CHECK POINT™

SE Masters - 2025 Introduction to CloudGuard WAF

Web & API Deployment on a Kubernetes Cluster

Vince Mammoliti – Head of Channel Engineering Canada

Rolando Panez – Cloud Security Architect

Dec 9-10 2025, Miami

YOU DESERVE THE BEST SECURITY

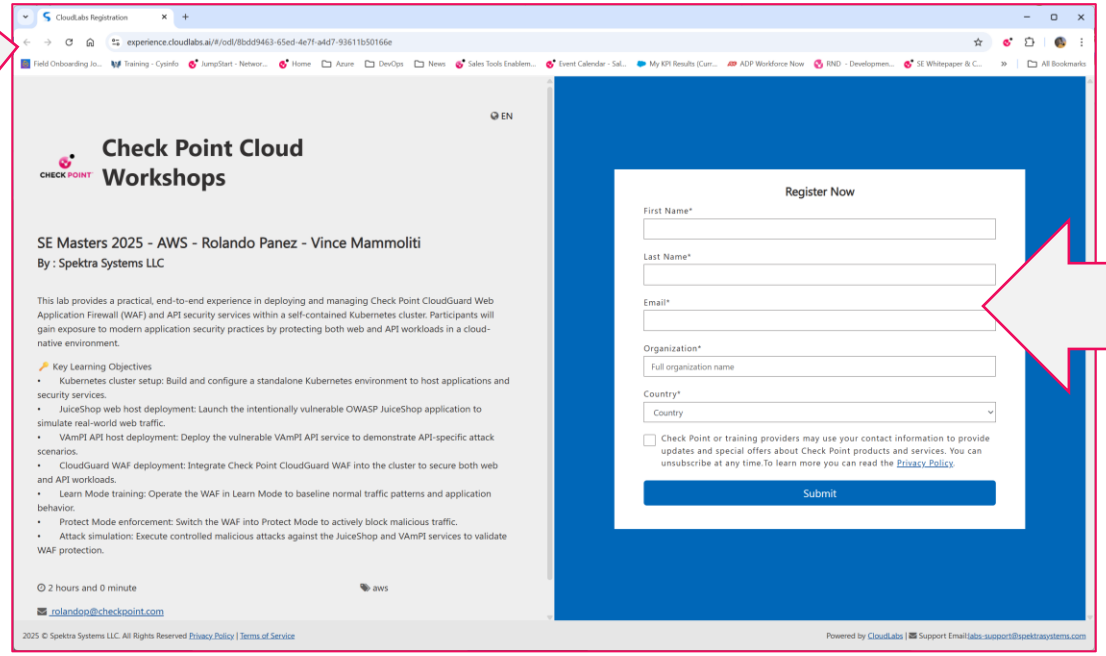
Lab Login Setup

Register and Start Lab

Enter URL

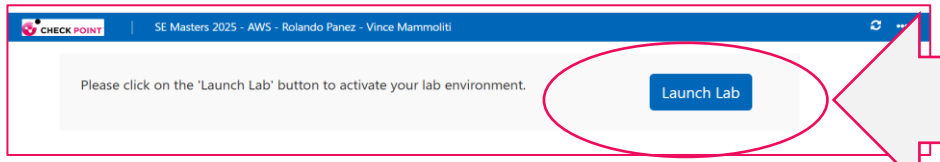
https://bit.ly/48A9WK0

1



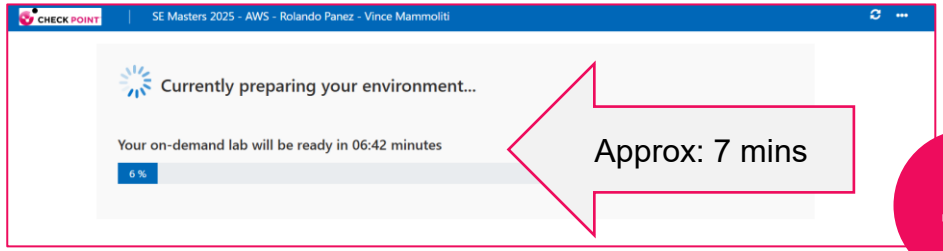
2

Register for Lab



Launch Lab

3



Approx: 7 mins

4

©2025 Check Point Software Technologies Ltd.

Agenda

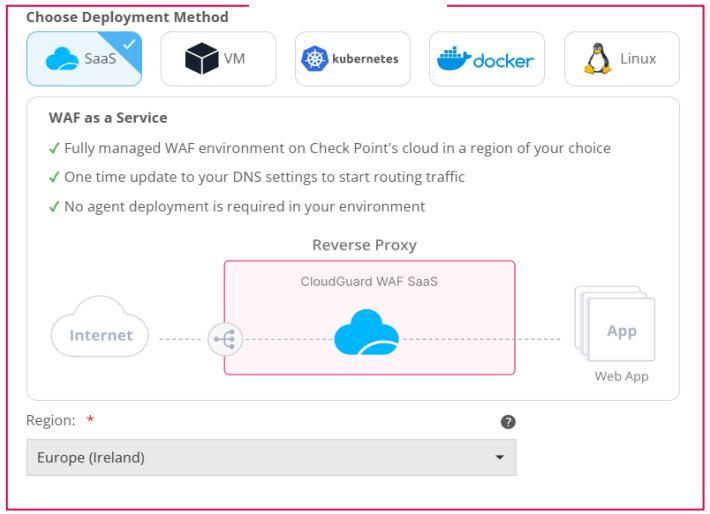
- Register and Start Virtual Lab Environment
- Lab Overview
- Objectives
- Login into Infinity Portal and Create WAF Assets in Learn Mode
- Configure Virtual WAF Lab and Start Kubernetes Containers
- Validate Lab Environment is Properly Functioning
- Generate Known Good Web and API Traffic
- Review Finding
- Switch WAF to Protect Mode and Generate Malicious Traffic
- Review Findings

©2025 Check Point Software Technologies Ltd.

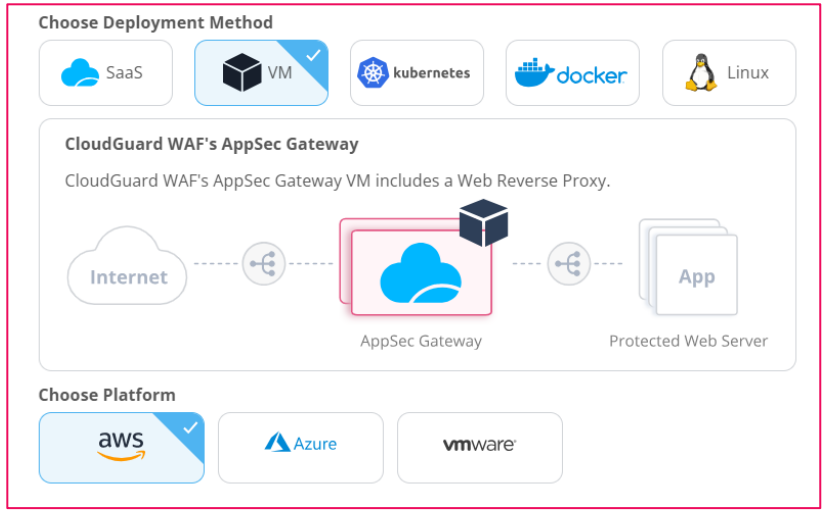
CloudGuard WAF

Deployment Methods

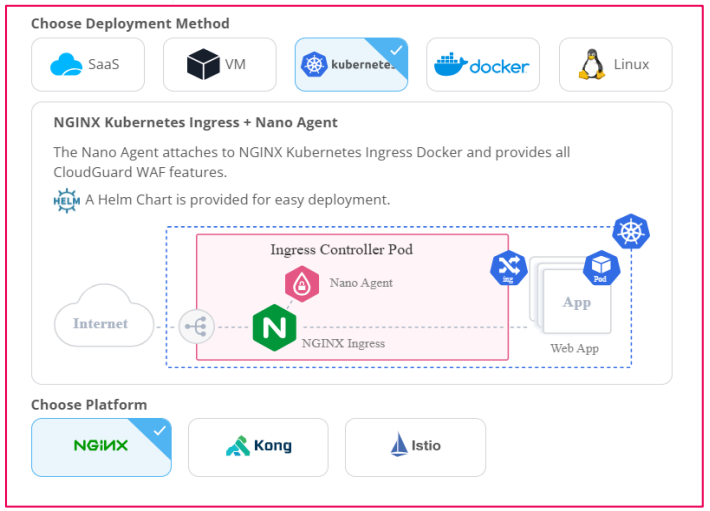
SaaS



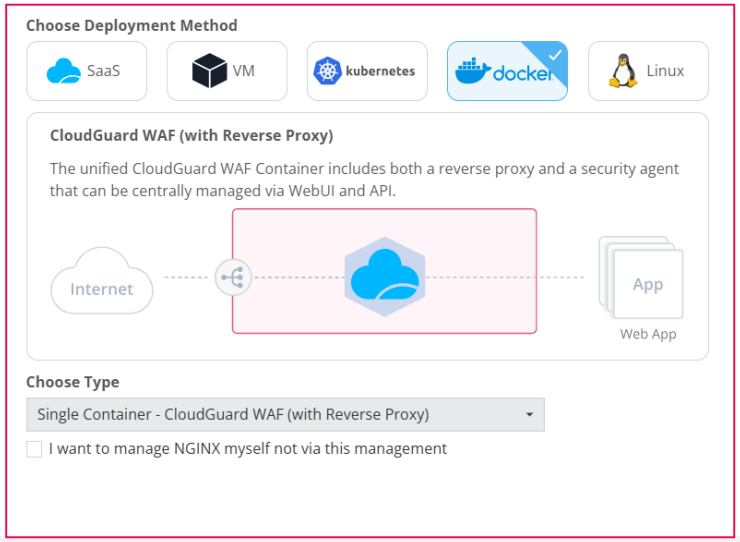
VM



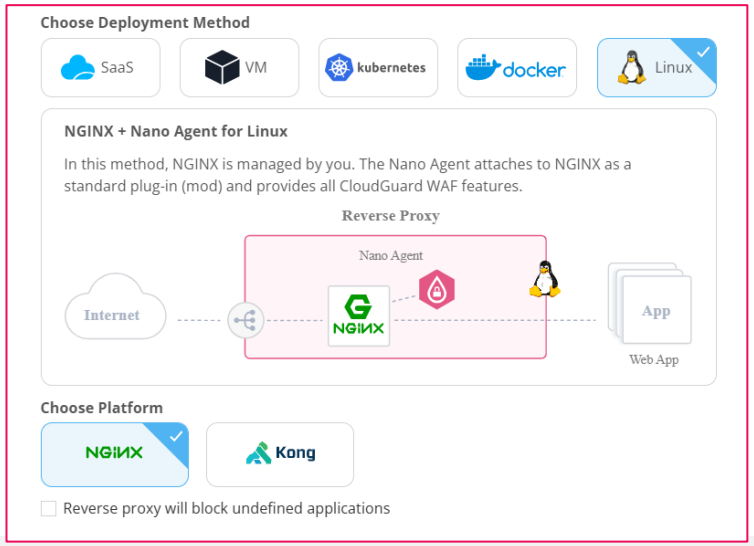
kubernetes



docker



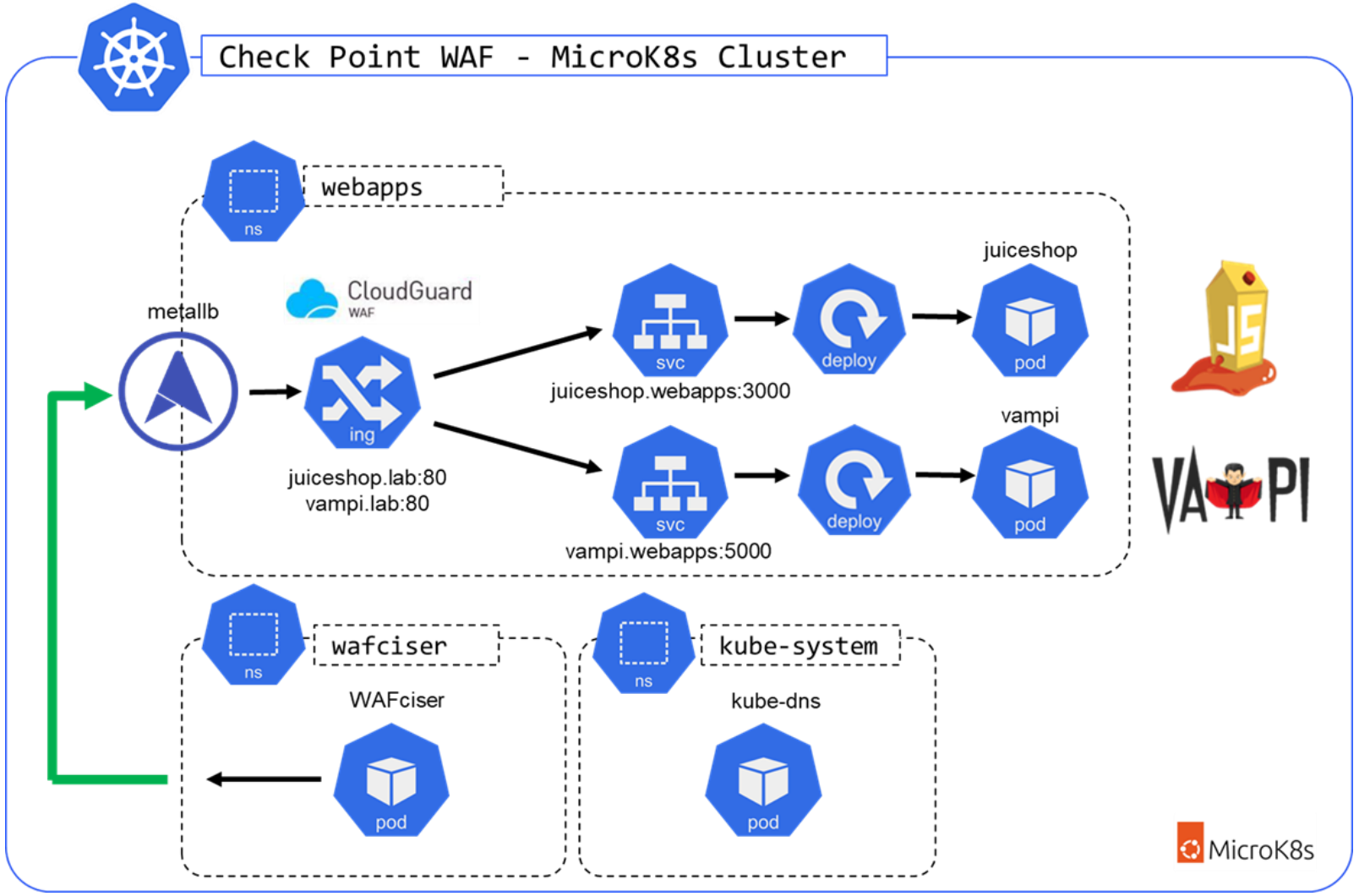
Linux



©2025 Check Point Software Technologies Ltd.

Lab Architecture Overview

Ubuntu MicroK8S Kubernetes Deployment



WAF

- Web Application Firewall

Kubernetes

- K8S – Open-Source auto scaling, container deployment management

MicroK8s

- Lightweight K8S distribution

Juice-Shop

- Insecure Web Host

VAmPI

- Vulnerable API Host

©2025 Check Point Software Technologies Ltd.

Objectives

- Introductions to Check Point CloudGuard WAF
- Configure Virtual WAF Lab and Start Kubernetes Containers
- Understand the Learning and Monitoring Capabilities
- Leave with understanding on to deploy and support CloudGuard WAF

©2025 Check Point Software Technologies Ltd.

