The Insider Threat

Third-Party Applications in Your Cluster

Introducing: These Two Guys

Dagan Henderson

(RAFT)

techdagan

dagan

Will Kline

DARK WOLF SOLUTIONS

Third-Party Applications

Why we love them. The threat they pose.

The Glorious Third-Party Application

- Service Meshes
- CSI Drivers
- CNI Drivers
- Admission Controllers

- Continuous Delivery Agents
- Metric Scrapers & Visualizers
- Log Forwarders
- Database Engines

- … Your Base Containers
- … Kubernetes

When “Their” Code Is Vulnerable …

Image Credit: Malaymukherjee, CC BY-SA 4.0, via Wikimedia Commons

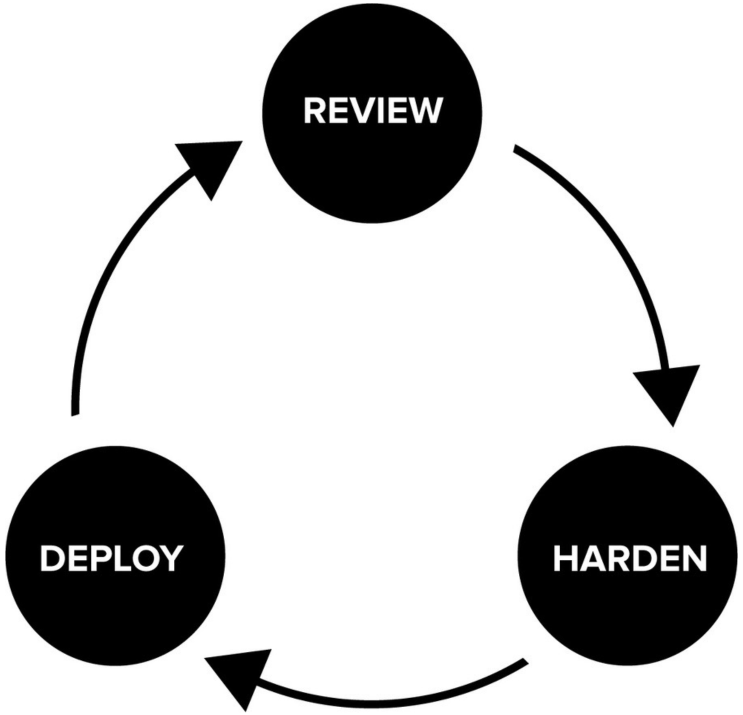
SHORT CUT OF DEF CON DEMO:
Cluster Takeover via 3rd Party Apps

When “Their” Code Is Vulnerable …

Image Credit: Malaymukherjee, CC BY-SA 4.0, via Wikimedia Commons

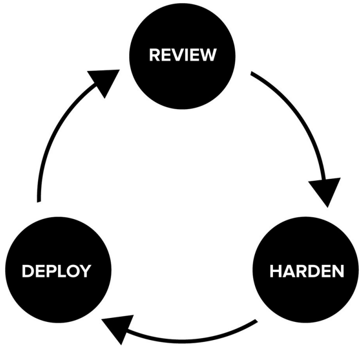
…Your Clusters Are Vulnerable

Third-Party Applications the *Right Way*™



Evaluating Third-Party Applications

Solve your common problems without creating a new ones



Consider the Project, Not the Point In Time

- Don’t think about releases. Think about projects.
- Every project has a release cadence. Some more regular than others.
- A scan today won’t find a vulnerability published tomorrow.
- Vulnerabilities take time to patch.

Answer These Questions

- Who are the maintainers and how is the project licensed?
- Does the project practice good hygiene?
- Does it have a security policy and publish security advisories?
- Do releases include notes? Are breaking changes called out?
- Are configuration parameters documented?
- Is there specific guidance for secure deployments?

