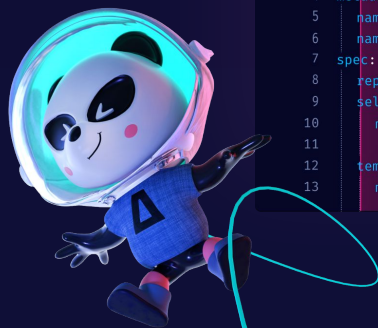
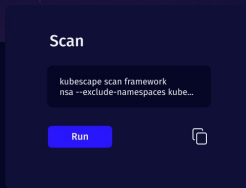


# Guardians of the Runtime: Leveraging Behavioral Analysis and Policies



```
1 ---
2 apiVersion: apps /V1
3 kind: Deployment
4 metadata:
5   name: front-end
6   namespace: sock-shop
7 spec:
8   replicas: 1
9   selector:
10    matchLabels:
11      name: front-end
12   template:
13     metadata:
```



**ARMO**

Ben Hirschberg CTO of ARMO



# /whoami

**Ben** Hirschberg

**Co-founder** & CTO @ARMO

**Kubescape** maintainer

**Whitehat** in the past (unofficially still ;-)

**Fluent** in Hebrew, Hungarian, C, ASM and Go (not English)

**Contributor** in CNCF + organizer of CNCF Jerusalem

**Father** of 4 <3



**@Ben Hirschberg**



Ben-hirschberg



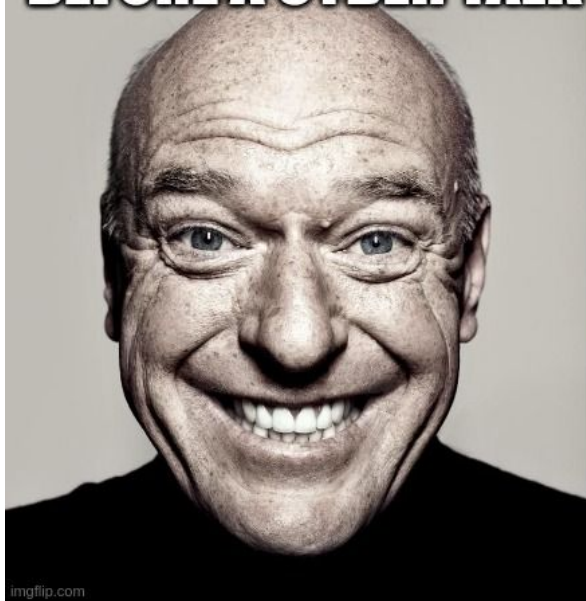
@slashben81



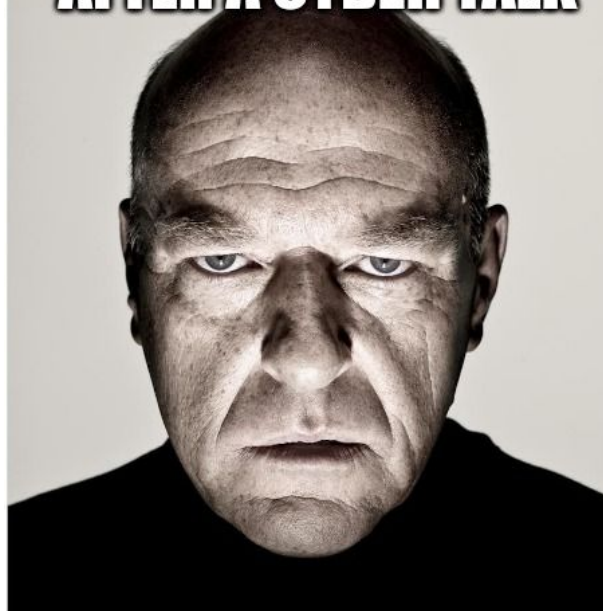
github.com/slashben

/usually...

