IntentShield

An Intent-Powered Security Policy Operator Framework for Kubernetes

BOM KIM, SEUNGSOO LEE

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

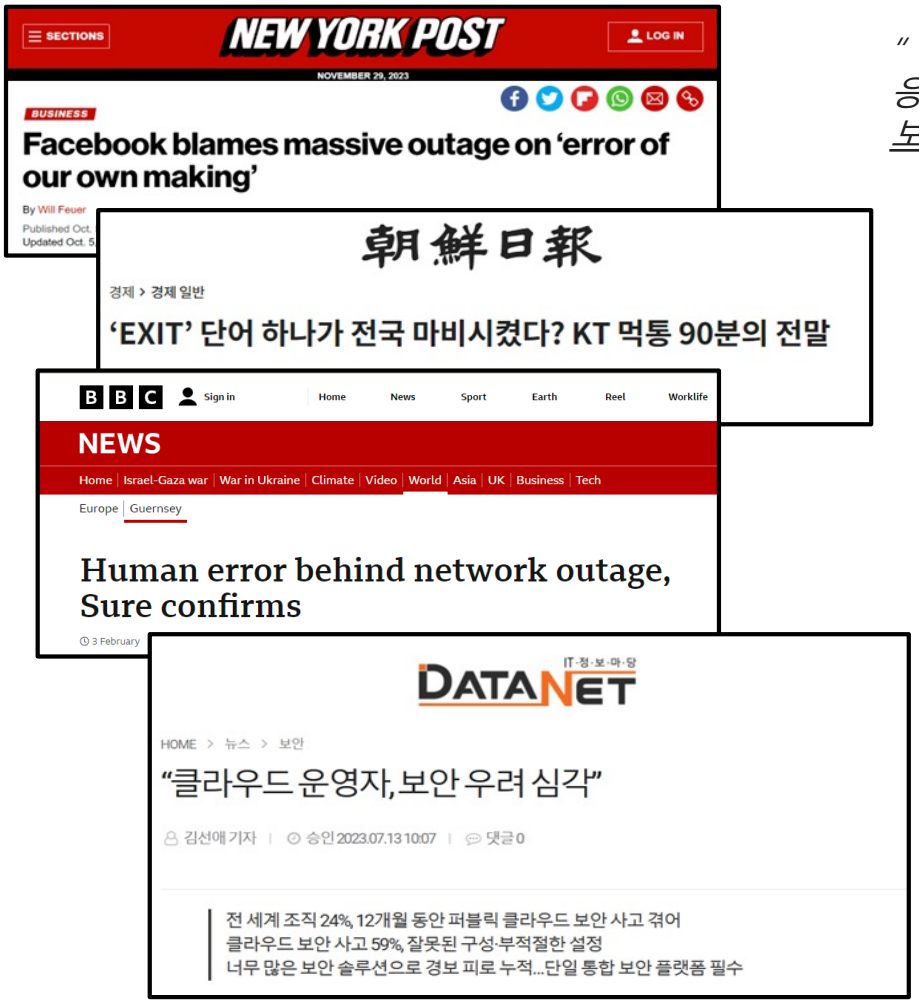
INCHEON NATIONAL UNIVERSITY

Content

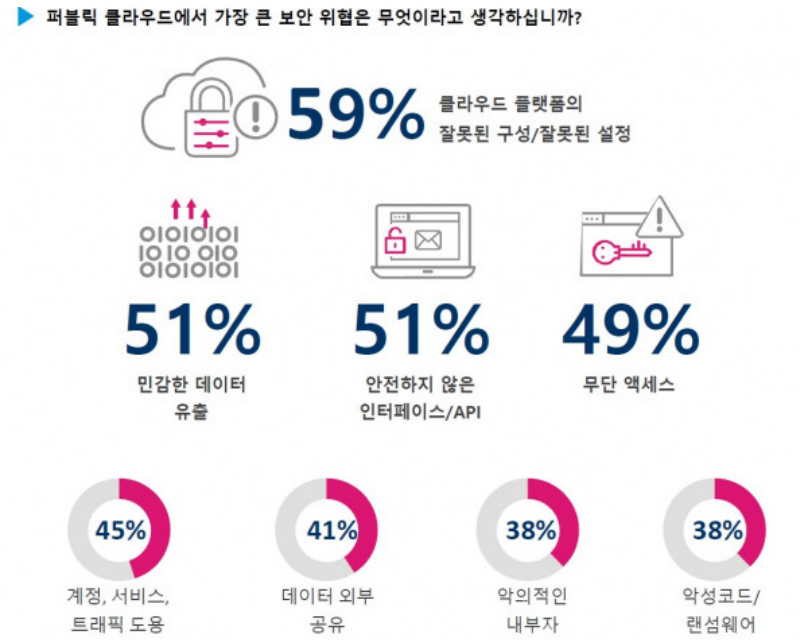
Abstract

- Research **automated security policy enforcement** for better security management in cloud environments.
- Suggest **IntentShield** for Automated Policy Management.
- Demonstrate the **automation potential** of your policies.

Challenges: Accidents Caused by Manual Management



" 응답자의 76%는 클라우드 보안에 대해 우려하고 있으며, 응답자의 24%가 지난 12개월 사이 퍼블릭 클라우드 관련 보안 사고를 경험 "