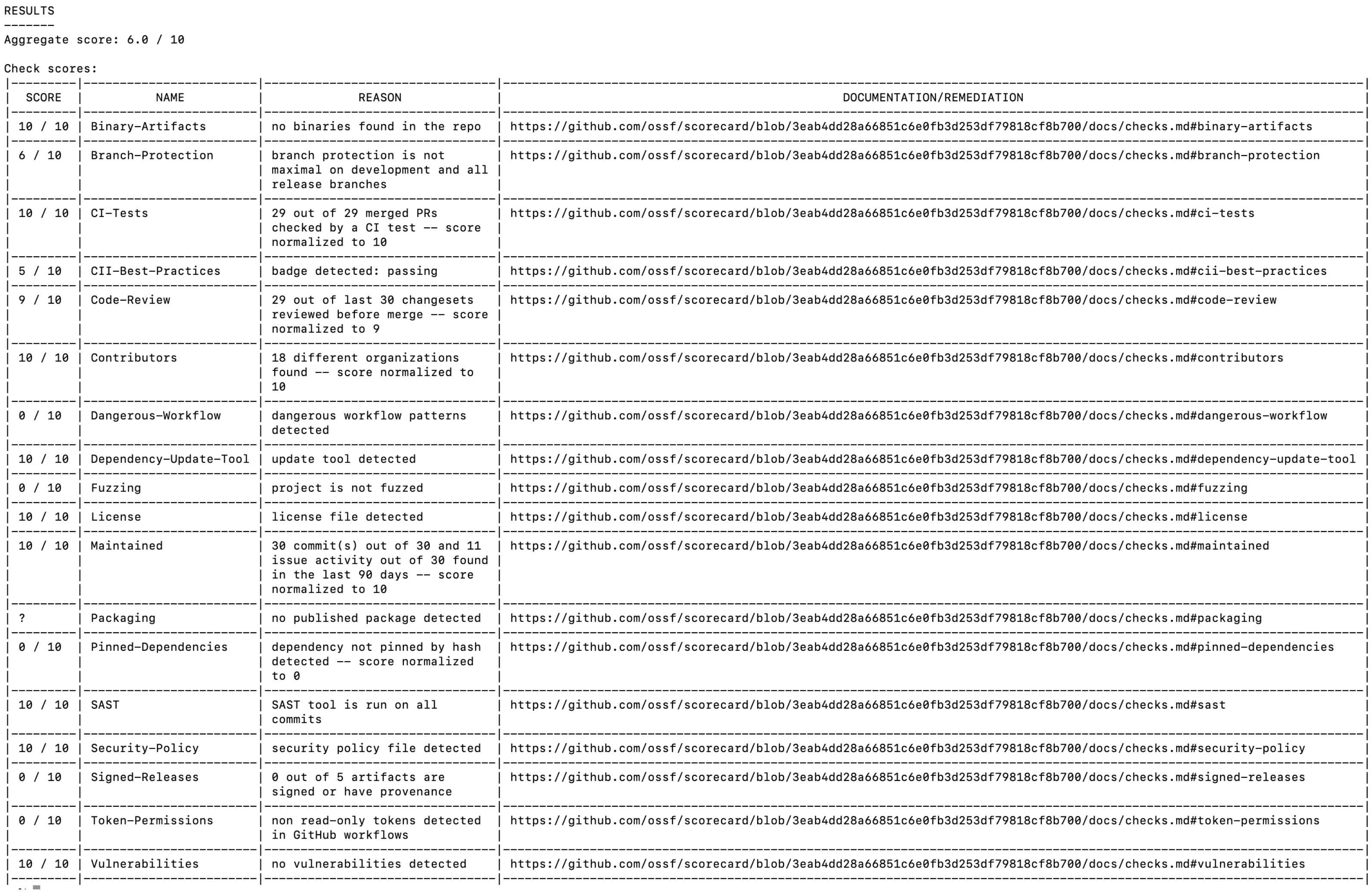
Walkthrough: We Need Some Secrets

- Source of truth for organization secrets is HashiCorp Vault
- Multiple clusters, multiple tenants
- Identified several options:
  - Sealed Secrets
  - Vault Secret Operator
  - External Secrets
  - SOPS
  - Vault Kubernetes Injector
  - Secrets Store CSI Driver