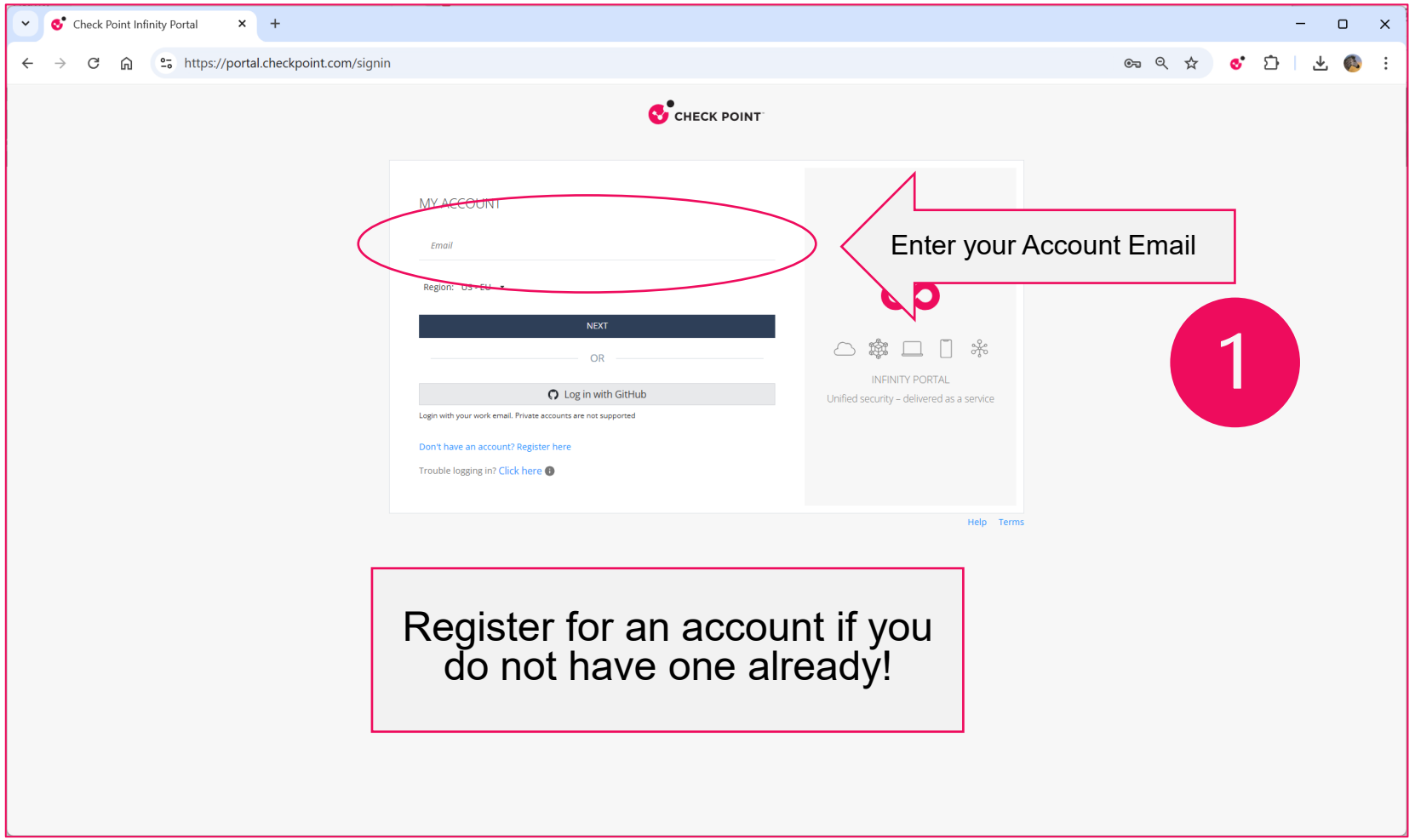
Agenda

- Register and Start Virtual Lab Environment
- Lab Overview
- Objectives
- Login into Infinity Portal and Create WAF Assets in Learn Mode
- Configure Virtual WAF Lab and Start Kubernetes Containers
- Validate Lab Environment is Properly Functioning
- Generate Known Good Web and API Traffic
- Review Finding
- Switch WAF to Protect Mode and Generate Malicious Traffic
- Review Findings

©2025 Check Point Software Technologies Ltd.

Infinity Portal

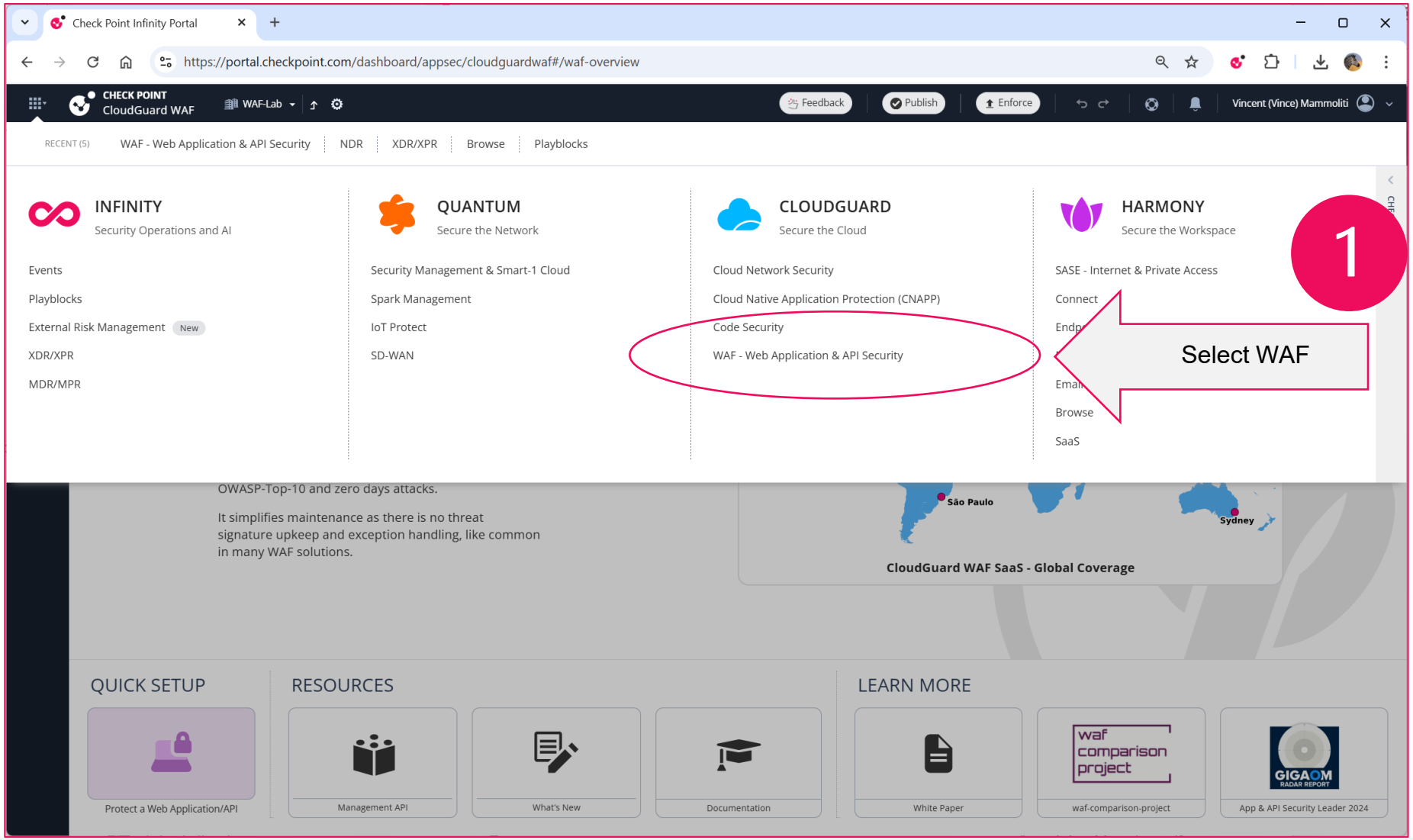
Login into the US-EU Infinity Portal



©2025 Check Point Software Technologies Ltd.

Infinity Portal

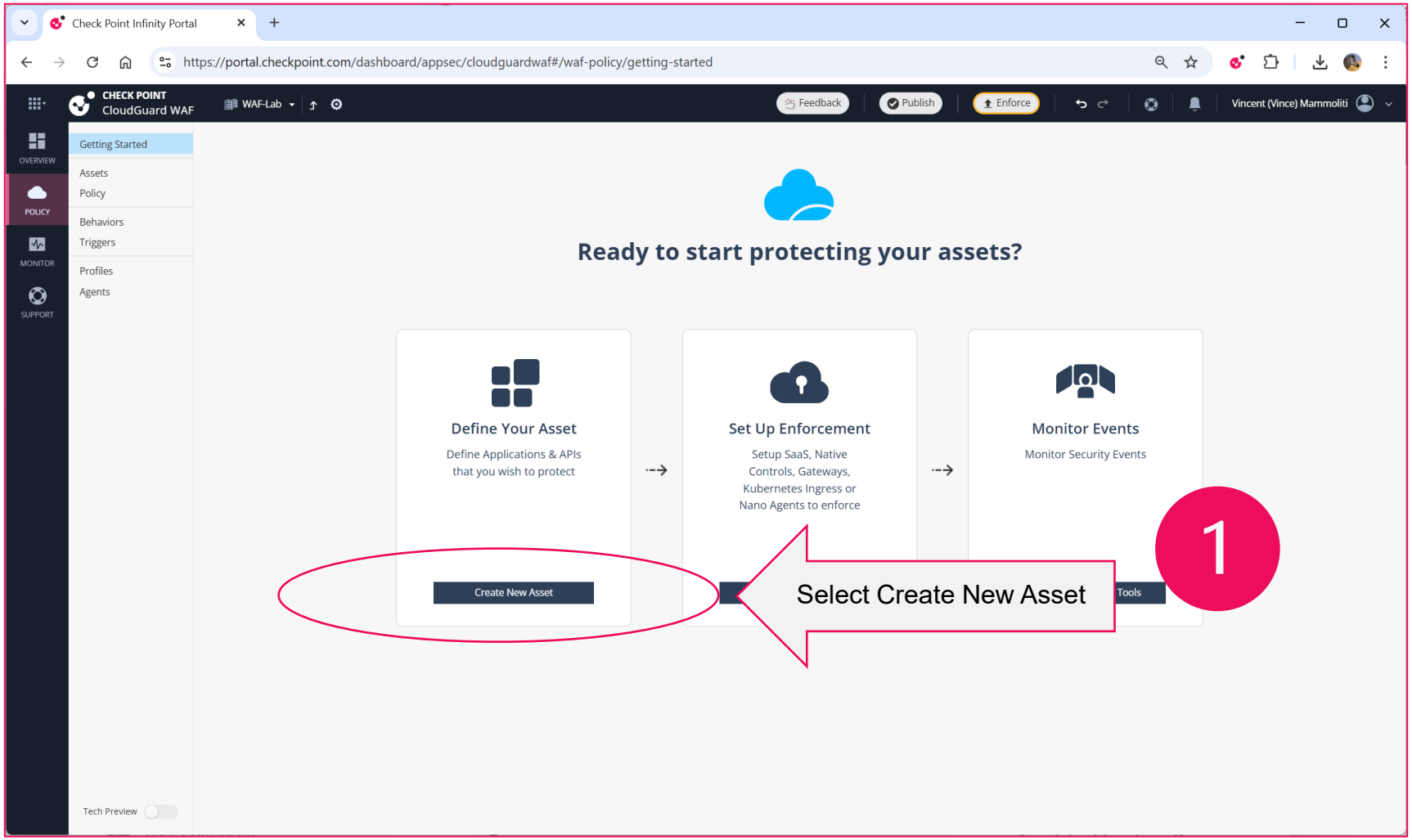
Selecting WAF – Web Application & API Security



©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

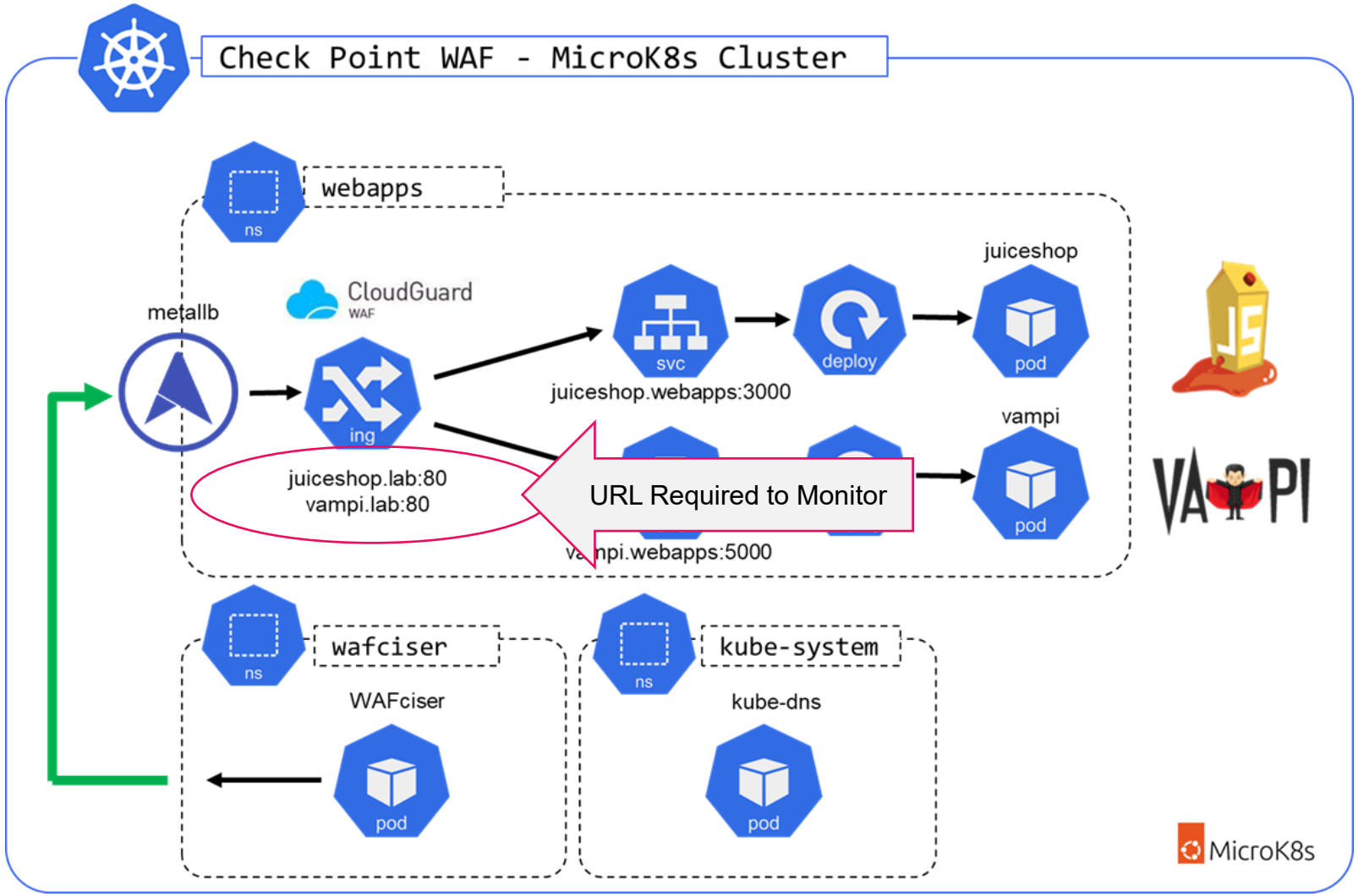
Creating a New Asset



©2025 Check Point Software Technologies Ltd.

Lab Architecture Overview

URLs for WAF to Monitor



Kubernetes

- K8S – Open-Source auto scaling, container deployment management

MicroK8s

- Lightweight K8S distribution

Juice-Shop

- Insecure Web Host

VAmPI

- Vulnerable API Host

©2025 Check Point Software Technologies Ltd.

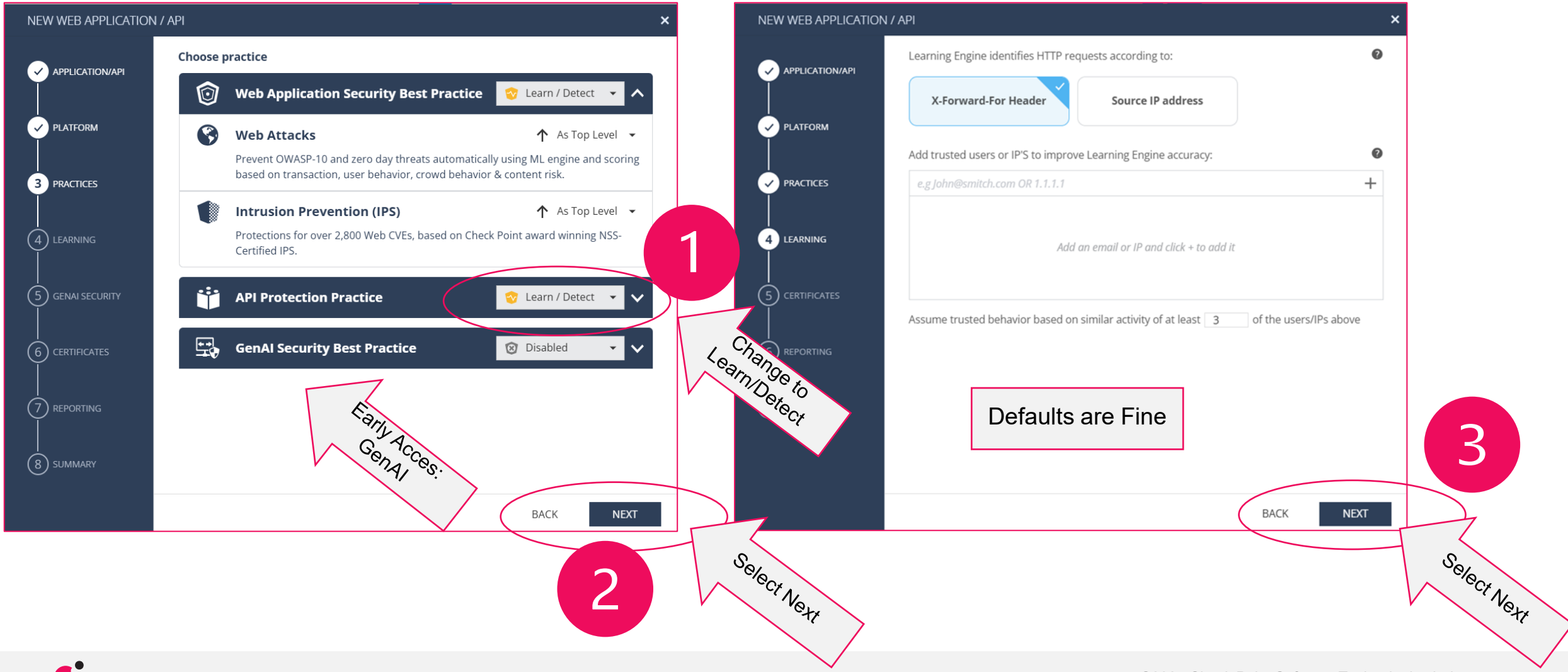
CloudGuard WAF

Creating the Kubernetes based WEB Asset – NGINX Ingress Controller

©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

Selecting Web Application to Lean/Detect – Using X-Forward-For Header for traffic identification



©2025 Check Point Software Technologies Ltd.

