Date 25/01/2023

Défi 02 "Gestion des risques pour tests de pénétration"

Groupe de travail défi 02

Christophe Ponsard, CETIC
Antoine Sacré, UNamur
Serey Touch, UNamur
Justine Ramelot, UCLouvain
Sébastien Dupont, Guillaume Ginis, CETIC

digital wallonia 4.cyberwal

Wallonie recherche SPW

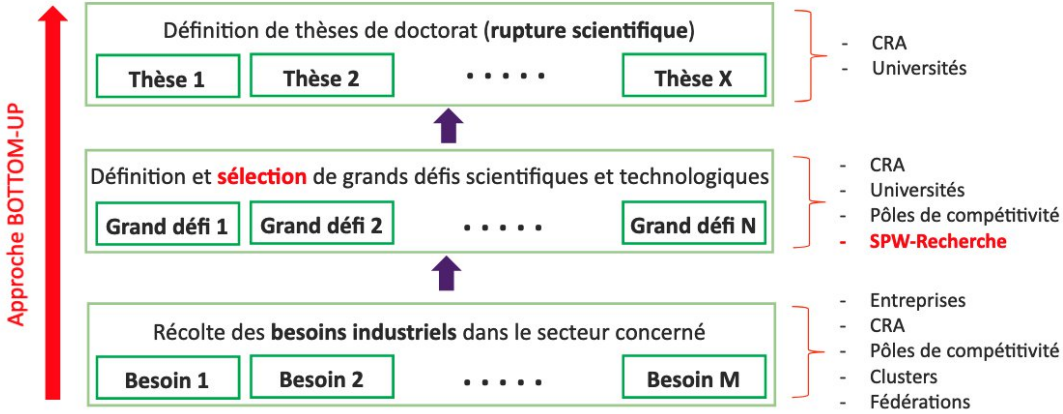
https://cyberwal.be
https://cyberexcellence.be

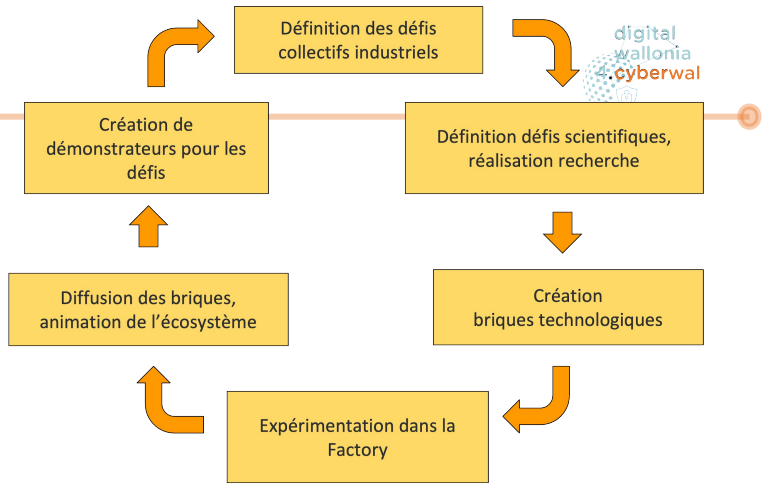
Agenda

15:00-15:05	Rappel projet CyberExcellence, expérimentation dans la factory, et défi 02	Philippe Massonet
15:05-15:25	Présentation des problèmes de recherches liés au défi: - Eval de conformité d'un SI Ⓟ aspect processus, approche amont - Adaptive Self-guarded Honeypot Ⓟ apprentissage "run-time" - Cyber Range Scenarios Ⓟ aspect humains: utilisabilité, profils - Retour apprentissage analyse de risques Ⓟbesoins/focus	Antoine Sacré, Serey Touch, Justine Ramelot C. Ponsard
15:25-15:40	Présentation des potentielles études de cas pour expérimenter des techniques de tests de pénétration dirigées par les risques	Guillaume Ginis, Sébastien Dupont
15:40-16:00	Discussion sur le type de vulnérabilités, contraintes à prendre en compte et l'organisation du groupe	Tous

Projet CyberExcellence et Défis Collectifs Industriels

- Projet CyberExcellence
  - Projet de recherche en cybersécurité, 01/01/2022, 18,9 millions de budget)
  - Partenaires : 5 universités + 2 CRA
  - Recherche fondamentale mais **au bénéfice du tissu industriel**: réponds aux besoins des entreprises/administrations
- Défi Collectif Industriel
  - Récolte des besoins industriels dans le secteur concerné
  - Identification des défis Collectif Industrie
- Factory
  - Production de briques technologiques





WP

WP1 : Rendre les systèmes résilients aux cyberattaques : phase de conception.

WP2 : Détection, Réponse, Réaction : Phase Dynamique

WP3 : RGPD et Open data : sécurité à la conception

WP4 : La protection et le partage des données au cœur des préoccupations

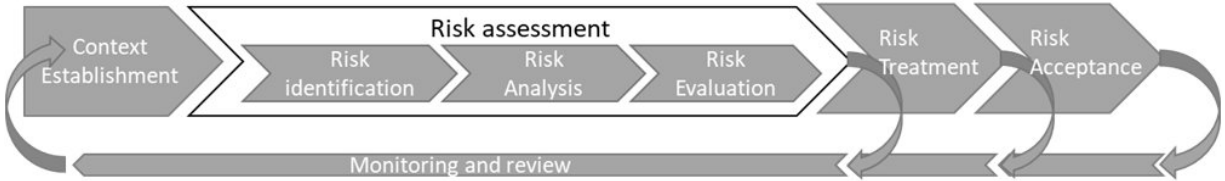
WP5 : Laboratoires d'expérimentation, de validation, et d'entraînement

WP6 : Factory et grands défis

Défi 02 "Gestion des risques pour tests de pénétration"

- **Résumé du défi:**
  - Systèmes industriels de plus en plus exposés aux attaques cyber (transfo numérique vs systèmes SCADA « legacy »)
  - Aspect également de plus en plus régulé dans les domaines essentiels (NIS) avec des **référentiels**/standards spécifiques IT/OT
  - Activités de test de pénétration très coûteuse en ressources et potentiellement inefficace si pas couplée à une démarche d'analyse des risques % scénarios envisagés

- **Challenges de recherche**:
  - Génération automatique/apprentissage de scénarios d'attaque ou de défense pour l'entraînement et la recherche (UCLouvain, UNamur)
  - Facilitation de l'alignement avec des référentiels existants, nouveaux, e.g. NIS2 (CETIC,UNamur)
  - Conception de processus d'ingénierie DevSecOps : modélisation, performance, en particulier collecte d'indicateurs orienté risque (CETIC)



ARRCIS : Évaluation et renforcement de la conformité d'un système d'information

Antoine Sacré | 25/01/2023

Contexte du projet

La **pression normative** est en croissance sur les systèmes d'information et plusieurs défis découlent de cette pression

Conformité indispensable

Les contraintes normatives doivent faire partie des contraintes à considérer dans ces systèmes.

Normes complexes

Contexte du projet

La prise en compte des exigences des normes dans les **développements informatique** est complexe et coûteux

Processus manuel

Ce processus se fait habituellement manuellement et peut demander beaucoup de temps et d'efforts.

Identification complexe des normes pertinentes

Il est difficile d'identifier les normes qui s'appliquent à un système ou une partie de système particulier.

Évolution rapide des systèmes d'information

Les systèmes informatiques évoluent vite et sont de plus en plus complexe à évaluer.

