



<http://unicorn-project.eu>



@unicorn\_H2020



European  
Commission

Horizon 2020  
European Union funding  
for Research & Innovation



# UNICORN

## UNICORN Project Overview

Manos Papoutsakis

FORTH

*UNICORN: A Novel Framework for Multi-cloud Services Development, Orchestration, Deployment and Continuous Management Fostering Cloud Technologies Uptake from Digital SMEs and Startups*



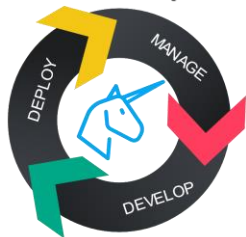
# Unicorn Objectives

- **to facilitate the design and deployment of cloud applications and services** by developing a security and elasticity by design framework.
- **to improve developers' productivity** by reducing cloud application design time via code annotations and blueprints for security.
- **to prove the applicability and value of the UNICORN results**, demonstrating against a pre-defined set of use cases.

# What is Unicorn?

- A framework that allows the **design** and **deployment** of **secure** and **elastic by design** cloud applications and services.

## Unified DevOps Tool



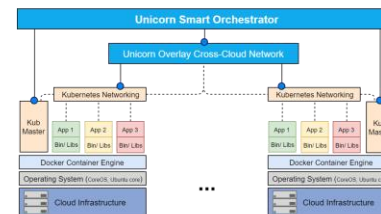
Offer a single tool for application **development**, **deployment**, and **management** during the whole application lifecycle

## Monitoring & Resource Adaptation



Unicorn **elasticity library** supports apps to elastically **(de-)allocate resources** and provides **real-time monitoring and analytics**

## True Multi-Cloud Deployments



Unicorn supports **transparent** and **automated multi-cloud deployments** for services to span across cloud zones and geographical regions

## Privacy & Security Adoption



Unicorn **security** and **privacy design libraries** prevent **data breaches** and **ensure** customer **privacy**

# What is Unicorn?

## Unified DevOps Tool



Offer a single tool for application **development, deployment, and management** during the whole application lifecycle

