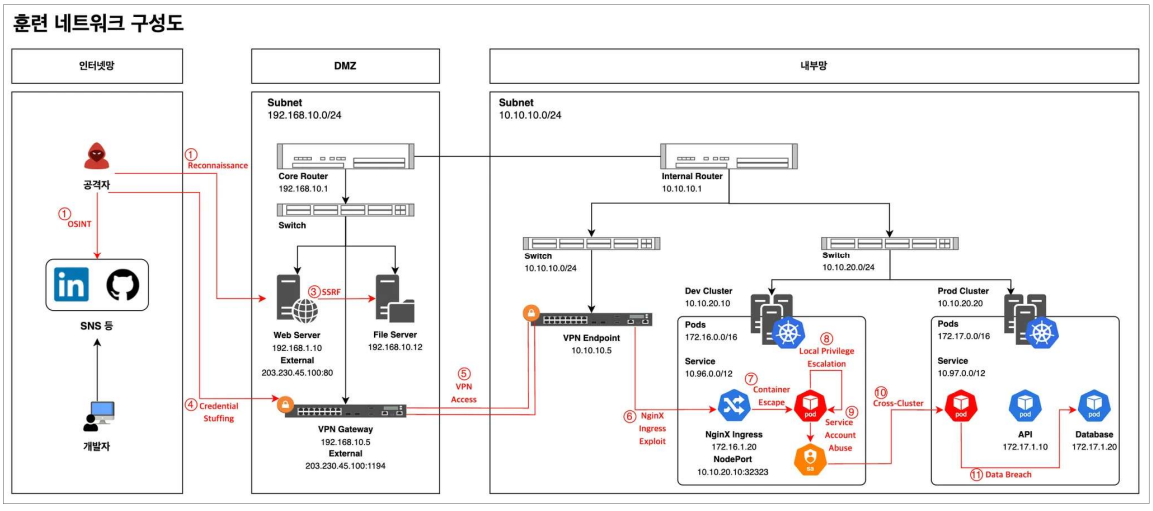
<붙임 2> 시나리오 제출양식

시나리오 제목
클라우드 네이티브 환경 침투 및 방어
시나리오 단계
7
시나리오 목적
OSINT 정보 수집, 웹 취약점 공격, VPN 침투, 컨테이너 탈출, 권한 상승 및 클라우드 네이티브(Kubernetes) 환경 침투 및 방어 훈련
시나리오 줄거리
공격자는 OSINT를 통해 타겟 기업의 정보를 수집하고, LinkedIn과 GitHub에서 개발자 계정 정보를 획득한다. 네트워크 스캔으로 발견한 홈페이지의 Next.js SSRF 취약점을 악용하여 DMZ 내부 서버에서 VPN 설정 파일을 탈취한다. 획득한 VPN 설정과 계정 정보로 크레덴셜 스터핑 공격을 수행하여 내부망에 침투한 후, 네트워크 스캔을 통해 개발 및 운영 Kubernetes 클러스터를 발견한다. 개발 클러스터에서 취약한 버전의 NGINX Ingress Controller를 확인하고, 취약점을 악용하여 컨테이너를 장악한다. Docker Socket 노출과 Privileged 권한 설정 오류를 이용해 컨테이너에서 호스트(Worker Node)로 탈출한다. 호스트에서 sudo 설정 오류를 발견하여 권한 상승을 통해 root 권한을 획득한다. 설치된 kubectl과 과도하게 부여된 ServiceAccount 권한을 확인하여 운영 클러스터로 수평 이동한 후, 데이터베이스에서 개인정보를 탈취한다.
시나리오 네트워크 구성도
- 전체 망 구성은 Openstack 또는 클라우드를 통해 구현 가능하도록 설계하였음 - 사용되는 전체 구성은 오픈소스를 활용하여 저작권 문제가 없도록 하였음 

