German OWASP Day 2025

ALL THE WAF POWER TO THE DEVS

why it reduces friction... and where it backfires

Lukas Funk

German OWASP Day 2025

Lukas Funk

Security Solution Architect

United Security Providers AG

lukas.funk@united-security-providers.ch

lukas-funk-ch

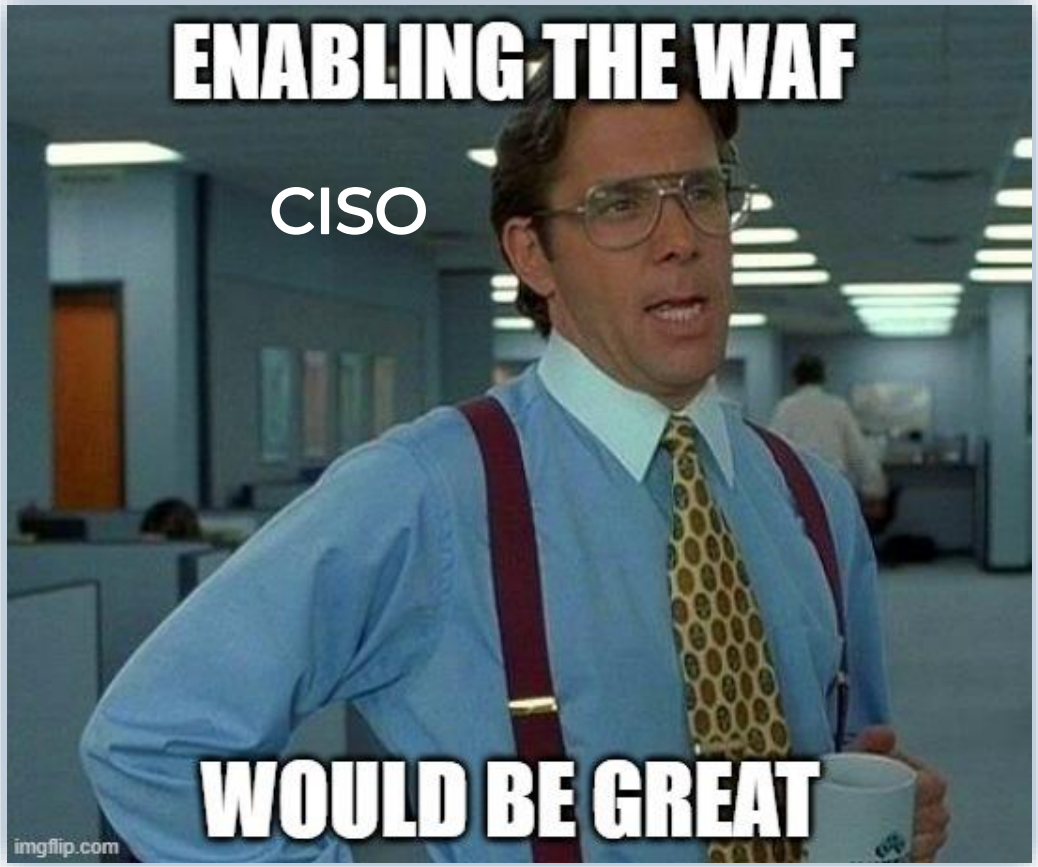
UNITED SECURITY PROVIDERS

ZERO TRUST UNIVERSE

German OWASP Day 2025

Web Application Firewall

CISOs LIKE WAFs



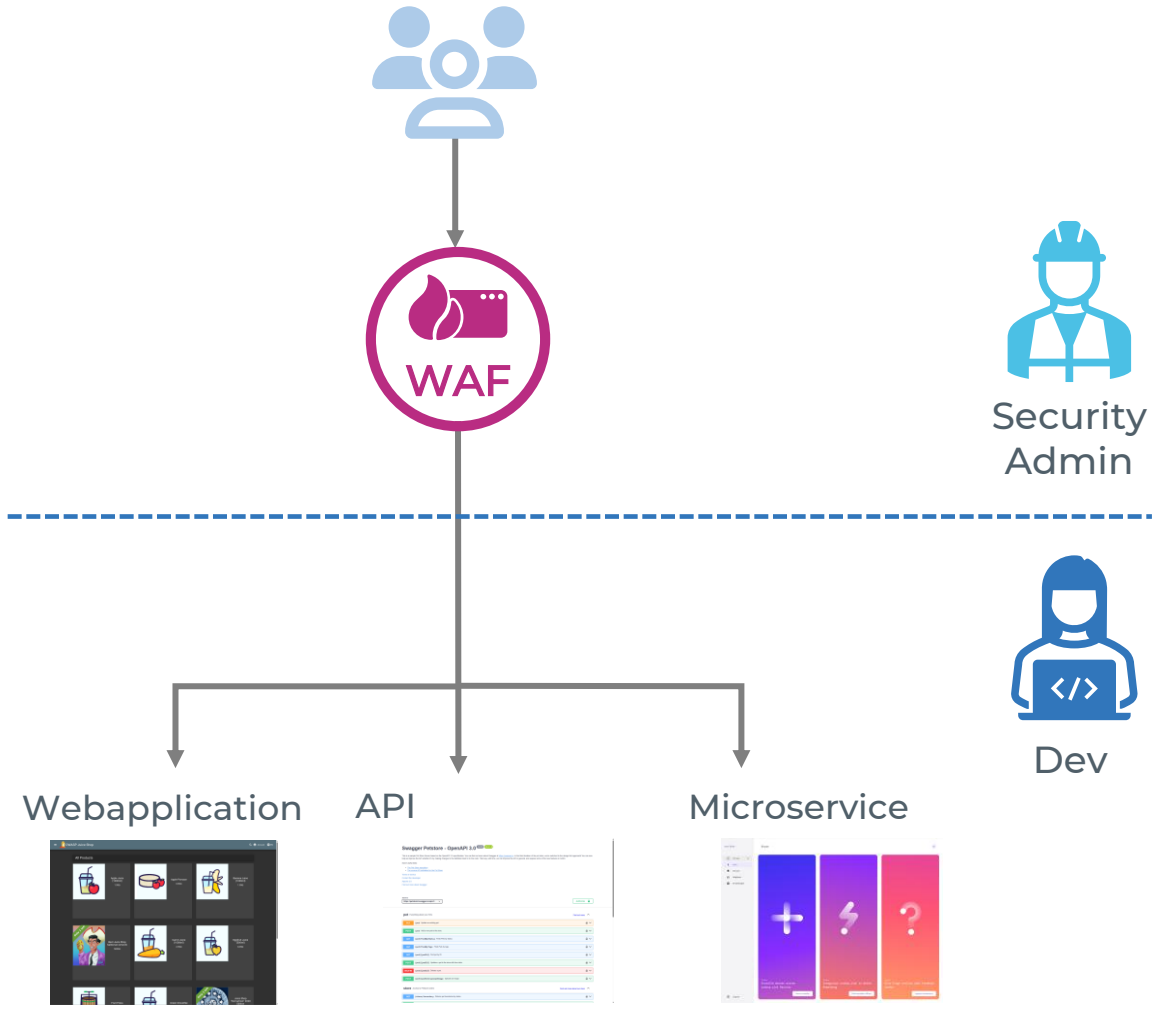

```
/?redirect_uri=%0d%0a%0d%0a<script>alert(document.domain)</script>]
```

```
/setextno.jsp?user_ids=(99999)+union+all+select+1,2,(md5(999999999)),4]
```

```
/../../../../../../../../../../../../../etc/passwd
```

