RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: CSV-R04

Security recipes for the new digital era v.1.0.1

Tomás Herranz

Head of Engineering & SecDevOps – Security Architecture
BBVA
@tomasherranz

Introduction

Current situation

€ 746	65	35	9,250	29,330	137,904
billion in total assets	million customers	countries	branches	ATMs	employees

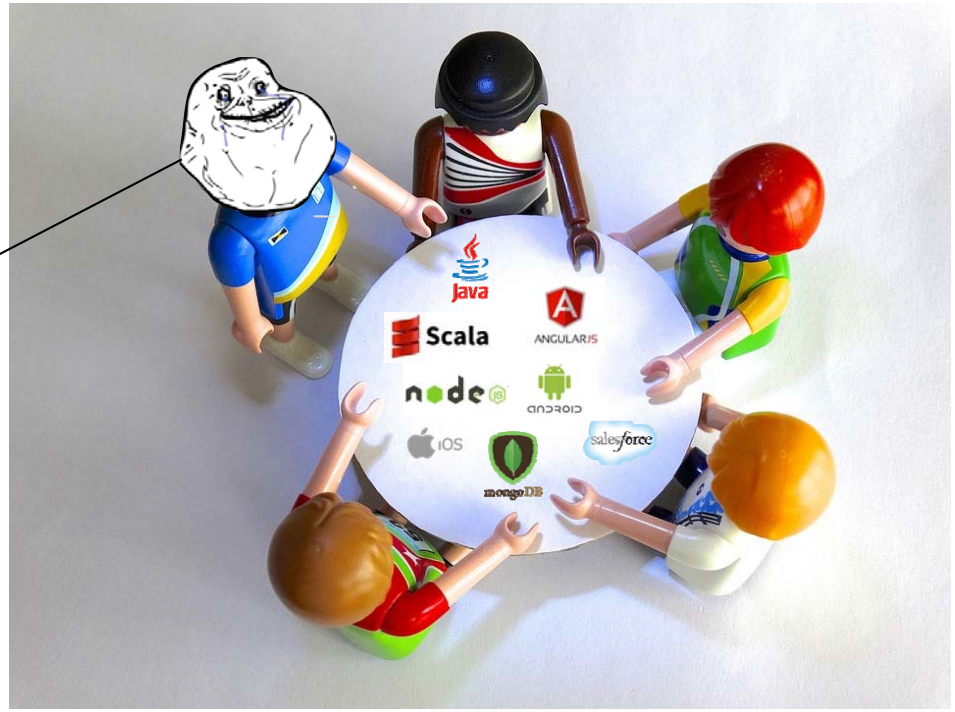
Data at the end of September 2015. It includes Garanti starting July

Introduction

- +135k employees company
- +20 different innovation teams
- +50 different innovation projects
- Agile methodologies
- +100 different technologies … and growing!

Introduction

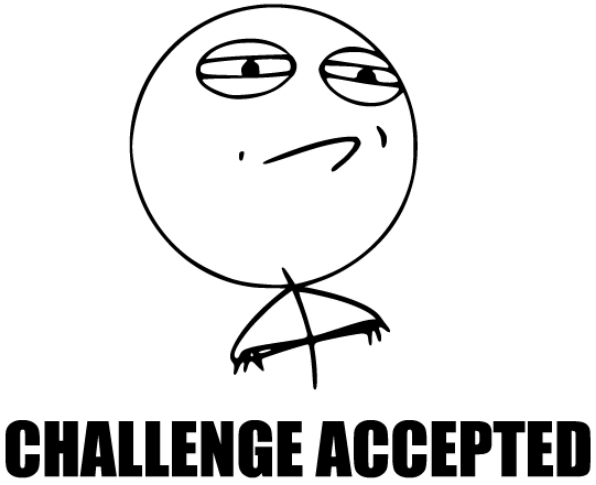
Bad news : And they all require security !



