CYBER RANGE SCENARIOS

Mapping MITRE ATT&CK and D3FEND to the ECSF for cyber range scenarios generation

UCLouvain

Benoît Duhoux, Lionel Metongnon, Justine Ramelot, Daniela Magalhaes Azevedo, Ramin Sadre, Suzanne Kieffer, Axel Legay

cetic
Your Connection to ICT Research

***Sébastien Dupont**, Laurent Gravez, Malik Bouhou, Maher Badri, Philippe Massonet*

RHEA GROUP

Matteo Merialdo, Artem Korytnyi

Wallonie recherche SPW

A Win2Wal project

CYBER RANGE SCENARIOS

Talk outline

Context and motivation

- Cyber ranges, challenges for creating training scenarios
- ENISA Cybersecurity Skills Framework (ECSF)
- Mapping MITRE and ECSF

Illustration - A sample training scenario

- Securing a software supply chain

Conclusion and perspectives

CYBER RANGE SCENARIOS

Training ground

for security activities

Cyber Range Scenarios

Attack and defense exercises on vulnerable assets

Motivation

CYBER RANGE SCENARIOS

Challenge: How to design training scenarios?

- need experts
- understand user needs
- time-consuming
- not really reusable

Motivation

CYBER RANGE SCENARIOS

⇒ Need for a solution to facilitate the work of cyber range scenario designers.

Scenarios constraints:

- within a certain budget, duration
- specific software or hardware architecture
- trainee skills improvement objectives
- …

How to measure cyber competence?

CYBER RANGE SCENARIOS

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

ECSF

12 Cyber profiles and associated competences

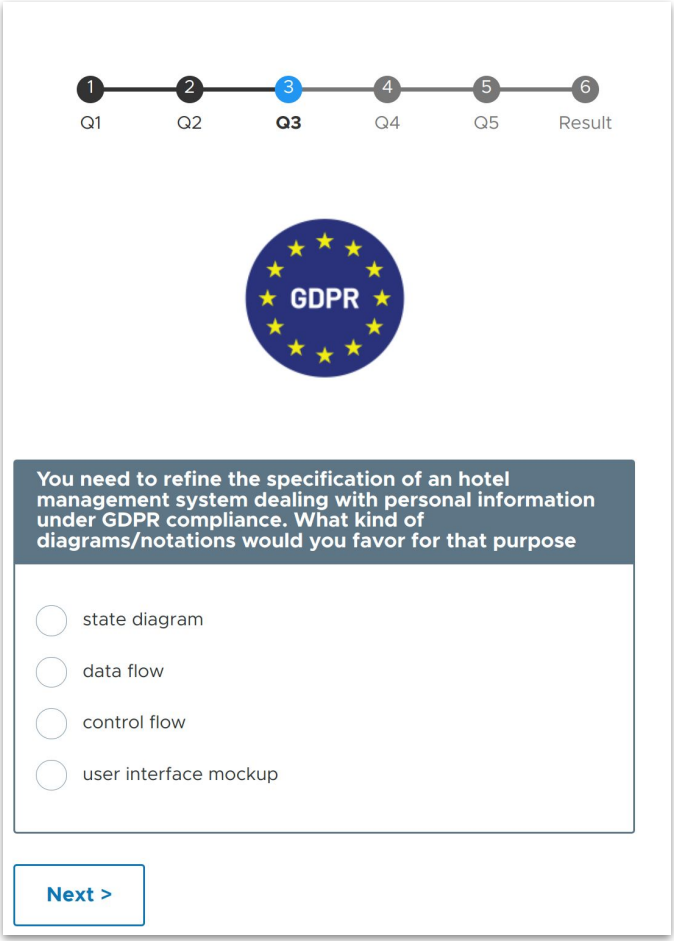
"The main purpose of this framework is to create a common understanding between individuals, employers and providers of learning programmes across EU Member States, making it a valuable tool to bridge the gap between the cybersecurity professional workplace and learning environments."

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

How to measure cyber competence?