**BEFORE A CYBER TALK**

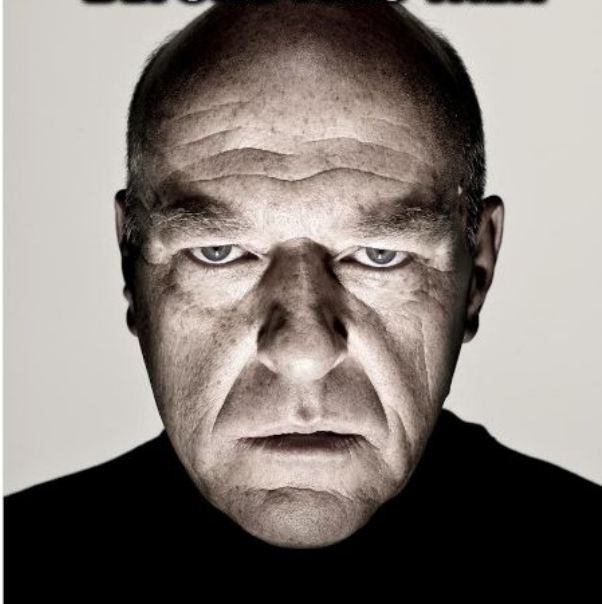


**AFTER A CYBER TALK**

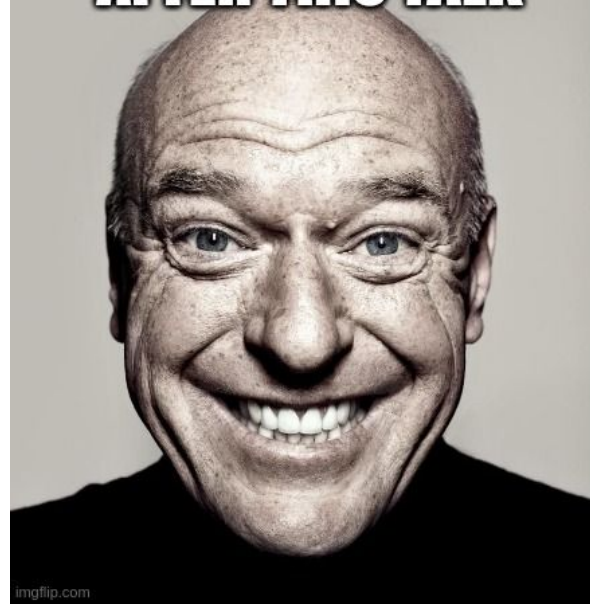


/but this time

**BEFORE THIS TALK**



**AFTER THIS TALK**



imgflip.com

# /cat agenda

- **Kubernetes-native policies**

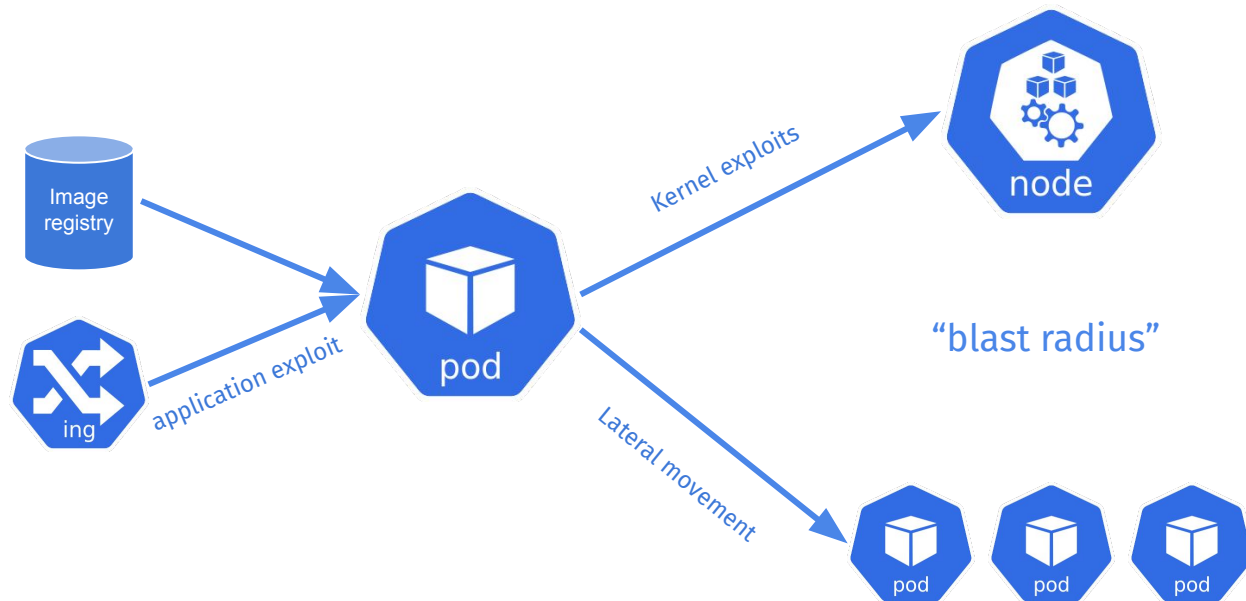
- **Generate vulnerability and policies from behavior**