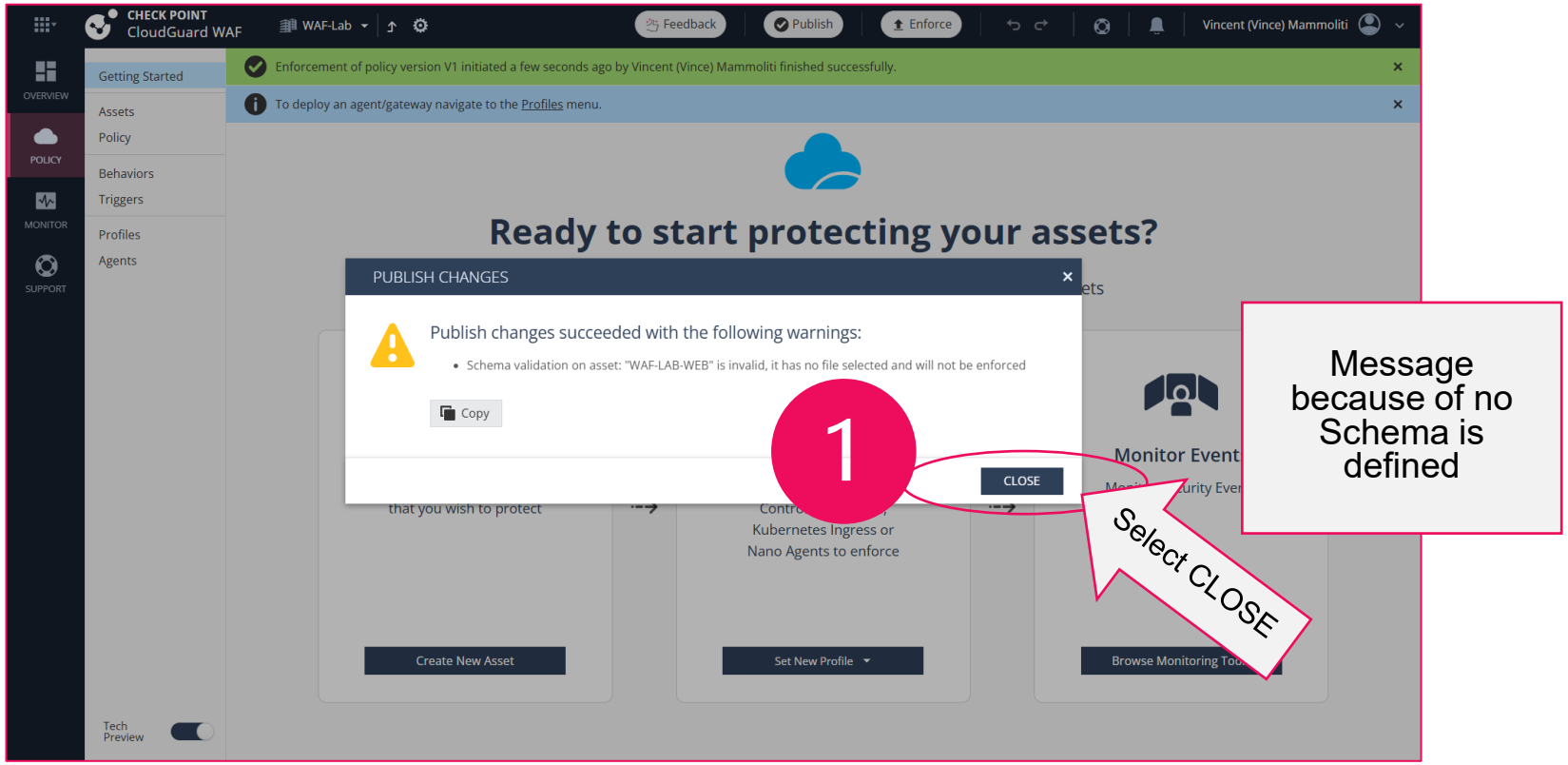
CloudGuard WAF

Certificates, Reports & Final Summary

©2025 Check Point Software Technolog

CloudGuard WAF

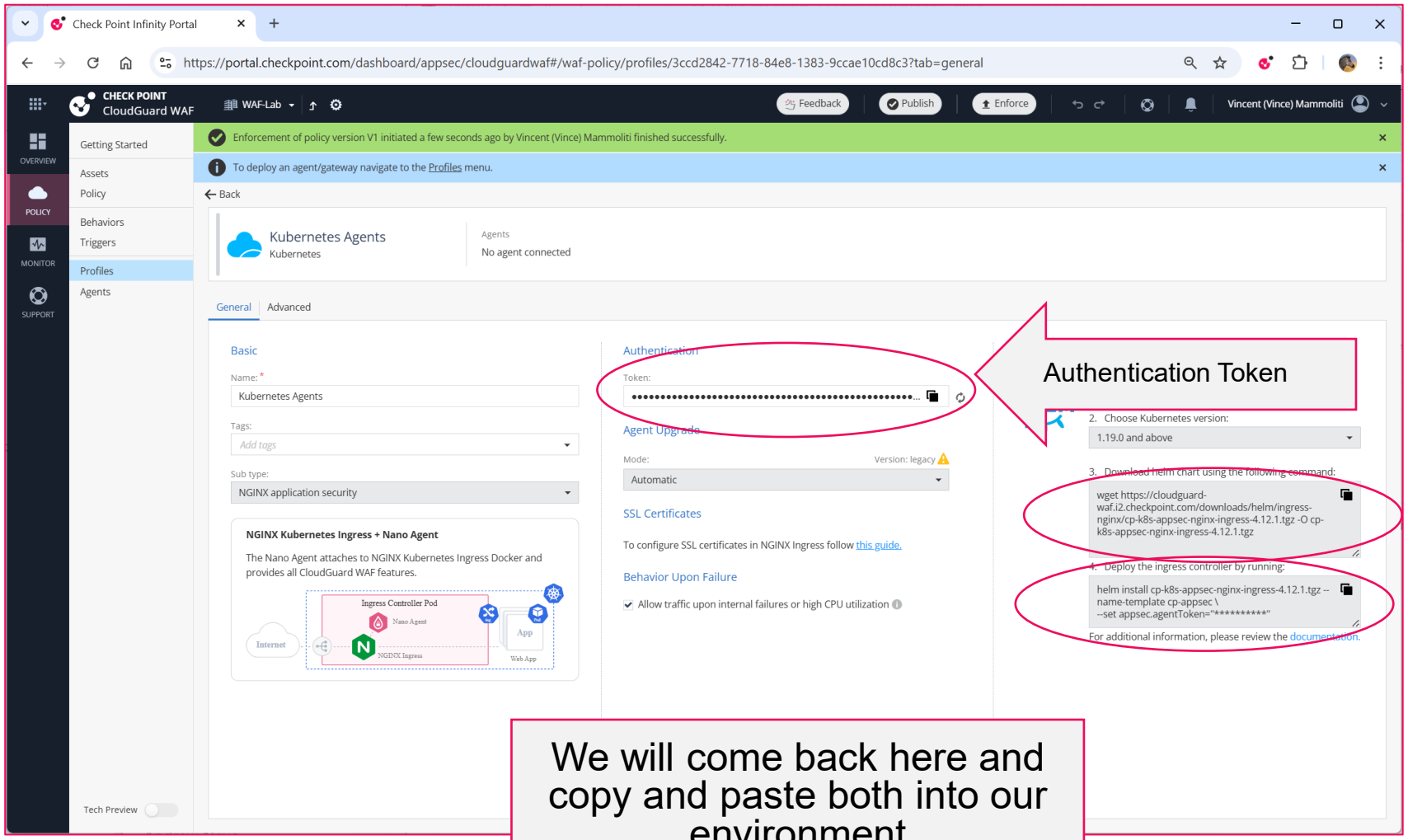
Certificates, Reports & Final Summary



©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

WAF Agent Profile – Acquire Key and Helm Chart to Deploy



Authentication Token

1

wget – fetches WAF ingress controller

Helm command to install WAF

2

We will come back here and copy and paste both into our environment

©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

Enforce

Need to be Selected
To
Deploy and Enforce Changes

The Orange Ring indicates you need to Select to Deploy and Enforce Changes

©2025 Check Point Software Technologies Ltd.

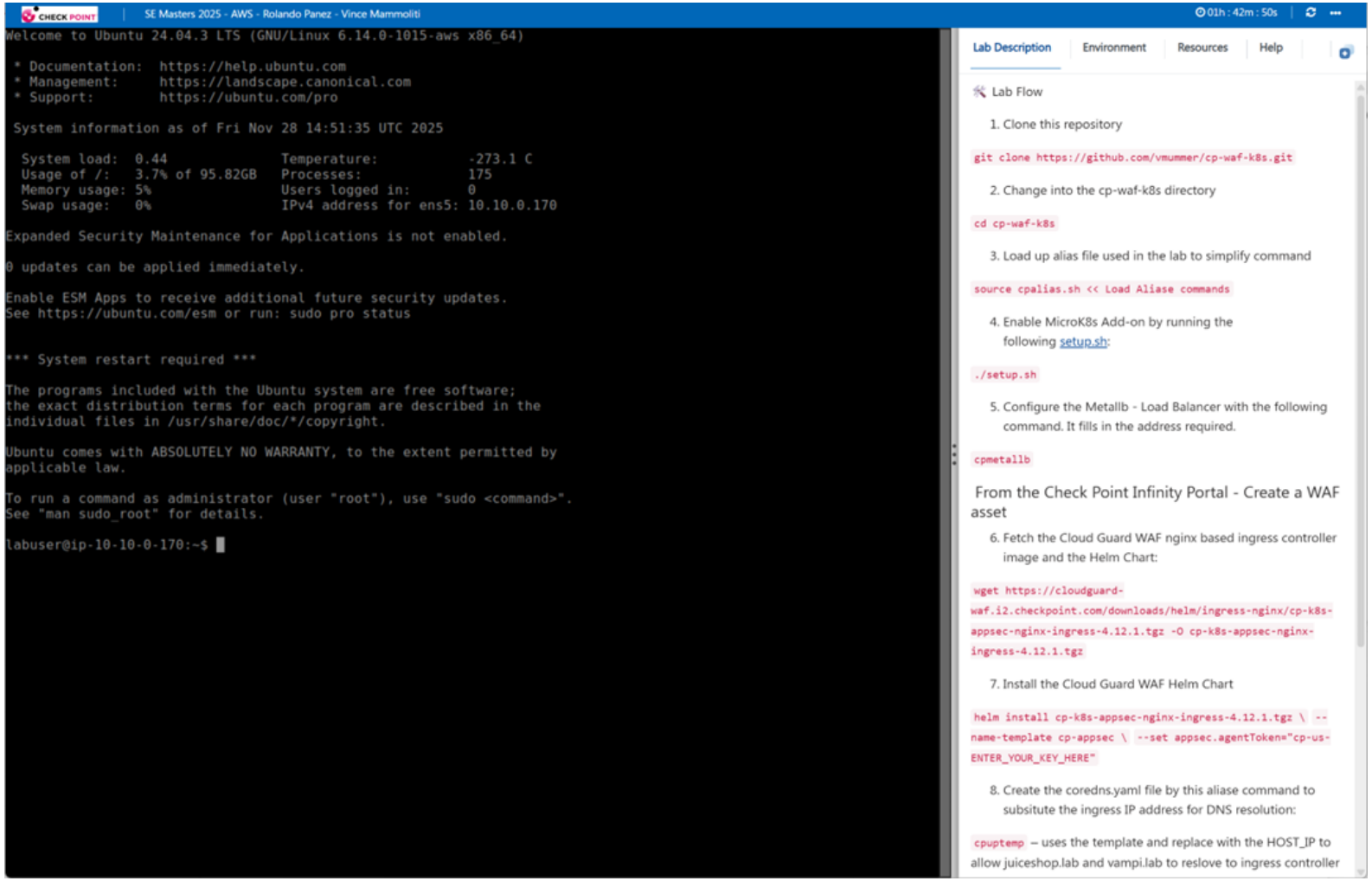
Agenda

- ❑ Register and Start Virtual Lab Environment
- ❑ Lab Overview
- ❑ Objectives
- ❑ Login into Infinity Portal and Create WAF Assets in Learn Mode
- ❑ Configure Virtual WAF Lab and Start Kubernetes Containers
- ❑ Validate Lab Environment is Properly Functioning
- ❑ Generate Known Good Web and API Traffic
- ❑ Review Finding
- ❑ Switch WAF to Protect Mode and Generate Malicious Traffic
- ❑ Review Findings

©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

Lab Ready

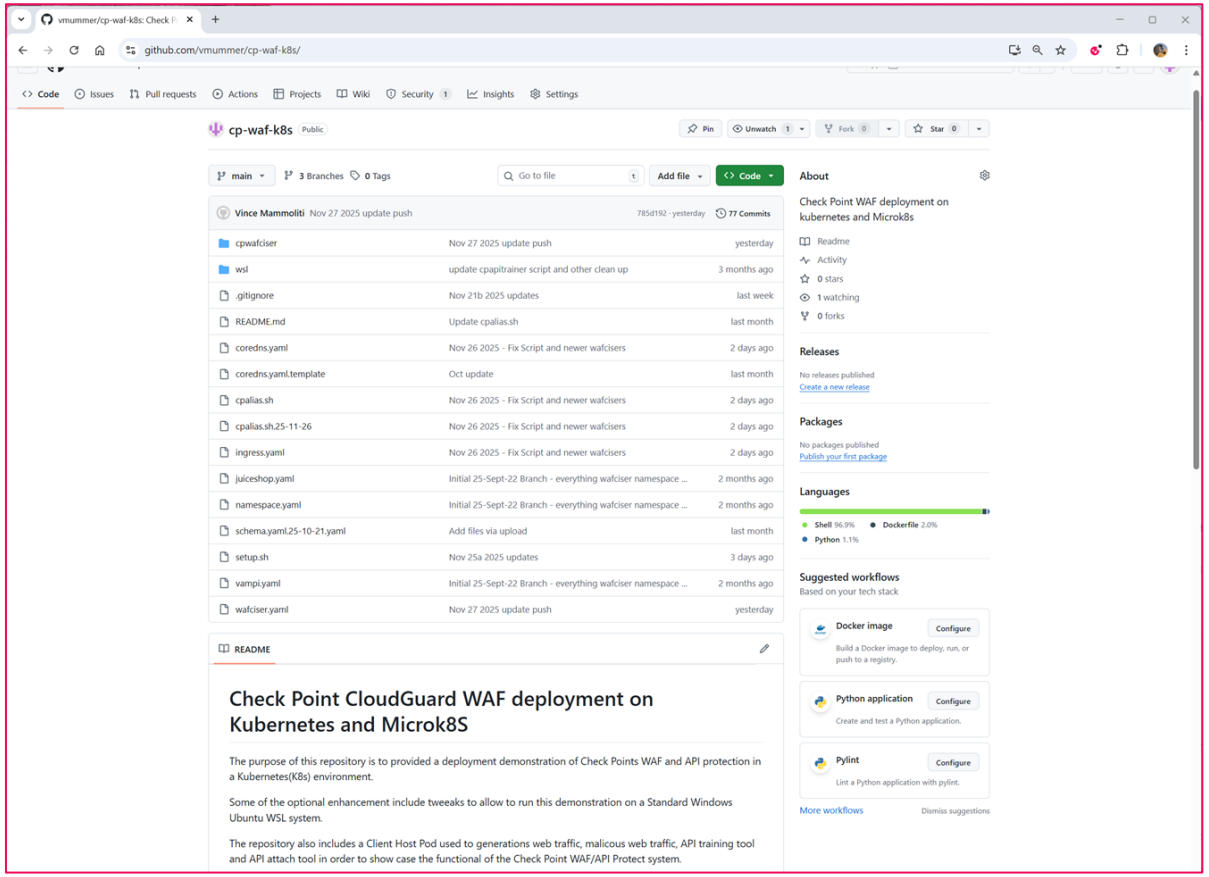


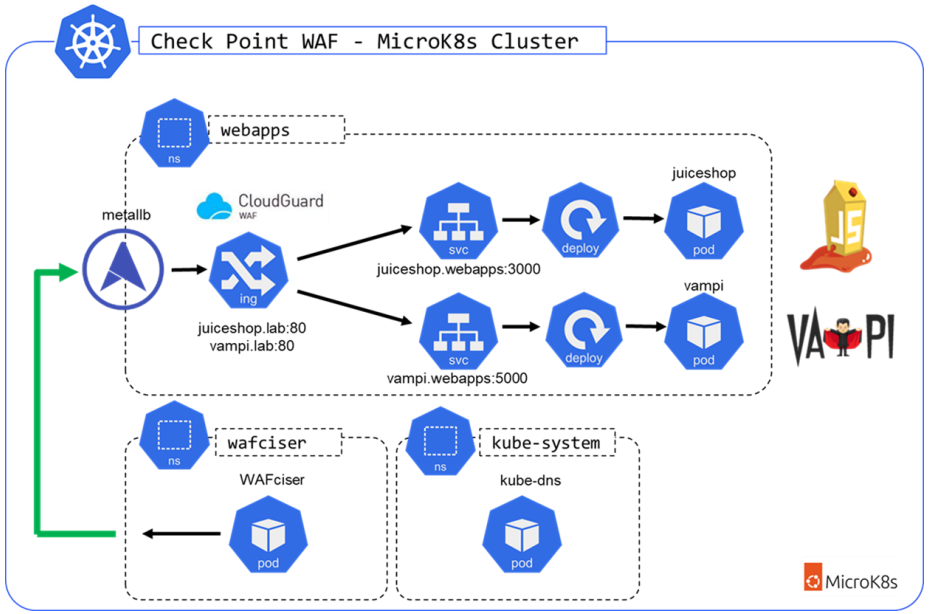
©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

