EUROPEAN CYBER SECURITY CHALLENGE

Evil prevails when good humans do nothing!

European Cyber Security Challenge CTF System

Wuhan
May 21th, 2016

OWASP
The Open Web Application Security Project

ECSC 2016

Motivation for National CTF

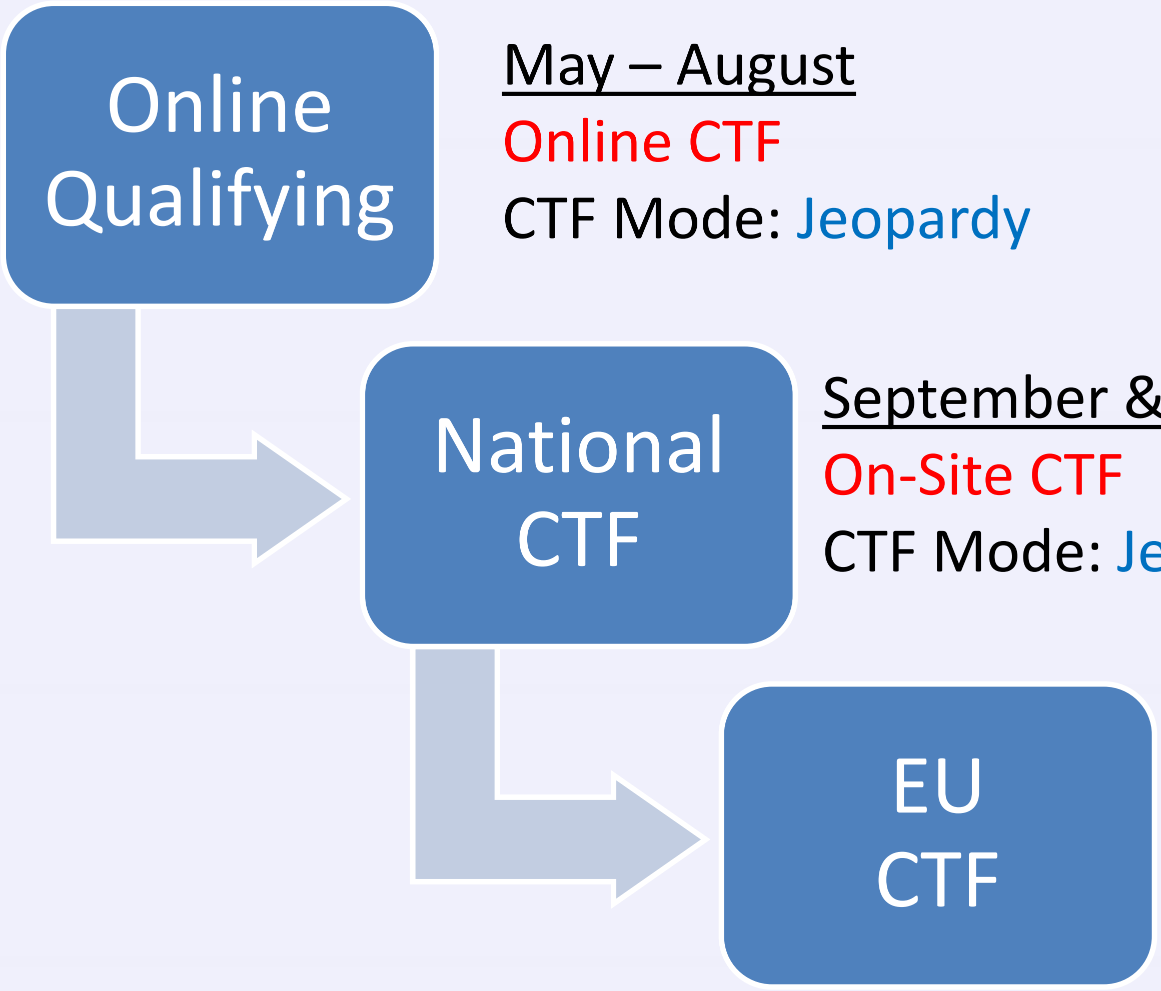
- Today, most European countries lack sufficient and talented IT security professionals to protect their IT infrastructure.
- To help mitigate this problem, Europe is setting up national cyber security competitions for finding young cyber talents and for encouraging them to pursue a career in cyber security.

Network & Collaborate

- The European Cyber Security Challenge (ECSC) leverages these competitions in that it adds a pan-European layer to them:
- The top cyber talents from each country meet to network and collaborate and finally compete against each other to determine which country has the best cyber talents.

ECSC is a 3-step competition

OWASP
The Open Web Application Security Project



Online Qualifying

May – August
Online CTF
CTF Mode: Jeopardy

National CTF

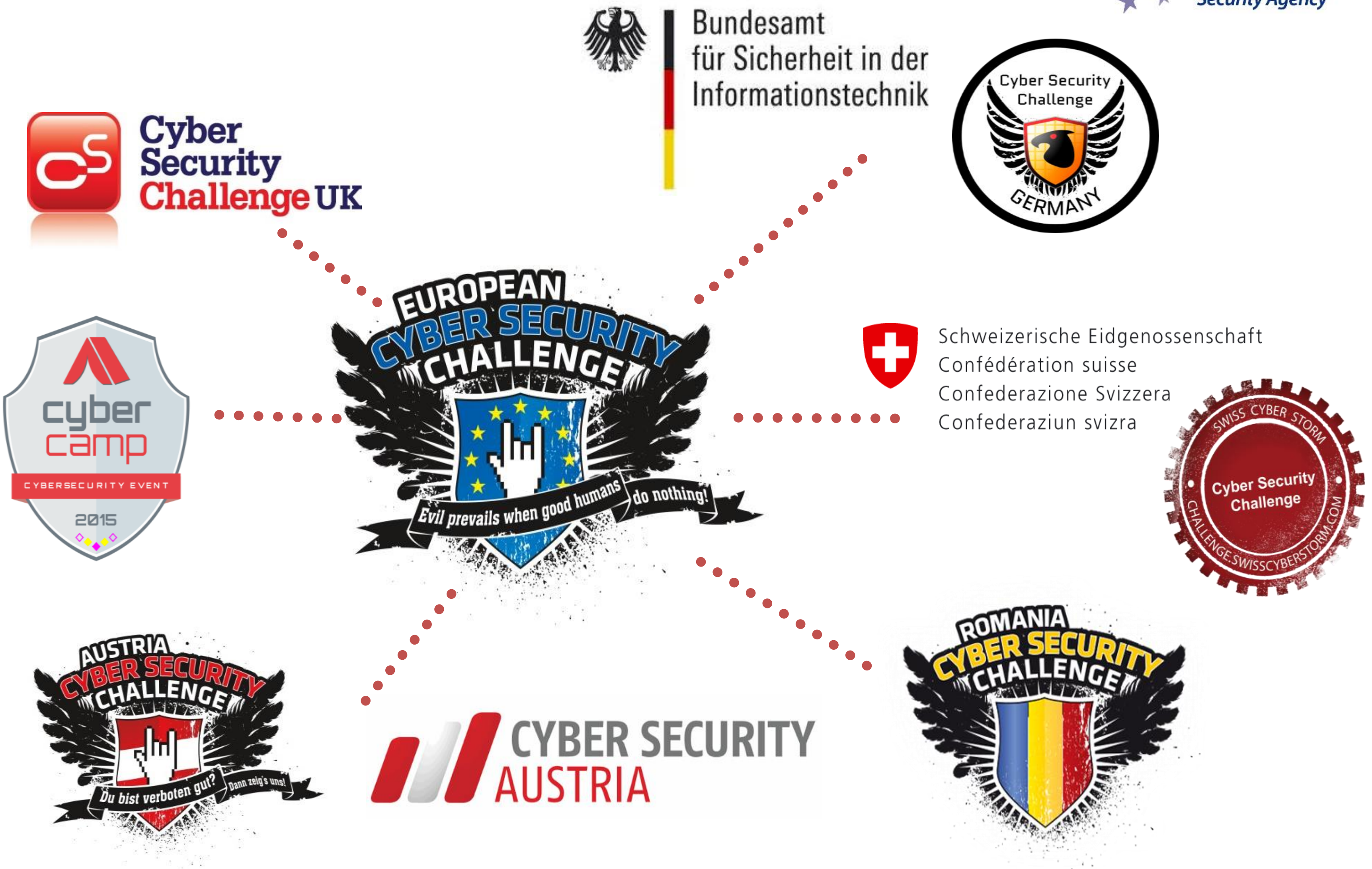
September & October
On-Site CTF
CTF Mode: Jeopardy

EU CTF

November
On-Site CTF
CTF Mode: Attack and Defense (mixed mode)

European Cyber Security Challenge 2015

enisa
European Network and Information Security Agency


Bundesamt für Sicherheit in der Informationstechnik
Cyber Security Challenge GERMANY
Cyber Security Challenge UK
EUROPEAN CYBER SECURITY CHALLENGE
Evil prevails when good humans do nothing!
cyber camp
CYBERSECURITY EVENT
2015
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
SWISS CYBER STORM
Cyber Security Challenge
CHALLENGE.SWISSCYBERSTORM.COM
AUSTRIA CYBER SECURITY CHALLENGE
Du bist verboten gut?
Dann zeig's uns!
CYBER SECURITY AUSTRIA
ROMANIA CYBER SECURITY CHALLENGE

ECSC – Who can participate?

- Who is allowed to participate?
  - – Everyone between 14-30 years old
  - – without a master diploma (MSc)
- What is the size of the teams per country?
  - – 5 people between 14 and 20 years old
  - – 5 people between 21 and 30 years old
  - – 2 coaches (not allowed to help during the CTF competition)
  - – TOTAL = 12 people per country

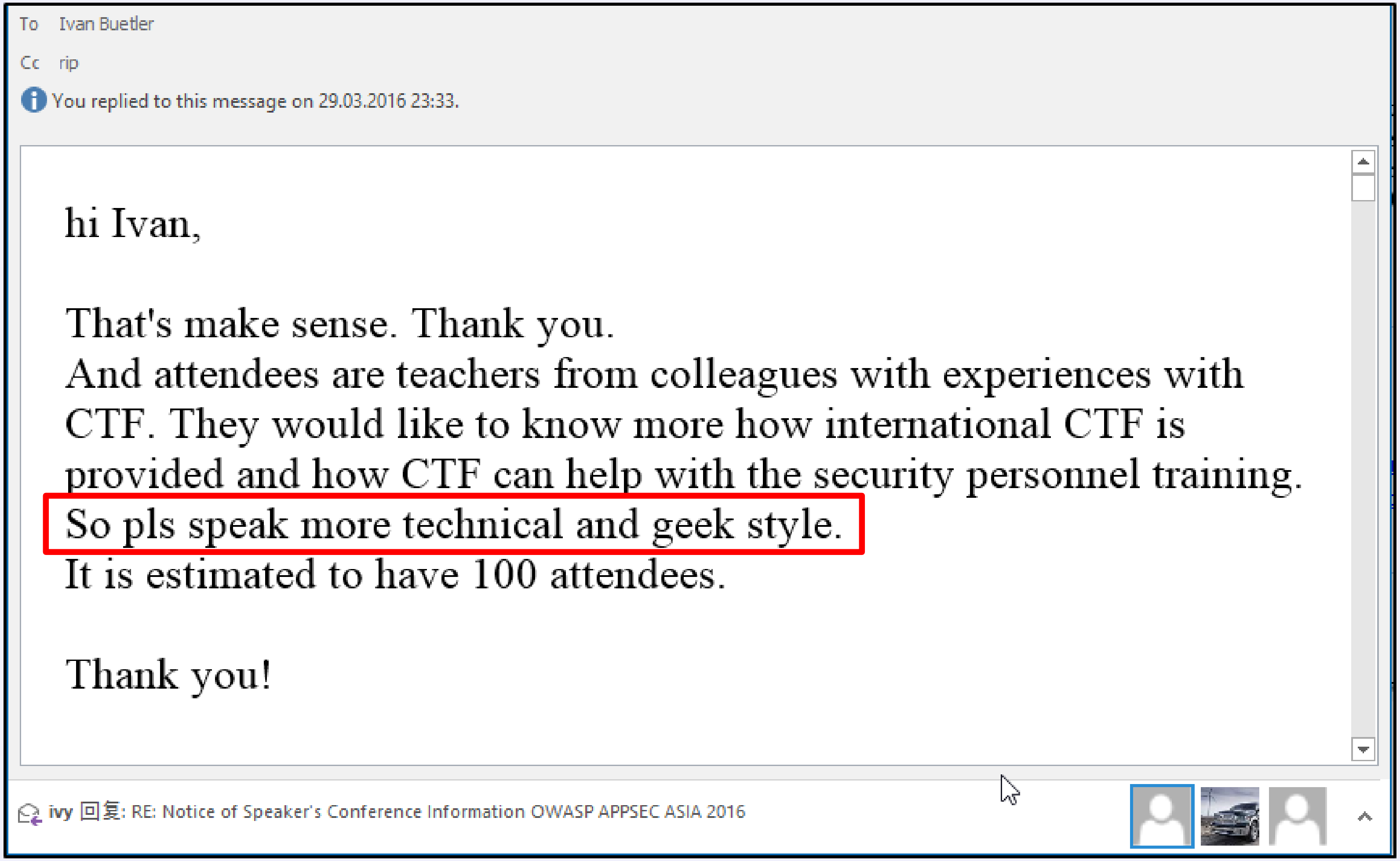
What is the CTF about?

OWASP
The Open Web Application Security Project

- Exploiting & Penetration Testing
- Reverse Engineering
- Crypto
- Fixing Vulnerabilities & Hardening
- IT Operations -> System Engineering Tasks
- IT Development -> Secure Programming
- Incident Handling -> Forensics -> APT Analysis
- Communication -> Presentation

What is this talk about?

- Speak more technical and **geek style**



To Ivan Buetler

Cc rip

You replied to this message on 29.03.2016 23:33.

hi Ivan,

That's make sense. Thank you.
And attendees are teachers from colleagues with experiences with CTF. They would like to know more how international CTF is provided and how CTF can help with the security personnel training.
So pls speak more technical and geek style.
It is estimated to have 100 attendees.

Thank you!

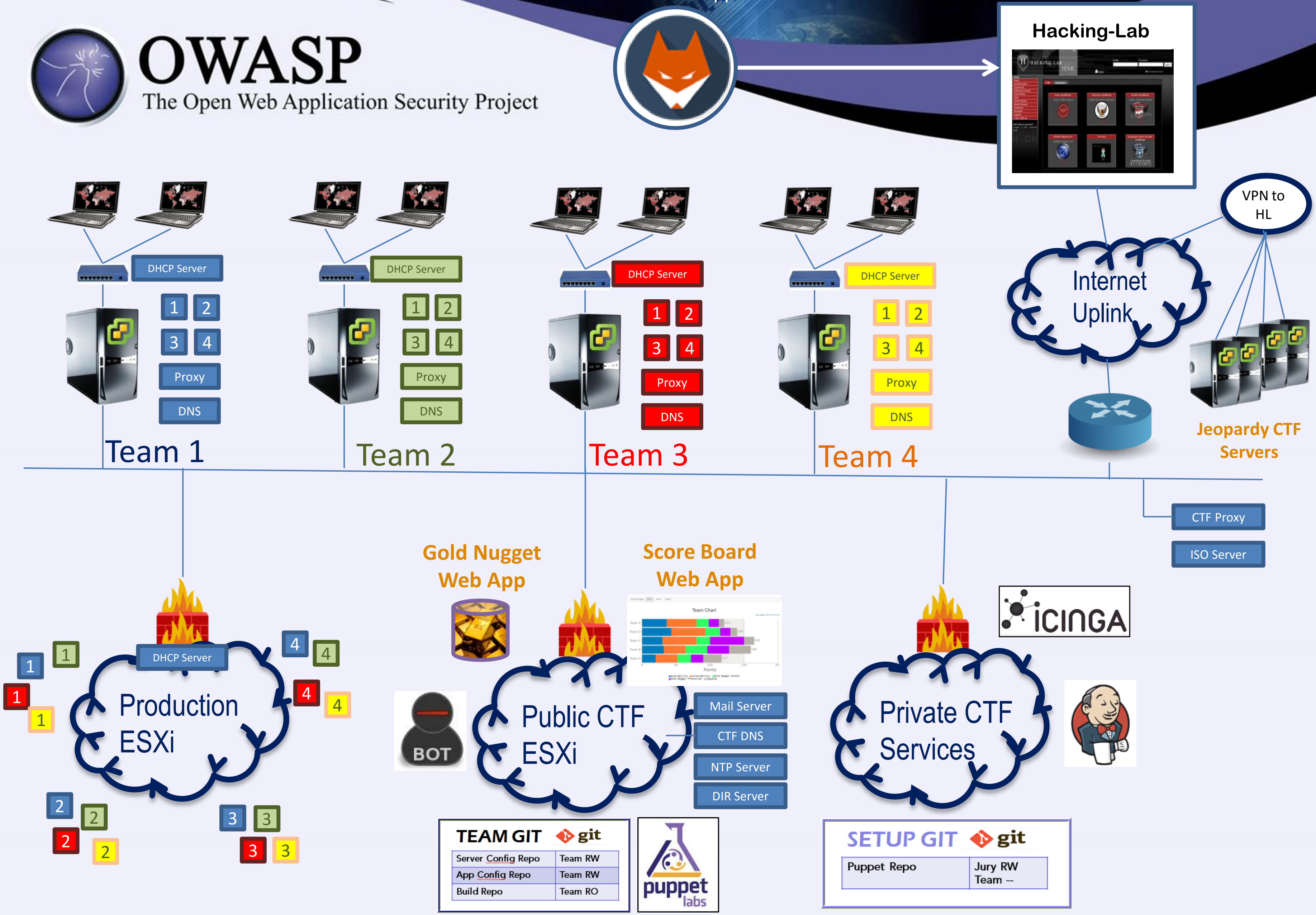
ivy 回复: RE: Notice of Speaker's Conference Information OWASP APPSEC ASIA 2016

