

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

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

Dcetic

RHER Matteo Merialdo, Artem Korytnyi

A Win2Wal project



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



Training ground

for security activities

Cyber Range Scenarios

Attack and defense exercises on vulnerable assets



Challenge: How to design training scenarios?

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



⇒ 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?



Compliance Officer

Auditor

Cybersecurity

Researcher

Penetration

Tester

01010 11101 00101



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."



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



How to measure cyber competence?





Cyber Competence Assessment





Cyber competence assessment





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



	Application Design
Aj	plication Development
	Architecture Design
Busir	ness Change Management
0	omponent Integration
Da	ta Science and Analytics
Do	cumentation Production
Educa	tion and Training Provision
IC	T Quality Management
IC	T Systems Engineering
Informatio	n and Knowledge Manageme
Inform	ation Security Management
Informatio	Security Strategy Developme
ormation Syst	ems and Rusiness Strategy Ali
Inform	nation Systems Governance
	Innovating
Р	ersonnel Development
	Problem Management
	,
	Process Improvement
Re	lationship Management
	Risk Management
	Solution Deployment
Tock	nology Trand Manitoring
leci	nology nena monitoring
	Testing
	resting





ECSF Competences vs MITRE D3FEND tactics

01

3

fo

SKILLS FRAMEWORK

자

EUROPEAN

CYBERSECURITY

02





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





SKILLS FRAMEWORK



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 profiles, competences



CYBER RANGE SCENARIOS

Vulnerabilities:

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

Ň

6

逊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.