https://www.datanet.co.kr/news/articleView.html?idxno=185235

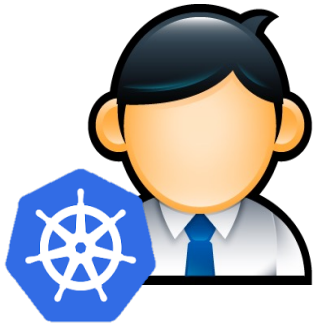
Challenges: Manually Managing Kubernetes Policies

Real-Time Policy
Update Difficulties

Difficulty in
Maintaining Consistency

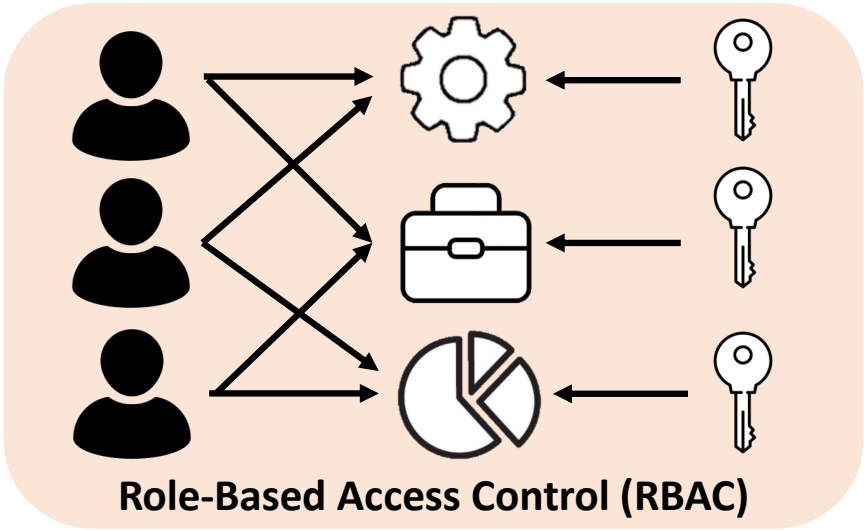
Difficulty in receiving
a prompt response.

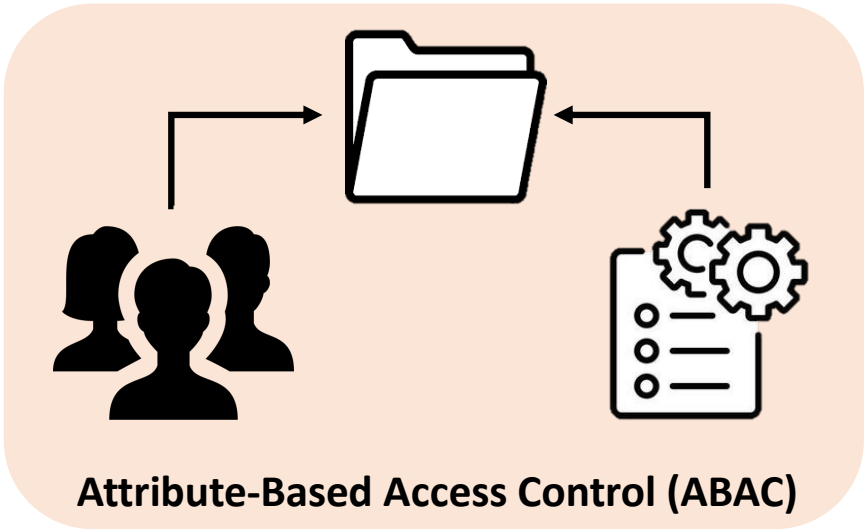
Human Error
Susceptibility



Security Policy
Complexity

Limitations: Existing Security Policy Management





- Static and Inflexible
- Complexity in Management
- Limited Contextual Awareness
- Difficulty in Rapid Adaptation