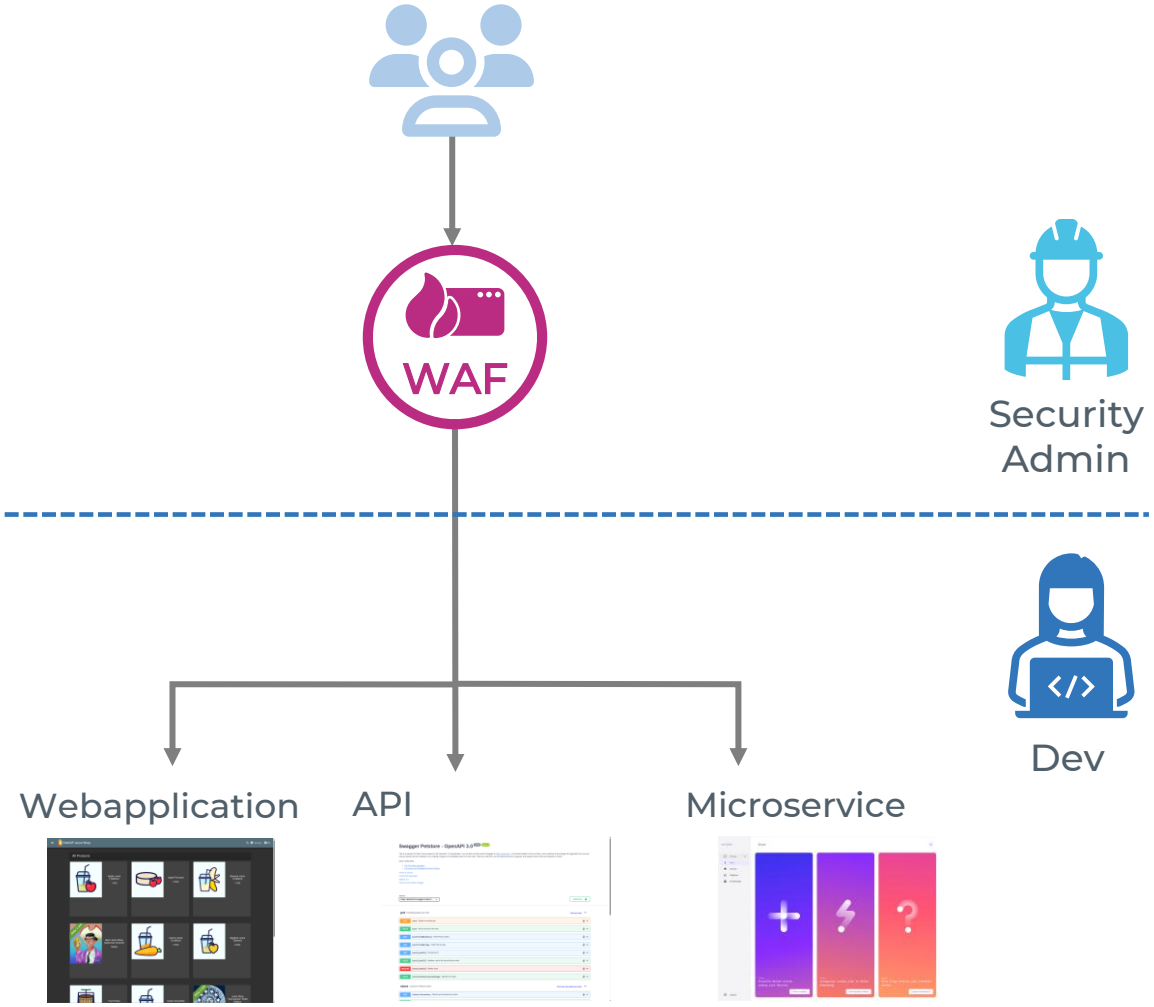
Customer installations with >100.000 of such requests per month