# What is Unicorn?

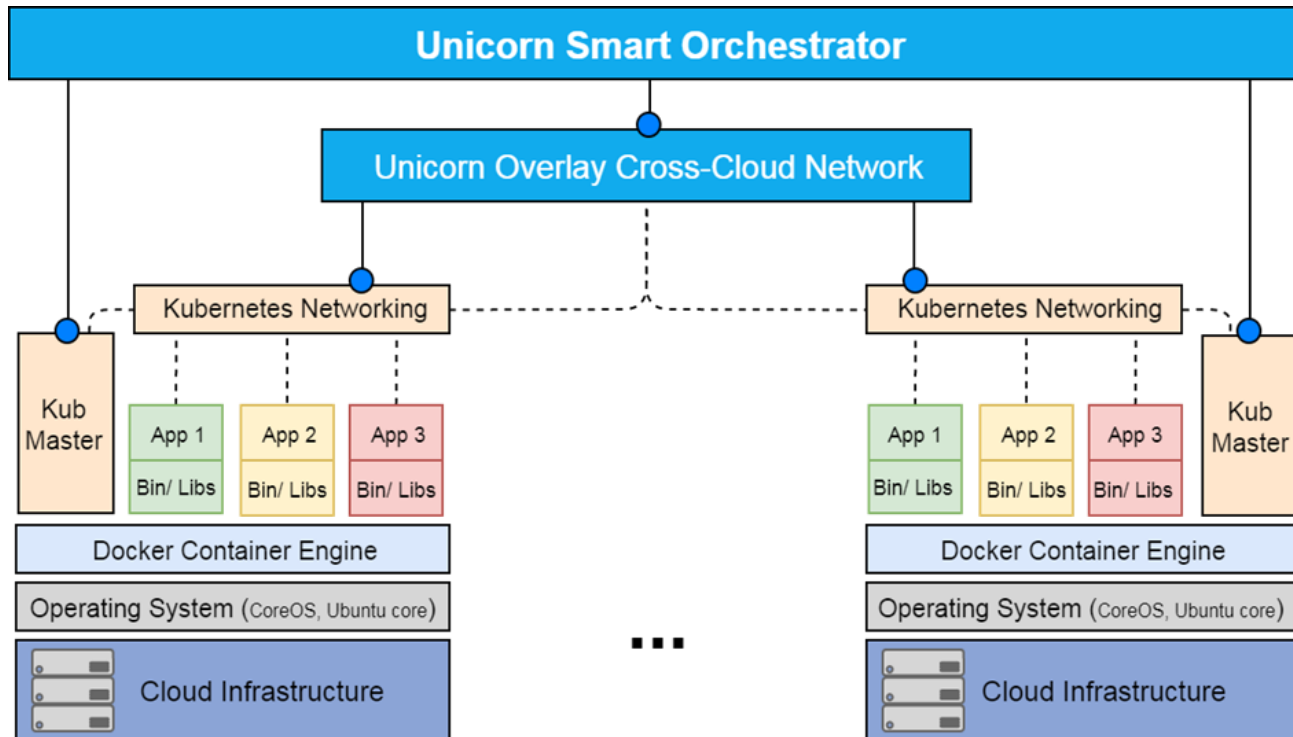
## Monitoring & Resource Adaptation



Unicorn **elasticity library** supports  
apps to elastically **(de-)allocate**  
**resources** and provides **real-time**  
**monitoring** and **analytics**

# What is Unicorn?

## True Multi-Cloud Deployment



# What is Unicorn?

## Privacy & Security Adoption



Unicorn **security** and **privacy**  
**design libraries** prevent **data**  
**breaches** and **ensure** customer  
**privacy**

