



How Tetragon Can Help You Take Your AKS Defense to the Next Level

Cilium & AKS Workshop Day, June 2023



 **Microsoft**
Solutions Partner
Digital & App Innovation
Azure

Specialist
Modernization of Web
Applications

Who we are



Philip Welz

(Senior DevOps & Kubernetes Engineer,
Azure MVP)



+49 8031 230159-0



Philip.welz@whiteduck.de



@philip_welz



www.linkedin.com/in/philip-welz



Nico Meisenzahl

(Head of DevOps Consulting & Operations,
Cloud Solution Architect)



+49 8031 230159-0



nico.meisenzahl@whiteduck.de



@nmeisenzahl



www.linkedin.com/in/nicomeisenzahl

Agenda

- Why you should think about Container and K8s security
- What is Tetragon?
- Demo: Getting started with Tetragon
- Demo: Prevent Log4Shell attack with Tetragon
- Demo: Awareness and Observability

Why you should think about Container and K8s security

Do we need to care about security?

In the past 12 months, what security incidents or issues related to containers and/or Kubernetes have you experienced? (pick as many as apply)

53% Detected misconfiguration



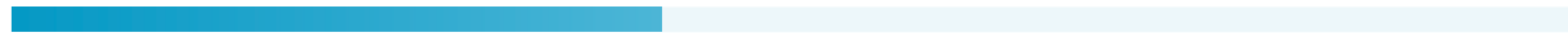
38% Major vulnerability to remediate



30% Security incident during runtime



22% Failed audit



7% None



In the last 12 months, have you experienced revenue/customer loss due to a container/Kubernetes security or compliance issue/incident?

69% No

31% Yes

Yes!

In the past 12 months, what security incidents or issues related to containers and/or Kubernetes have you experienced? (Select all that apply.)



Runtime Security in a nutshell

1. **Detecting** malicious activity in real time
2. **Reporting** when malicious events occur
3. Even better, **preventing** them

What is Tetragon?

Tetragon

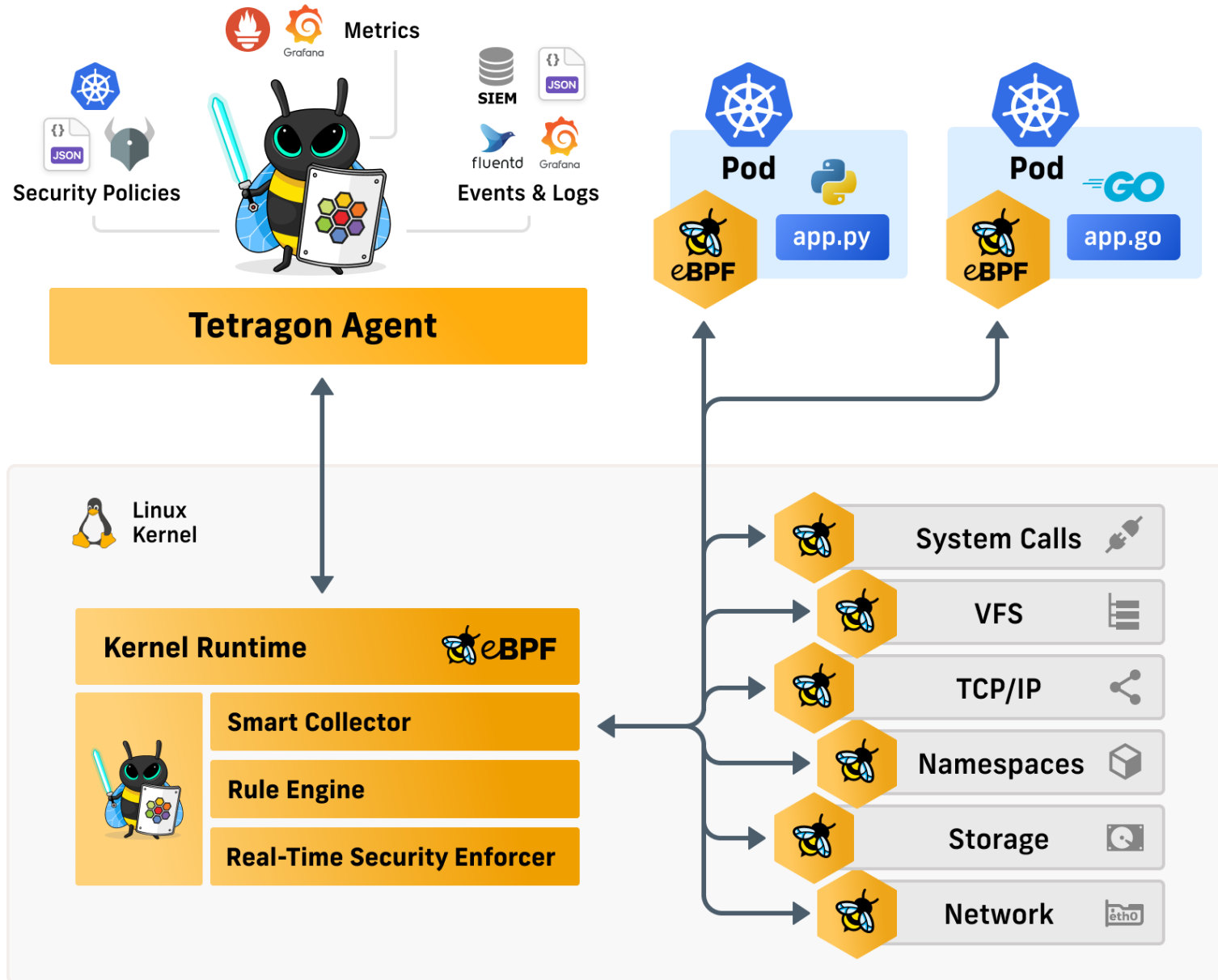
- “eBPF-based Security Observability and Runtime Enforcement”
- gives you awareness into your cluster
 - without that you won't know what is going on
- alerts you on malicious events and workloads
- real-time enforcement



