



Replik8s , a Modern Security Tool for Kubernetes

Xavier Garceau-Aranda   
Principal Security Engineer @ Latacora



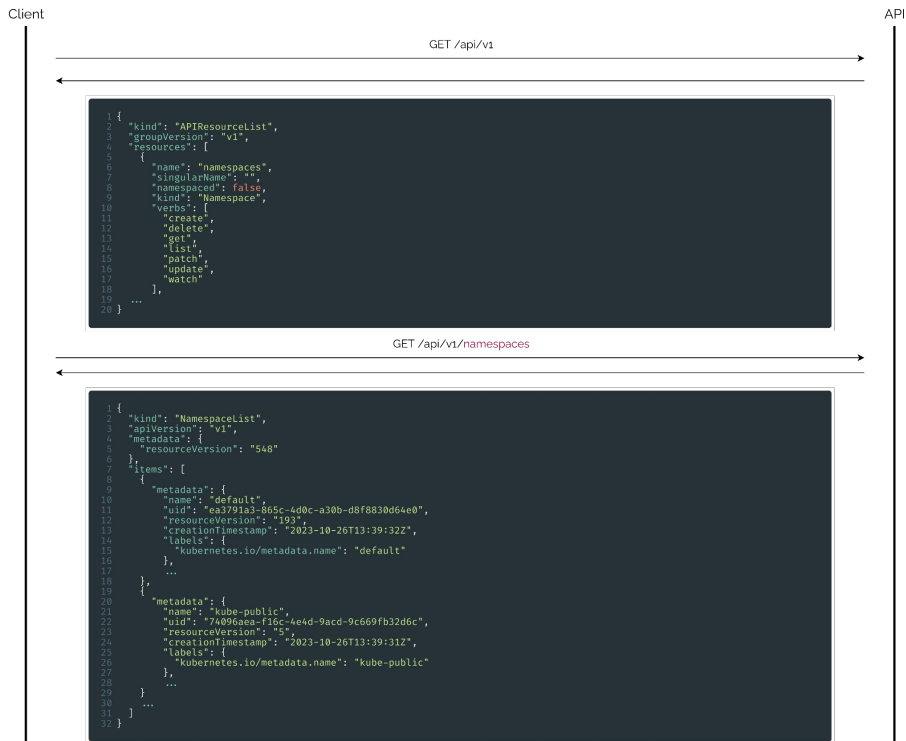
Current state of security tooling



Our approach



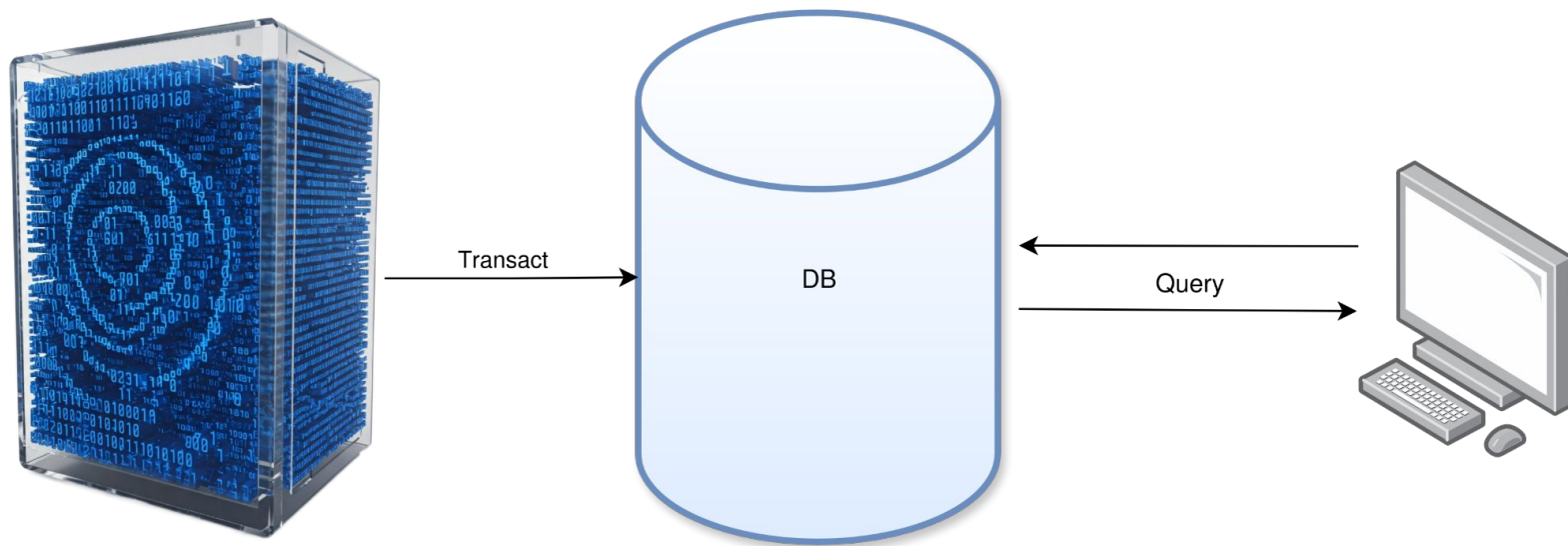
Collecting Kubernetes APIs



Snapshots



Queries



Datascript Queries - Listing Pods

```
(d/q '[:find ?timestamp ?host ?namespace ?name
      :keys timestamp host namespace pod
      :in $ %
      :where
      [?snapshot :metadata ?snapshot-metadata]
      [?snapshot-metadata :host ?host]
      [?snapshot-metadata :timestamp ?timestamp-int]
      [(com.latacora.replik8s.utils/datetime→date-str ?timestamp-int) ?timestamp]
      [?snapshot :resources ?r]
      [?r :api_v1_pods ?pods]
      [?pods :items ?i]
      [?i :metadata ?metadata]
      [?metadata :name ?name]
      [?metadata :namespace ?namespace]
      [?i :spec ?spec]]
  db rules)
```


Datascript Queries - Listing Pods via Rules

```
(d/q '[:find ?timestamp ?host ?namespace ?name
      :keys timestamp host namespace pod
      :in $ %
      :where
      (pod ?timestamp ?host ?namespace ?name ?owner-kind ?owner-name ?spec)]
db rules)
```

