ADDO

ALL DAY DEVOPS

NOVEMBER 6, 2019

Abhisek Datta, Appsecco

Application Security Workflow Automation

Using Docker and Kubernetes

About Me – Abhisek Datta

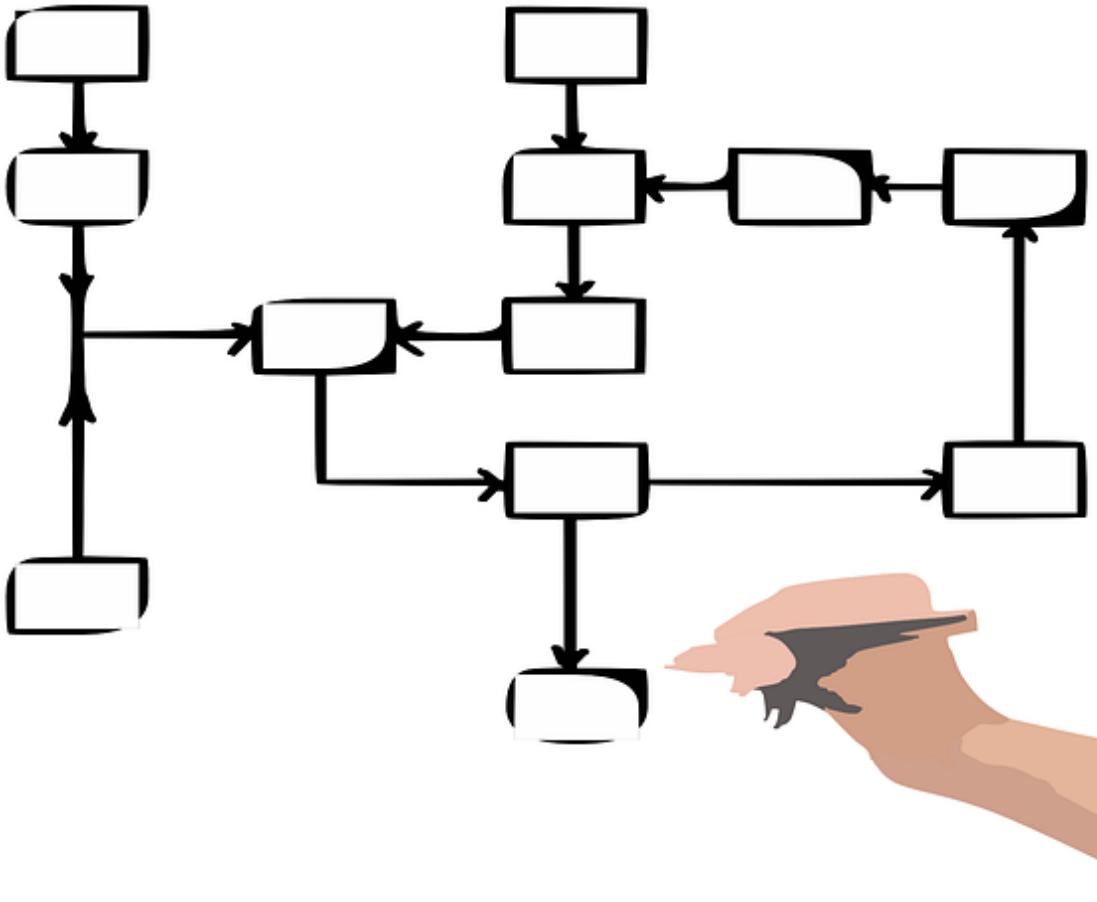
- Head of Technology (appsecco.com)
  - A boutique security consulting company
- TechWing @ null0x00 (null.co.in)
  - An Open Security Community
- Security Researcher
  - Discovered vulnerabilities in MS Office, Internet Explorer, HP SiteScope etc.
- Certified Kubernetes Application Developer (CKAD) :-P

