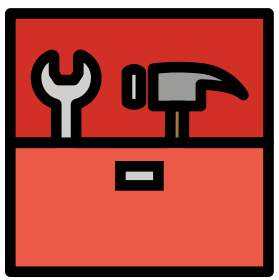
Continuous Security Testing with OWASP secureCodeBox in Kubernetes

DSOMM / JuiceShop User Day
OWASP Global AppSec San Francisco 2024

Jannik Hollenbach

What is the OWASP secureCodeBox?

What is it for?

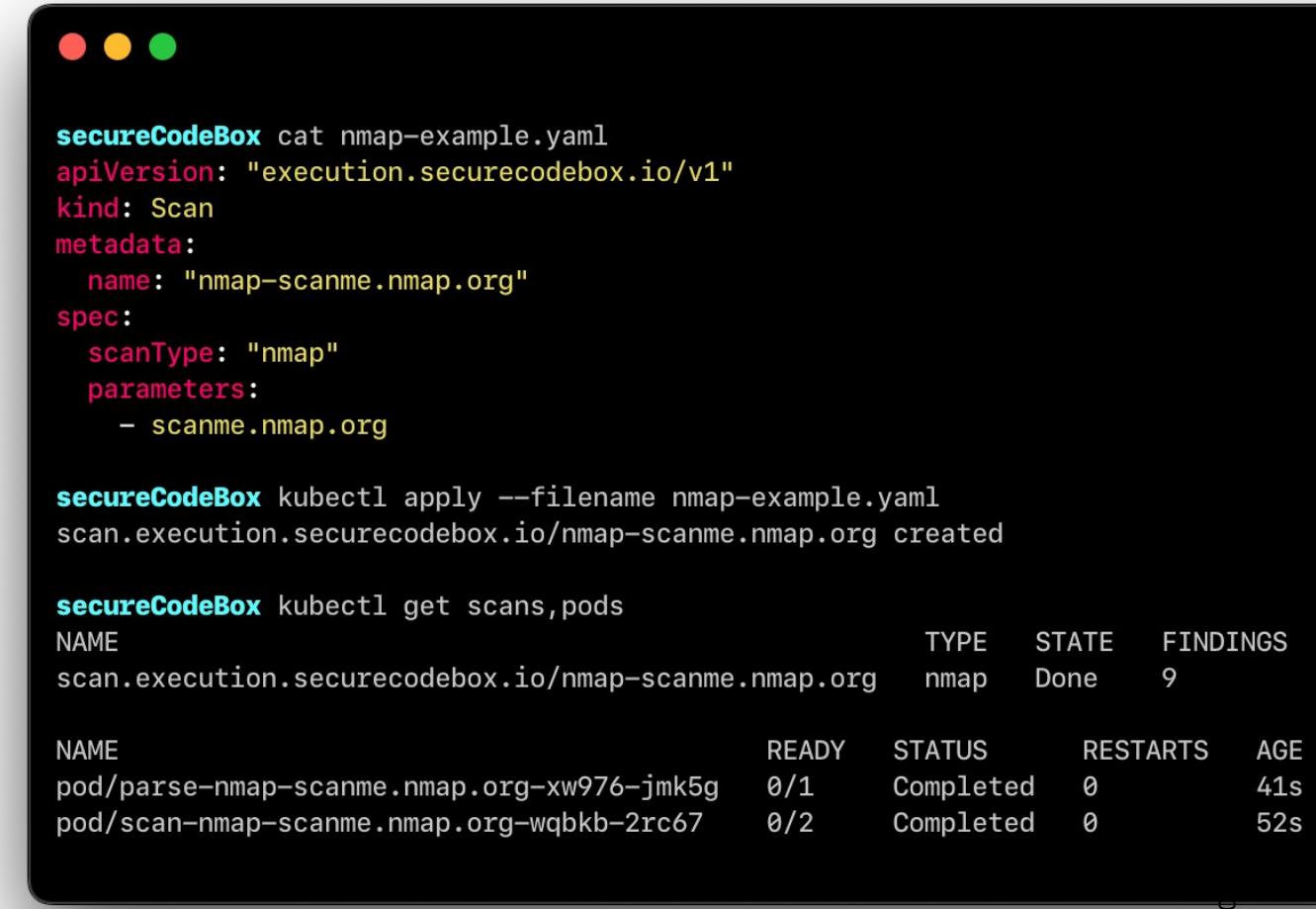


- Open Source Project to help automate security scanning tools
- Supports both 20+ Dynamic (DAST) and Static (SAST) Scanning tools out of the box
  - nmap, nuclei, ZAP… for DAST
  - Trivy, Semgrep, gitleaks… for SAST

What is the OWASP secureCodeBox?