Limitations: Existing Security Analysis Methods

> “ **How can we overcome the complexity of Kubernetes and the reality of manual management?** ”

- Inadequate Response to Changes

- Advanced Persistent Threats (APT)
- Volume of Data
- Automation Limitations

Workflow: IntentShield

Intent File

```
apiVersion: intent.k8s.cclab.com/v1
kind: IntentPolicy
metadata:
  name: my-intent-1
  namespace : my-intent-netpol
spec:
 network:
    - enforce : "Allow TCP 90"
...
  system:
    - enforce : "Block attempts to execute the '/bin/sleep' process."
...
```

Managed by User

Oper. Transform/Create

Managed by Operator

System Policy (e.g. KubeArmor)

```
apiVersion:security.kubearmor.com/v1
kind:KubeArmorPolicy
metadata:
  name: proc-path-block-my-intent-1
  namespace : my-intent-netpol
spec:
...
   description: "Block attempts to execute the '/bin/sleep' process."
   process:
    matchPaths:
    - path: /bin/sleep
  action: Block
...
```

Network Policy (e.g. Cilium)

```
apiVersion: cilium.io/v2
kind: CiliumNetworkPolicy
metadata:
  name: allow-tcp-90-my-intent-1
  namespace : my-intent-netpol
spec:
  description: "Allow TCP 90"
  ingress:
...
  - ports:
      - port: "90"
        protocol: TCP
...
```

Oper. Validate/Apply

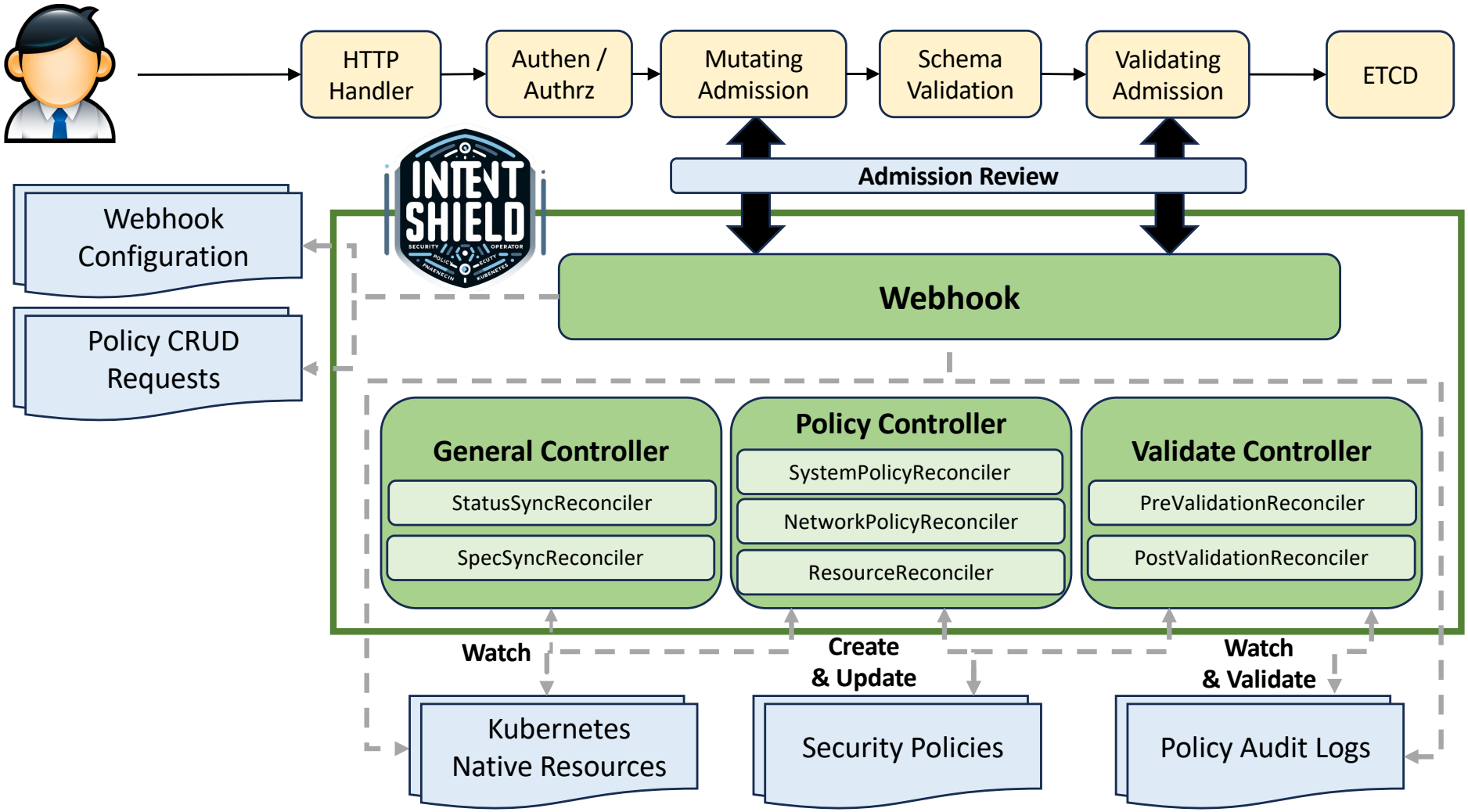
Design: Intend-Based Security CRD (SecurityIntent)