Poor security guy

Introduction

Good news : Change of paradigm



Introduction

Security skills revisited

- : Prepare to code (again)
- / Flexible
- 5 Keep updated (Self-learner)
- 8 Become an transformation enabler, not a stopper

Introduction

½ FROM

- Tailor made solutions
- Months to develop + deploy
- Hard to administrate & monitor
- Monolithic architecture
- Expensive $$$

TO ¼

- Generic Solutions
- Minutes to deploy
- Central administration & monitoring
- Modular architecture
- Almost ‘free’ Office [3]1

Slide 7

Office [3]1 of licence, not in hours and some pain

Microsoft Office User, 1/4/2016

Introduction

Ĭ

Build

- Competitive Advantage
- Innovation
- Flexible

Y

¿

Buy

- Commodity
- Mature
- Business as usual

Security cook book

Based on :

- What we learnt
- What worked for us

Recipe :

- Set of ingredients
- Set of instructions

Recipe #1: One proxy to rule them all

One proxy to rule them all

Ingredients :

WAF : ModSecurity + OWASP core rule set
Web Server: Apache/Nginx

Spring security
MongoDB
Redis

AV : ClamAV (Optional)

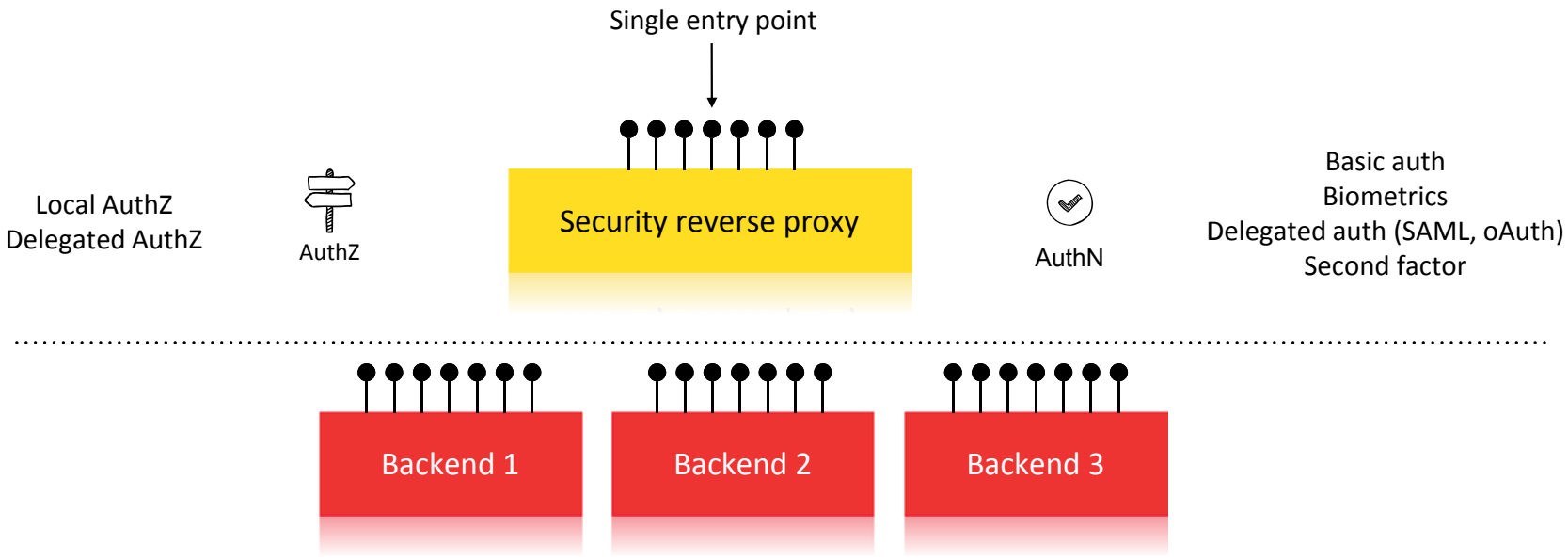
Instructions :

- Single entry point
- Technology agnostic, just http services
- Standard & homogeneous solutions

BBVA

Recipe #1 : One proxy to rule them all

One proxy to rule them all : AuthN + AuthZ



Recipe #1 : One proxy to rule them all

Features

Modular
Every functionality is separated into modules that can be deployment independently of all the others.

API-fied
Developer ready for easy integration.

Ready 4 Cloud
Tested and designed to get full advantage of Cloud Technology.

Hot Protection
All can be configured live on a dashboard.

OpenSource
Based on Open-Source technologies.

WAF + AV
Layer 7 Firewall and Antivirus protection built-in.