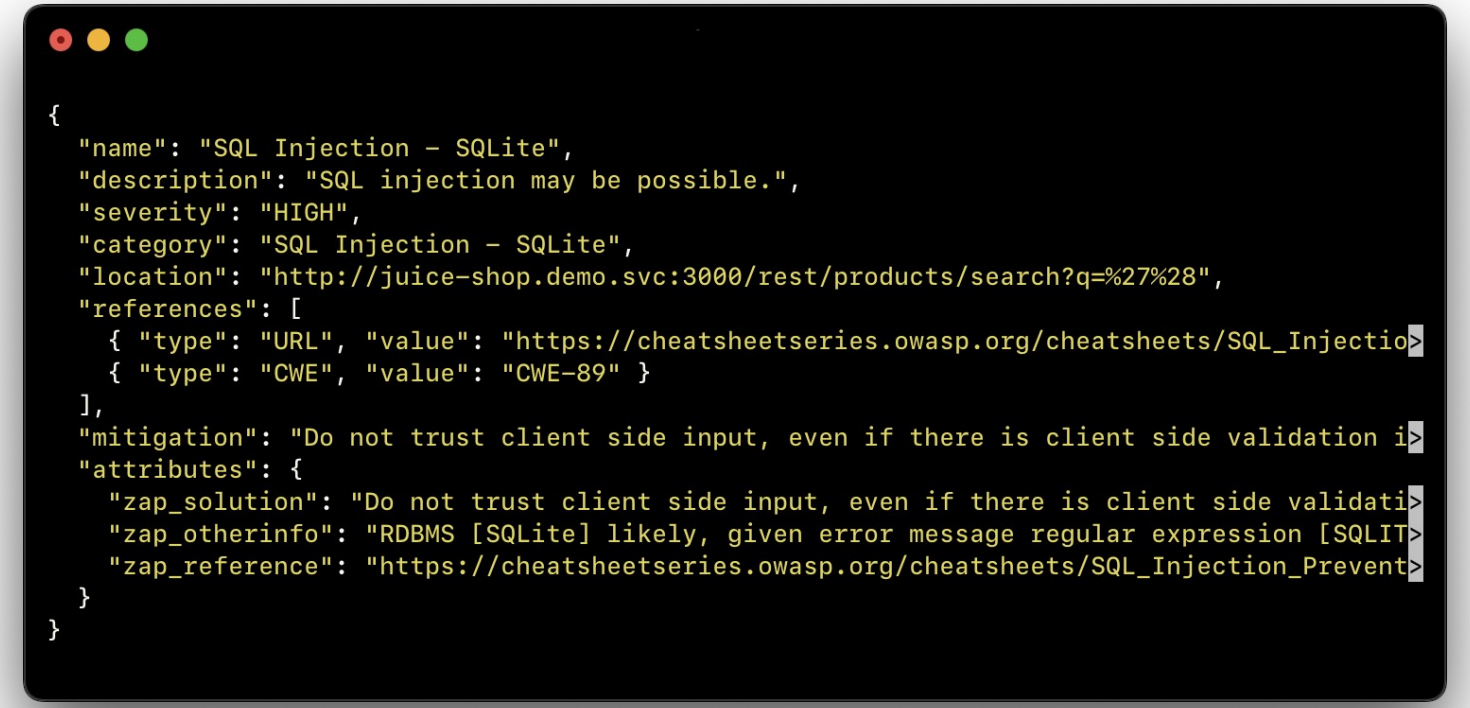
Orchestration

- **Kubernetes Operator** to manage security scanning tools via Custom Resource inside of Kubernetes
- **Scan** CRD to run Scans on the Cluster
- Scans are using a **ScanType** CRD which describes how to turn the scan into a job
  - 20+ scanner integrations are maintained by the secureCodeBox team, installable via helm



What is the OWASP secureCodeBox?