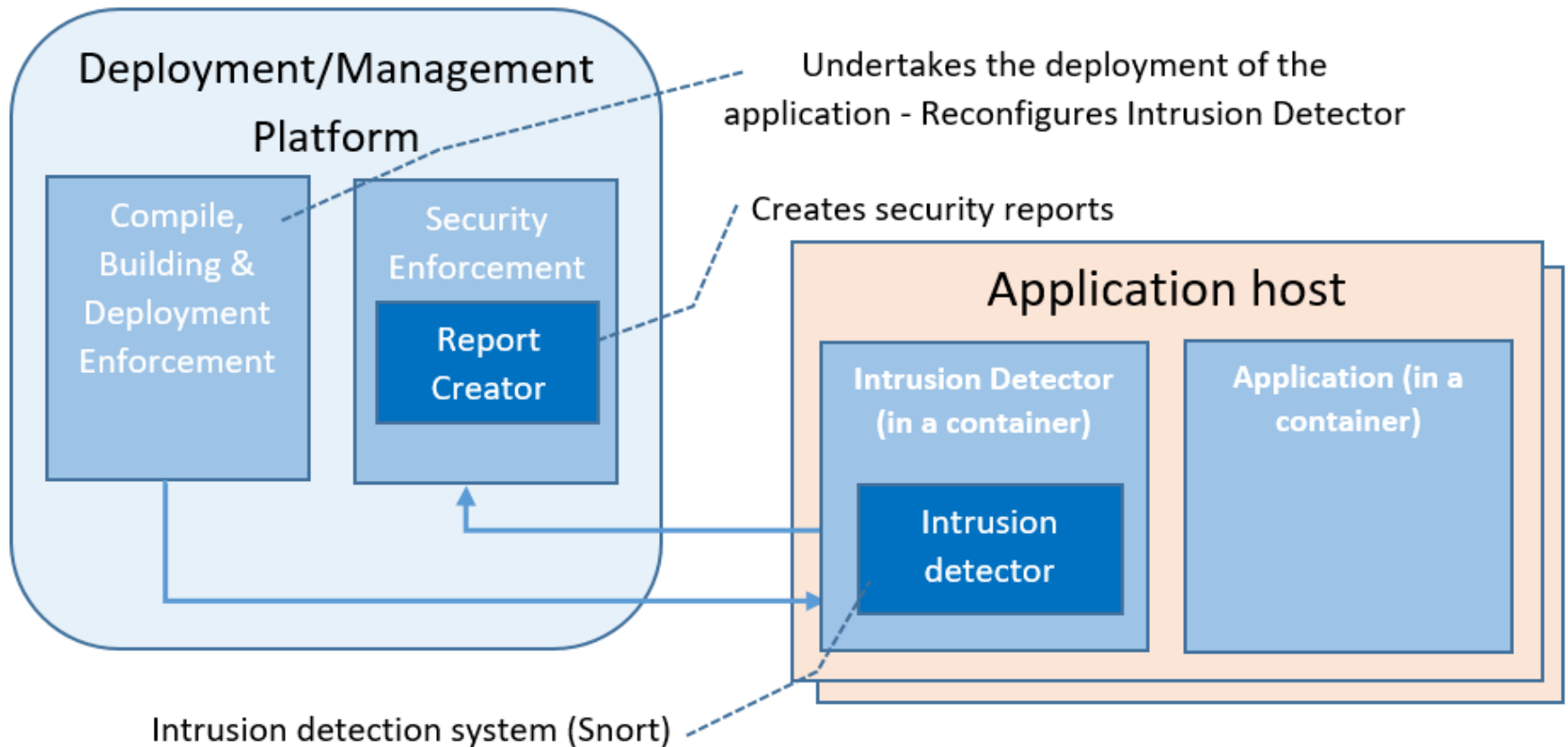
# Project Status

- Platform is available as closed **beta**
- Development of all functionalities has concluded
  - Currently integrating updates and fixed on functionalities
- Validating Unicorn
  - through 4 Real Life Demonstrators
  - through a contest where 12 companies are using Unicorn





# Unicorn Security Service



# Unicorn Security Service



- DASHBOARD
- INSTANCES
- APPLICATIONS
- COMPONENTS
- SSH KEYS
- RESOURCES
- DETECTION RULES**
- PLUGINS
- CONFIGURATION >

Intrusion Detection Rulesets > Edit

Intrusion Detection Rulesets | Edit

Intrusion Detection Rulesets Management

Name \*

testVM\_ruleset

Alerting Rules

Rule

alert tcp 10.142.0.4 any -> \$HOME\_NET any (msg:"packet from 10.142.0.4"; GID:1; sid:10000007; rev:001;)



Rule

alert tcp 34.73.160.110 any -> \$HOME\_NET any (msg:"packet from 34.73.160.110"; GID:1; sid:10000006; rev:001;)