Évolution des normes

Les normes évoluent et demandent une attention régulière

Une solution est envisageable

La situation actuelle n’est pas adéquate, une nouvelle solution est donc à envisager

Solutions actuelles peu satisfaisantes

Aucune solution peu couteuse et accessible existe

Une conception différente permet une diminution des couts

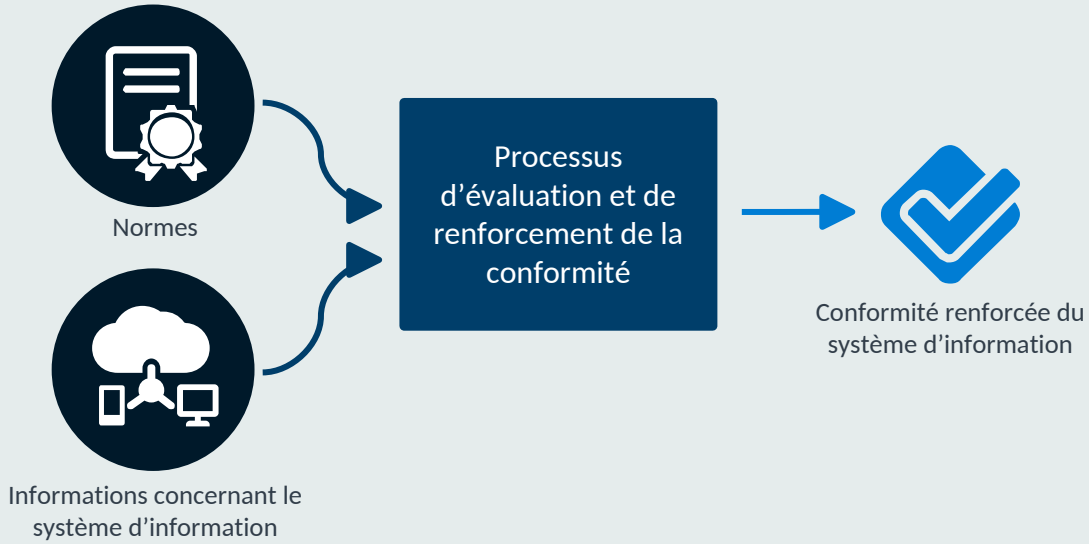
En ayant un processus qui est utilisable dés la conception, on évite un potentiel refactoring couteux.

Les développeurs de logiciels devraient être mieux équipés

Si l'utilisation des logiciels devient inévitable dans la vie courante, l'e-gouvernement, les services essentiels (eau, électricité…)…

Notre projet

Développer une méthodologie outillée qui permettrait de vérifier la conformité d'un système d'information par rapport aux normes et qui permettrait d'établir une liste d'actions priorisées pour améliorer la conformité.

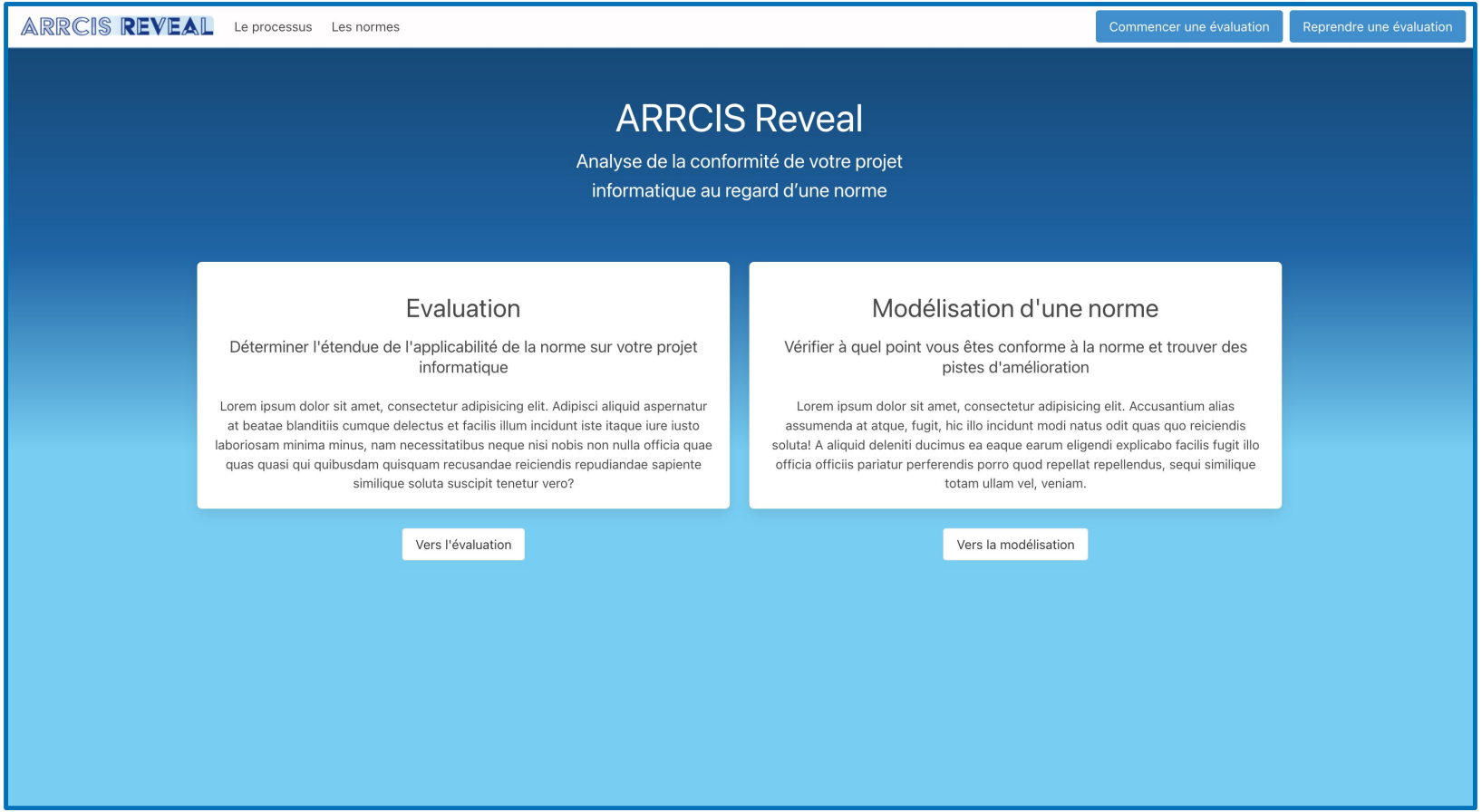


Étude de cas

Normes légales :
MDR
GDPR

Normes techniques :
ISO 62304
ISO 27701
…

Application mobile d'aide au suivi du traitement par les patients, afin d'améliorer l'observance thérapeutique.