Walkthrough: OSSF Scorecards

- Open Source Security Foundation’s Scorecards automate a lot of work
- Automated evaluation of:
  - Vulnerable code
  - Build Hygiene
  - Code Hygiene
  - Maintenance Practices
  - Continuous Testing Practices

Walkthrough: External Secrets Scorecard



```
RESULTS
-------
Aggregate score: 6.0 / 10

Check scores:
|---------|------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
|  SCORE  |          NAME          |             REASON             |                                              DOCUMENTATION/REMEDIATION                                                |
|---------|------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 10 / 10 | Binary-Artifacts       | no binaries found in the repo  | https://github.com/ossf/scorecard/blob/3eab4dd28a66851c6e0fb3d253df79818cf8b700/docs/checks.md#binary-artifacts       |
|---------|------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 6 / 10  | Branch-Protection      | branch protection is not       | https://github.com/ossf/scorecard/blob/3eab4dd28a66851c6e0fb3d253df79818cf8b700/docs/checks.md#branch-protection      |
|         |                        | maximal on development and all |                                                                                                                       |
|         |                        | release branches               |                                                                                                                       |
|---------|------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 10 / 10 | CI-Tests               | 29 out of 29 merged PRs        | https://github.com/ossf/scorecard/blob/3eab4dd28a66851c6e0fb3d253df79818cf8b700/docs/checks.md#ci-tests               |
|         |                        | checked by a CI test -- score  |                                                                                                                       |
|         |                        | normalized to 10               |                                                                                                                       |
|---------|------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 5 / 10  | CII-Best-Practices     | badge detected: passing        | https://github.com/ossf/scorecard/blob/3eab4dd28a66851c6e0fb3d253df79818cf8b700/docs/checks.md#cii-best-practices     |
|---------|------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 9 / 10  | Code-Review            | 29 out of last 30 changesets   | https://github.com/ossf/scorecard/blob/3eab4dd28a66851c6e0fb3d253df79818cf8b700/docs/checks.md#code-review            |
|         |                        | reviewed before merge -- score |                                                                                                                       |
|         |                        | normalized to 9                |                                                                                                                       |
|---------|------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 10 / 10 | Contributors           | 18 different organizations     | https://github.com/ossf/scorecard/blob/3eab4dd28a66851c6e0fb3d253df79818cf8b700/docs/checks.md#contributors           |
|         |                        | found -- score normalized to   |                                                                                                                       |
|         |                        | 10                             |                                                                                                                       |
|---------|------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 0 / 10  | Dangerous-Workflow     | dangerous workflow patterns    | https://github.com/ossf/scorecard/blob/3eab4dd28a66851c6e0fb3d253df79818cf8b700/docs/checks.md#dangerous-workflow     |
|         |                        | detected                       |                                                                                                                       |
|---------|------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 10 / 10 | Dependency-Update-Tool | update tool detected           | https://github.com/ossf/scorecard/blob/3eab4dd28a66851c6e0fb3d253df79818cf8b700/docs/checks.md#dependency-update-tool |
|---------|------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 0 / 10  | Fuzzing                | project is not fuzzed          | https://github.com/ossf/scorecard/blob/3eab4dd28a66851c6e0fb3d253df79818cf8b700/docs/checks.md#fuzzing                |
|---------|------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 10 / 10 | License                | license file detected          | https://github.com/ossf/scorecard/blob/3eab4dd28a66851c6e0fb3d253df79818cf8b700/docs/checks.md#license                |
|---------|------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 10 / 10 | Maintained             | 30 commit(s) out of 30 and 11  | https://github.com/ossf/scorecard/blob/3eab4dd28a66851c6e0fb3d253df79818cf8b700/docs/checks.md#maintained             |
|         |                        | issue activity out of 30 found |                                                                                                                       |
|         |                        | in the last 90 days -- score   |                                                                                                                       |
|         |                        | normalized to 10               |                                                                                                                       |
|---------|------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| ?       | Packaging              | no published package detected  | https://github.com/ossf/scorecard/blob/3eab4dd28a66851c6e0fb3d253df79818cf8b700/docs/checks.md#packaging              |
|---------|------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 0 / 10  | Pinned-Dependencies    | dependency not pinned by hash  | https://github.com/ossf/scorecard/blob/3eab4dd28a66851c6e0fb3d253df79818cf8b700/docs/checks.md#pinned-dependencies    |
|         |                        | detected -- score normalized   |                                                                                                                       |
|         |                        | to 0                           |                                                                                                                       |
|---------|------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 10 / 10 | SAST                   | SAST tool is run on all        | https://github.com/ossf/scorecard/blob/3eab4dd28a66851c6e0fb3d253df79818cf8b700/docs/checks.md#sast                   |
|         |                        | commits                        |                                                                                                                       |
|---------|------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 10 / 10 | Security-Policy        | security policy file detected  | https://github.com/ossf/scorecard/blob/3eab4dd28a66851c6e0fb3d253df79818cf8b700/docs/checks.md#security-policy        |
|---------|------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 0 / 10  | Signed-Releases        | 0 out of 5 artifacts are       | https://github.com/ossf/scorecard/blob/3eab4dd28a66851c6e0fb3d253df79818cf8b700/docs/checks.md#signed-releases        |
|         |                        | signed or have provenance      |                                                                                                                       |
|---------|------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 0 / 10  | Token-Permissions      | non read-only tokens detected  | https://github.com/ossf/scorecard/blob/3eab4dd28a66851c6e0fb3d253df79818cf8b700/docs/checks.md#token-permissions      |
|         |                        | in GitHub workflows            |                                                                                                                       |
|---------|------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 10 / 10 | Vulnerabilities        | no vulnerabilities detected    | https://github.com/ossf/scorecard/blob/3eab4dd28a66851c6e0fb3d253df79818cf8b700/docs/checks.md#vulnerabilities        |
|---------|------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
```