APPSECCO

Key Take Away

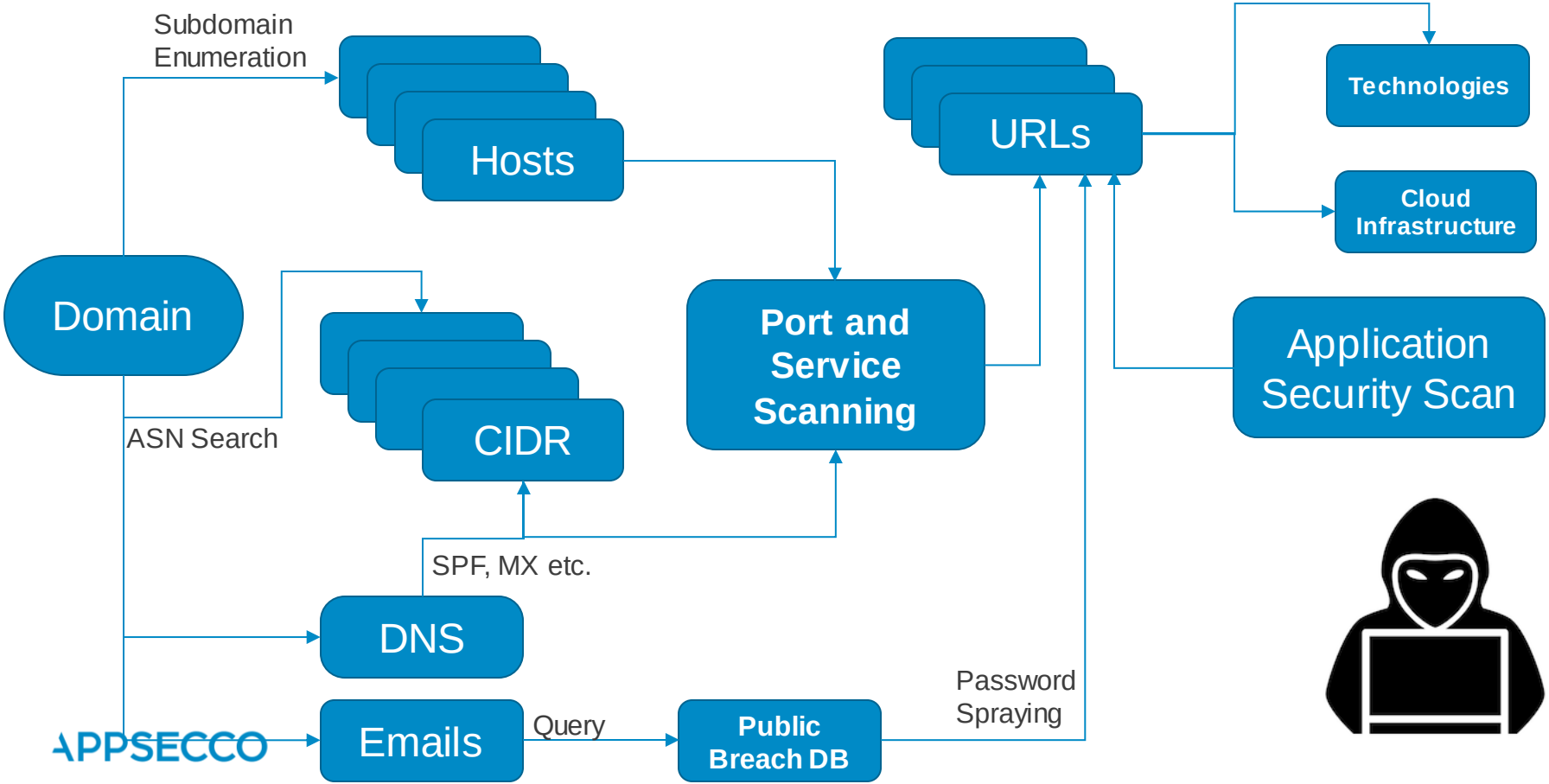
1. How does an Application Security Workflow look like (Our opinion)
2. Our approach of security automation using Kubernetes native technologies
3. How to get started in automating Application Security Workflow using **KubeSecO**