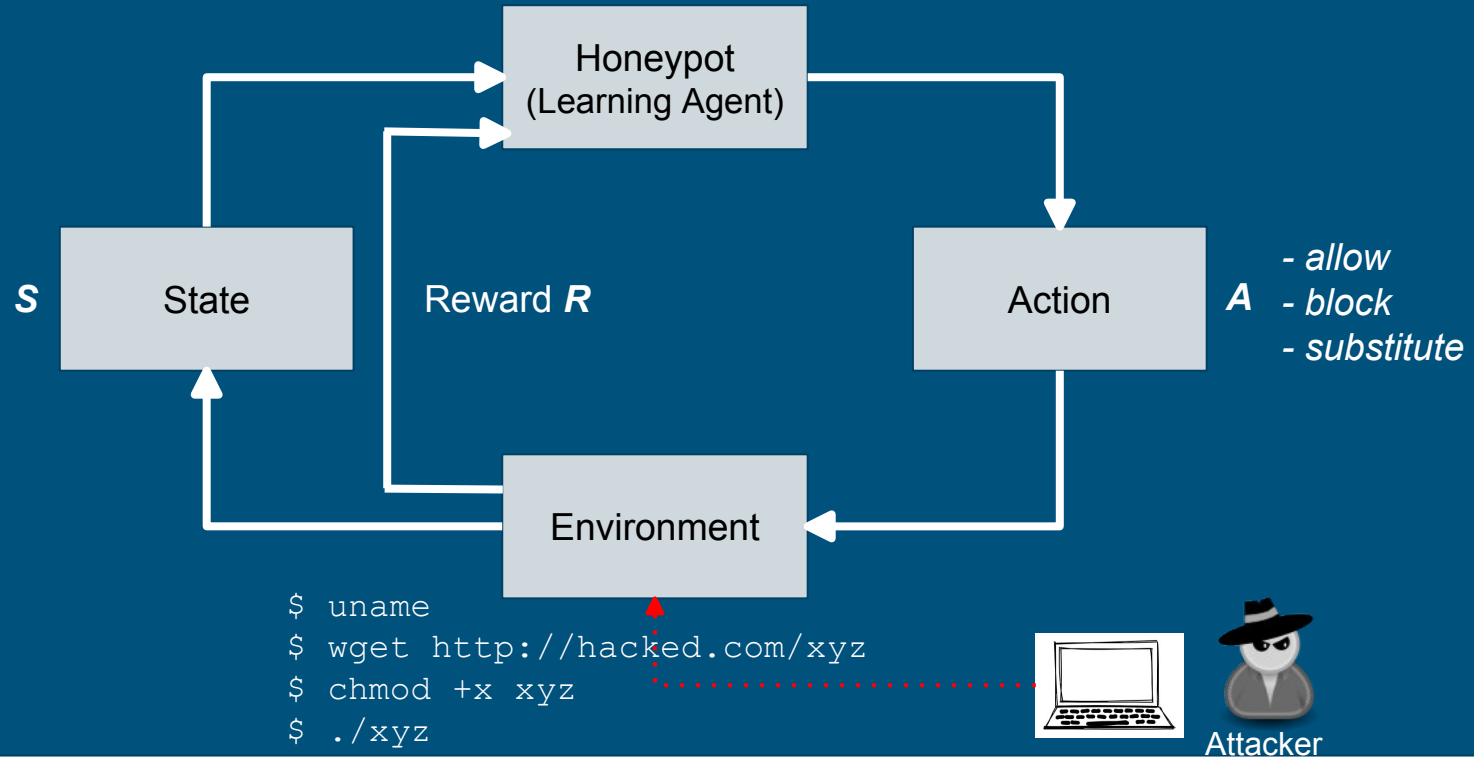


Research Topic: Adaptive Self-guarded Honeypot

Objective: build an adaptive (smart) honeypot using the SSH protocol to achieve two primary objectives:

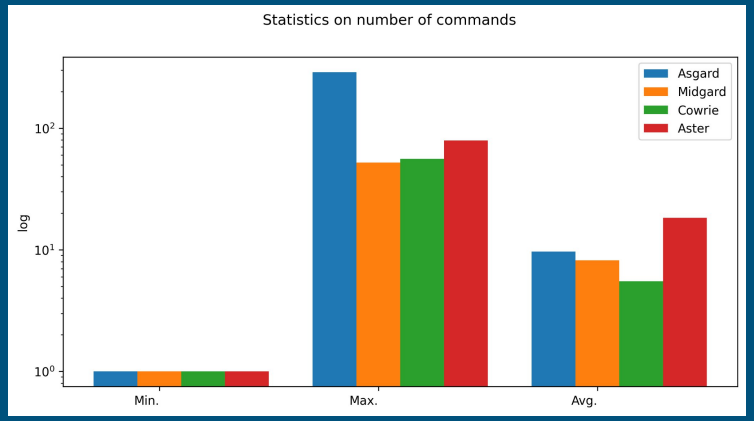
1. Interact with the attackers to collect their tools
2. Defend itself from being deeply compromised

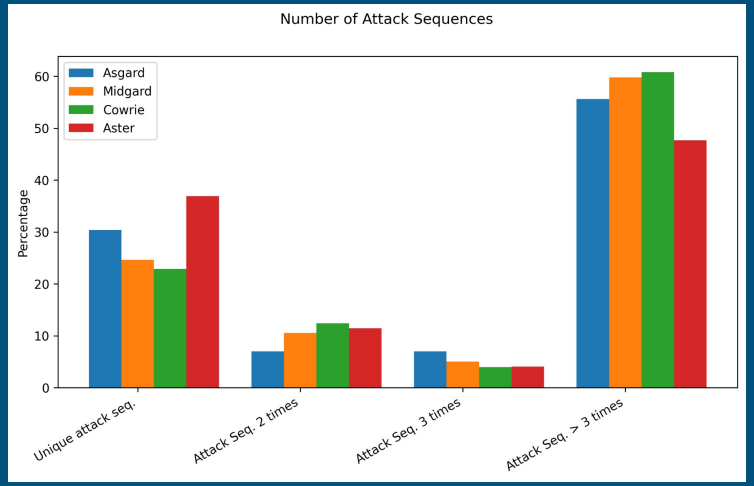
Our approach: a honeypot as a RL agent



First Result: Asgard [1]

- Simple environment state
  - command
- Action:
  - Allow
  - Block
  - Substitute
- Reward function
  - Environment state + action
- Learning Algorithm
  - Q-learning: a model-free
- Evaluation [2]
  - Cowrie: an ssh emulator
  - Aster: a real Linux system
  - Midgard: a variant of Asgard





[1] Touch, S., & Colin, J. N. (2021, October). Asguard: Adaptive Self-guarded Honeypot. In *17th International Conference on Web Information Systems and Technologies-Volume 1: DMMLACS*, (pp. 565-574). SciTePress.

[2] Touch, S., & Colin, J. N. (2022). A Comparison of an Adaptive Self-Guarded Honeypot with Conventional Honeypots. *Applied Sciences*, *12*(10), 5224

Expected collaboration

- Define and design various test scenarios
  - To adapt and integrate our system to meet the needs of the company.
  - To deploy and test our system in a real environment.
  - To collect and analyse the obtained data to validate and improve the system.

UCLouvain

Institute for Language and Communication

Cyber Range Scenarios (CRS2)

