{deepfactor}

OWASP®

AppSec 2.0: Reimagine AppSec with Runtime Analysis

OWASP LA Meetup

August 23, 2023

KIRAN KAMITY, CEO AND FOUNDER, DEEPFACTOR

What we'll cover today:

1. Limitations of first-gen AppSec tools

2. AppSec 2.0 powered by runtime

3. What can it help us accomplish?
   A. Runtime Enriched SCA
   B. Runtime Security

4. Technical deep dive & Demo

# # #

Alert Fatigue w/ SCA?

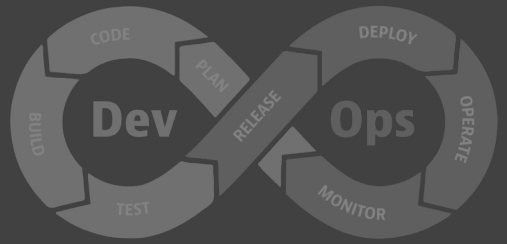
// AppSec 2.0

Correlate

Prioritize SCA & SBOM findings based on usage

Scan (OSS or Containers)

Generate SBOM and detect known vulns by scanning dependencies & containers during dev and CI



Run

- SCA scan at runtime
- Detect unknown vulns by observing runtime

Integrate

With dev and CI tools

// How Can Runtime Visibility Turbocharge AppSec

1. Runtime Enriched SCA

Correlate SCA scans with runtime to prioritize CVEs that matter and remove unused packages

2. Runtime Analysis In Dev & Test

Identify unknown vulnerabilities that can't be detected by SAST/SCA by analyzing running apps

3. Runtime Container Scans

Scan containers/ dependencies for CVEs in K8S environments

4. Runtime Security In Prod

Detect insecure file, network & memory behaviors for compliance with SOC2 & other