Integration

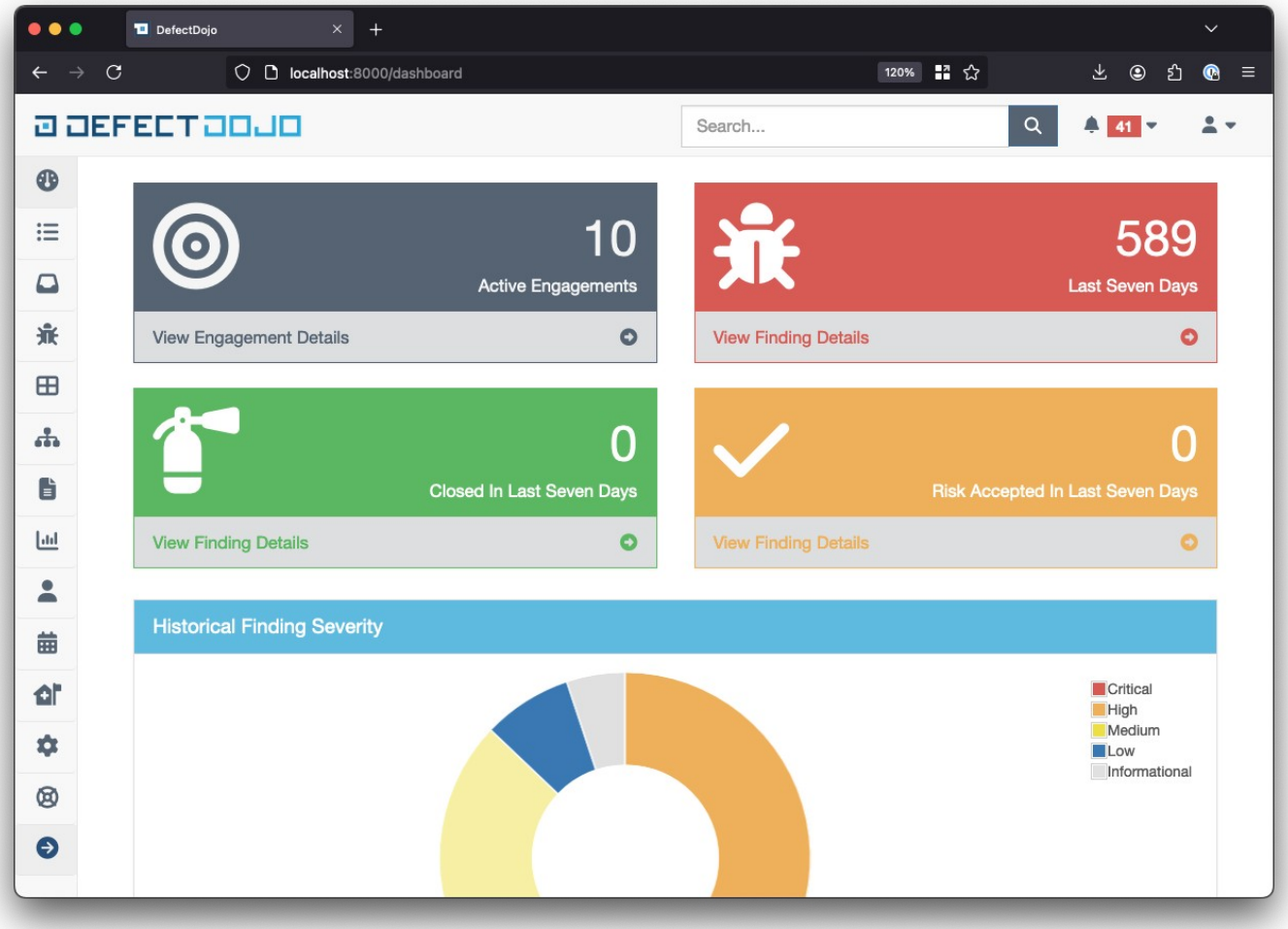


```
{
  "name": "SQL Injection - SQLite",
  "description": "SQL injection may be possible.",
  "severity": "HIGH",
  "category": "SQL Injection - SQLite",
  "location": "http://juice-shop.demo.svc:3000/rest/products/search?q=%27%28",
  "references": [
    { "type": "URL", "value": "https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injectio>
    { "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 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