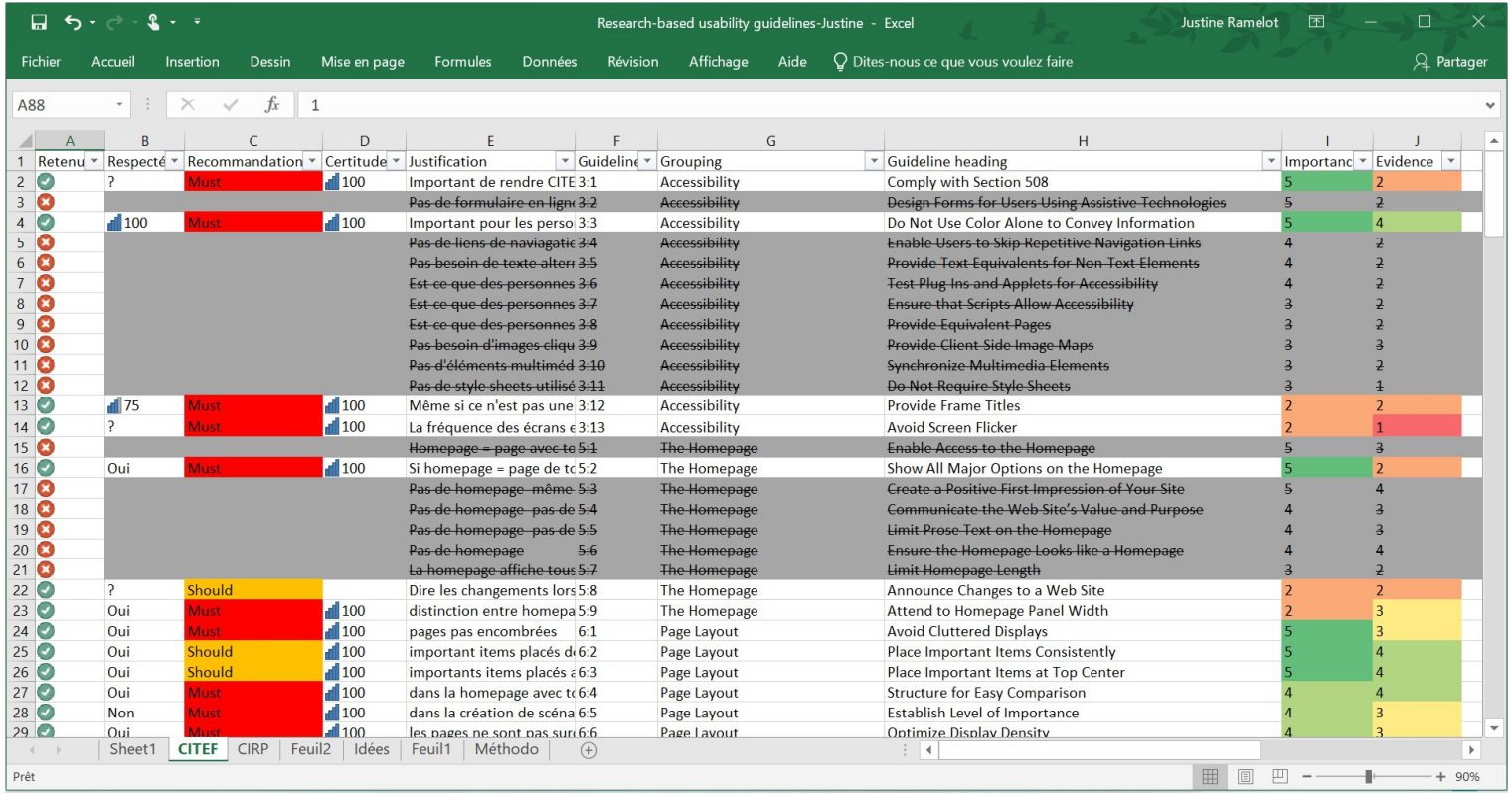
January 25 - Justine Ramelot

Who am I?

- Justine Ramelot
- justine.ramelot@uclouvain.be
- Research assistant
- Cyber Range Scenarios (CRS2) : generate the most realistic and appropriate training scenarios possible
- Cyber Range: a real-world simulation platform that allows security teams to train (attack and defense), develop their expertise, and manage their human resources planning
- UX team

Compliance with guidelines formulated across 4 criteria: relevance of guideline, respect, recommandation, certainty

Shneiderman & Leavitt (2006)



	Retenu	Respecté	Recommandation	Certitude	Justification	Guideline	Grouping	Guideline heading	Importanc	Evidence
2	✓	?	Must	100	Important de rendre CITE	3:1	Accessibility	Comply with Section 508	5	2
3	✗				~~Pas de formulaire en ligne~~	~~3:2~~	~~Accessibility~~	~~Design Forms for Users Using Assistive Technologies~~	~~5~~	~~2~~
4	✓	100	Must	100	Important pour les perso	3:3	Accessibility	Do Not Use Color Alone to Convey Information	5	4
5	✗				~~Pas de liens de naviagatic~~	~~3:4~~	~~Accessibility~~	~~Enable Users to Skip Repetitive Navigation Links~~	~~4~~	~~2~~
6	✗				~~Pas besoin de texte alter~~	~~3:5~~	~~Accessibility~~	~~Provide Text Equivalents for Non-Text Elements~~	~~4~~	~~2~~
7	✗				~~Est ce que des personnes~~	~~3:6~~	~~Accessibility~~	~~Test Plug-Ins and Applets for Accessibility~~	~~4~~	~~2~~
8	✗				~~Est ce que des personnes~~	~~3:7~~	~~Accessibility~~	~~Ensure that Scripts Allow Accessibility~~	~~3~~	~~2~~
9	✗				~~Est ce que des personnes~~	~~3:8~~	~~Accessibility~~	~~Provide Equivalent Pages~~	~~3~~	~~2~~
10	✗				~~Pas besoin d'images cliqu~~	~~3:9~~	~~Accessibility~~	~~Provide Client-Side Image Maps~~	~~3~~	~~3~~
11	✗				~~Pas d'éléments multimédi~~	~~3:10~~	~~Accessibility~~	~~Synchronize Multimedia Elements~~	~~3~~	~~2~~
12	✗				~~Pas de style sheets utilisé~~	~~3:11~~	~~Accessibility~~	~~Do Not Require Style Sheets~~	~~3~~	~~1~~
13	✓	75	Must	100	Même si ce n'est pas une	3:12	Accessibility	Provide Frame Titles	2	2
14	✓	?	Must	100	La fréquence des écrans e	3:13	Accessibility	Avoid Screen Flicker	2	1
15	✗				~~Homepage = page avec te~~	~~5:1~~	~~The Homepage~~	~~Enable Access to the Homepage~~	~~5~~	~~3~~
16	✓	Oui	Must	100	Si homepage = page de to	5:2	The Homepage	Show All Major Options on the Homepage	5	2
17	✗				~~Pas de homepage- même~~	~~5:3~~	~~The Homepage~~	~~Create a Positive First Impression of Your Site~~	~~5~~	4
18	✗				~~Pas de homepage- pas de~~	~~5:4~~	~~The Homepage~~	~~Communicate the Web Site's Value and Purpose~~	4	~~3~~
19	✗				~~Pas de homepage- pas de~~	~~5:5~~	~~The Homepage~~	~~Limit Prose Text on the Homepage~~	4	~~3~~
20	✗				~~Pas de homepage~~	~~5:6~~	~~The Homepage~~	~~Ensure the Homepage Looks like a Homepage~~	4	4
21	✗				~~La homepage affiche tous~~	~~5:7~~	~~The Homepage~~	~~Limit Homepage Length~~	~~3~~	~~2~~
22	✓	?	Should		Dire les changements lors	5:8	The Homepage	Announce Changes to a Web Site	2	2
23	✓	Oui	Must	100	distinction entre homepa	5:9	The Homepage	Attend to Homepage Panel Width	2	3
24	✓	Oui	Must	100	pages pas encombrées	6:1	Page Layout	Avoid Cluttered Displays	5	3
25	✓	Oui	Should	100	important items placés d	6:2	Page Layout	Place Important Items Consistently	5	4
26	✓	Oui	Should	100	importants items placés a	6:3	Page Layout	Place Important Items at Top Center	5	4
27	✓	Oui	Must	100	dans la homepage avec te	6:4	Page Layout	Structure for Easy Comparison	4	4
28	✓	Non	Must	100	dans la création de scéna	6:5	Page Layout	Establish Level of Importance	4	3
29	✓	Oui	Must	100	les pages ne sont pas sur	6:6	Page Layout	Optimize Display Density	4	3

Creation of a questionnaire for guidelines for which we are unsure

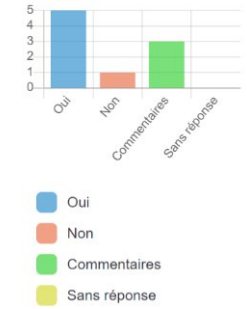
Résumé des réponses

Réponses complètes	6
Réponses incomplètes	3
Nombre total de réponses	9

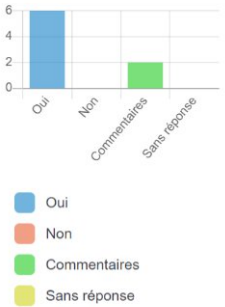
Résumé des réponses

Réponses complètes	1
Réponses incomplètes	0
Nombre total de réponses	1

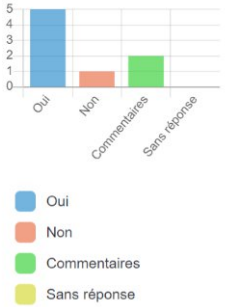
Est-ce que les champs de saisie de données obligatoires sont facilement distinguables des champs de saisie de données facultatifs ?



Est-ce que c'est possible de passer d'un champ de données à l'autre en utilisant la tabulation ?

