German OWASP Day 2025

German OWASP Day 2025

Continuous Vulnerability Scanning with OWASP secureCodeBox

Jannik Hollenbach

iteratec

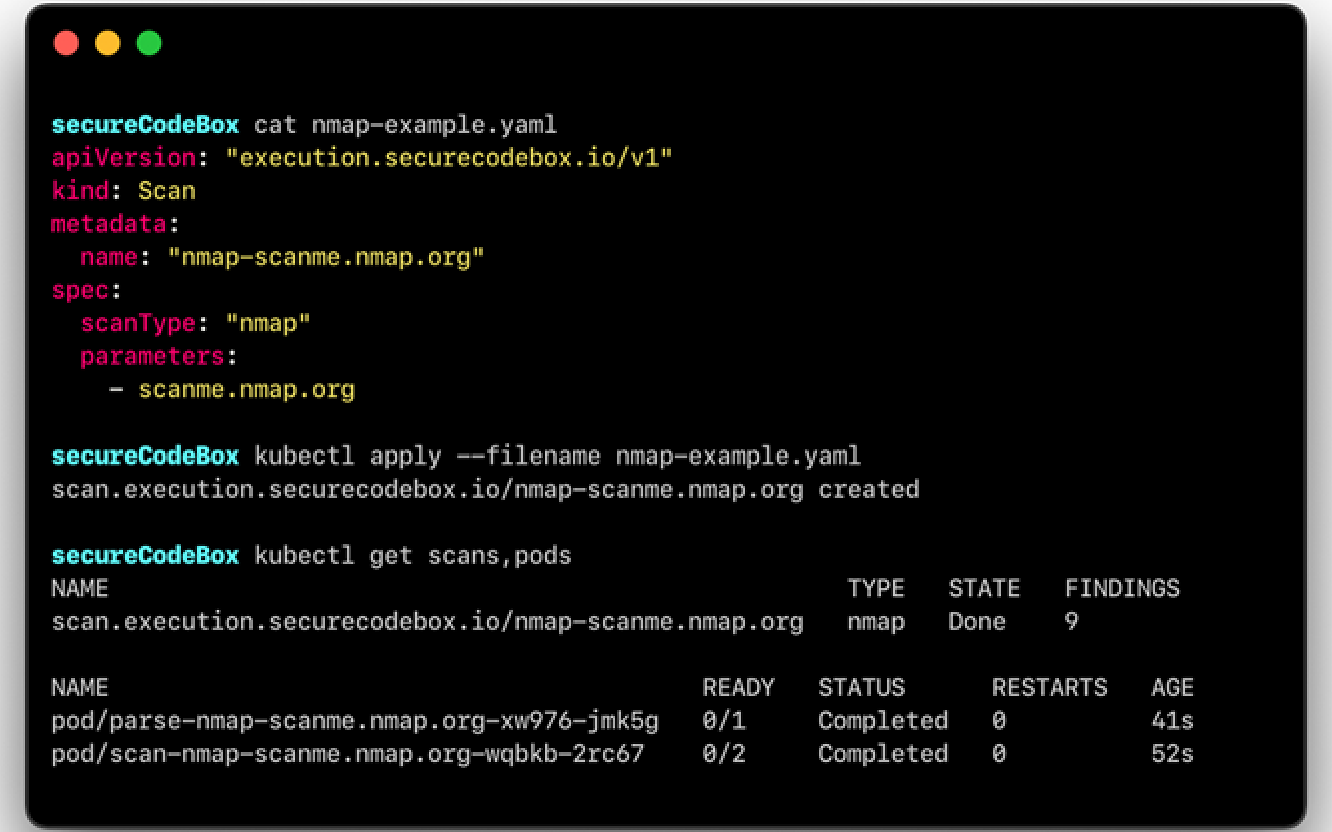
- ❑ Jannik Hollenbach
- ❑ Living in **Hamburg**
- ❑ **Software Security Engineer** at **iteratec**
- ❑ Project Lead @ **OWASP secureCodeBox & JuiceShop**

What is the OWASP secureCodeBox?

