Using Containers, Kubernetes and Serverless to Automate App Sec and OSINT Workflows

NULLCON X

APPSECCO

A/B Test for Logo

Option A

SPLAT

Option B

APPSECCO

Workshop Steps

Setup

- We will take you through all the pre-requisites needed
- How to get them ready
- Do the cluster setup

in about 30 minutes

Reports

- We will run our workflow against a target
- Go through generated report
- Demo our OAuth configurations

in about 15 minutes

Internals

- We will discuss our infra & security tool choices
- Limitations of the system
- Doing state management

in about 30 minutes

Future

- We will demo how to add a new security tool
- Map tools used here with cloud native services
- Talk a bit about our plan for SPLAT

in about 15 minutes

APPSECCO

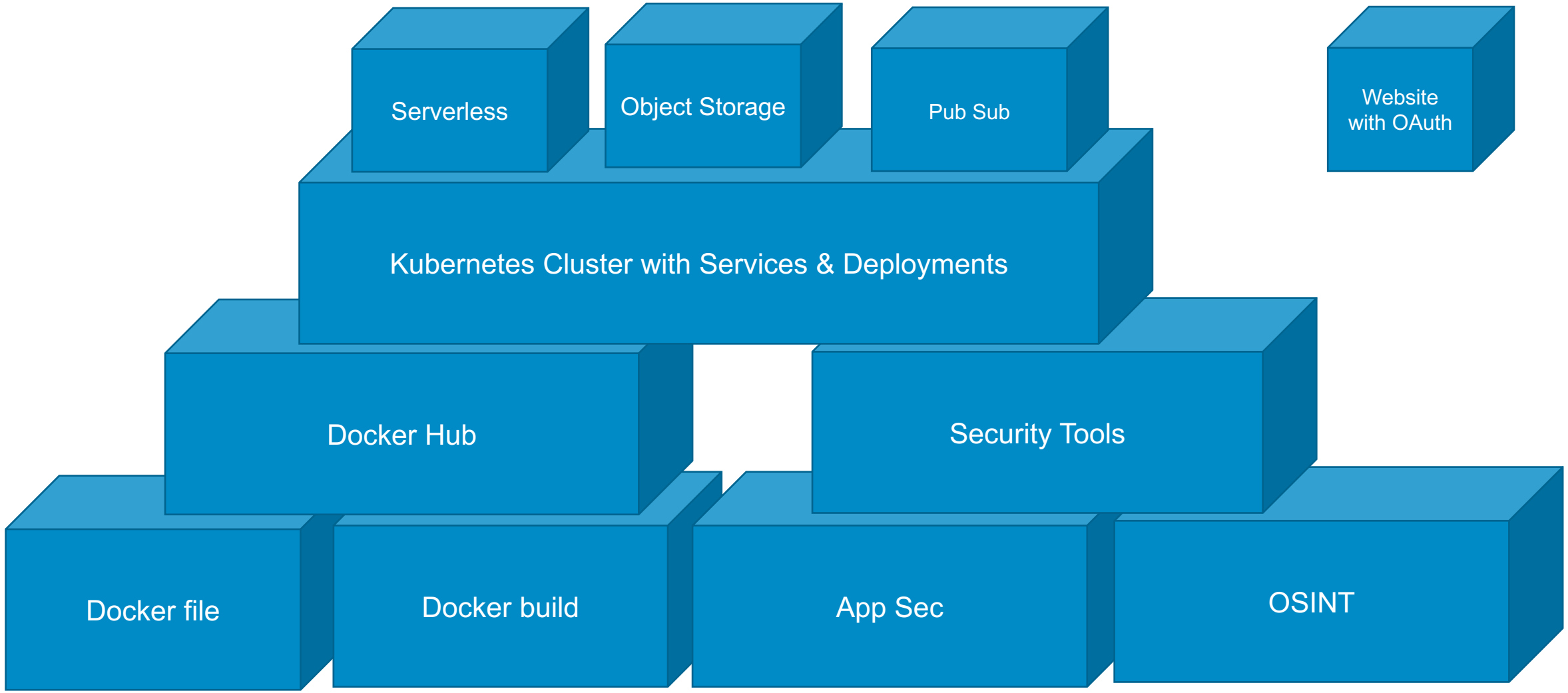
Workshop Checklist

- ❑ Setup that we are going to use
- ❑ Run our security tooling against a target domain
- ❑ Get a report generated
- ❑ Understand how to automate this when using bunch of tools together
- ❑ How you can get started with this
- ❑ Explain our choices of tools, architecture and patterns
- ❑ What else to integrate as a security tool
- ❑ How to repeat this in a cloud native manner