Walkthrough: External Secrets Review

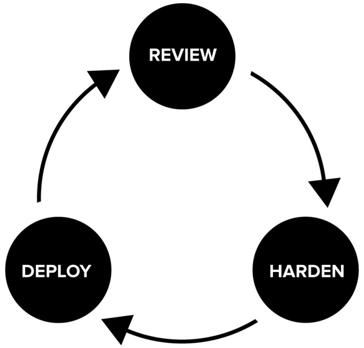
- OSSF Scorecards are super helpful, but there’s no silver bullet
- With the scorecard results in hand, also consider:
    - A security contact is published
    - A security policy is in place
    - A clear supported version policy is published
    - A deprecation policy is published
    - The project is under active development both for patches and new Kubernetes versions
    - The project’s maintainers say it is in beta development
    - The Helm chart configuration options are fully documented

Walkthrough: We Have a Candidate

- External Secrets meets our operational requirements
- A wholistic evaluation of the project is very positive
- Are we done here?

Hardening Third-Party Applications

Make a good thing even gooderer



Require Internal Ownership

- Each external applications requires internal ownership
- The owners’ efforts can scale out, but every team that deploys an application is responsible for maintaining their deployment(s)
- Teams deploying the application *must* accept their responsibility

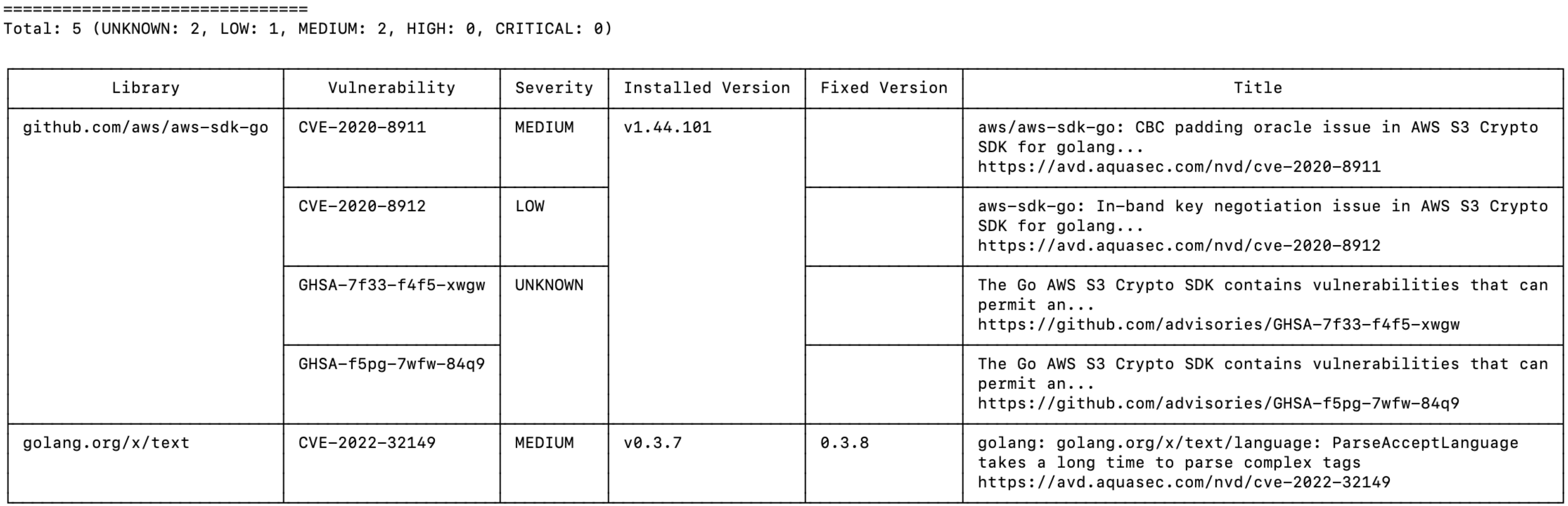
Hardening Images

- Hardened third-party images should meet the same requirements as internally developed applications
- A good starting point is:
  - Do NOT run as `root`
  - Default to your most-secure configuration
- But also, do NOT have any significant vulnerabilities

Walkthrough: Scanning With Trivy

- Aqua Security's Trivy scanner is the open-source scanner hat trick
  - Scans for OS and language-specific dependencies (including Distroless)
  - Scans for secrets (e.g., SSH keys, AWS Credentials, etc.)
  - Scans for misconfigurations, including Kubernetes manifests

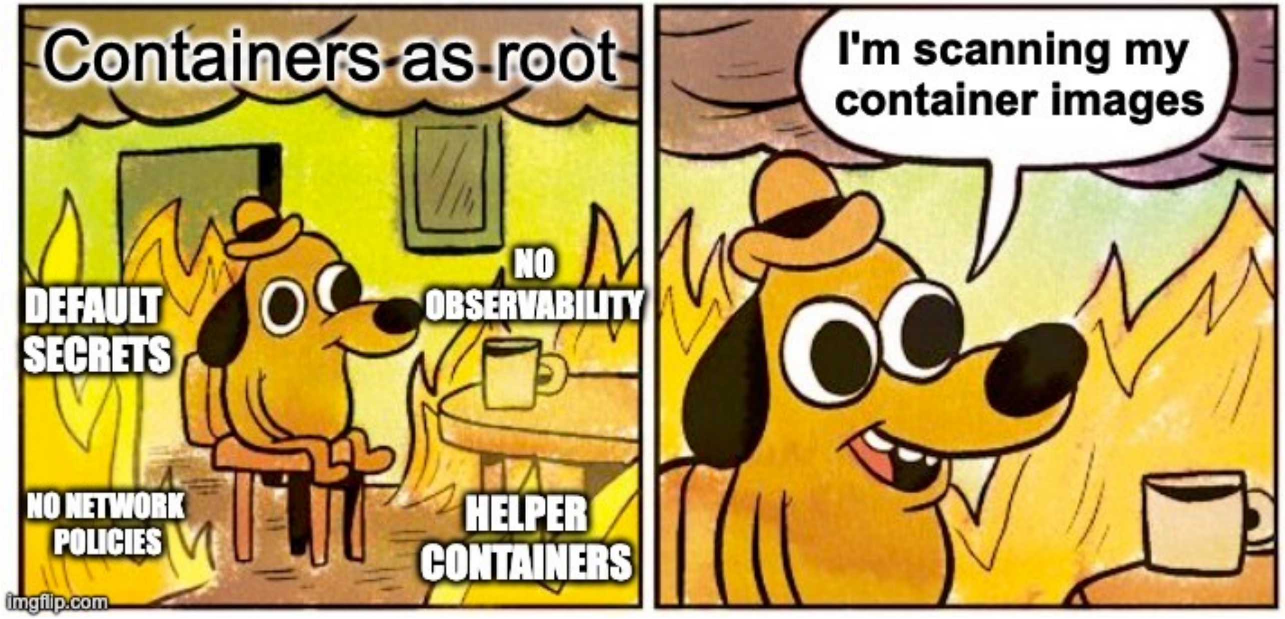
Walkthrough: External Secret Vulnerabilities