Application Security Workflow

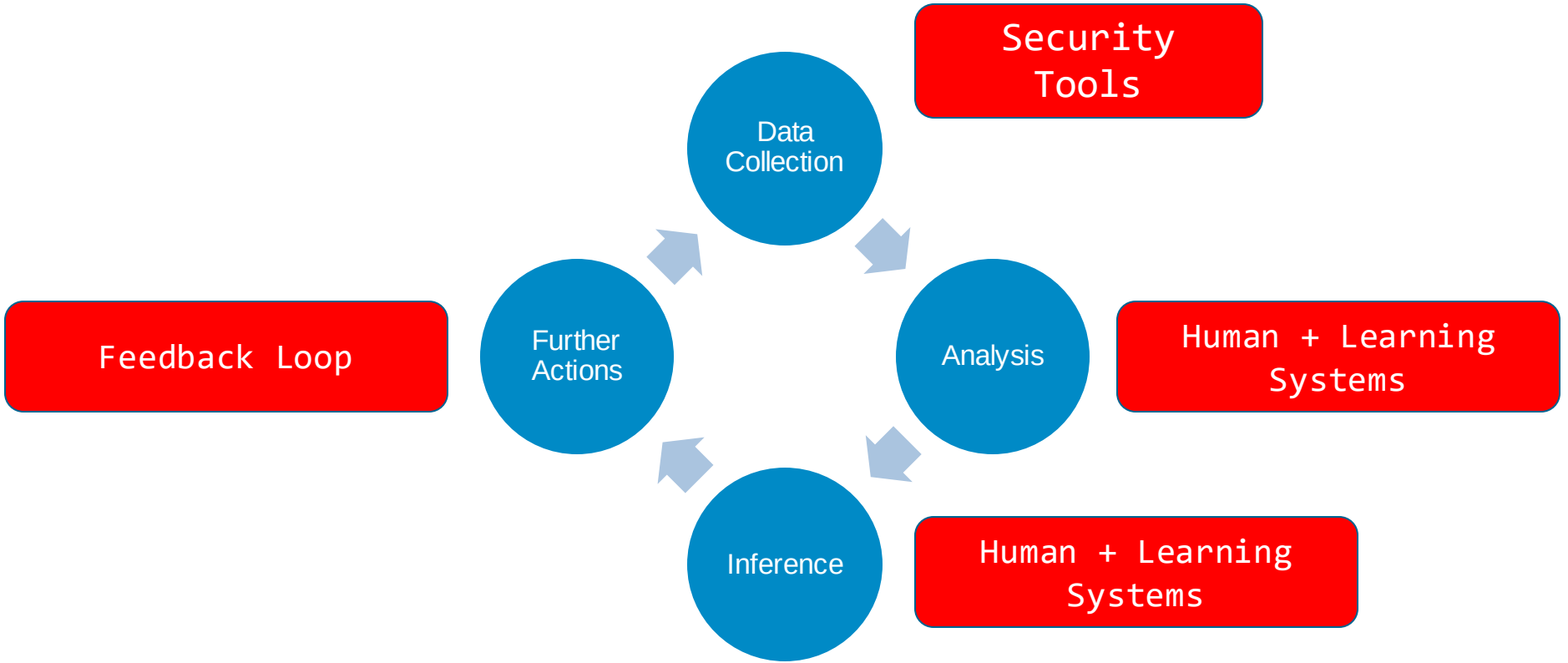


APPSECCO

An Example AppSec Workflow



How does it look like from Automation Perspective?



Automating AppSec Workflow

KubeSecO Live in Action

```
➜  ~ curl -s -H "Content-Type: application/json" \
-d '{ "asset_type":"domain", "asset_value":"example.com"}' \
http://localhost:3000/scans | jq .

{
  "status": "success",
  "response": {
    "asset_type": "domain",
    "asset_value": "example.com",
    "scan_id": "0866c974-8f33-4cf7-961f-5e68f33142c8"
  }
}
```