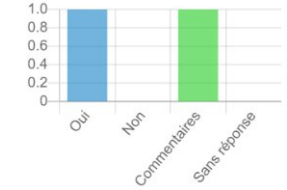


Lors de la création d'un scénario, est-ce que tous les items nécessaires à la création d'un scénario sont disponibles et affichés sur l'écran ?

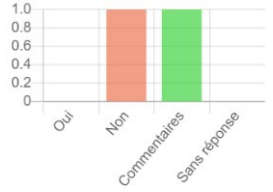


Est-ce que CIRP est également adressé à des personnes souffrant d'un handicap (visuel, mouvement, sonore, apprentissage) ?

Est-ce que les pages web de CIRP ont une fréquence supérieure à 2 Hz et inférieure à 55 Hz pour éviter le scintillement d'écran ?



Est-ce que les changements apportés à CIRP sont annoncés sur la page d'accueil ?



Creation of a questionnaire to assess the skills of trainees and adapt the scenario

Based on European Cybersecurity Skills Framework (ECSF)

The ECSF's 12 Role Profiles for Cybersecurity Professionals

Examples of e-Competences (from e-CF)

E.7 Business Change Management

Assesses the implications of digital transformation, potential digital disruption and change. Defines the requirements and quantifies the business benefits. Manages change taking into account structural and cultural issues. Maintains business and process continuity throughout change, monitoring the impact, taking any required remedial action and refining approach.

Level 1	-
Level 2	-
Level 2	Evaluates change requirements and exploits specialist skills to identify possible methods and standards that can be deployed
Level 3	Provides leadership to plan, manage and implement significant ICT led business change
Level 4	Applies pervasive influence to embed organisational change.

E.8 Information Security Management

Manages information and systems security policy accounting for technical, human, organisational and other relevant threats, in line with the IT and business strategy and reflecting the risk culture of the organisation. Deploys and manages the operational and specialist (for e.g. forensics, threat intelligence and intrusion detection) resources needed to ensure the capacity to manage security incidents, and makes recommendations for the continuous improvement of security policy and strategy.

Level 1	-
Level 2	Systematically scans the environment to identify and define vulnerabilities and threats. Records and escalates non- compliance.
Level 2	Evaluates security management measures and indicators and decides if compliant to information security policy. Investigates and instigates remedial measures to address any security breaches
Level 3	Provides leadership for the integrity, confidentiality and availability of data stored on information systems and complies with all legal requirements.
Level 4	-

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Survey and Guidelines about Learning Cyber Security Risk Assessment

cetic
Your Connection to ICT Research

Setting:

- 35 people working in different organisations (after work classes)
- EBIOS method with basic tooling

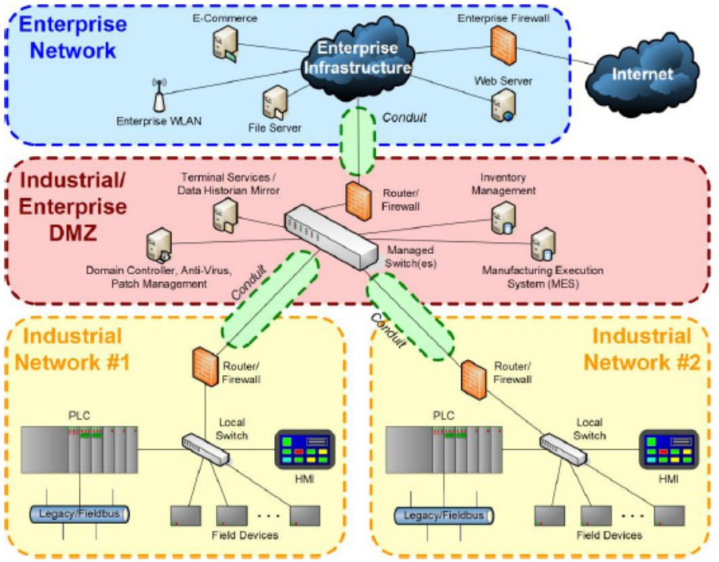
Outcome

- quality level quite satisfactory (above with few problematic audits
  Ⓟ either due to immature businesses (e.g. early game development)
  or R&D topics (e.g. firmware updates)
- Decreasing quality across workflow
  Ⓟ due to the accumulation of flaws
  Ⓟ switch in complexity
  from more descriptive tasks (until risk
  to more prescriptive tasks (actions)
- cases involving citizen: lower score.
  Ⓟ more open context of such analysis
  including privacy issues (PIA advised)

#	Topic (anonymised)	Domain	Target (GDPR)	NIS	Context	Existing Measures	Dreaded Events	Threats	Risks	Measures	GLOBAL
1	online forms	administration	citizen		9	8	8	10	5	4	7
2	public aids	administration	corporate		10	10	5	6	3	3	6
3	firmware update	automotive	citizen	X	7	5	5	3	5	3	4
4	tourism	business	citizen		10	10	8	8	8	8	8
5	ecommerce	business	citizen		9	3	8	5	4	5	5
6	recruitment	business	citizen		9	10	10	9	8	6	9
7	recruitment	business	citizen		9	8	5	6	5	8	7
8	insurance	business	corporate		10	10	9	9	6	6	8
9	real estate	business	corporate		10	10	10	10	9	10	10
10	ERP	business	corporate		7	10	8	8	9	8	8
11	N/A	defense	corporate		10	5	5	8	5	5	6
12	high school	education	citizen		10	10	10	8	5	5	8
13	high school	education	citizen		9	5	10	8	5	6	7
14	online game	entertainment	citizen		6	8	4	4	4	6	5
15	event management	entertainment	citizen		10	10	10	10	9	9	10
16	online forms	entertainment	citizen		8	5	8	8	8	8	7
17	online game	entertainment	citizen		10	8	5	5	3	3	5
18	covid	homeworking	citizen		9	10	8	8	6	4	7
19	water management	industrie (OT)	corporate	X	9	8	8	8	10	8	8
20	water management	industrie (OT)	corporate	X	10	10	10	10	8	8	9
21	manufacturing	industrie (OT)	corporate		9	10	5	10	1	4	7
22	store	logistics	corporate		9	5	8	9	6	7	7
23	store	logistics	corporate		9	8	10	9	7	8	8
24	hospital	medical	corporate		10	10	9	8	9	9	9
25	digital service provider	telecom	corporate	X	7	8	8	5	5	5	6
26	digital service provider	telecom	corporate	X	8	8	8	10	8	8	8
	MEAN				8,7	8,0	7,5	7,5	6,0	6,1	7,3
	STANDARD DEVIATION				1,2	2,2	2,0	2,0	2,2	2,1	1,4

Lessons Learned #1 - Avoiding Uncontrolled Growth of the Number of Risks

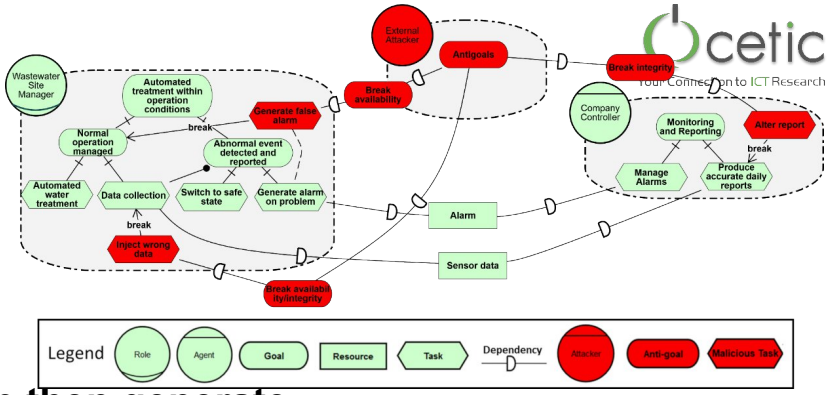
- Typically: # business assets x #security properties
- Standard recommendations: focus on major assets (scoping) or group
  Ⓟ loss in precision/granularity
- Better tactics:
  - Rely on assumptions Ⓟ identify strong protection, low residual risk
    or push responsibility to prove to another part
  - Domain analysis Ⓟ rule out impossible scenarios,
    requires more precise modelling
  - Refinement levels
    - **Coarse-grained/high level analysis Ⓟ targeted analysis**
    - E.g. IEC 62443 industrial systems ZCR2 Ⓟ ZCR5
  - Breaking into subsystems
    - (related to previous)
    - **segmentation in zones and conduits (also in IEC 62442)**
    - focus on interfaces
  - Early prioritization, focus on major risks
    - Idea: measure will have wider impact, assess residual risk iterate
    - EBIOS Risk manager evolution
  - Stage security requirements using security levels



