



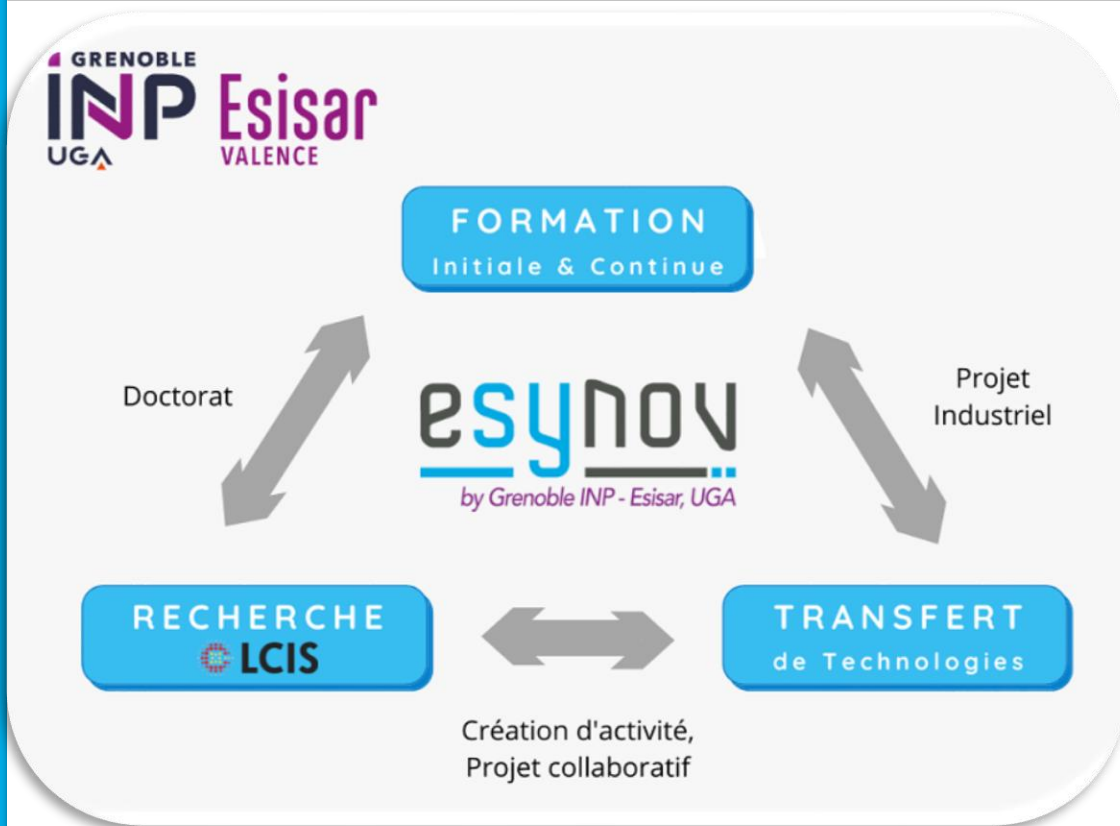
Cybersécurité des dispositifs médicaux : Du « Security by Design » jusqu'au exgiences de pentests indépendants

Mickaël SEIGNOBOS – Ingénieur Cybersécurité Produit

Activités Cybersécurité Produits

MEDI'NOV CONNECTION – 01/07/2026

Esynov : Qui sommes-nous ?



La plateforme **Esynov** mène des actions de transfert de technologies (**formation/expertise**) dans les domaines :

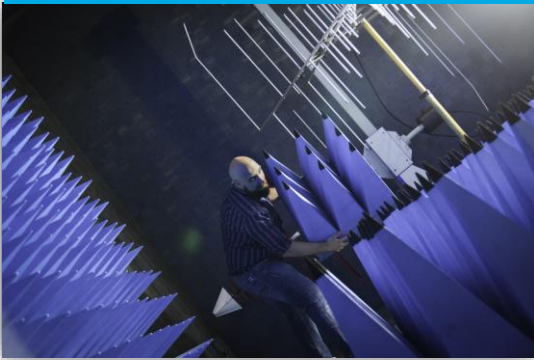
- **CEM / radiofréquence,**
- **Cybersécurité des Systèmes d'Informations,**
- **Cybersécurité produits/systèmes embarqués,**
- **Intelligence Artificielle.**