- **Adding policy generation to your CI/CD**



/why

## Threat model

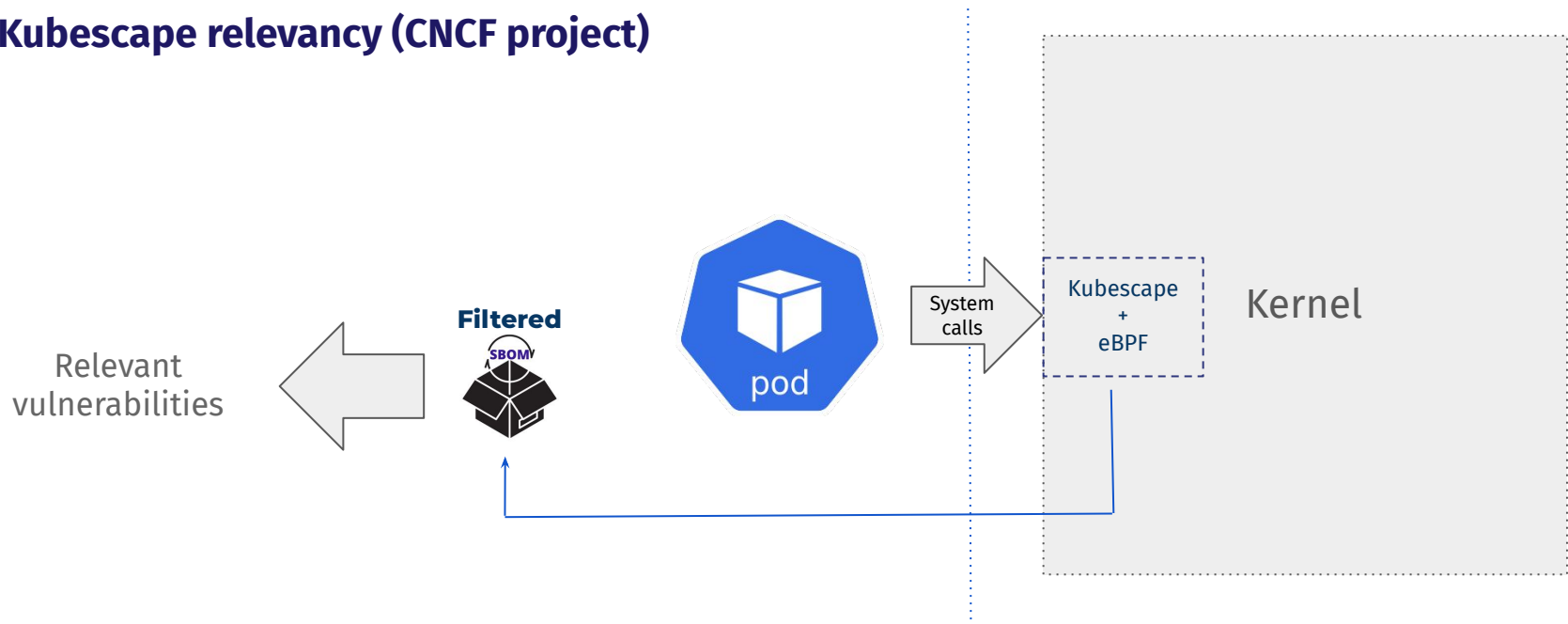


# /app\_vulnerabilities

## Vulnerability discovery in workloads

- Standard tools list all container contents
- Average application/database image “has” **100+** vulnerabilities
- Very expensive to manage