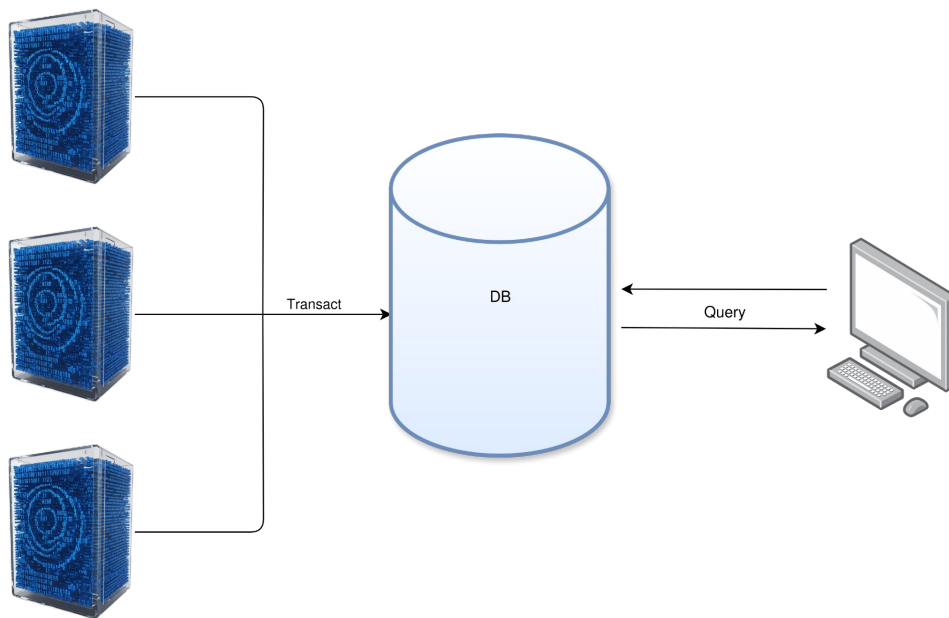
Datascript Queries for Findings

```
(defn containers-with-sensitive-hostpath-mounts
  "Query for containers mounting sensitive host paths."
  [db]
  (d/q '[:find ?timestamp ?host ?namespace ?owner-kind ?owner-name ?pod-name ?volume-name ?host-path ?container-name ?mount-path
        :keys timestamp host namespace owner-kind owner-name pod volume-name host-path container mount-path
        :in $ %
        :where
        (container ?timestamp ?host ?namespace ?pod-name ?owner-kind ?owner-name ?spec ?container ?container-name ?container-image)
        ;; pod volume
        [?spec :volumes ?volume]
        [?volume :name ?volume-name]
        [?volume :hostPath ?hp]
        [?hp :path ?host-path]
        ;; container
        [?container :volumeMounts ?volumeMount]
        [?volumeMount :name ?volume-name]
        [?volumeMount :mountPath ?mount-path]
        (or [(= ?host-path "/")]
            [(= ?host-path "/etc")]
            [(= ?host-path "/proc")]
            [(= ?host-path "/var/run/docker.sock")]
            [(= ?host-path "/root")]
            [(clojure.string/starts-with? ?host-path "/var/log")]))]
  db rules))
```