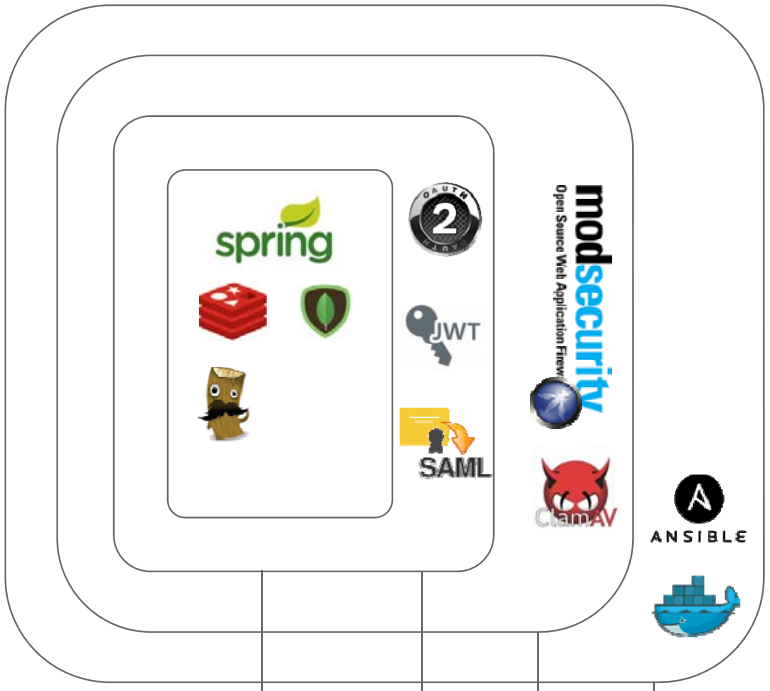
Easy to deploy
The solution can be deployed using Ansible Playbooks or Docker containers.

Monitored
Health and state are monitored live.

Standard
Compatible with JWT Tokens and oAuthv2 to consume REST Services.

Recipe #1 : One proxy to rule them all

What we used



Docker Container, Ansible Playbook
ModSecurity WAF + OWASP RuleSet + ClamAV
oAuth2, JWT, SAMLv2
Spring Security, Redis, MongoDB, Logstash

Spring Security
Powerful and highly customizable authentication and access-control framework.

Standard
OAuthv2 + JWT, SAMLv2.

ModSecurity
OpenSource Layer 7 Application Firewall with OWASP Core Rule Set.

ClamAV
OpenSource Antivirus.