How to get the best value from this workshop

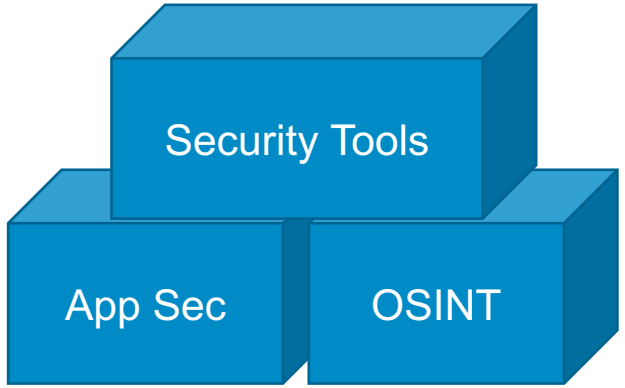
Step	Time	Outcomes	Useful if
1	30	1. Learn all the building blocks 2. Get everything in place 3. Cluster is up and running	✓ You are new to Docker & Kubernetes ✓ You want to try at home later ✓ You want your cluster running
2	15	1. See a scan complete 2. See the report 3. See how to add OAuth for security	✓ You want to see and understand the report ✓ You want to protect the reporting website
3	30	1. Discussion about our tool choices 2. Discussion about the current limitations 3. How state management is difficult here	✓ You want to know why we chose those tools ✓ Understanding the limitations is important for you
4	15	1. Demo on how to add a new security tool 2. Mapping this to Cloud Native 3. Our plans for SPLAT	✓ You want to integrate your tools ✓ You prefer to do this outside Kubernetes

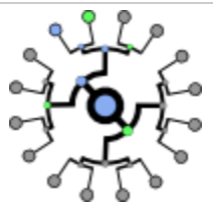
Basic Building Blocks – Complete Picture



Basic Building Blocks – Security Knowledge

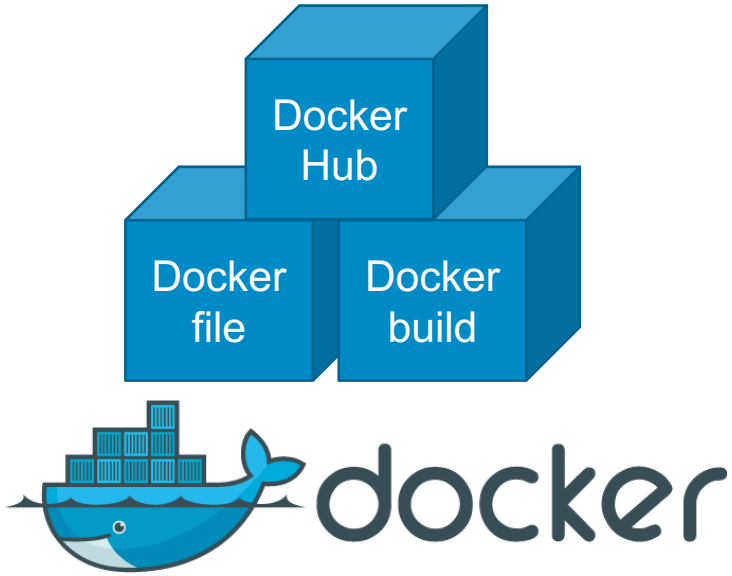
1. Knowledge of OWASP ZAP
2. Knowledge of Certificate Transparency Logs
3. Knowledge of nmap