CTF Details

geek language

CTF Architecture

OWASP
The Open Web Application Security Project



Mobile CTF App

Hacking-Lab

VPN to HL

Internet Uplink

Jeopardy CTF Servers

CTF Proxy

ISO Server

DHCP Server

1 2 3 4

Proxy

DNS

Team 1

Team 2

Team 3

Team 4

Gold Nugget Web App

Score Board Web App

Team Chart

Points

Production ESXi

Public CTF ESXi

Private CTF Services

BOT

Mail Server

CTF DNS

NTP Server

DIR Server

ICINGA

puppet labs

TEAM GIT git

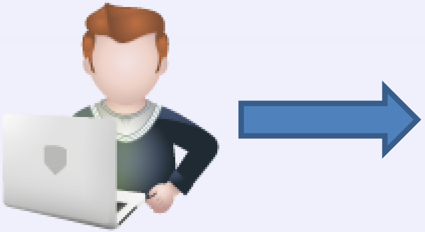
Server Config Repo	Team RW
App Config Repo	Team RW
Build Repo	Team RO

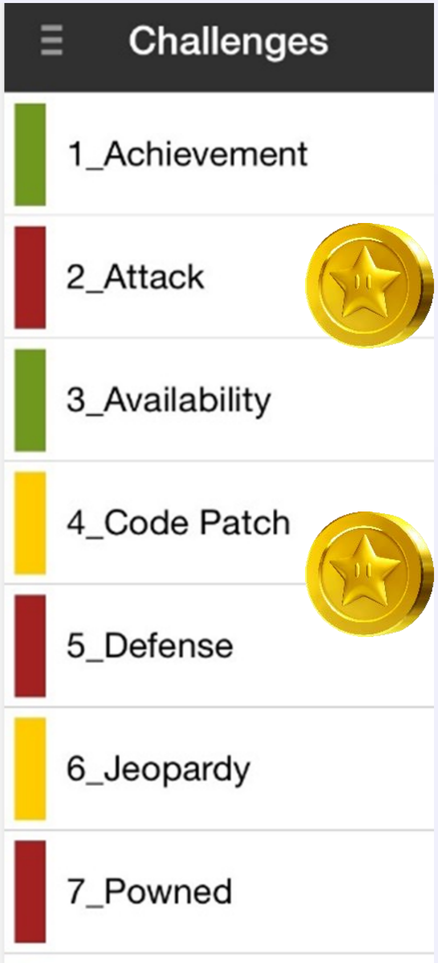
SETUP GIT git

Puppet Repo	Jury RW Team --

CTF Tasks

CTF Tasks





☰ Challenges

🟩 1_Achievement

🟥 2_Attack

🟩 3_Availability

🟨 4_Code Patch

🟥 5_Defense

🟨 6_Jeopardy

🟥 7_Powned

Setup and maintain a service like DNS, Proxy, E-Mail, Apache, WordPress, …

Hack in other CTF team servers and services and steal the gold nugget (EXPLOITATION)

Keep own services up and running (IT OPS)

Fix vulnerable software & services (IT DEV)

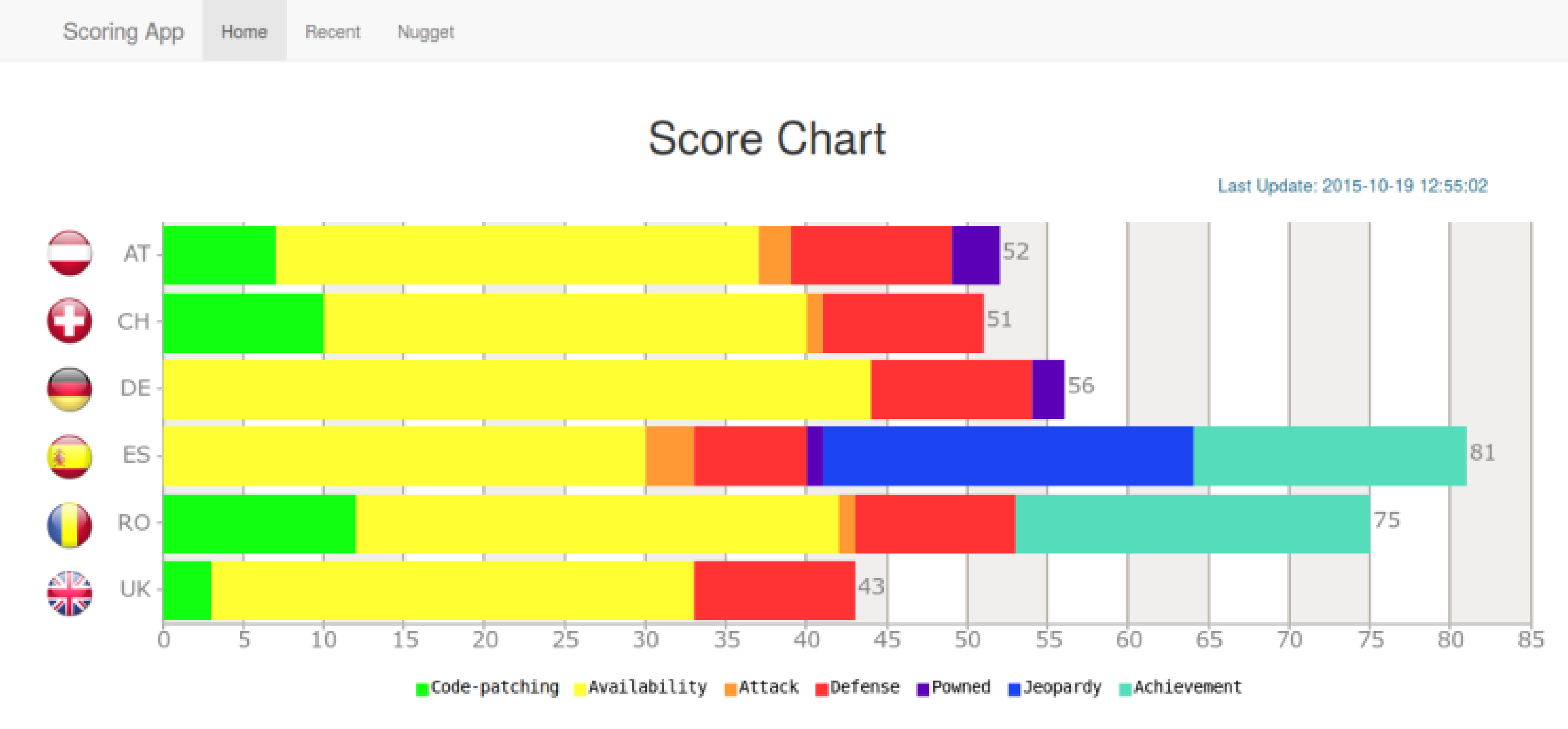
Safe guard own gold nuggets

Solving jeopardy challenges

Own a device/server and prove the attack by leaving a special gold nugget, known ad evidence nugget (0-day)

Scoring

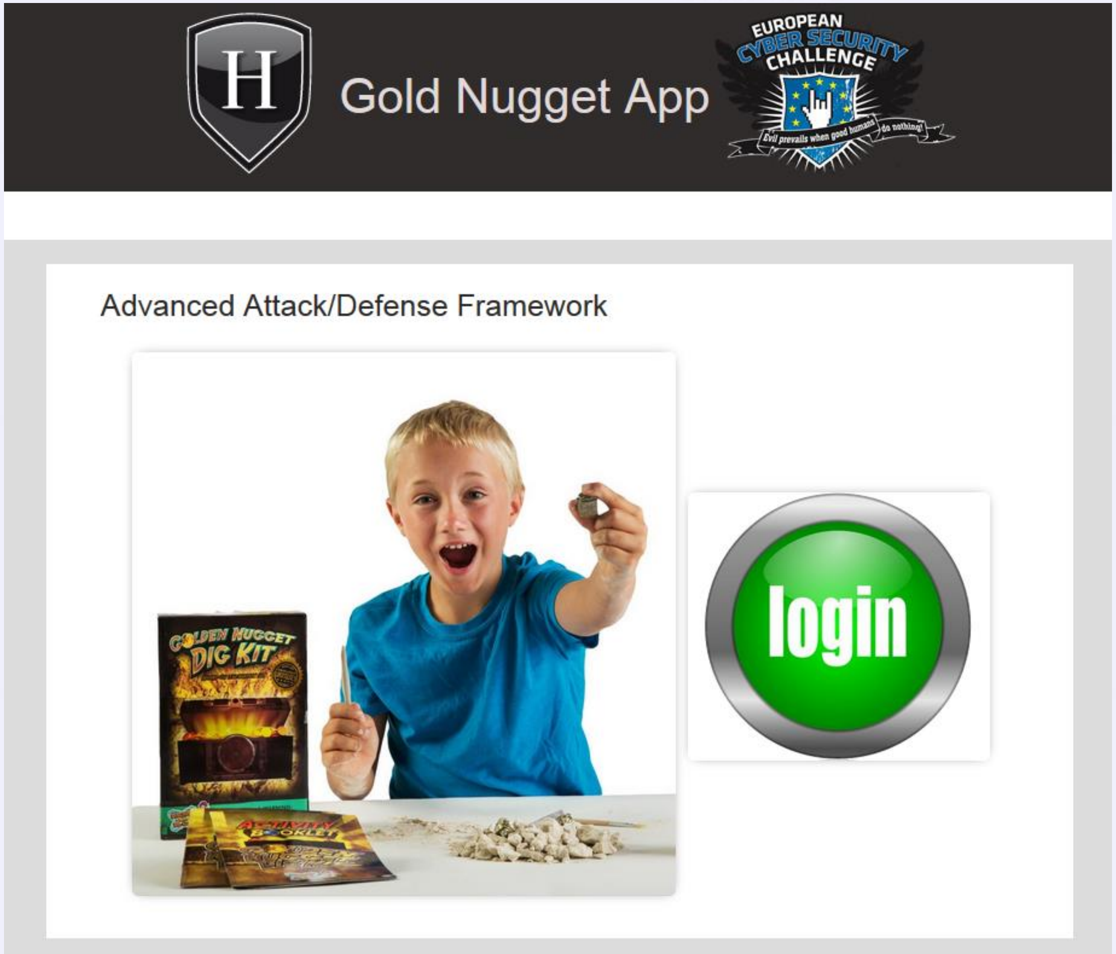
- Code Patching & Availability & Attack …



The CTF Glue

CTF players must find/hack/disclose a string, known as gold nugget, from the 'vulnerable' services of the other teams

The purpose of the gold nugget is to claim points for a successful attack



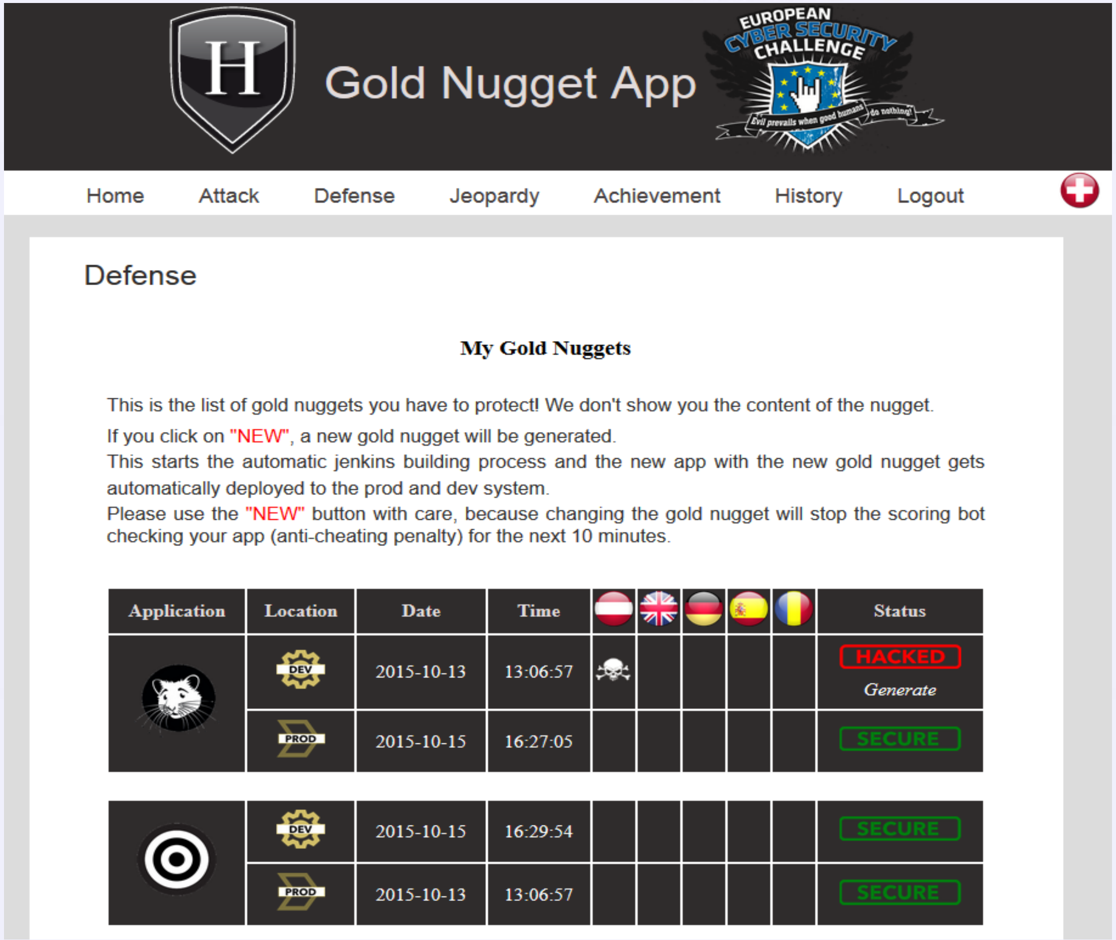
Gold Nugget App

Advanced Attack/Defense Framework

H
EUROPEAN CYBER SECURITY CHALLENGE
Evil prevails when good humans do nothing!
GOLDEN NUGGET DIG KIT
ACTIVITY BOOKLET
login

The CTF Glue
Gold Nuggets

Gold Nuggets are digitally signed strings. The gold nugget app is issuing them. The gold nugget app knows, who owns what gold nugget


H
EUROPEAN CYBER SECURITY CHALLENGE
Evil prevails when good humans do nothing!