NOT EVERYONE LIKES THE WAF



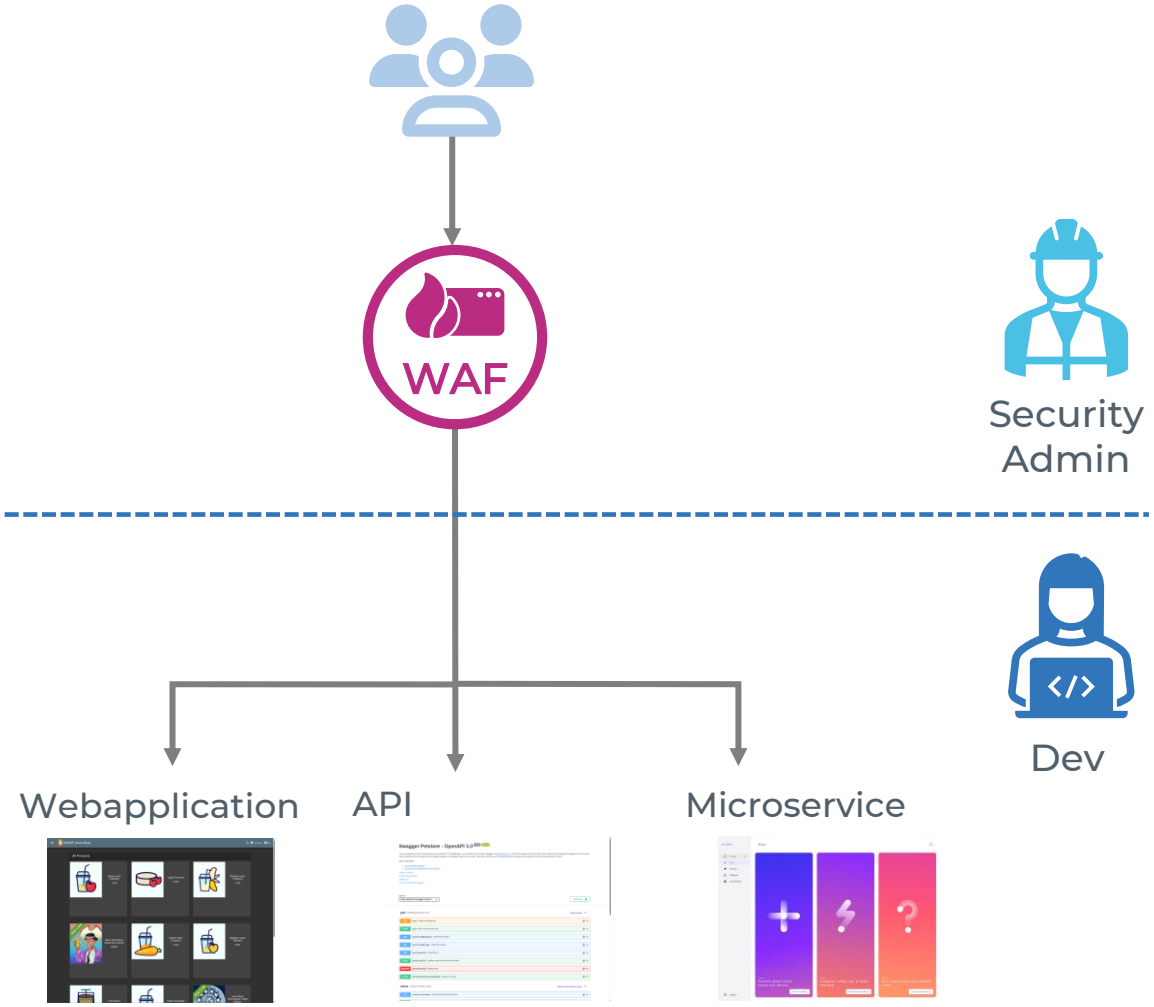
CHALLENGE IN PROCESS

- WAF comes **often late** into play and may **affect functionality** of the app



CHALLENGE IN PROCESS

- **Separated deployment process**, can't be integrated in CI/CD process
- **No visibility** because Dev and Ops are using **different tools**
- **Update paralysis**, difficult to judge the impact on the whole chain.