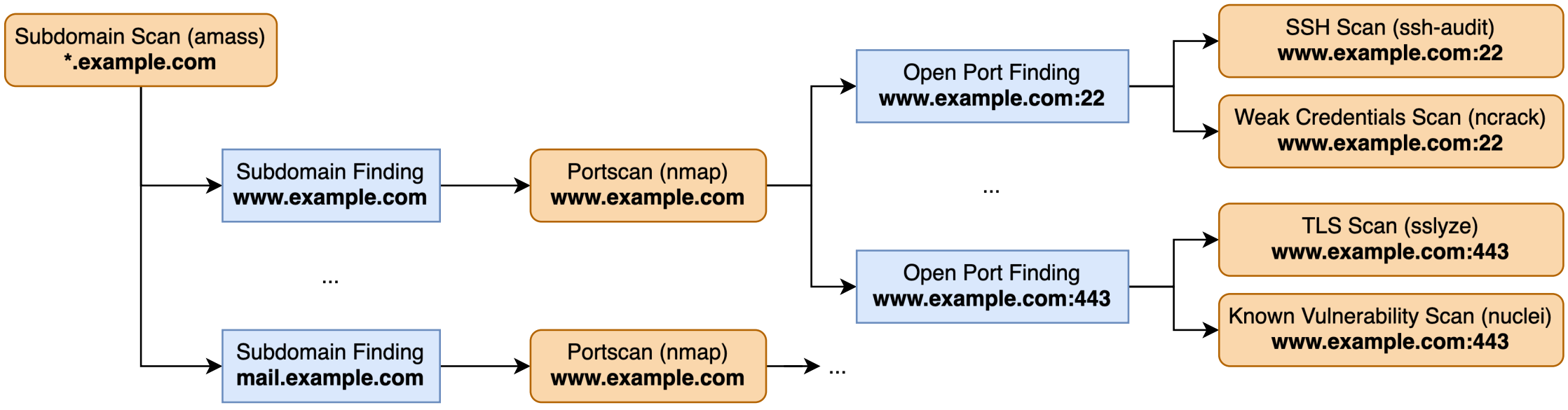


- Hooks allow to handle findings and automatically send them to external systems
- Official Hooks for sending
  - Findings to:
    - OWASP DefectDojo
    - Elastic Stack
  - SBOMs to:
    - OWASP DependencyTrack
  - Notifications to:
    - Slack
    - MS Teams
    - Email

secureCodeBox techniques to use to scan
entire Networks / Cluster / Organisations

#1: Scanning the external Attack Surface of Company