**ACCOMPAGNER LES ENTREPRISES DANS LEURS ACTIVITÉS
D'INNOVATION ET DÉVELOPPEMENT PRODUITS / R&D**

Esynov : Nos moyens techniques

Moyens CEM / Radiofréquence :

CEM Industrielle



CEM Champs forts



RFID



Moyens Cybersécurité produits :

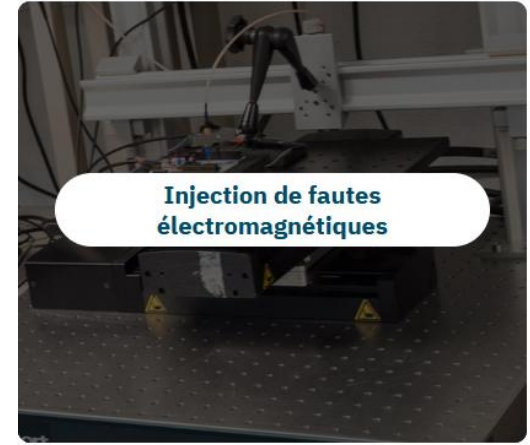
Analyse de canaux auxiliaires



Audit de la sécurité des appareils IoT



Injection de fautes électromagnétiques



La démonstration de la robustesse face aux cyberattaques apparaît dans l'ensemble du cadre réglementaire : MDR 2017/745, IEC 80001-5-1, guidance FDA, etc.

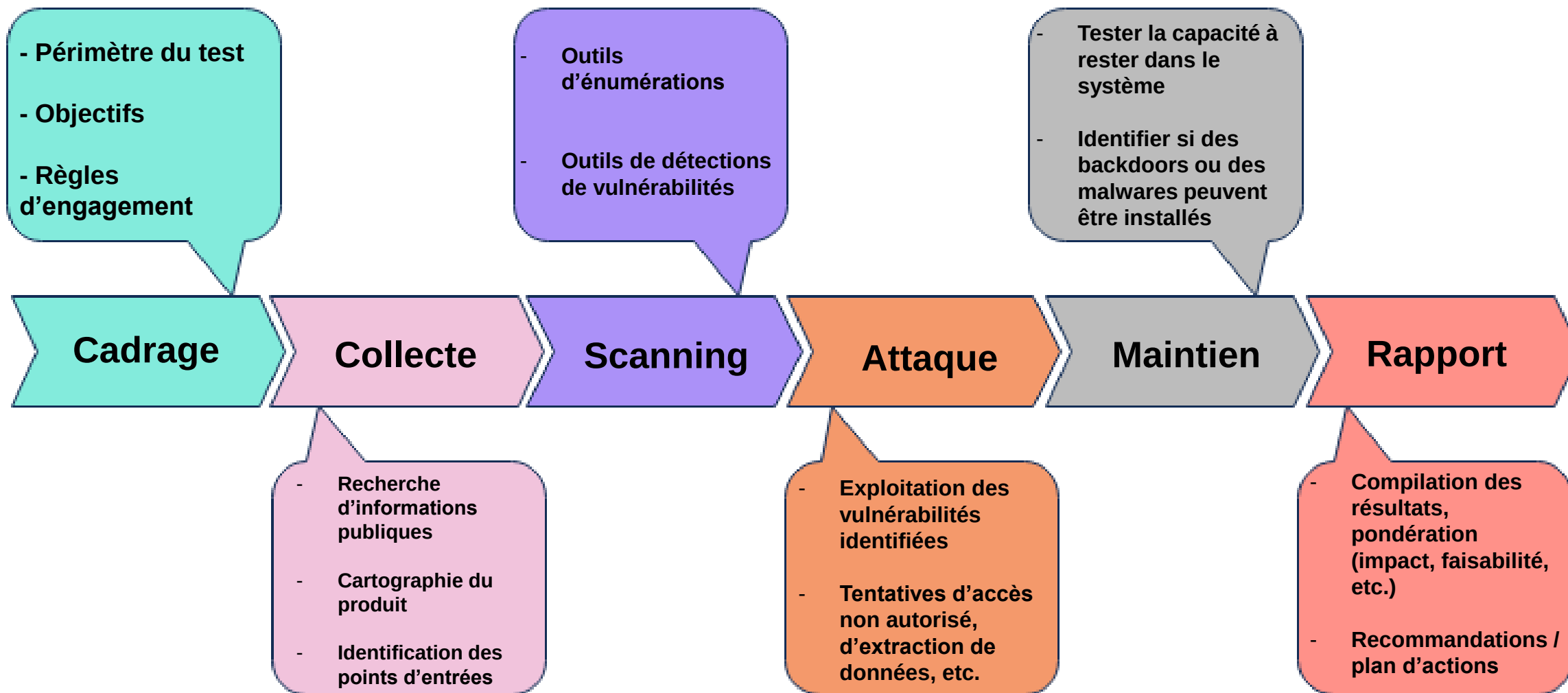
FDA Guidance September 27, 2023 :