Dev

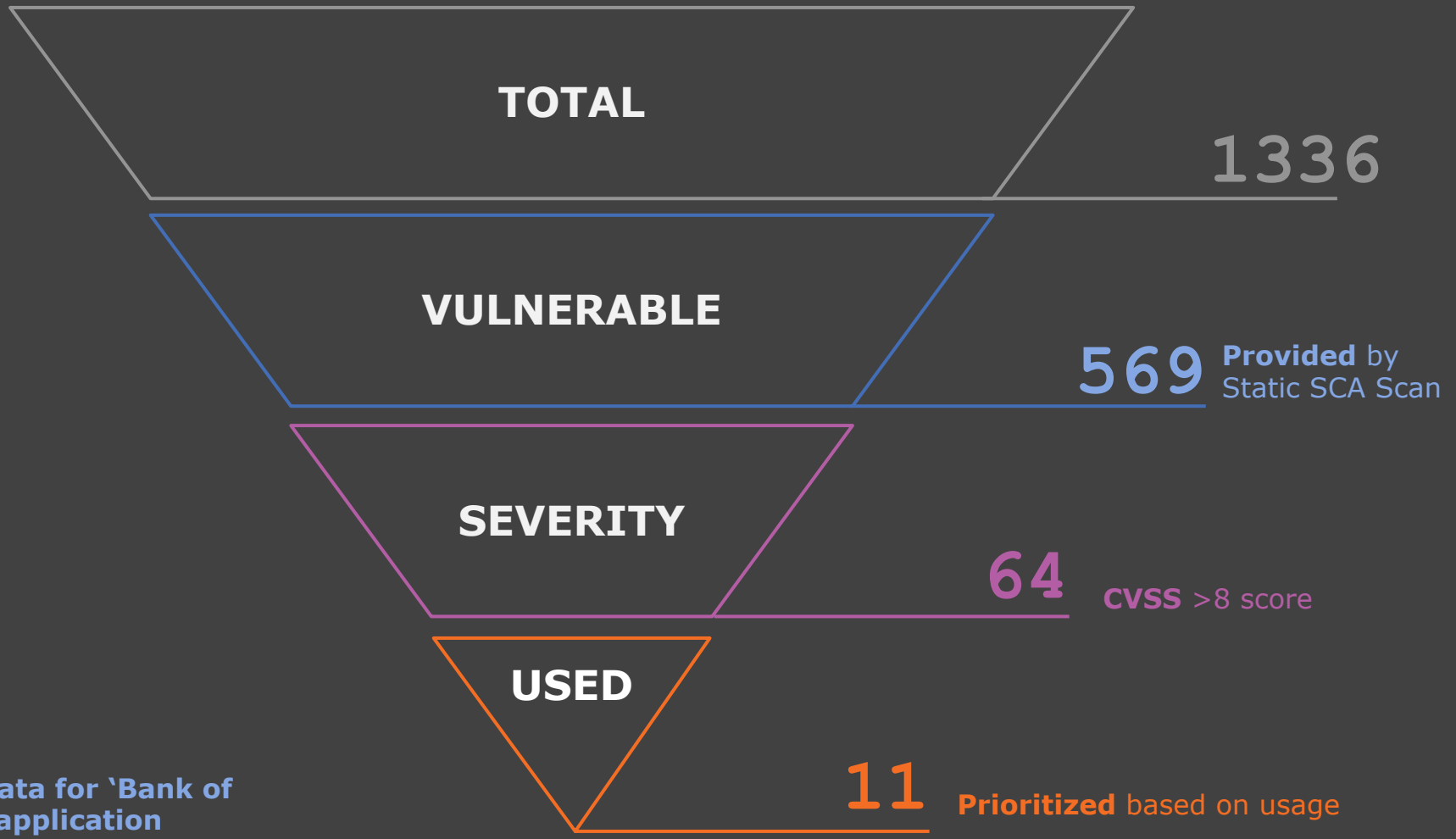
Prod

Runtime Software Composition Analysis

# # #

{df}

//The Holy Grail: Prioritize Based On Actual Usage



Actual Data for 'Bank of Anthos' application with 9 microservices

// Filtering SCA False Positives & Reducing Alerts

// Reachability & Usage: Technical Approaches

	Runtime Analysis	Call Graph Analysis
Ability to detect reachable modules in dependencies		
Support for OS packages used in containers		
Ability to detect actual usage for dependencies and/or OS packages		
Ability to detect dynamically loaded modules (such as reflections)		
De-prioritization of deadcode/unused code		
Language Agnostic		

