Security Community Kickoff

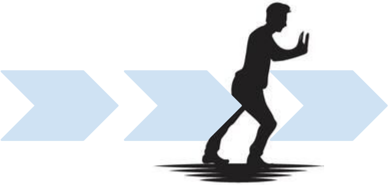
Developing Systems Security Know-how

Miloš Karas, Climber and Professional Test Engineer

Security Community Proposal

What is the Motivation?

People



Fintechs

6th in the world in number of Fintechs

Barcelona and **Madrid** hosts most of Fintechs

Valencia · Sevilla · Málaga · Bilbao

IoT Security

By 2010 **25%** of enterprise attacks will involve IoT

10% of IT security budget allocated to IoT

Current Mandates

Roche · hp · others … ?

[1] OBSERVATORIO FINTECH 2018
http://www.finnovating.com/report/observatorio-fintech-2018/

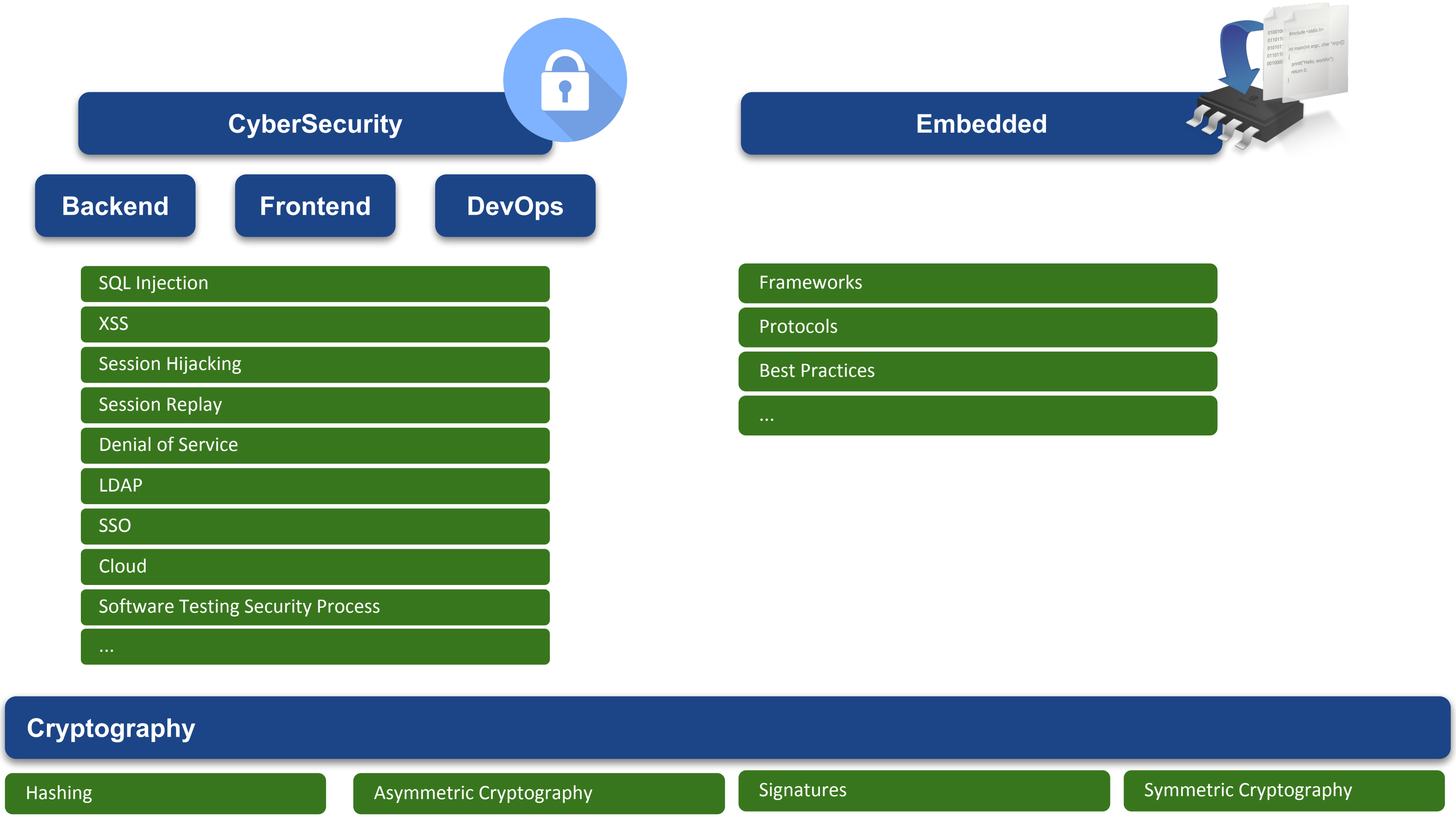
[2] Fintech Inovacion al Servicio del Cliente
https://assets.kpmg.com/content/dam/kpmg/es/pdf/2017/11/fintech-innovacion-servicio-cliente.pdf