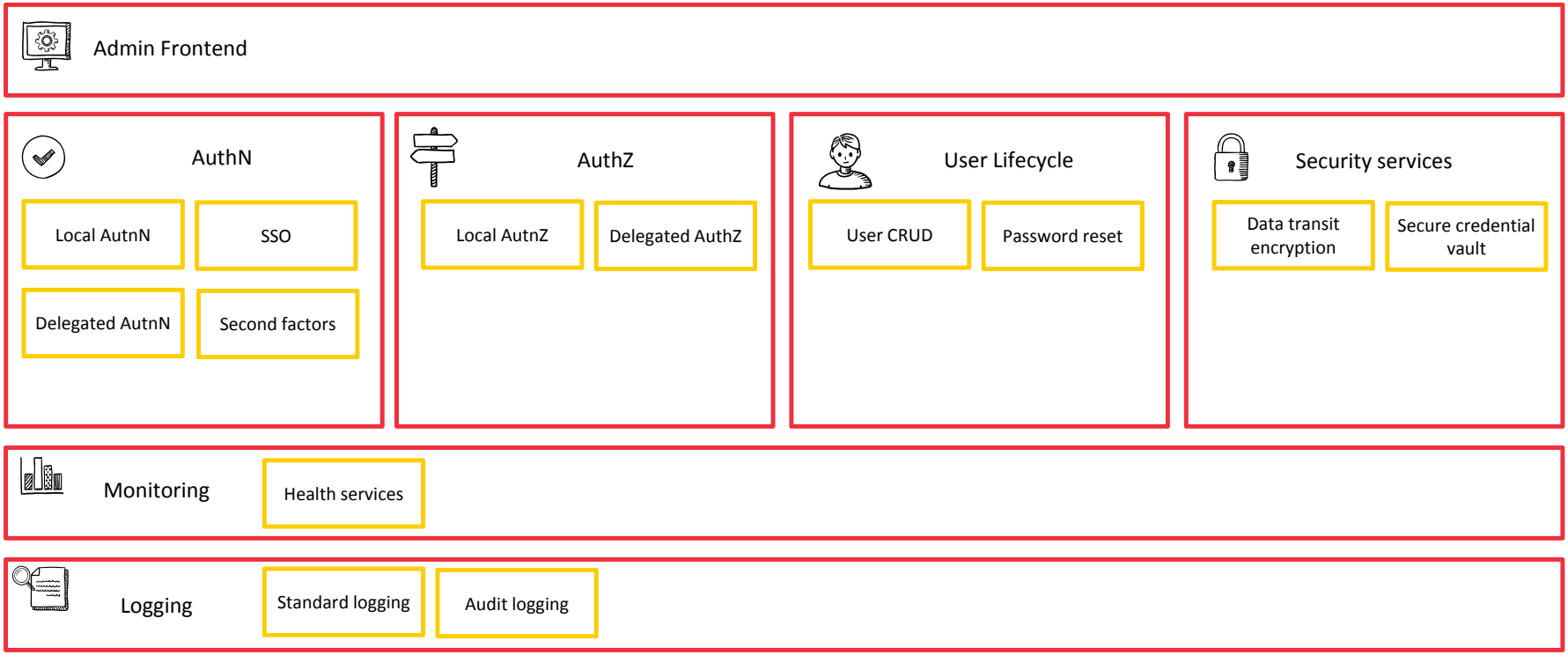
ELK Stack
ElasticSearch + Logstash + Kibana
Collect, parse, and store logs for later use.

Docker and Ansible
Open platform for developers and sysadmins to build, ship, and run distributed applications.