## Kubescape relevancy (CNCF project)

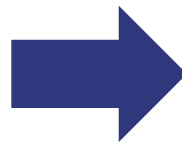




# /kernel\_protection

## Pod security context

- User/group ID
- Process capabilities + privileges
- Seccomp



CVE-2021-31440,  
CVE-2022-0185,  
CVE-2022-0492

# /seccomp\_profiles

## Seccomp profiles

- Premade application profiles
- Manual definition
- Generating from application behavior

# /kspo\_profile\_gen

## Kubernetes Security Profile Operator (sig-security project!)

```
apiVersion: security-profiles-operator.x-k8s.io/v1beta1
kind: SeccompProfile
metadata:
  namespace: my-namespace
  name: profile1
spec:
  defaultAction: SCMP_ACT_LOG
```



System  
calls

SPOD  
+  
eBPF

Kernel



# /network\_protection

## Network policies

- Reconnaissance
- Lateral movement
- Data extraction

# /network\_hardships

Defining policies

Maintenance



Developers

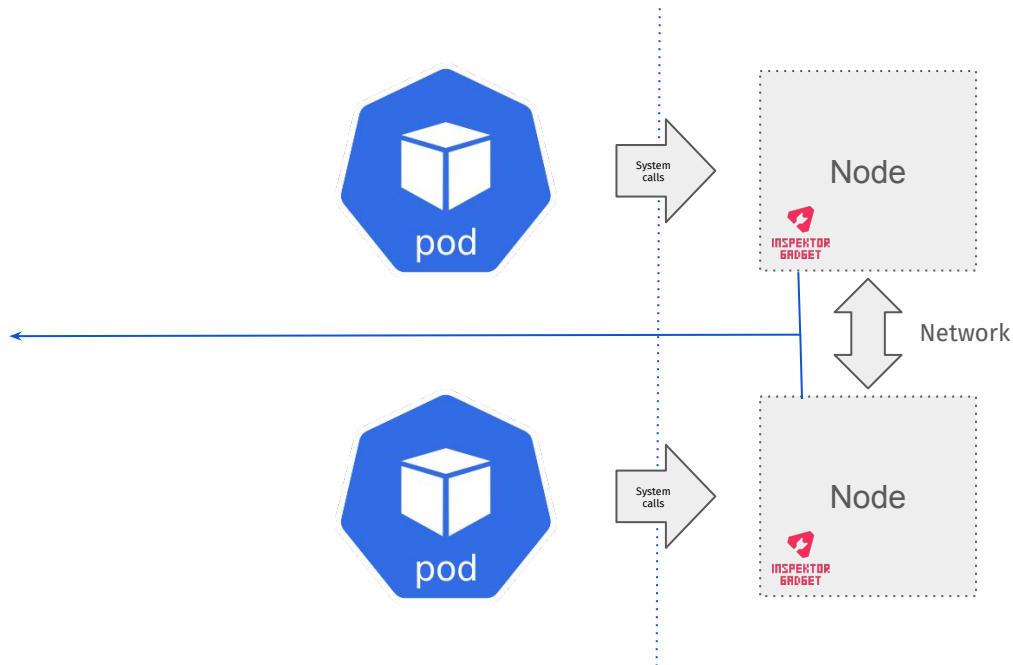
DevOps/SRE

Security/DevSecOps

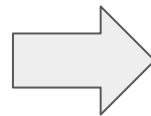
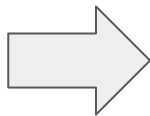
# /inspektor\_gadget\_advise