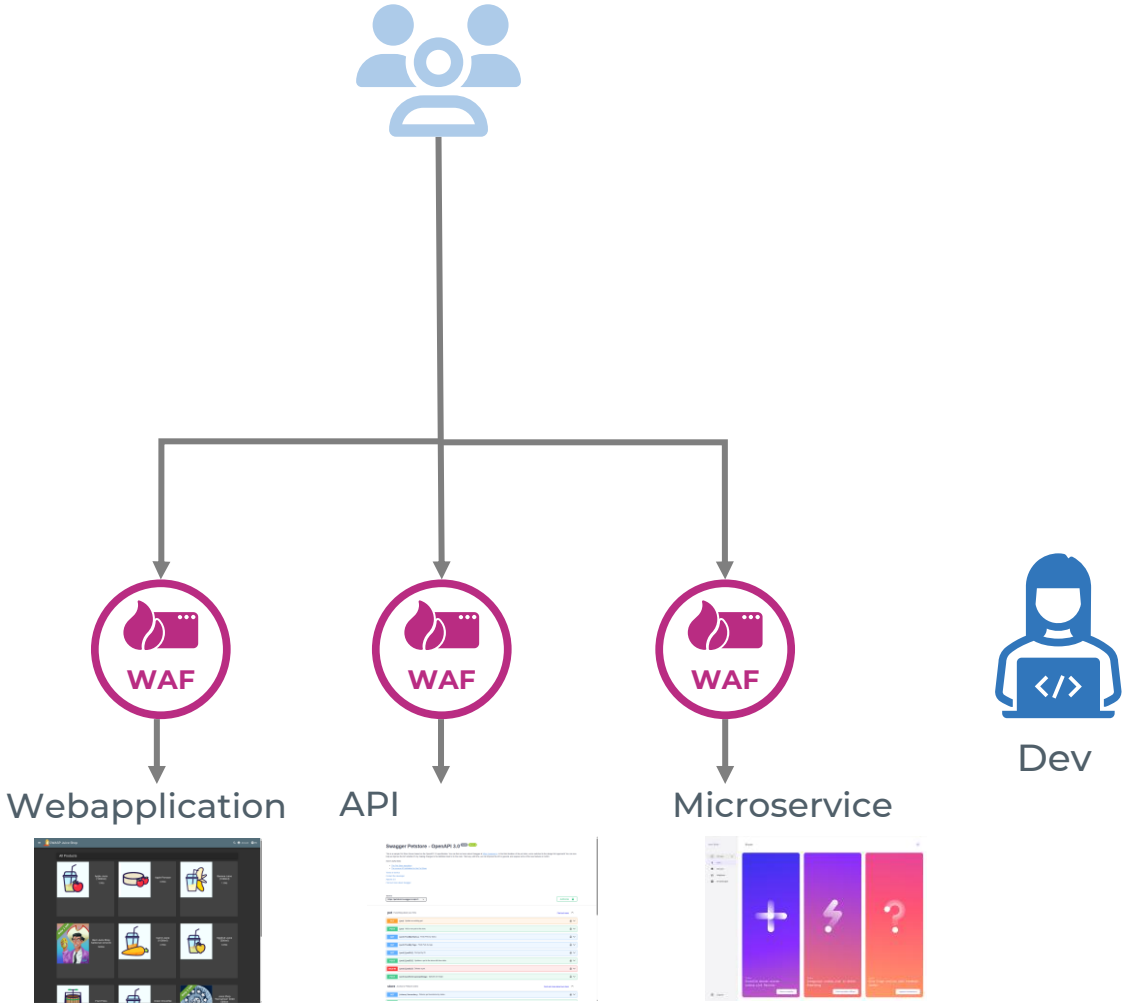
CHALLENGE IN TECHNOLOGY

- **Scalability & Availability** requirements for a hybrid cloud environment is not given

German OWASP Day 2025

App-centric WAF

APP-CENTRIC VISION



SHIFT LEFT THE WAF

- It should be an **integral part** of the **development process**!
- Setup should allow easy **integration with CI/CD processes** to automate deployments.
- Fit into modern **cloud- & container-native architectures**
- **Agility & easy of use** without compromise in security