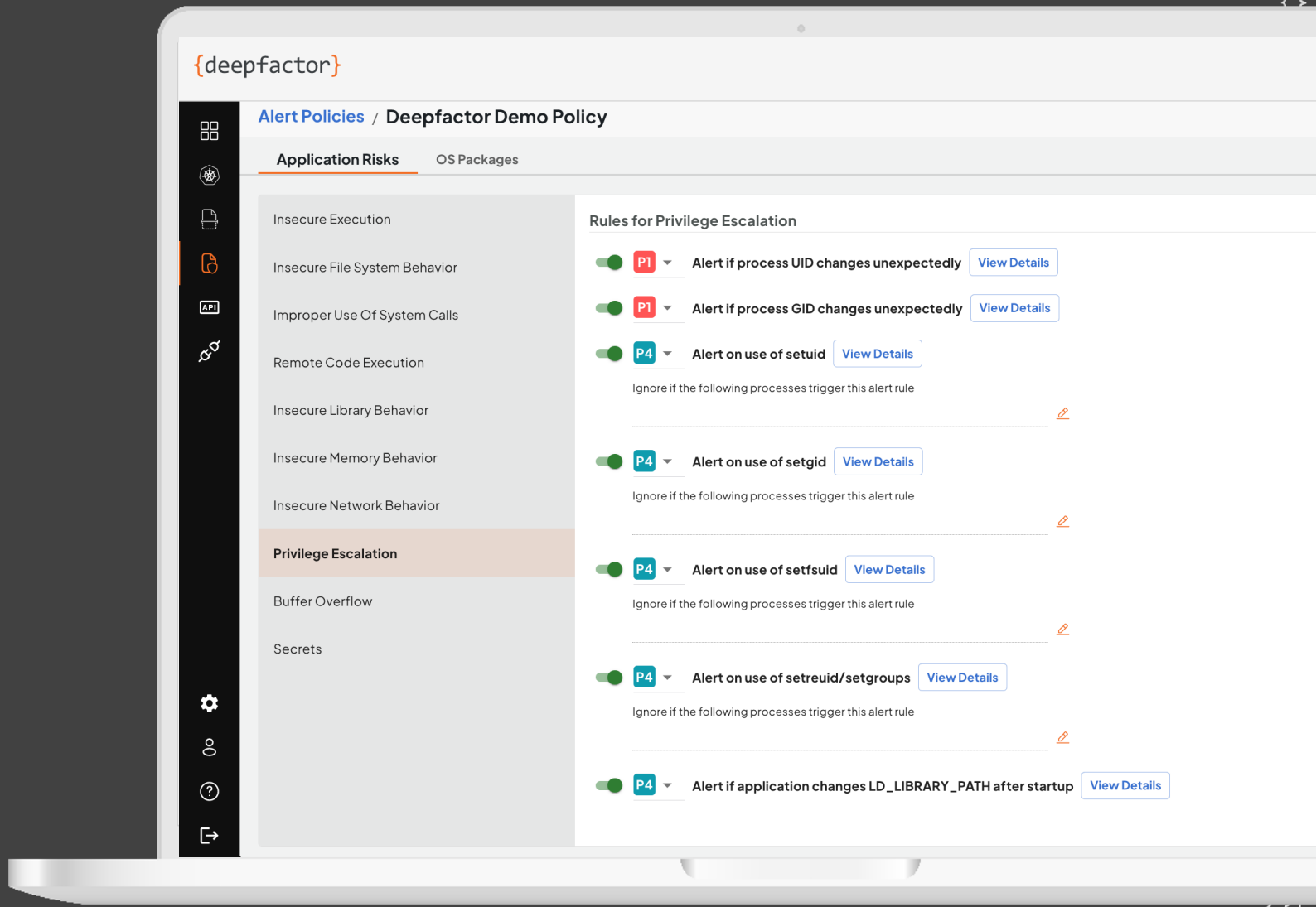
Runtime Analysis & Security

# # #

// Detecting Insecure Behaviors at Runtime

Runtime Security

- Execution
- File system behavior
- System calls
- Remote code execution
- Library behavior
- Memory behavior
- Network behavior
- Privilege escalation
- Buffer overflow
- Secrets