Using the **CascadingScans** Hook: Automatically starting more detailed scans for identified targets



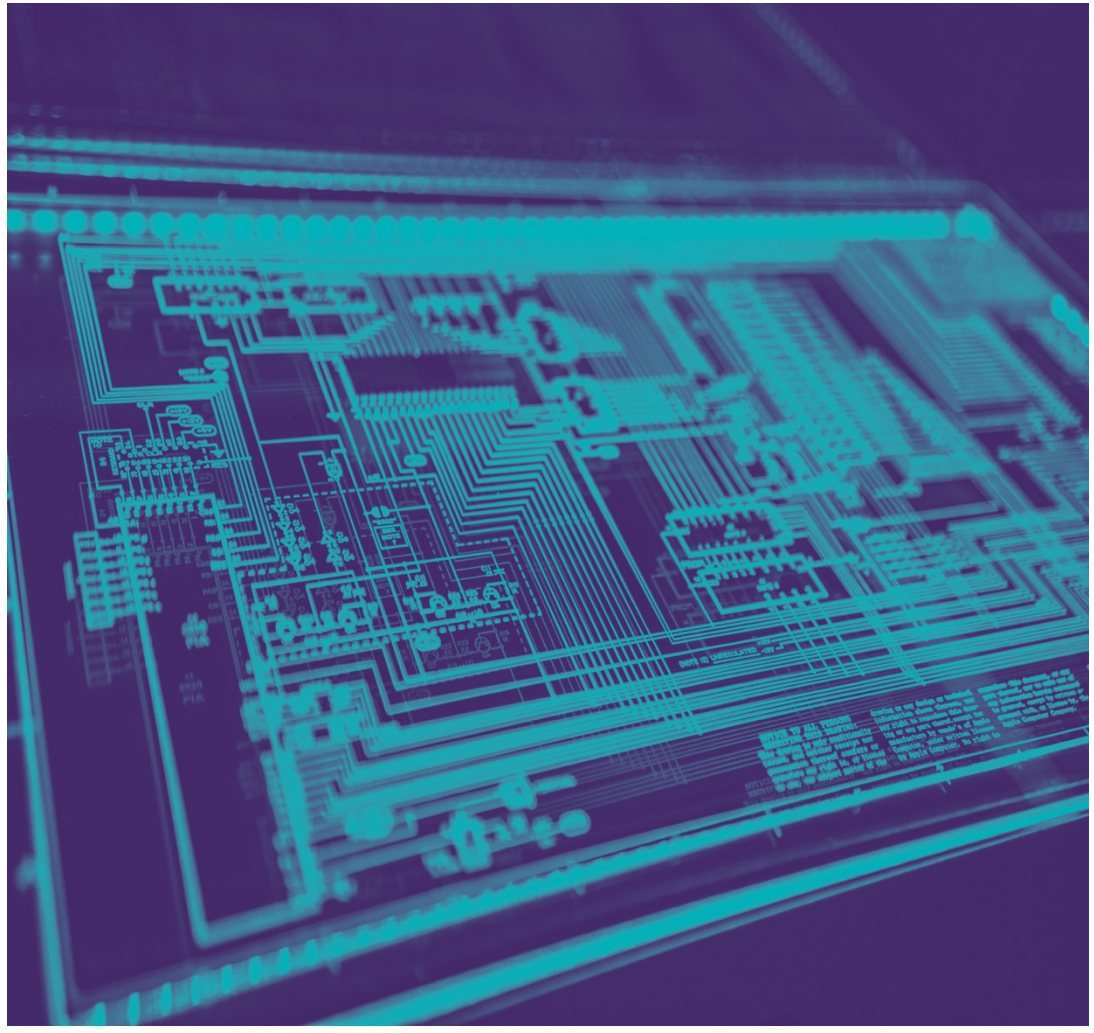
https://www.securecodebox.io/docs/how-tos/scanning-networks

#2: Scanning Software Deployed to Kubernetes

AutoDiscovery

- The AutoDiscovery is a optional component in the secureCodeBox
- It „watches“ the cluster for „scannable“ resources and then starts scans for them.
- E.g. when a container is started the AutoDiscovery can directly start a trivy scan for the underlying image