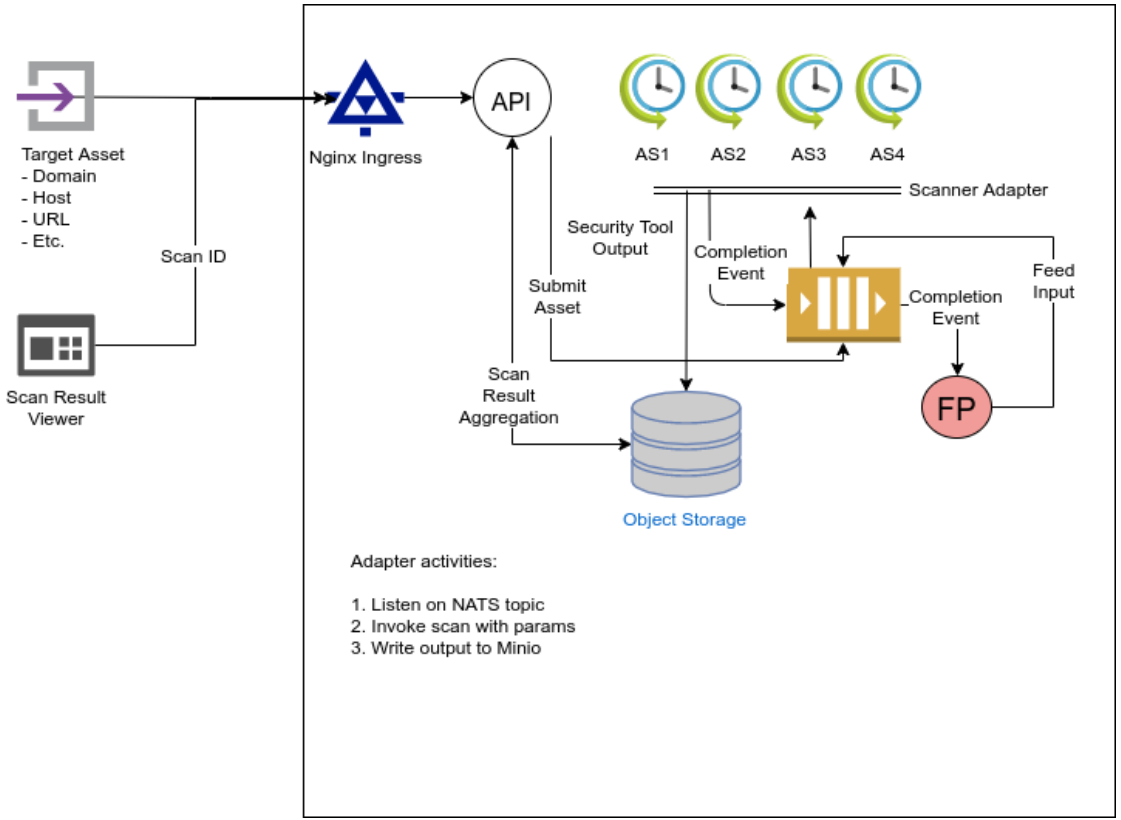
github.com/appsecco/kubeseco

What's under the hood?