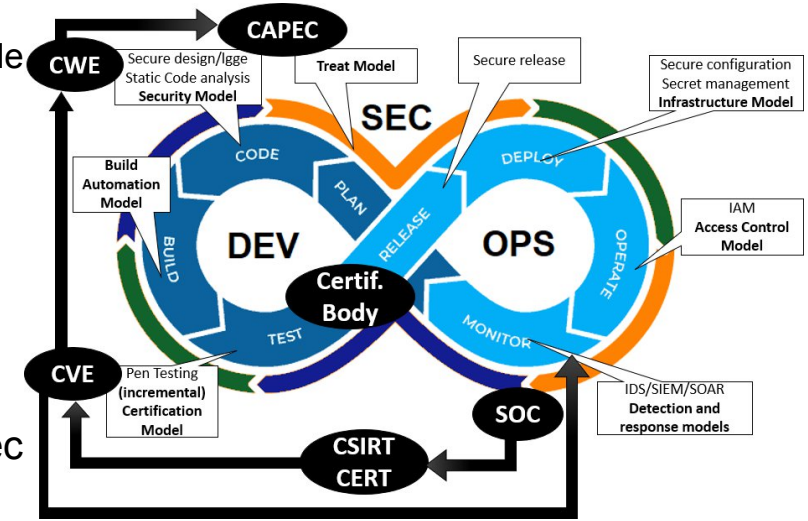
Lessons Learned #2 – Need for Deeper Modelling

- EBIOS “flat”:
  - table-based, very light modelling
  - “worst-case” analysis by default
  - complementary models (e.g. FTA) not integrated

  è lack of precision, too pessimistic



- Emerging trends: **MODEL-BASED Ⓟ model, reason then generate**
  - Infrastructure modelling:
    - Information flow, using zones/conduits segmentation
    - Tools: threat dragon, Threagile, Microsoft Threat Modelle
  - Attack (defense) trees:
    - connecting business and technical level
    - mixing bottom-up and top-down
      + further change impact of system (new threats)
  - Goal-oriented modelling
    - Reasoning at organization level about intent, impact, avoidance, regulation
    - GORE languages: i*, KAOS, GRL, GSN…



- Extra benefits: reuse, collaboration, integration in DevSec

Lessons Learned #3 – Need for **Tool Support**

- Required for realistic risk analysis
  - Main limiting bottleneck: managing consistency/completeness in growing document
  - Model-based approach: work in model and generate document

- Tool types
  - Method specific, e.g. Risk Manager (EBIOS, FR), Monarc (L)
  - Generic platform, e.g. OpenCert [AMASS, Polarsys, 2018]

- Collaboration dimension
  - Though workflow and/or model
  - Internal to break silos, e.g. safety/security coengineering
  - Wider, e.g. between regulators and regulees for NIS [Mayer,2020)
  - DevSecOp Integration

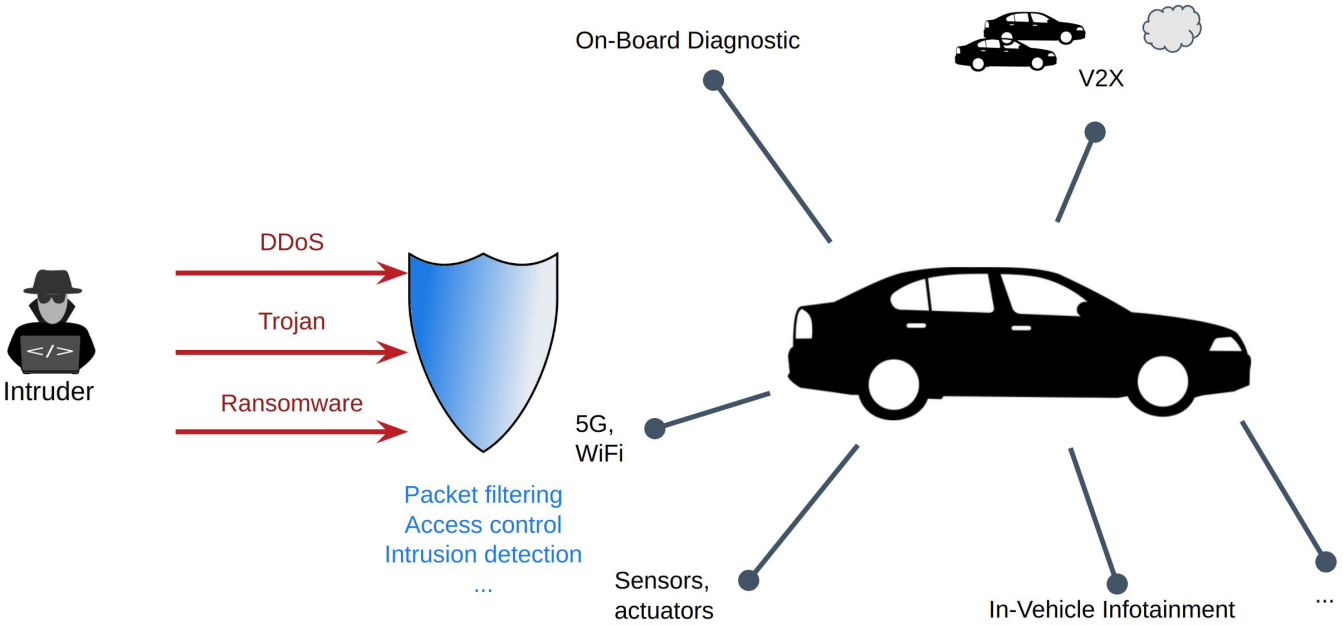
Etudes de cas

- Etude de cas « opérationnelle »: peloton de voiture (platooning)
  - Proto CETIC issu du projet EU Sparta
  - En cours sur le défi 1, focus essentiellement sur les techniques de fuzzing
  - Monter à la couche système pour identifier les interfaces, faiblesses dans les interactions entre sous-systèmes, avec acteurs humains,…
  - Utilisation d'honeypot, approche DevSecOps déjà en cours
  - Domaine: automobile

- Etudes de cas complémentaires: ouverte aux débat/propositions
  - Intérêt norme, e.g. NIS2
  - Intérêt domaine, e.g. systèmes contrôle industriel IT/OT, orienté data, critiques médicaux (risques spécifiques)

Présentation de l'étude de cas - Platooning

Connected vehicles security



- vehicles are getting more and more connected, which increases their attack surface, making them more vulnerable
- increased computing capabilities in cars allow better protection strategies to counter those new threats

V2X - vehicle to vehicle, vehicle to infrastructure, vehicle to manufacturer, ...

Case Study - Platooning

Platooning with connected vehicles

One **leader** vehicle is followed by N other vehicles (« **followers** »).

The vehicles can exchange information on a **V2V** (vehicule to vehicule) interface and/or the follower can uses sensors to keep distance and direction.

