**모집 분야별 운영계획서**

**1. SNIPER2팀**

|  |  |
| --- | --- |
| 직무명 | IPS 제품 개발 및 시험 |
| 교육목표 | \* 네트워크 보안 기술에 대한 이해\* 네트워크 프로토콜에 분석 능력\* DevOps CI/CD 에 대한 전반적인 지식 |
| 직무개요 | \* 네트워크 취약점 조사 및 분석을 통해 그에 대한 방어 방법을 강구하고 탐지 모듈을 개발한다.\* 네트워크 보안 제품에 대한 이해를 통해 보안 위협을 방어하는 방법을 습득한다.\* 주요 프로토콜과 네트워크 장비에 대한 학습을 통해 네트워크 보안 제품에 대한 기능검증 방법을 습득한다.\* DevOps 기반의 CI/CD 에 대한 지식과 자동화 테스트 모듈을 개발한다. |
| 운영 및 지도계획 | \* 1주차 : 오리엔테이션, 입사서류 작성 및 회사 소개, PC 셋팅\* 2주차 : 자사 보안 제품 및 네트워크 관련 교육\* 3주차~8주차 :- 네트워크 보안 기술, 프로토콜에 대한 분석 및 교육- 테스트 자동화 케이스 개발\* 9주차 : DevOps 구성 관련 교육 및 실습\* 10주차~14주차 : - 네트워크 기반 취약점 탐지 방법 연구- CI/CD 구성요소 개발\* 15주차~22주차 : 네트워크 기반 취약점 탐지 모듈 개발 교육 및 실습\* 23주차~27주차 : 네트워크 프로토콜 및 서비스 분석 결과 정리 |

**2. 서비스개발팀**

|  |  |
| --- | --- |
| 직무명 | 솔루션 개발 |
| 교육목표 | \* SNIPER BD1 솔루션 구조, 동작 이해\* SNIPER BD1 웹 GUI 구조, 동작 이해\* SNIPER BD1 검색 기능 통한 빅데이터 분석 이해 |
| 직무개요 | \* AI 보안 관제 솔루션을 이해하고, 개발에 필요한 WEB기술 및 빅데이터 기술에 대한 실무 업무 및 테스트 모듈 개발을 진행함. (Jest, playwrite, Junit, python 등) |
| 운영 및 지도계획 | \* 1주차 : 오리엔테이션, 입사서류 작성 및 회사소개, PC 세팅 \* 2주차~4주차 : SNIPER BD1 솔루션 및 웹/엔진 개념 이해 \* 5주차~7주차 : SNIPER BD1 기능 테스트 시나리오 개발\* 8주차~10주차 : SNIPER BD1 설정 변경 테스트 시나리오 개발\* 11주차~13주차 : SNIPER BD1 빅데이터 검색 기능 테스트 시나리오 개발 \* 14주차~16주차 : SNIPER BD1 테스트 결과 저장 및 가시화\* 17주차~19주차 : SNIPER BD1 기술 문서 작성 및 리뷰\* 20주차~27주차 : SNIPER BD1 테스트 시나리오에 대한 로그, 예외 처리 추가 개발 |