CYBER RANGE SCENARIOS



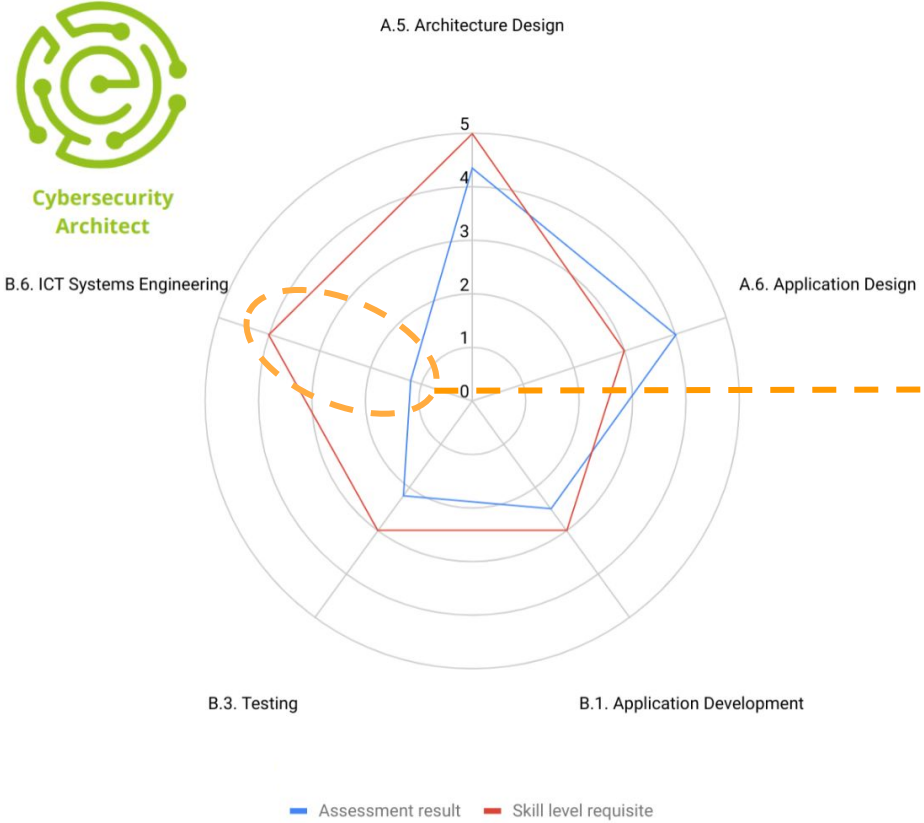
Cyber Competence Assessment

Special thanks to Denis Darquennes for his GDPR expertise

Cyber competence assessment

CYBER RANGE SCENARIOS

Cybersecurity Architect



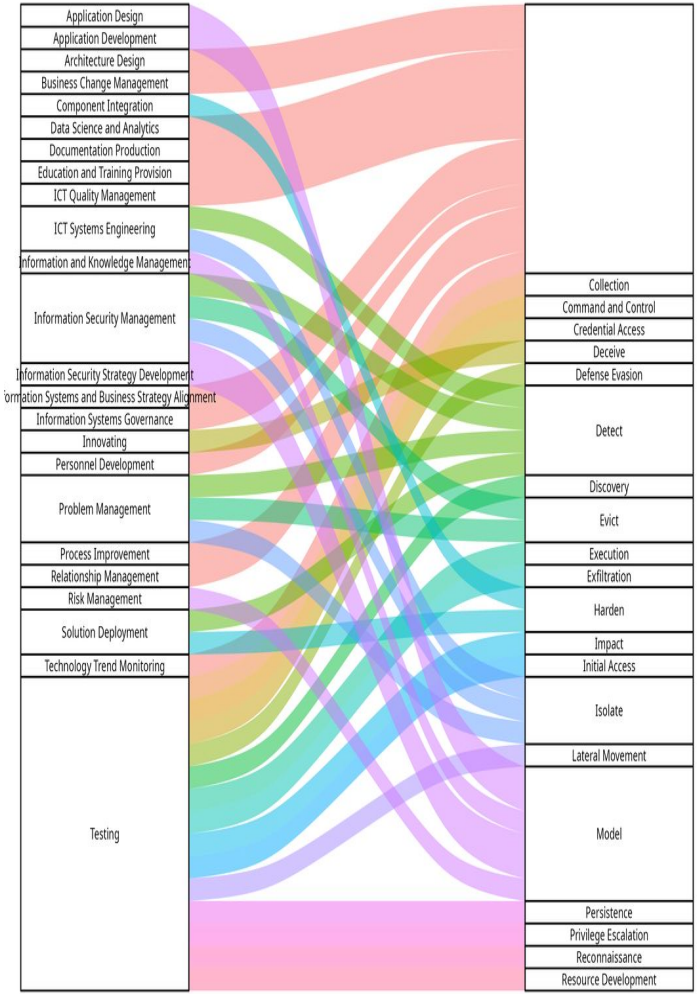
B.6. ICT Systems Engineering
Builds the required networks/network connections, components and interfaces. (...) Ensures information security, data protection and energy efficiency. Performs tests to ensure requirements are met.