Orchestration

- OWASP Lab Project
- **Headless Scan Orchestration Engine**
- Executing **open-source scanning** tools on any **Kubernetes** cluster
- About 20 scanner integrations are maintained by the secureCodeBox team
  - Discovery: Nmap, Subfinder
  - DAST’isch: Nuclei, ZAP, ssh-audit, ncrack
  - SAST’isch: Semgrep, Trivy, gitleaks
- Build in integrations to send scan results to your already existing finding management

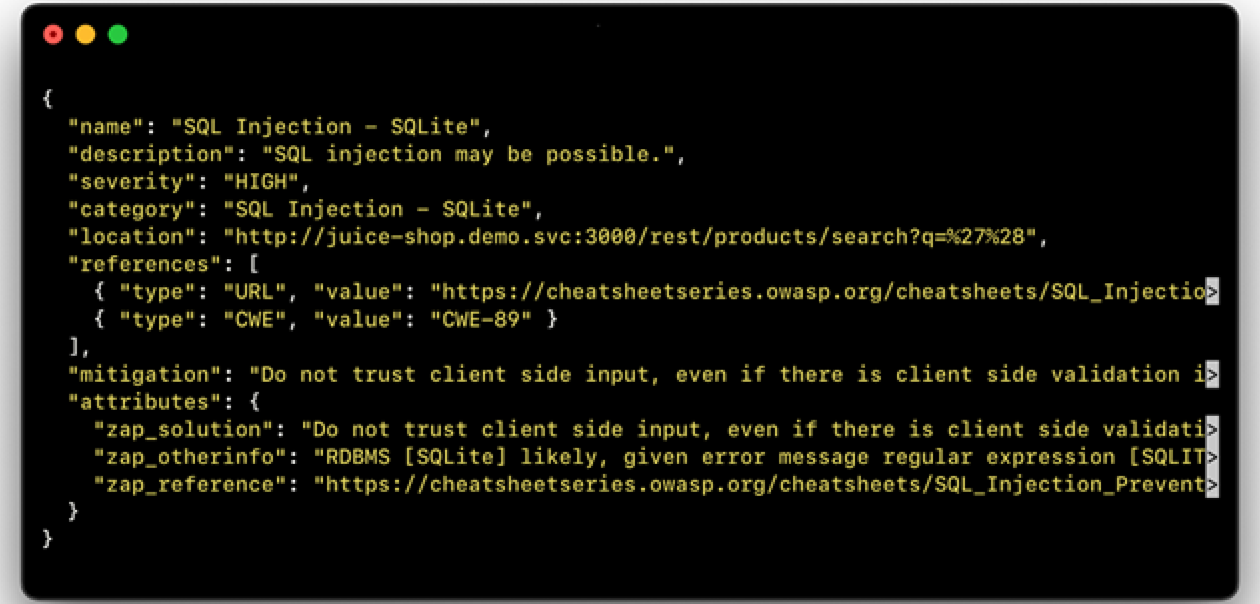
https://github.com/secureCodeBox



```
secureCodeBox cat nmap-example.yaml
apiVersion: "execution.securecodebox.io/v1"
kind: Scan
metadata:
  name: "nmap-scanme.nmap.org"
spec:
  scanType: "nmap"
  parameters:
    - scanme.nmap.org

secureCodeBox kubectl apply --filename nmap-example.yaml
scan.execution.securecodebox.io/nmap-scanme.nmap.org created

secureCodeBox kubectl get scans,pods
NAME                                                TYPE   STATE   FINDINGS
scan.execution.securecodebox.io/nmap-scanme.nmap.org   nmap   Done    9

NAME                                          READY   STATUS      RESTARTS   AGE
pod/parse-nmap-scanme.nmap.org-xw976-jmk5g    0/1     Completed   0          41s
pod/scan-nmap-scanme.nmap.org-wqbkb-2rc67     0/2     Completed   0          52s
```

What is the OWASP secureCodeBox?