단계 번호		1
단계 명		OSINT 및 네트워크 스캔
주요 목표		공개 자료 및 네트워크 스캔을 통한 계정, 기술 스택 및 외부 자산 식별
유형	**공격**	정찰
	방어	탐지, 대응
주요 활동		[공격] ○ LinkedIn, Github 등 검색을 통한 계정, 기술 정보 수집 ○ Shodan, Google Dorking을 통한 노출 정보 검색 ○ 서브 도메인 수집 ○ 네트워크 스캔(Nmap)을 통한 외부 노출 자산 식별 [방어] ○ 외부 노출 정보 정기 점검 수행 및 삭제
주요 사용 도구 및 기술		Google Dorking, Subfinder, Nmap
예상 결과물 및 상태		○ 계정 수집 정보 (계정 목록) ○ 기술 스택 파악 정보 (Kubernetes 사용 등) ○ 서브 도메인 및 네트워크 스캔 정보 (외부 홈페이지 및 버젼 정보, VPN 게이트웨이 주소)

단계 번호		2
단계 명		SSRF 취약점을 통한 내부 서버 접근
주요 목표		Next.js SSRF 취약점 식별 및 악용으로 DMZ 내 서버 접근 후 VPN 설정 파일 탈취
유형	**공격**	취약점 악용
	방어	탐지, 대응
주요 활동		[공격] ○ 공개된 Next.js SSRF 취약점(CVE-2024-34351) 존재 확인 ○ SSRF 취약점 공격 및 취약점을 통한 DMZ 내부 스캔 ○ 내부 서버 식별 및 접근 후 VPN 설정 파일 탈취 [방어] ○ SSRF 공격 시도 탐지 또는 비정상 응답 증가 탐지 ○ 취약한 Next.js 버전 업데이트 ○ VPN 설정 파일 서버 접근 대역을 내부망으로 수정 *※ 방어 시나리오 사용 시 DMZ 대역 WAF 및 서버 내 로그 수집기 추가 (Promtail+Loki, Wazuh Agent: 수집 -> Grafana: 시각화, Wazuh: SIEM)*
주요 사용 도구 및 기술		Python, Burpsuite
예상 결과물 및 상태		○ VPN 설정 파일 ○ DMZ 내부 네트워크 구성도

단계 번호		3
단계 명		VPN 설정 파일을 통한 내부 네트워크 침투
주요 목표		VPN 연결 확보를 통한 내부 네트워크 접속 및 내부망 스캔
유형	**공격**	정찰, 취약점 악용
	방어	탐지, 대응
주요 활동		[공격] ○ OpenVPN 크레덴셜 스터핑 도구 작성 ○ 단계 '1'에서 획득한 계정 정보 및 단계 '2'에서 획득한 설정 파일을 조합하여 크레덴셜 스터핑 공격으로 OpenVPN 연결 ○ 내부망 접속 후 네트워크 스캔을 통해 내부망 구조 파악 [방어] ○ VPN 인증 시도 및 실패 횟수 증가 탐지 ○ VPN 인증 시도 임계치 적용 *※ 방어 시나리오 사용 시 VPN 인증 로그 수집* *(Promtail+Loki, Wazuh Agent: 수집 -> Grafana: 시각화, Wazuh: SIEM)*
주요 사용 도구 및 기술		OpenVPN, Nmap
예상 결과물 및 상태		○ 내부망 스캔 정보 (Kubernetes 클러스터, 네트워크 대역 등)

단계 번호		4
단계 명		Kubernetes 환경 초기 침투
주요 목표		Kubernetes 클러스터 내 취약점 식별 및 공격을 통한 원격 코드 실행
유형	**공격**	취약점 악용, 명령 및 제어
	방어	탐지, 분석, 대응
주요 활동		[공격] ○ NGINX Ingress 사용 발견 및 식별 ○ IngressNightmare(CVE-2025-1974) 취약점 악용을 위한 c 코드 제작 및 컴파일 ○ IngressNightmare(CVE-2025-1974) PoC 사용 및 Reverse Shell 획득 ○ 컨테이너 및 클러스터 내부 정보 수집 [방어] ○ NGINX Ingress 비정상 트래픽 로그 탐지 ○ Kubernetes 내부 정보 수집 시 발생 감사 로그 탐지, 분석 ○ 취약한 NGINX Ingress 버전 업데이트 수행 *※ 방어 시나리오 사용 시 NGINX ingress, Kubernetes 감사 로그 수집 (Promtail+Loki, Wazuh Agent: 수집 -> Grafana: 시각화, Wazuh: SIEM)*
주요 사용 도구 및 기술		Python, Burpsuite, C, gcc, Reverse Shell, Kubectl,
예상 결과물 및 상태		○ 개발 Kubernetes 클러스터 내 pod의 쉘 확보 ○ Kubernetes 내부 정보 수집 결과