Competence level:
- **required: 4**
- **measured: 1.2**

ECSF Competences vs MITRE tactics

CYBER RANGE SCENARIOS

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

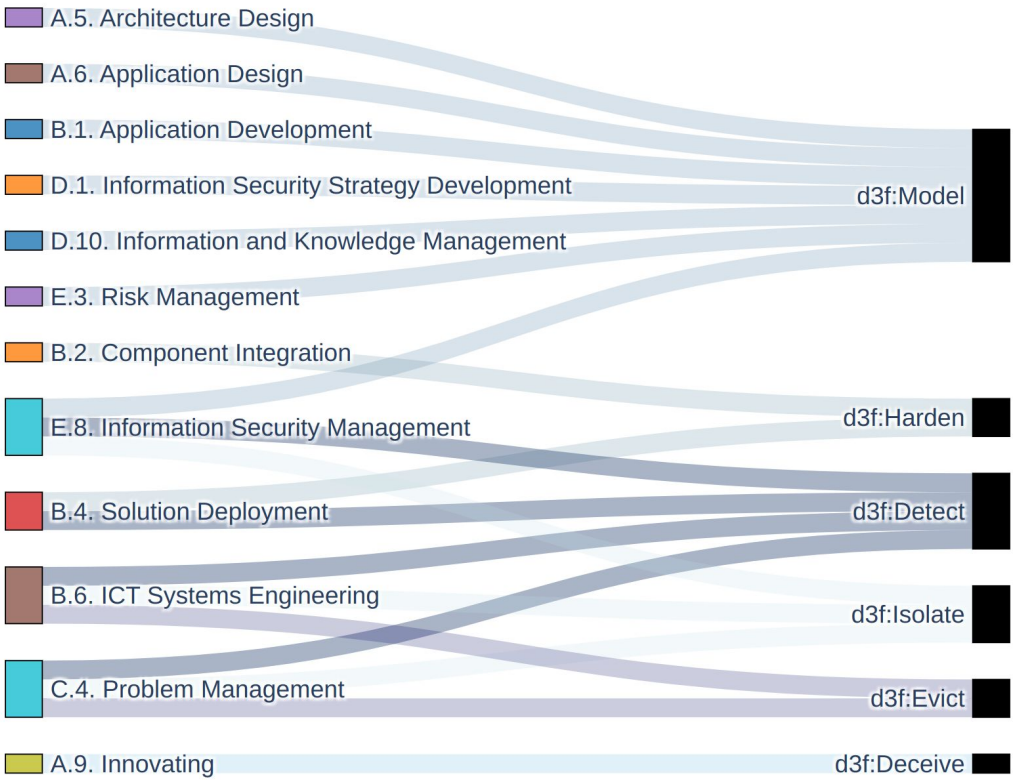


MITRE ATT&CK®

DEFEND™

ECSF Competences vs MITRE D3FEND tactics

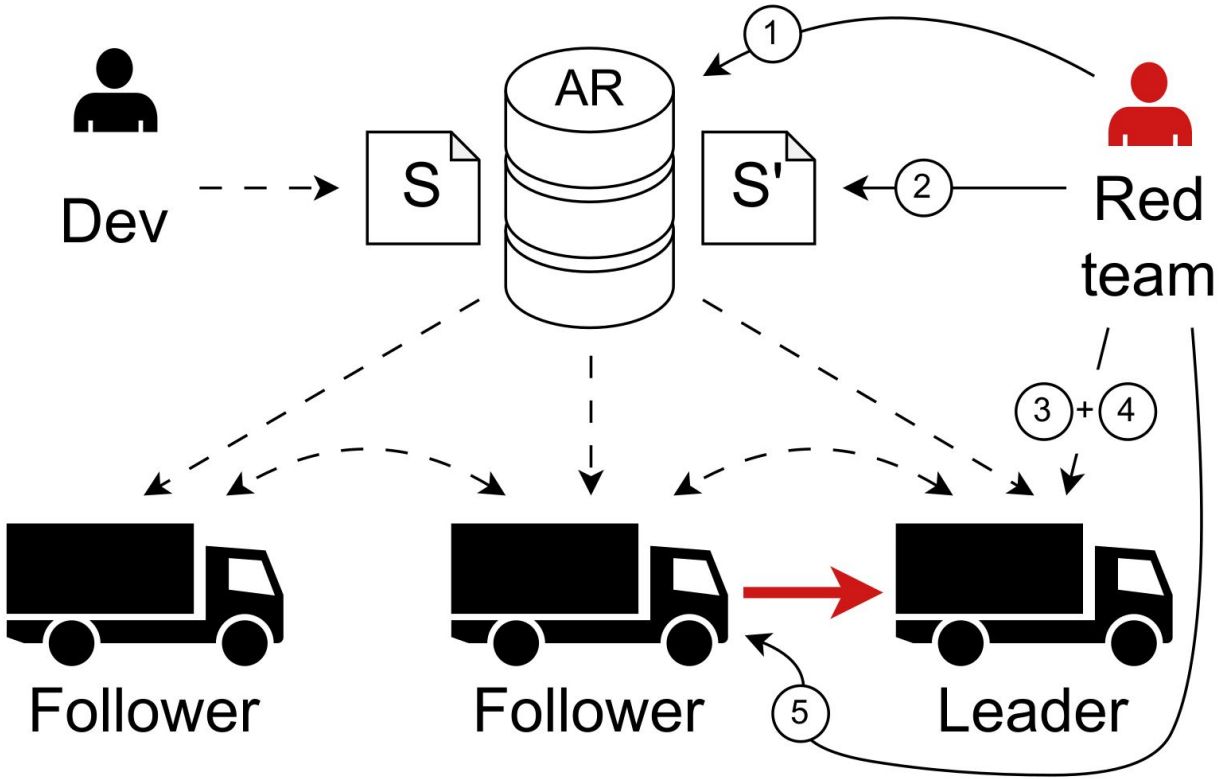
CYBER RANGE SCENARIOS



MITRE DEFEND™

Attack scenario

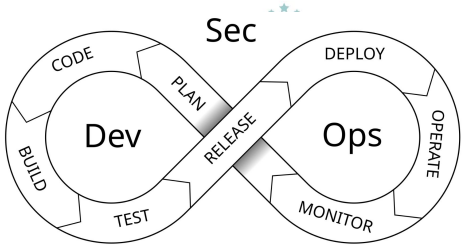
Inject backdoor in software update

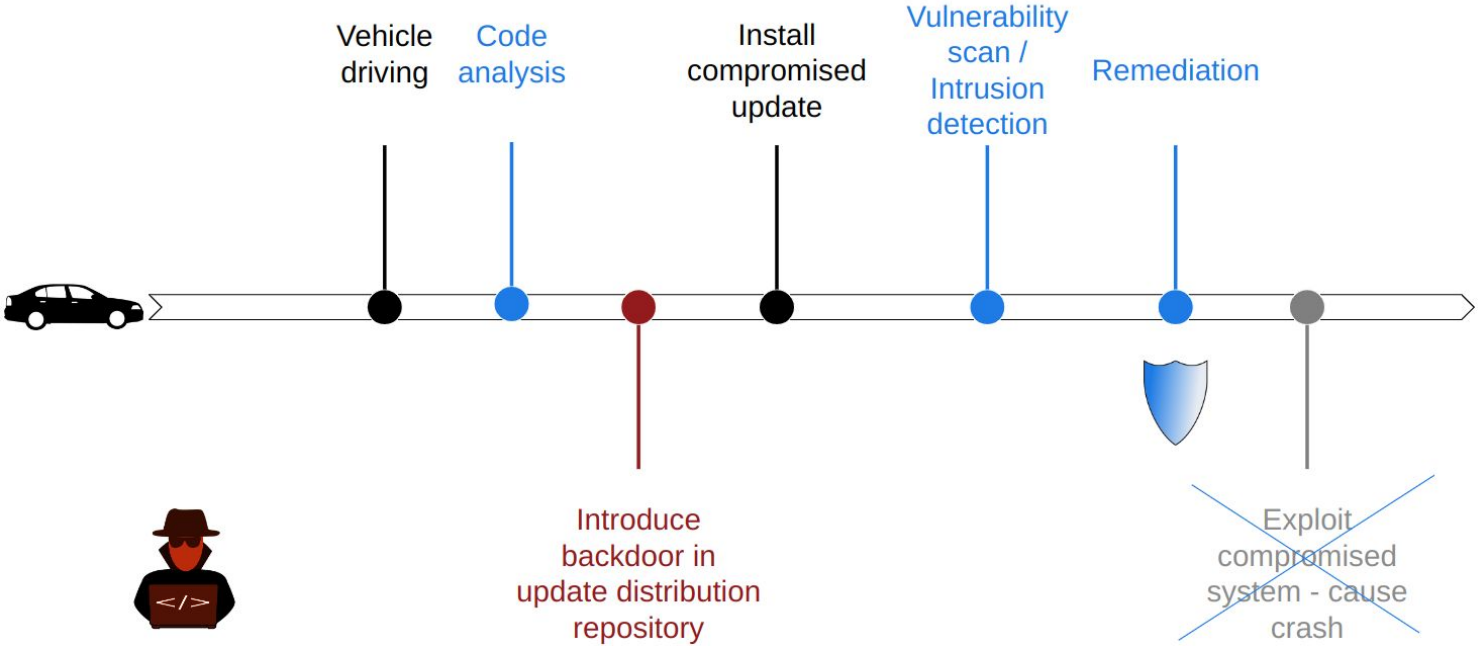


1. obtain credentials
2. release a compromised version
3. take control of the leader