**3. 품질보증팀**

|  |  |
| --- | --- |
| 직무명 | 품질보증 |
| 교육목표 | \* 네트워크 환경 구성 기본 지식 습득\* 네트워크 트래픽 분석 도구 사용법 습득\* 침입탐지/방어시스템, 방화벽, 통합보안관리제품 등 네트워크 보안 지식 습득\* 패킷 분석 기본 지식 습득\* 소프트웨어 테스트 방법론 및 실무 경험\* 소프트웨어 테스트를 위한 테스트케이스 설계 및 실행 경험 |
| 직무개요 | \* 네트워크 보안 장비 기능의 정상성 확인을 위해 시험망 구성 및 장비 세팅 후 공격 트래픽 발생 후 정상탐지, 차단 동작 확인\* 네트워크 보안 장비의 테스트를 위한 테스트케이스 설계 및 실행 |
| 운영 및 지도계획 | \* 1주차 : 오리엔테이션, PC세팅, 직무 기본 교육 및 목표 설명\* 2주차 : 네트워크 보안 개요 교육\* 3주차 : 네트워크 보안 제품 매뉴얼을 통한 기본 숙지\* 4주차 : 네트워크 보안 제품 시험망 구성 실습\* 5주차 : 테스트케이스 설계 및 실행 실습\* 6주차 : 품질관리 프로세스 교육, 테스트케이스 리뷰 교육\* 7주차~9주차 : 네트워크 보안 제품 테스트 실무 투입\* 10주차 : 품질관리 프로세스 교육, 테스트케이스 리뷰 교육\* 11주차~13주차 : 네트워크 보안 제품 테스트 실무 투입\* 14주차 : 품질관리 프로세스 교육, 테스트케이스 리뷰 교육\* 15주차~17주차 : 네트워크 보안 제품 테스트 실무 투입\* 18주차 : 품질관리 프로세스 교육, 테스트케이스 리뷰 교육\* 19주차~21주차 : 네트워크 보안 제품 테스트 실무 투입\* 22주차 : 품질관리 프로세스 교육, 테스트케이스 리뷰 교육\* 23주~27주 : 네트워크 보안 제품 테스트 실무 투입 |

**4. 분석팀**

|  |  |
| --- | --- |
| 직무명 | 취약점 및 악성코드 분석 |
| 교육목표 | \* 취약점- 취약점 환경 Docker 구축 및 PoC 기반 공격 실습- 취약점 Wireshark 기반 분석- 취약점 패턴 개발 (Snort) 및 보고서 작성\* 악성코드- 악성코드 분석 툴을 활용한 어셈블리 분석- 악성코드 패턴 개발 (Yara) 및 보고서 작성 |
| 직무개요 | \*정보보안 기술 연구\*취약점 분석\*어플리케이션 취약점 및 서비스 분석 |
| 운영 및 지도계획 | \* 1주차: 오리엔테이션, 입사서류 작성 및 회사소개, PC 세팅 \* 2주차 ~ 4주차: Snort 및 어셈블리 언어 스터디 및 발표\* 5주차: 취약점 환경 구성 및 취약점 환경 Docker 구축 및 PoC 공격 실습\* 6주차: 취약점 Wireshark 분석 및 취약점 패턴 개발 (Snort) 및 보고서 작성\* 7주차: 악성코드 분석 툴을 활용한 어셈블리 분석\* 8주차: 악성코드 패턴 개발 (Yara) 및 보고서 작성\* 9주차: 패턴 릴리즈 SCA 등록 교육\* 10주차~27주차: 자사 취약점 및 악성코드 패턴 개발 (지속)- 9주차~13주차: 취약점 분석 및 보고서 작성- 14주차~18주차: 악성코드 분석 및 보고서 작성- 19주차~23주차: 취약점 분석 및 보고서 작성- 24주차~27주차: 악성코드 분석 및 보고서 작성 |

**5. TS실**

|  |  |
| --- | --- |
| 직무명 | 기술 협력사 기술 문의 대응 |
| 교육목표 | \* ONE-i/d 이론/실습을 통한 주요기능의 이해\* ONE-i/d 기본적인 설치/패치/HW교체 방법 숙지\* ONE-i/d (기초)기술문의 대응 |
| 직무개요 | \* ONE-i/d 기술협력사 기술문의 대응- 인증서갱신, 패턴업데이트, 기능문의 대응- 기본적인 설치/패치/HW교체 문의 대응 |
| 운영 및 지도계획 | \* 1주차 : 업무환경준비, 조직구성소개\* 2주차~4주차 : ONE-i/d 제품 교육\* 5주차 : 인증서, 패턴업데이트 요청 건 처리방법 교육/TSS처리\* 6주차~8주차 : HW 교체방법 교육, 교체절차서 보완\* 9주차 : HW 교체 요청 건 대응방법 교육/TSS처리\* 10주차~13주차 : TSS-FAQ 기능부분 테스트, 내용보완\* 14주차~16주차 : 기능동작 문의 건 대응방법 교육/TSS처리\* 17주차~19주차 : OS, Engine 패치 교육/TSS처리\* 20주차~27주차 : HW, SW 장애 문의 건 대응방법 교육/TSS처리 |