Techniques, tactics

Software⁻

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

MITRE Attack Flow



MITRE Attack Flow



TACTIC.ID TA0003 TECHNIQUE_ID T1554	ļ	ASSET Artifact repository DESCRIPTION	SOFTWARE Sonaty Version	pe Nexus	ү 9-9630
ACTION Upload con TACTIC_ID TACOOT TECHNIQUE_ID T1195	mpromised package	X X	×		
\backslash	$\langle \rangle$				
Reconnaissance	Resource	Initial Access	Execution	Persistence	Privilege Escalation
Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques
Reconnaissance 10 techniques Active Scanning (3)	Resource Development 8 techniques Acquire Access	Initial Access 9 techniques Drive-by Compromise	Execution 14 techniques Cloud Administration Command	Persistence 19 techniques	Privilege Escalation 13 techniques Abuse Elevation Contro Mechanism (4)
Reconnaissance 10 techniques Active Scanning (3) Gather Victim Host nformation (4)	Resource Development 8 techniques Acquire Access Acquire Access Acquire Access	Initial Access 9 techniques Drive-by Compromise Exploit Public-Facing Application	Execution 14 techniques Cloud Administration Command and Scripting	Persistence 19 techniques 1 Account Manipulation (5) BITS Jobs	Privilege Escalation 13 techniques Abuse Elevation Contro Mechanism (4) Manjoulation (5)
Reconnaissance 10 techniques Active Scanning (3) Gather Victim Host Information (4) Gather Victim Identity Information (3)	Resource Development 8 techniques Acquire Access n Acquire Infrastructure (s Accounts (s)) n Acquire Infrastructure (s Accounts (s))	Initial Access 9 techniques 9 techniques Drive-by Compromise Application External Remote Services	Execution 14 techniques Cloud Administration Command and Scripting Interpreter (9) Container Administration	Persistence 19 techniques Account Manipulation (5) BITS Jobs BITS Jobs Boot or Logon Autostart Execution (14)	Privilege Escalation 13 techniques Abuse Elevation Contro Mechanism (4) Access Token Manipulation (5) Boot or Logon Autostar
Reconnaissance 10 techniques Active Scanning (3) Gather Victim Host Information (4) Gather Victim Identity Information (3) Gather Victim Network	Resource Development 8 techniques Acquire Access n Compromise Infrastructure (7)	Initial Access 9 techniques Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions	Execution 14 techniques Cloud Administration Command and Scripting Interpreter (9) Container Administration Command	Persistence 19 techniques 19 techniques 10 Account Manipulation (5) BITS Jobs BITS Jobs 11 Boot or Logon Autostart Execution (14) 12 Boot or Logon	Privilege Escalation 13 techniques Abuse Elevation Contro Mechanism (4) Access Token Manipulation (5) Boot or Logon Autostar Execution (14)
Reconnaissance 10 techniques Active Scanning (3) Gather Victim Host Information (4) Gather Victim Identity Information (3) Gather Victim Network Information (6) Control Victim Ocn	Resource Development 8 techniques Acquire Access I Acquire Infrastructure (8 Accounts (3) I Compromise Accounts (3) I Compromise Infrastructure (7) I Develop Capabilities (4)	Initial Access 9 techniques Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions 1 Phishing (3) Dedication Through	Execution 14 techniques Cloud Administration command and Scripting Interpreter (9) Container Administration command	Persistence 19 techniques 19 techniques Manipulation (5) BITS Jobs BITS Jobs Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (5)	Privilege Escalation 13 techniques 14 Abuse Elevation Contro Mechanism (4) 16 Access Token Manipulation (5) 17 Boot or Logon Autostar Execution (14) 18 Boot or Logon Initialization Scripts (5)
Reconnaissance 10 techniques Active Scanning (3) Gather Victim Host Information (4) Gather Victim Identity Information (3) Gather Victim Network Information (6) Gather Victim Org Information (4)	Resource Development 8 techniques Acquire Access I Acquire Infrastructure (8 Accounts (3) I Compromise Accounts (3) I Compromise Infrastructure (7) I Develop Capabilities (4) I Establish Accounts (3)	Initial Access 9 techniques Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions I Phishing (3) Replication Through Removable Media	Execution 14 techniques Cloud Administration Command and Scripting Interpreter (9) Container Administration Command Deploy Container Exploitation for Client Execution	Persistence 19 techniques 19 techniques 10 Account Manipulation (5) BITS Jobs 10 Boot or Logon Autostart Execution (14) 10 Boot or Logon 11 Initialization Scripts (5) Browser Extensions 2 Comparise Olivert	Privilege Escalation 13 techniques 14 Abuse Elevation Contro Mechanism (4) 15 Abuse Slevation Contro Manipulation (5) 16 Boot or Logon Autostar Execution (14) 17 Boot or Logon Initialization Scripts (5) 10 Create or Modify
Reconnaissance 10 techniques Active Scanning (3) Gather Victim Host Information (4) Gather Victim Identity Information (3) Gather Victim Network Information (6) Gather Victim Org Information (4) Phishing for Information (3)	Resource Development 8 techniques Acquire Access n Acquire Access n Acquire Access n Compromise Infrastructure (7) n Develop Capabilities (4) n Establish Accounts (3) n Obtain Capabilities (6)	Initial Access 9 techniques Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions I Phishing (3) Replication Through Removable Media I Supply Chain I Compromise control	Execution 14 techniques Cloud Administration Command and Scripting Interpreter (9) Container Administration Command Deploy Container Exploitation for Client Execution	Persistence 19 techniques 19 techniques 19 Techniques 10 Account Manipulation (5) BITS Jobs 10 Boot or Logon Autostart 10 Execution (14) 10 Boot or Logon 11 Initialization Scripts (5) Browser Extensions Compromise Client Software Binary	Privilege Escalation 13 techniques 13 techniques 14 Abuse Elevation Control Mechanism (4) 14 Access Token Manipulation (5) 15 Boot or Logon Autostar Execution (14) 16 Boot or Logon Initialization Scripts (5) 17 Create or Modify System Process (4) Domain Policy

Validation: Cyber Physical Systems testbed







- Chassis: Donkey Car
- Brain: RaspBerry Pi / Jetson Nano
- Sensors:
 - 2D Lidar
 - Ultrasonic
 - Wide Lens camera
 - https://www.ros.org/ IIROS
- RHEA Group's Cyber Integration, Test and Evaluation Framework





Conclusion













Perspectives:

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

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

Sébastien Dupont, Expert Research engineer @CETIC



()) <u>https://www.cetic.be/Sebastien-Dupont?lang=en</u>

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

sebastien.dupont@cetic.be