German OWASP Day 2025

App-Centric WAF by Example

CORAZA WAF FOR KUBERNETES

coraza
WEB APPLICATION FIREWALL

CRS

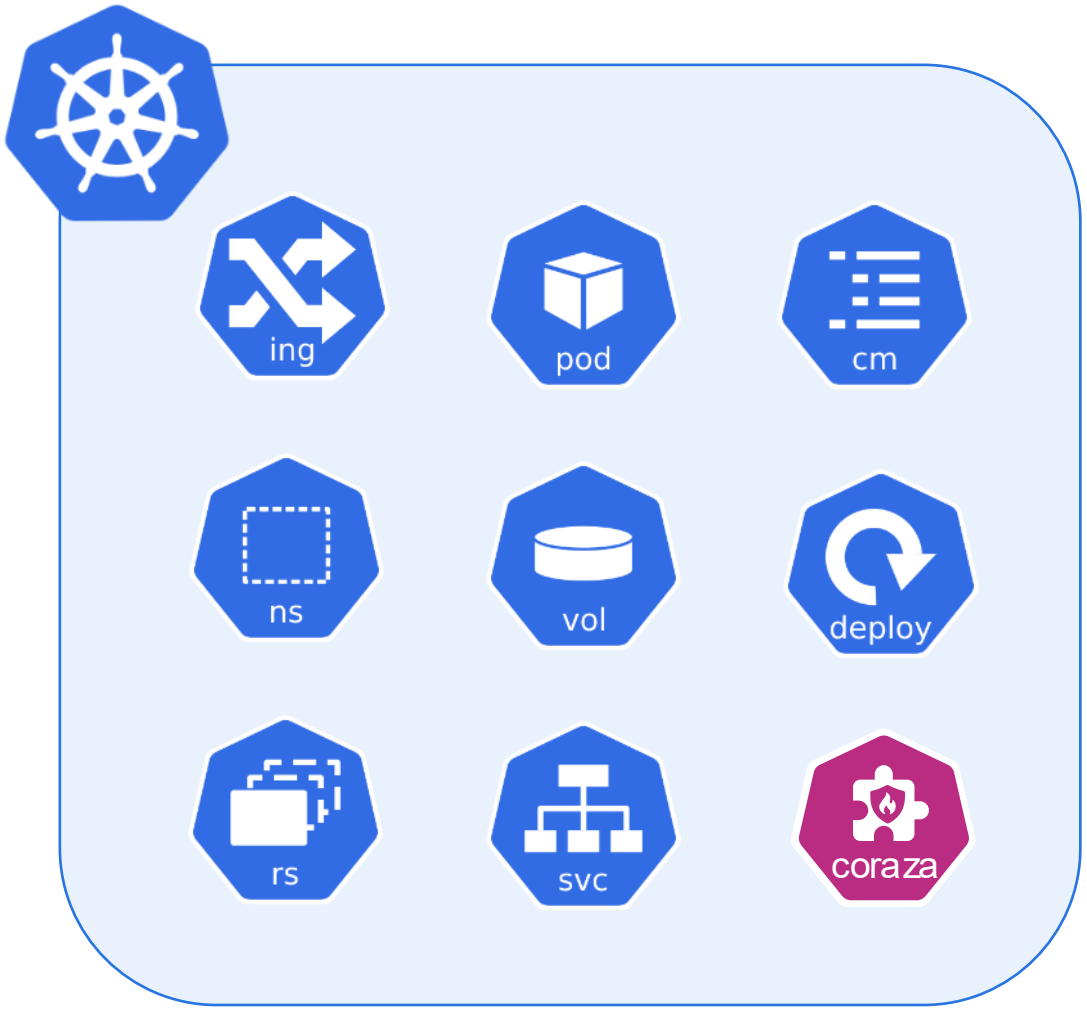
envoy

Dataplane

Controlplane

Simplified Management using
Coraza WAF K8s Operator

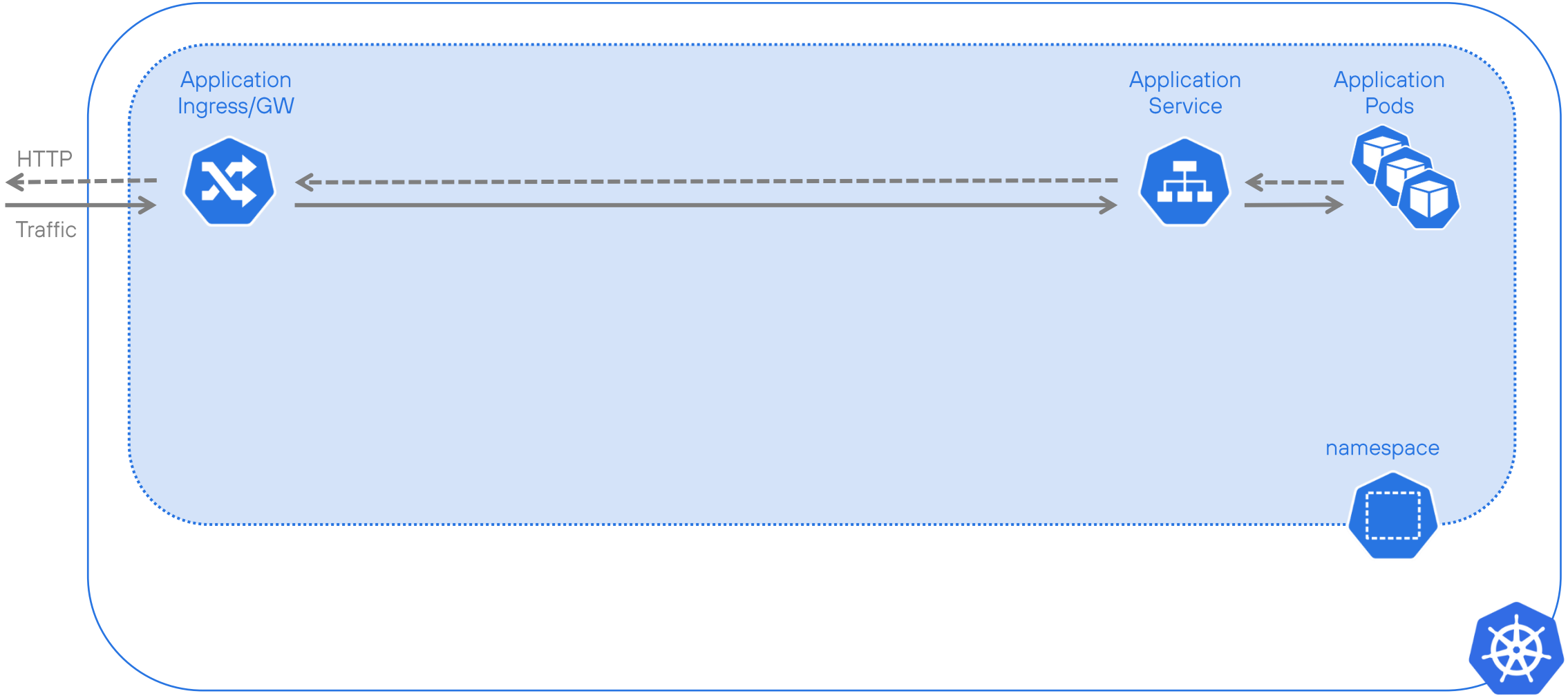
CORAZA WAF OPERATOR




```yaml
---
apiVersion: oss.u-s-p.ch/v1alpha1
kind: CorazaWaf
metadata:
  name: app-centric-waf
  namespace: default
spec:
  backend:
    hostname: "juice-shop"
    port: 8000
  crs:
    enabledRequestRules:
      - REQUEST_911_METHOD_ENFORCEMENT
      - REQUEST_913_SCANNER_DETECTION
      - REQUEST_920_PROTOCOL_ENFORCEMENT
      - REQUEST_921_PROTOCOL_ATTACK
      - REQUEST_922_MULTIPART_ATTACK
      - REQUEST_930_APPLICATION_ATTACK_LFI
      - REQUEST_931_APPLICATION_ATTACK_RFI
      - REQUEST_932_APPLICATION_ATTACK_RCE
      - REQUEST_933_APPLICATION_ATTACK_PHP
      - REQUEST_934_APPLICATION_ATTACK_GENERIC
      - REQUEST_941_APPLICATION_ATTACK_XSS
      - REQUEST_942_APPLICATION_ATTACK_SQLI
      - REQUEST_943_APPLICATION_ATTACK_SESSION_FIXATION
      - REQUEST_944_APPLICATION_ATTACK_JAVA
    paranoiaLevel:
      detecting: 2
      enforcing: 1
```