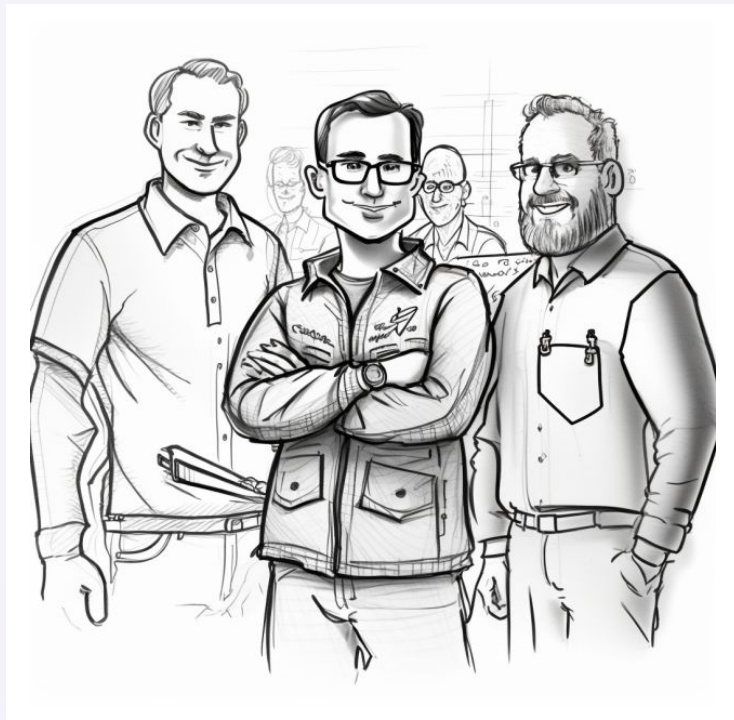


```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  creationTimestamp: null
  name: cartservice-network
  namespace: demo
spec:
  egress:
  - ports:
    - port: 6379
      protocol: TCP
    to:
    - podSelector:
        matchLabels:
          app: redis-cart
  - ports:
    - port: 53
      protocol: UDP
    to:
    - namespaceSelector:
        matchLabels:
          kubernetes.io/metadata.name: kube-system
      podSelector:
        matchLabels:
          k8s-app: kube-dns
  ingress:
  - from:
    - podSelector:
        matchLabels:
          app: checkoutservice
    ports:
    - port: 7070
      protocol: TCP
  - from:
    - podSelector:
        matchLabels:
          app: frontend
```