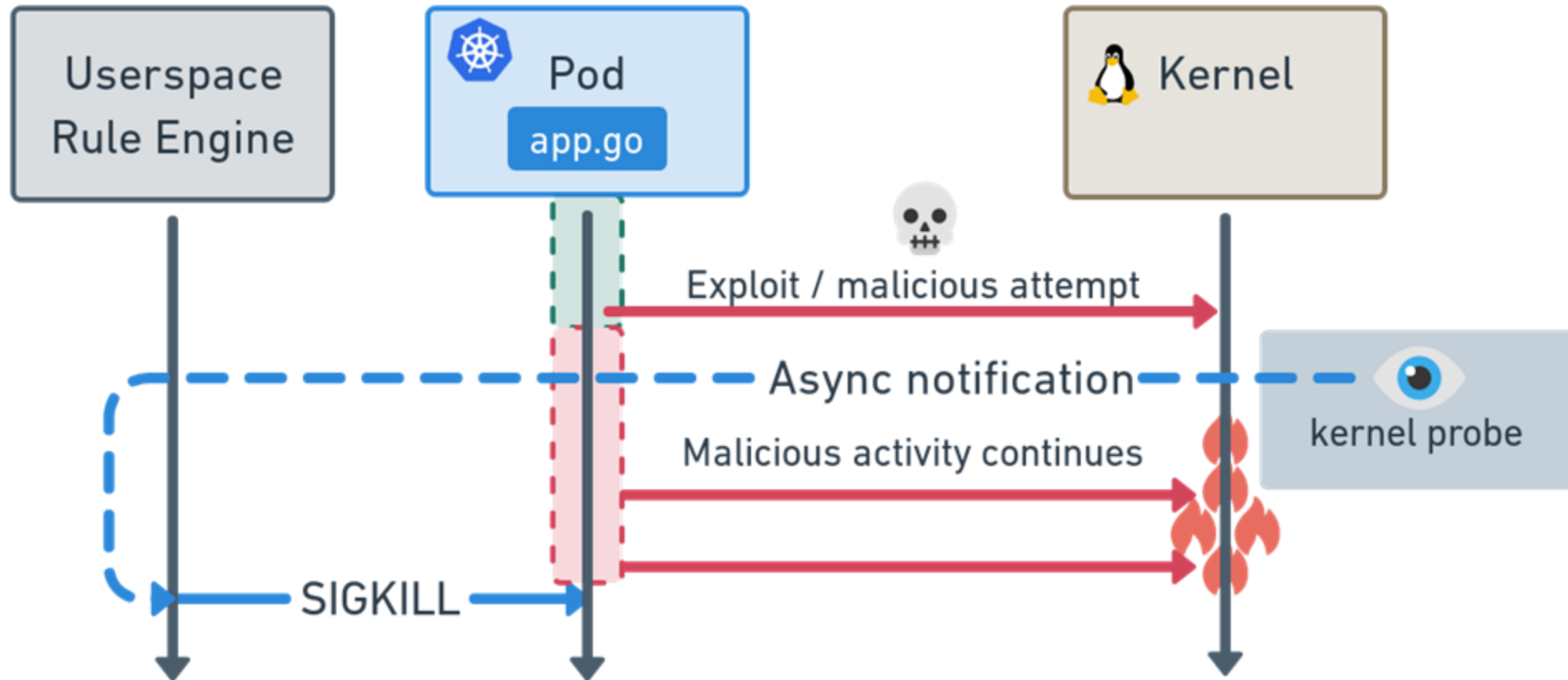
Tetragon and Kubernetes

- is Kubernetes-aware
 - understands Kubernetes identities such as namespaces, pods and so-on
- detects and can react to security-significant events, such as
 - Process execution events
 - System call activity
 - I/O activity including network & file access
- agents are running as DaemonSet on all nodes