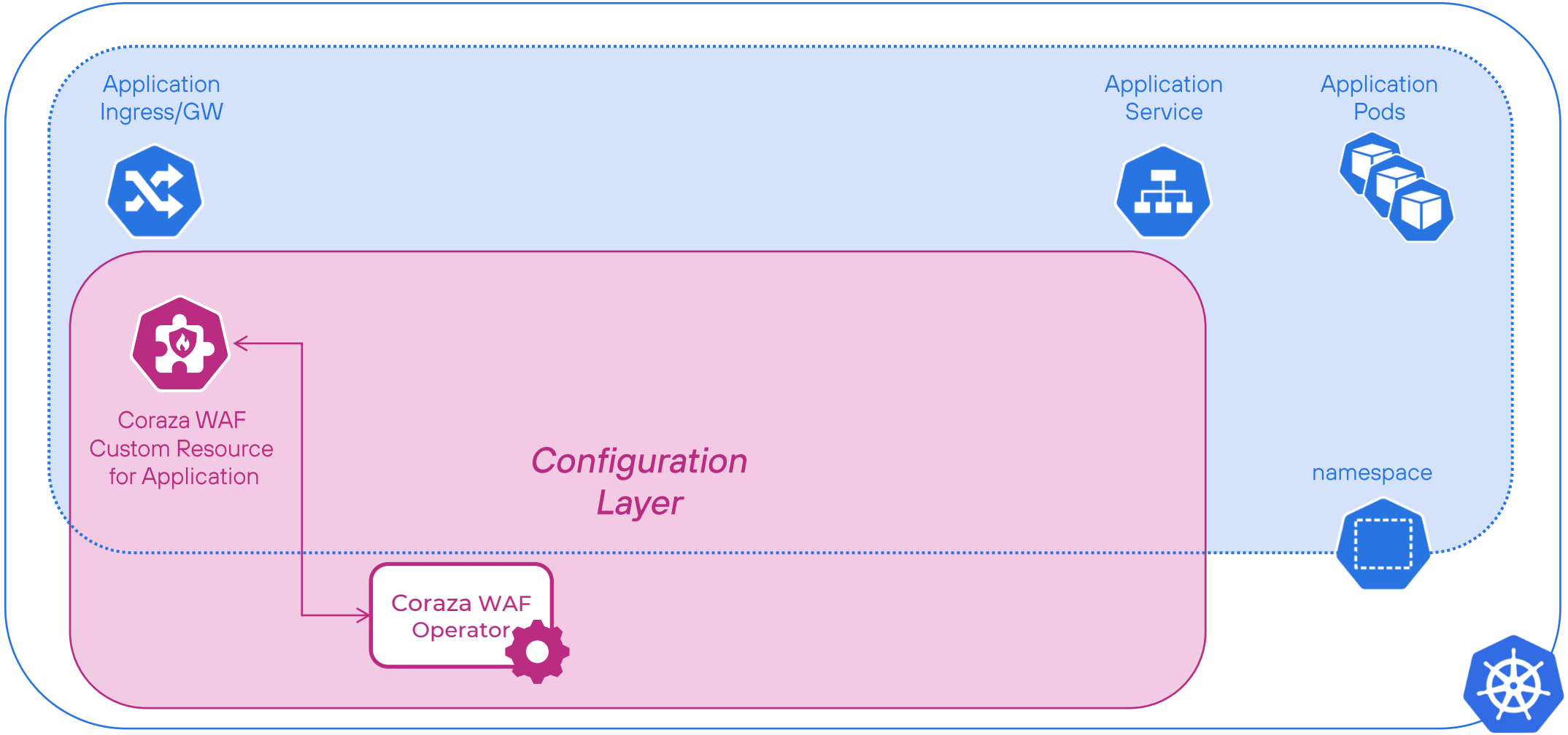
German OWASP Day 2025

KUBERNETES DEPLOYMENT



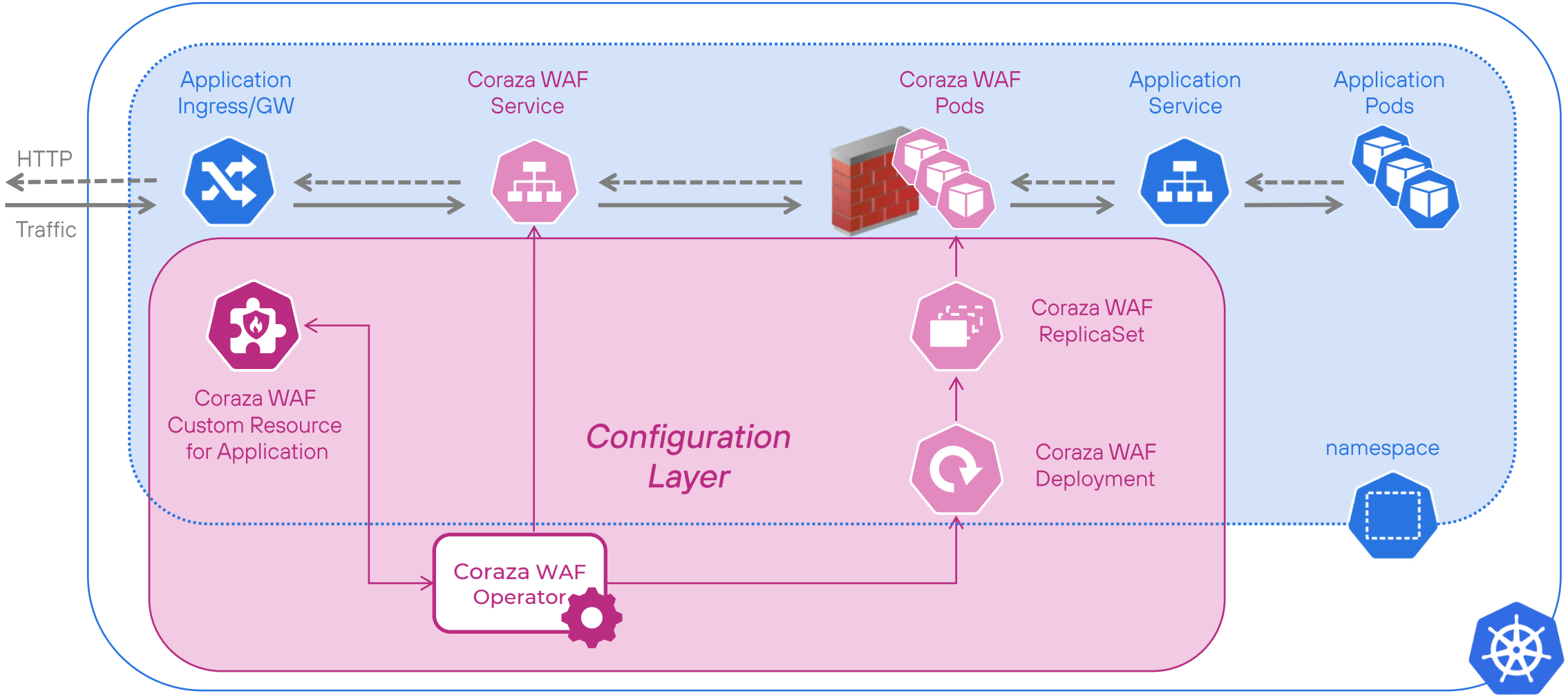
Legend: *Kubernetes

APPLICATION-CENTRIC CONFIGURATION



German OWASP Day 2025