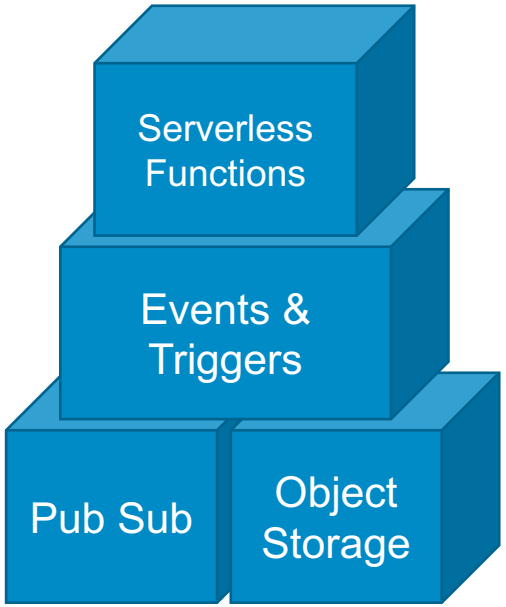
Basic Building Blocks – Docker Parts

1. Choose a security tool
2. Write a Docker file
3. Build the Docker
4. Push the Docker image to the hub
5. Pull the image when required



Basic Building Blocks – Enterprise Message Patterns

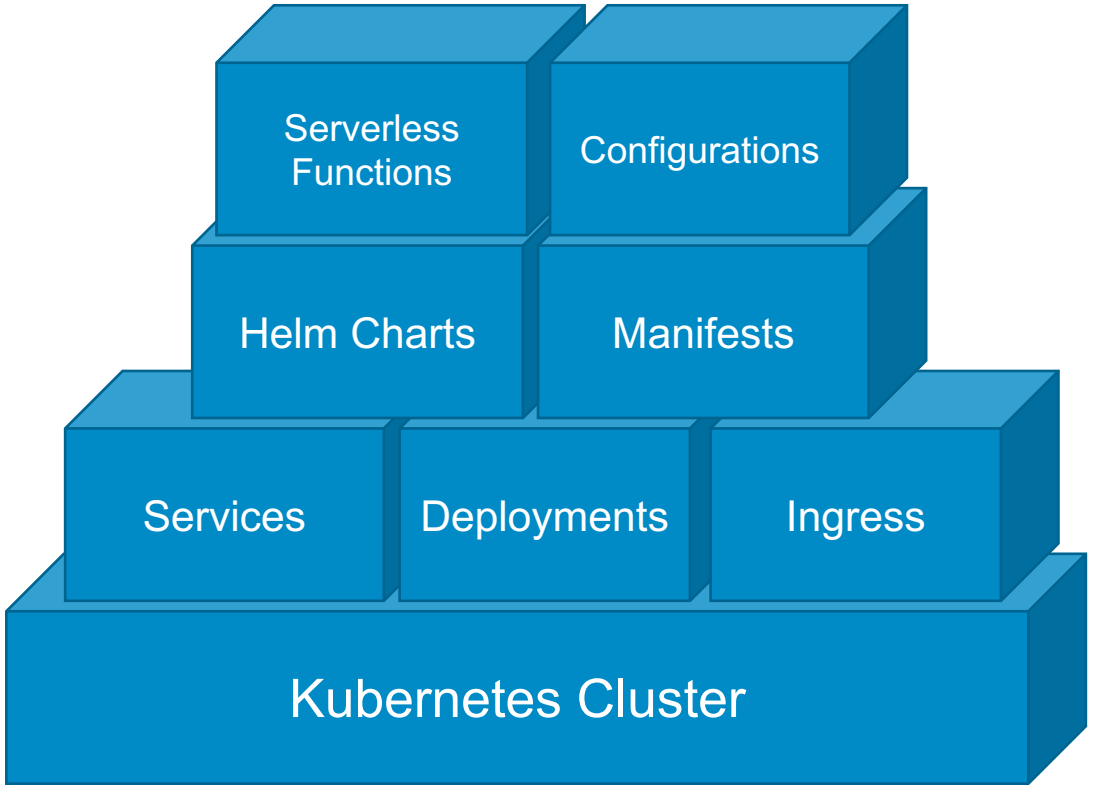
1. Where will we store stuff?
2. How will we pass messages?
3. What will tell us that something has happened and now something needs to be done



NATS Kubeless MINIO

Basic Building Blocks – Kubernetes

1. How do we add a new service on a cluster?
2. How do we deploy our software?
3. How do we expose it?
4. How do we deploy functions?
5. Where do we store the configs?