BBVA

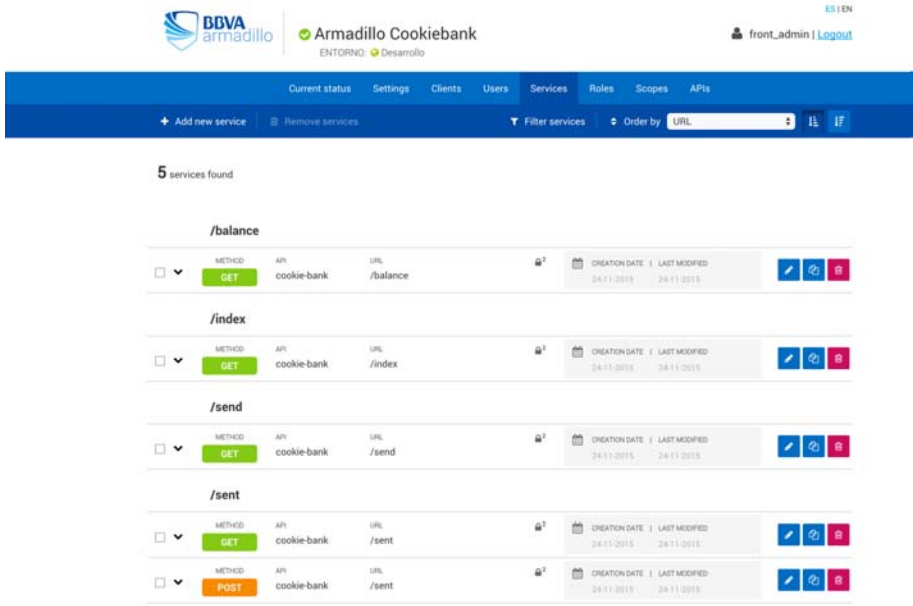
Recipe #1 : One proxy to rule them all

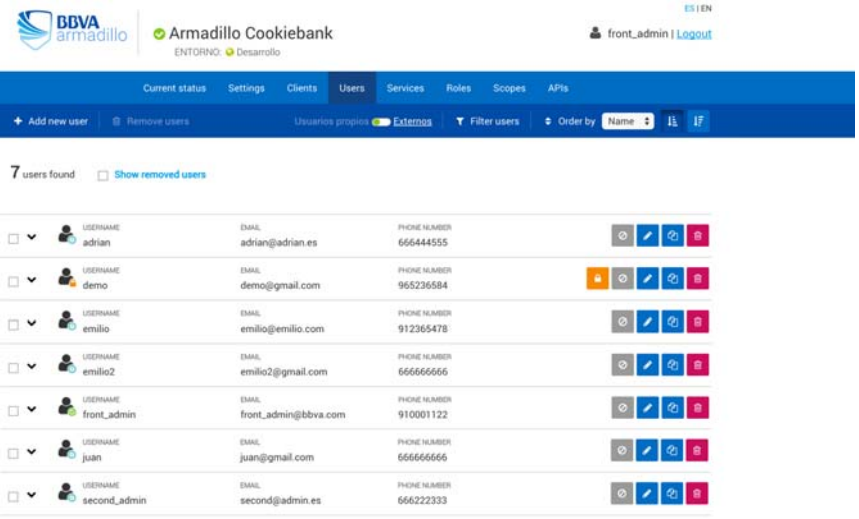
Introducing BBVA armadillo



Recipe #1 : One proxy to rule them all

Frontend Screenshots





BBVA

RSAConference2016

Recipe #2: Policy enforcement

Policy enforcement

Ingredients :

WSO2 Identity Server (PDP)
Security proxy (PEP)
External apps info (PIP)

Instructions :

- Segregate access decision from point of use
- Use standards

Recipe #2 : Policy enforcement

Policy enforcement

- XACML 3.0 (JSON Support)