Git Lab Repository

https://github.com/vmummer/cp-waf-k8s

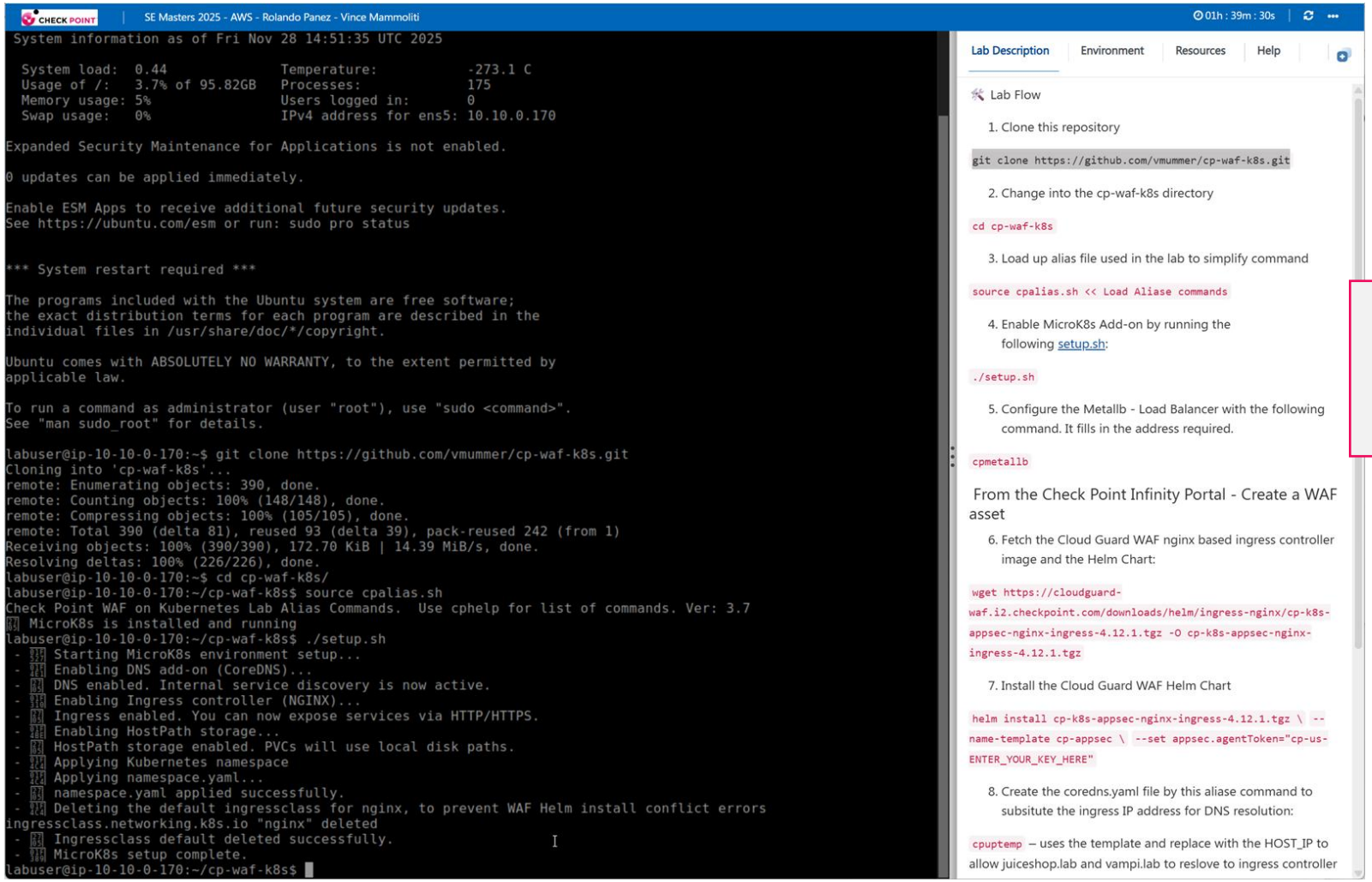




©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

Setup MicroK8s Environment

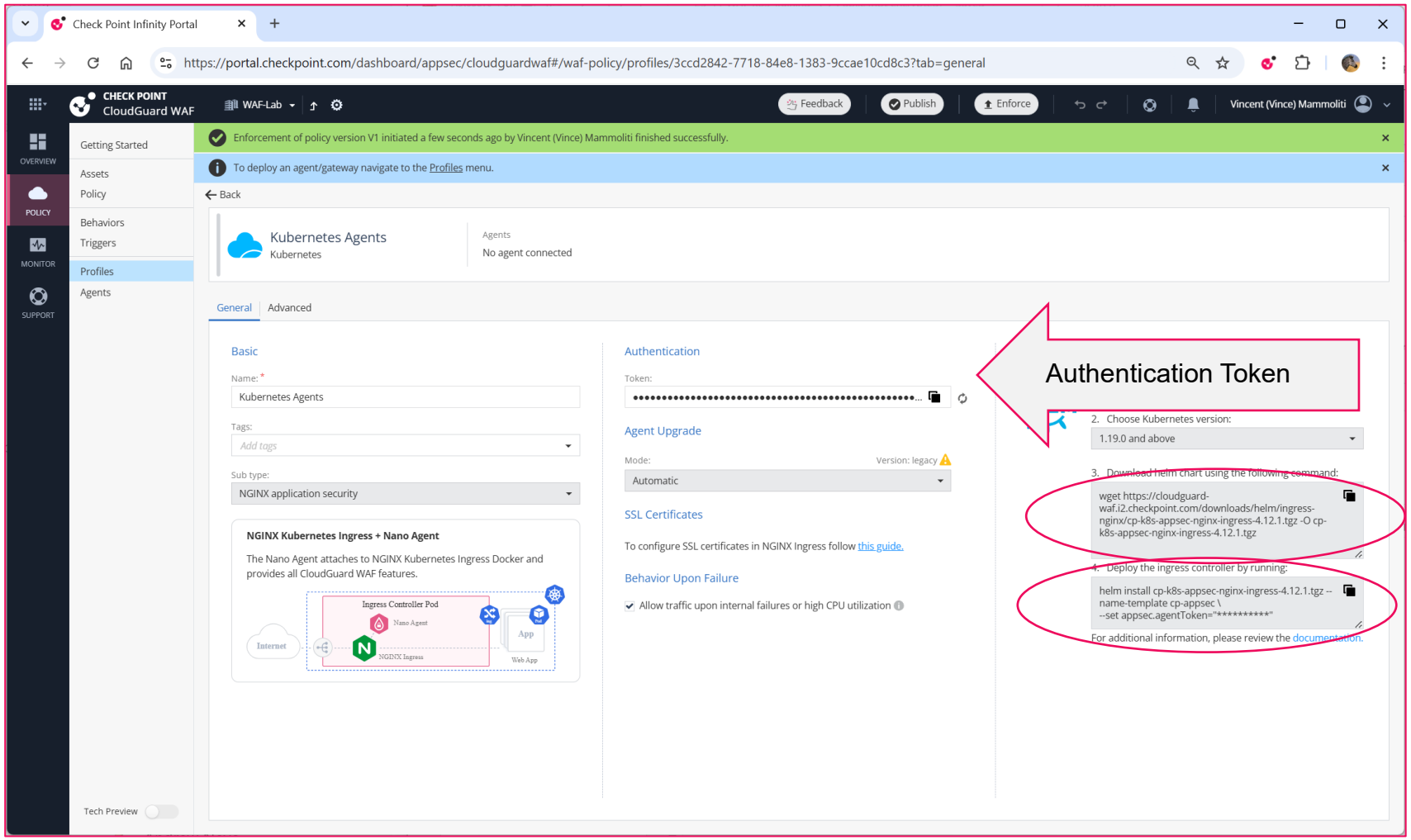


Follow the Instructions in the LAB

©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

WAF Agent Profile – Acquire Key and Helm Chart to Deploy

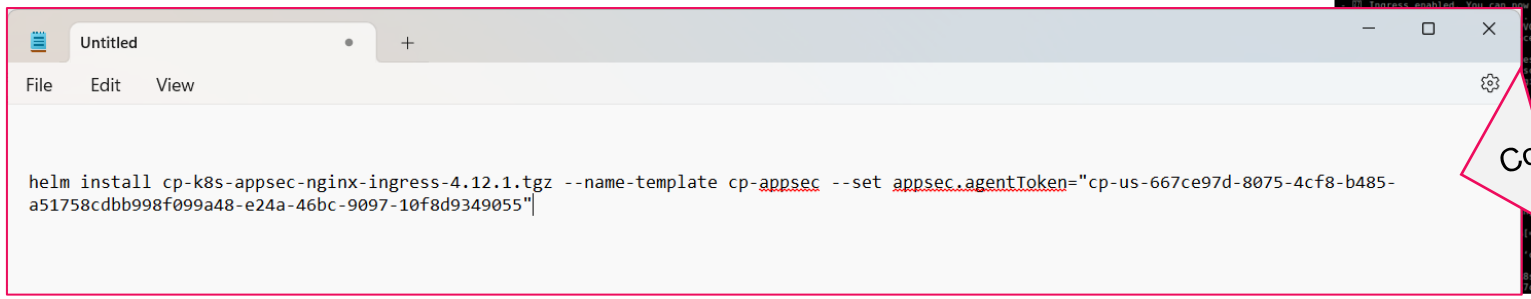


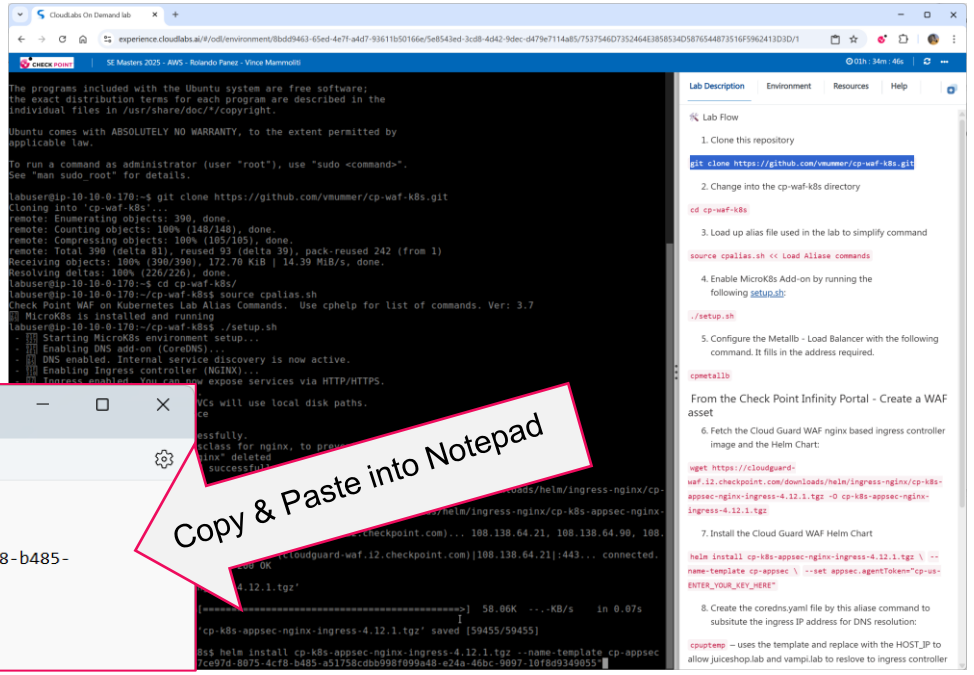
©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

Copy and Paste HELM install command

```
helm install cp-k8s-appsec-nginx-ingress-4.12.1.tgz --name-template cp-appsec \
--set appsec.agentToken="cp-us-e2ba52de-1582-41bf-b15f-XXXXXXX-068b-42dd-9f5e-XXXXXXXX"
```






```
helm install cp-k8s-appsec-nginx-ingress-4.12.1.tgz --name-template cp-appsec --set appsec.agentToken="cp-us-e2ba52de-1582-41bf-b15f-XXXXXXX-068b-42dd-9f5e-XXXXXXXX"
```

Copy & Paste into Note Pad,
make it one line,
then Copy & Paste into Lab

©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

Enable microK8s metallb (Load Balancer) and remainder of Services

cpmetallb	Installs Micro8Ks Metalb Loadbalancer
cpuptemp	Creates coredns.yaml from template
ka –f coredns.yaml	Load K8S DNS with juiceshop.lab & vampi.lab
ka –f juiceshop.yaml –f vampi.yaml –f wafciser.yaml	Start web applications
ka –f ingress.yaml	Enable Ingress Controller
cpurltest	Check if Juice Shop and VAmPI pods are reachable
cpdnscheck	Validate the K8s DNS is provided IP for Juice Shop and VAmPI pods
wafciser –l http://vampi.webapps:5000	Initialize VAmPI Database

©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

WAFciser

WAFciser is a demonstration tool designed to showcase the capabilities of a Check Point Web Application Firewall (WAF). The tool's primary intent is to train the WAF using normal web traffic directed at a Juice Shop host and API traffic against a VAmPI host. Once the WAF has been trained and switched to protect mode, WAFciser is then used to generate malicious traffic targeting both the Juice Shop host and the VAmPI API host.

```
wafciser -h
WAFciser - Check Point WAF Demonstration Tool - Version 1.0.8a - by Vince Mammoliti -
Usage: /home/cp/cpwafciser.sh (-a|--app) web|api [OPTIONS...]

Options:
  -a, --app web|api    Target application type (required) (default: web)
  -g, --good           Send good/benign traffic (default)
  -m, --malicious      Send malicious traffic
  -r, --ratelimit      Run ratelimit test (web only)
  -n, --repeat N       Number of times to repeat (default: 1)
  -d, --delay N        Delay in seconds between requests (default: 1)
  -i, --initdb         Initialize API DB (api only)
  -s, --sql            Run SQL injection test (api only)
  -u, --sqlupdate      Update sqlmap database
  -v, --verbose        Show detailed output
  -h, --help           Show this help message

Examples:
  /home/cp/cpwafciser.sh --app web --good --repeat 5
  /home/cp/cpwafciser.sh --app api --malicious --repeat 3
  /home/cp/cpwafciser.sh --app api --initdb
  /home/cp/cpwafciser.sh --app web --ratelimit --repeat 100 --delay 10

Environment Variables:
  DEFAULT_URL_CPTRAFFIC  Override default WEB URL
  DEFAULT_URL_CPAPI      Override default API URL
```


©2025 Check Point Software Technologies Ltd.