  - Works for updated deployments too, e.g. when updating the image tag of a deployment

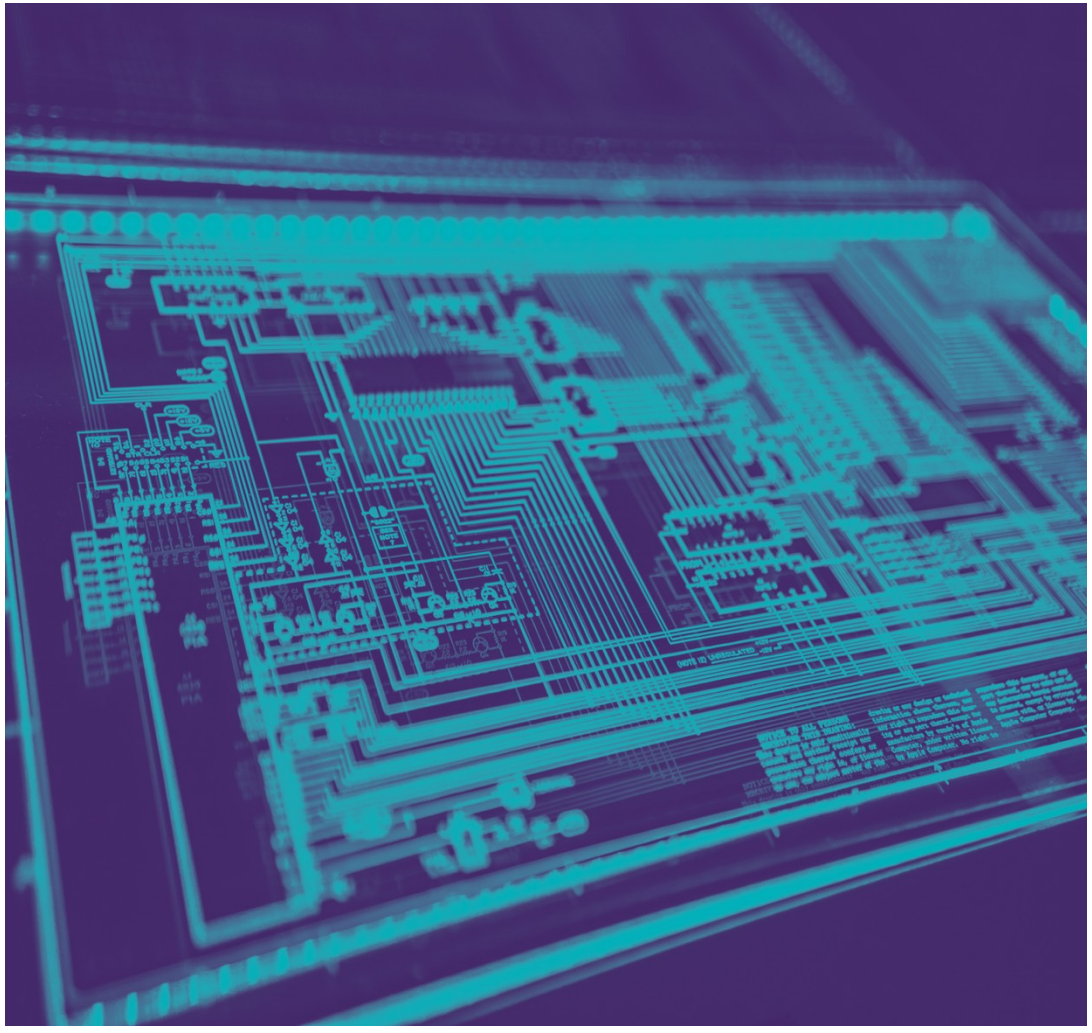
https://www.securecodebox.io/docs/how-tos/autodiscovery



#2: Scanning Software Deployed to Kubernetes

AutoDiscovery

- Which scans are triggered can be configured.
- Default Config:
  - Trivy scans for container images
  - ZAP scans for services with http(s) ports



https://www.securecodebox.io/docs/how-tos/autodiscovery