

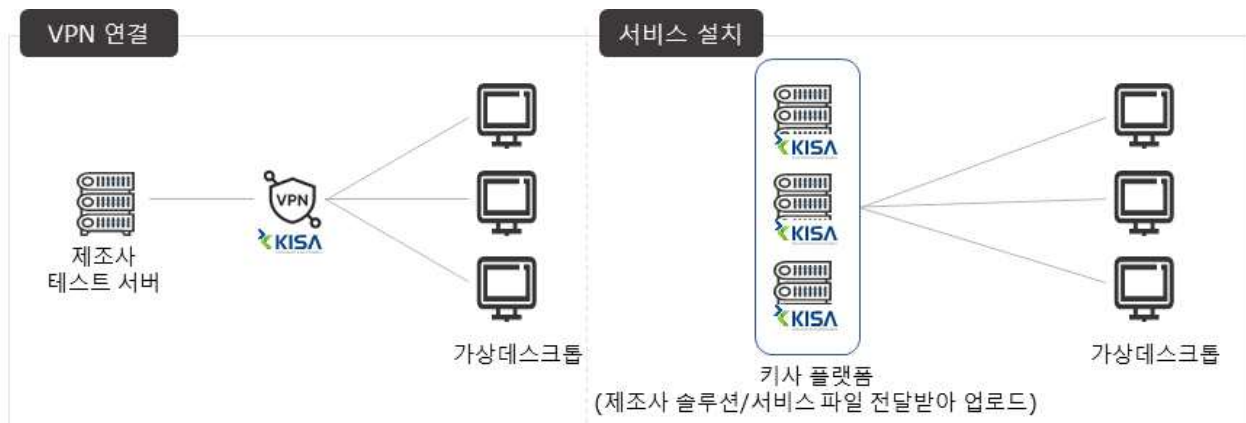
1 담당자 역할

가. 제조사 담당자

- 제조사는 아래와 같은 담당 업무를 맡아 버그바운티 진행

구분	담당업무	비고
1	버그바운티 환경 구축 방법 결정	VPN 연동 / 해더챌린지 플랫폼 업로드 중 선택
2	VPN 연동 시 세부 정보 제공	제조사에서 접속 방식, 계정 정보, 포트 등 정보 전달
3	해더챌린지 플랫폼 업로드 시 환경 이전 협조	제조사에서 분석 플랫폼 내 기업 서비스 설치 ※ KISA에서 일부 기술 지원
4	해더챌린지 플랫폼 VDI에 테스트 계정으로 접속하여 자사 솔루션/서비스 환경구축 확인	KISA에서 VPN 및 VDI 테스트 계정 제공
5	신고된 취약점 및 평가 내역 확인 및 의견 제출	KISA에서 평가 내역 및 취약점 정보 제공
6	보안패치 컨설팅 및 시상식 참여	KISA에서 보안 컨설팅 및 시상식 진행(감사패 전달)

2 버그바운티 환경 구축 방식 선택



- VPN 연결 설치 장점

1. 제조사에서 기존에 테스트 서버를 보유하고 있거나 구축 가능한 경우, 별도의 솔루션 파일 제공 없이 제조사 테스트 서버 그대로 사용 가능
(단, 자체 VPN 사용 시 설치 방법 접속 가이드 등 지원 필요)
2. 해더챌린지 플랫폼과 VPN으로 연결하여, 솔루션/서비스 파일 KISA측에 전달 불필요
3. 제조사 쪽에서 접속 제어 용이 (접속 제한 등 설정 편이)

- 키사 플랫폼 서비스 설치 장점

1. 버그바운티 대상 파일 해더챌린지 플랫폼에 업로드(일부 기사에서 지원 가능)
2. 해더챌린지 플랫폼으로 업로드 시, 화이트해커는 플랫폼 접속 후 **내부 자료 외부 반출 차단 기능**으로 인해 소스코드 등의 정보 유출이 근본적으로 차단되어 안전한 환경에서 진행 가능