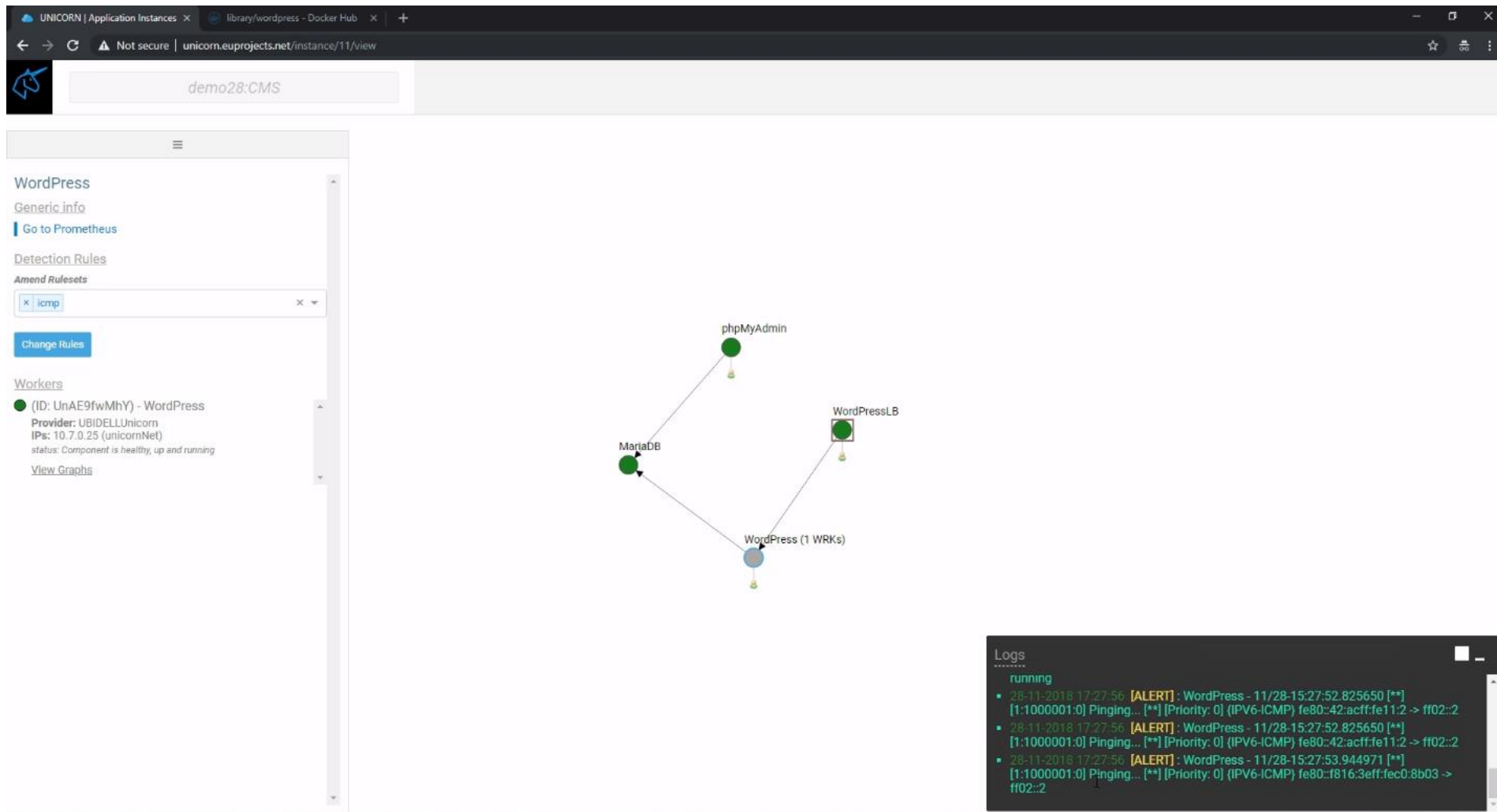


# Unicorn Security Service

The screenshot displays the Unicorn Security Service interface. On the left, a sidebar shows a navigation menu with a 'demo28' input field and a 'Select Provider' dropdown set to 'UBIDELLUicorn'. Below this is a 'Proceed' button. The main area features a diagram of a security architecture with nodes: 'phpMyAdmin', 'MariaDB', and 'WordPress'. 'phpMyAdmin' is connected to 'MariaDB' via a 'sqlinterface' component, and 'MariaDB' is connected to 'WordPress' via another 'sqlinterface' component. A red box highlights the 'Configure "WordPress" Component' panel on the right. This panel includes the following fields and options:

- Configure "WordPress" Component** (ID: UnAE9fwMhY)
- Select SSH Key:** myLaptop
- Select Provider:** UBIDELLUicorn
- Select Region \*:** eu-east
- Prevention Rules:** ☒ Activate IPS
- Detection Rules:** ☒ Activate IDS
- Select Rulesets:** icmp, mysql
- Workers:** Minimum Workers: 1, Maximum Workers: 1
- Flavor:** vCPUs \*: 1, RAM \*: 2048, Storage \*: 20

# Unicorn Security Service



The screenshot displays the Unicorn Security Service web interface. The browser address bar shows the URL `unicorn.euprjects.net/instance/11/view`. The page title is `demo28:CMS`.