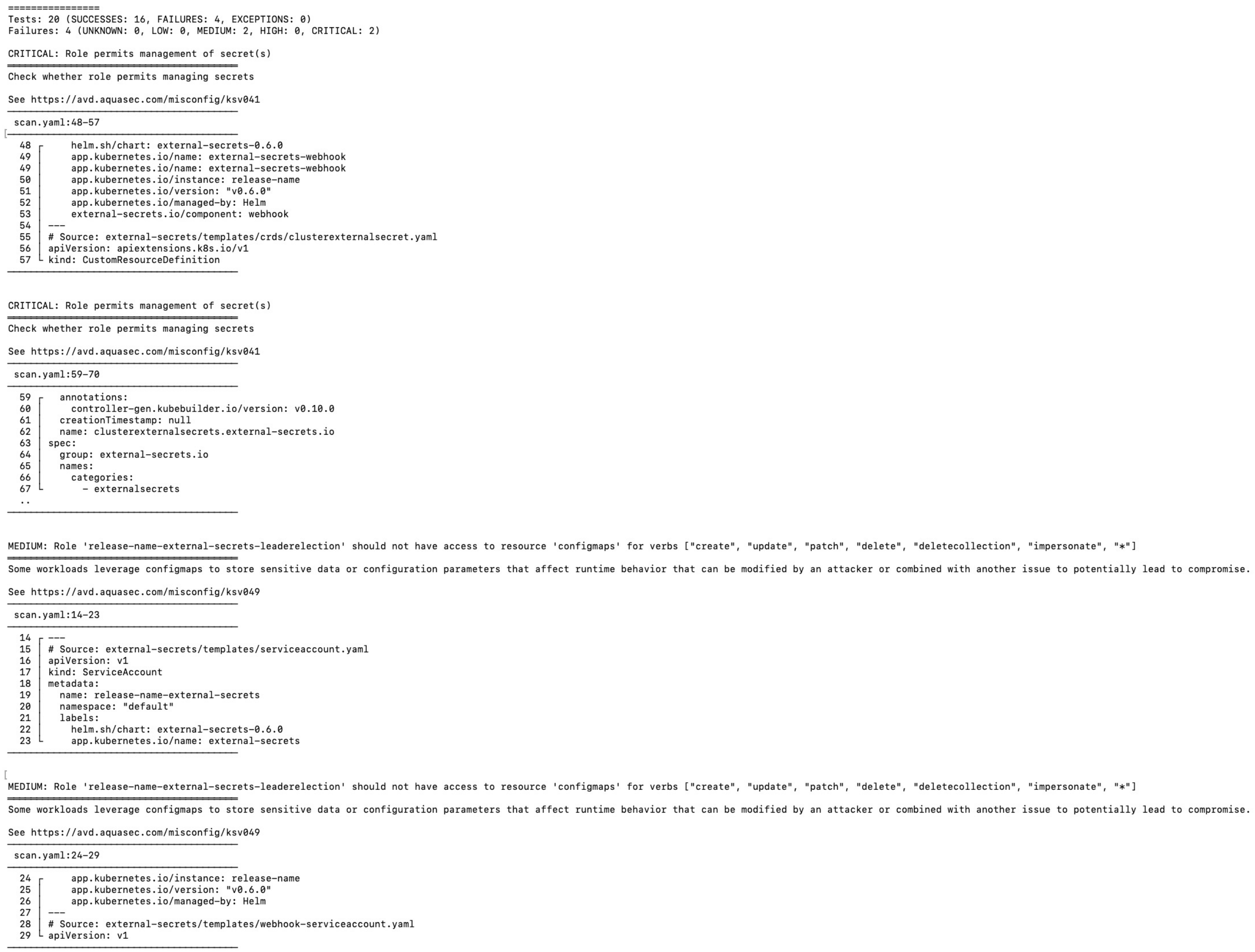
```
===============================
Total: 5 (UNKNOWN: 2, LOW: 1, MEDIUM: 2, HIGH: 0, CRITICAL: 0)
```