Basic Building Blocks

- Docker
  - Dockerfile
  - Dockerbuild
  - Docker hub
- Enterprise Messaging Patterns
  - NATS PubSub
- Kubernetes
  - Deployment
  - Services
- Serverless
  - Deployment

Time	Outcomes	Useful if
30	1. Learn all the building blocks 2. Get everything in place 3. Cluster is up and running	✓ You are new to Docker & Kubernetes ✓ You want to try at home later ✓ You want your cluster running

Deploy the Cluster

- Use *gcloud* command line to create a managed Kubernetes cluster on Google Cloud Platform
  - 5 node cluster
  - Autoscaling enabled
  - By default only 1 node is alive
  - Auto scaled to max 5 nodes based on load

Deploy Apps and Services

- Infrastructure Services
  - NATS (PubSub)
  - Minio (Object Storage)
  - Kubeless (Kubernetes native Serverless Platform)
- App Services
  - Sub-domain Enumeration (Serverless function)
  - OWASP ZAP Scanner (Pod)
  - Nmap Scanner (Pod)
  - Reporting Engine (Pod)
- Ingress
  - Expose API to submit a scan
  - Expose API to generate report

Execute the OSINT Workflow

- Sub-domain enumeration using CRT.SH
- Input is received from NATS (PubSub)
- Output is stored in object storage

Execute the Appsec Workflow

- OWASP ZAP Passive Scan
- Input is received from NATS (PubSub)
- Output is stored in object storage

Kubernetes SideCar Adapter

- Generic Go-lang program used as a adapter to integrate external tools such as OWASP ZAP, Nmap etc.
  - Listens on NATS (PubSub) Topic
  - Executes external tool based on PubSub input
  - Persists output to object storage

Target

appseck8sworkshop.com

Time	Outcomes	Useful if
15	1. See a scan complete 2. See the report 3. See how to add OAuth for security	✓ You want to see and understand the report ✓ You want to protect the reporting website

Results

- Output of a scan

Tech being used

- Static website generator based on aggregation of tool output
  - JSON as data source for EJS views
  - A random static website generator being used called Nanogen
  - Custom EJS views for templating
  - Basic CSS using Bulma