4. impersonate the leader
5. send a false acceleration command

Defense scenario

DevSecOps good practices





MITRE techniques for an ECSF profile

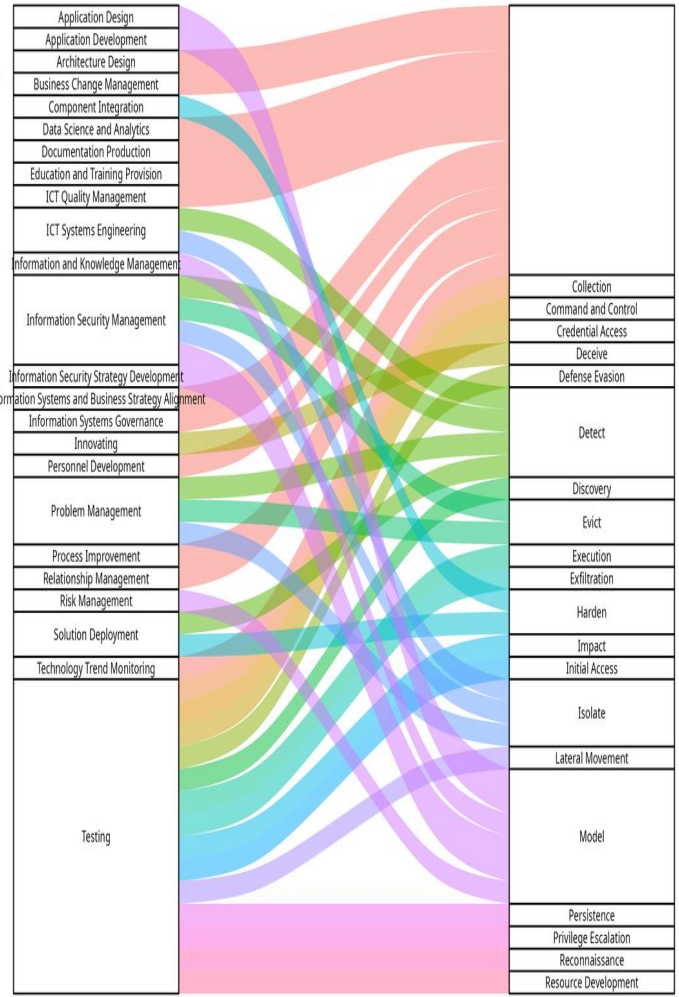
CYBER RANGE SCENARIOS

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

MITRE ATT&CK DEFEND

Cybersecurity Architect

Penetration Tester



Persistance / Impact / C&C:

- Compromise Client Software Binary (MITRE T1554)
- Remote Access Software (MITRE T1219)
- Data Manipulation (MITRE T1565)

Detect:

- File Metadata Hash Verification (MITRE DS0022)
- Network Traffic Content (MITRE DS0029)

Isolate / Evict :

- Code signing (MITRE M1045)
- Filter Network Traffic (MITRE M1037)
- Network Segmentation (MITRE M1030)
- Encrypt sensitive information (MITRE M1041)

Scenario software and vulnerabilities

CYBER RANGE SCENARIOS

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

Cyber profiles, competences

CVE®

Vulnerabilities:

- CVE-2019-9630
- CRS-2022-0001
- CRS-2022-0002
- CRS-2022-0003

CVE-2019-9630 Detail

Description

Sonatype Nexus Repository Manager before 3.17.0 has a weak default of giving any unauthenticated user read permissions on the repository files and images.