**WordPress Configuration Panel:**

- WordPress**
  - [Generic info](#)
  - [Go to Prometheus](#)
- Detection Rules**
  - [Amend Rulesets](#)
  - Input field: `icmp`
  - [Change Rules](#)
- Workers**
  - (ID: UnAE9fwMhY) - WordPress
  - Provider: UBIDELLUnicorn
  - IPs: 10.7.0.25 (unicornNet)
  - Status: Component is healthy, up and running
  - [View Graphs](#)

**Network Diagram:**

```

graph TD
    MariaDB((MariaDB)) --> WP1[WordPress (1 WRKs)]
    phpMyAdmin((phpMyAdmin)) --> WP1
    WP1 --> WP2[WordPressLB]
  
```

**Logs:**

```

running
28-11-2018 17:27:56 [ALERT] : WordPress - 11/28-15:27:52.825650 [**]
[1:1000001:0] Ping... [**] [Priority: 0] (IPV6-ICMP) fe80::42:acff:fe11:2 -> ff02::2
28-11-2018 17:27:56 [ALERT] : WordPress - 11/28-15:27:52.825650 [**]
[1:1000001:0] Ping... [**] [Priority: 0] (IPV6-ICMP) fe80::42:acff:fe11:2 -> ff02::2
28-11-2018 17:27:56 [ALERT] : WordPress - 11/28-15:27:53.944971 [**]
[1:1000001:0] Ping... [**] [Priority: 0] (IPV6-ICMP) fe80::f816:3eff:fec0:8b03 -> ff02::2
  
```

# Security Annotations

@Override

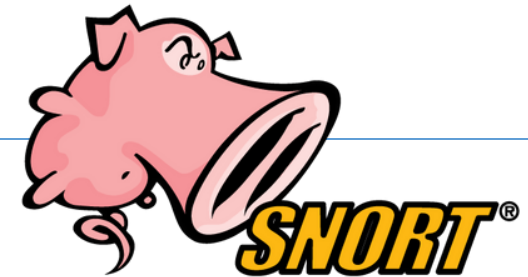
@Deprecated

```
@UnicornIDSRule(snortRule="alert icmp any any ->  
$HOME_NET any (msg:\"ICMP test detected\";  
GID:1; sid:10000001; rev:001;)")
```

# Security Annotations

- `@UnicornIDSRule("SnortRule")`
- `@UnicornIDSRuleset("SnortRulesetPath")`
- `@UnicornIDSPredefinedRuleset("SnortRulesetName")`

# IDS Rulesets



## Level 2 (7 categories)

community.rules

registered.rules

network-protocol.rules

policy.rules

attacks-detection.rules

exploit-vulnerabilities-files.rules

unwanted-application.rules

## Level 1 (52 categories)

exploit-kit.rules

malware-other.rules

malware-backdoor.rules

malware-tools.rules

malware-cnc.rules

indicator-scan.rules

netbios.rules

indicator-compromise.rules

indicator-obfuscation.rules

file-pdf.rules

policy-other.rules

sql.rules

app-detect.rules

pua-adware.rules

pua-p2p.rules

pua-other.rules

pua-toolbars.rules

# Performance testing

- Dataset from the Canadian Institute for Cybersecurity comprising labelled network flows, including full packet payloads in pcap format
  - 5 days of traffic
  - 25 users
  - HTTP, HTTPS, FTP, SSH and email
  - Brute Force FTP, Brute Force SSH, DoS, Heartbleed, Web Attack, Infiltration, Botnet and DDoS
- Google cloud platform
  - VM instance of type n1- standard-1
  - Snort in NIDS mode
  - Test application (a web server that renders a webpage that uses a cgi script)
- Snort configured in two ways:
  - Application-specific manner
  - Default configuration (baseline)