Library	Vulnerability	Severity	Installed Version	Fixed Version	Title
github.com/aws/aws-sdk-go	CVE-2020-8911	MEDIUM	v1.44.101		aws/aws-sdk-go: CBC padding oracle issue in AWS S3 Crypto SDK for golang... https://avd.aquasec.com/nvd/cve-2020-8911
	CVE-2020-8912	LOW			aws-sdk-go: In-band key negotiation issue in AWS S3 Crypto SDK for golang... https://avd.aquasec.com/nvd/cve-2020-8912
	GHSA-7f33-f4f5-xwgw	UNKNOWN			The Go AWS S3 Crypto SDK contains vulnerabilities that can permit an... https://github.com/advisories/GHSA-7f33-f4f5-xwgw
	GHSA-f5pg-7wfw-84q9				The Go AWS S3 Crypto SDK contains vulnerabilities that can permit an... https://github.com/advisories/GHSA-f5pg-7wfw-84q9
golang.org/x/text	CVE-2022-32149	MEDIUM	v0.3.7	0.3.8	golang: golang.org/x/text/language: ParseAcceptLanguage takes a long time to parse complex tags https://avd.aquasec.com/nvd/cve-2022-32149

Hardening Deployments



Walkthrough: Scanning With Trivy (Again)



```
================
Tests: 20 (SUCCESSES: 16, FAILURES: 4, EXCEPTIONS: 0)
Failures: 4 (UNKNOWN: 0, LOW: 0, MEDIUM: 2, HIGH: 0, CRITICAL: 2)

CRITICAL: Role permits management of secret(s)
════════════════════════════════════════
Check whether role permits managing secrets

See https://avd.aquasec.com/misconfig/ksv041
────────────────────────────────────────
 scan.yaml:48-57
────────────────────────────────────────
  48 ┌       helm.sh/chart: external-secrets-0.6.0
  49 │       app.kubernetes.io/name: external-secrets-webhook
  49 │       app.kubernetes.io/name: external-secrets-webhook
  50 │       app.kubernetes.io/instance: release-name
  51 │       app.kubernetes.io/version: "v0.6.0"
  52 │       app.kubernetes.io/managed-by: Helm
  53 │       external-secrets.io/component: webhook
  54 │ ---
  55 │ # Source: external-secrets/templates/crds/clusterexternalsecret.yaml
  56 │ apiVersion: apiextensions.k8s.io/v1
  57 └ kind: CustomResourceDefinition
────────────────────────────────────────


CRITICAL: Role permits management of secret(s)
════════════════════════════════════════
Check whether role permits managing secrets

See https://avd.aquasec.com/misconfig/ksv041
────────────────────────────────────────
 scan.yaml:59-70
────────────────────────────────────────
  59 ┌   annotations:
  60 │     controller-gen.kubebuilder.io/version: v0.10.0
  61 │   creationTimestamp: null
  62 │   name: clusterexternalsecrets.external-secrets.io
  63 │ spec:
  64 │   group: external-secrets.io
  65 │   names:
  66 │     categories:
  67 └       - externalsecrets
  ..
────────────────────────────────────────


MEDIUM: Role 'release-name-external-secrets-leaderelection' should not have access to resource 'configmaps' for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"]
════════════════════════════════════════
Some workloads leverage configmaps to store sensitive data or configuration parameters that affect runtime behavior that can be modified by an attacker or combined with another issue to potentially lead to compromise.

See https://avd.aquasec.com/misconfig/ksv049
────────────────────────────────────────
 scan.yaml:14-23
────────────────────────────────────────
  14 ┌ ---
  15 │ # Source: external-secrets/templates/serviceaccount.yaml
  16 │ apiVersion: v1
  17 │ kind: ServiceAccount
  18 │ metadata:
  19 │   name: release-name-external-secrets
  20 │   namespace: "default"
  21 │   labels:
  22 │     helm.sh/chart: external-secrets-0.6.0
  23 └     app.kubernetes.io/name: external-secrets
────────────────────────────────────────


MEDIUM: Role 'release-name-external-secrets-leaderelection' should not have access to resource 'configmaps' for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"]
════════════════════════════════════════
Some workloads leverage configmaps to store sensitive data or configuration parameters that affect runtime behavior that can be modified by an attacker or combined with another issue to potentially lead to compromise.

See https://avd.aquasec.com/misconfig/ksv049
────────────────────────────────────────
 scan.yaml:24-29
────────────────────────────────────────
  24 ┌     app.kubernetes.io/instance: release-name
  25 │     app.kubernetes.io/version: "v0.6.0"
  26 │     app.kubernetes.io/managed-by: Helm
  27 │ ---
  28 │ # Source: external-secrets/templates/webhook-serviceaccount.yaml
  29 └ apiVersion: v1
────────────────────────────────────────
```