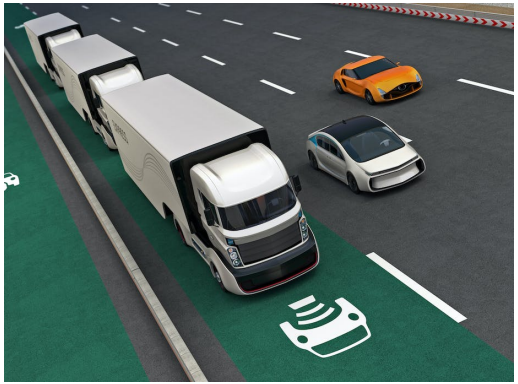
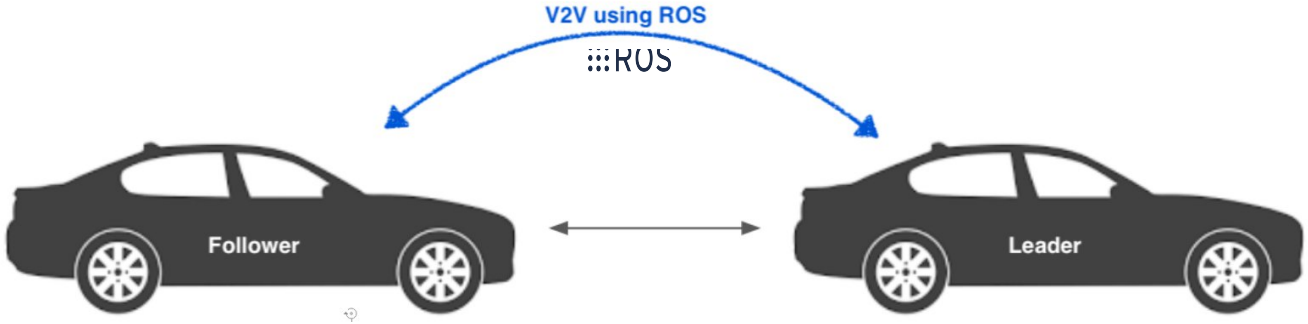
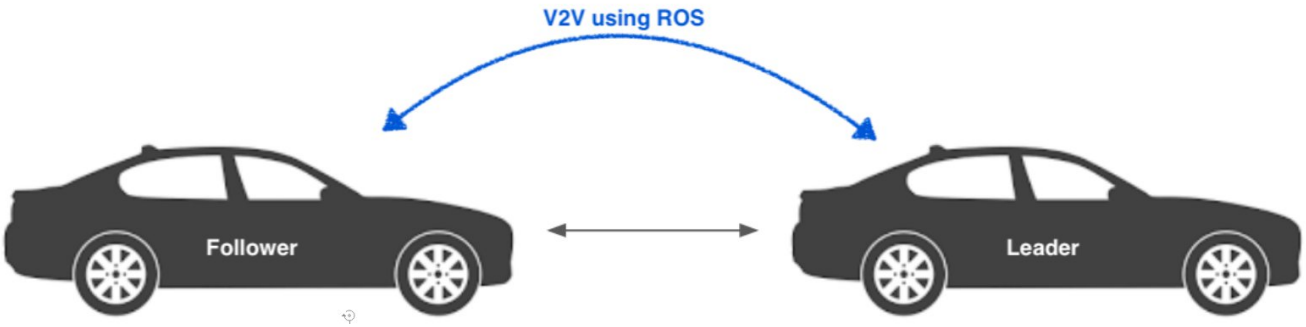


Image source: https://theconversation.com/coming-soon-to-a-highway-near-you-truck-platooning-87748



Case Study - Platooning

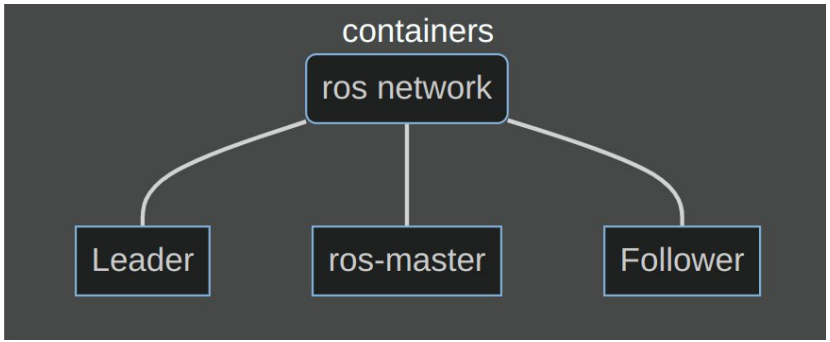
Platooning security vulnerabilities



Any intrusion in the communication can have serious consequences

ROS Protocol v1 :

- Publish/Subscribe mechanism with topics
- Use a master to manage communication
- **No encryption**
- **No authentication**
- Basically **No security**

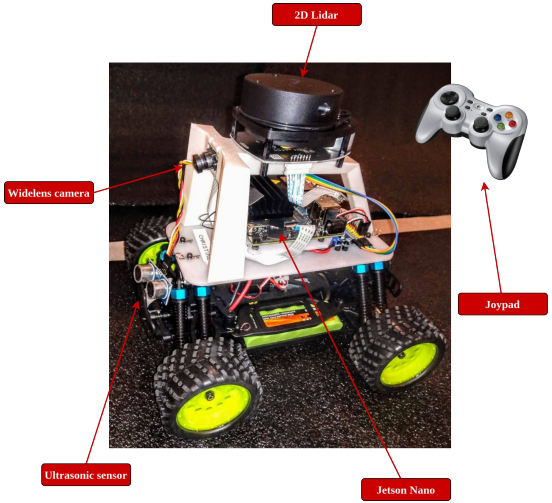


Case Study - Platooning

Exploiting Vulnerabilities

The attacker uses this vulnerability to modify the car behavior and create an accident:

- *forces acceleration, brake, steering*
- *poison camera sensor input*
- *impersonate leader or infrastructure*

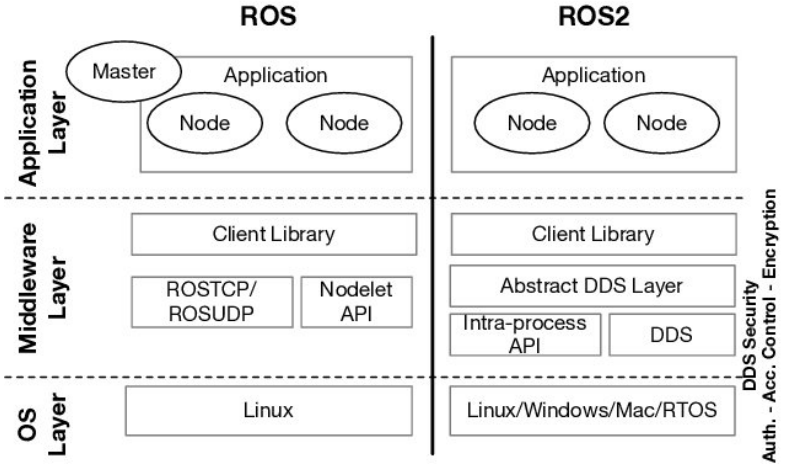


https://youtu.be/fZ8goQkyGUs

Case Study - Platooning

Testing a **protected** system for vulnerabilities and defects

ROS



Mazzeo, Giovanni & Staffa, Mariacarla. (2020). TROS: Protecting Humanoids ROS from Privileged Attackers. International Journal of Social Robotics. 12. 10.1007/s12369-019-00581-4.

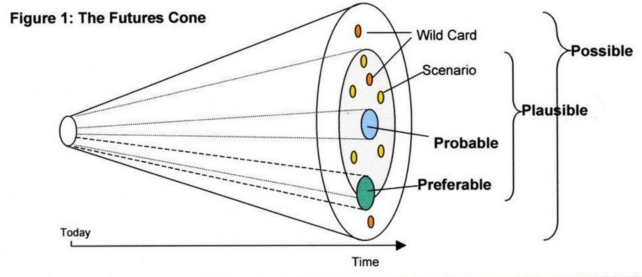
ROS2 introduces:

- security - AuthN, AuthZ, communication encryption
- real time
- distributed processing
- resilience & robustness
- ...