Agenda

- ❑ Register and Start Virtual Lab Environment
- ❑ Lab Overview
- ❑ Objectives
- ❑ Login into Infinity Portal and Create WAF Assets in Learn Mode
- ❑ Configure Virtual WAF Lab and Start Kubernetes Containers
- ❑ Validate Lab Environment is Properly Functioning
- ❑ Generate Known Good Web and API Traffic
- ❑ Review Finding
- ❑ Switch WAF to Protect Mode and Generate Malicious Traffic
- ❑ Review Findings

©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

Check WAF is registered and updated Policy

cpnanol

- cpnanol is an alias command that sessions into the WAF agent and reports on the status

```
lab@lab:~/cp-waf-k8s$ cpnanol
Defaulted container "cloudguard-waf" out of: cloudguard-waf, controller
Last update attempt: None
Last update: None
Last update status: None
Policy version:
Last policy update: None
Last manifest update: None
Last settings update: None
Registration status: Succe
Agent ID: None
Profile ID:
Tenant ID
```

Repeat command until you see Succeeded

```
lab@lab:~/cp-waf-k8s$ cpnanol
Defaulted container "cloudguard-waf" out of: cloudguard-waf, controller
Last update attempt: 2025-12-04T19:13:03.837692
Last update: 2025-12-04T19:13:03.866290
Last update status: Succeeded
Policy version: 1
Last policy update:  19:09:07.579183
Last manifest update: 2025-1 434868
Last settings update: 2025-12-04T19:0
Registration status: Succeeded
Agent ID: None
Profile ID: None
Tenant ID: None
```

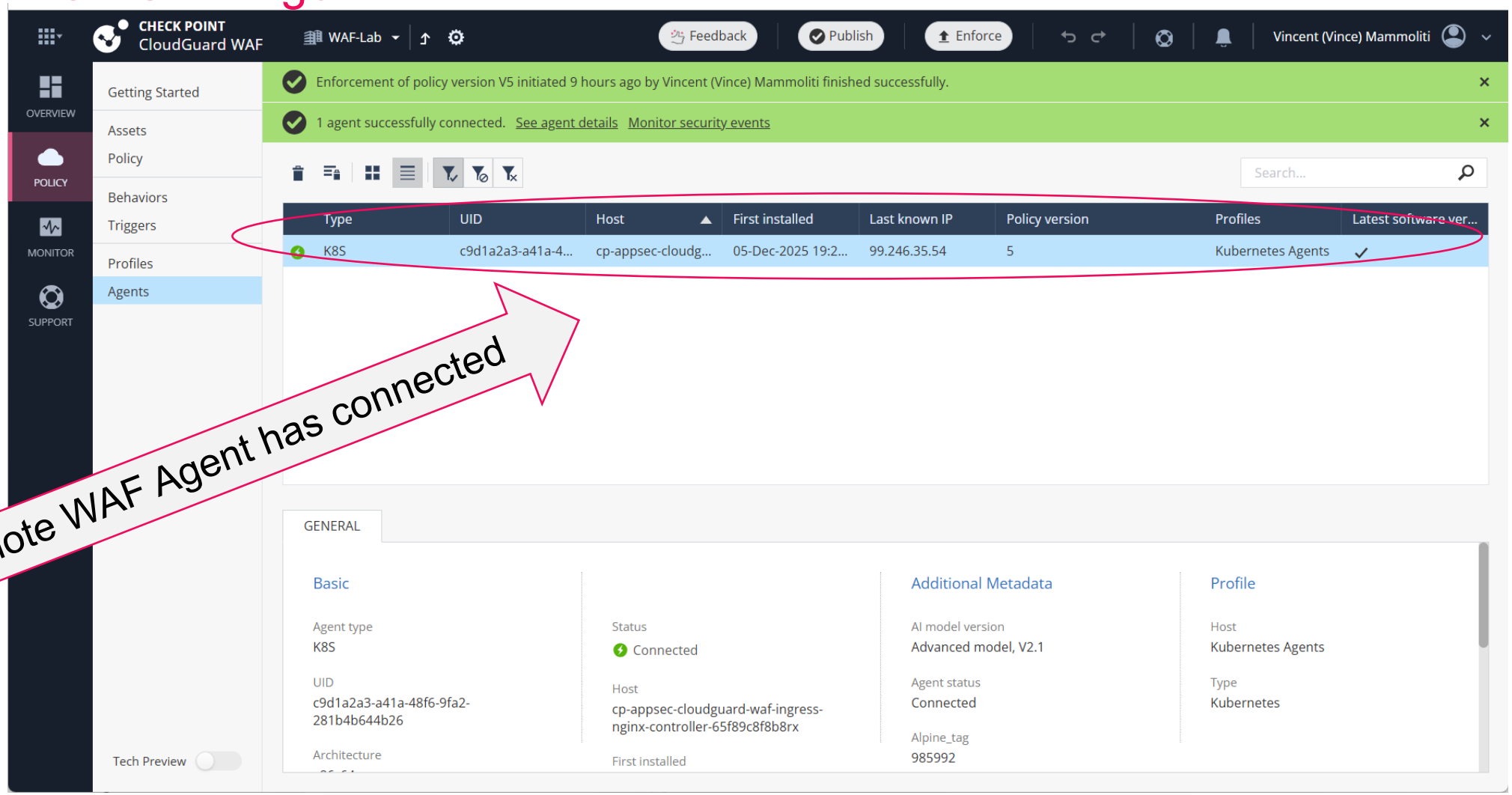
Receive a Policy Version

©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

Check WAF is registered and updated Policy via Poral

POLICY > Agent

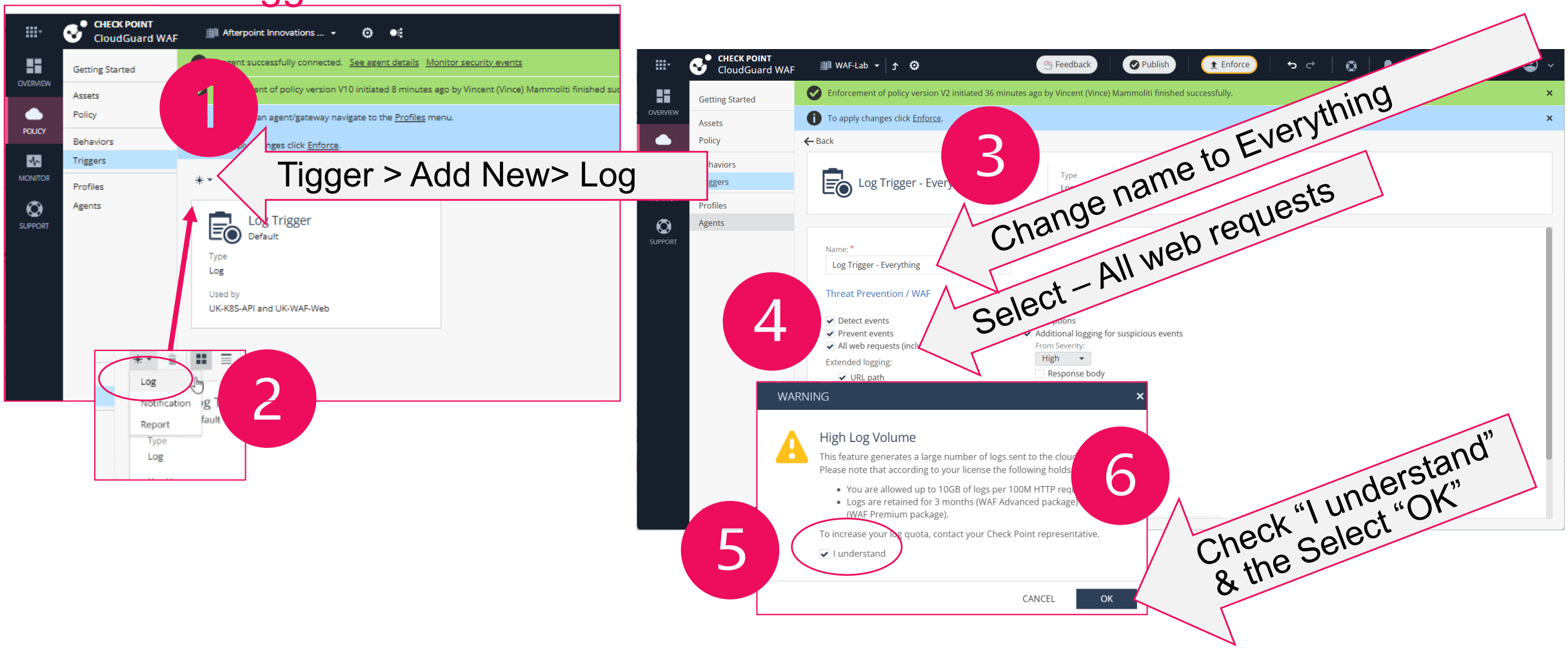


©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

Create Log Trigger 1 – Log All Web requests

POLICY > Trigger

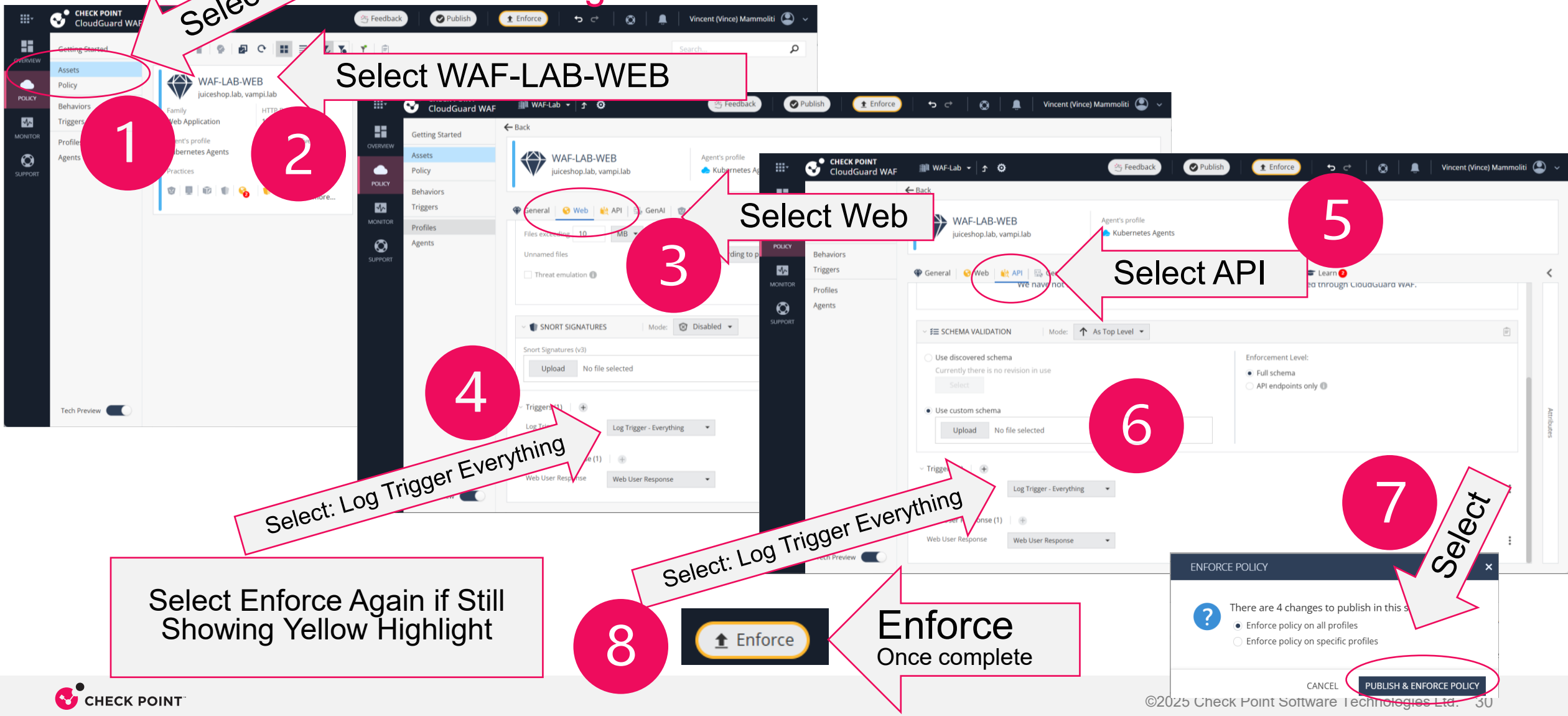


©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

Enable Enhanced Loggin

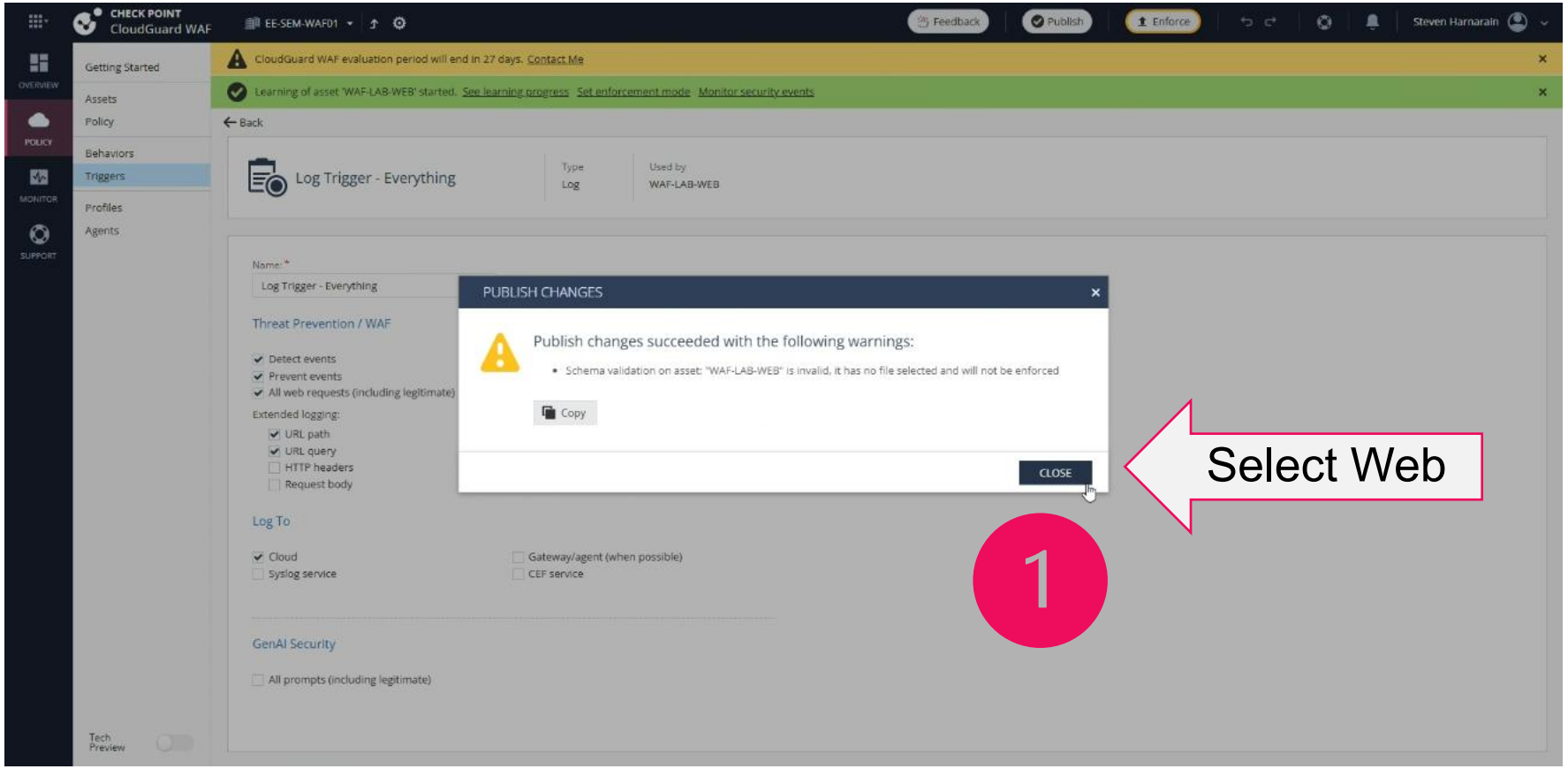
POLICY > Agent > WAF-LAB-WEB



©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

Acknowledge No Learned



©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

Check WAF is registered and updated Policy

cpnanol

```
lab@lab:~/cp-waf-k8s$ cpnanol
Defaulted container "cloudguard-waf" out of: cloudguard-waf, controller
Last update attempt: 2025-12-04T19:13:03.837692
Last update: 2025-12-04T19:13:03.866290
Last update status: Succeeded
Policy version: 1
Last policy update:  04T19:09:07.579183
Last manifest update: 2025-12-04T19:08:28.434868
Last settings update: 2025-12-04T19:07:45.274958
Registration status: Succeeded
Agent ID: None
Profile ID: None
Tenant ID: None
```

Note: Policy Version

```
lab@lab:~/cp-waf-k8s$ cpnanol
Defaulted container "cloudguard-waf" out of: cloudguard-waf, controller
Last update attempt: 2025-12-04T19:13:03.837692
Last update: 2025-12-04T19:13:03.866290
Last update status: Succeeded
Policy version: 2
Last policy update: 2025-12-04T19:09:07.579183
Last manifest update: 2025-12-04T19:08:28.434868
Last settings update: 2025-12-04T19:07:45.274958
Registration status: Succeeded
Agent ID: None
Profile ID: None
Tenant ID: None
```

Version update to match Portal

©2025 Check Point Software Technologies Ltd.

Agenda

- ❑ Register and Start Virtual Lab Environment
- ❑ Lab Overview
- ❑ Objectives
- ❑ Login into Infinity Portal and Create WAF Assets in Learn Mode
- ❑ Configure Virtual WAF Lab and Start Kubernetes Containers
- ❑ Validate Lab Environment is Properly Functioning
- ❑ Generate Known Good Web and API Traffic
- ❑ Review Finding
- ❑ Switch WAF to Protect Mode and Generate Malicious Traffic
- ❑ Review Findings

©2025 Check Point Software Technologies Ltd.