[3] Payments Trends
https://www.capgemini.com/wp-content/uploads/2017/12/payments-trends_2018.pdf

[4] DDoS Attack: A Wake-Up Call for IoT
https://datafloq.com/read/ddos-attack-a-wake-up-call-for-iot/2480

Security Community Proposal

Community Pillars



CyberSecurity

- Backend
- Frontend
- DevOps

- SQL Injection
- XSS
- Session Hijacking
- Session Replay
- Denial of Service
- LDAP
- SSO
- Cloud
- Software Testing Security Process
- ...

Embedded

- Frameworks
- Protocols
- Best Practices
- ...

Cryptography

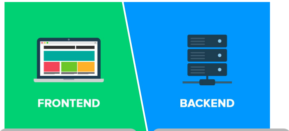
- Hashing
- Asymmetric Cryptography
- Signatures
- Symmetric Cryptography

Security Community Proposal

Transversal community composed of SME from other communities

Embedded

- Frameworks
- Protocols
- Best Practices



Frontend

.NET

- SQL Injections
- XSS
- Session Hijacking
- Session Replay
- Denial of Service
- ...

Devops

- LDAP
- SSO
- Cloud

QA

- Software Testing Security Process
- The Penetration Testing Process

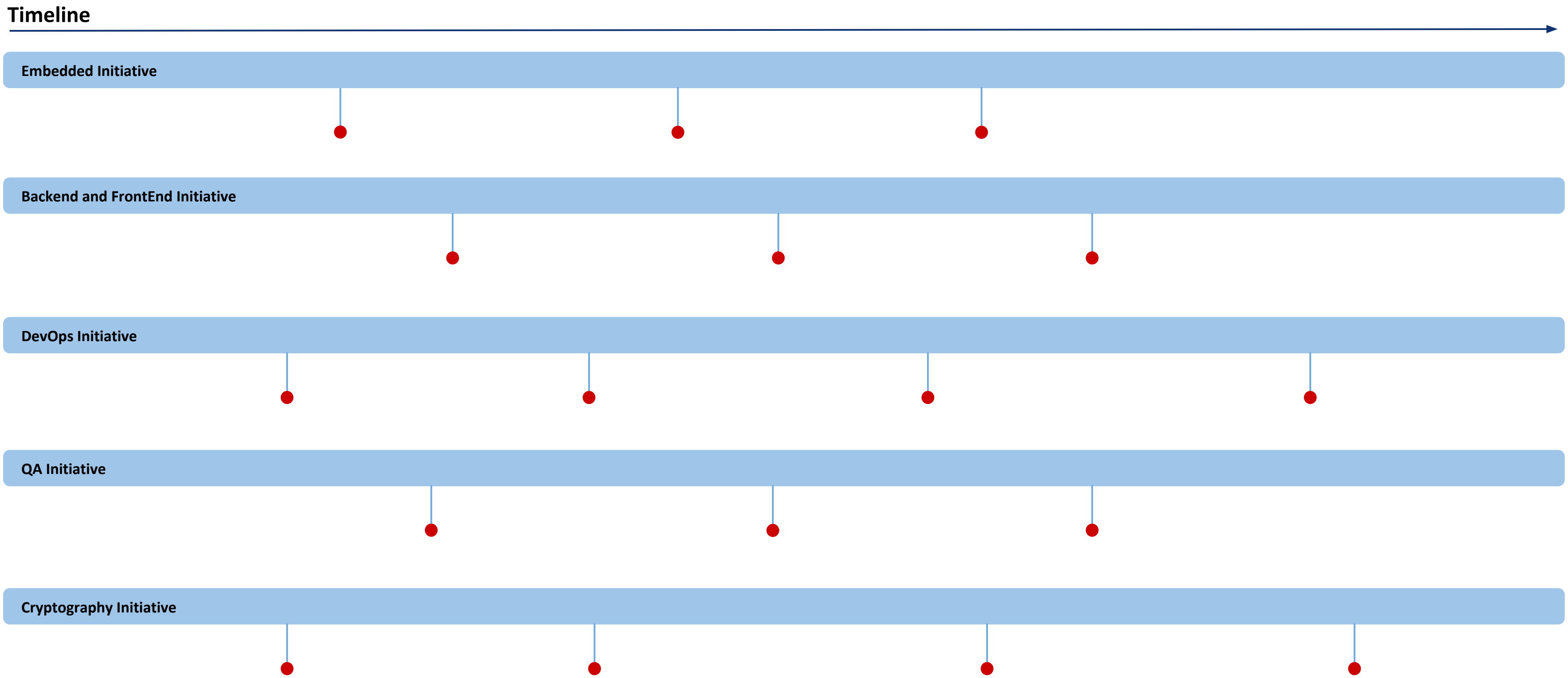
Cryptography

- Hashing
- Symmetric Cryptography
- Asymmetric Cryptography
- Signatures
- Transversal