PEP — Policy enforcement point

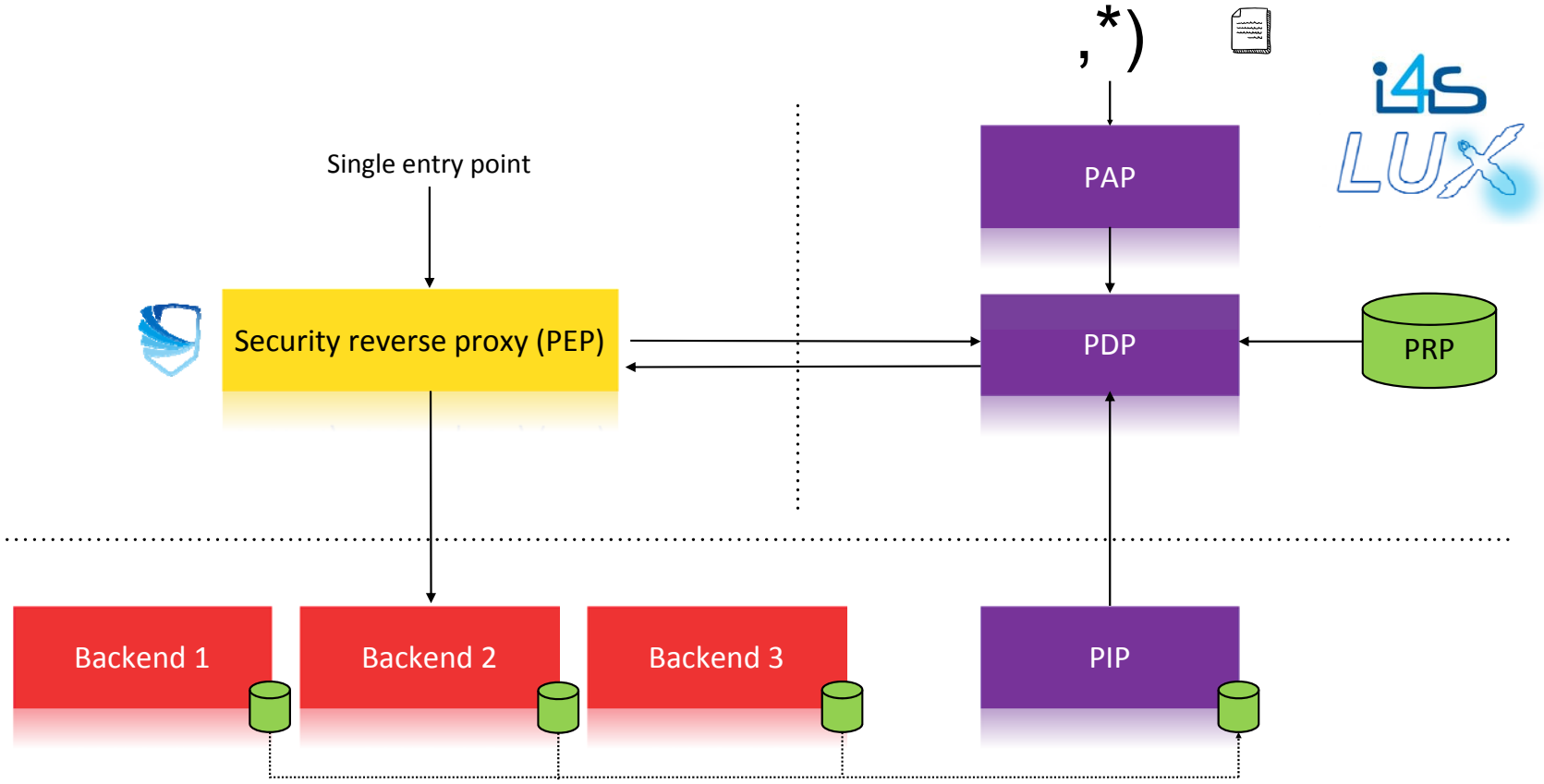

PDP — Policy decision point


PAP — Policy administration point


PIP — Policy information point


PRP — Policy retrieval point

Recipe #2 : Policy enforcement



Recipe #2 : Policy enforcement

Sample policies

Business policy

```
Allow access to resource Accounts with attribute CustomerID=x
     if Subject match AccountOwner
     and action is read
with obligation
     on Permit: doLog_Inform(CustomerID, Subject, time)
     on Deny : doLog_UnauthorizedLogin(CustomerID, Subject, time)
```

Security policy

```
Allow access to resource Accounts with attribute CustomerID=x
     if SourceIP match KnownIPList
     and action is write
with obligation
     on Permit: doLog_Inform(CustomerID, Subject, time)
     on Deny : doLog_UnauthorizedLogin(CustomerID, Subject, time)
```

- Code repository (e.g Git)
- Versionable
- ‘Human readable’

If you want to go further …

- Historical data
- Behavior analysis
- Scoring System (Policy chain)

Recipe #3 : Speedy surf board : Automating security deployments

Speedy surf board : Automating security deployments

Ingredients :

Ansible
Terraform

Instructions :