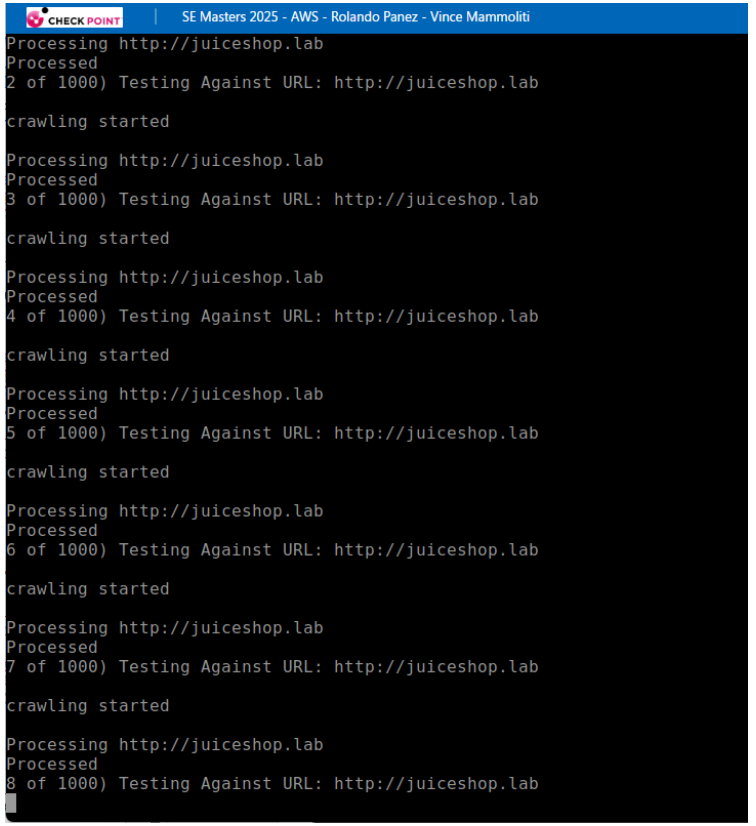
CloudGuard WAF

Use WAFciser to generate WEB Training Traffic

wafciser -n 1000

Generate Web Training Traffic

- This will web-crawl the default http://juiceshop.lab site 1000 times. We are using this to train the behavior of the WAF



©2025 Check Point Software Technologies Ltd.

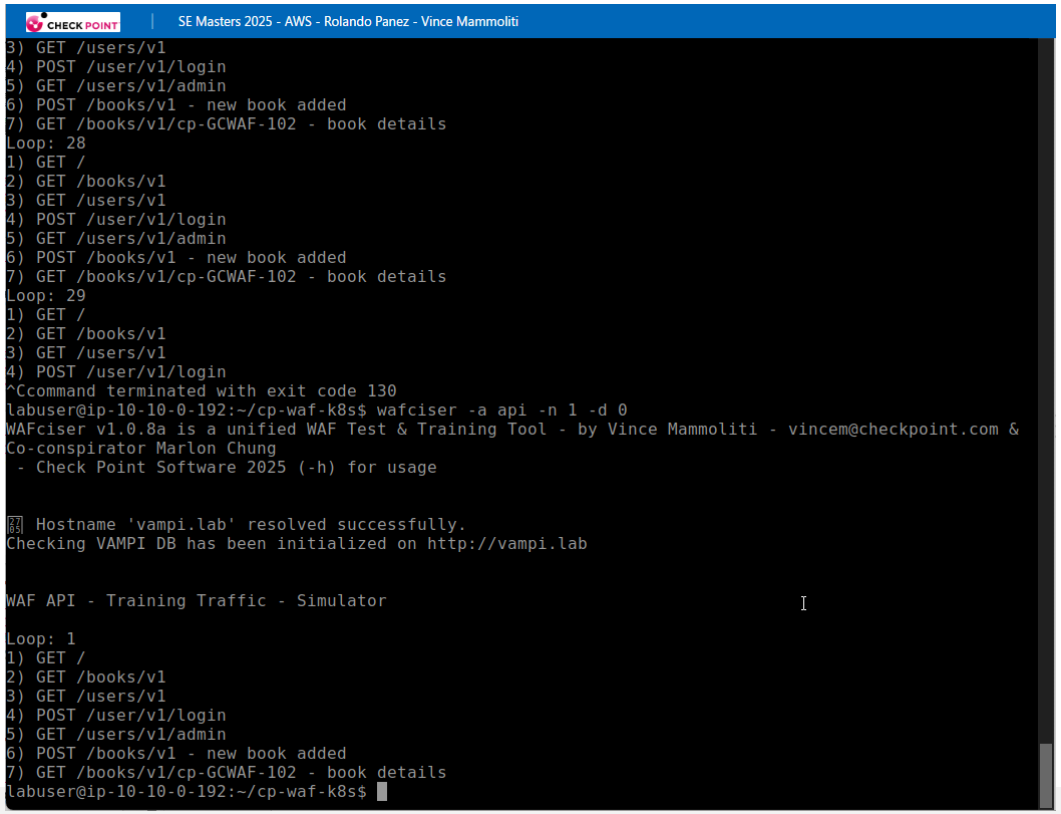
CloudGuard WAF

Use WAFciser to generate API Training Traffic

wafciser -i http://vampi.webapps:5000 ← Initialize VAmPI database

wafciser -a api -n 1000 -d 0 ← Generate API Training Traffic

- This will call the VAmPI API with default of http://vampi.lab site 1000 times
- From this we will auto discover the API and normal behavioral training



©2025 Check Point Software Technologies Ltd.

Agenda

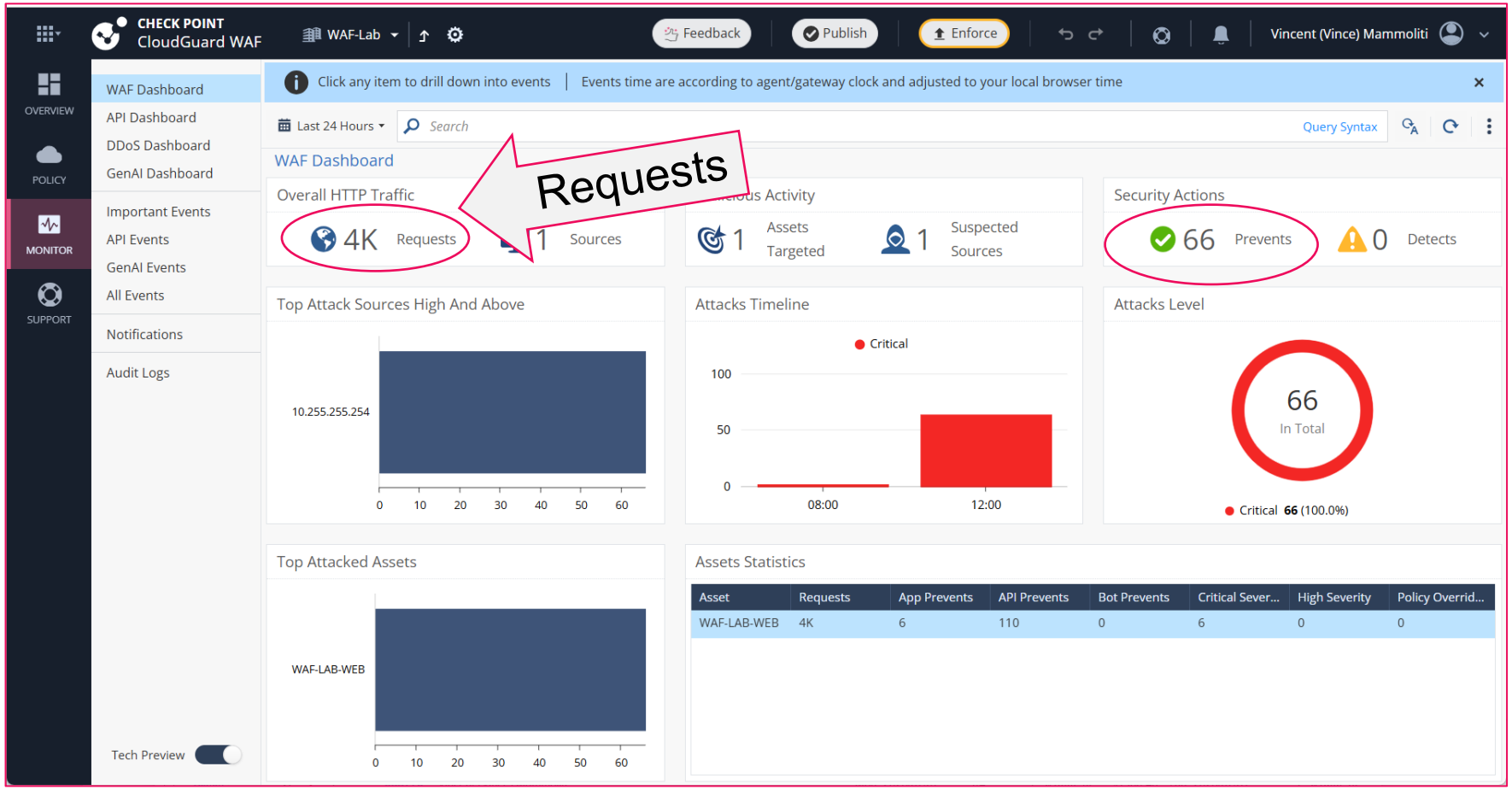
- ❑ Register and Start Virtual Lab Environment
- ❑ Lab Overview
- ❑ Objectives
- ❑ Login into Infinity Portal and Create WAF Assets in Learn Mode
- ❑ Configure Virtual WAF Lab and Start Kubernetes Containers
- ❑ Validate Lab Environment is Properly Functioning
- ❑ Generate Known Good Web and API Traffic
- ❑ **Review Finding**
- ❑ **Switch WAF to Protect Mode and Generate Malicious Traffic**
- ❑ **Review Findings**

