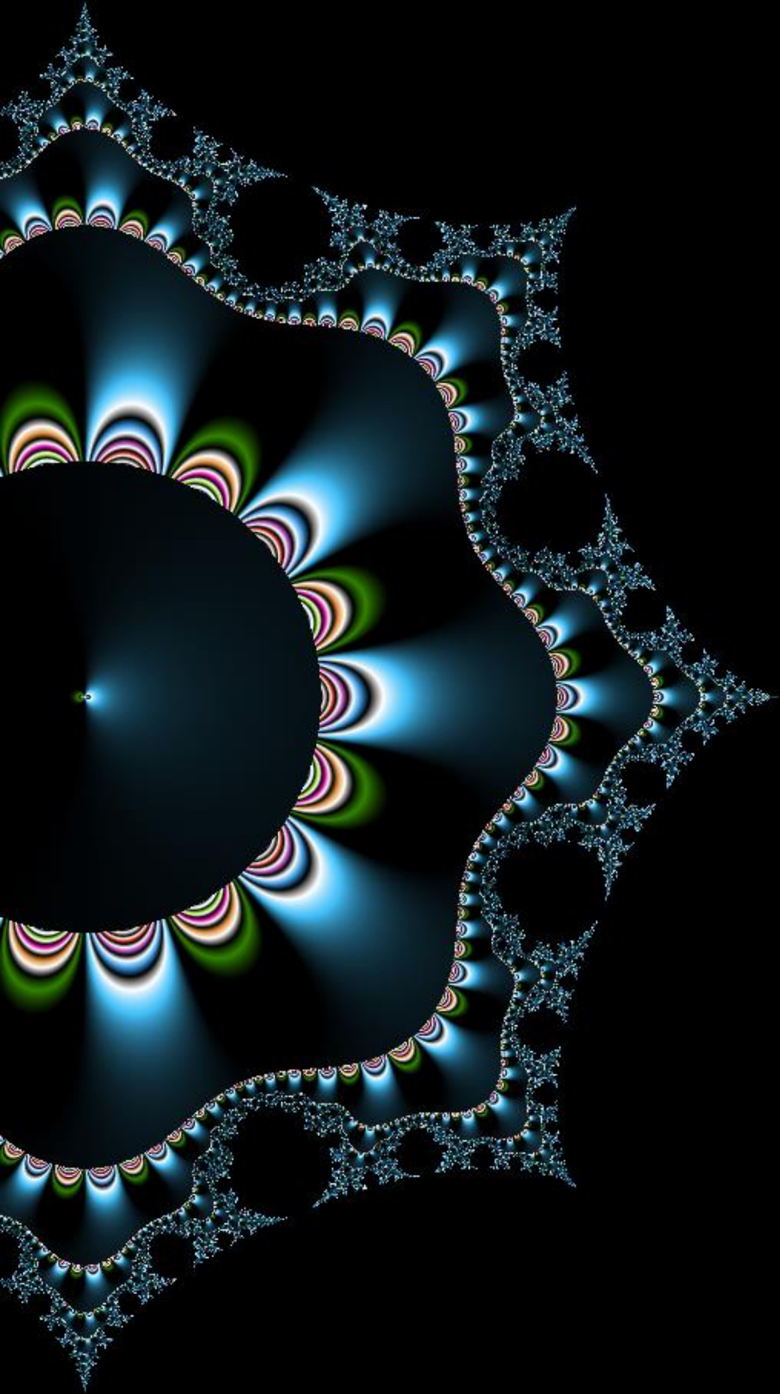


03 Introduction

Security (of) softwares

Thibaut HENIN

www.arsouyes.org

What is a software vulnerability ?