Integration

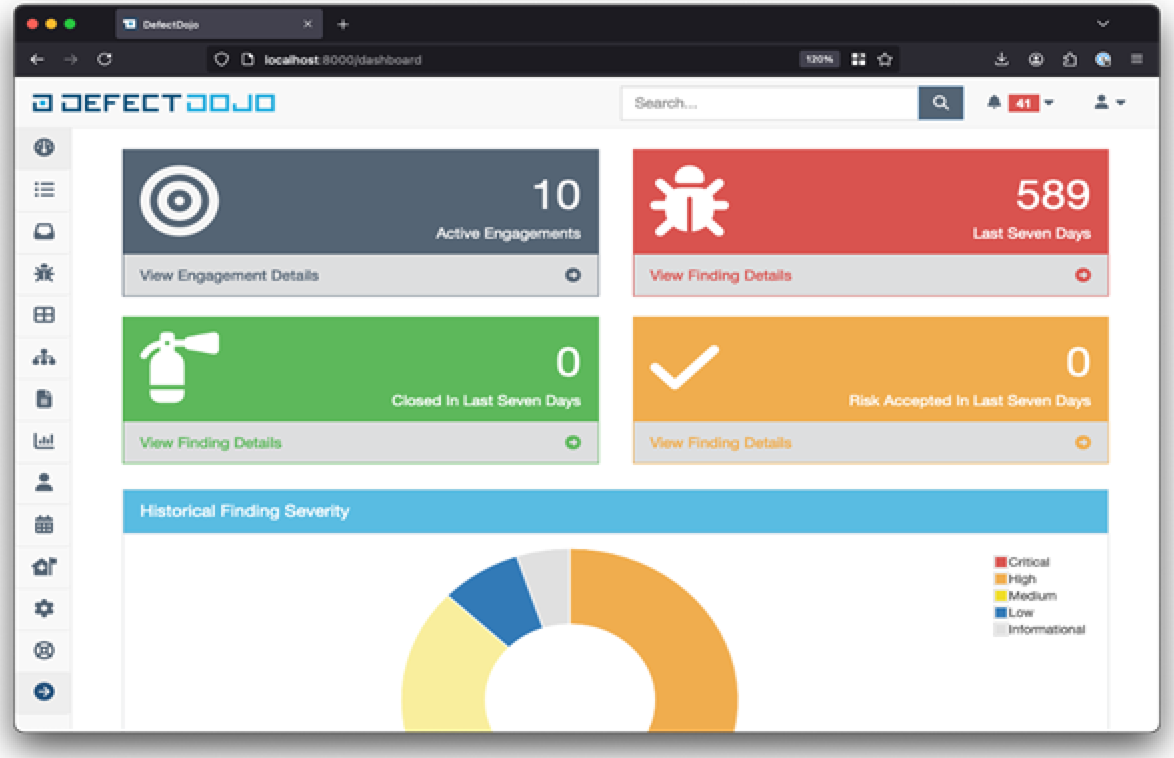


```
{
  "name": "SQL Injection - SQLite",
  "description": "SQL injection may be possible.",
  "severity": "HIGH",
  "category": "SQL Injection - SQLite",
  "location": "http://juice-shop.demo.svc:3000/rest/products/search?q=%27%28",
  "references": [
    { "type": "URL", "value": "https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injectio>
    { "type": "CWE", "value": "CWE-89" }
  ],
  "mitigation": "Do not trust client side input, even if there is client side validation i>
  "attributes": {
    "zap_solution": "Do not trust client side input, even if there is client side validati>
    "zap_otherinfo": "RDBMS [SQLite] likely, given error message regular expression [SQLIT>
    "zap_reference": "https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevent>
  }
}
```

- ❑ Findings from all scanners are translated into a **uniform JSON** format
- ❑ Each finding has a name, location, category, severity which are set for every scanner
- ❑ This allows **uniform handling** of findings. E.g. sending a Slack message for all high severity findings

What is the OWASP secureCodeBox?