Oauth Configuration

- Our simple way to enable OAuth

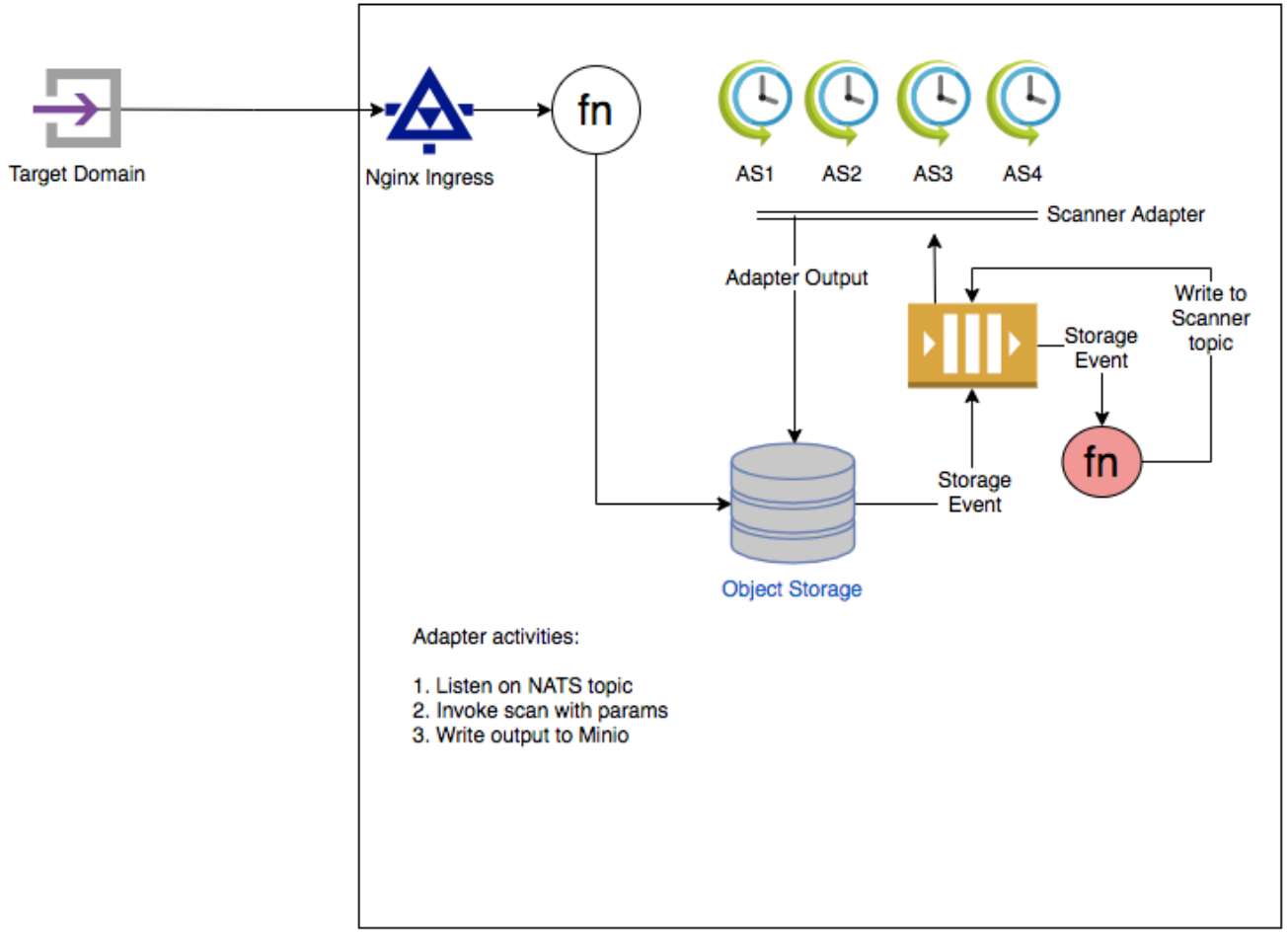
If you want to get started

- Get the code, config and documentation from https://github.com/appsecco/using-docker-kubernetes-for-automating-appsec-and-osint-workflows
- We will release this tomorrow 2nd of March 2019

APPSECCO

Time	Outcomes	Useful if
30	1. Discussion about our tool choices 2. Discussion about the current limitations 3. How state management is difficult here	✓ You want to know why we chose those tools ✓ Understanding the limitations is important for you

Architecture – How everything is glued in



Current Known Limitations

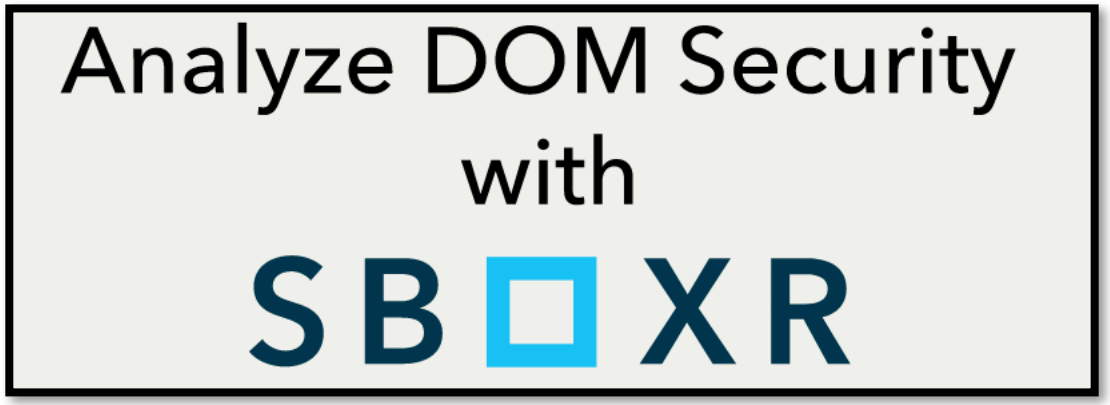
- Report is generated based on manual trigger through HTTP API
  - This is due to limitations in scan state management
- Running NATS in preemptible node results in issues with persistent connection with clients