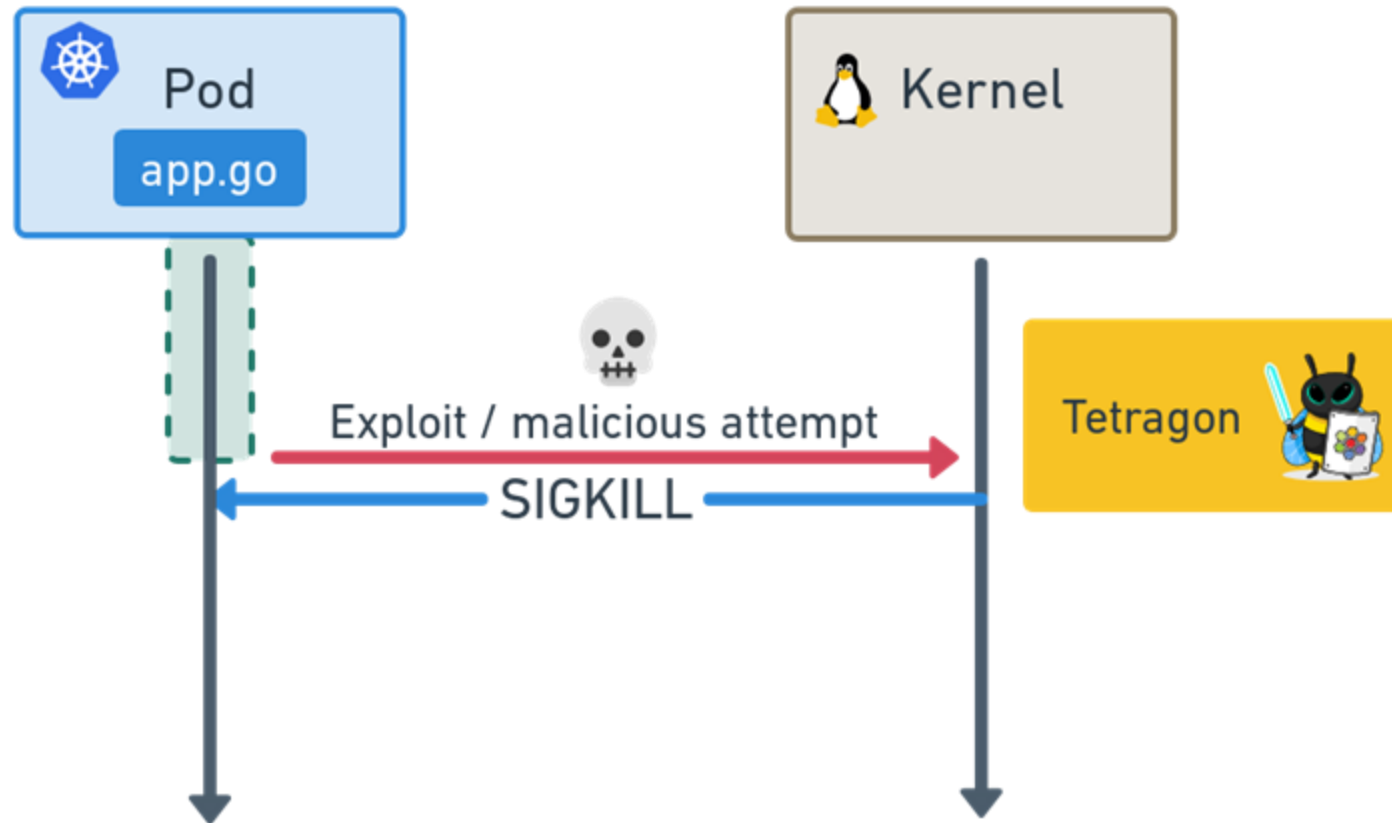
Big picture



An attack with prevention from user space



An attack with prevention via eBPF and Tetragon



Tetragon Policies

- are used to
 - extend Tetragon events
 - enforcement policies
- implemented via CRDs (Custom Resource Definitions)
- supports cluster-wide and namespaced policies
 - TracingPolicy
 - TracingPolicyNamespaced (Beta)
- allows Pod label filters via "PodSelector" (Beta)

TracingPolicy resource

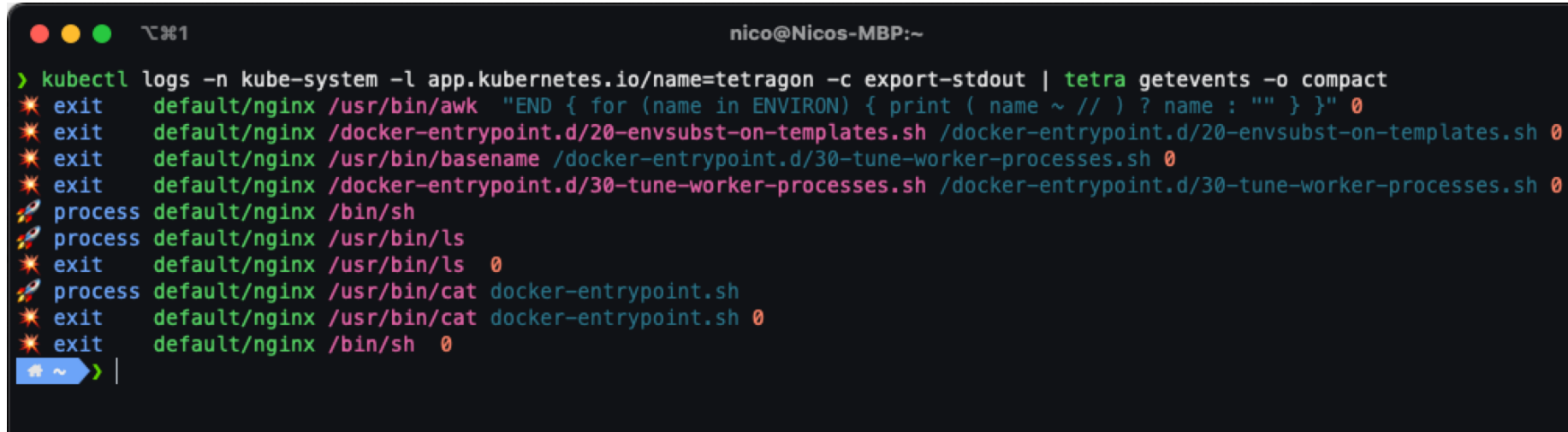
```
apiVersion: cilium.io/v1alpha1
kind: TracingPolicyNamespaced
metadata:
  name: "namespaced-policy"
  namespace: "my-namespace"
spec:
  kprobes:
    - call: "sys_write"
```

```
apiVersion: cilium.io/v1alpha1
kind: TracingPolicy
metadata:
  name: "pod-label-policy"
spec:
  podSelector:
    matchLabels:
      app: "my-app"
  kprobes:
    - call: "sys_write"
```

```
apiVersion: cilium.io/v1alpha1
kind: TracingPolicy
metadata:
  name: "cluster-wide-policy"
spec:
  kprobes:
    - call: "sys_write"
      syscall: true
      args:
        - index: 0
          type: "fd"
        - index: 1
          type: "char_buf"
          sizeArgIndex: 3
        - index: 2
          type: "size_t"
  selectors:
    - matchPIDs:
        - operator: NotIn
          followForks: true
          isNamespacePID: true
          values:
            - 0
            - 1
      matchArgs:
        - index: 0
          operator: "Prefix"
          values:
            - "/etc/passwd"
      matchActions:
        - action: Sigkill
```