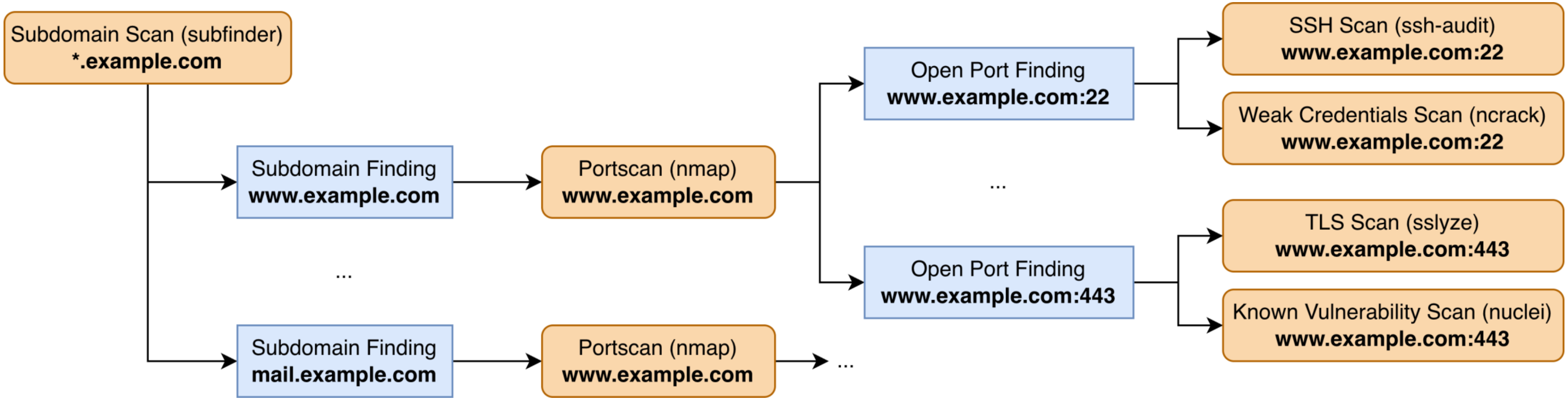
Modularity & Extendability



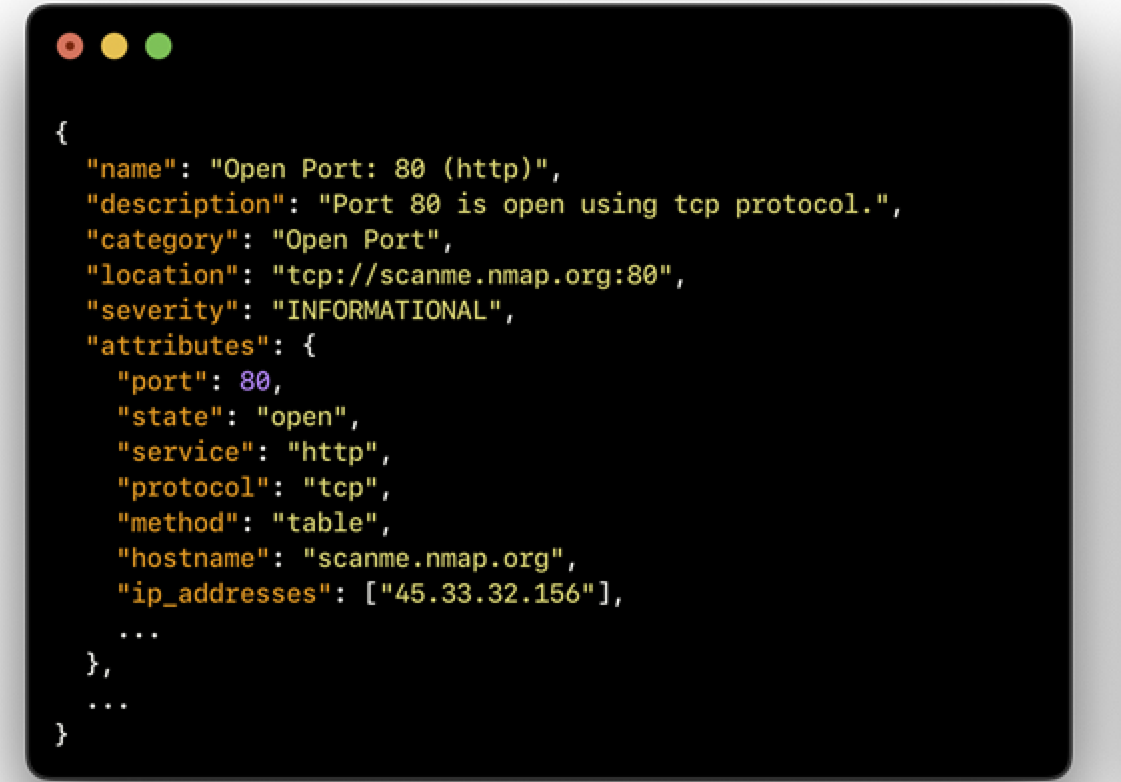
- ❑ Hooks allow to handle findings e.g. sending them to external systems
- ❑ Official Hooks for sending
  - ❑ **Findings** to:
    - ❑ OWASP DefectDojo
    - ❑ Elasticsearch / OpenSearch
  - ❑ **SBOMs** to:
    - ❑ OWASP DependencyTrack
  - ❑ **Notifications** to:
    - ❑ Slack
    - ❑ Microsoft Teams
    - ❑ E-Mail

Scanning entire in-/external Attack Surfaces

Using "Cascading Scans"