Community Sessions

Projects Timeline Example and Community Sessions

● **New Community Session**



Timeline

Embedded Initiative

Backend and FrontEnd Initiative

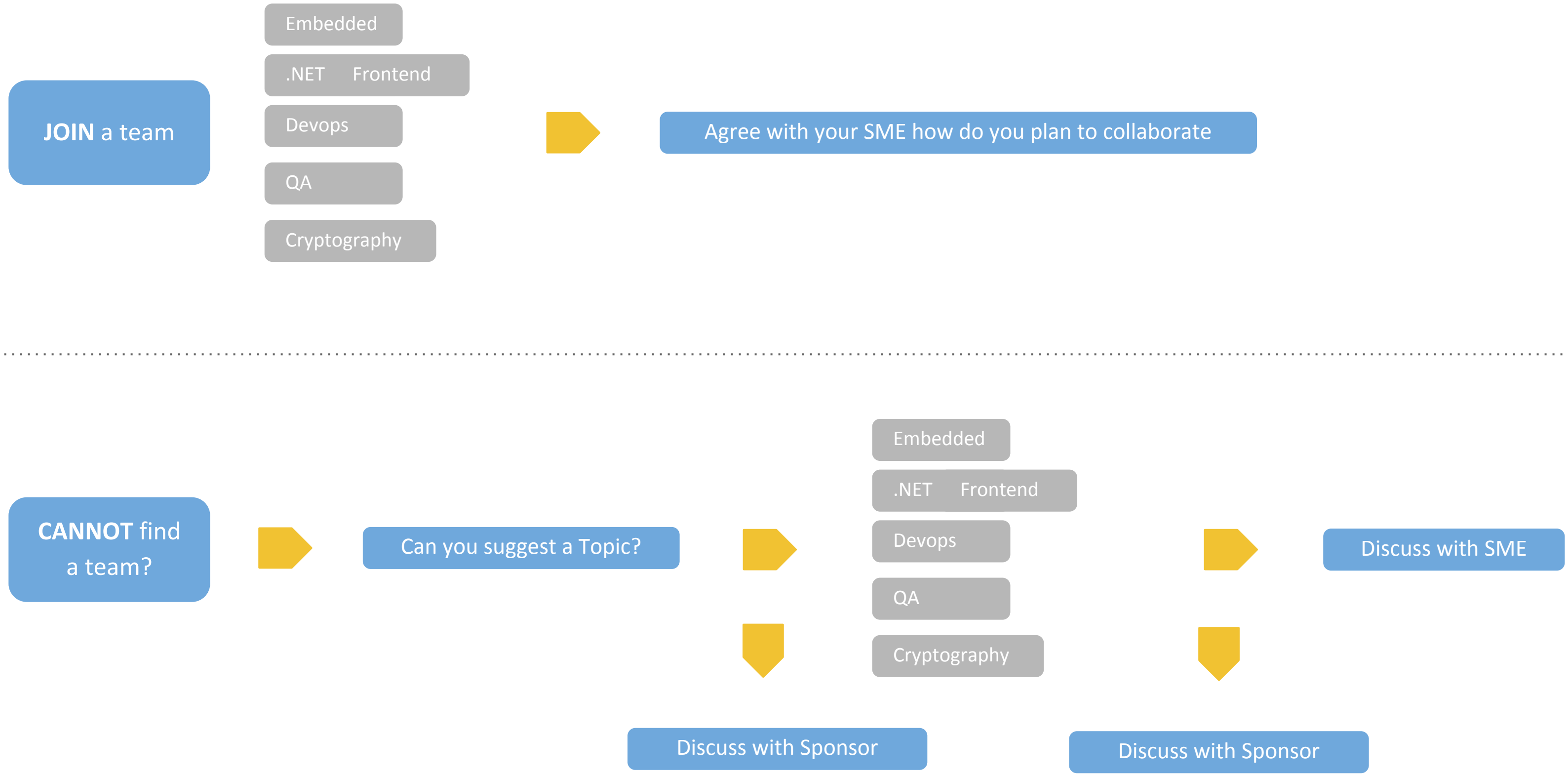
DevOps Initiative

QA Initiative

Cryptography Initiative

How to Get Involved?

Join or Suggest a Project



JOIN a team

Embedded

.NET Frontend

Devops

QA

Cryptography

Agree with your SME how do you plan to collaborate

CANNOT find a team?

Can you suggest a Topic?