tetra CLI

- `kubectl logs \`
 `-n kube-system \`
 `-l app.kubernetes.io/name=tetragon \`
 `-c export-stdout -f \`
 `| tetra getevents -o compact`
- `kubectl exec -it -n kube-system \`
 `ds/tetragon -c tetragon -- tetra getevents -o compact`



```
nico@Nicos-MBP:~  
> kubectl logs -n kube-system -l app.kubernetes.io/name=tetragon -c export-stdout | tetra getevents -o compact  
✱ exit default/nginx /usr/bin/awk "END { for (name in ENVIRON) { print ( name ~ // ) ? name : "" } }" 0  
✱ exit default/nginx /docker-entrypoint.d/20-envsubst-on-templates.sh /docker-entrypoint.d/20-envsubst-on-templates.sh 0  
✱ exit default/nginx /usr/bin/basename /docker-entrypoint.d/30-tune-worker-processes.sh 0  
✱ exit default/nginx /docker-entrypoint.d/30-tune-worker-processes.sh /docker-entrypoint.d/30-tune-worker-processes.sh 0  
✱ process default/nginx /bin/sh  
✱ process default/nginx /usr/bin/ls  
✱ exit default/nginx /usr/bin/ls 0  
✱ process default/nginx /usr/bin/cat docker-entrypoint.sh  
✱ exit default/nginx /usr/bin/cat docker-entrypoint.sh 0  
✱ exit default/nginx /bin/sh 0  
~> |
```