가. VPN을 통해 진행하는 경우

① VPN 연동 방법 선택

- 방법 1 : 제조사 IPsec VPN ↔ 해더챌린지 플랫폼 IPsec VPN 연결
- 방법 2 : 제조사 SSL VPN ↔ 해더챌린지 플랫폼 VDI 연결
- 방법 3 : 제조사에서 VPN이 없는 경우 KISA에서 Openvpn 설치 지원하여 연결
- 방법 4 : 방화벽만 열어서 접근

※ 방법 2의 통신정책(외부에 대한 통신 허용 등)은 서버 쪽에서 설정 가능

구분	IPsec VPN	SSL VPN
보안 방식	네트워크 계층(Layer 3) 암호화	전송 계층(Layer 4)~애플리케이션 계층(Layer 7) 암호화
연결방식	특정 네트워크(IP 주소)를 통해 연결	VDI에 터널링
설치 필요 여부	VPN 클라이언트(소프트웨어) 필요	웹 브라우저, VPN 클라이언트(소프트웨어) 등으로 접근 가능
성능	속도가 빠르고 대량 트래픽 처리 가능	보안은 강하지만 속도는 다소 느릴 수 있음

※ VPN 연결 시 필요한 정보

- 자료 1 : 솔루션 접속 클라이언트 파일
- 자료 2 : Config 정보(IP, Port 정보 등 네트워크 관련 정보)
- 자료 3 : 로그인 방식(아이디 패스워드 접속 방식 등)
- 자료 4 : 로그인 계정 생성 방식

② VPN 연동 시 제조사/KISA 담당자 협의사항

- 방법 1,2의 경우 제조사는 위의 'VPN 연결 시 필요한 기본 정보'를 KISA에 전달, KISA는 해당 정보를 수신 후 플랫폼 담당자가 VPN 연결 및 테스트 진행
- 방법 3과 같이 제조사에서 VPN이 없는 경우 플랫폼 담당자가 제조사 측에 OpenVPN 전달 및 기술적 지원

나. 해더챌린지 플랫폼에 제조사 솔루션/서비스를 올리는 경우

- ① 제조사에서 받은 솔루션/서비스 코드를 받아 핵더챌린지 플랫폼 환경으로 이전
 - 방법 1 : 제조사 내에서 AWS에 구축해놓은 서비스/솔루션을 핵더챌린지 플랫폼 (NCP 환경)에 이전하는 경우
 - 방법 2 : 온프레미스(물리 서버) 환경에서 핵더챌린지 플랫폼으로 이전하는 경우
 - 제조사가 Tomcat, Apache, MySQL 등으로 운영하는 경우

② 제조사 솔루션/서비스 이전 시 제조사/KISA 담당자 협의사항

- 방법 1의 경우 제조사에서 서비스/솔루션 패키지(Docker 이미지, JAR/WAR 파일 등), 환경 설정파일, 네트워크 설정 정보(포트 정보 등) 제공 및 구축
 - 방법 2의 경우 클라우드에서 표준화된 정보와 맞추기 위해 서버 인프라 및 어플리케이션 구성 정보(Tomcat 설치 경로, 주요 설정 파일, Docker 이미지, JAR/WAR 파일 등) 플랫폼 이전을 통한 정보 제공 및 설치 지원 필요
- ※ 설치 시 일부 KISA 기술적 지원 가능

다. 제조사에서 VPN – VDI 접속 후 테스트 계정을 통해 보안솔루션/서비스 환경 구축 확인

- ① KISA에서 제조사 측이 환경 구축 확인을 하실 수 있도록 VPN, VDI 접속 가이드 및 테스트 계정 제공
- ② 테스트 계정을 통해 정상적으로 솔루션/서비스가 작동하는지 확인 필요

라. 최종 확인 후 핵더챌린지 플랫폼에서 분석환경 구축을 위해 필요 시 VDI 다중 인스턴스 생성 진행

- ① 플랫폼 담당자는 정상적으로 동작하는지 확인 후 분석가 환경 구성을 위해서 다중 인스턴스 생성