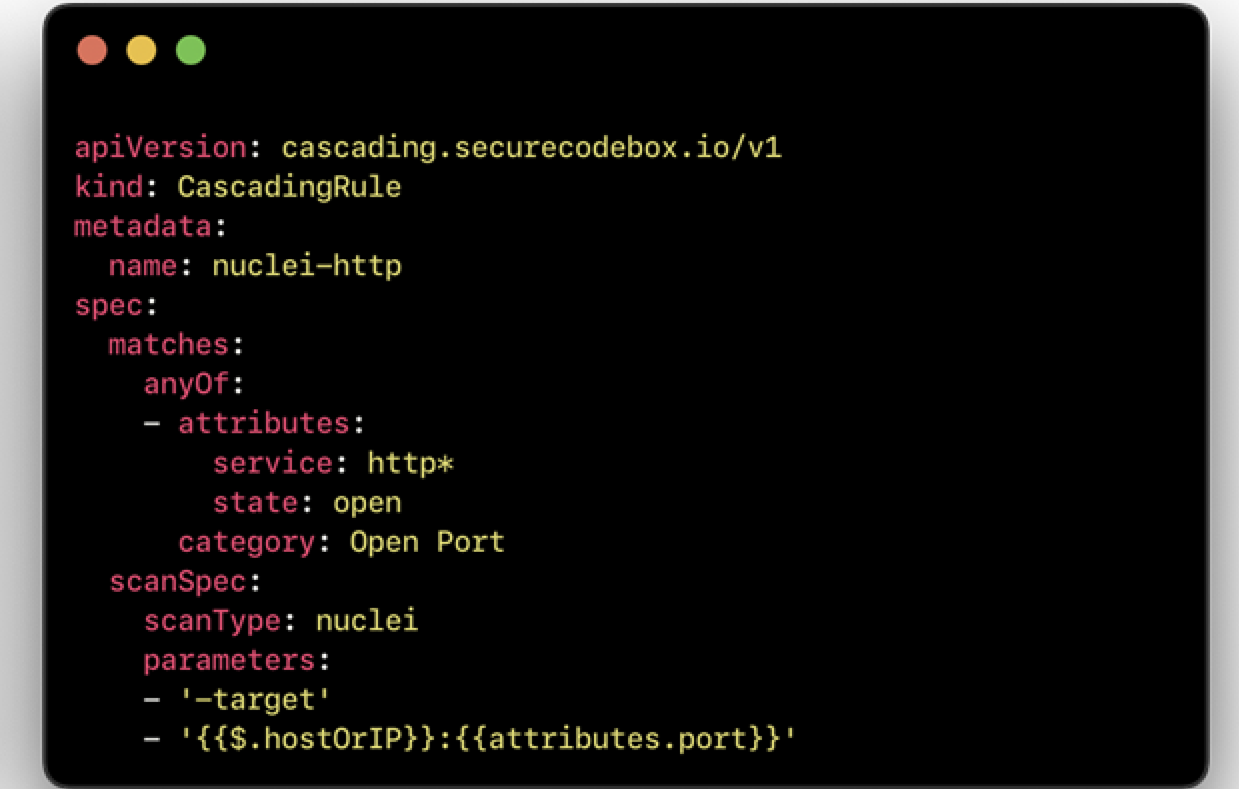


Finding



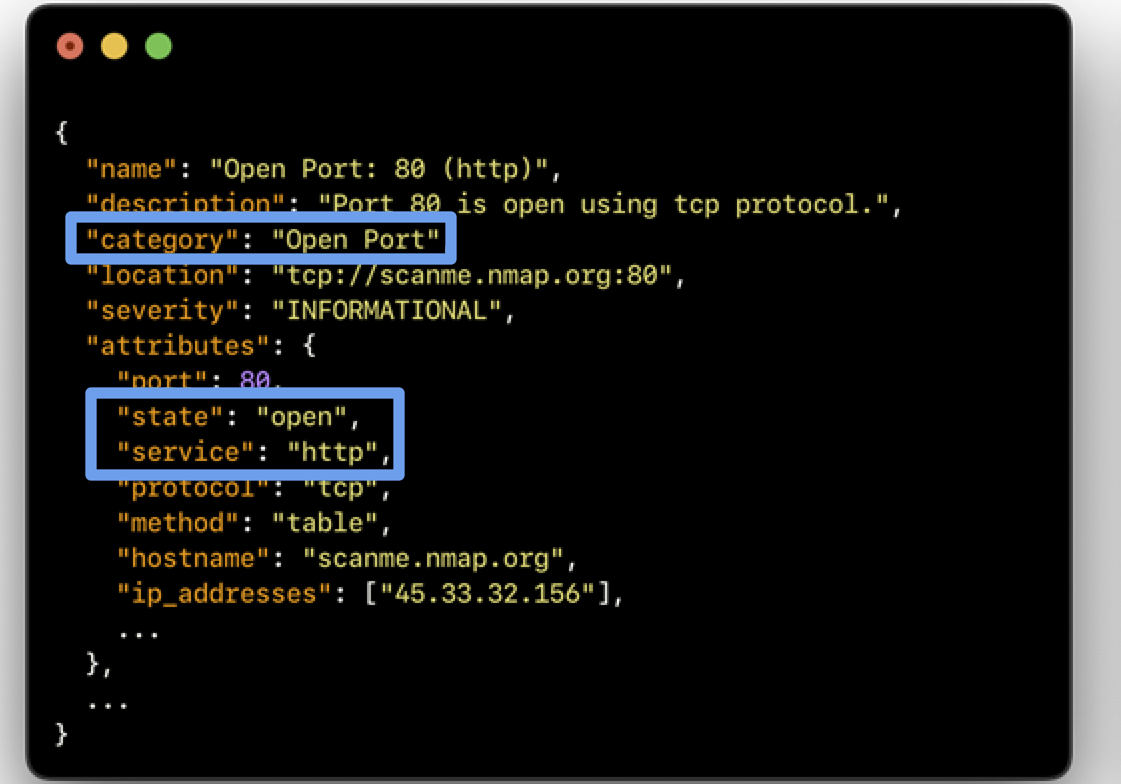
```
{
  "name": "Open Port: 80 (http)",
  "description": "Port 80 is open using tcp protocol.",
  "category": "Open Port",
  "location": "tcp://scanme.nmap.org:80",
  "severity": "INFORMATIONAL",
  "attributes": {
    "port": 80,
    "state": "open",
    "service": "http",
    "protocol": "tcp",
    "method": "table",
    "hostname": "scanme.nmap.org",