APPLICATION-CENTRIC – NEW WAF SERVICE



German OWASP Day 2025

OWASP Coraza Envoy Go-filter

https://github.com/united-security-providers/coraza-envoy-go-filter

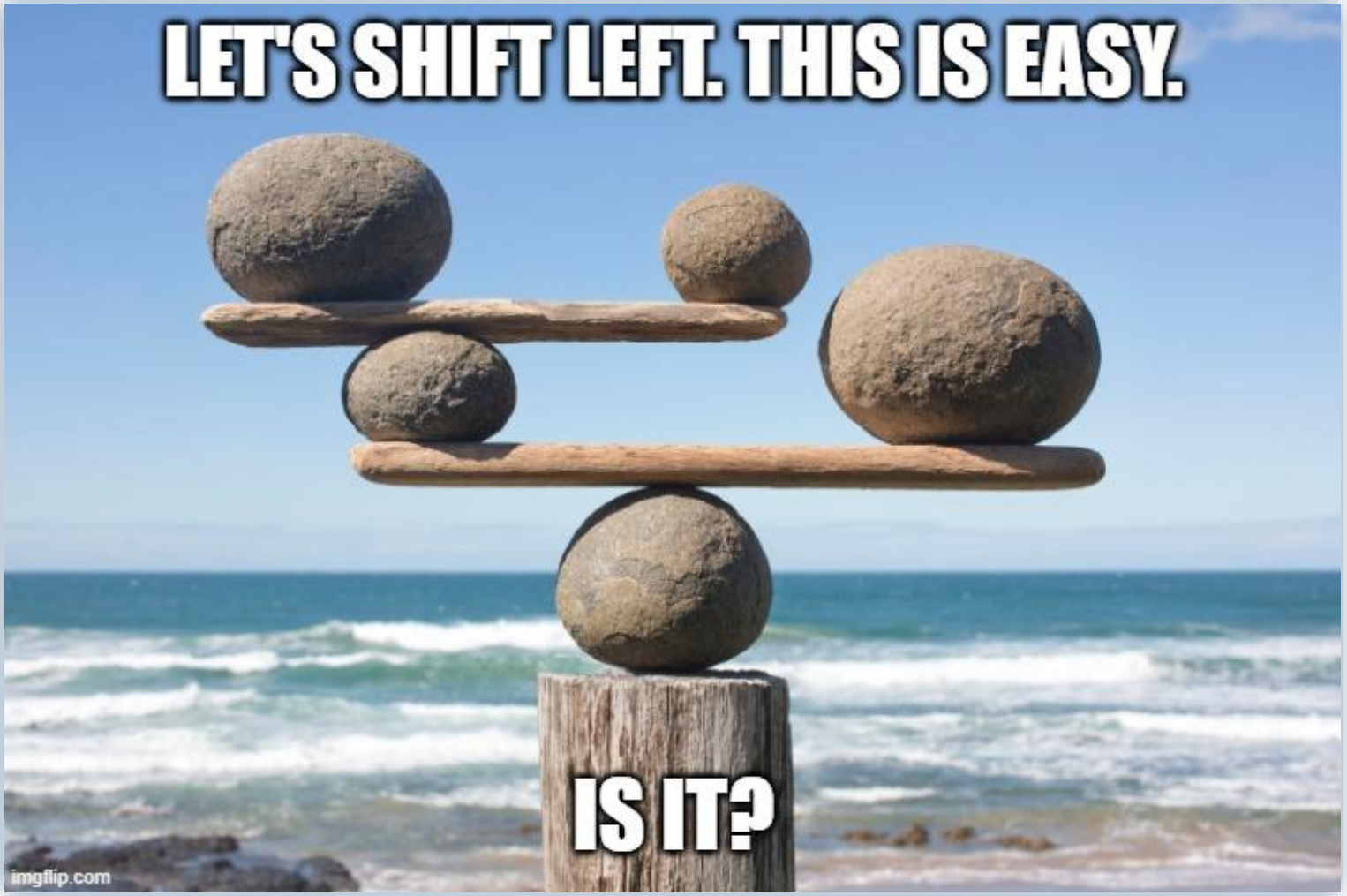
Kubernetes App-centric Coraza WAF Operator