Embedded

.NET Frontend

Devops

QA

Cryptography

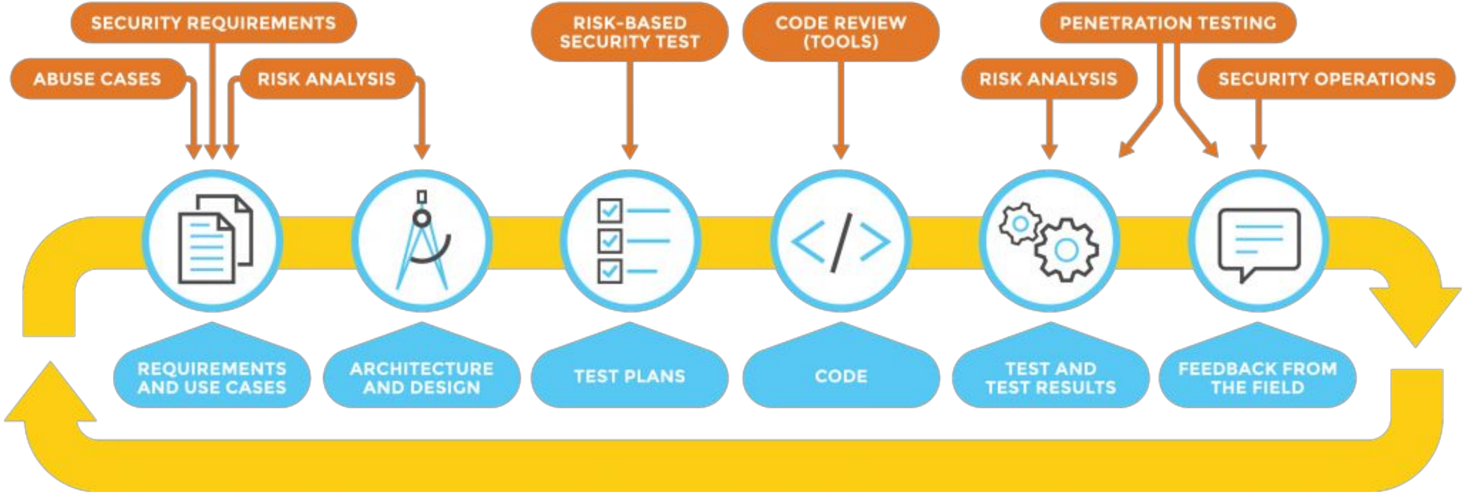
Discuss with SME

Discuss with Sponsor

Discuss with Sponsor

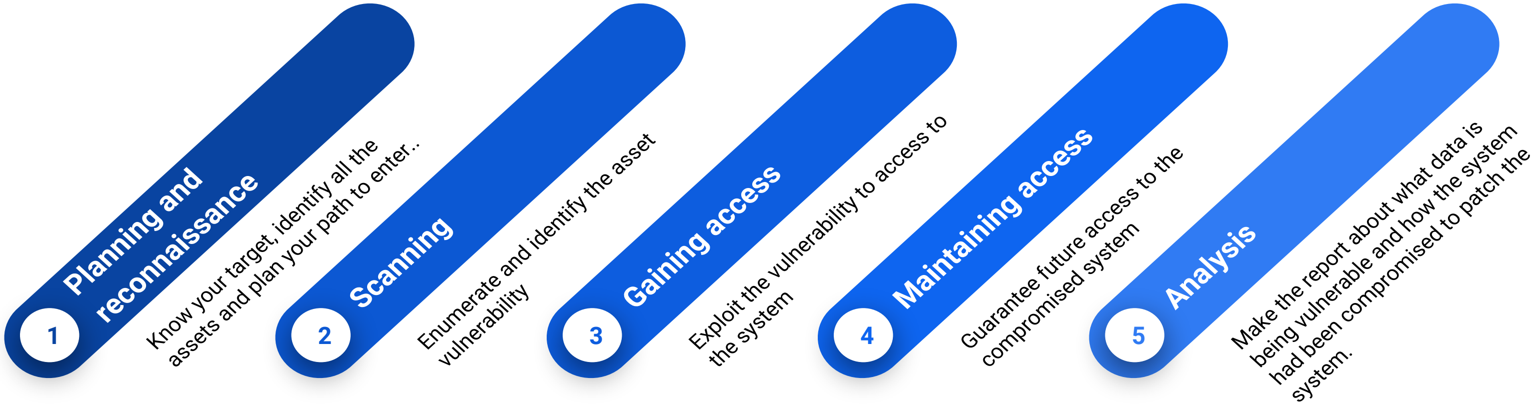
Software Security Testing Process Initiative

Security Testing though the SDLC



Software Security Testing Process Initiative

The Pentesting Process



1 **Planning and reconnaissance**
Know your target, identify all the assets and plan your path to enter..

2 **Scanning**
Enumerate and identify the asset vulnerability

3 **Gaining access**
Exploit the vulnerability to access to the system