    "ip_addresses": ["45.33.32.156"],
    ...
  },
  ...
}
```

Cascading Rule



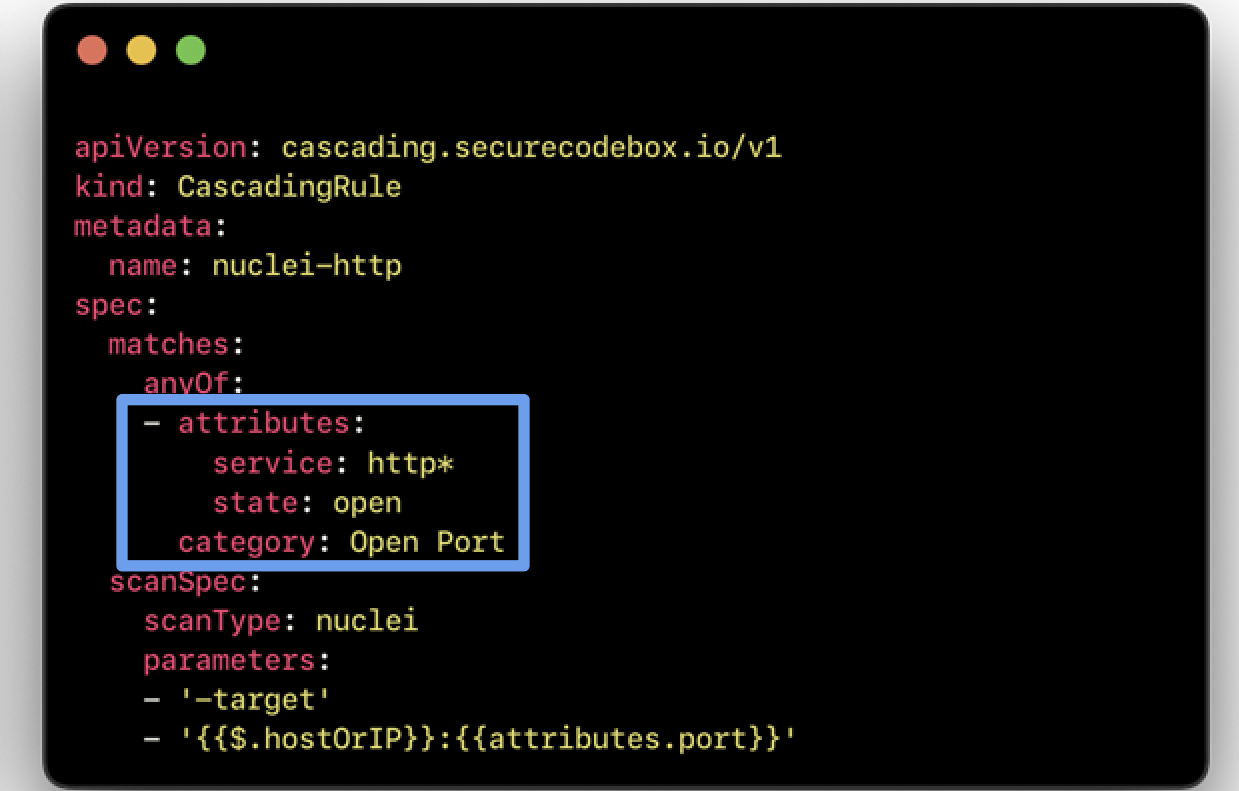
```
apiVersion: cascading.securecodebox.io/v1
kind: CascadingRule
metadata:
  name: nuclei-http
spec:
  matches:
    anyOf:
    - attributes:
        service: http*
        state: open
      category: Open Port
  scanSpec:
    scanType: nuclei
    parameters:
    - '-target'
    - '{{$.hostOrIP}}:{{attributes.port}}'
```