©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

MONITOR > WAF Dashboard

MONITOR > WAF Dashboard

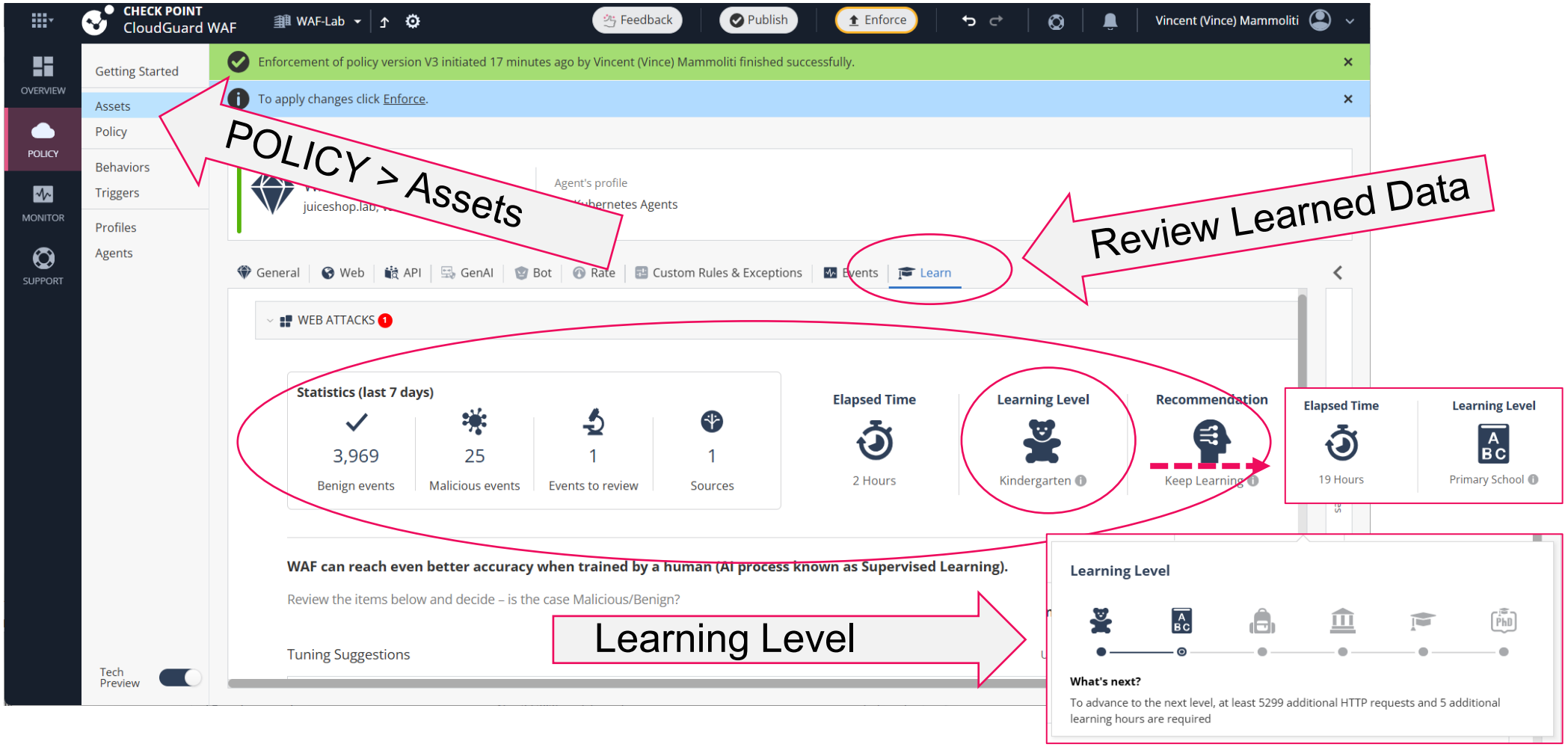


©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

Review WAF Dashboard

POLICY> Assets > WAF-LAB-WEB > Learn

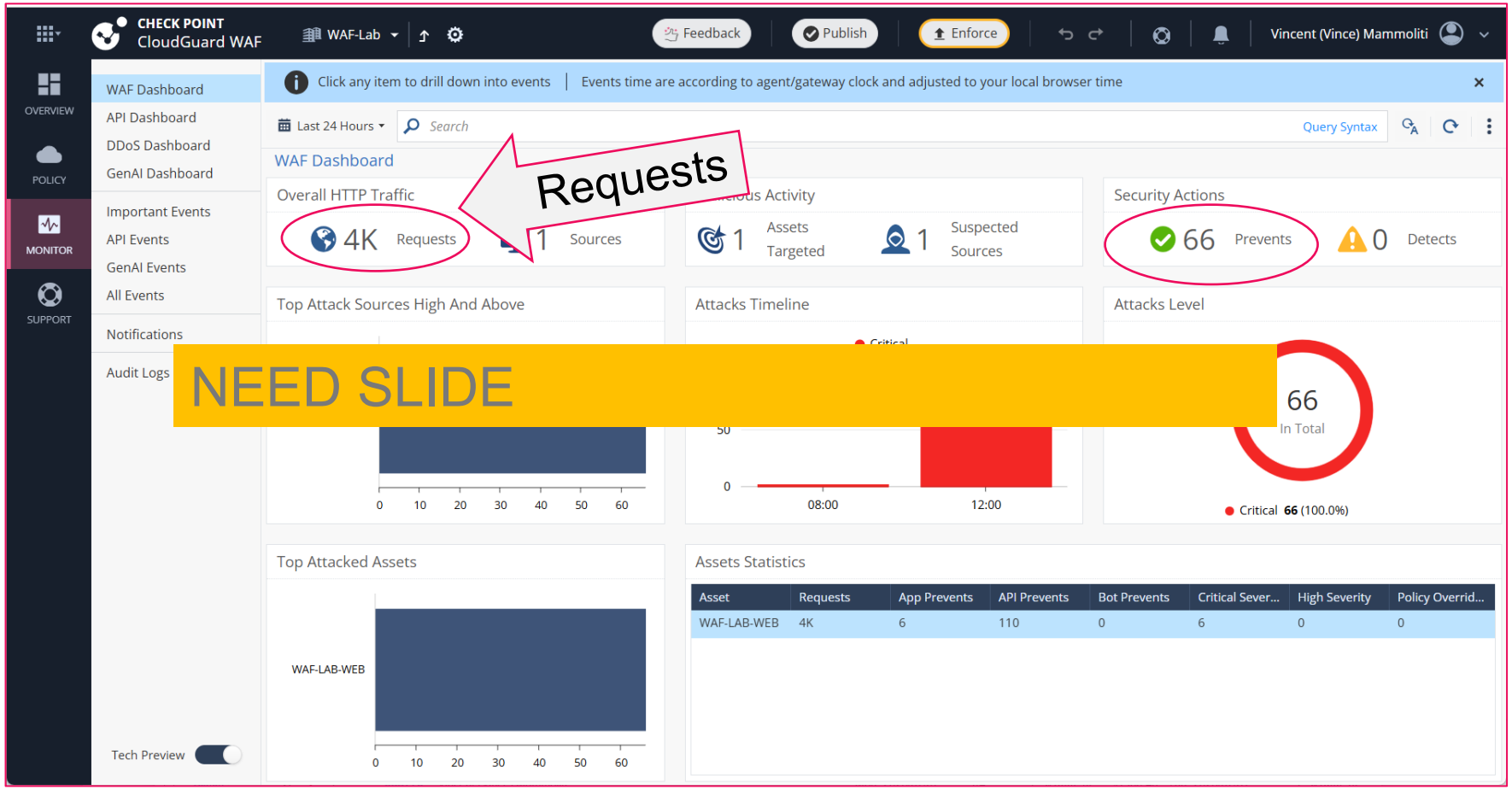


©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

MONITOR > API Dashboard

MONITOR > API Dashboard

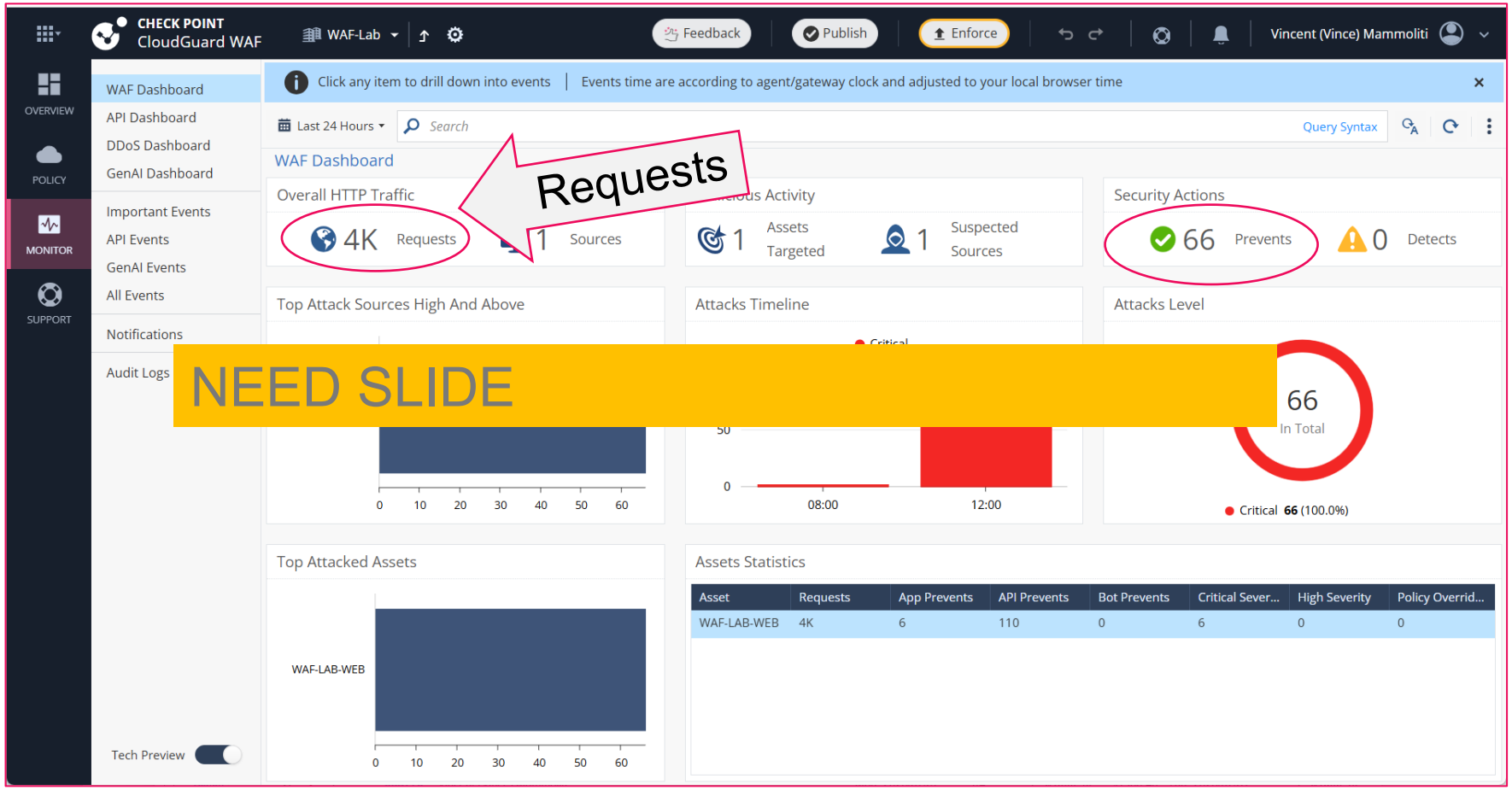


©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

MONITOR > API Events

MONITOR > API Events



©2025 Check Point Software Technologies Ltd.

Agenda

- ❑ Register and Start Virtual Lab Environment
- ❑ Lab Overview
- ❑ Objectives
- ❑ Login into Infinity Portal and Create WAF Assets in Learn Mode
- ❑ Configure Virtual WAF Lab and Start Kubernetes Containers
- ❑ Validate Lab Environment is Properly Functioning
- ❑ Generate Known Good Web and API Traffic
- ❑ Review Finding
- ❑ **Switch WAF to Protect Mode and Generate Malicious Traffic**
- ❑ **Review Findings**

©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

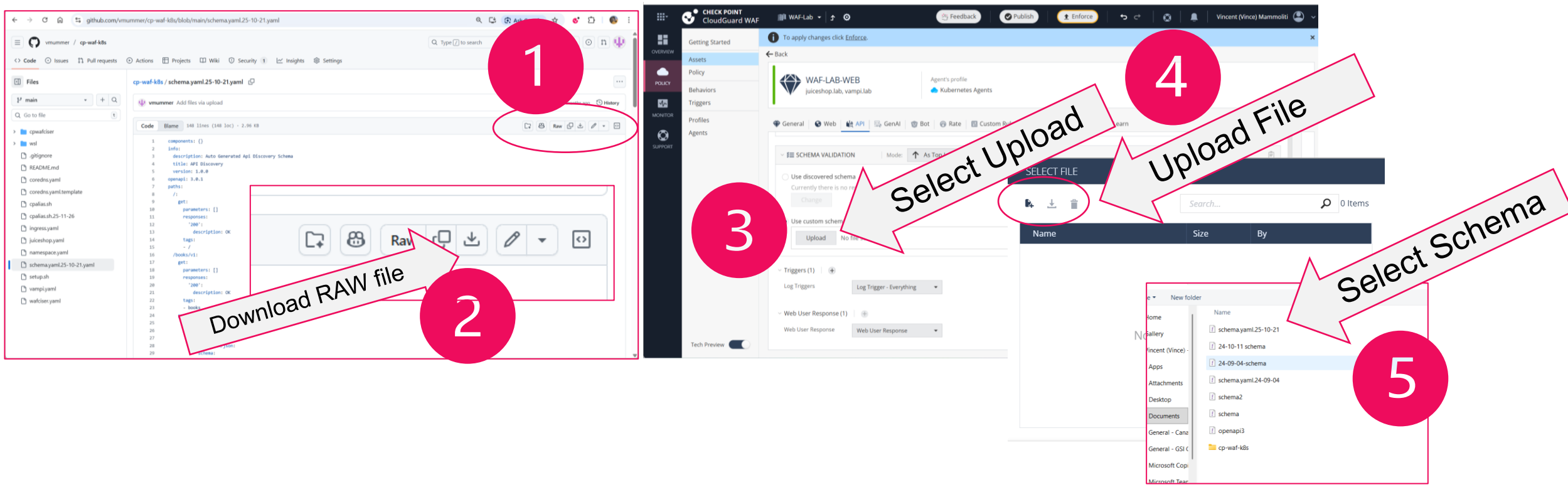
Enable Prevent

©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

Upload Defined Schema

https://github.com/vmummer/cp-waf-k8s/blob/main/schema.yaml.25-10-21.yaml

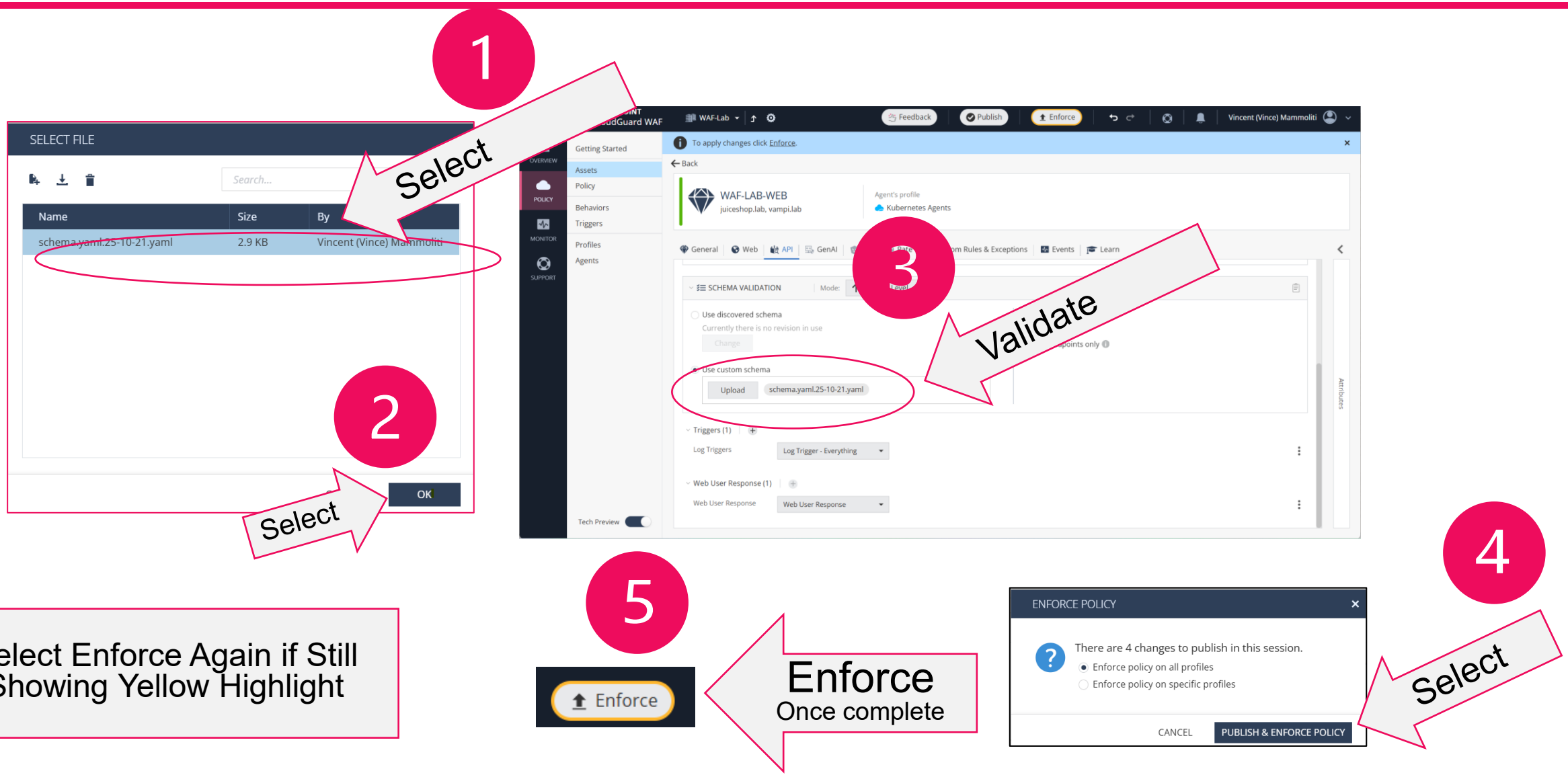


POLICY> Assets > WAF-LAB-WEB > API > SCHEMA >Upload

©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

Apply Schema and Enforce Protect



Select Enforce Again if Still Showing Yellow Highlight

©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

Check WAF is registered and updated Policy

cpnanol

```
lab@lab:~/cp-waf-k8s$ cpnanol
Defaulted container "cloudguard-waf" out of: cloudguard-waf, controller
Last update attempt: 2025-12-04T19:13:03.837692
Last update: 2025-12-04T19:13:03.866290
Last update status: Succeeded
Policy version: 2
Last policy update:  04T19:09:07.579183
Last manifest update: 2025-12-04T19:08:28.434868
Last settings update: 2025-12-04T19:07:45.274958
Registration status: Succeeded
Agent ID: None
Profile ID: None
Tenant ID: None
```

Note: Policy Version

```
lab@lab:~/cp-waf-k8s$ cpnanol
Defaulted container "cloudguard-waf" out of: cloudguard-waf, controller
Last update attempt: 2025-12-04T19:13:03.837692
Last update: 2025-12-04T19:13:03.866290
Last update status: Succeeded
Policy version: 3
Last policy update: 2025-12-04T19:09:07.579183
Last manifest update: 2025-12-04T19:08:28.434868
Last settings update: 2025-12-04T19:07:45.274958
Registration status: Succeeded
Agent ID: None
Profile ID: None
Tenant ID: None
```

Version update to match Portal

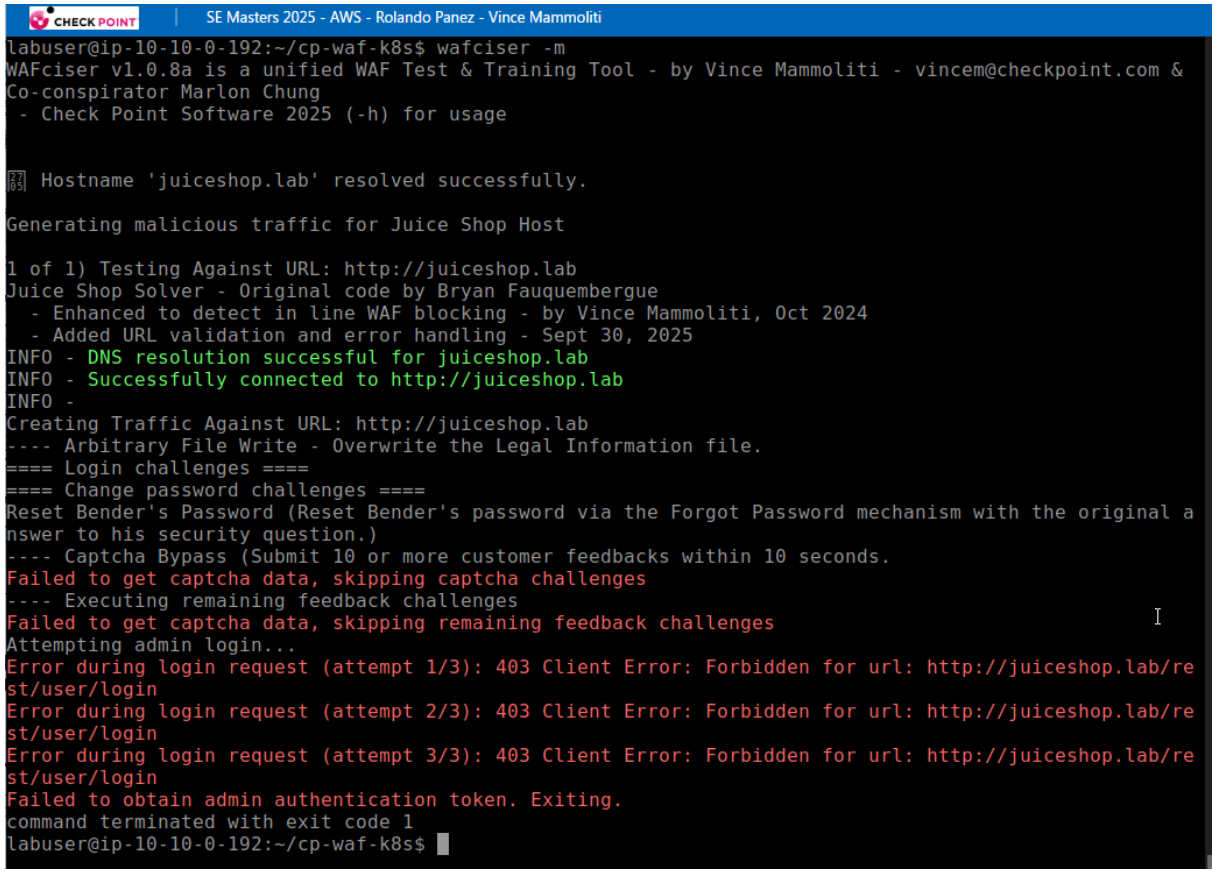
©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

Use WAFciser to generate Malicious WEB Traffic

wafciser -m

Generate Malicious Traffic



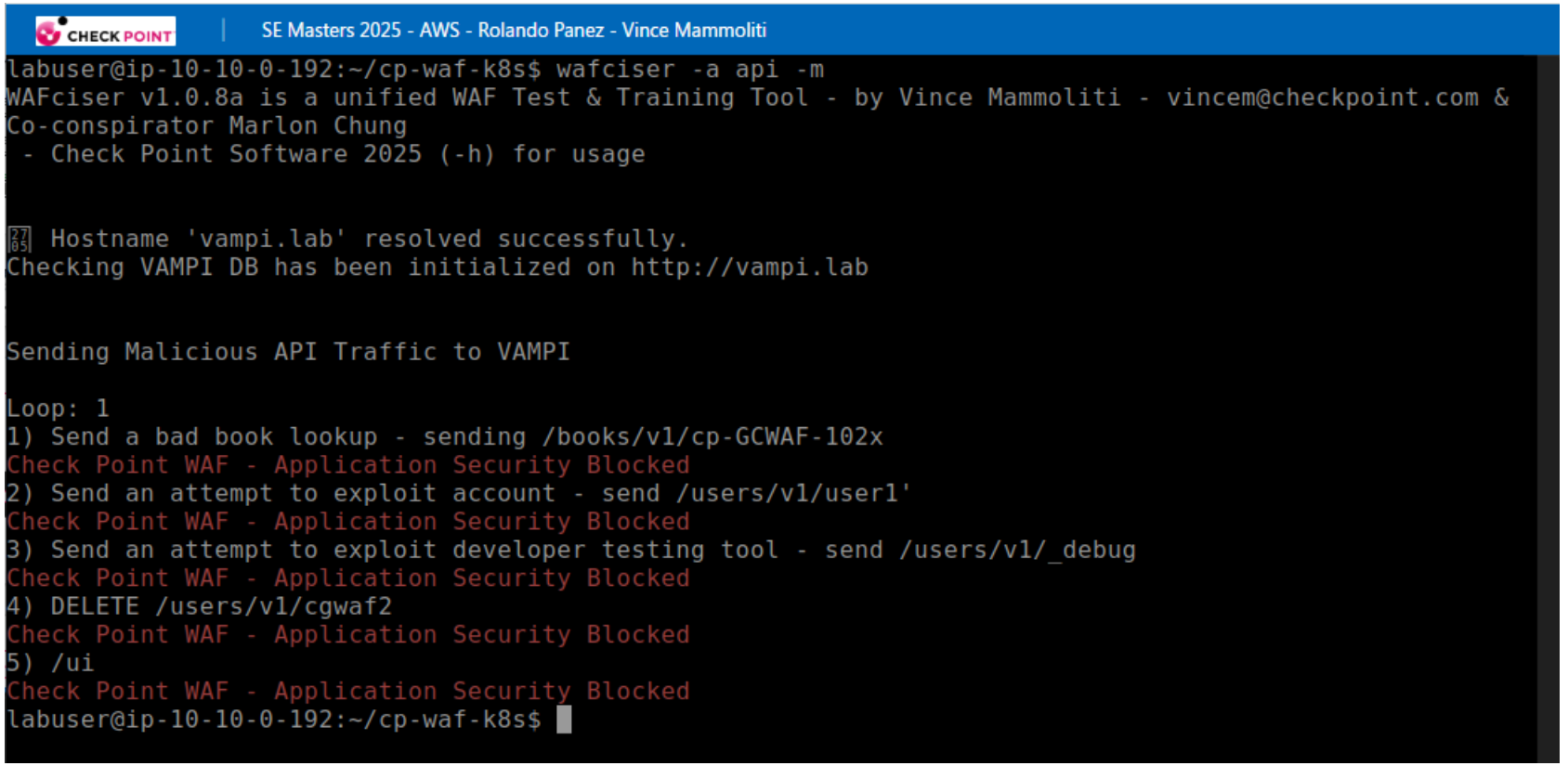
©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

Use WAFciser to generate Malicious API Traffic

wafciser -a api -m

Generate Malicious Traffic



©2025 Check Point Software Technologies Ltd.