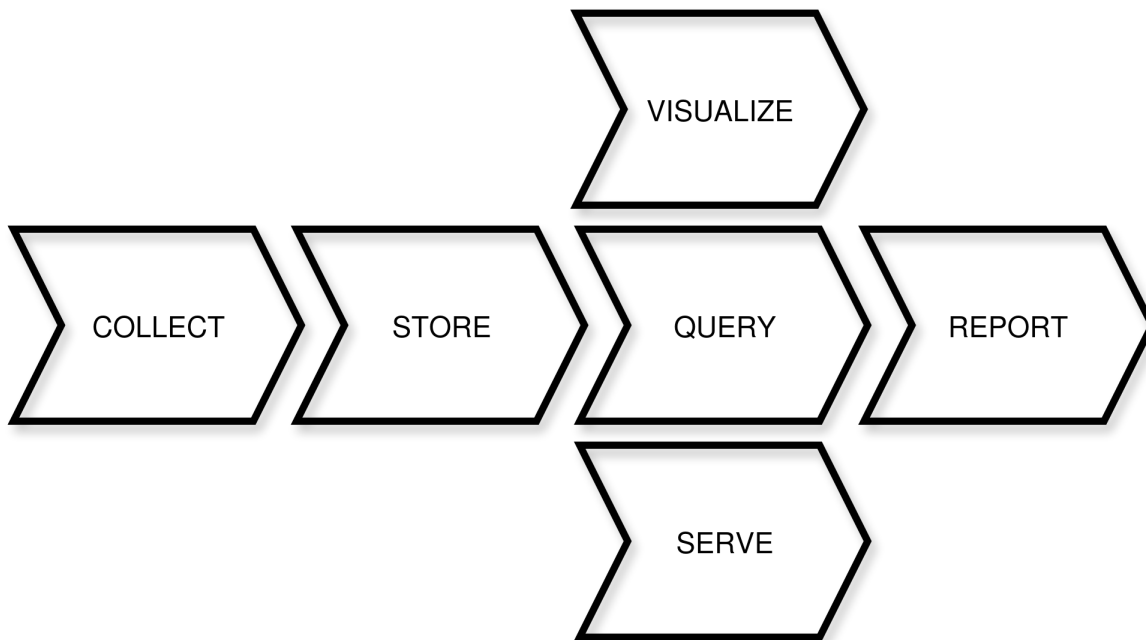
Pods Vulnerable to Ingress Nightmare (CVE-2025-1974)

```
(d/q '[:find ?timestamp ?host ?namespace ?name ?label-name ?label-version
      :keys timestamp host namespace pod label-name label-version
      :in $ %
      :where
      [?snapshot :metadata ?snapshot-metadata]
      [?snapshot-metadata :host ?host]
      [?snapshot-metadata :timestamp ?timestamp-int]
      [(com.latacora.replik8s.utils/datetime→date-str ?timestamp-int) ?timestamp]
      [?snapshot :resources ?r]
      [?r :api_v1_pods ?pods]
      [?pods :items ?i]
      [?i :metadata ?metadata]
      [?metadata :name ?name]
      [?metadata :namespace ?namespace]
      [?metadata :labels ?labels]
      [?labels :name "ingress-nginx"]
      [?labels :name ?label-name]
      [?labels :version ?label-version]
      ;; This vulnerability is fixed in Ingress NGINX Controller version 1.12.1 and 1.11.5.
      (or-join [?label-version]
        [(= ?label-version "1.12.0")]
        [(not (com.latacora.replik8s.utils/version-greater-or-equal? ?label-version "1.11.5"))]))
db rules)
```

