

OR : : OPA Regular

OPA를 활용한 K8S 보안 스캔 툴 제작



NAME. 정다연(PM, Infra, Research)
김세연(Backend)
최아록(Frontend)

개발 배경



쿠버네티스 보안 위협

쿠버네티스 도입은 증가하지만 보안 투자는 X
성과 및 제품에 부정적 영향



Policy As Code

정책 전용 언어로 전체 거버넌스 통제
rego 언어 기반의 OPA 등장



OPA의 장점

JSON으로 표현하면 어떤 언어든 사용 가능
도메인에 제한 X, 확장성 ↑



사전 보안 점검의 장점

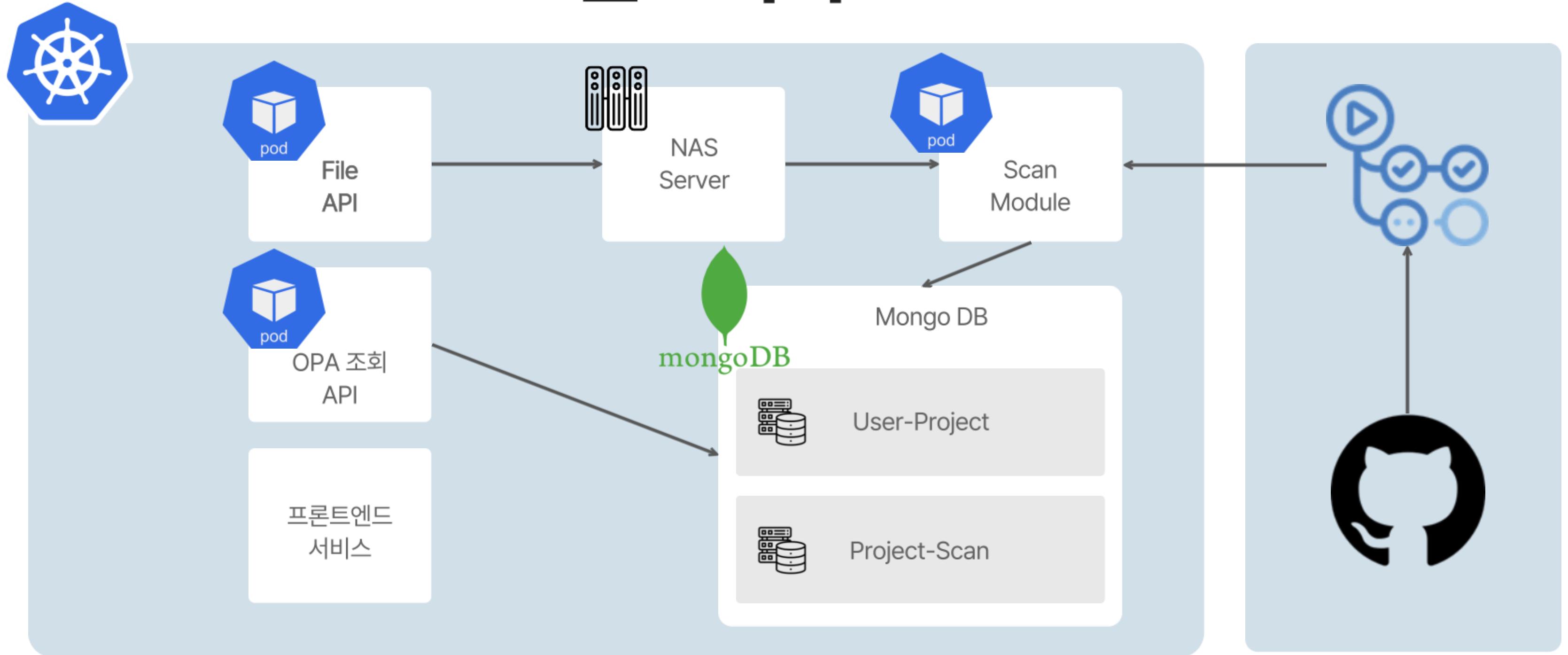
구축 초기 단계에서의 보안 위협 최소화
문제에 대한 조치 비용 절감 가능