Software vulnerability

definition

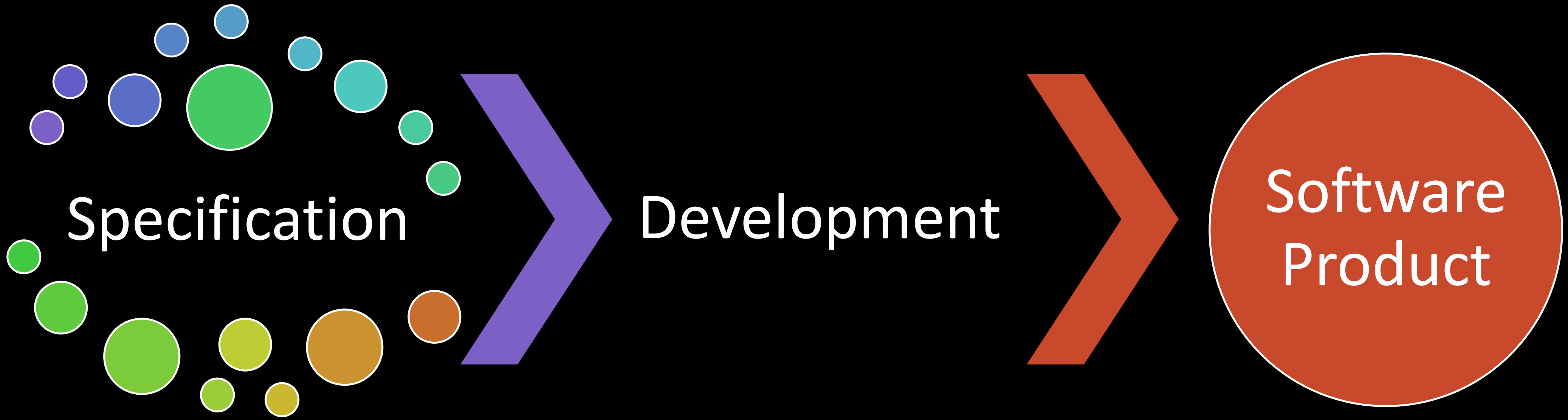
A defect

that allows

unauthorized actions

Software engineering

How we turn dreams into reality



Specification

Development

Software Product

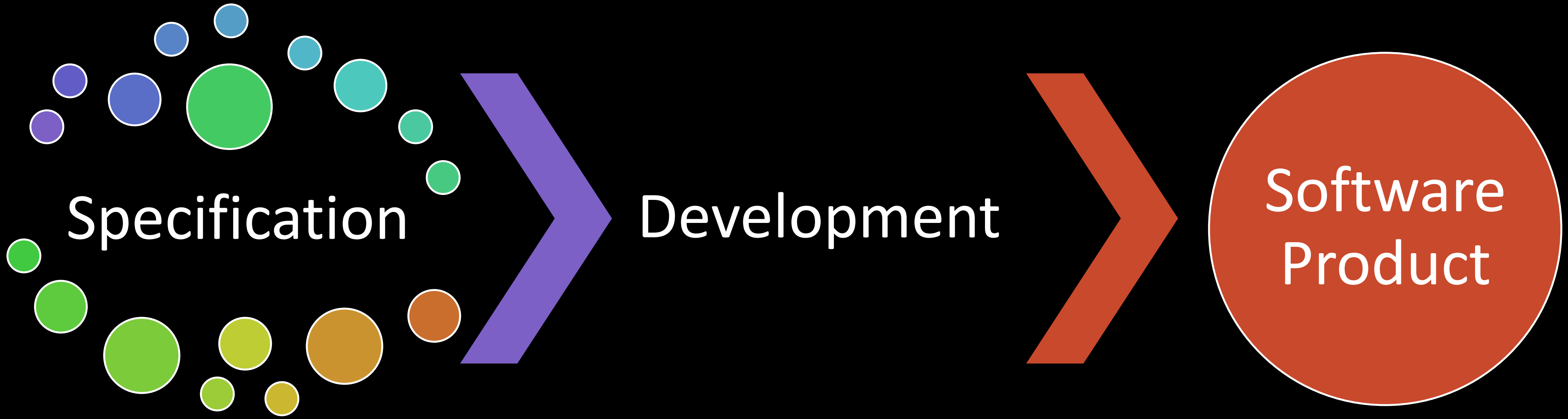
What we wants

This is where the magic happens

What we get

Software Security

How we turn nightmares reality



Specification

Development

Software Product

What we wants

What we get

Security Policy

Vulnerabilities

Agenda

of these lectures

Monday 30th October	Tuesday 1st November	Wednesday 2nd November
03 - Introduction		
04 - Injections PHP, SQL, JS		05 - Overflows & shellcodes
Over The Wire		06 - Memory management
-		CSPN – Presentations
CSPN – Target		Over The Wire