Finding



```
{
  "name": "Open Port: 80 (http)",
  "description": "Port 80 is open using tcp protocol.",
  "category": "Open Port"
  "location": "tcp://scanme.nmap.org:80",
  "severity": "INFORMATIONAL",
  "attributes": {
    "port": 80,
    "state": "open",
    "service": "http",
    "protocol": "tcp",
    "method": "table",
    "hostname": "scanme.nmap.org",
    "ip_addresses": ["45.33.32.156"],
    ...
  },
  ...
}
```

Cascading Rule



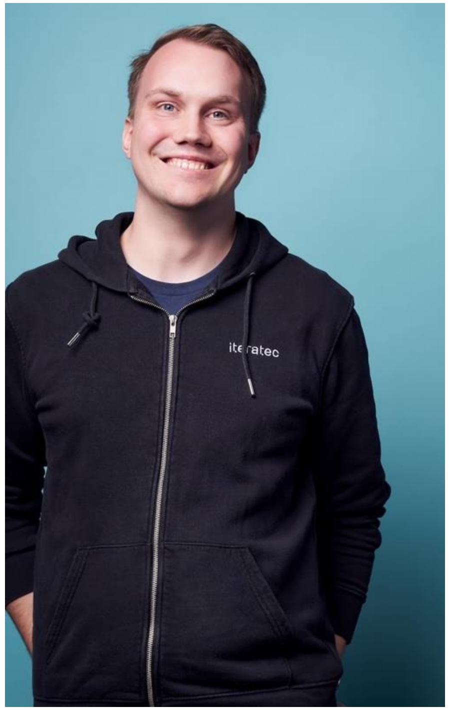
```
apiVersion: cascading.securecodebox.io/v1
kind: CascadingRule
metadata:
  name: nuclei-http
spec:
  matches:
    anyOf:
    - attributes:
        service: http*
        state: open
      category: Open Port
  scanSpec:
    scanType: nuclei
    parameters:
    - '-target'
    - '{{$.hostOrIP}}:{{attributes.port}}'
```

Demo 🤞

Scanning Software in Kubernetes Clusters

Using “Kubernetes AutoDiscovery”

- The AutoDiscovery is an optional component in the secureCodeBox
- „Watches“ the cluster for „scannable“ resources and then starts scans for them.
- Currently supported:
  - **Pods**: Automatically start container image scans for newly created containers. E.g. for **trivy**
  - **Services**: Automatically start network scans for updated network services. E.g. for **ZAP** or **Nuclei**
- Automatically starts new scans once a service is updated.



Jannik Hollenbach

Software Security Engineer

Mail: jannik.hollenbach@owasp.org
Mastadon: infosec.exchange/@jannik

German OWASP Day 2025

THANK YOU!