Gold Nugget App

Home
Attack
Defense
Jeopardy
Achievement
History
Logout

Defense

My Gold Nuggets

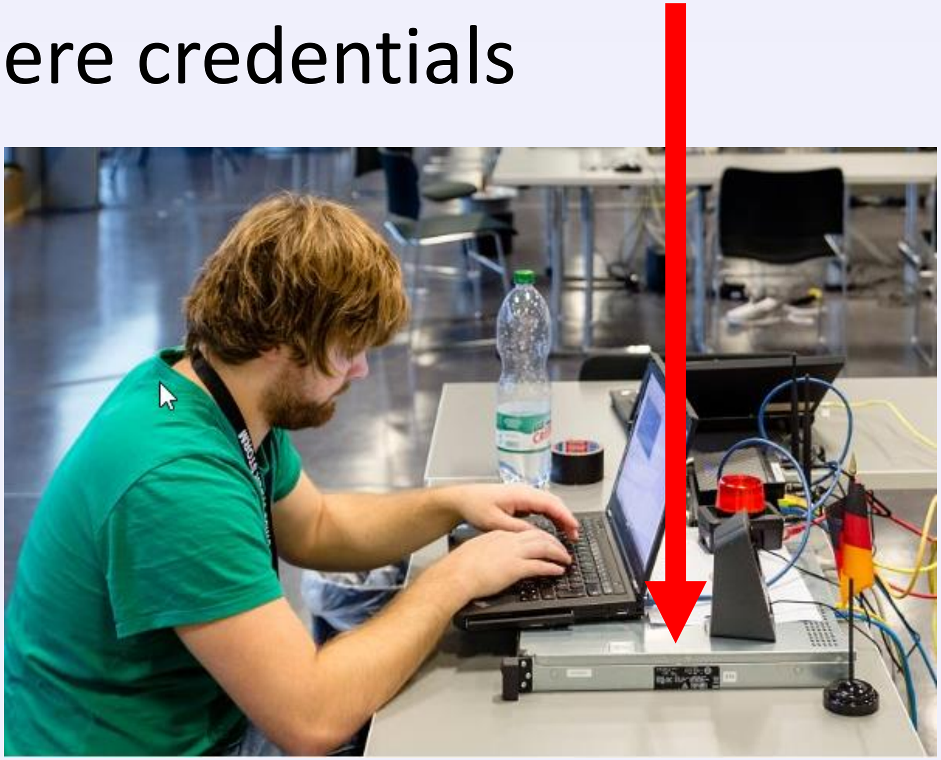
This is the list of gold nuggets you have to protect! We don't show you the content of the nugget.

If you click on "NEW", a new gold nugget will be generated.
This starts the automatic jenkins building process and the new app with the new gold nugget gets automatically deployed to the prod and dev system.
Please use the "NEW" button with care, because changing the gold nugget will stop the scoring bot checking your app (anti-cheating penalty) for the next 10 minutes.

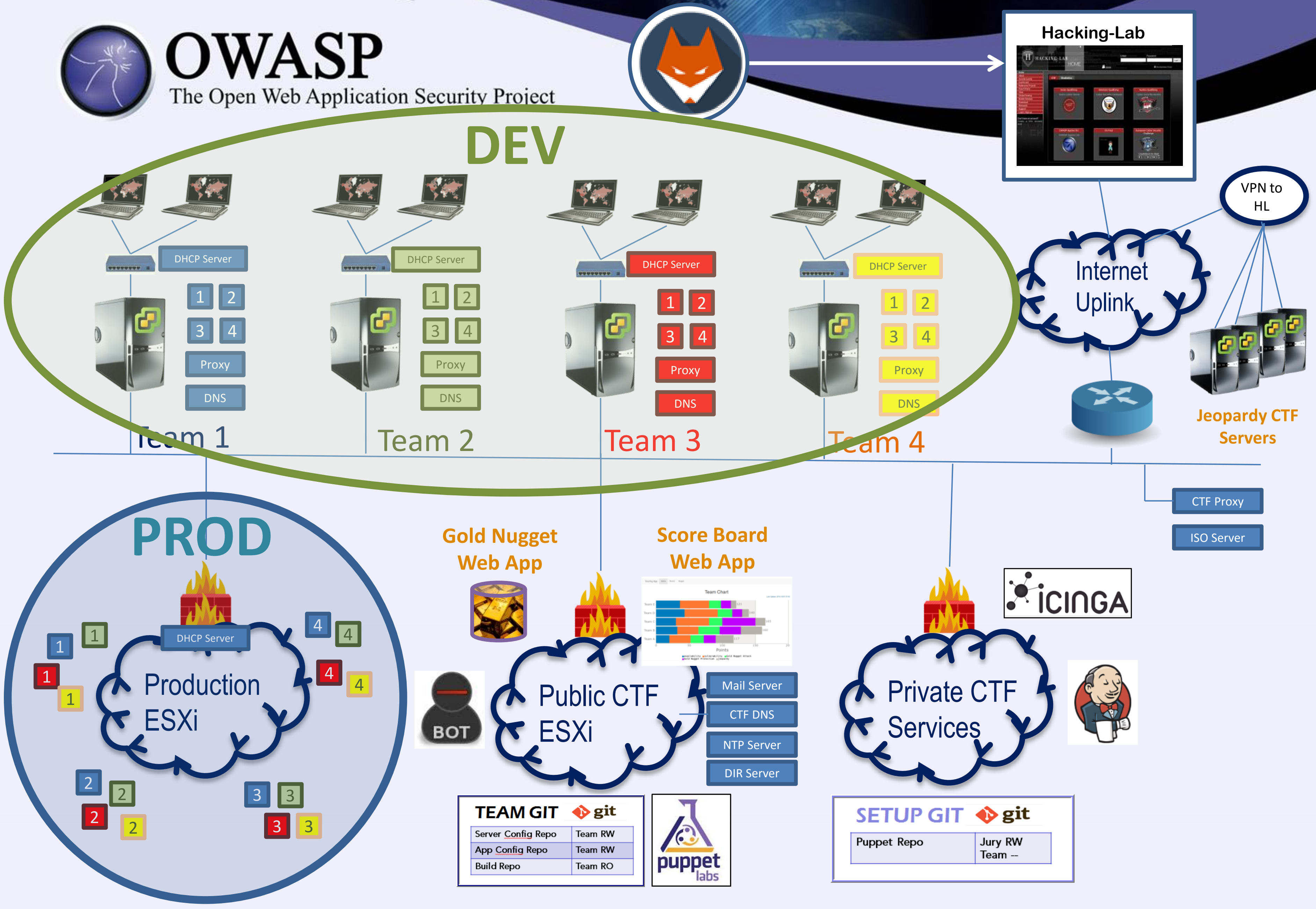
Application	Location	Date	Time	🇦🇹	🇬🇧	🇩🇪	🇪🇸	🇷🇴	Status
	DEV	2015-10-13	13:06:57	☠					HACKED *Generate*
	PROD	2015-10-15	16:27:05						SECURE
◎	DEV	2015-10-15	16:29:54						SECURE
	PROD	2015-10-13	13:06:57						SECURE

Team ESX = DEV SYSTEM

- Every CTF team gets a physical server (ESXi) and the proper vSphere credentials
- The ESXi is pre-configured with several pre-installed VM's
- The team ESXi is named as "**DEV**" system



CTF Architecture



TEAM GIT git

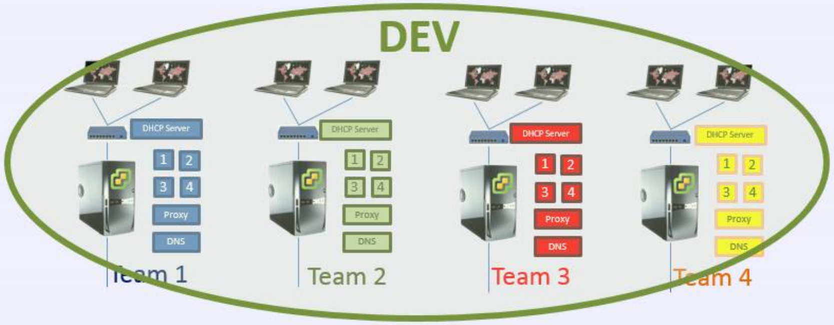
Server Config Repo	Team RW
App Config Repo	Team RW
Build Repo	Team RO

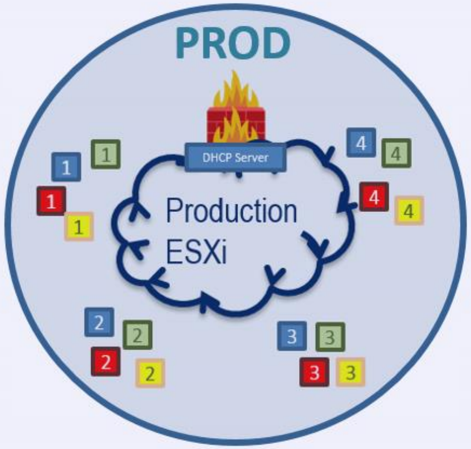
SETUP GIT git

Puppet Repo	Jury RW Team --

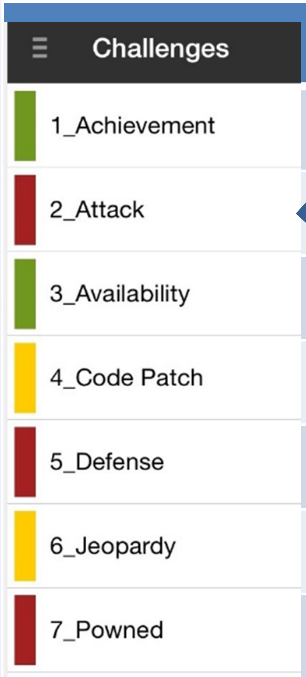
Production ESXi

- The apps on **DEV** is ‘equal’ or ‘identical’ as on **PROD**
- On **DEV**, teams have root access (SSH)
- On **PROD** teams do *NOT* have root or interactive access





Attacking



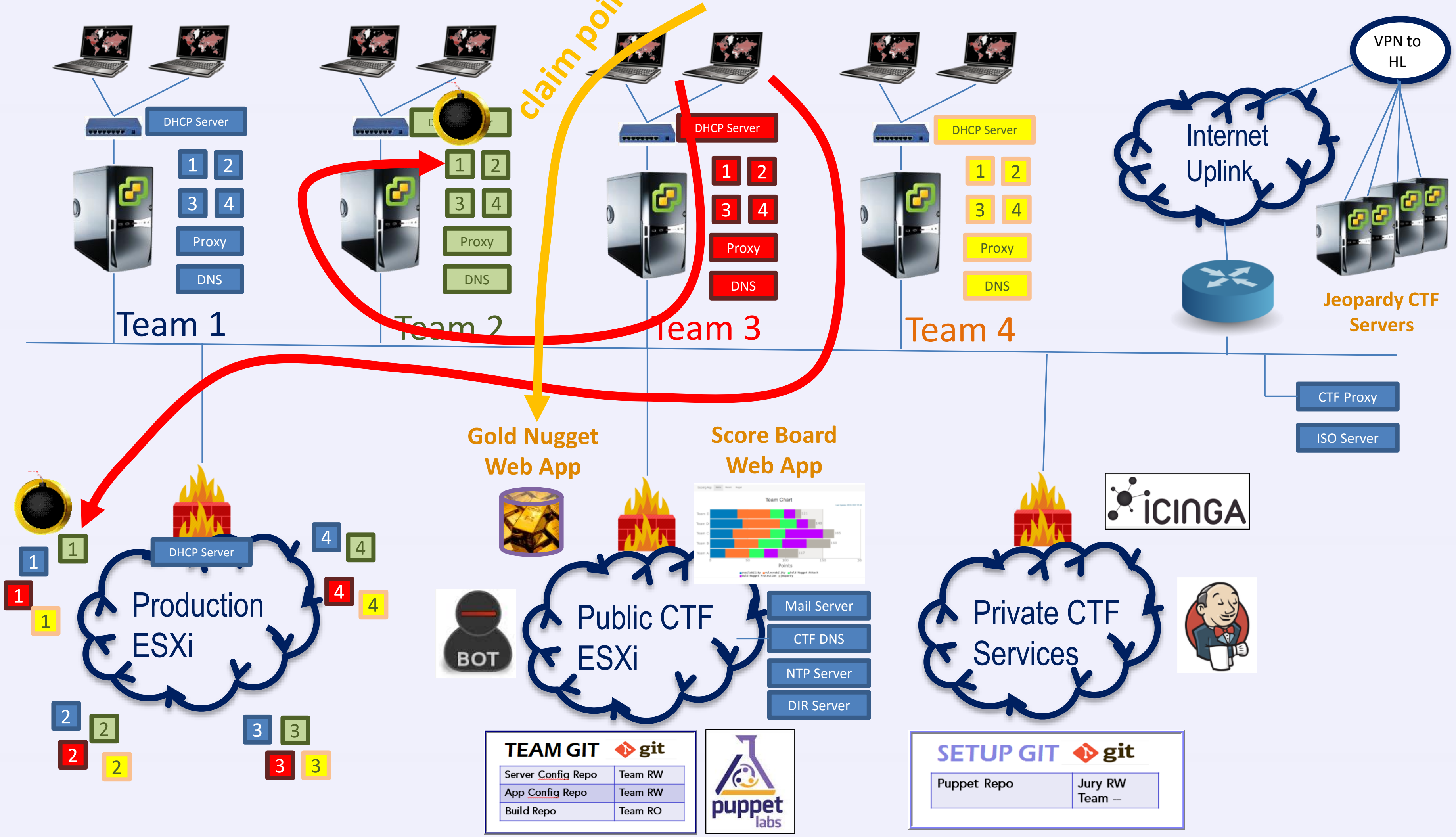
Challenges		
🟩 1_Achievement		
🟥 2_Attack	⇦	Stealing Gold Nugget
🟩 3_Availability		
🟨 4_Code Patch		
🟥 5_Defense		
🟨 6_Jeopardy		
🟥 7_Powned		

Attacking

- Every team is allowed to attack other teams on the **DEV** or **PROD** environment
- On success, the attacking team discloses the gold nugget from the victim team
- The gold nugget is different in **DEV** and **PROD** for any team and app (every gold nugget is unique)
- The gold nugget must be used to claim points using the gold nugget app