- Declaratively express user security intent to Kubernetes with a SecurityIntent CRD.
- Automate security policies without complex setup.

```
apiVersion: intent.k8s.cclab.com/v1
kind: SecurityIntent
metadata:
  name: my-intent-1
  namespace: my-intent-pol
spec:
  network:
    - enforce: "Allow TCP 90"
...
  system:
    - enforce: "Block attempts to execute the '/bin/sleep' process."
...
```

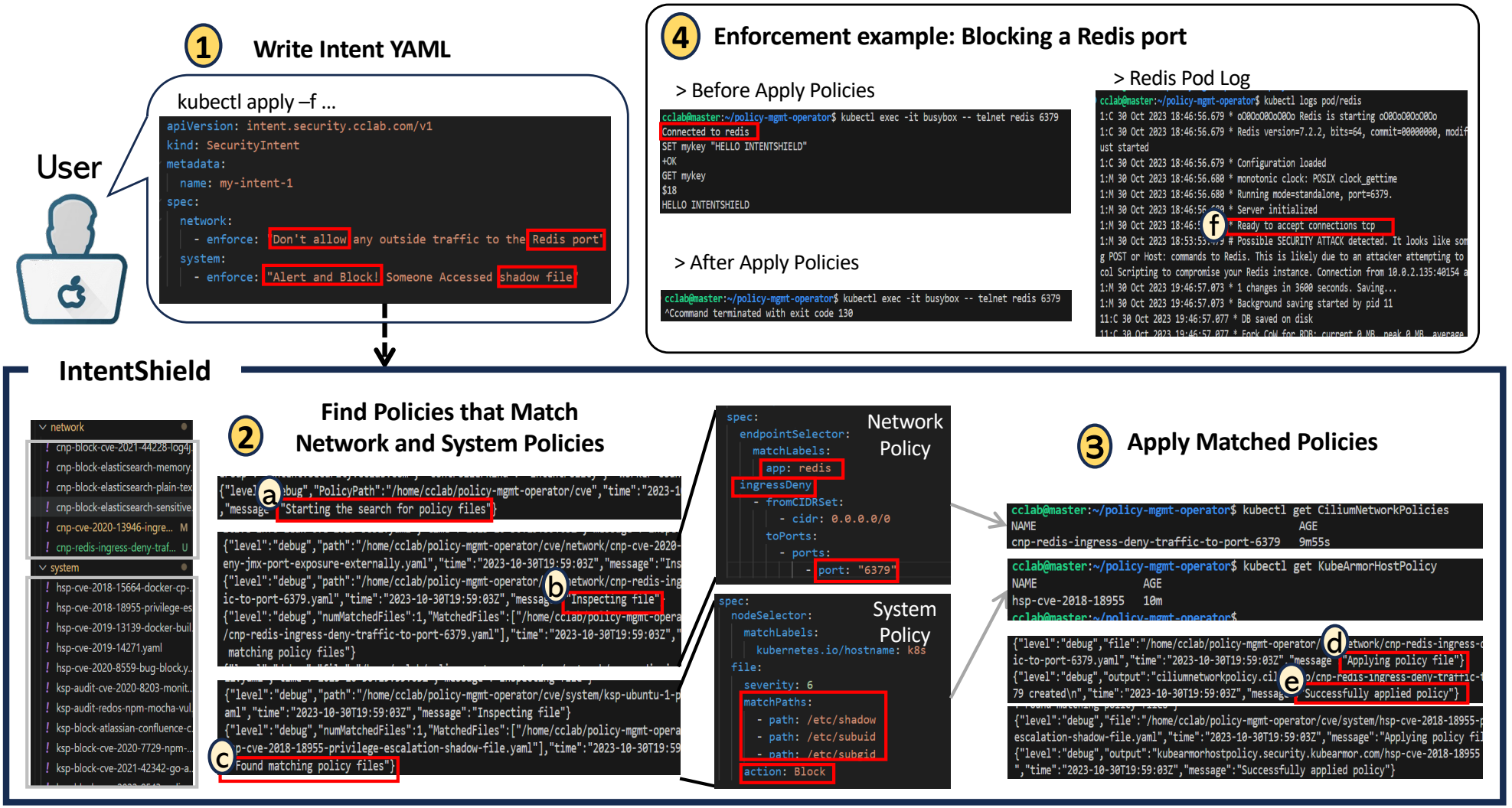
Design: IntentShield

- Suggest a Kubernetes operator to automatically manage policies.

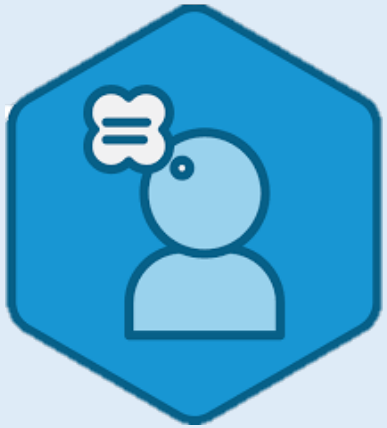


Evaluation: Demonstrate Feasibility

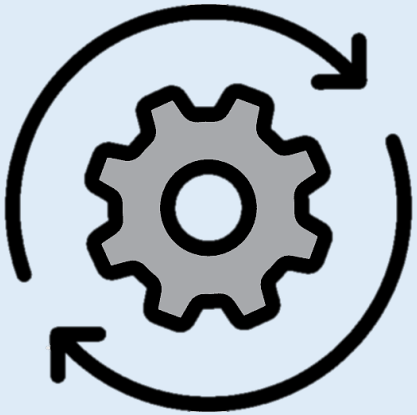
- How does IntentShield automate the alignment of user intent with security policies?



Conclusion

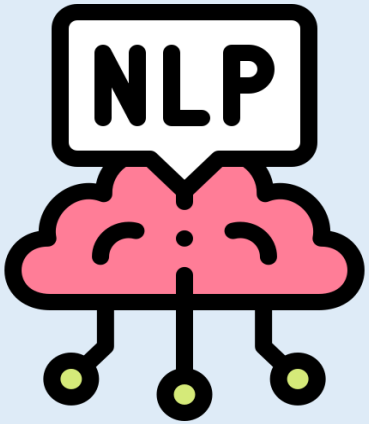


Design user-centered security policies



Automation and continuous security

Limitation and Future Work



Rely on intent-identical description matching

Scalability and Flexibility for Policies

Extend policy validation with CEL
(Common Expression Language)

Reference

[1] Almehmadi, Abdulaziz, and Khalil El-Khatib. "On the possibility of insider threat prevention using intent-based access control (IBAC)." IEEE Systems Journal 11.2 (2015): 373-384.

[2] KubeArmor, Oct 2023, [online] Available: https://github.com/kubearmor /KubeArmor

[3] Cilium - Network Policy, Oct 2023, [online] Availble: https://docs.cilium.io/en/latest/security/policy/

[4] KubeArmor - policy-templates, Oct 2023, [online] Availble: https://git hub.com/kubearmor/policy-templates.

Any Questions?

THANK YOU