




Kubernetes Sleuthing with RepliK8s

Xavier Garceau-Aranda   
Principal Security Engineer @ Latacora

Hello, World 44CON



LATACORA



the
BROWSER
COMPANY
of NEW YORK



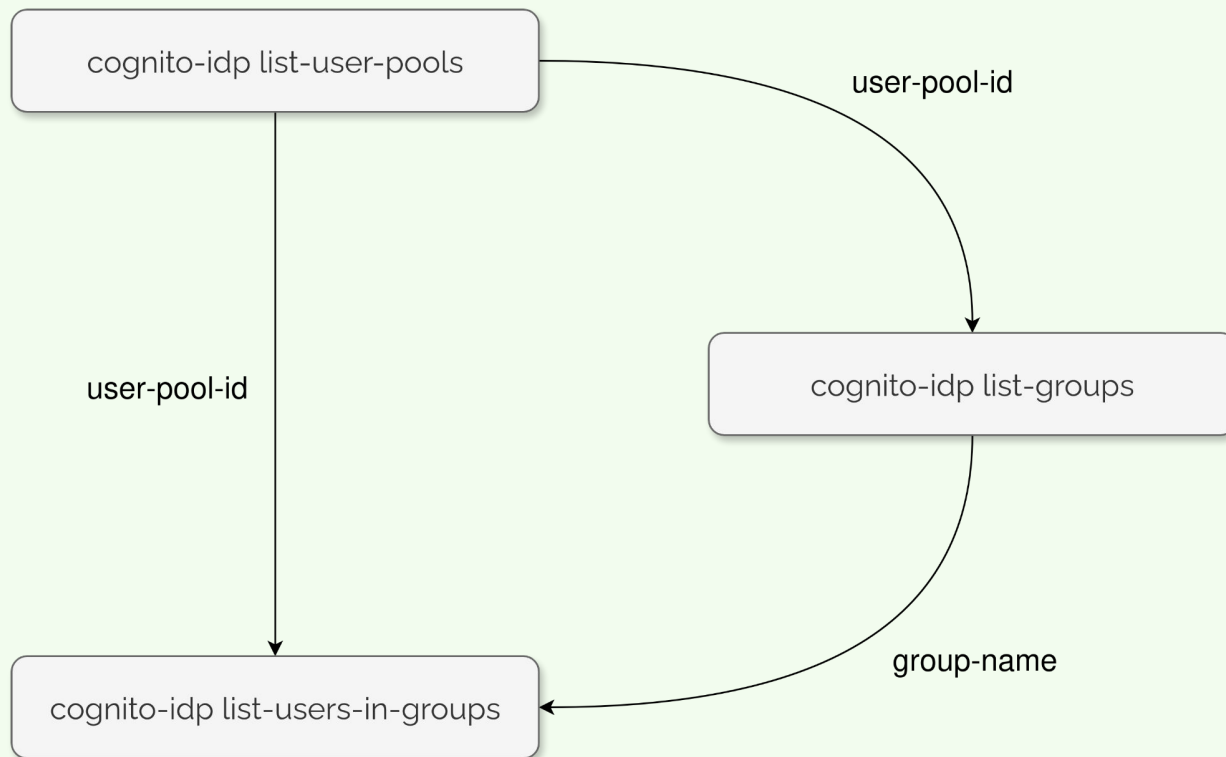
Current state of security tooling



Our approach



First step: retrieving "all the things"



Simple APIs (K8s)

Client

API

GET /api/v1

```
1 {
2   "kind": "APIResourceList",
3   "groupVersion": "v1",
4   "resources": [
5     {
6       "name": "namespaces",
7       "singularName": "",
8       "namespaced": false,
9       "kind": "Namespace",
10      "verbs": [
11        "create",
12        "delete",
13        "get",
14        "list",
15        "patch",
16        "update",
17        "watch"
18      ],
19      ...
20    }
21  ]
22 }
```