Over The Wire follow up: 8th November / 17th November / 23rd November / 2nd December

Over the Wire

What you will have to do

`https://overthewire.org/wargames/`

Wargames / Challenge

Bandit (0.1 pts/pass)

Natas (0.4pts /pass)

Narnia (1.0pts /pass)

Due before 1st January 2023 00:00 UTC

Login & password in .ini files mailed to thibaut.henin@gmail.com

CSPN – Security Target

What you will have to do

`https://www.arsouyes.org/products/UBS_Security`

Oral presentation on 2nd November 2023 afternoon

Written document before 1st January 2023 00:00 UTC

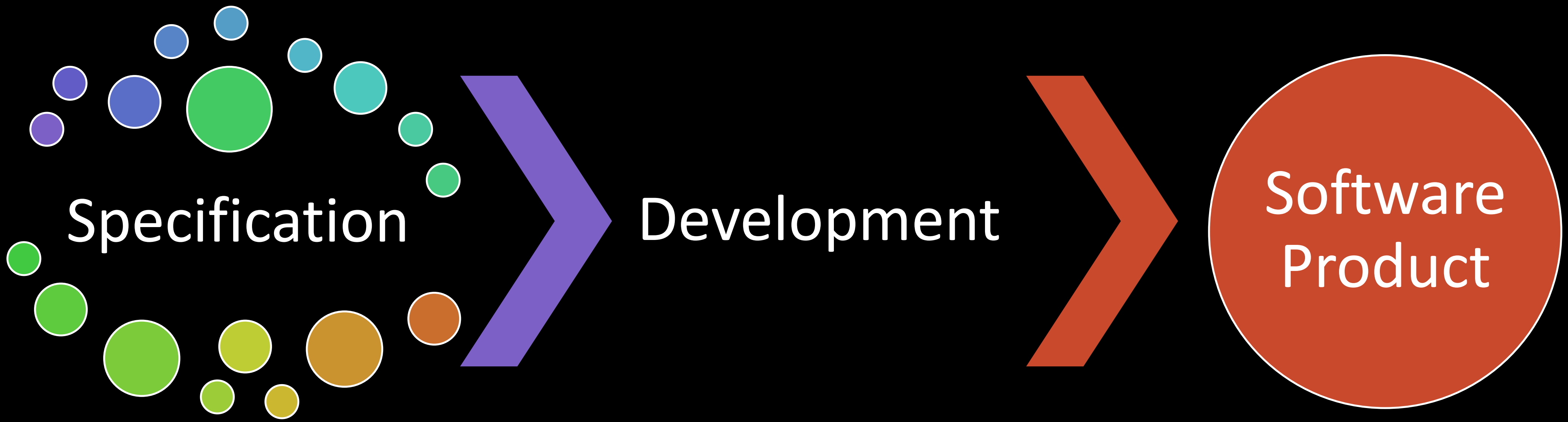
Professionnal pdf document mailed to thibaut.henin@gmail.com

CSPN

Short Introduction

CSPN

Two phases



Specification

Development

Software Product

What we wants

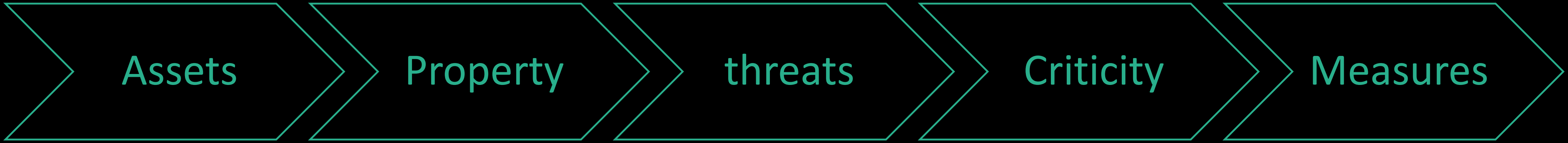
Security Target

What we get

Security Evaluation

Security Target / Policy

(from risk management)