Walkthrough: External Secrets Configuration

- Again, Trivy’s configuration scanner is super helpful, but not a silver bullet
- The warning about managing Secrets is *very* helpful, but in this case, that is entirely expected
- The excessive verbs for ConfigMaps is not expected and should likely be cleaned up

A Brief Aside: Basic Threat Modeling

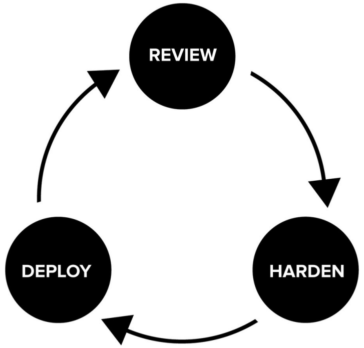
- Improving security by identifying threats
  - Understanding Cost and Frequency
  - And figure out how to mitigate them
- S.T.R.I.D.E
  - Spoofing
  - Tampering
  - Repudiation
  - Information Disclosure
  - Denial of Service
  - Elevation of Privilege

Walkthrough: External Secrets Configuration

- Consider what we know now:
  - Our general security guidance
  - Application-specific configuration options
  - Our threat model
  - Scan findings
- Now we fork the upstream Helm chart
  - Meets our organizational requirements
  - Adds organization-required resources and configurations.
  - Ensures the *default* install is the most-secure install

Deploying Third-Party Applications

```
helm install [NAME] [CHART] [flags]
```

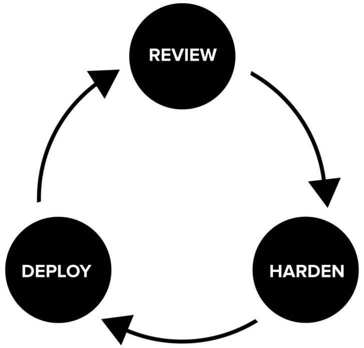


Walkthrough: The Easy Part

- Any image or Helm chart you want to install *must* be from a private registry
- Use GitOps. Do not expose the Kubernetes API server to an untrusted network (e.g., the Internet)
- Monitor your third-party application metrics and alert at reasonable thresholds
- Forward audit logs to your organization’s SIEM solution

The Third-Party Lifecycle

Applying STRIDE to other types of threats



Constantly Monitor Vulnerability Scans

- Vulnerability scans should happen daily.
- Critical vulnerabilities need to be patchable in fewer than 7 days.
- Response requires good intra-organization communication.

Periodically, Answer These Questions (Part II)

- Is the project still actively maintained?
- Is the focus of the project the same?
- Have any security incidents/vulnerabilities occurred?
- Do the current internal owners still want ownership?
- Is it meeting your organization’s needs?
- What does the ecosystem look like now?

Questions?

Feedback?