Attacking

OWASP
The Open Web Application Security Project



TEAM GIT git

Server Config Repo	Team RW
App Config Repo	Team RW
Build Repo	Team RO

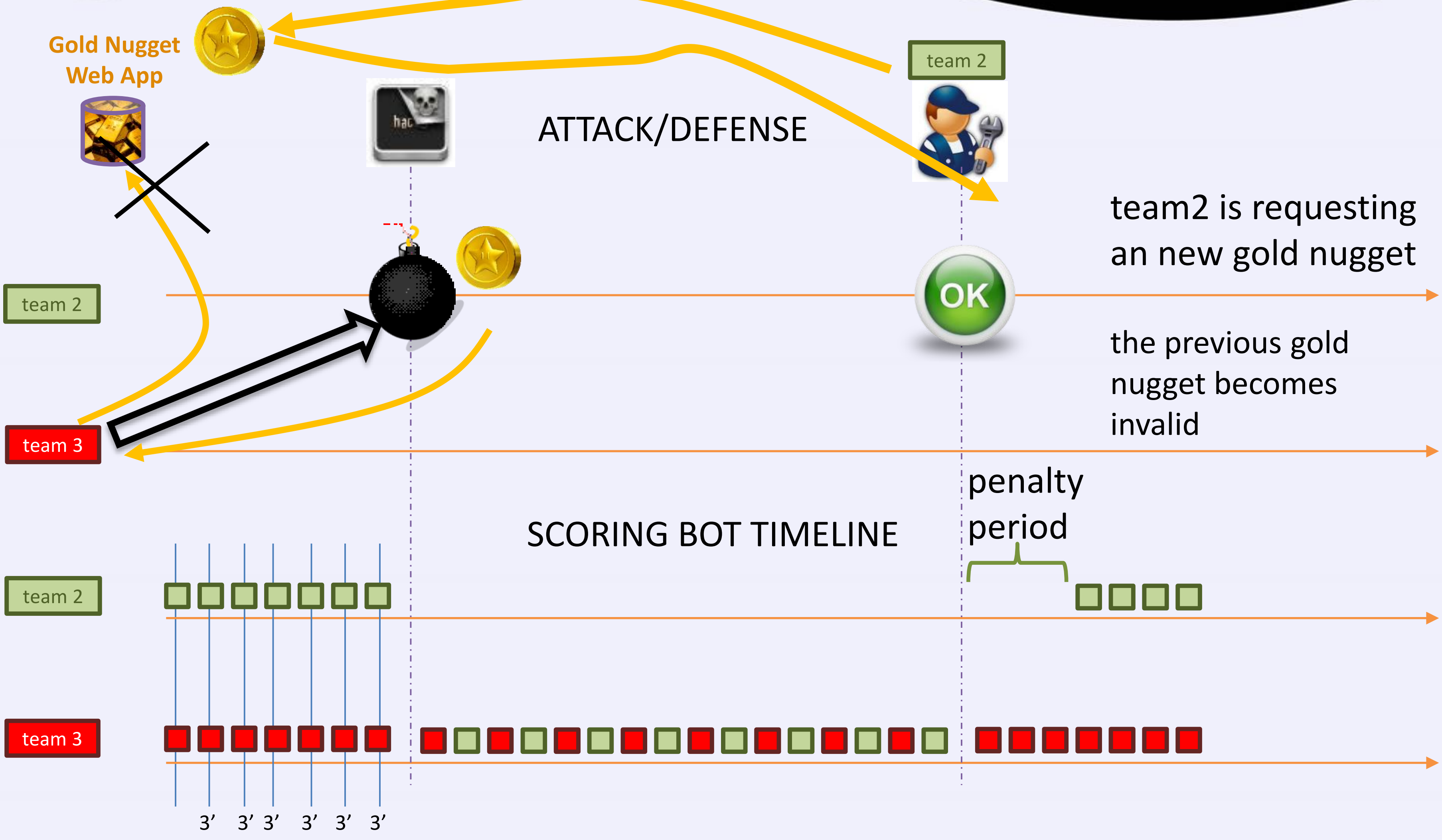
SETUP GIT git

Puppet Repo	Jury RW Team --

Scoring per Time Unit

OWASP

The Open Web Application Security Project



ATTACK/DEFENSE

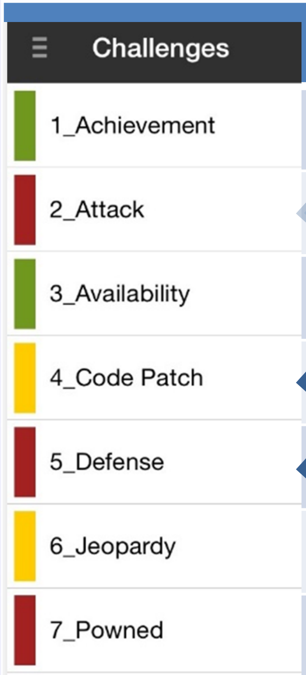
team2 is requesting an new gold nugget

the previous gold nugget becomes invalid

SCORING BOT TIMELINE

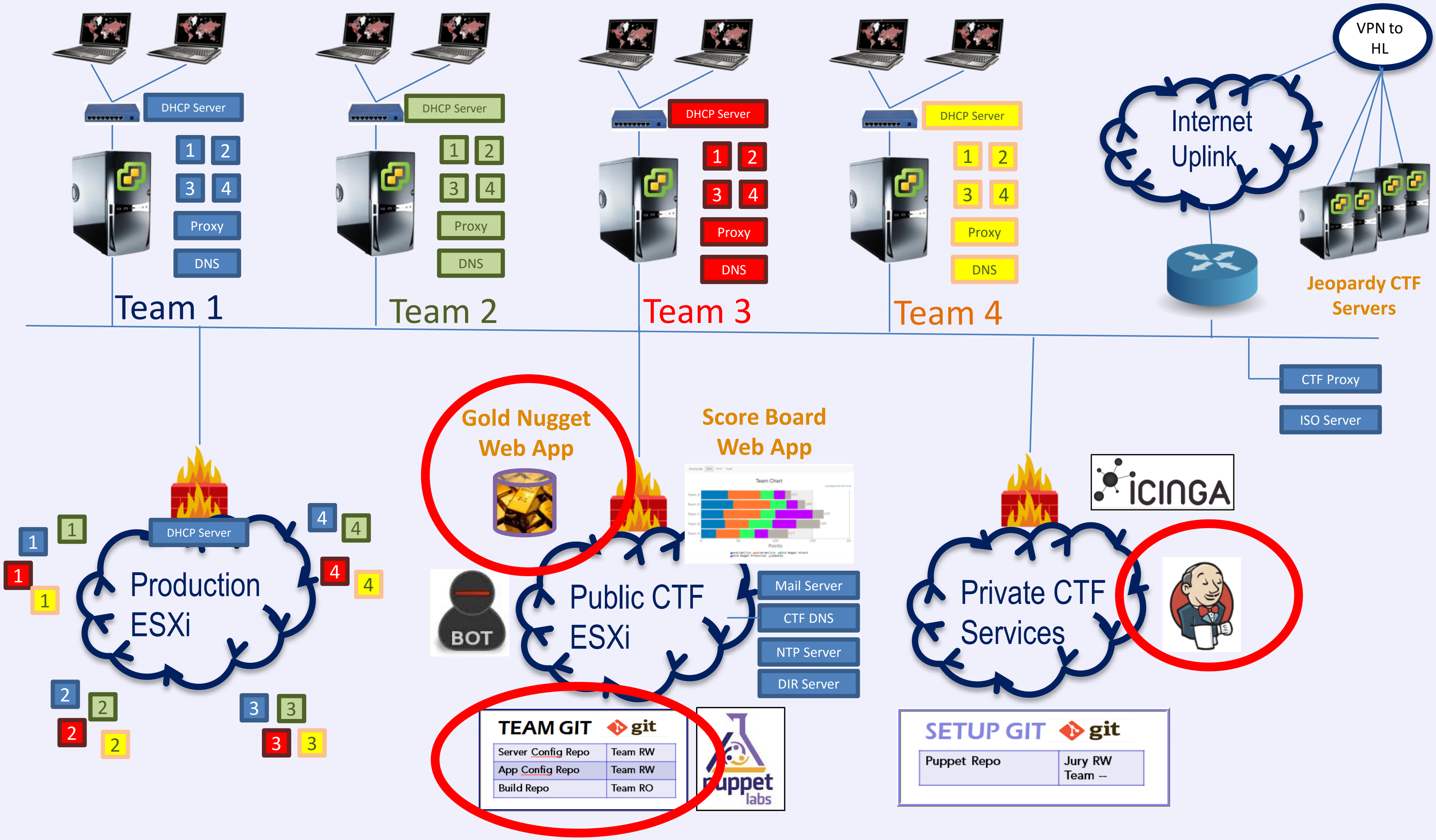
penalty period

Fixing Vulnerable Apps



Challenges		
1_Achievement		
2_Attack	⇦	Stealing Gold Nugget
3_Availability		
4_Code Patch	⇦	Fix vulnerable software & services
5_Defense	⇦	Safe guard own gold nuggets
6_Jeopardy		
7_Powned		

Fixing vulnerable apps



VPN to HL

Internet Uplink

Jeopardy CTF Servers

CTF Proxy

ISO Server

Team 1: DHCP Server, 1, 2, 3, 4, Proxy, DNS

Team 2: DHCP Server, 1, 2, 3, 4, Proxy, DNS

Team 3: DHCP Server, 1, 2, 3, 4, Proxy, DNS

Team 4: DHCP Server, 1, 2, 3, 4, Proxy, DNS

Production ESXi

DHCP Server

Gold Nugget Web App

Score Board Web App

BOT

Public CTF ESXi

Mail Server

CTF DNS

NTP Server

DIR Server

Private CTF Services

iCINGA

puppet labs

TEAM GIT git

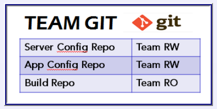
Server Config Repo	Team RW
App Config Repo	Team RW
Build Repo	Team RO

SETUP GIT git

Puppet Repo	Jury RW Team --

Fixing vulnerable apps

- Teams have access to the source code of the vulnerable apps



TEAM GIT git

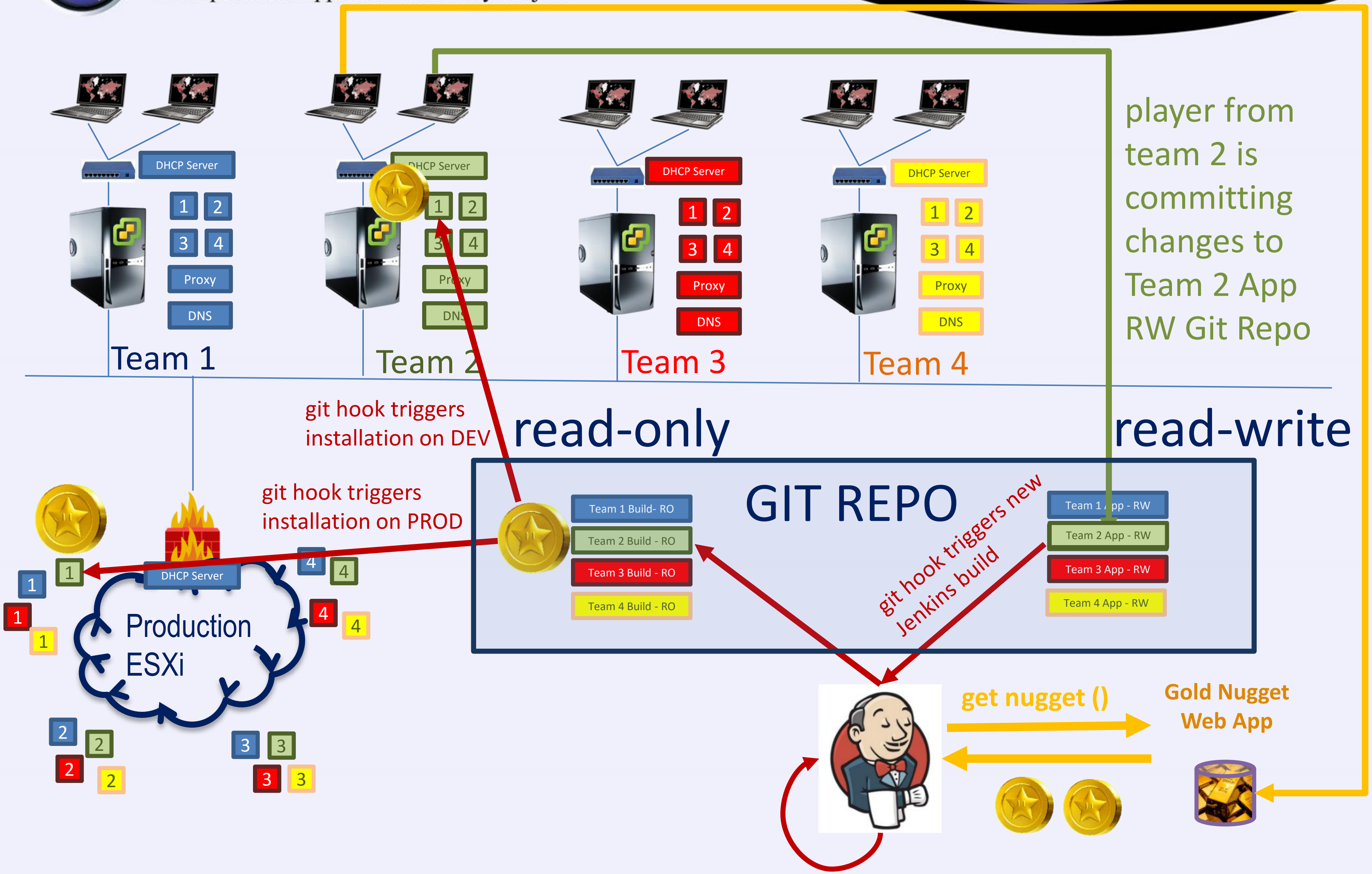
Server Config Repo	Team RW
App Config Repo	Team RW
Build Repo	Team RO

- Teams must fix the vulnerabilities and commit changes to the source code repository = GIT
- The Jenkins-based building infrastructure is building the new release of the app
- The Jenkins-based building infrastructure is packaging the current team's gold nugget into the new release
- The building infrastructure is automatically deploying the new app to **DEV** and **PROD**

Fixing vulnerable apps

OWASP
The Open Web Application Security Project

player is issueing a new gold nugget for App 01 of team 2



player from team 2 is committing changes to Team 2 App RW Git Repo

DHCP Server

1 2 3 4

Proxy

DNS

Team 1

Team 2

Team 3

Team 4

git hook triggers installation on DEV

git hook triggers installation on PROD

read-only

read-write

GIT REPO

Team 1 Build- RO

Team 2 Build - RO

Team 3 Build - RO

Team 4 Build - RO

Team 1 App - RW

Team 2 App - RW

Team 3 App - RW

Team 4 App - RW

git hook triggers new Jenkins build

Production ESXi

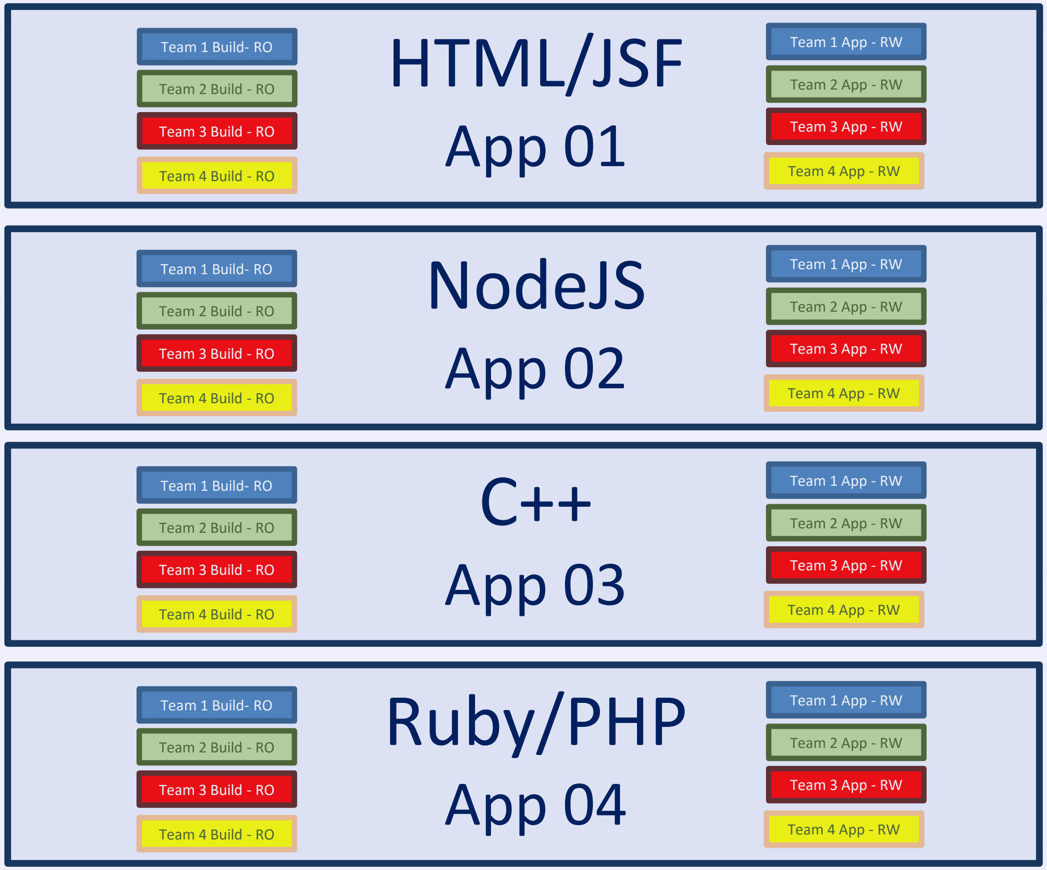
get nugget ()

Gold Nugget Web App

Fixing vulnerable apps

OWASP
The Open Web Application Security Project

read-only read-write



HTML/JSF
App 01

Team 1 Build- RO
Team 2 Build - RO
Team 3 Build - RO
Team 4 Build - RO

Team 1 App - RW
Team 2 App - RW
Team 3 App - RW
Team 4 App - RW

NodeJS
App 02

Team 1 Build- RO
Team 2 Build - RO
Team 3 Build - RO
Team 4 Build - RO

Team 1 App - RW
Team 2 App - RW
Team 3 App - RW
Team 4 App - RW

C++
App 03

Team 1 Build- RO
Team 2 Build - RO
Team 3 Build - RO
Team 4 Build - RO

Team 1 App - RW
Team 2 App - RW
Team 3 App - RW
Team 4 App - RW

Ruby/PHP
App 04

Team 1 Build- RO
Team 2 Build - RO
Team 3 Build - RO
Team 4 Build - RO

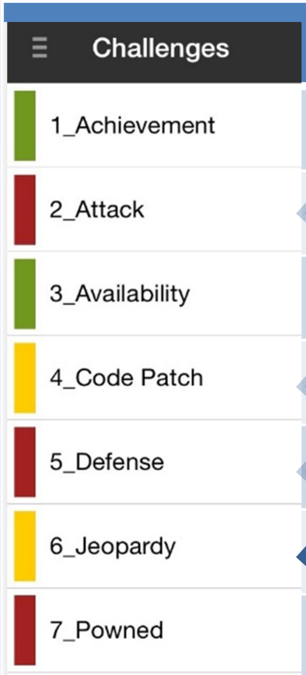
Team 1 App - RW
Team 2 App - RW
Team 3 App - RW
Team 4 App - RW

During the CTF, teams must attack and defend the vulnerable apps

On **DEV** , teams could apply infrastructure mitigations (mod_security, iptables, WAF, …)

On **PROD**, teams must fix the source code in order to make the app secure!! That's why teams do not have ssh or root access on **PROD**