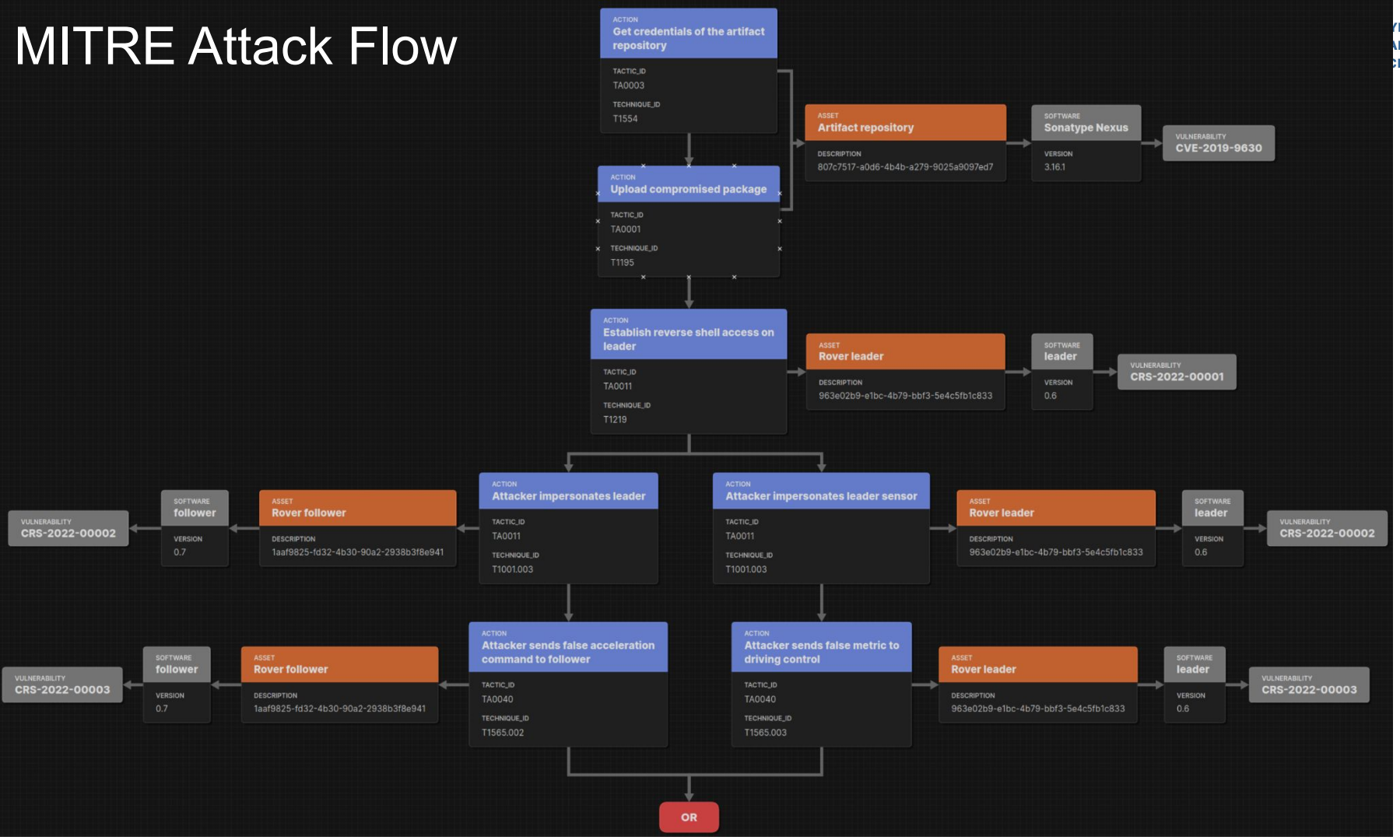
MITRE ATT&CK® DEFEND™

Techniques, tactics

Software:

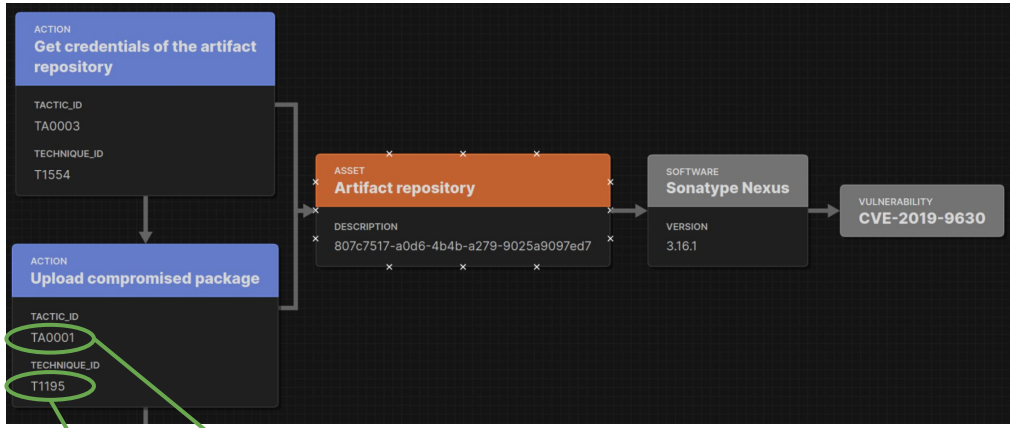
- Sonatype Nexus (Vulnerabilities)
- Leader/Follower (Vulnerabilities) ROS
- Metasploit (Attack)
- Falco (Mitigation/Detection)
- The Hive (Mitigation)
- Vacsine (Mitigation)

MITRE Attack Flow



MITRE Attack Flow

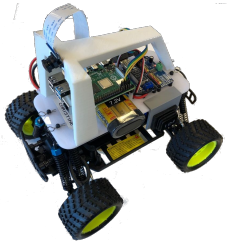
CYBER RANGE SCENARIOS

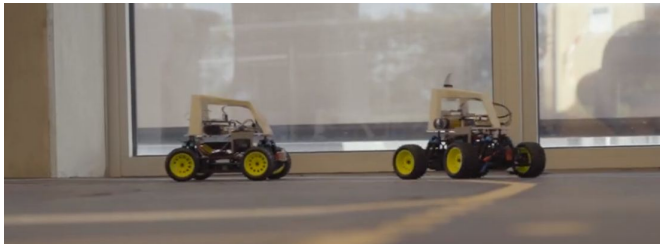


Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation
10 techniques	8 techniques	9 techniques	14 techniques	19 techniques	13 techniques
Active Scanning (3)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Exploit Public-Facing Application	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)
Gather Victim Identity Information (3)	Compromise Accounts (3)	External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)
Gather Victim Network Information (6)	Compromise Infrastructure (7)	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)
Gather Victim Org Information (4)	Develop Capabilities (4)	Phishing (3)	Exploitation for Client Execution	Browser Extensions	Create or Modify System Process (4)
Phishing for Information (3)	Establish Accounts (3)	Replication Through Removable Media	Inter-Process Communication (3)	Compromise Client Software Binary	Domain Policy Modification (2)
Search Closed Sources (2)	Obtain Capabilities (6)	Supply Chain Compromise (3)		Create Account (3)	
	Stage Capabilities (6)	Trusted Relationship	Native API		

Validation: Cyber Physical Systems testbed

CYBER RANGE SCENARIOS





- Chassis: Donkey Car
- Brain: RaspBerry Pi / Jetson Nano
- Sensors:
  - 2D Lidar
  - Ultrasonic
  - Wide Lens camera
- https://www.ros.org/ ROS

- RHEA Group's Cyber Integration, Test and Evaluation Framework

RHEA GROUP

CITEF

Conclusion

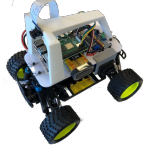
CYBER RANGE SCENARIOS

MITRE ATT&CK® DEFEND™

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

CVE®

CITEF



Training scenario generation driven by user's needs through cyber competences

Perspectives:

- training session feedback and recommendations
- Defend scenario flow
- non-IT profiles

Sébastien Dupont, Expert Research engineer @CETIC

https://www.cetic.be/Sebastien-Dupont?lang=en

https://www.linkedin.com/in/s%C3%A9bastien-dupont-91424326/

sebastien.dupont@cetic.be