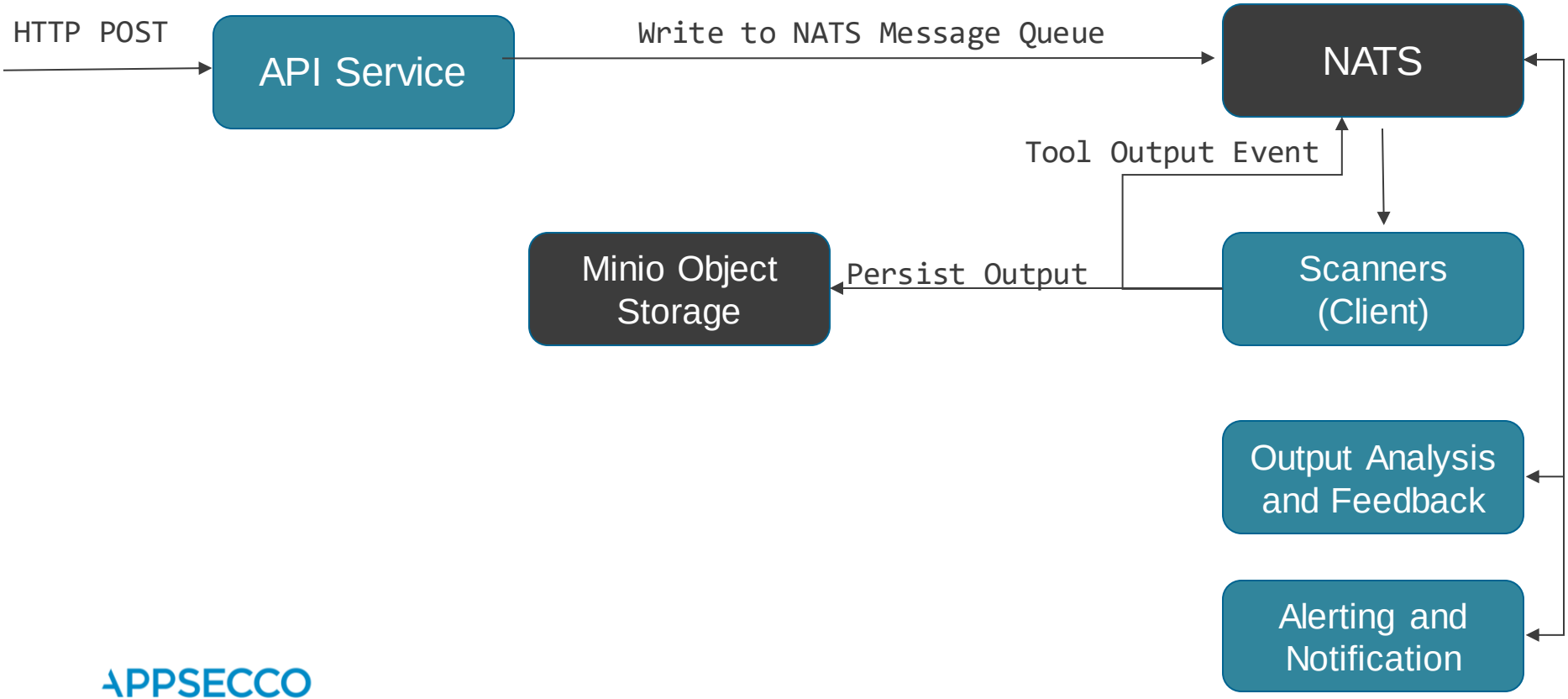
```
→  ~ kubectl get pods
NAME                                    READY
api-service-app-6669464864-wbsq4        1/1
appdiscovery-tool-65879d97bc-prctd      1/1
appdiscovery-tool-65879d97bc-sqzfl      1/1
certspotter-tool-67899fc7cb-g9rcq       1/1
feedback-processor-app-9d9d46f65-vg595  1/1
minio-585c55b5dd-9nf4b                  1/1
nats-nats-0                             1/1
```

github.com/appsecco/kubeseco

How does the system look like?



Driving the System – Events FTW!



The Tool Adapter (Pattern)

- 3rd Party Tools are not in our control
- We need to be able to
  - Receive input from NATS
  - Run tool with tool specific command line
  - Receive output or check for error
  - Persist output to Minio

Adding a Security Tool (3rd Party)

1. Package 3rd party tools as Docker containers
2. Add Tool Adapter binary and set as entrypoint
3. Write Kubernetes deployment spec (YAML)
4. Deploy to Kubernetes
5. Write YAML rules for *Feedback Processing*

Security Tool Dockerfile

```
1   FROM alpine:3.7
2
3   ADD https://storage.googleapis.com/
    appsec-workflow-k8s-poc/tool-adapter/v1.0.0/
    tool-adapter /usr/bin/workflow-tool-adapter
4
5   RUN apk update && \
6     apk add --no-cache curl jq libc6-compat && \
7     chmod +x /usr/bin/workflow-tool-adapter
8
9   CMD ["/usr/bin/workflow-tool-adapter"]
```