Jeopardy Challenges

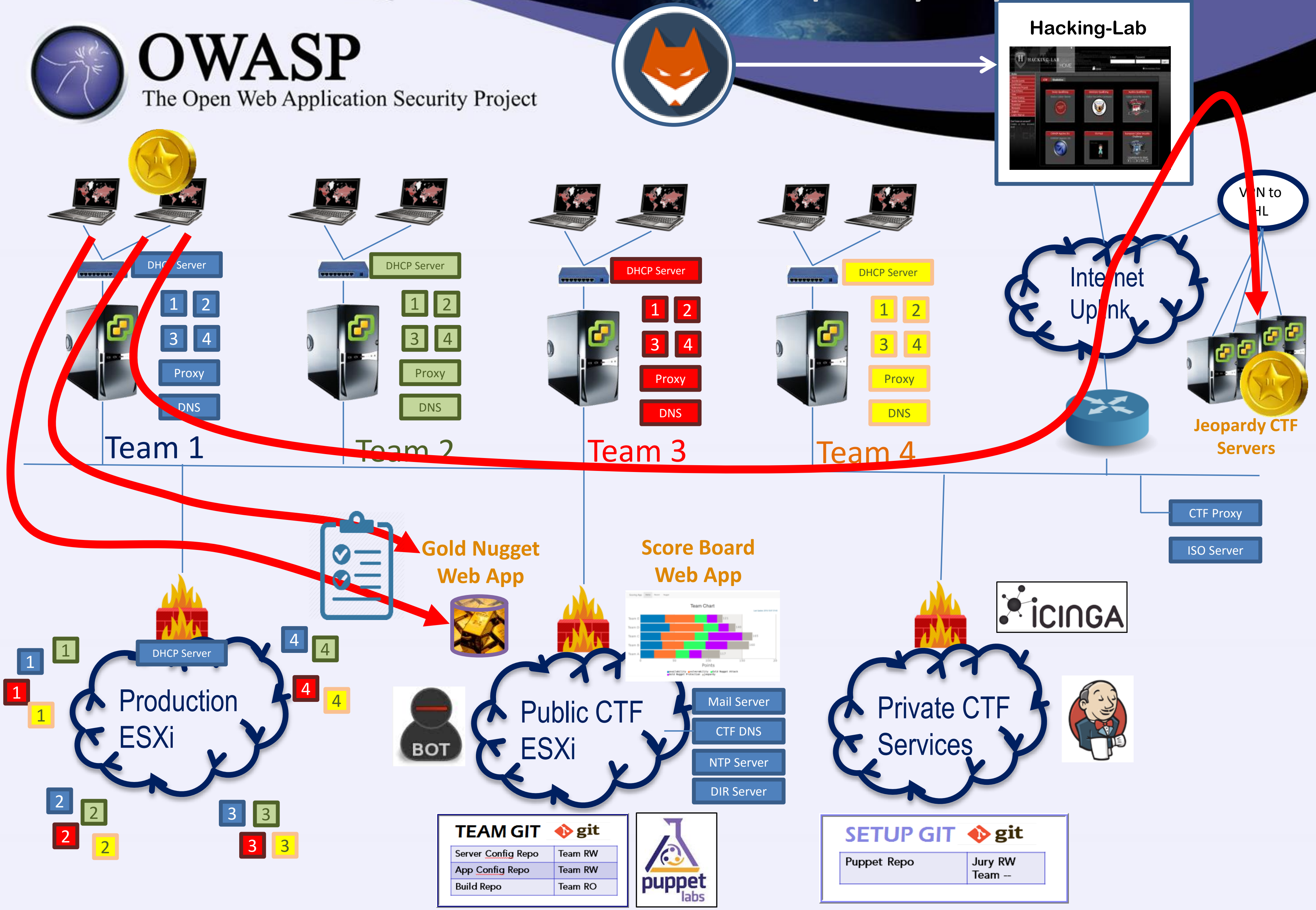


☰ Challenges	
🟩 1_Achievement	
🟥 2_Attack	Stealing Gold Nugget
🟩 3_Availability	
🟨 4_Code Patch	Fix vulnerable software & services
🟥 5_Defense	Safe guard own gold nuggets
🟨 6_Jeopardy	Solving jeopardy challenges
🟥 7_Powned	

Jeopardy-style CTF

- Jeopardy-style CTFs have a couple of tasks in range of categories. For example, Web, Reverse Engineering, Crypto, Binary, Forensics, …
- Gold Nugget app is introducing the task (mission)
- Teams gain points for every solved task
- More points for more complicated tasks
- Teams are not fighting against each others
- The earlier a team solves the challenge, the more points they get

Jeopardy-style CTF



TEAM GIT git

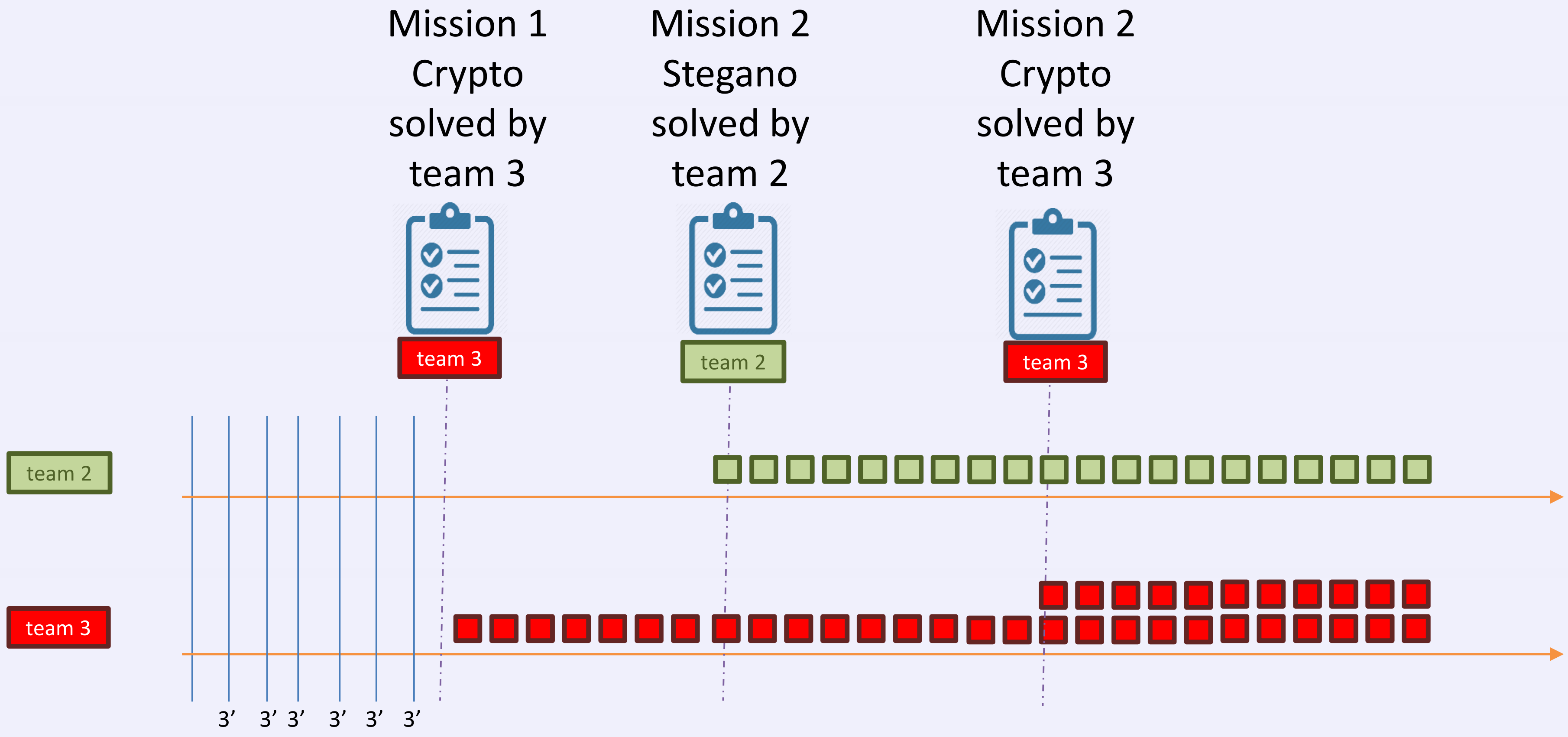
Server Config Repo	Team RW
App Config Repo	Team RW
Build Repo	Team RO

SETUP GIT git

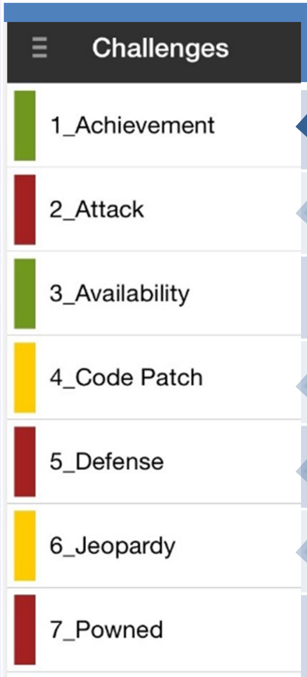
Puppet Repo	Jury RW Team --

Scoring per Time Unit

OWASP
The Open Web Application Security Project



Achievements



Challenges	
🟩 1_Achievement	Setup and maintain a service
🟥 2_Attack	Stealing Gold Nugget
🟩 3_Availability	
🟨 4_Code Patch	Fix vulnerable software & services
🟥 5_Defense	Safe guard own gold nuggets
🟨 6_Jeopardy	Solving jeopardy challenges
🟥 7_Powned	

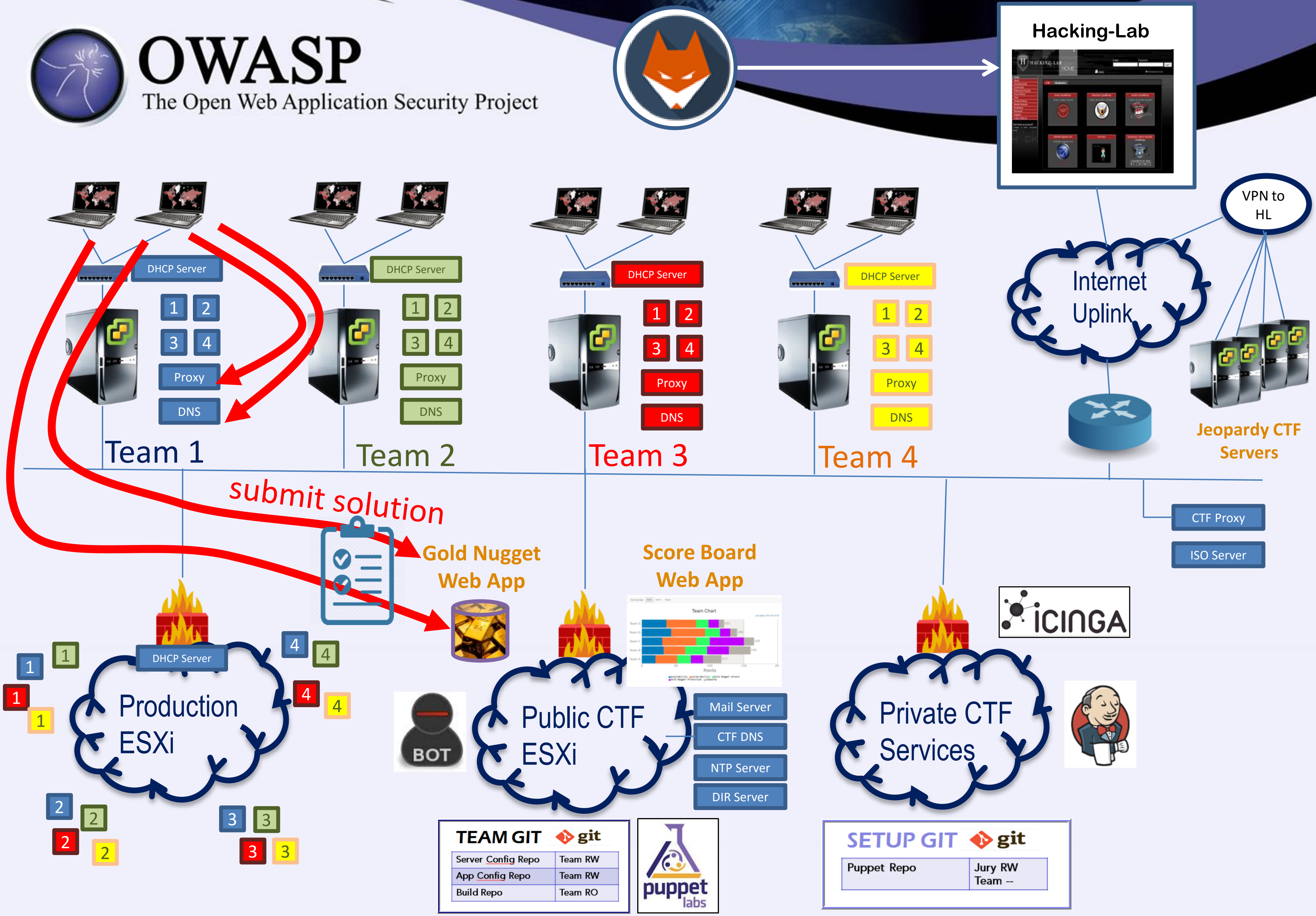
Achievements

OWASP
The Open Web Application Security Project

- Technical Achievements
  - Teams must setup and maintain services
  - DNS, Proxy, Apache, NodeJS, AngularJS, …
- Non-Technical Achievements (Management)
  - Write press release
  - Announce news
  - Create crisis organization during CTF game
  - Presentation / Talk

Achievements

OWASP
The Open Web Application Security Project



Hacking-Lab

VPN to HL

Internet Uplink

Jeopardy CTF Servers

CTF Proxy

ISO Server

Team 1: DHCP Server, 1, 2, 3, 4, Proxy, DNS

Team 2: DHCP Server, 1, 2, 3, 4, Proxy, DNS

Team 3: DHCP Server, 1, 2, 3, 4, Proxy, DNS

Team 4: DHCP Server, 1, 2, 3, 4, Proxy, DNS

submit solution

Gold Nugget Web App

Score Board Web App

ICINGA

Production ESXi

DHCP Server

BOT

Public CTF ESXi

Mail Server

CTF DNS

NTP Server

DIR Server

Private CTF Services

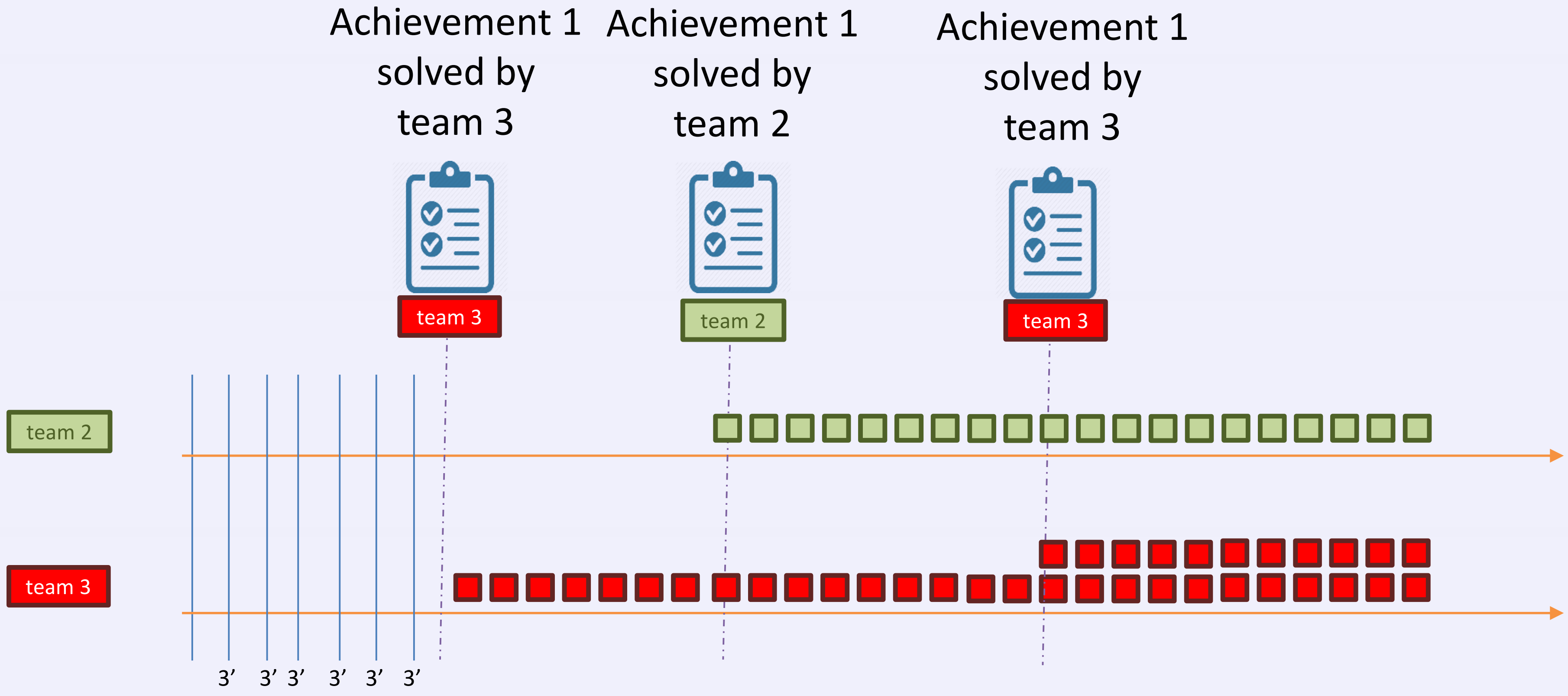
TEAM GIT git	
Server Config Repo	Team RW
App Config Repo	Team RW
Build Repo	Team RO

puppet labs

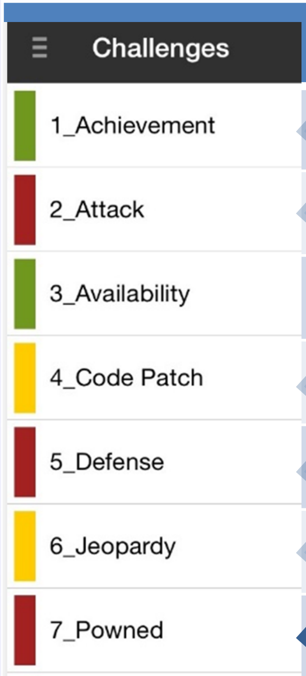
SETUP GIT git	
Puppet Repo	Jury RW Team --