KEYWORD

- 클라우드 보안 위협에 발맞춘 쿠버네티스 기반 보안 설정 OPA 제작
- Github CICD 자동화 과정에서 실시간으로 파악할 수 있는 대시보드 제작

appendix

인프라 구조도



Chapter 4

K8S 규제별 스캔

<https://github.com/octocat/Hello-World/pull/1347>

GET http://localhost:8080/repos/inpyu/Backend-Assignment-1/pulls/2 Send

Params Auth Headers (9) Body Pre-req. Tests Settings Cookies

	Key	Value
<input type="checkbox"/>	Authorization	eyJhbGciOiJIUzI1NCIsInR5cCI6IkpXZWQib3B1dUBot
<input type="checkbox"/>	X-Github-API-Version	2022-11-28
<input checked="" type="checkbox"/>	Accept	application/vnd.github+json
	Key	Value

Body Cookies Headers (5) Test Results 200 OK 2.35 s 298 B Save Response






Pretty Raw Preview Visualize JSON

```

1 {
2   "number": 2,
3   "title": "Settings: 작업용 디렉토리 생성",
4   "login": null,
5   "created_at": "2023-07-10T08:35:56Z",
6   "repo": null
7 }
```

The screenshot shows the Postman interface with a GET request to `http://localhost:8080/output`. The response is a JSON object with the following structure:

```
{
  "id": {
    "timestamp": 1699918443,
    "date": 1699918443000
  },
  "deny": [
    {
      "alertMessage": "service account: john-dev has the following permissions in the cluster: test",
      "alertObject": {
        "externalObjects": {
          "kind": "ServiceAccount",
          "name": "john-dev",
          "namespace": "default",
          "relatedObjects": [
            {
              "apiVersion": "rbac.authorization.k8s.io/v1",
              "kind": "Role"
            }
          ]
        }
      }
    }
  ]
}
```

<input type="checkbox"/>	Name	Namespace	Containers	Restarts	Controlled By	Node	QoS	Age	Status	
<input type="checkbox"/>	mongodb-deployment-f694f6dd5-n	default		0	ReplicaSet	opa-sdev-default	BestEffort	6h18m	Running	
<input type="checkbox"/>	opa-main-deployment-5b5f75744-n	default		0	ReplicaSet	opa-sdev-default	BestEffort	115m	Running	

K8S 규제별 스캔



NHH	03 January 2023 02:47 PM	검사중 1
NHH	#120 Set the initial length of set[T] in sets.KeySet 03 January 2023 02:47 PM	검사중 1
NHH	#119 gofmt fix Error string should not be capitalized or end with punctuation 03 January 2023 02:47 PM	검사중 1
NHH	#118 kubeadm: change SystemPrivilegedGroup in apiserve-kubelet-client.crt 03 January 2023 02:47 PM	검사중 1
AllYak	#121 e2e: avoid redundant labels in JUnit file 03 January 2023 02:47 PM	위험 요소 7
AllYak	#120 Set the initial length of set[T] in sets.KeySet 03 January 2023 02:47 PM	위험 요소 10
AllYak	#119 gofmt fix Error string should not be capitalized or end with punctuation 03 January 2023 02:47 PM	위험 요소 8
NHH	#118 kubeadm: change SystemPrivilegedGroup in apiserve-kubelet-client.crt 03 January 2023 02:47 PM	위험 요소 7
NHH	#119 gofmt fix Error string should not be capitalized or end with punctuation 03 January 2023 02:47 PM	위험 요소 7
NHH	#118 kubeadm: change SystemPrivilegedGroup in apiserve-kubelet-client.crt 03 January 2023 02:47 PM	위험 요소 23