“The testing should identify and characterize security-related issues via tests that focus on **discovering and exploiting security vulnerabilities in the product.**

Penetration test reports should provide and include the following elements :

- **Independence** and technical expertise of testers;
- Scope of testing;
- Duration of testing;
- Testing methods employed; and
- Test results, findings, and observations.”

Un pentest, concrètement c'est quoi ?



Détermination de la surface d'attaque

Firmware injection



Fuzzing

Network scanning



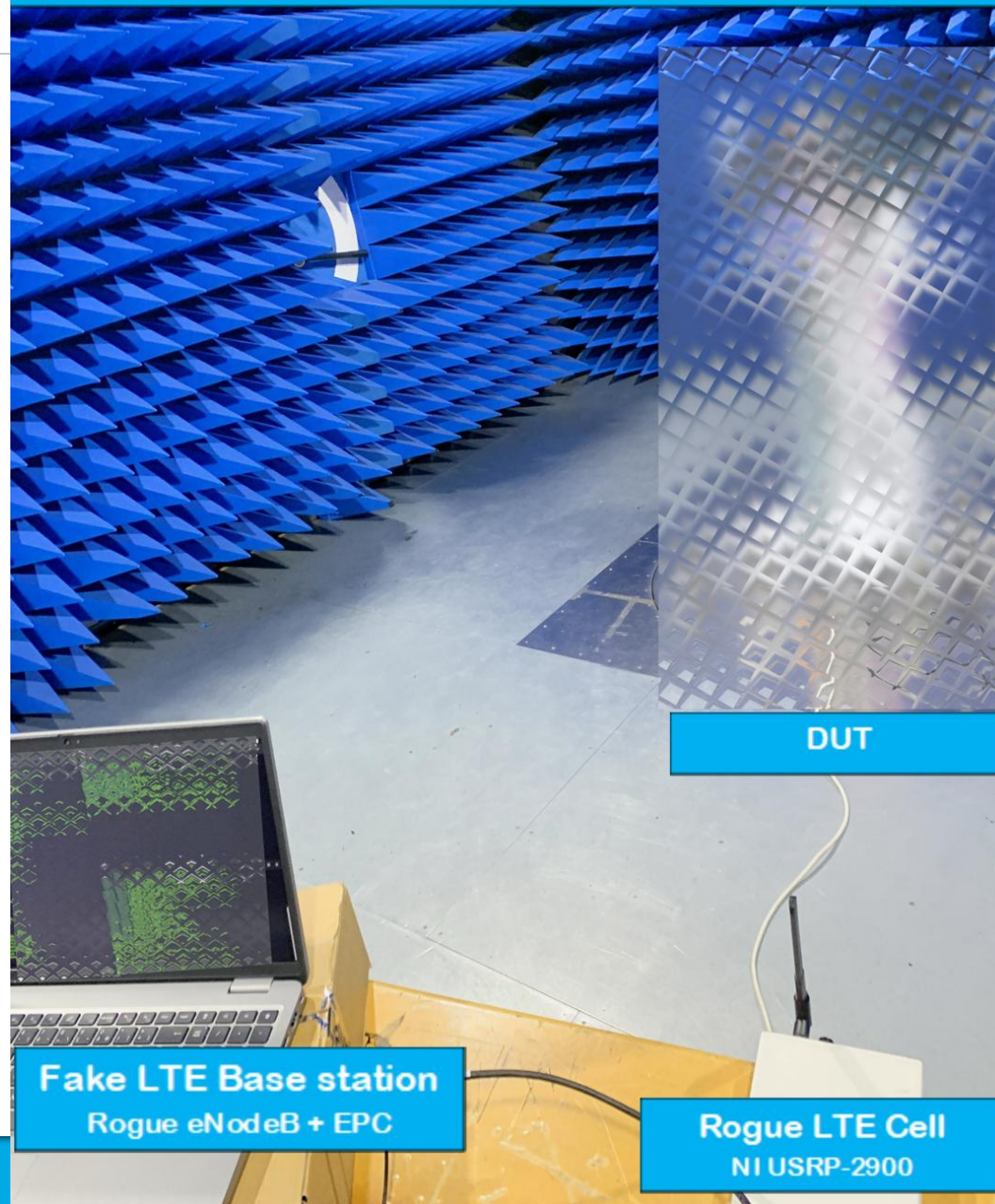
Downgrade attack
IMSI Catcher



WPA2 Deauth attack
WPA2 Dictionary Attack

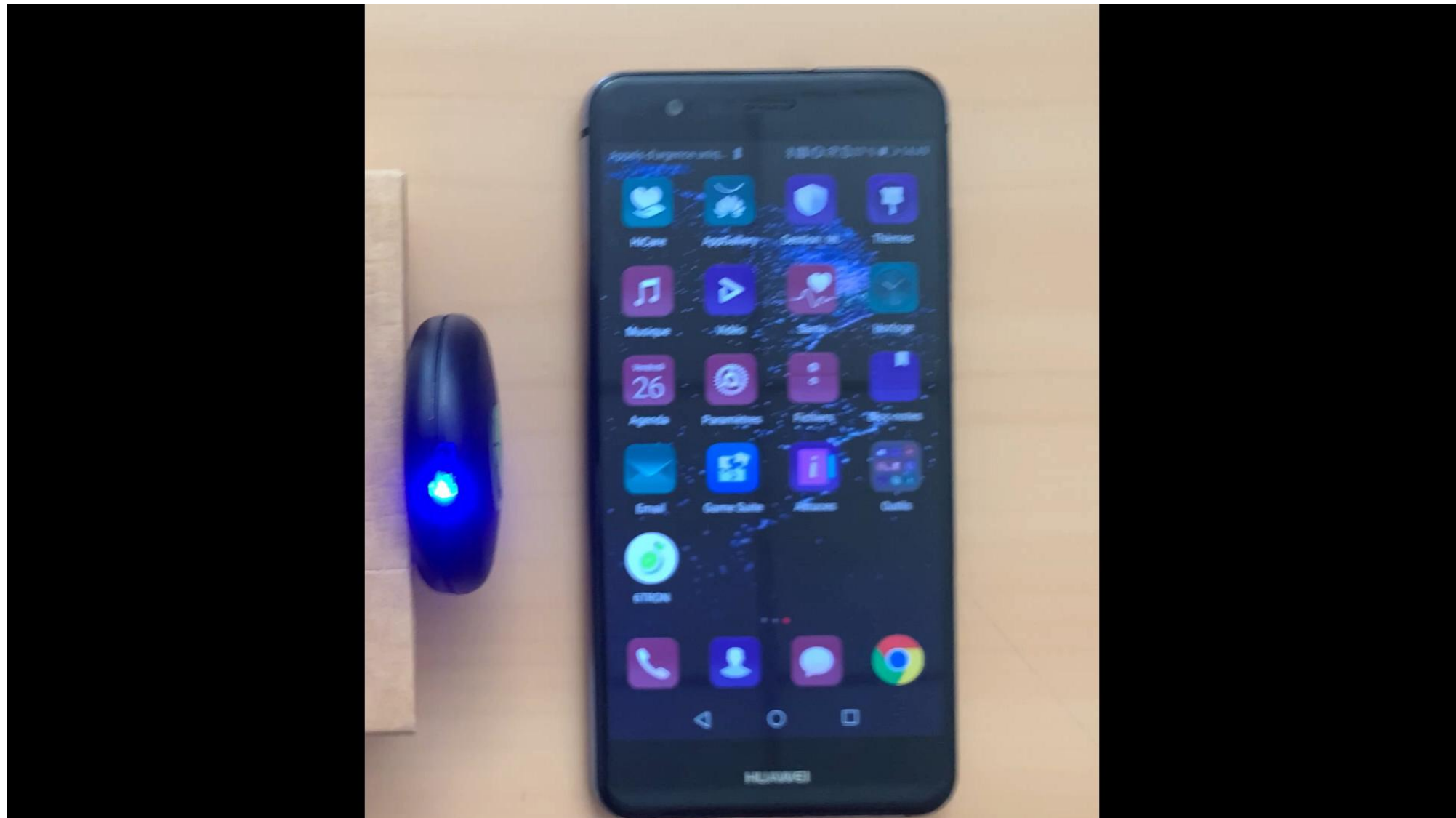


BLE Scan
BLE MitM



4G Attack - Esynov

Un exemple concret pour la phase d'attaque :



Outillage nécessaire pour une attaque sur le BLE

Downloading Free Open-Source Software :

<https://github.com/RCayre/mirage>

MIRAGE - 1.2