Scoring per Time Unit

OWASP
The Open Web Application Security Project


Achievement 1 solved by team 3
Achievement 1 solved by team 2
Achievement 1 solved by team 3
team 3
team 2
team 3
team 2
team 3
3’
3’
3’
3’
3’
3’

Pown’ed



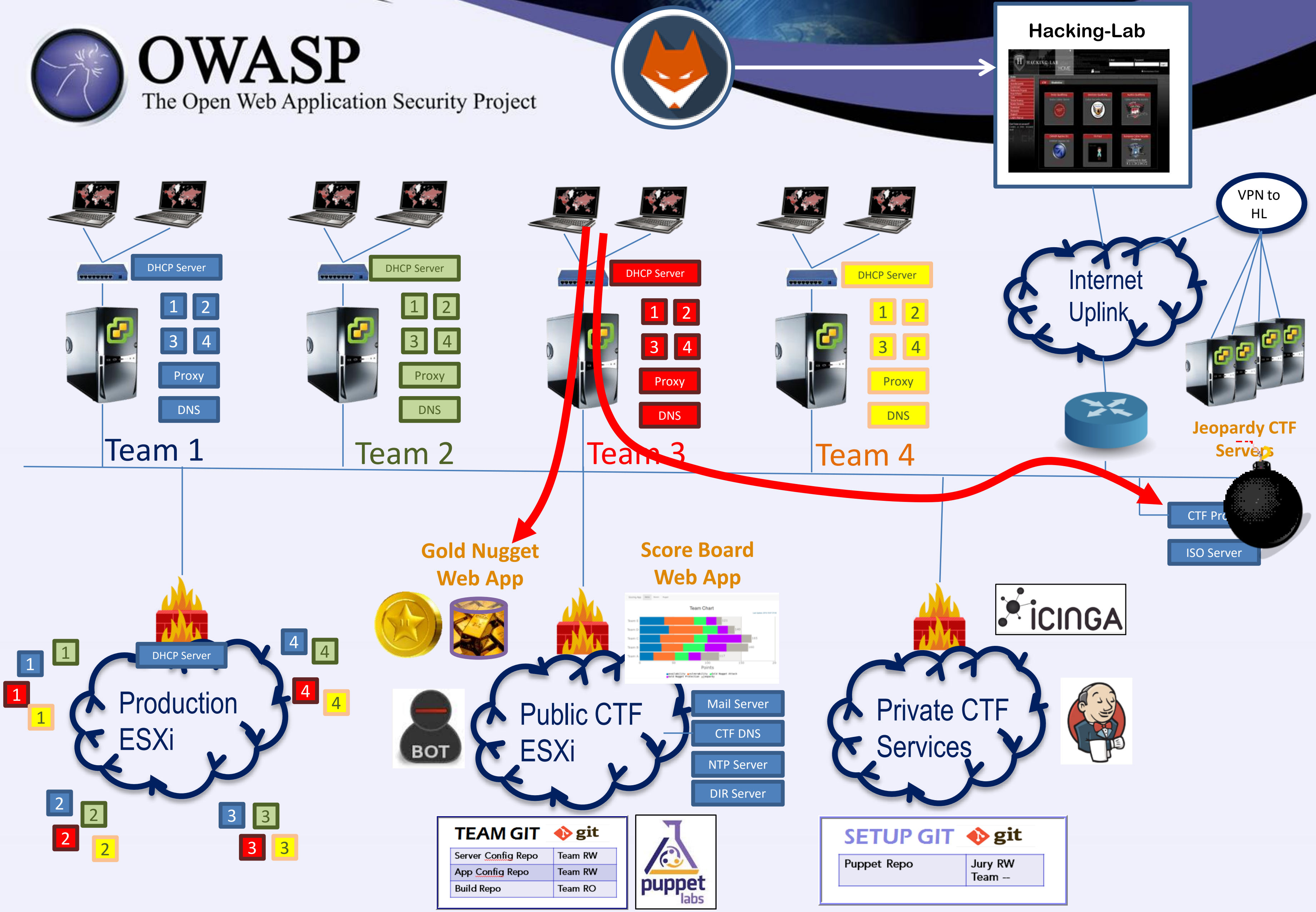
☰ Challenges	
🟩 1_Achievement	Setup and maintain a service
🟥 2_Attack	Stealing Gold Nugget
🟩 3_Availability	
🟨 4_Code Patch	Fix vulnerable software & services
🟥 5_Defense	Safe guard own gold nuggets
🟨 6_Jeopardy	Solving jeopardy challenges
🟥 7_Powned	Own a device/server

Pown’ed

- Teams may find vulnerabilities that are not known to the CTF jury
- If a team could hack such a service, then the team could get a special gold nugget and leave it on the hacked server as ‘evidence’
- This special gold nugget is defined as the “evidence gold nugget”
- Teams can request such an evidence gold nugget from the gold nugget app, but only one at a time until it’s being verified by the jury

Pown'ed

OWASP
The Open Web Application Security Project



TEAM GIT git

Server Config Repo	Team RW
App Config Repo	Team RW
Build Repo	Team RO

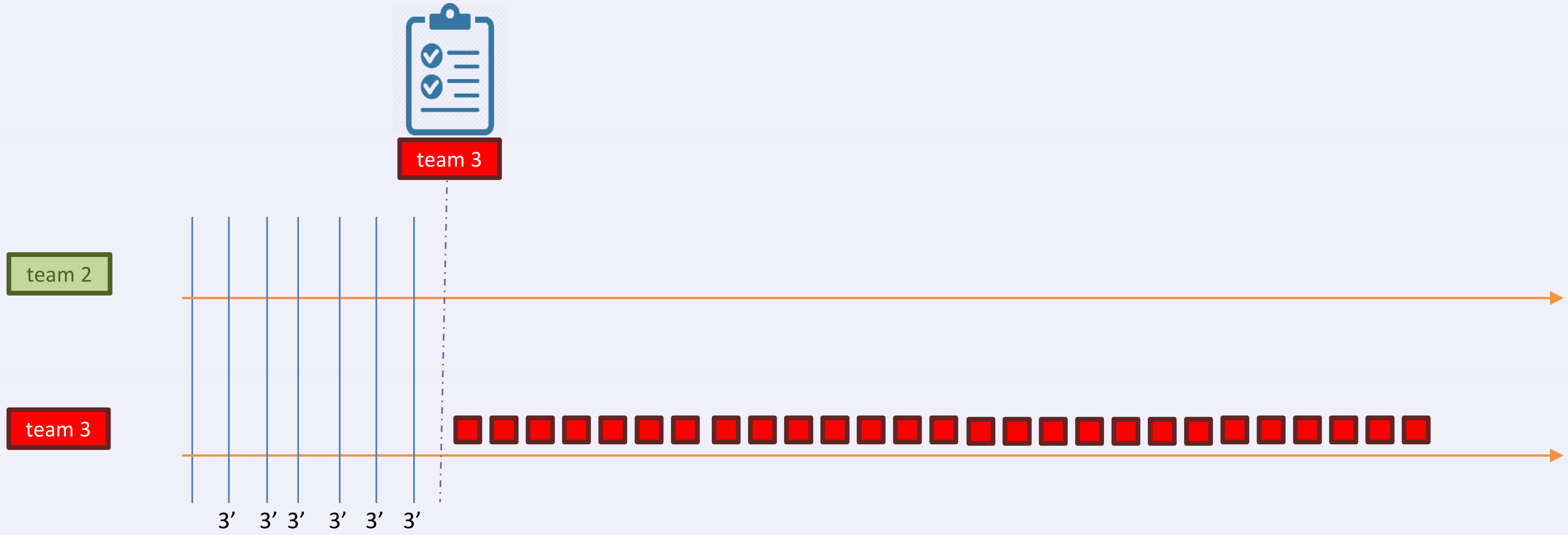
SETUP GIT git

Puppet Repo	Jury RW Team --

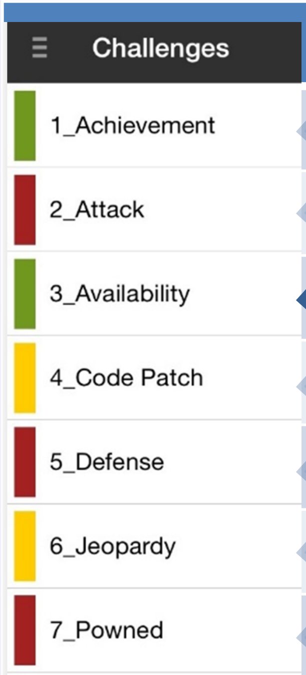
Scoring per Time Unit

OWASP
The Open Web Application Security Project

team 3 found a 0-day
exploit and left
an evidence nugget
on the server



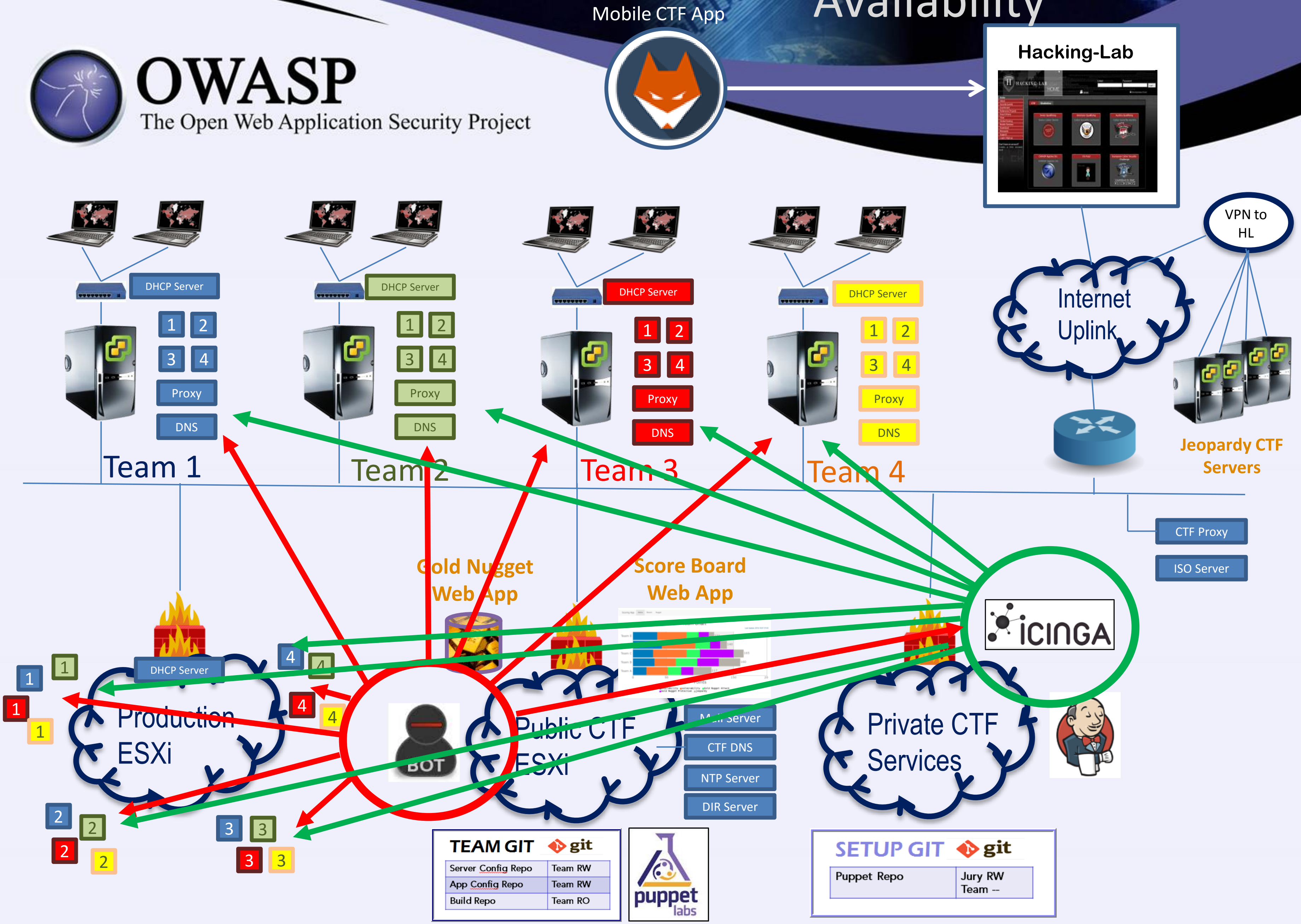
Availability



Challenges	
🟩 1_Achievement	Setup and maintain a service
🟥 2_Attack	Stealing Gold Nugget
🟩 3_Availability	**Keep own services up and running**
🟨 4_Code Patch	Fix vulnerable software & services
🟥 5_Defense	Safe guard own gold nuggets
🟨 6_Jeopardy	Solving jeopardy challenges
🟥 7_Powned	Own a device/server

Availability

OWASP
The Open Web Application Security Project



TEAM GIT git

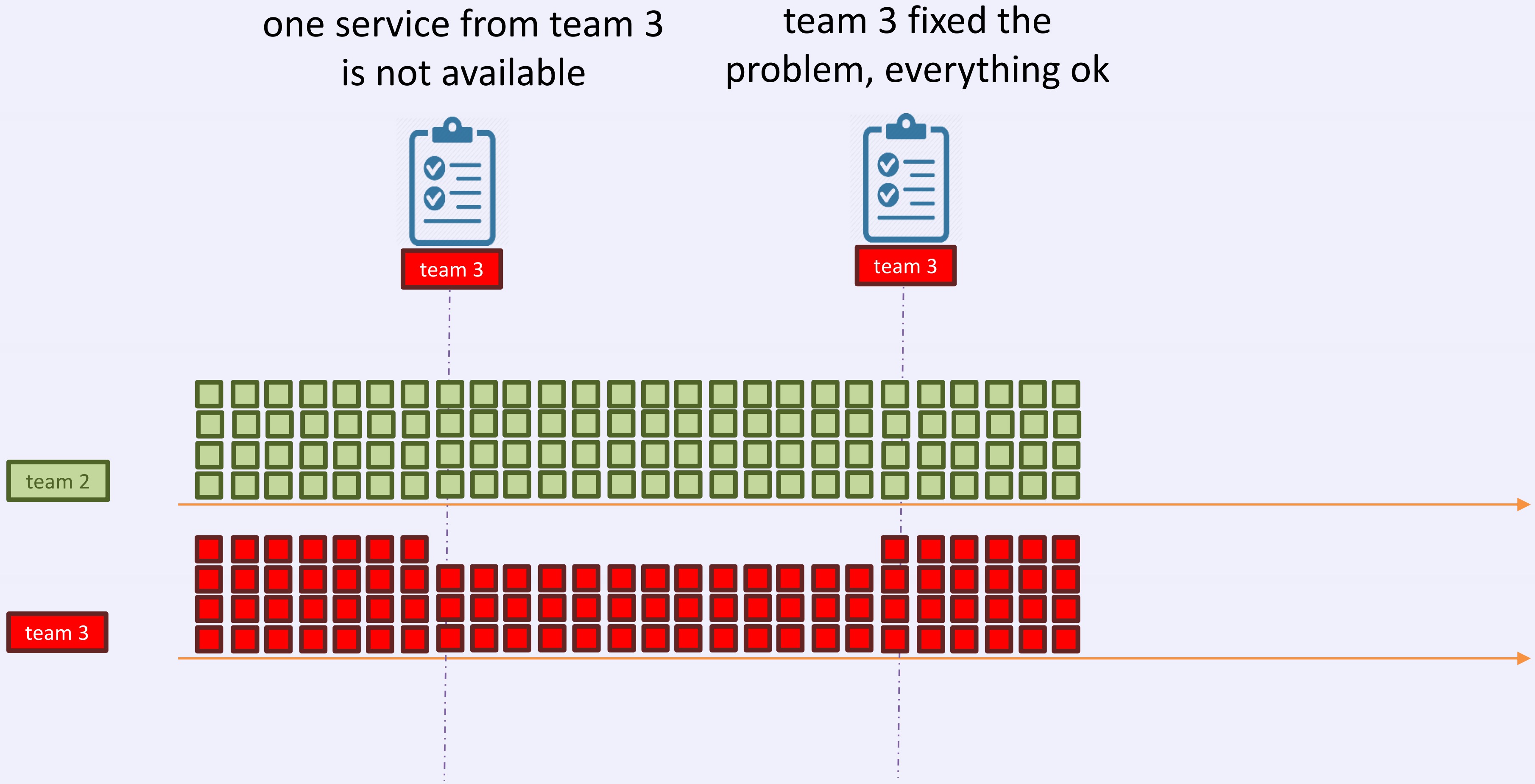
Server Config Repo	Team RW
App Config Repo	Team RW
Build Repo	Team RO