Time	Outcomes	Useful if
15	1. Demo on how to add a new security tool 2. Mapping this to Cloud Native 3. Our plans for SPLAT	✓ You want to integrate your tools ✓ You prefer to do this outside Kubernetes

Adding a new tool

- Lets add `dnsrecon` as a tool for sub-domain enumeration

Another tool that we will be adding soon



Cloud Native Alternatives

Technology	Current Setup	AWS	Google Cloud Platform
Serverless	Kubeless	Lambda	Cloud Functions
Object Storage	Minio	S3	Cloud Storage
PubSub	Nats and Nats Queue	SQS	Cloud PubSub
Containers	Docker	ECS	GKE
Orchestrator	Kubernetes	AKS	GKE
Events and Triggers	Nats Triggers	CloudWatch Events	Cloud PubSub

Security Platform Led Automated Testing (SPLAT)

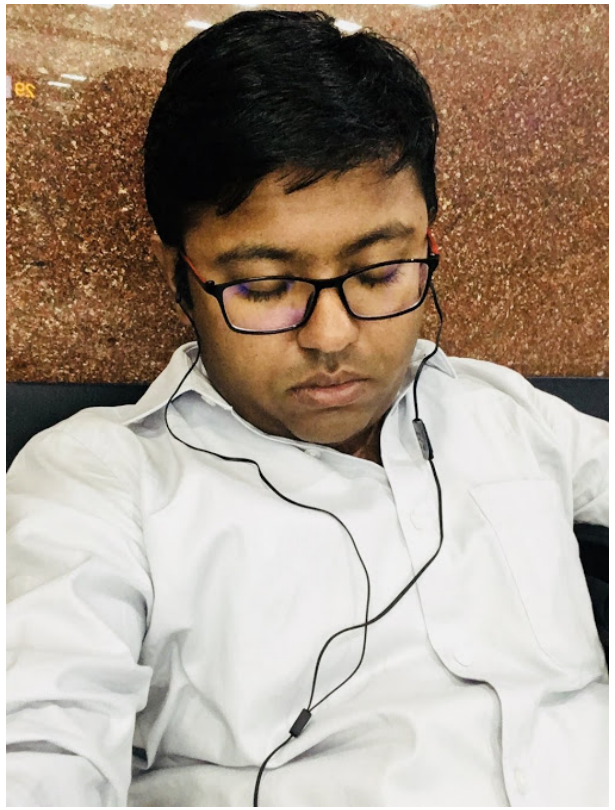
SPLAT is an automation platform, which allows for easy deployment of application security workflows supported by OSINT workflows such as security testing and variety of tasks traditionally carried out by InfoSec teams

APPSECCO

Primary Actors

Uber Ops – Madhu Akula

Uber Dev – Abhisek Datta



Advantages for a product security team

- Continuous Security is becoming a requirement
- All security tooling and servers which need to run all the time require operational security since these become high value targets
- Product Security Teams should embrace Infrastructure As Code and Immutable Infrastructure to deploy tooling to complete their application security workflows
- Once the workload is completed, tear down the infrastructure

DevOps & SecOps Parity

- Security workloads can be committed just like code
- These workloads can be triggered as part of CI/CD pipelines
- While the infrastructure is generating data, the data can be consumed by other tools, ticketing systems, alerting and monitoring systems

Cluster Tear Down

- Use *gcloud* command to tear down the cluster

Any Questions or thoughts?

Abhisek Datta| abhisek@appsecco.com | @abh1sek
Akash Mahajan | akash@appsecco.com | @makash
Madhu Akula | madhu@appsecco.com | @madhuakula

NULLCON X