Assets

Property

threats

Criticity

Measures

Step 0 – the product

Who it is

Identification

(name, version, editor, …)

Description

(features / use cases, users, prerequisites, …)

Step 1 - Assets

definition

A resource

(information, data, hardware, functionnality, …)

That need to be protected

(against malicious agent)

Step 1 - Assets

Example

Business assets	Support assets
A1 - Articles	*A4 - Passwords*
A2 - Nicknames	*A5 - Files – configuration*
A3 - Web browsers	*A6 – Files – source code*
	A7 - Servers

Step 2 - Security Properties

Three main ones

Confidentiality

(only authorized agend can read)

Integrity

(only authorized agent can write)

Availability

(asset can be accessed)

Step 2 - Security Properties

Other usefull ones

Authenticity

(the resource is the one that have been sent)

Traceability

(access are recorded on a log)

Non repudiation

(nobody can say « it’s not me » or « it’s someone else »)

Step 2 - Coverage matrix

Assets and properties

Assets	Confidentiality	Availability	Integrity
A1 - Articles			✓
A2 - Nicnkames			✓
A3 - Web browsers	✓		✓
A4 - Passwords	✓		✓
A5 - Files - configuration	✓		✓
A6 - Files – source code			✓
A7 - Servers	✓		✓

Step 3 – Threats

Definition

Feared event

(what wrong can happen)

Step 3 – Threats

Example

T1 – Fraudulent modification of article

T2 – Execution on browser

T3 – Fraudulent deletion of article

T4 – Impersonation of writers

T5 – Password theft

T6 – Theft of account

T7 – Fraudulent access to files

T8 – Fraudulent modification of files

T9 – Execution on server

Step 3 – Coverage matrix

Assets by threats

Threats	A1 Articles	A2 Nicknames	A3 Browsers		A4 Passwords		A5 Files Config		A6 Files Source code	A7 Servers	
	I	I	C	I	C	I	C	I	I	C	I
T1 - Modification article	✓	✓									
T2 - Execution, browser	✓	✓	✓	✓							
T3 - Deletion article	✓	✓				✓					
T4 - Impersonation	✓	✓									
T5 - Password theft	✓	✓			✓						
T6 - Account theft	✓	✓				✓					
T7 - File access					✓		✓			✓	
T8 - File changes	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
T9 - Execution, server	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Step 3b - Criticity

Product of two parameters

Gravity - Consequences on the asset

e.g. if articles are defaced, the branding of the editor is hurt

Probability - Ease of the threat

e.g. access to writers' password database

Step 3b - Criticity

Visually

For sure	4	8	12	16
Probable	3	6	9	12
May occurs	2	4	6	8
Not expected	1	2	3	4
	no effect	It hurts	Low damage	High damage

Step 3b - Criticity

Optionnal for software (since we use booleans)

	no effect	Some effects
Possible	0	1
Impossible	0	0

Step 5 - Measures

a.k.a. security function / security features

Things to mitigate the risks

Eg. Access control, backups, updates, training, monitoring, …

Step 5 - Coverage matrix

Threats by measures

Mesure	Article modification	Password theft	Execution on server
Authentication & access control	✓		
Secure storage of password		✓	
Input data filtering			✓

Step 5b - Residual risk

Value after measure take effects

Mesure	New Probability	New Gravity	New Risk
Article modification → Access control	1 → 0	1	1 → 0
Password theft → Secure storage	1	1 → 0	1 → 0
Execution on server → Input filtering	1 → 0	1	1 → 0

Security Policy

Definition

Document that tells :

« What it means to be secure »

(all previous content)

What is a software vulnerability ?

Vulnerability

Bypass of Security Policy

Exploit

Software that automate the bypass