https://github.com/united-security-providers/coraza-operator-oss

German OWASP Day 2025

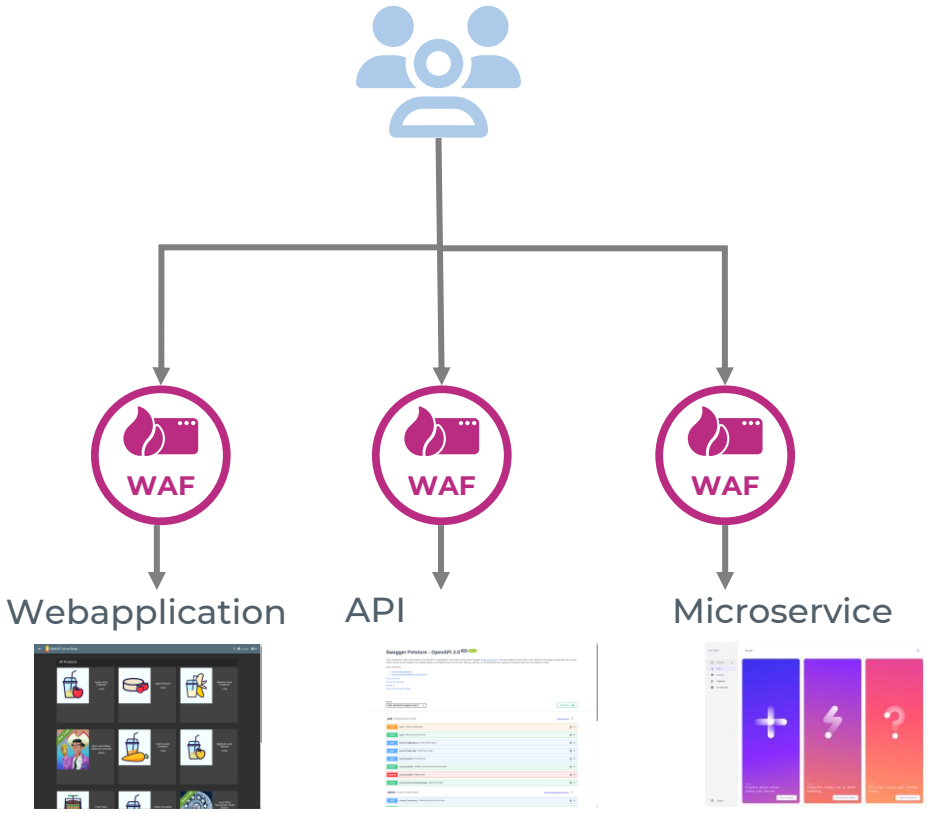
Lessons learned

LESSONS LEARNED

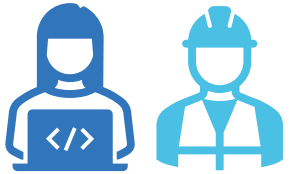


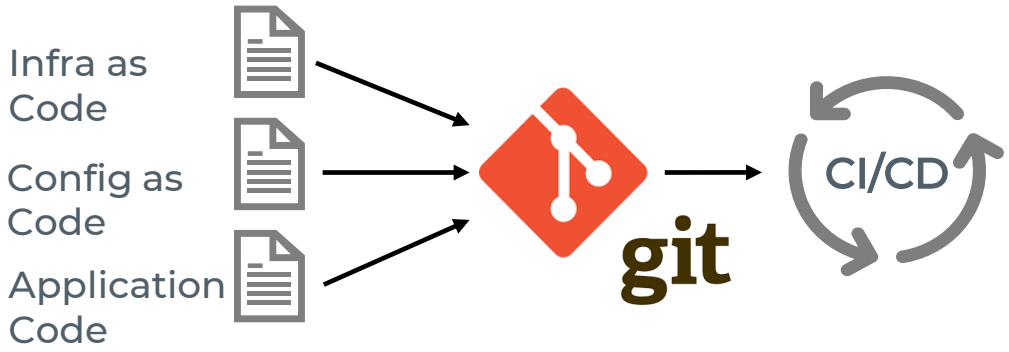
ACHIEVEMENT

Bringing the WAF closer to the application



Using a uniform tool chain throughout the entire process





LESSONS LEARNED

Developers and WAF Admins are not used to working like this

Separation of duty

- Get familiar with **the new process**
- **Connect** developers with the WAF Expert and implement **review processes**
- “**Managed Service**” by the WAF experts
- **Ease of use** is important!

TOPICS TO ADDRESS

It's not on the perimeter!

- **TLS Termination & IP-address related security features** typically not part of the app-centric WAF

Global Virtual Patching is cumbersome!

Global Policy Enforcement

- Use of a **policy engine** to enforce a minimal company policy for the WAF configuration
- **NetworkPolicies** should in be in place, so traffic is always routed through the WAF

German OWASP Day 2025

ALL THE WAF POWER TO THE DEVS

why it reduces friction... and where it backfires

German OWASP Day 2025

THANK YOU!