- Eat
- Sleep
- AUTOMATE
- Repeat

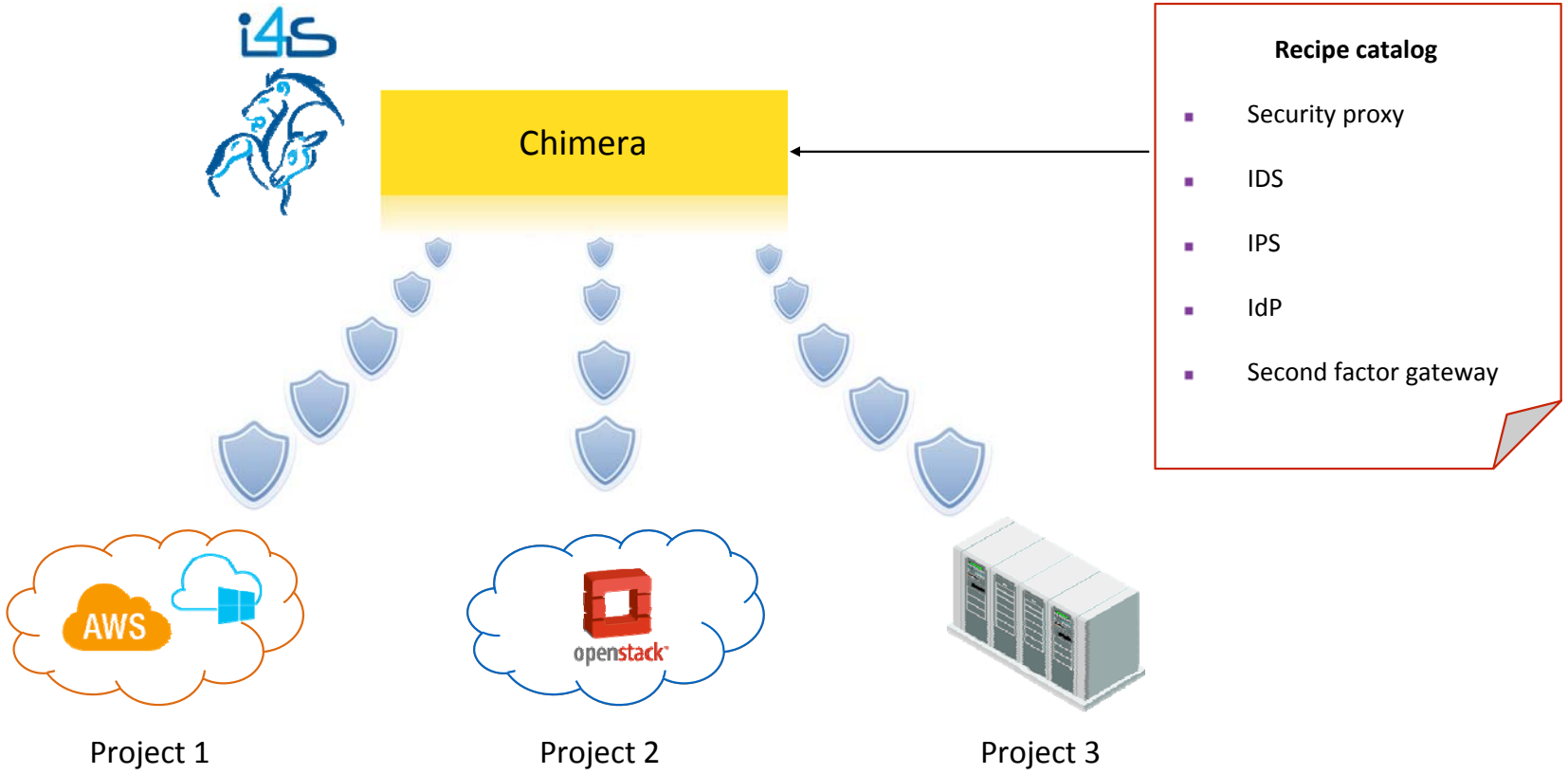
Recipe #3: Speedy surf board : Automating security deployments