/magic\_box









**CONTINUOUS**



**INTEGRATION**



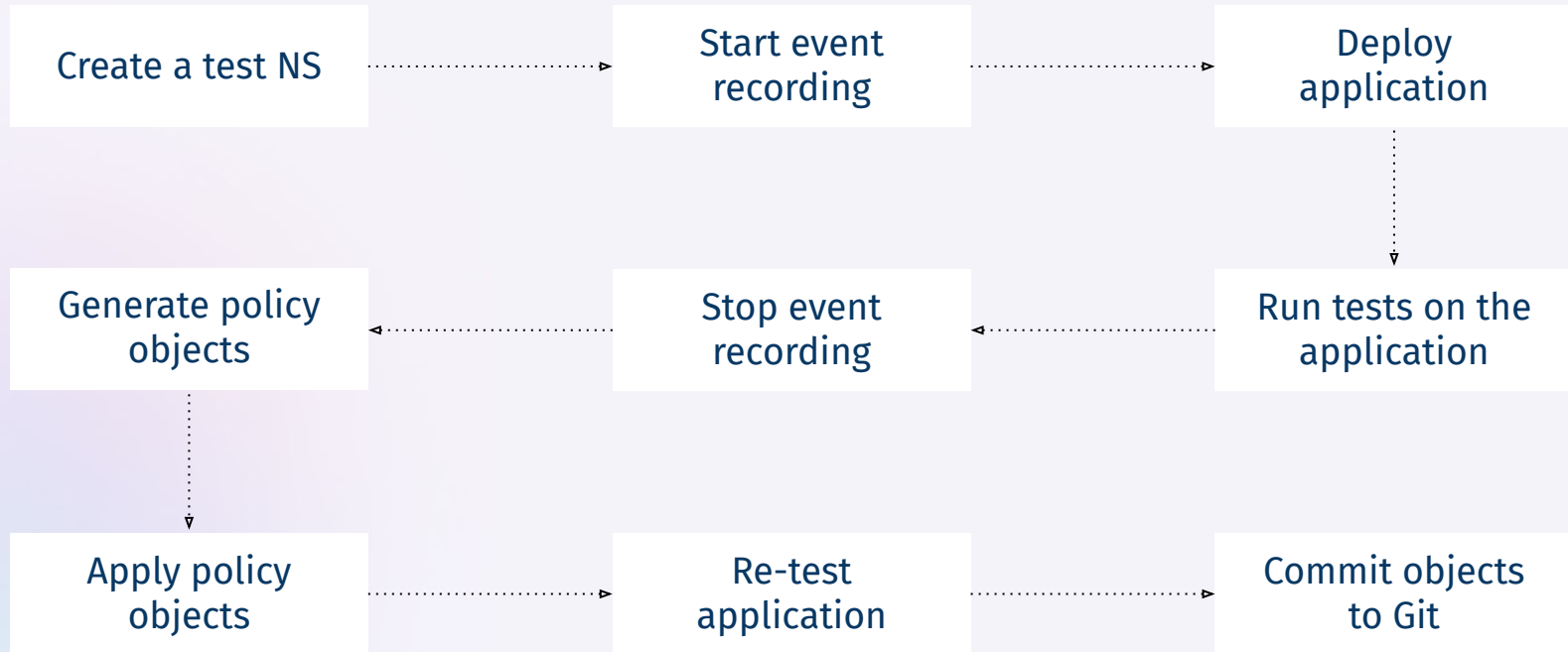
**CONTINUOUS DEPLOYMENT**



**CONTINUOUS SECURITY**

imgflip.com

# /cs-process-overview

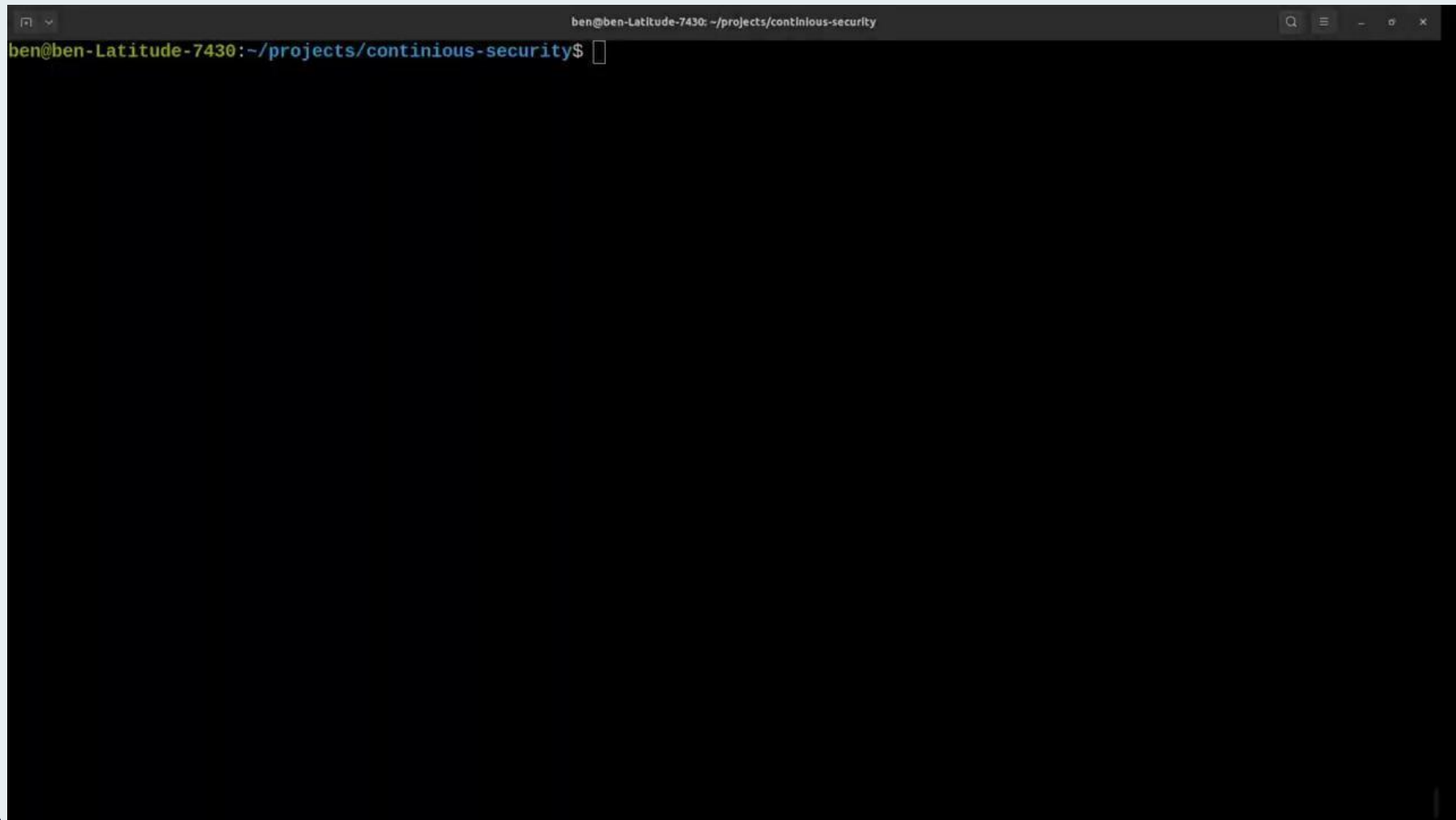




# /demo-time

1. Environment setup
2. Seccomp profile generation
3. Testing the seccomp profiles
4. Network policy generation
5. Testing the network policies







## /caveats


- Extra resources at generation and testing phases
- Tools are not broadly adopted and tested
- Tool interfaces with CRs are not easy
- Missing tests paths leading to broken policies
- Incomplete system leading to broken policies



# /advantages

- Applying these improves security posture considerably
- Considerably less vulnerabilities to handle
- Setup once and more or less forget
- Least privilege principle applied


# /see\_yourself

 Search or jump to... / Pull requests Issues Codespaces Marketplace Explore

slashben / cn-continuous-security-demo (Public) Pin Unwatch 1 ...

<> Code Issues Pull requests Actions Projects Wiki Security Insights Settings

main 1 branch 0 tags Go to file Add file <> Code

 slashben Both working 55396bb yesterday 2 commits

network-policies	Both working	yesterday
scripts	Both working	yesterday
seccomp-profiles	Both working	yesterday
.gitignore	Both working	yesterday