This framework is released as an opensource project using the MIT License.

Mirage is a powerful and modular framework dedicated to the security analysis of wireless communications. It currently provides :

- multiple lightweight and hackable wireless protocol stacks (e.g. Bluetooth Low Energy, Enhanced ShockBurst, WiFi, Zigbee ...)
- multiple highly customizable offensive modules (e.g. Man-in-the-Middle, sniffing, jamming, hijacking, cloning ...)

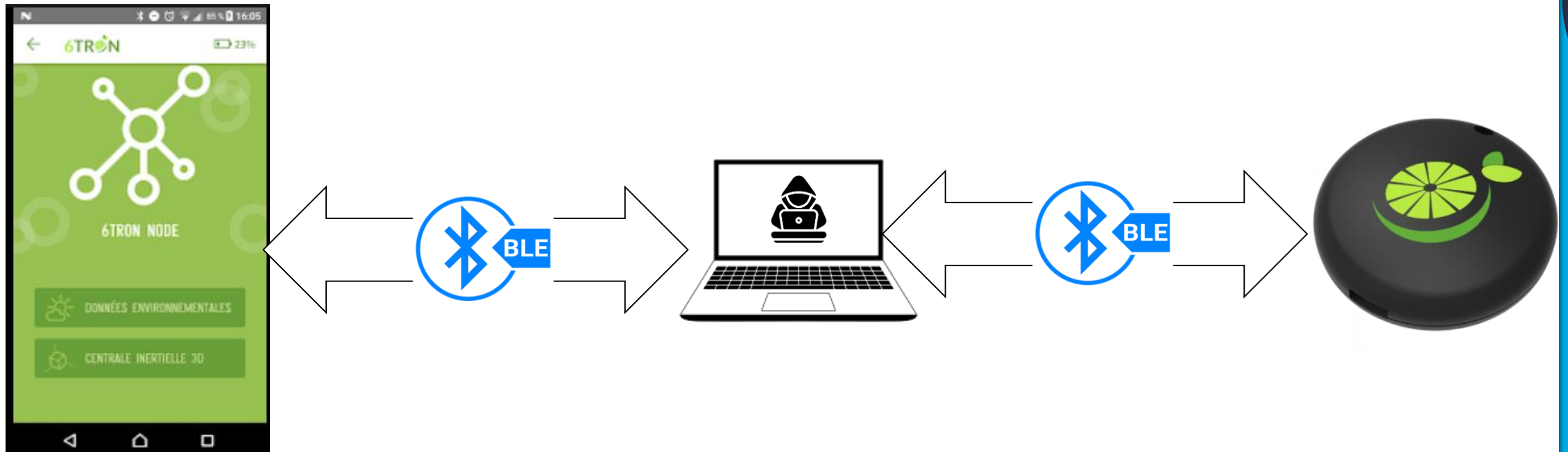
+

2x USB-Bluetooth Dongles :