Demo: Getting started with Tetragon

Demo

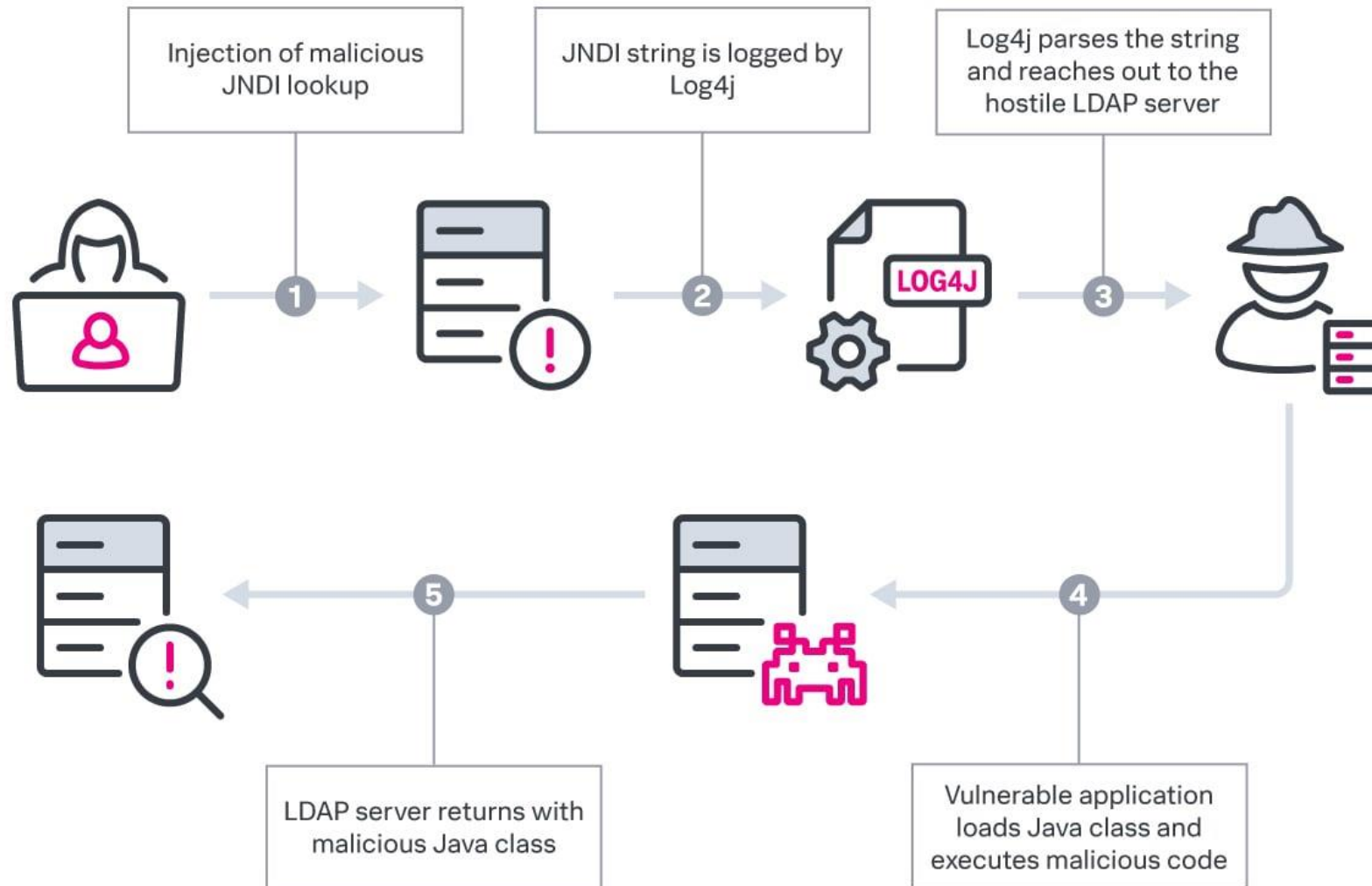
- observing with the tetra CLI
- first tracing policies

Demo: Prevent Log4Shell attack with Tetragon

Demo

- we will inject into a Pod via Log4Shell (Reverse shell)
- then observe the process execution
- and finally block it

Log4Shell



Demo: Awareness and Observability

Demo

- higher awareness and observability
- integrate Tetragon with Prometheus and Grafana

Links & Getting started

- <https://github.com/whiteducksoftware/cilium-aks-workshop-day>
- <https://github.com/cilium/tetragon>
 - <https://github.com/cilium/tetragon/tree/main/docs>
 - <https://github.com/cilium/tetragon/tree/main/examples/tracingpolicy>
- <https://tetragon.cilium.io/docs>
- <https://cilium.io/use-cases/runtime-enforcement>

Questions?



Philip Welz
(Senior DevOps & Kubernetes Engineer,
Azure MVP)

☎ +49 8031 230159-0
✉ Philip.welz@whiteduck.de
🐦 [@philip_welz](https://twitter.com/philip_welz)
in www.linkedin.com/in/philip-welz



Nico Meisenzahl
(Head of DevOps Consulting & Operations,
Cloud Solution Architect)

☎ +49 8031 230159-0
✉ nico.meisenzahl@whiteduck.de
🐦 [@nmeisenzahl](https://twitter.com/nmeisenzahl)
in www.linkedin.com/in/nicomeisenzahl



Thank you!