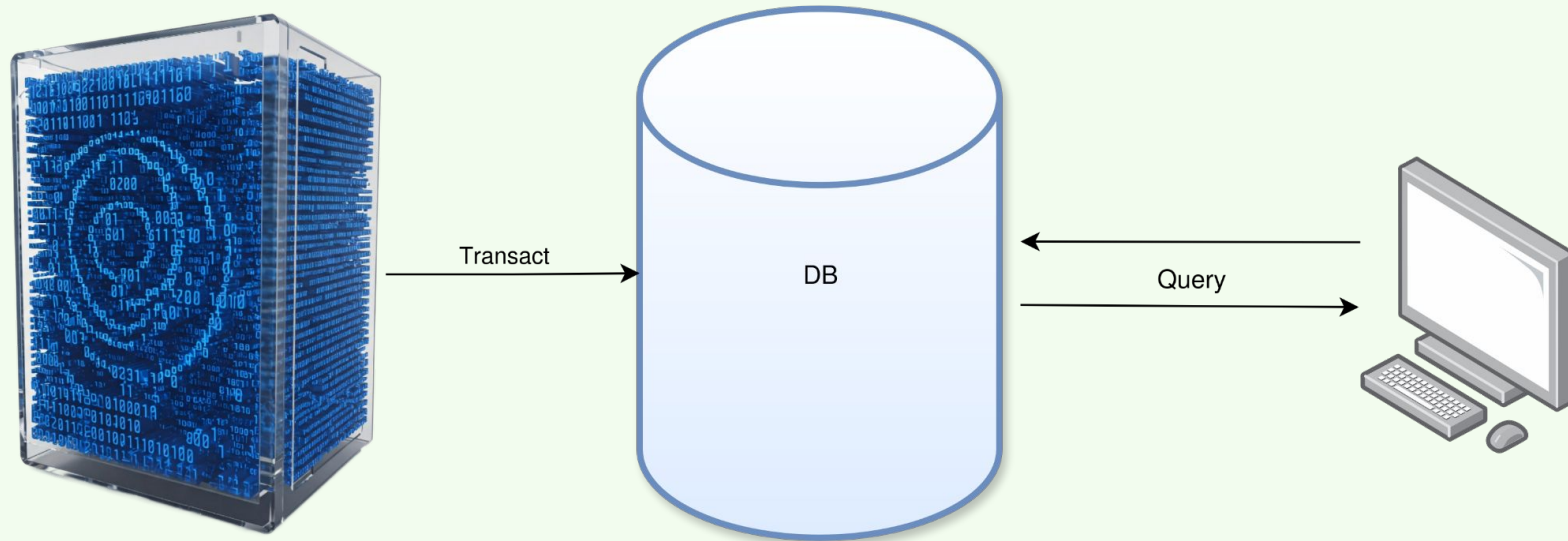
GET /api/v1/namespaces

```
1 {
2   "kind": "NamespaceList",
3   "apiVersion": "v1",
4   "metadata": {
5     "resourceVersion": "548"
6   },
7   "items": [
8     {
9     "metadata": {
10      "name": "default",
11      "uid": "ea3791a3-865c-4d0c-a30b-d8f8830d64e0",
12      "resourceVersion": "193",
13      "creationTimestamp": "2023-10-26T13:39:32Z",
14      "labels": {
15        "kubernetes.io/metadata.name": "default"
16      },
17      ...
18    },
19    ...
20  ],
21  "metadata": {
22    "name": "kube-public",
23    "uid": "74096aea-f16c-4e4d-9acd-9c669fb32d6c",
24    "resourceVersion": "5",
25    "creationTimestamp": "2023-10-26T13:39:31Z",
26    "labels": {
27      "kubernetes.io/metadata.name": "kube-public"
28    },
29    ...
30  },
31  ...
32 }
```

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)
```

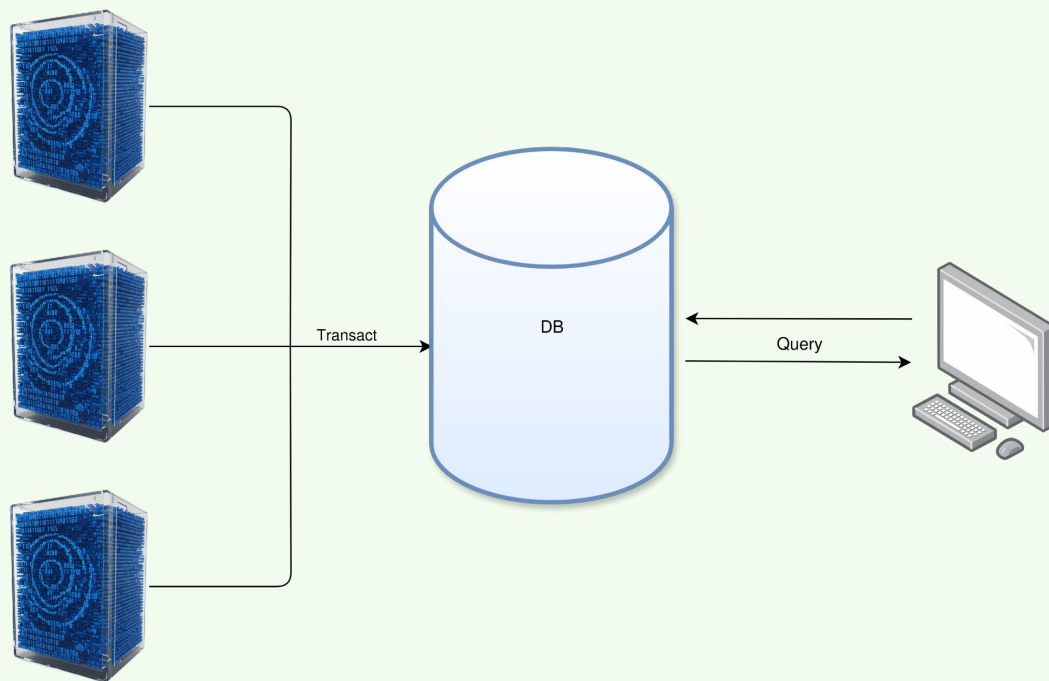
Datascript Queries for Findings