4 **Maintaining access**
Guarantee future access to the compromised system

5 **Analysis**
Make the report about what data is being vulnerable and how the system had been compromised to patch the system.

BURPSUITE OWASP KALI LINUX Tor

metasploit® Nessus AIRCRACK-NG

Software Security Testing Process Initiative

Learning process

Security concepts

Tools

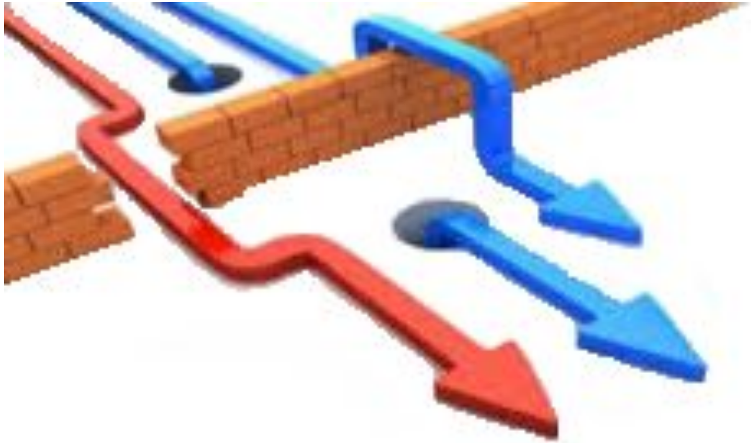
- Threat Modeling
- Kali Linux
- …

Penetration Testing Hands on workshops

- Pre-engagement
- Reconnaissance
- Vulnerability identification
- Exploitation
- Analysis & Reporting

Competitions!