README.md	Both working	yesterday

README.md

## Continuous Security (CS) demo

Welcome to the documentation for our Cloud Native security demo that shows you to create policy objects from application behavior with ease. This demo showcases how you can seamlessly integrate this tool into your CI/CD pipelines, enabling you to generate network policy objects and Seccomp profile objects that meet your application's specific needs.

The demo utilizes Google's microservice-demo application, providing an excellent opportunity to see how our tool works in real-time. With the help of our tool, you can take your cloud-native application security to the next level, ensuring that your policies align with your application's behavior perfectly.

The documentation is designed to guide you through the process of using the tool and integrating it into your CI/CD pipelines. We have included step-by-step instructions on how to generate network policy objects and Seccomp profile

### About

No description, website, or topics provided.

- Readme
- 0 stars
- 1 watching
- 0 forks

### Releases

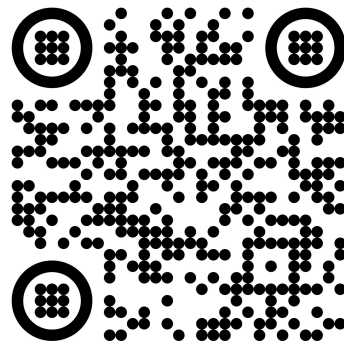
No releases published  
[Create a new release](#)

### Packages

No packages published  
[Publish your first package](#)

### Languages

Shell 100.0%





Thank you\_

ΔRMO