# 쿠버네티스 노드 구성도 및 작업 내역

```yaml
# 컨트롤 플레인
- role: control-plane
  extraPortMappings:
  # DevSecOps 웹 서비스 포트
  # - 외부에서 웹 애플리케이션 접근용
  # - 호스트 접근: http://localhost:30080
  - containerPort: 30080
    hostPort: 30080
    listenAddress: "0.0.0.0"
    protocol: TCP

  # Wazuh 대시보드 포트
  # - Wazuh 보안 모니터링 웹 UI
  # - 호스트 접근: http://localhost:30601
  - containerPort: 30601
    hostPort: 30601
    listenAddress: "0.0.0.0"
    protocol: TCP

  # Jenkins 웹 인터페이스 포트
  # - CI/CD 파이프라인 관리 웹 UI
  # - 빌드 및 배포 모니터링
  # - 호스트 접근: http://localhost:8080
  - containerPort: 30800
    hostPort: 8080
    listenAddress: "0.0.0.0"
    protocol: TCP

  # Jenkins JNLP 에이전트 포트
  # - Jenkins 워커 노드 연결
  # - 분산 빌드 에이전트 통신
  # - 호스트 접근: localhost:50000
  - containerPort: 30850
    hostPort: 50000
    listenAddress: "0.0.0.0"
    protocol: TCP

  # SonarQube 웹 인터페이스 포트
  # - 코드 품질 분석 웹 UI
  # - 호스트 접근: http://localhost:30900
  - containerPort: 30900
    hostPort: 30900
    listenAddress: "0.0.0.0"
    protocol: TCP
```

Control Plane

```yaml
# 워커 노드 1: 웹서버
- role: worker
  labels:
    node-type: webserver
    purpose: apache-php
```

WorkNote

```yaml
# 워커 노드 2: Jenkins
- role: worker
  labels:
    node-type: jenkins
    purpose: jenkins
```

WorkNote2

```yaml
# 워커 노드 3: 백업 DB
- role: worker
  labels:
    node-type: backup-db
    purpose: backup-storage
```

WorkNote3

```yaml
# 워커 노드 4: 보안 프로그램
- role: worker
  labels:
    node-type: security
    purpose: wazuh-snort
```

WorkNote4

```yaml
# 워커 노드 5: 로그 DB
- role: worker
  labels:
    node-type: log-db
    purpose: log-storage
```

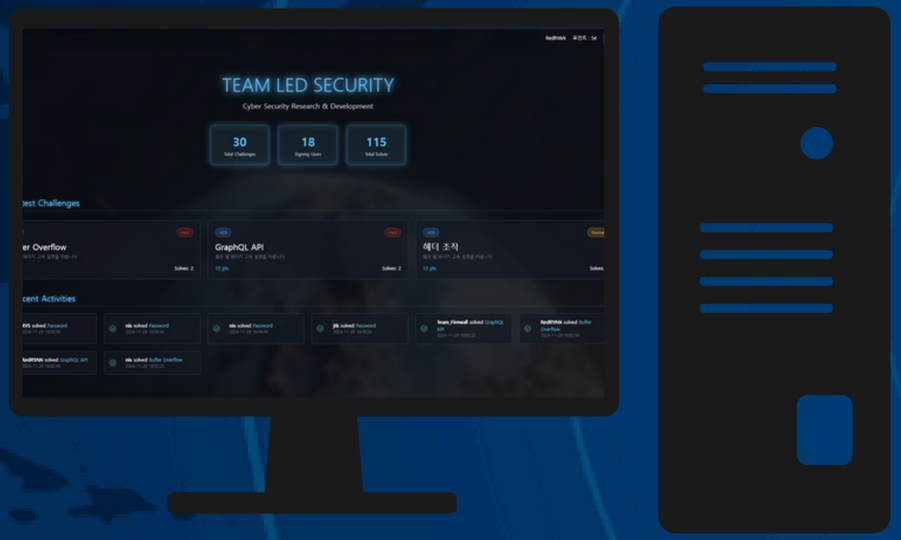
WorkNote5

```yaml
# 워커 노드 6: 웹 DB
- role: worker
  labels:
    node-type: web-db
    purpose: mariadb-web
```

WorkNote6

**Kind Kubernetes**

kubernetes




# WarGame Site

- 인증 및 인가 테스트
  - 로그인 시스템 취약점 검사
  - 세션 관리 취약점
  - 권한 우회 가능성 점검
  - JWT 토큰 보안성 검사
- GraphQL API 취약점
  - GraphQL 인젝션
  - 권한 검증 우회
  - 깊이 제한 우회
  - 속도 제한 우회
  - 내부 정보 노출 여부
- 버퍼 오버플로우 취약점
  - 입력값 검증 우회
  - 메모리 손상 가능성
  - 스택/힙 오버플로우
- 일반적인 웹 취약점
  - XSS (크로스 사이트 스크립팅)
  - CSRF (크로스 사이트 요청 위조)
  - SQL 인젝션
  - 파일 업로드 취약점
  - 정보 노출 취약점
- 인프라 보안
  - 서버 설정 오류
  - 불필요한 포트 개방
  - SSL/TLS 설정 취약점
  - 서버 버전 정보 노출
- 기능별 테스트
  - 각 챌린지 기능의 입력값 검증
  - 비즈니스 로직 취약점
  - 에러 처리 검증

코드 작성(Dev)
코드 커밋 (GitHub)