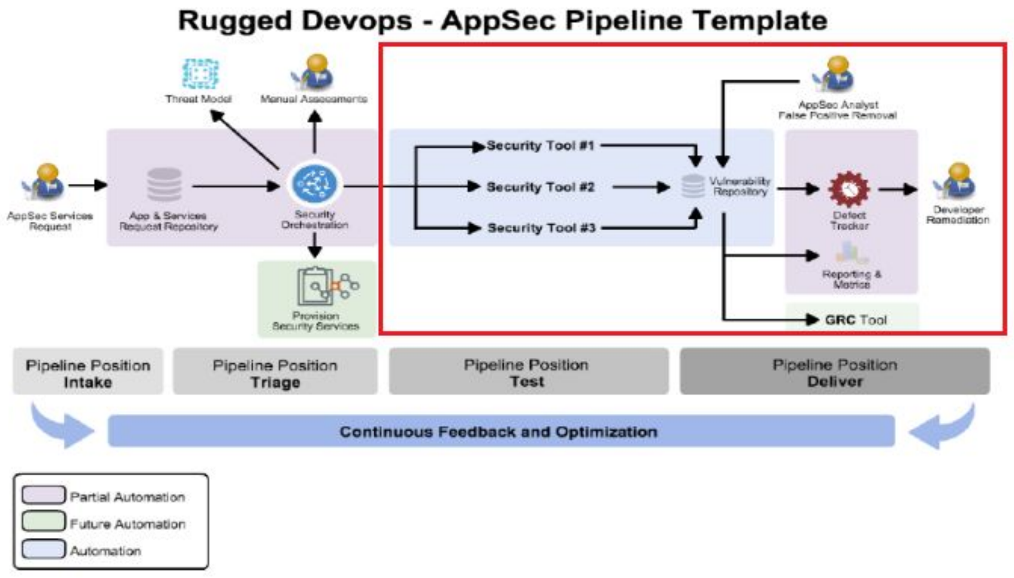
- CTF Contest
- Challenges



Software Security Testing Process Roadmap

Task
Introduction to ethical hacking and technical pills (Introduction)
Security Testing Framework
Introduction to Kali Linux
In deep acknoledge about Planning and reconaissance
Scanning (Passive)
Scanning (Active)
Gaining access
Privilege scalation
Maintaining access
Analisis and report
Threat Modeling & Risk Assessment

ERNI AppSec Pipeline Design Pattern



Aaron Weaver, CC ShareAlike 3.0

Objective

- Collection of security tools for security verifications
- Mostly focused on Static Analysis and Penetration Testing
- Reports consolidation

Which tools?

How to consolidate reports?