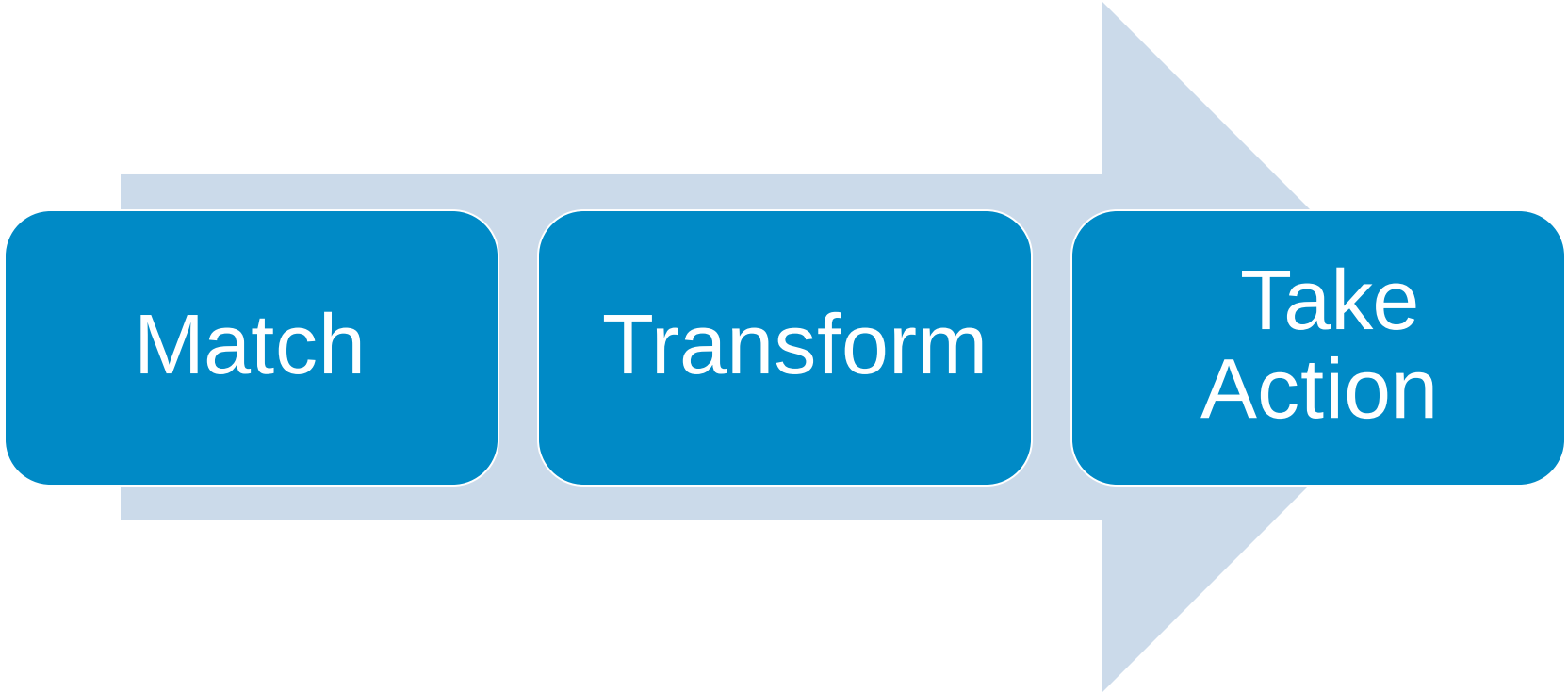
Security Tool Kubernetes Spec (YAML)

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: certspotter-tool
  labels:
    app: certspotter
[...]

    spec:
      containers:
      - name: certspotter-ctr
        imagePullPolicy: Always
        image: abh1sek/appsec-workflow-certspotter
        command: ["/usr/bin/workflow-tool-adapter"]
        env:
[...]
        - name: TOOL_EXEC_PATTERN
          value: "curl -s https://certspotter.com/api/v0/certs?
          domain={{TARGET}} | jq '[.[].dns_names] | flatten | sort |
           unique'"
```

APPSECCO

Feedback Processor (Driving the System)



Feedback Processor - Example

```yaml
workflow:
  name: Demo Workflow
  version: 1.0.0
  author: root@localhost.local
rules:
  - name: certspotter-feedback
    match:  # Match any attribute of Input Event using regex
      tool_name: certspotter
      target_info.asset_type: domain
    transform:  # Must always transform to an array of values
      jsonpath: $
    actions:
      - type: enqueue
        on: item  # item/bulk
        queue_name: input.host
        asset_type: host
```

APPSECCO

Challenges, Constraints and Things to do

- State management is difficult due to asynchronous nature of the system
- NATS connection issue with preemptible nodes on GKE
- Capacity planning and analysis
- Cost analysis

How to Contribute

1. Clone the repository from Github
2. Try out and report bugs
3. Add new security tools
4. Add feedback processor rules
5. Submit PR

github.com/appsecco/kubeseco

That’s all for now..

Questions?

abhisek@appsecco.com

https://appsecco.com

@abh1sek

github.com/abhisek

github.com/appsecco/kubeseco