Technical Deep-dive & Demo

# # #

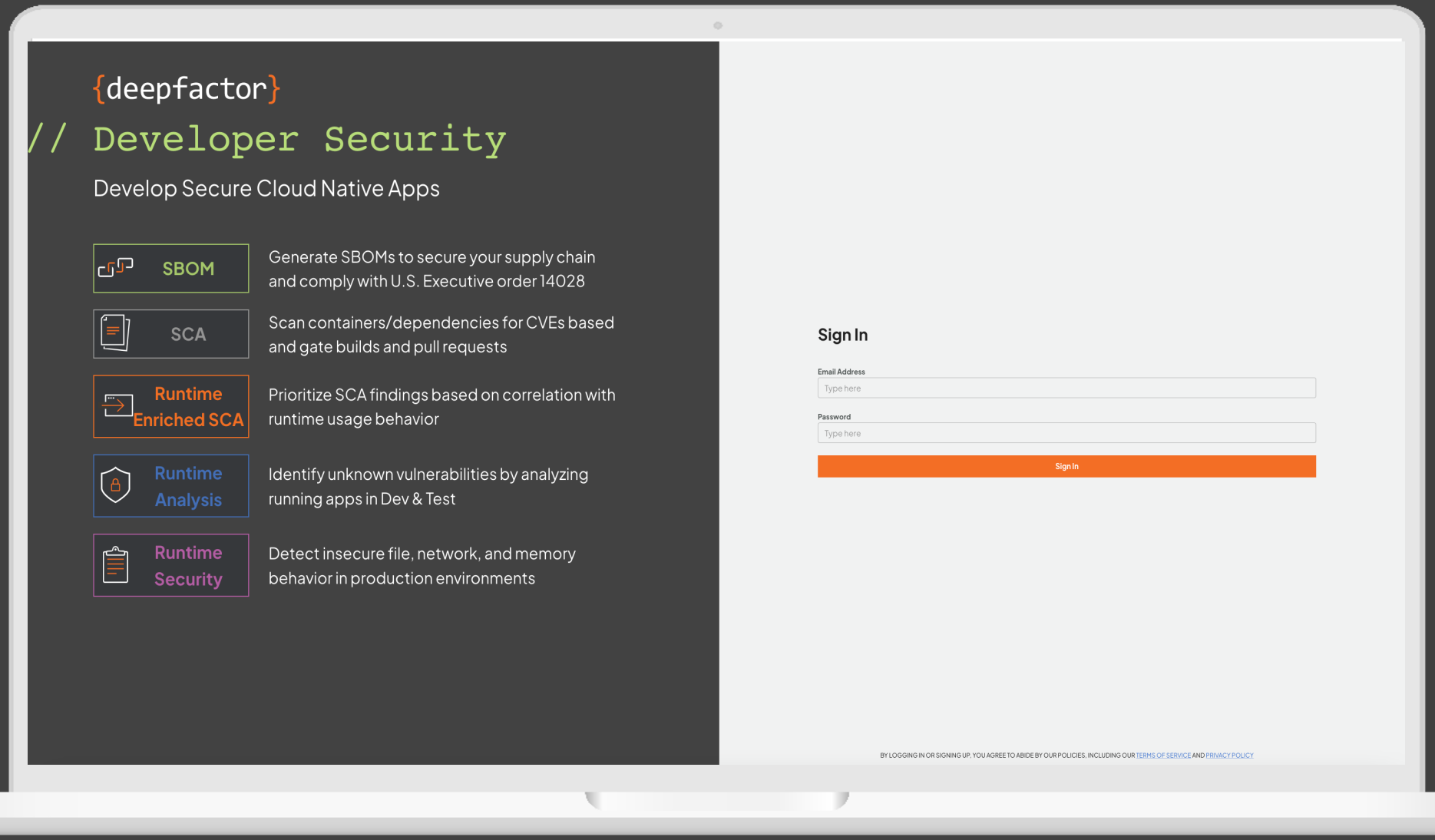
// Userspace Interception vs eBPF

	Deepfactor	eBPF
Best suited for	Dev (shift left runtime security & correlation with SCA)	Ops (Live threat detection)
Technical Approach	LD_PRELOAD & language agents	Enabling eBPF in the host OS
Granularity	Enable at a process/container level	Enable at host level
Performance Overhead	Low	Low
Language Agents	Visibility into classes loaded etc. (required for correlation with SCA)	No visibility at the language agent level
Support for AWS Fargate, Lambda w/ containers, AWS ECS, Docker Swarm etc..	Supported (Docker build w/ libdf.so)	No support
Visibility into userspace of process	Yes (visibility into certificates, memory allocation behaviors, process behaviors ..)	No visibility above system call layer

// Observing Running Apps For Various Deployment Types

- Monolithic applications
  - dfctl run -a "my application" --cmd COMMAND_WITH_ARGUMENTS
- Containers
  - dfctl run -a "my application" --docker-run DOCKER_RUN_OPTIONS --image IMAGE
- Kubernetes
  - helm --install df-webhook-stable -n df-webhook deepfactor/webhook --set clusterName=CLUSTER_NAME_OF_YOUR_CHOICE --create-namespace -f webhook-override.yaml
- Docker Swarm, AWS ECS, Lambda w/ container …
  - docker build -f Dockerfile.df --build-arg "APP_IMAGE=${APP_IMAGE}" --build-arg "APP_IMAGE_ID=`docker inspect ${APP_IMAGE} --format '{{.Id}}'`" --build-arg "DF_APP_NAME=my application" .

// Demo


{deepfactor}
// Developer Security
Develop Secure Cloud Native Apps
SBOM
Generate SBOMs to secure your supply chain and comply with U.S. Executive order 14028
SCA
Scan containers/dependencies for CVEs based and gate builds and pull requests
Runtime Enriched SCA
Prioritize SCA findings based on correlation with runtime usage behavior
Runtime Analysis
Identify unknown vulnerabilities by analyzing running apps in Dev & Test
Runtime Security
Detect insecure file, network, and memory behavior in production environments
Sign In
Email Address
Type here
Password
Type here
Sign In
BY LOGGING IN OR SIGNING UP, YOU AGREE TO ABIDE BY OUR POLICIES, INCLUDING OUR TERMS OF SERVICE AND PRIVACY POLICY

// Learn More?

Deepfactor Free Trial

An integrated approach to next-gen AppSec: SCA, SBOM, Container Scans, Runtime SCA & Runtime Security

SCA 2.0 Whitepaper

A Framework to Prioritize Risk, Reduce False Positives, and Eliminate SCA Alert Fatigue”

Questions?

###

{deepfactor}

Thank you

Kiran Kamity

Connect on Linkedin

Email: kiran@deepfactor.io