Technological Stack

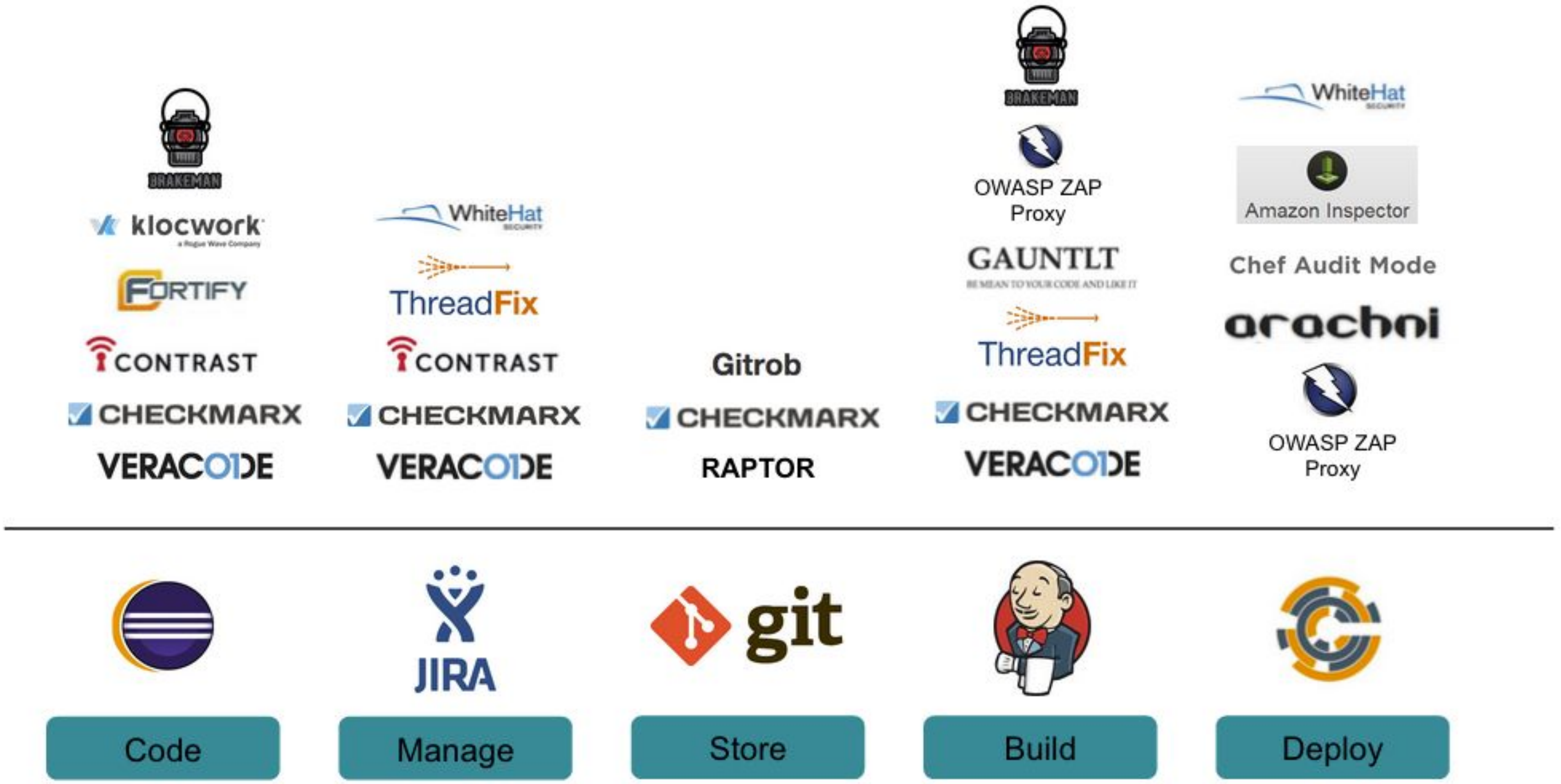
Pipeline Stack

Reporting Solution

ERNI AppSec Pipeline Design Pattern Roadmap

Task
-- Define GOAT Web Application
-- Tooling selection by Phase
---- Static Analysers
---- Checkers Definition
---- Security Functional Testing Tools
-- Reporting
---- Analyse Tooling Report Formats
---- Definition of Expected Report
---- Implementation of a Reporting Tools
---- Create a New Tool?
---- DefectDojo?
-- Documentation
---- Documentation of the Technological Stack
---- Documentation of the Pipeline Stack
---- Documentation of the Reporting Solution

ERNI AppSec Pipeline Design Pattern



Embedded Initiative

Embedded

Learn about security on several embedded frameworks and protocols.
Develop devices and sensors, keeping in mind the solution security.

Frameworks
Platforms
Libraries

ARM mbed
inside SECURE
MIRACL
STM32

Protocols
Technologies

WiFi
Bluetooth LOW ENERGY (4.0) / SMART
zigbee
6LoWPAN
LoRa
Z-WAVE

Projects
Devices
Sensors

Embedded Initiative RoadMap

Tasks
Discuss about a long term PoC project. I propose working in an HVAC system, with a Smart Thermostat developed using an ESP32 microcontroller, a local server using a RPi device, and a basic connection to a Cloud IoT Server. We ‘ll start with no security concerns and start adding security to the solution as the roadmap progresses.
Brief introduction to Frameworks & Platforms - Espressif SDK - Amazon’s FreeRTOS flavor - ARM embedded framework Hands On - ESP32 DevKit C - STM32 Eval Board
Cryptography libraries. - Different Libraries, Contents, Limitations, Licenses Hands On - ESP32 DevKit C - STM32 Eval Board

Tasks Embedded Cont..
Network Protocols - Wi-Fi - Brief Introduction - Security options - MQTT Hands On - ESP32 DevKit C - Raspberry Pi
Network Protocols - BLE - Brief Introduction - Security options Hands On - ESP32 DevKit C
Project closure - Integrate with Amazon IoT Greengrass environment - Integrate with AWS IoT cloud solution Hands On - ESP32 DevKit C - Raspberry Pi
Network Protocols – Zigbee - Brief Introduction - Security options Hands On - TBD
Network Protocols – 6LowPan - Brief Introduction - Other Sub-GHz alternatives - Security options Hands On - TBD