- Easily deploy security
- Technology agnostic
- Fast
- Repeatable

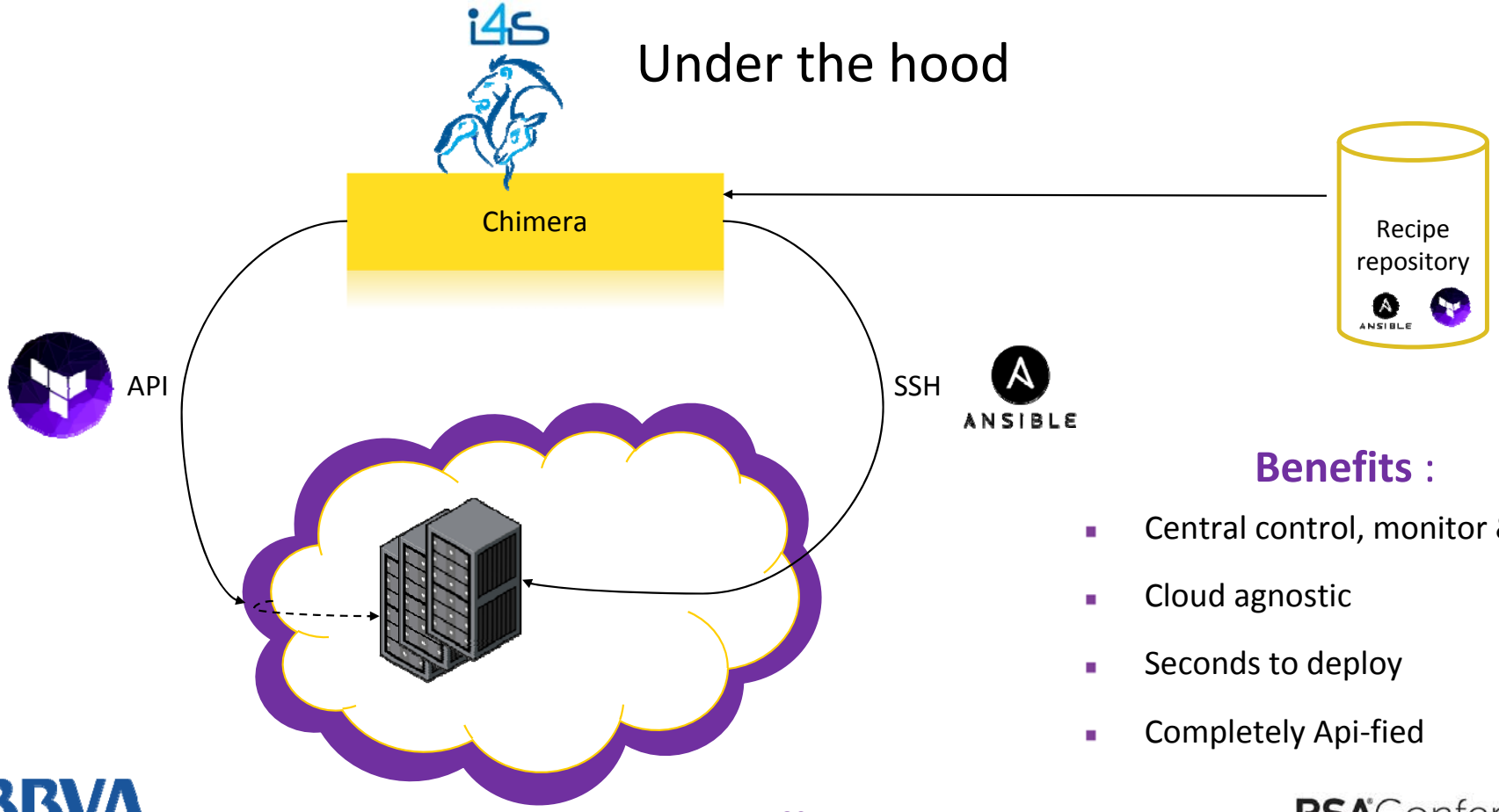
Automation becomes a MUST

The wave has come … and you need a speedy surfboard to ride it.

Recipe #3: Speedy surf board : Automating security deployments



Recipe #3: Speedy surf board : Automating security deployments



Benefits :

- Central control, monitor & audit
- Cloud agnostic
- Seconds to deploy
- Completely Api-fied

What we achieved

One proxy to rule them all

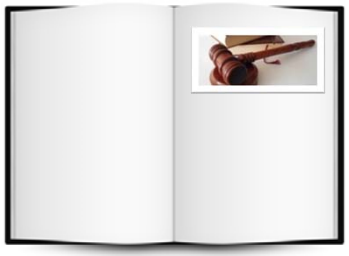
Metrics

- Time to protect

20+ days ¼ **3** days

Business impact

- New technologies enabled in a secure manner
- Security development cost reduced



Policy enforcement

Metrics

- Time to enforce

2 days ¼ **0** Instant !

Business impact

- Human interaction reduced (Less prone to errors)
- Centralized policies repository (Better control)

Speedy surf board : Automating security deployments

Metrics

- Time to deploy

3 days ¼ **1** minute

Business impact

- Security deployment costs reduced
- Reduced bureaucracy

Top ten tips

1) **Anticipate** to be able to run with business
2) **Adopt,** take advantage of new ways of doing things
3) **Change of attitude** : Less ‘No’ and more ‘Not that way’
4) Keep **transparent**
5) **Agile** and **flexible**

Office [2]1 transparent or invisible ??

Microsoft Office User, 1/4/2016

Top ten tips

6) Be **standard**
7) **Read, read** and **read …**
8) **Segregation** of duties
9) **Automate** as much as you can

BBVA

10) Just ride the wave …

Thanks !!!

Reference

WS02 Identity server

ELK stack explained

How to install ELK stack

IETF XAMCL 3.0

AAA authorization framework

Ansible

Terraform

* All the pictures used on this presentation are under the 'Creative commons CC0' license

icons

Qwertyuiopasdfghjklñzxcvbnm,.-
1234567890’¡ºQWERTYUIOP^*ASDFGHJKLÑ¨ÇªZXCVBNM;:_
¿?=)(/&%$·”!>><<|@#¢∞¬÷“”≠´,|{}[]–…„\ÅÊ¡ŪĭĹ½¼Ó×ê