```
(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))
```

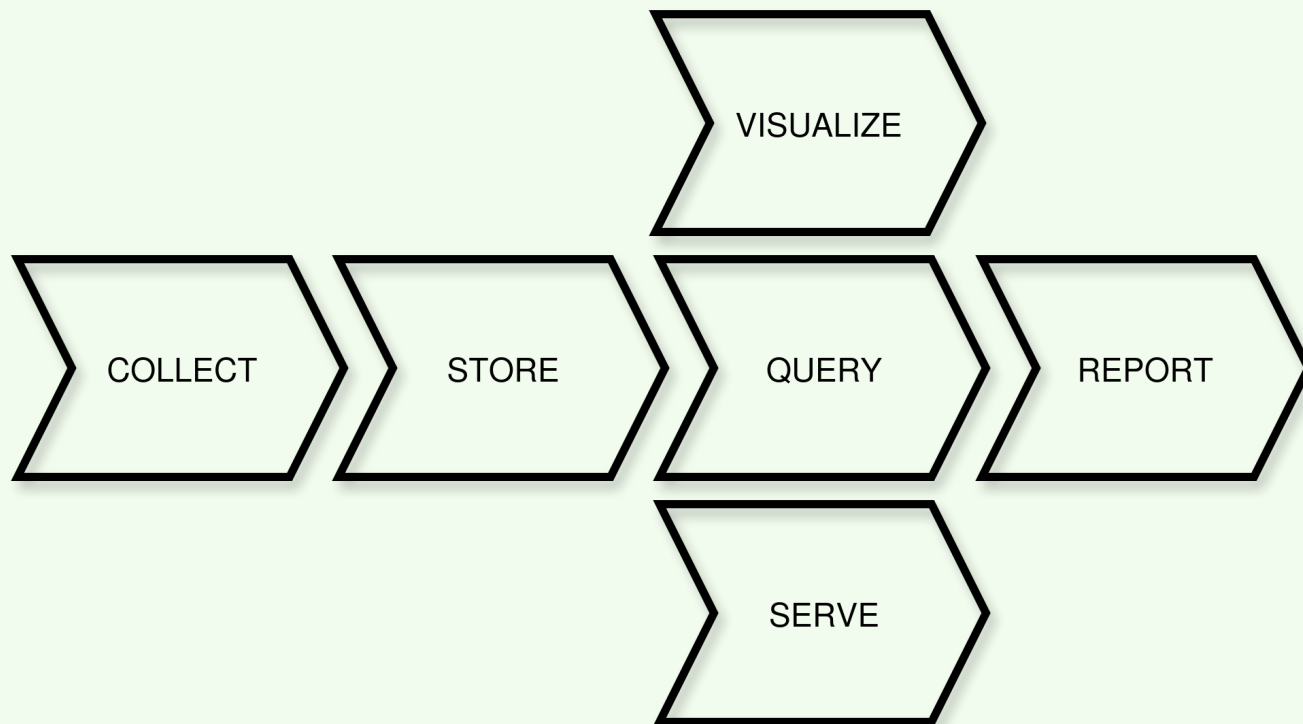
Pods Vulnerable to Ingress Nightmare (CVE-2025-1974)

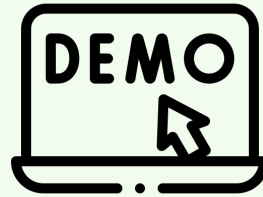
```
(d/q '[:find ?timestamp ?host ?namespace ?name ?label-name ?label-version
:keys timestamp host namespace pod label-name label-version
:in $ %
:where
[?snapshot :metadata ?snapshot-metadata]
[?snapshot-metadata :host ?host]
[?snapshot-metadata :timestamp ?timestamp-int]
[(com.latacora.replik8s.utils/datetime→date-str ?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