단계 번호		5
단계 명		컨테이너 탈출
주요 목표		Docker Socket 악용을 통한 컨테이너 탈출 및 호스트 침투
유형	**공격**	취약점 악용, 설치, 명령 및 제어
	방어	탐지, 분석, 대응
주요 활동		[공격] ○ 단계 '4'에서 수집한 Kubernetes 정보를 통해 Docker Socket 확인 ○ /var/run/docker.sock 확인 및 Privileged Container 생성 ○ nsenter/chroot 등으로 호스트 네임스페이스 진입 [방어] ○ Privileged/hostPath/docker.sock 접근 탐지 ○ 소켓 접근 및 호스트 네임스페이스 진입 이벤트 탐지, 분석 ○ 취약한 쿠버네티스 및 컨테이너 설정 점검 및 조치 *※ 방어 시나리오 사용 시 Kubernetes 이벤트 및 감사 로그 수집* *(Promtail+Loki, Wazuh Agent: 수집 -> Grafana: 시각화, Wazuh: SIEM)* *(컨테이너 보안 탐지를 위해 Falco 등 추가 구성 가능)*
주요 사용 도구 및 기술		Kubectl, Docker CLI
예상 결과물 및 상태		○ 호스트(Worker Node)의 기본 쉘 확보 ○ Privileged Container 신규 생성

단계 번호		6
단계 명		권한 상승
주요 목표		호스트의 취약한 설정 확인 및 악용을 통한 권한 상승, Kubernetes 정보 확인 및 ServiceAccount 토큰 확보
유형	**공격**	정찰, 취약점 악용
	방어	탐지, 분석, 대응
주요 활동		[공격] ○ /etc/sudoers 및 SUID 바이너리 분석을 통한 권한 상승 (Local Privilege Escalation) 수행으로 root 권한 획득 ○ Kubelet, Kubeconfig 설정 및 ServiceAccount 토큰 수집 [방어] ○ SUID 실행 및 권한 상승 시도 로그 탐지 및 분석 ○ 취약한 쿠버네티스 및 컨테이너 설정 점검 및 조치 *※ 방어 시나리오 사용 시 Kubernetes 이벤트 및 감사 로그 수집* *(Promtail+Loki, Wazuh Agent: 수집 -> Grafana: 시각화, Wazuh: SIEM)*
주요 사용 도구 및 기술		Python, Shell, Kubectl
예상 결과물 및 상태		○ 호스트(Worker Node)의 root 권한 확보 ○ Kubernetes 설정 정보 및 ServiceAccount 토큰 확보

단계 번호		7
단계 명		운영 클러스터 침투 및 개인정보 탈취
주요 목표		운영 클러스터로 수평 이동 및 개인정보 탈취
유형	**공격**	정찰, 취약점 악용, 목표 달성
	방어	탐지, 분석, 대응
주요 활동		[공격] ○ cluster-admin 토큰 악용으로 운영 클러스터 API에 접근 ○ 운영 클러스터에 Pod 배포 ○ 데이터베이스에 접근 및 덤프를 통한 개인정보(플래그) 탈취 [방어] ○ 클러스터 간 비정상 트래픽 발생 로그 탐지, 분석 ○ 데이터베이스 장시간 세션 연결, 덤프 탐지, 분석 ○ Kubernetes 감사 로그 탐지, 분석 ○ 취약한 쿠버네티스 및 컨테이너 설정 점검 및 조치 *※ 방어 시나리오 사용 시 Kubernetes 로그, DB 접속 및 쿼리 로그 수집 (Promtail+Loki, Wazuh Agent: 수집 -> Grafana: 시각화, Wazuh: SIEM)*
주요 사용 도구 및 기술		Kubectl, Postgresql 클라이언트 및 쿼리
예상 결과물 및 상태		○ 운영 클러스터 내 Pod 생성 및 장악 ○ 데이터베이스 내 개인정보(플래그) 탈취