 함양할 수 있음

○ 프로그램(모듈) 시간표

모듈명	세부내용	훈련시간
클라우드 보안 거버넌스 및 최신 법규	- 클라우드 책임 공유 모델 및 보안 거버넌스 수립 - 개보법, 정통망법 등 최신 개정 법령 상세 해설 [평가] 클라우드 도입 시 보안성 검토 체크리스트 작성	5
CSAP(클라우드 보안인증) 실무 가이드	- 공공/민간 클라우드 보안 인증 기준(SaaS, IaaS) 상세 분석 - 클라우드 서비스 유형별 인증 준비 절차 [평가] 가상 SaaS 서비스 대상 CSAP 인증 결함 보고서 작성	5
ISMS-P 인증 심화: 개인정보 라이프사이클	- 수집/이용/제공/파기 단계별 법적 준거성 점검 - 가명정보 처리 및 데이터 결합 시 보안 조치 [평가] 개인정보 흐름도(Data Flow Chart) 작성 및 위험 식별	5
클라우드 계정 (IAM) 및 네트워 크 보안 설정	- 정책과 기술의 연계: IAM(계정), VPC(네트워크) 설정 - 클라우드 보안 설정 진단 도구(CSPM) 활용 [평가] AWS 환경 보안 설정 취약점 진단 및 조치 실습	5
클라우드 데이터 암호화 및 로그 모니터링	- 스토리지(S3 등) 보안, 로깅 및 모니터링, 암호화 키 관리(KMS) - 서버리스(Serverless) 컴퓨팅 보안 [평가] 침해사고 발생 시 클라우드 로그 분석 및 증거 확보	5
공급망 보안 및 제3자 리스크 관리(TPRM)	- 소프트웨어 공급망 보안(SBOM) 및 오픈소스 리스크 관리 - 외부 협력업체 보안 평가 및 계약 시 보안 요구사항 [평가] 협력사 보안 실태 평가표 작성 및 개선 조치 요구	5
모의 감사(Audit) 및 결함 보고서 작성	- 인증 심사원 관점의 결함 도출 기법 및 인터뷰 스킬 - 증적 자료 검토 방법 및 보완 조치 확인 절차 [평가] 실제 감사 상황 롤플레잉(심사원 vs 피심사자)	5
차세대 보안 컨설팅 실무	- 가상의 중견기업 대상 ISMS-P 및 클라우드 보안 컨설팅 수행 - 위험평가 보고서 및 정보보호 대책 명세서 완성 [평가] 컨설팅 결과물 발표 및 현직 심사원 멘토링	5