SETUP GIT git

Puppet Repo	Jury RW Team --

Scoring per Time Unit

OWASP
The Open Web Application Security Project



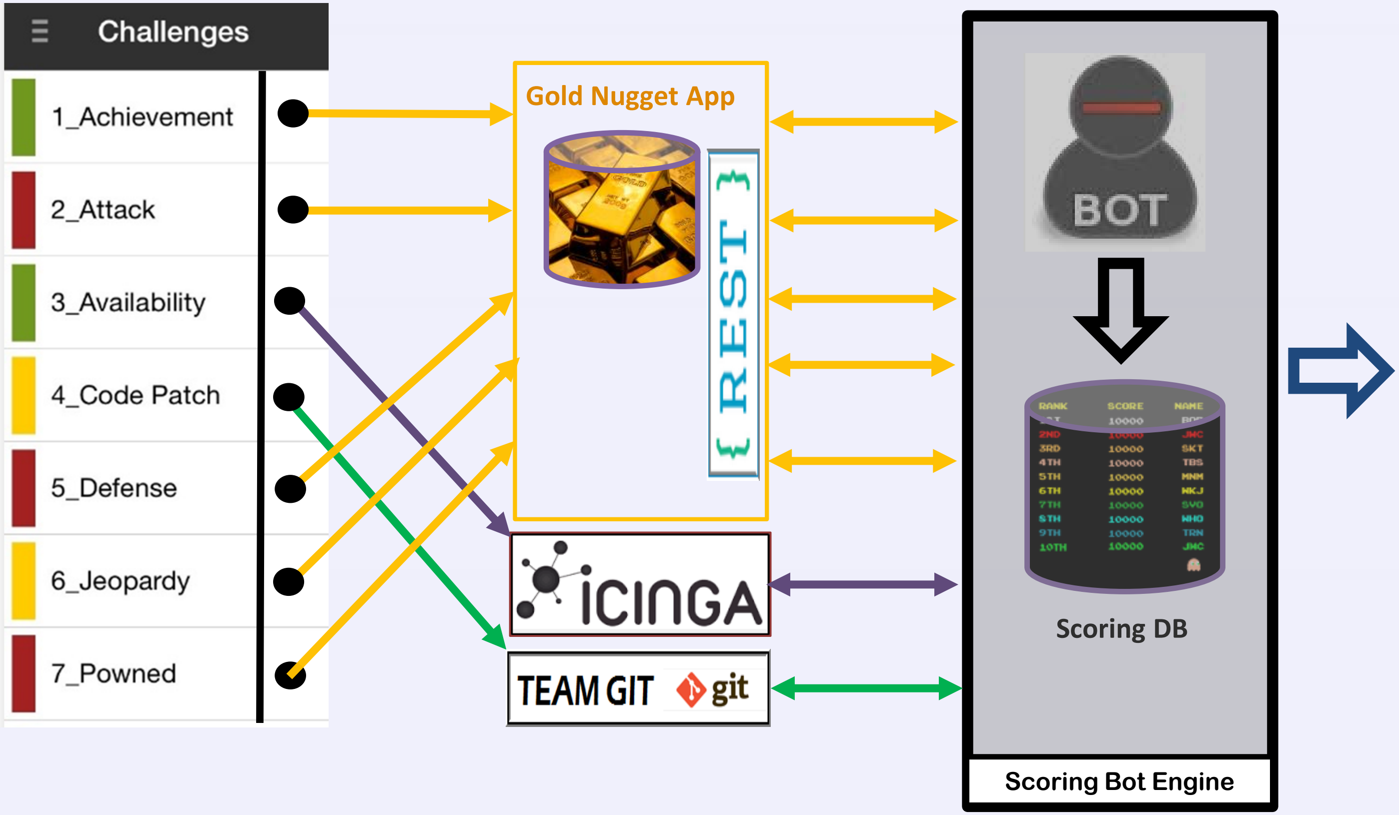
one service from team 3 is not available

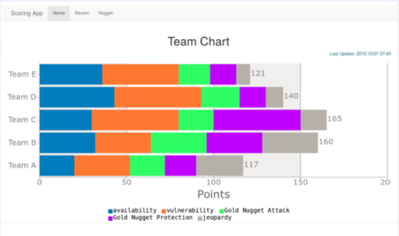
team 3 fixed the problem, everything ok

CTF Scoring

CTF Scoring

OWASP
The Open Web Application Security Project





ECSC Award Ceremony 2015

Thank You!

Open Question

- World-Championship?
- CTF in China ?

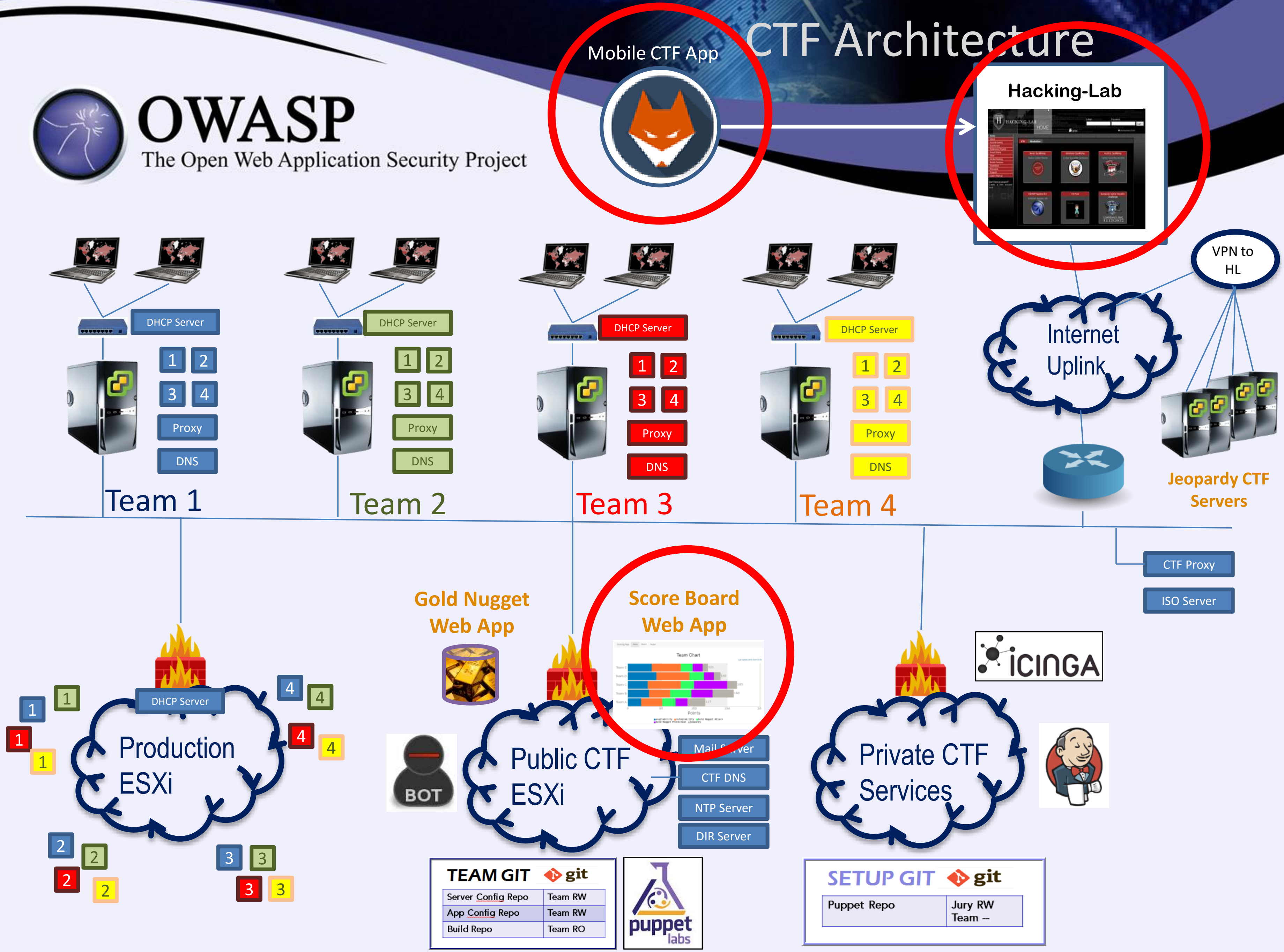
Appendix A

CTF Mobile App

(available and used in ECSC 2015)

CTF Architecture

OWASP
The Open Web Application Security Project



TEAM GIT

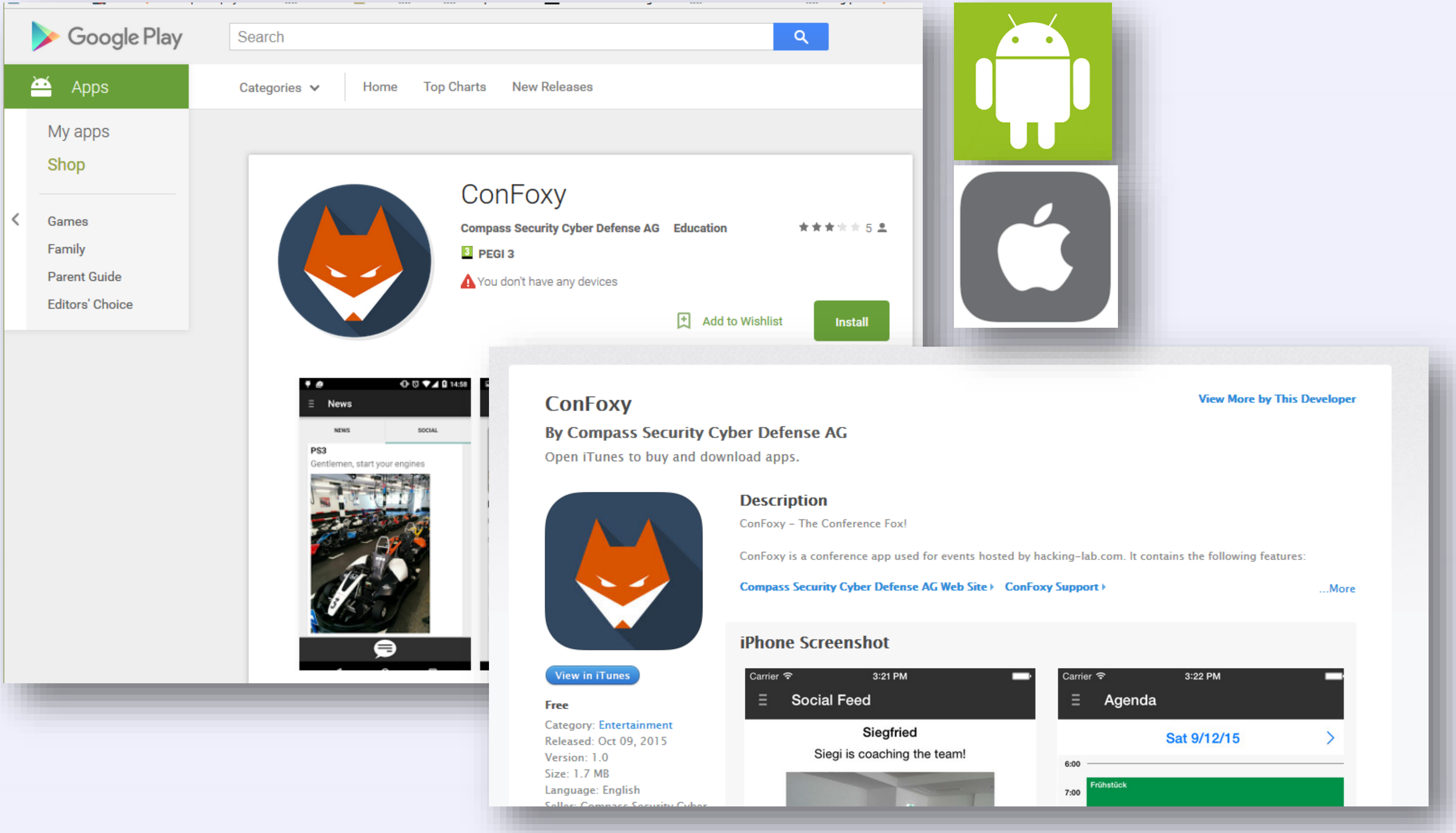
Server Config Repo	Team RW
App Config Repo	Team RW
Build Repo	Team RO

SETUP GIT

Puppet Repo	Jury RW Team --

Confoxy CTF Mobile App

OWASP
The Open Web Application Security Project



Google Play

Search

Apps

Categories

Home

Top Charts

New Releases

My apps

Shop

Games

Family

Parent Guide

Editors' Choice

ConFoxy

Compass Security Cyber Defense AG Education

★★★☆☆ 5

PEGI 3

You don't have any devices

Add to Wishlist

Install

News

NEWS SOCIAL

PS3

Gentlemen, start your engines

ConFoxy

View More by This Developer

By Compass Security Cyber Defense AG

Open iTunes to buy and download apps.

Description

ConFoxy – The Conference Fox!

ConFoxy is a conference app used for events hosted by hacking-lab.com. It contains the following features:

Compass Security Cyber Defense AG Web Site › ConFoxy Support ›

...More

View in iTunes

Free

Category: Entertainment

Released: Oct 09, 2015

Version: 1.0

Size: 1.7 MB

Language: English

Seller: Compass Security Cyber

iPhone Screenshot

Carrier 3:21 PM

Social Feed

Siegfried

Siegi is coaching the team!