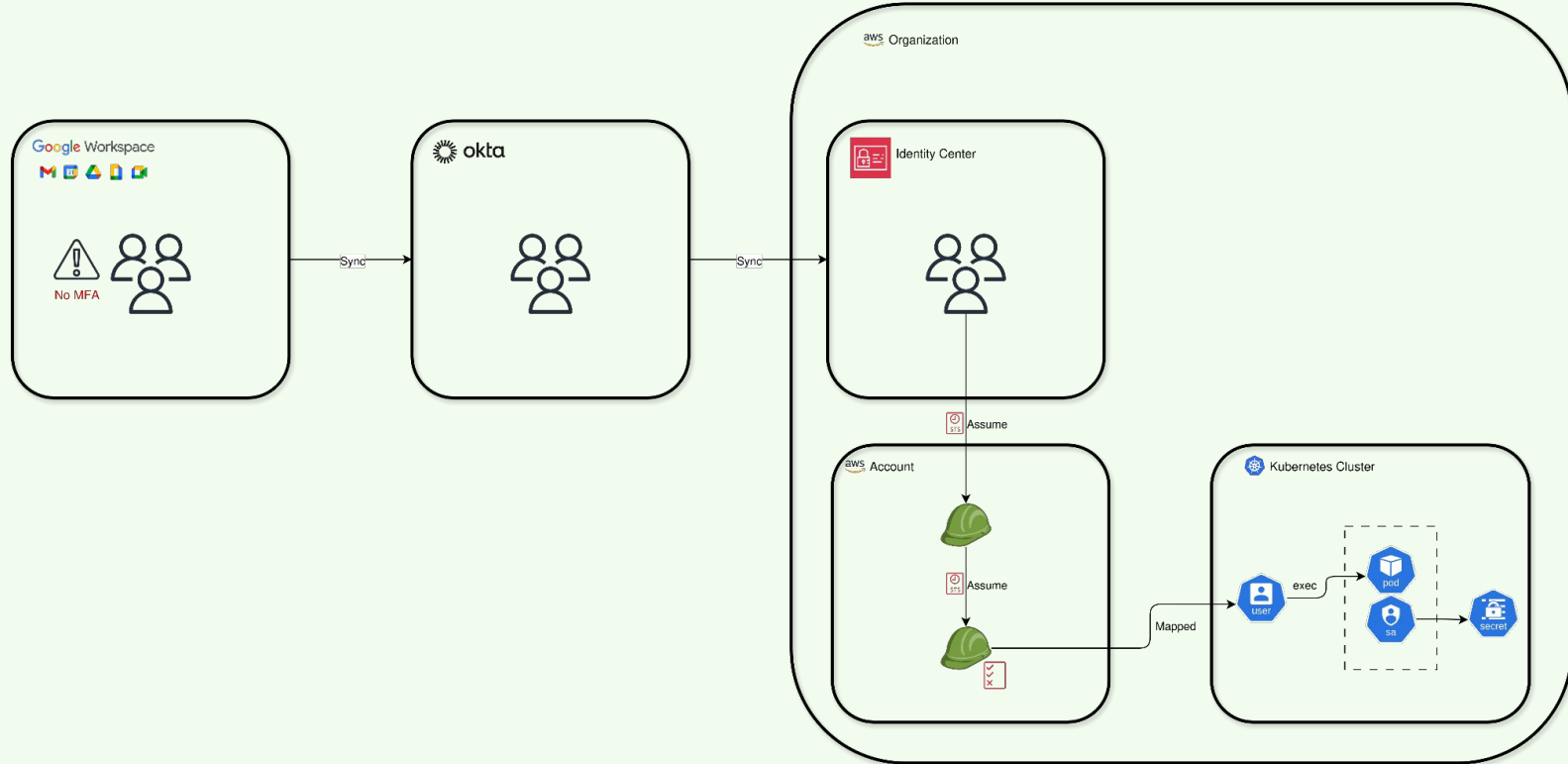


Replik8s (<https://github.com/latacora/replik8s>)

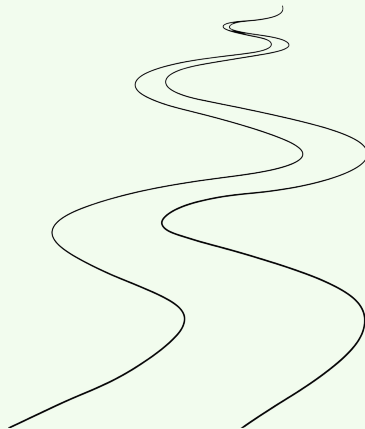




Treating providers as equals



Going Forward



Further reading:

- [Our Approach to Building Security Tooling | Latacora](#)
- [Datomic and Content Addressable Techniques: An Ultimate Data Wonderland | Latacora](#)
- [DevOpsCon San Diego: All the Data, All the Time - A New Strategy for Security Tooling](#)

Thank you!

Workshop @ 16h00