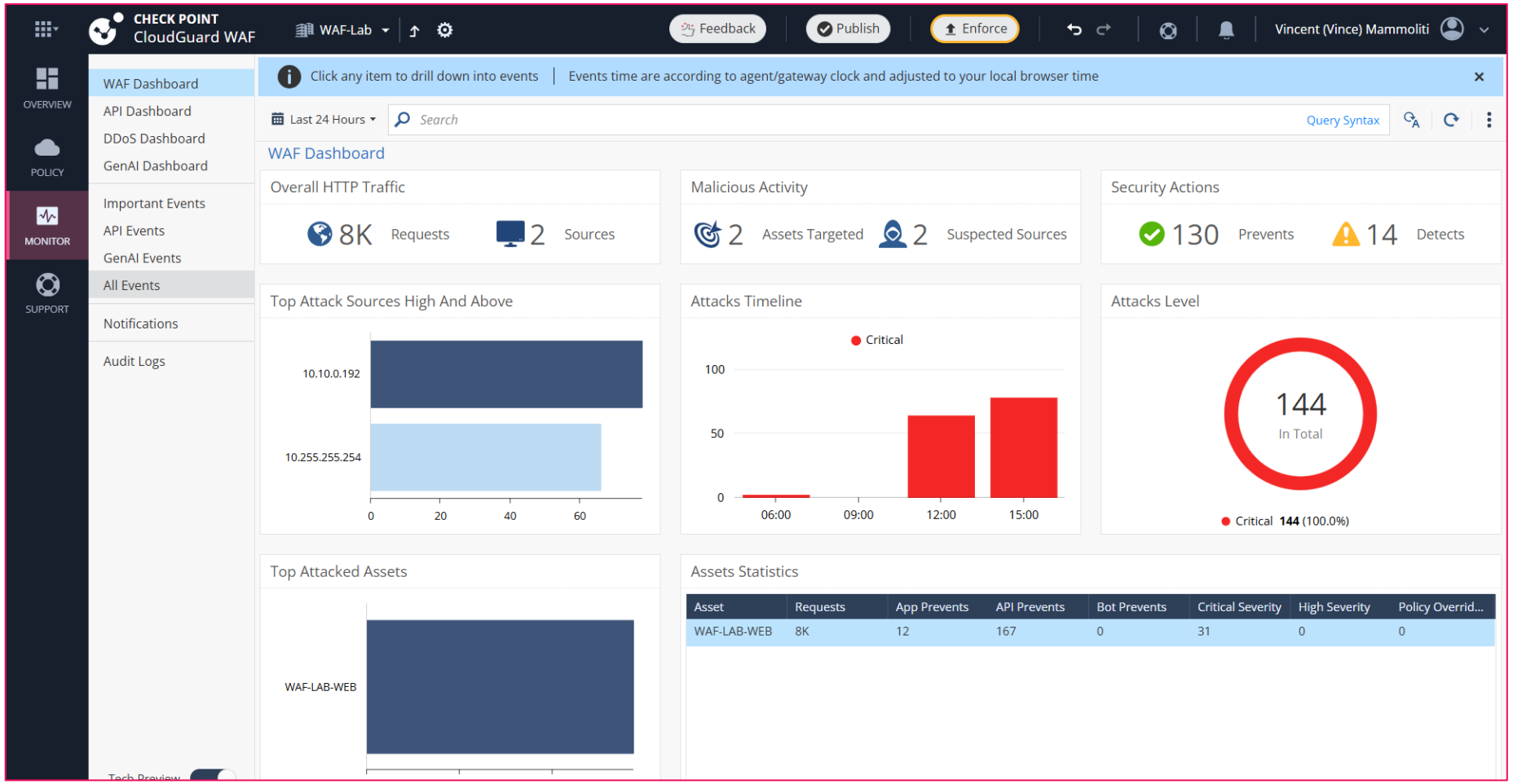
Agenda

- ❑ Register and Start Virtual Lab Environment
- ❑ Lab Overview
- ❑ Objectives
- ❑ Login into Infinity Portal and Create WAF Assets in Learn Mode
- ❑ Configure Virtual WAF Lab and Start Kubernetes Containers
- ❑ Validate Lab Environment is Properly Functioning
- ❑ Generate Known Good Web and API Traffic
- ❑ Review Finding
- ❑ Switch WAF to Protect Mode and Generate Malicious Traffic
- ❑ **Review Findings**

©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

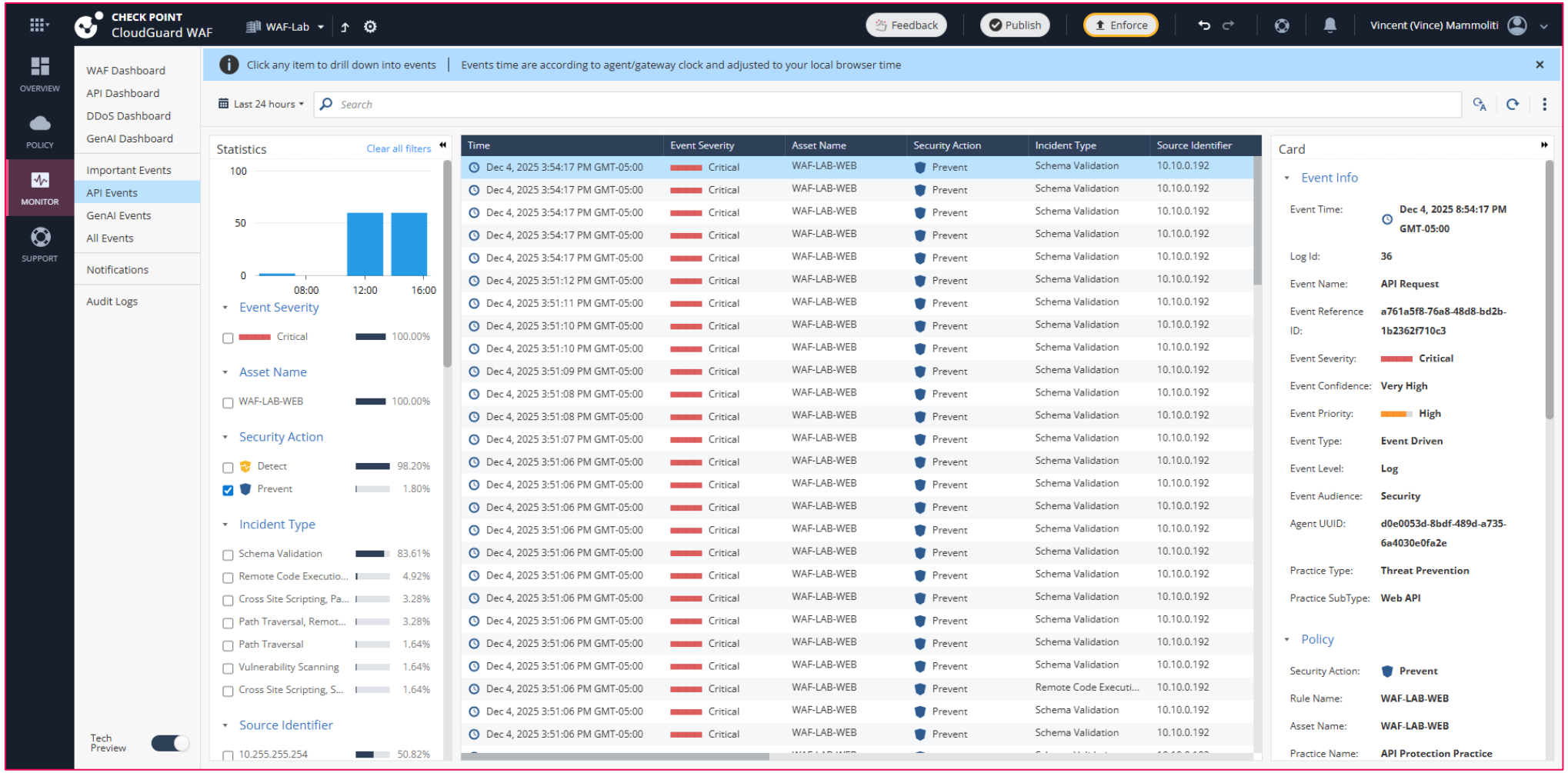
WAF Dashboard



©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

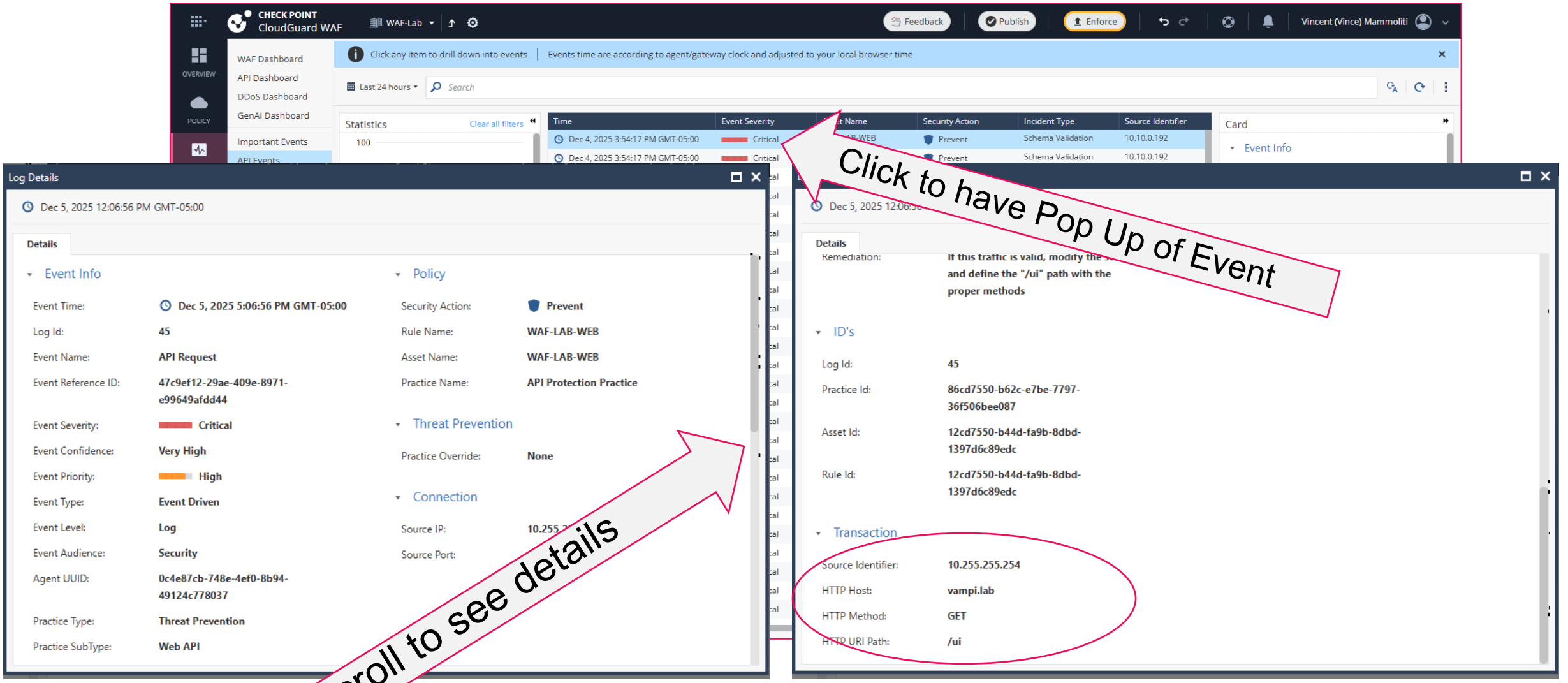
Monitor > API Events



©2025 Check Point Software Technologies Ltd.

CloudGuard WAF

Monitor > API Events



©2025 Check Point Software Technologies Ltd.

CHECK POINT™

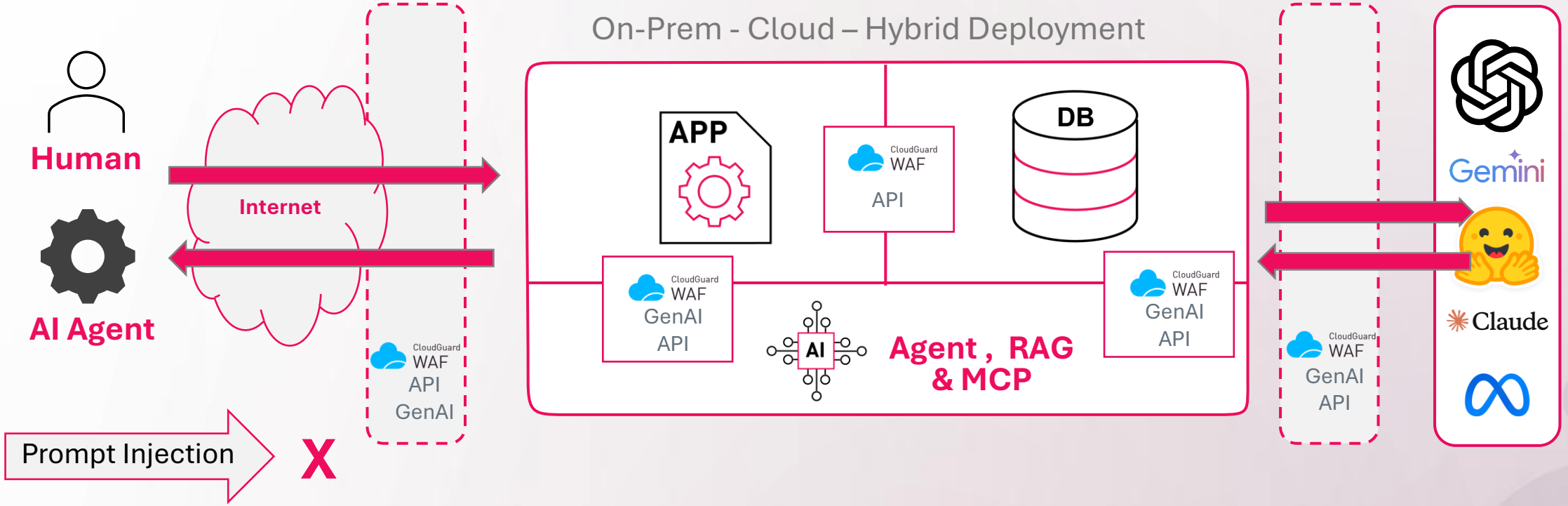
Thank You!

YOU DESERVE THE BEST SECURITY

How To Secure Your Digital Transformation

WAF GenAI Protection available in several ways:

- In-line protection between Human Users or Agent and the Application
- In-line protection between the Application and the SLM/LLM
- In-code protection of Applications/Agents as an API for Developers



©2025 Check Point Software Technologies Ltd.