Carrier 3:22 PM

Agenda

Sat 9/12/15

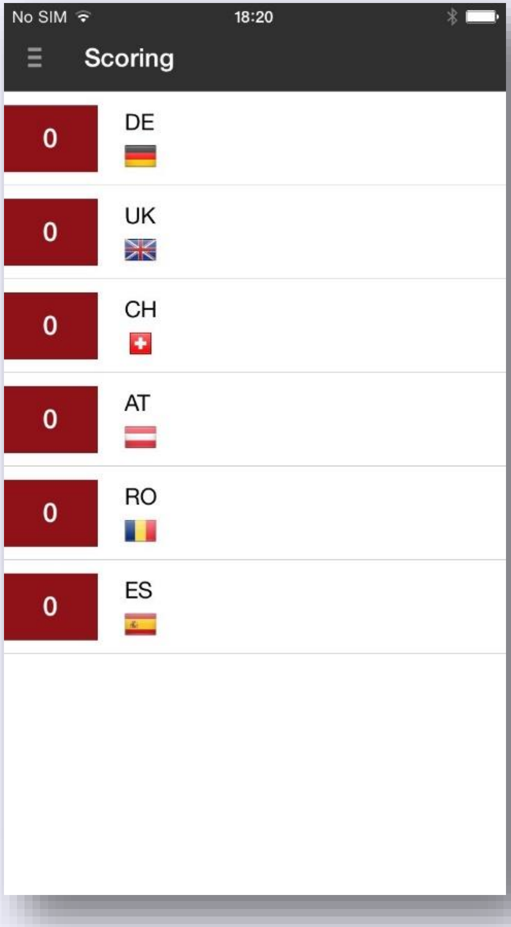
6:00

7:00

Frühstück

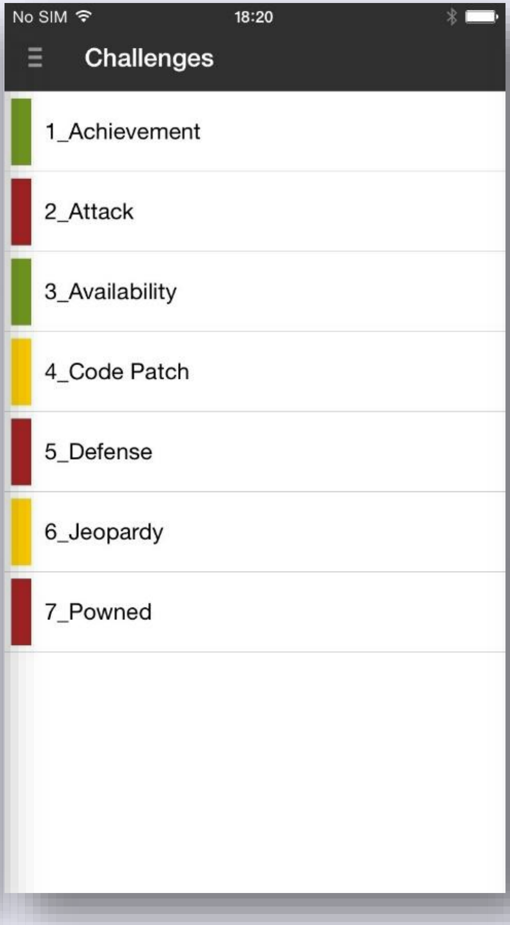
Confoxy CTF Mobile App

- CTF Mobile App



Scoring

0	DE
0	UK
0	CH
0	AT
0	RO
0	ES



Challenges

1_Achievement

2_Attack

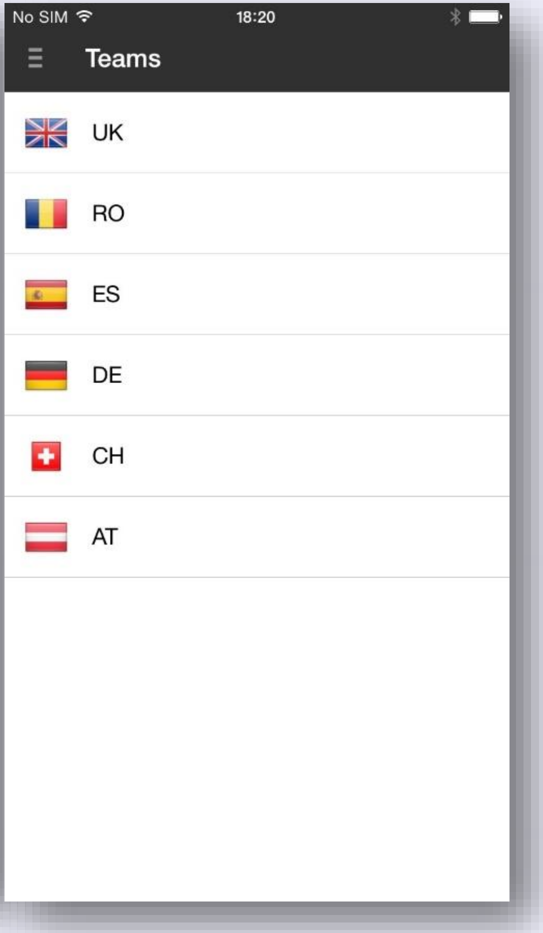
3_Availability

4_Code Patch

5_Defense

6_Jeopardy

7_Powned



Teams

UK

RO

ES

DE

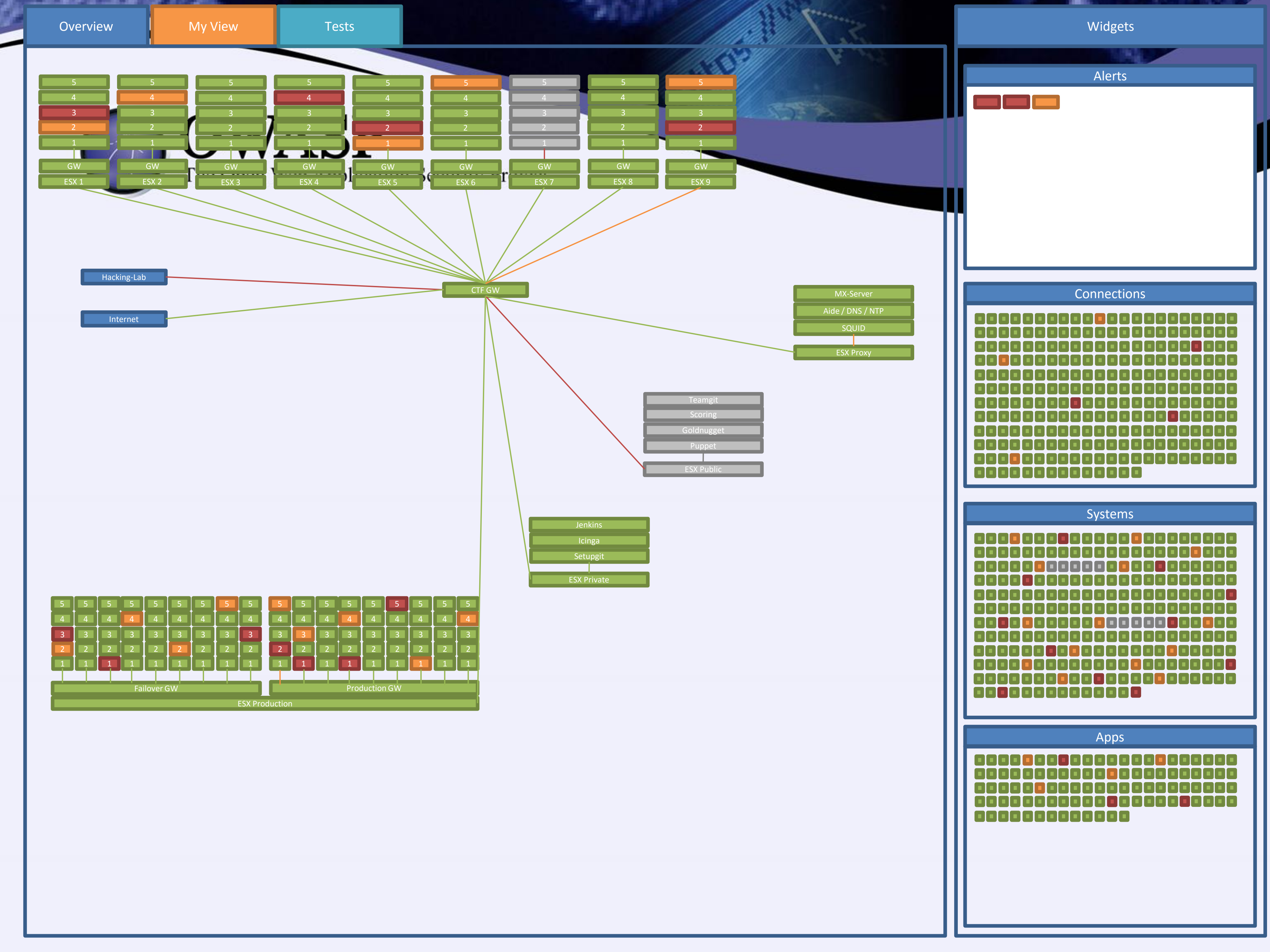
CH

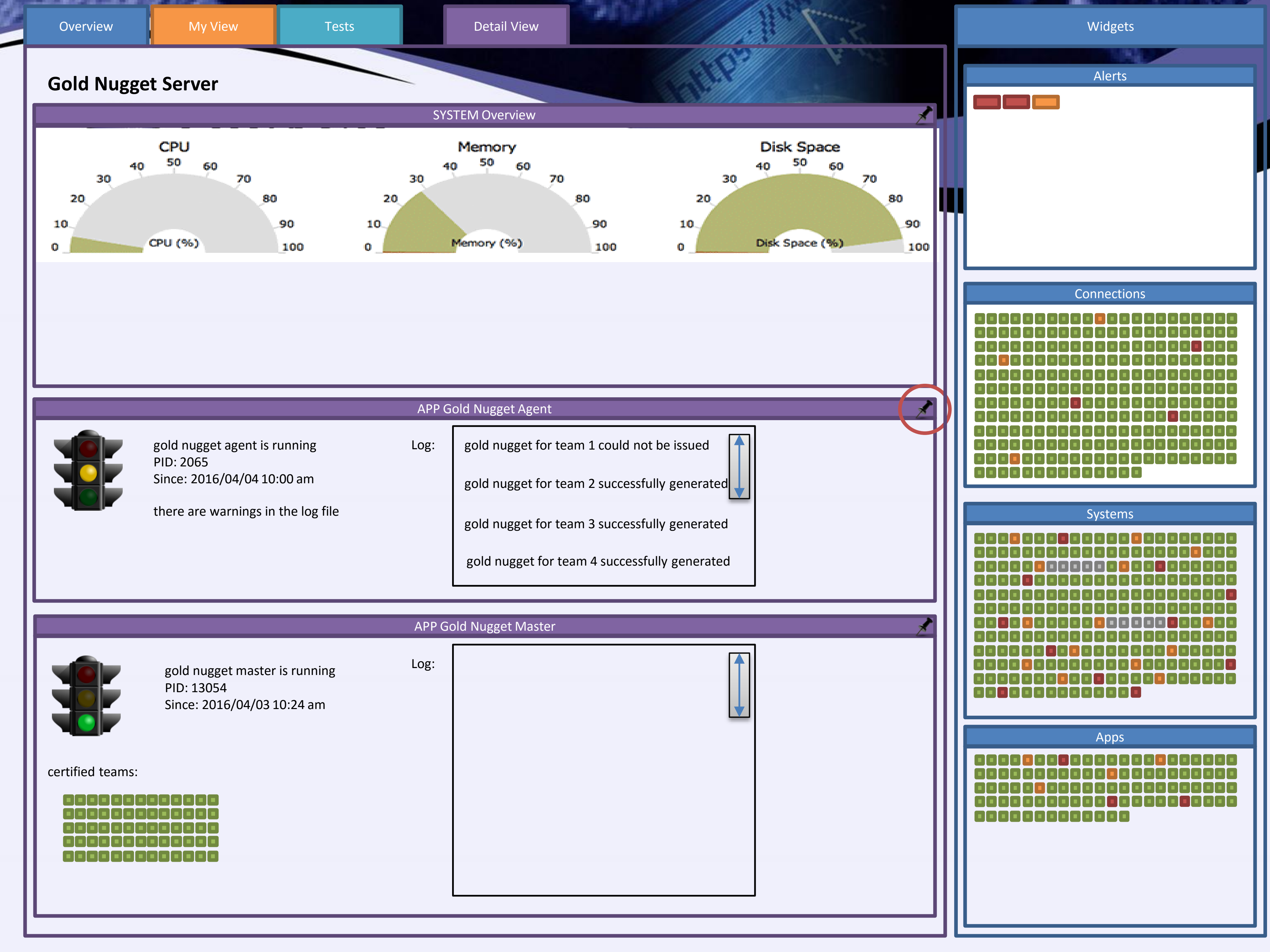
AT

Appendix B

CTF Cockpit

(not available yet)


Overview
My View
Tests
Widgets
Alerts
Connections
Systems
Apps
5
4
3
2
1
GW
ESX 1
ESX 2
ESX 3
ESX 4
ESX 5
ESX 6
ESX 7
ESX 8
ESX 9
Hacking-Lab
Internet
CTF GW
MX-Server
Aide / DNS / NTP
SQUID
ESX Proxy
Teamgit
Scoring
Goldnugget
Puppet
ESX Public
Jenkins
Icinga
Setupgit
ESX Private
Failover GW
Production GW
ESX Production



Gold Nugget Server

APP Gold Nugget Agent

gold nugget agent is running
PID: 2065
Since: 2016/04/04 10:00 am

there are warnings in the log file

Log:

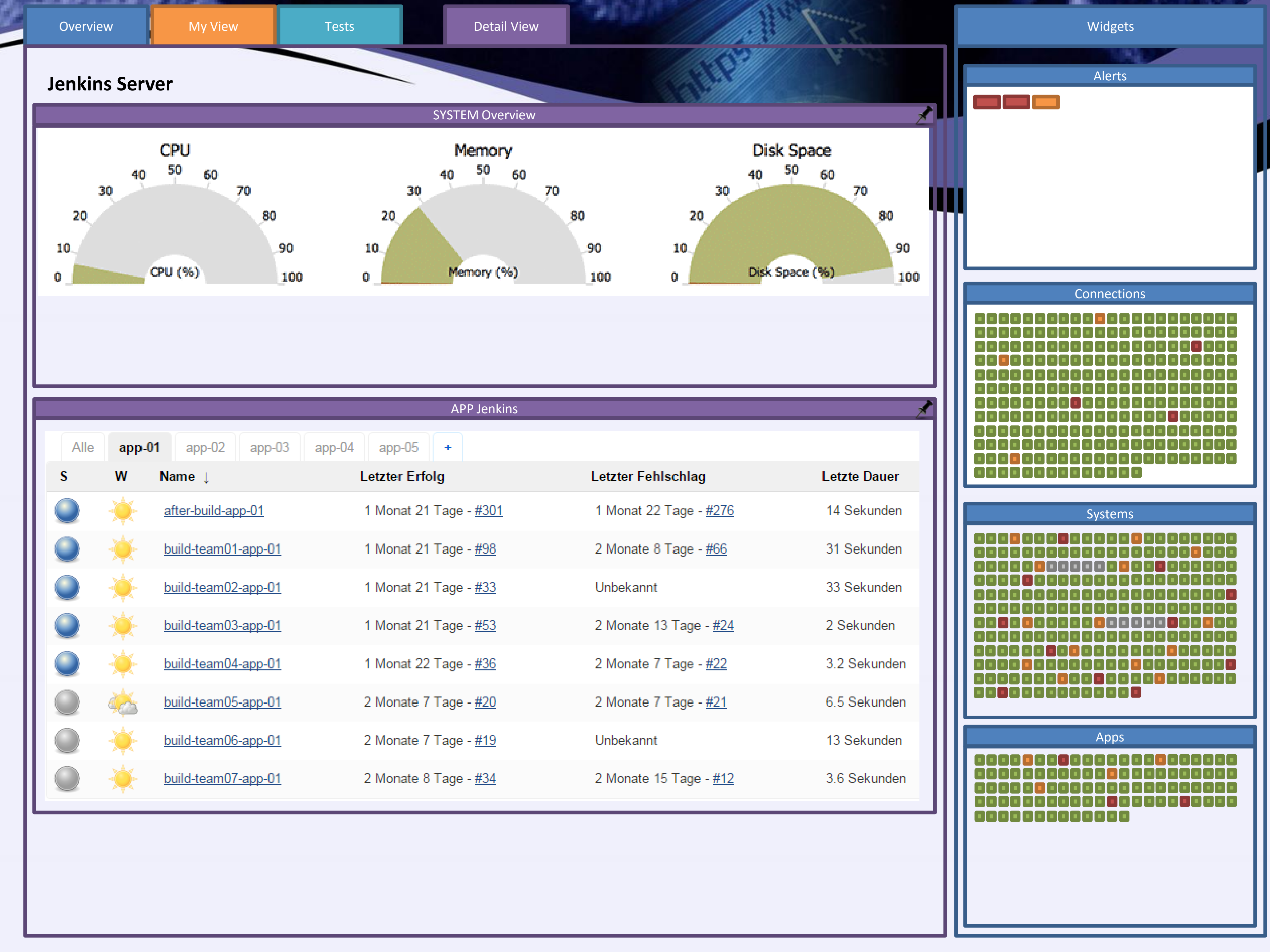
```
gold nugget for team 1 could not be issued

gold nugget for team 2 successfully generated

gold nugget for team 3 successfully generated

gold nugget for team 4 successfully generated
```

APP Gold Nugget Master

gold nugget master is running
PID: 13054
Since: 2016/04/03 10:24 am

certified teams:

Log:



Jenkins Server

SYSTEM Overview

APP Jenkins

S	W	Name ↓	Letzter Erfolg	Letzter Fehlschlag	Letzte Dauer
●	☀	after-build-app-01	1 Monat 21 Tage - #301	1 Monat 22 Tage - #276	14 Sekunden
●	☀	build-team01-app-01	1 Monat 21 Tage - #98	2 Monate 8 Tage - #66	31 Sekunden
●	☀	build-team02-app-01	1 Monat 21 Tage - #33	Unbekannt	33 Sekunden
●	☀	build-team03-app-01	1 Monat 21 Tage - #53	2 Monate 13 Tage - #24	2 Sekunden
●	☀	build-team04-app-01	1 Monat 22 Tage - #36	2 Monate 7 Tage - #22	3.2 Sekunden
○	⛅	build-team05-app-01	2 Monate 7 Tage - #20	2 Monate 7 Tage - #21	6.5 Sekunden
○	☀	build-team06-app-01	2 Monate 7 Tage - #19	Unbekannt	13 Sekunden
○	☀	build-team07-app-01	2 Monate 8 Tage - #34	2 Monate 15 Tage - #12	3.6 Sekunden