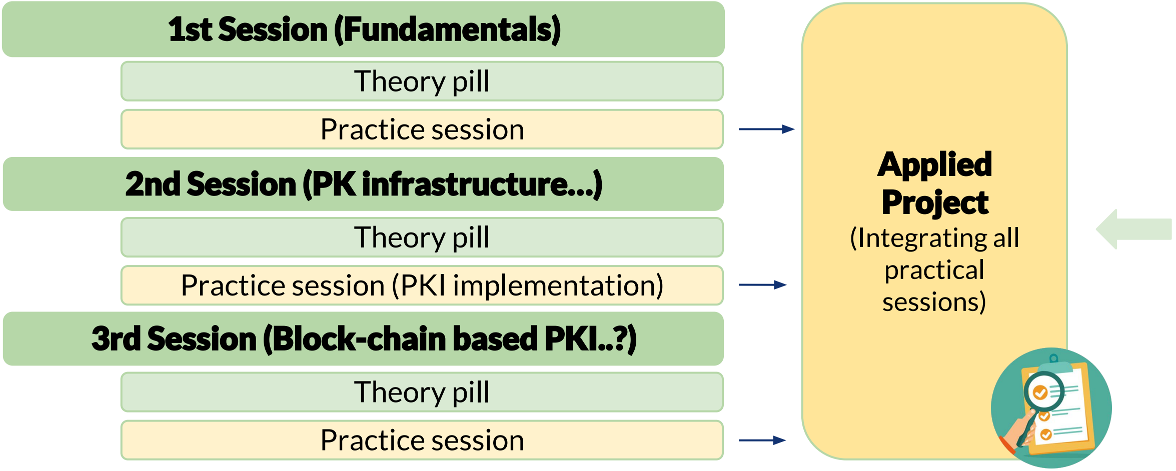
Cryptography

Cryptography is a vital component to every company's security posture and provides the means to securely access, transmit, verify, and dispose of data.

Theory + *Exercises* + *Project* = Learn by doing

· ***Independent*** *sessions*
· ***Integrated*** *project*

¿How will the **cryptography** module work?



1st Session (Fundamentals)

- Theory pill
- Practice session →

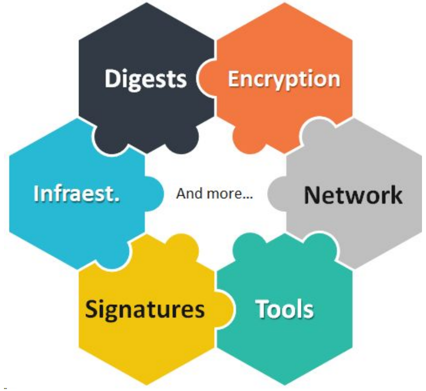
2nd Session (PK infrastructure...)

- Theory pill
- Practice session (PKI implementation) →

3rd Session (Block-chain based PKI..?)

- Theory pill
- Practice session →

Applied Project
(Integrating all practical sessions)



.
.
.

Feel free to propose!

- ***Cross - Module (transversal)***

Cryptography Roadmap

Cryptography
Cryptography Fundamentals
Overview
Symmetric Key Cryptography
AES, CIPHER, DES, 3DES...
Strengths and Weaknesses
Practical Lesson (Python)
Cryptography Fundamentals
Cryptography Fundamentals
RSA, ECC...
Strengths and Weaknesses
Practical Lesson (Python)
Public Key Infraestructure
Certificate Authorities and Digital Certificates
Public Key
Private Key
Tools
Implementing Public Key Infraestructure (Python)

Cryptography Roadmap

Cryptography (cont)
Integrity and Authentication
Hashing
OAUTH, SSL, TLS
Email, Files and Drives Encryption
Message Authentication
Hashing Algorithms
Practical Lesson
Cryptoanalysis (TBD)
Cryptoanalisis methods
Code-Breaking methods
Trickery and Deceit
Brute-Force
One-Time Pad and Frequency Analysis
Descentralized Systems (TBD)
BlockChain Security Fundamentals
Proof of Work
Freenet
TBD

Open Discussion

Discuss with the Leader of the initiative of your preference

Fill in the papers

better ask ERNI