# Performance testing

All Snort rule categories		Test application rule categories
app-detect.rules browser-chrome.rules browser-firefox.rules browser-ie.rules browser-other.rules browser-plugins.rules browser-webkit.rules exploit-kit.rules exploit.rules file-executable.rules file-flash.rules file-identify.rules file-image.rules file-multimedia.rules file-office.rules file-other.rules file-pdf.rules indicator-compromise.rules indicator-obfuscation.rules indicator-shellcode.rules malware-backdoor.rules malware-cnc.rules malware-other.rules malware-tools.rules netbios.rules os-linux.rules os-other.rules os-solaris.rules os-windows.rules	policy-multimedia.rules policy-other.rules policy.rules policy-social.rules policy-spam.rules protocol-finger.rules protocol-ftp.rules protocol-icmp.rules protocol-imap.rules protocol-pop.rules protocol-services.rules protocol-voip.rules pua-adware.rules pua-other.rules pua-p2p.rules pua-toolbars.rules server-apache.rules server-iis.rules server-mail.rules server-mssql.rules server-mysql.rules server-oracle.rules server-other.rules server-webapp.rules sql.rules	app-detect.rules exploit-kit.rules file-identify.rules indicator-compromise.rules indicator-obfuscation.rules malware-backdoor.rules malware-cnc.rules malware-other.rules malware-tools.rules os-linux.rules pua-adware.rules pua-other.rules server-apache.rules server-webapp.rules

# Performance testing

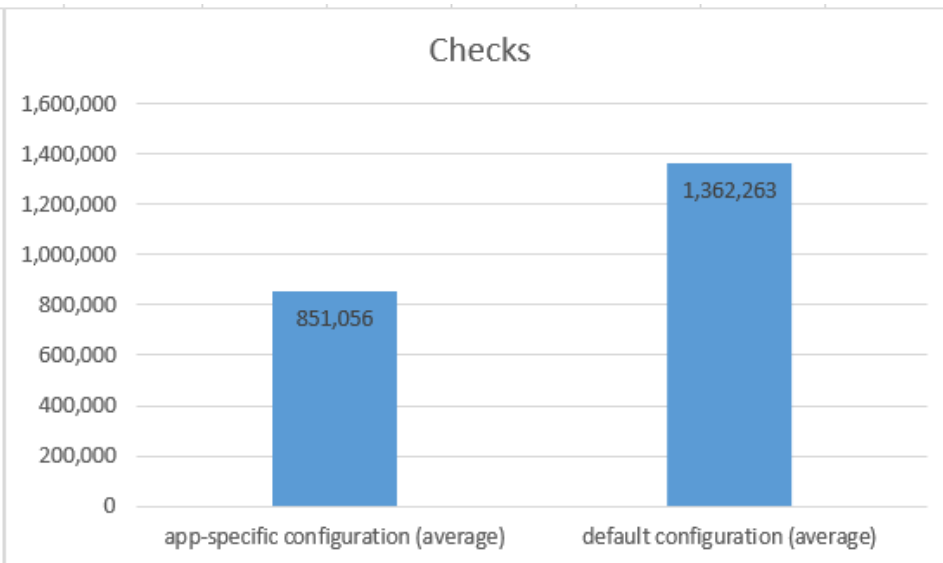
	Evaluated rules	Checks	Matches	Alerts	Microseconds
all_rules_Friday_1	956	1,874,184	65,031	3,788	2,730,707
all_rules_Friday_2	979	1,834,616	62,825	3,149	3,261,365
all_rules_Friday_3	983	1,845,098	64,280	4,040	2,739,264
all_rules_Friday_4	944	1,831,214	63,361	3,616	2,956,235
all_rules_Friday_5	955	1,762,221	61,420	3,340	2,567,531
average	963	1,829,467	63,383	3,587	2,851,020
	Evaluated rules	Checks	Matches	Alerts	Microseconds
myapp_rules_Friday_1	275	1,053,747	1,417	1,379	1,074,952
myapp_rules_Friday_2	275	1,002,469	1,402	1,373	1,038,686
myapp_rules_Friday_3	273	1,033,385	1,338	1,306	1,280,751
myapp_rules_Friday_4	273	1,017,684	1,411	1,388	1,152,017
myapp_rules_Friday_5	279	1,018,362	1,521	1,486	1,067,938
average	275	1,025,129	1,418	1,386	1,122,869