Case Study - Platooning

Protecting a system using plausibility analysis

Remote Access Software (MITRE T1219)
Data Manipulation (MITRE T1565)



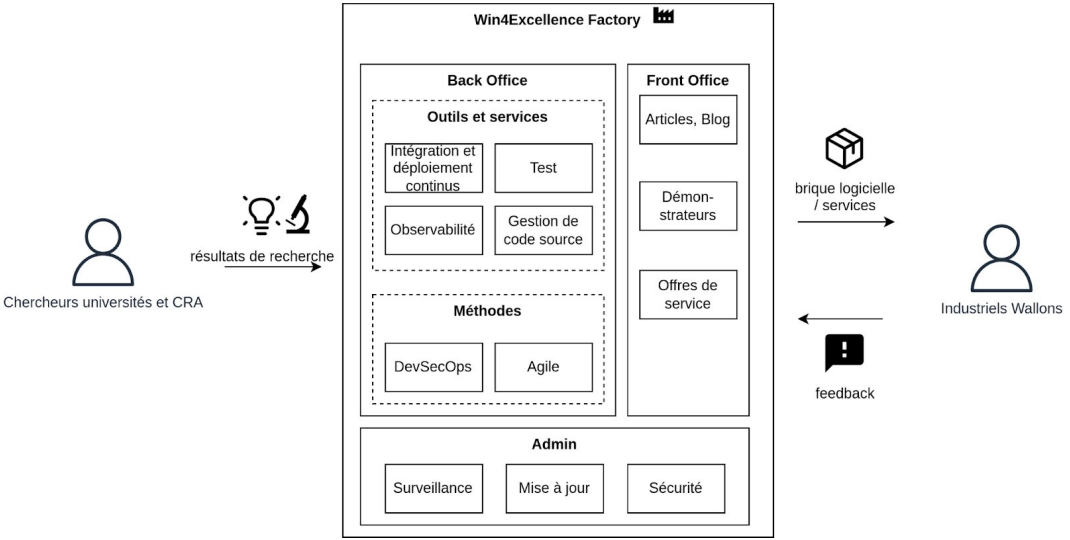
The cone of plausibility (adapted from Taylor, 1993; image retrieved from http://thinkingfutures.net/)

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	10 techniques	3 techniques	13 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Detect Operating Mode		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	I/O Image		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

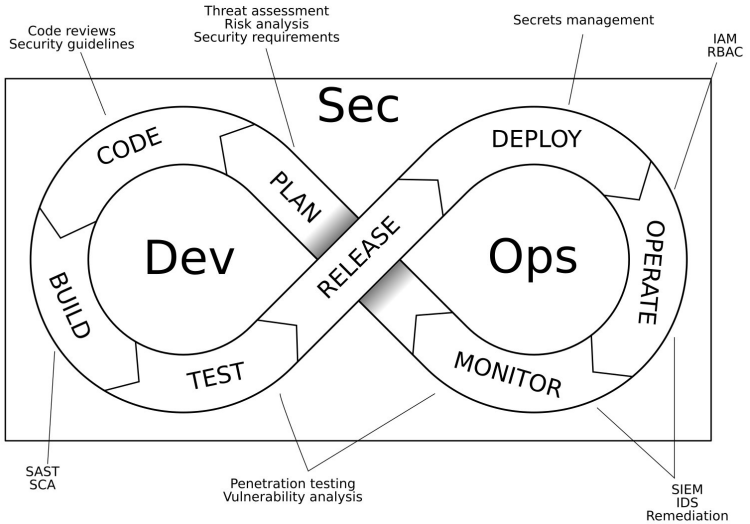
MITRE | ATT&CK®

Knowledge base of adversary tactics and techniques based on real-world observations

Case Study implementation - The Cyber Factory



La Cyber Factory est une usine logicielle (ou *Software Factory* en anglais). Cette plateforme matérielle et logicielle est utilisée sur les projets Win4Excellence pour favoriser la collaboration entre les acteurs de la recherche et de l'industrie wallons, et contribuer à la diffusion des résultats de recherche de ces projets.



DevSecOps - increase quality, speed and security

Discussion

- Type de vulnérabilités
  - HW, SW, humaines…
  - Sources: CVE, SOC, autoscan, honeypots…
- Conception des scénarios d'attaques pour pentest
  - Personnes: interne <-> consultant ? Formation ?
  - Niveau de « formalisation »: infra, notations…
  - Lien avec les frameworks/outils d'analyse de risques/threat modelling
- Evaluation
  - % oubli/apparition/aggravation de risques
  - Métriques Ⓟ monitoring
- …

Planning réunion de groupe de travail par Défi

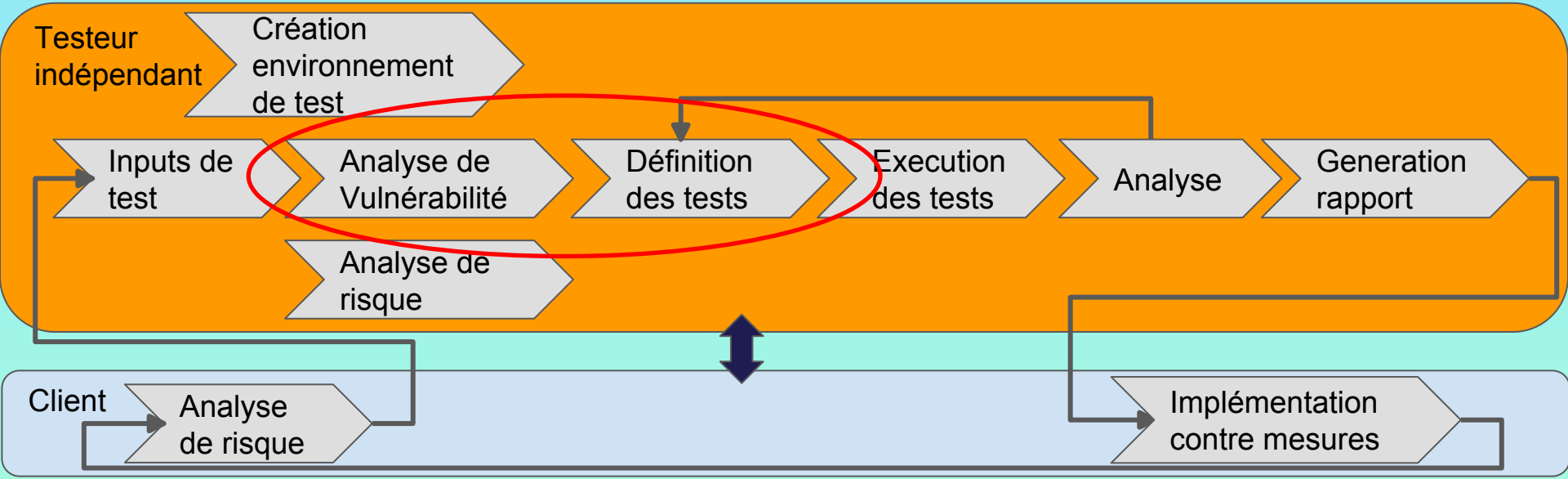
Date	Description
25/01/2023	Première réunion du groupe de travail
*/06/2023 ou */09/2023	Présentation des recherches et discussion sur les démonstrateurs
*/01/2024	Présentation des démonstrateurs
*/06/2024	Présentation des démonstrateurs finaux

Qui participe:

- Entreprises intéressées par le défi
- Responsable de défi
- Chercheurs contribuant au défi
- WSL

Merci de votre attention

Processus de Tests de Pénétration (https://www.cetic.be/CYRUS-EN)



Classes Outils

Network mapping with scanner
Database Scan
SAST
DAST & WAST
Fuzzing Tools
Wireless attacks
Compliance assessment
Sniffing
MITM
Vulnerability analysis
Firmware analysis
Password attacks
Exploitation tools
Hardware
Forensics