Beyond individual snapshots

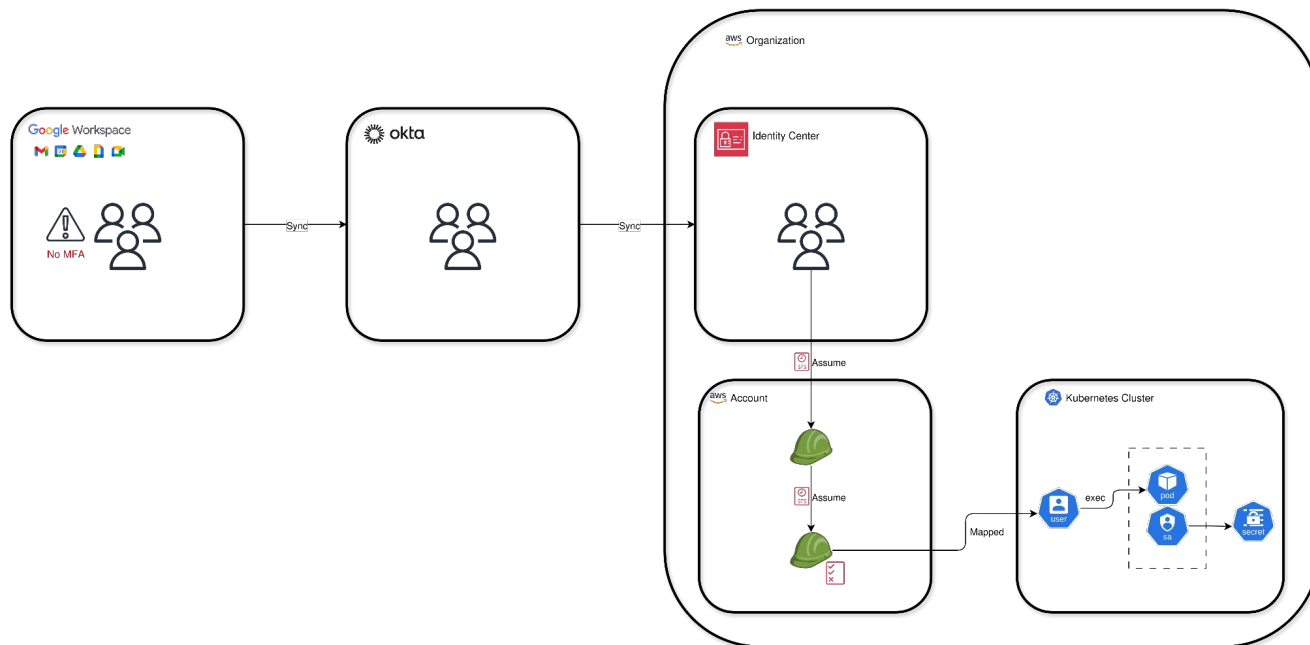


Replik8s (<https://github.com/latacora/replik8s>)





Treating providers as equals



Going Forward



Further reading:

- [Our Approach to Building Security Tooling | Latacora](#)
- [Datatomic and Content Addressable Techniques: An Ultimate Data Wonderland | Latacora](#)
- [DevOpsCon San Diego: All the Data. All the Time - A New Strategy for Security Tooling](#)
- [Introducing Replik8s, a Modern Security Tool for Kubernetes | Latacora](#)

Thank you!