# Performance testing

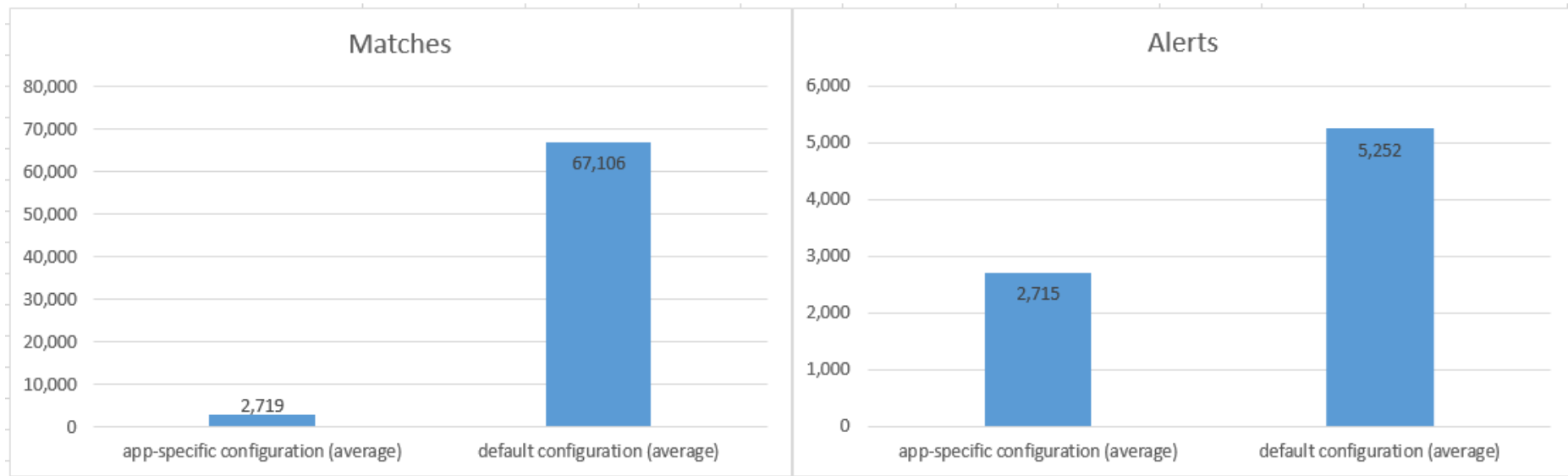
Evaluated rules



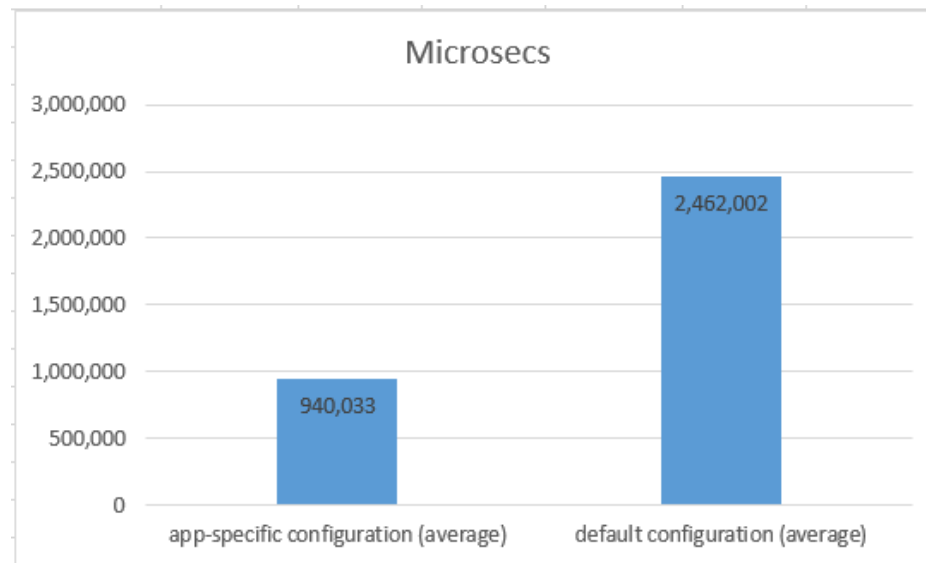
Checks



# Performance testing



# Performance testing



# Thank you!



## UNICORN



<http://unicorn-project.eu>



@unicorn\_H2020