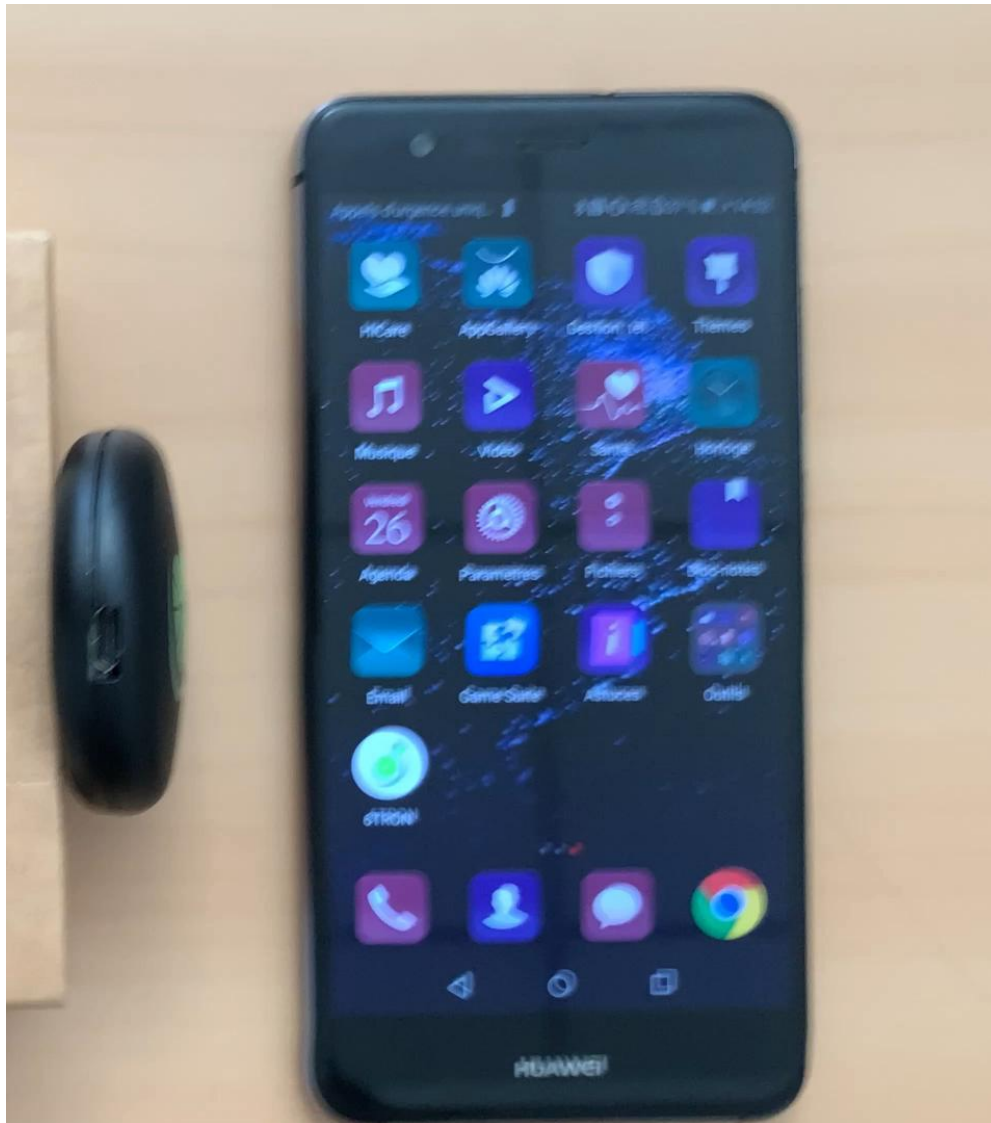


*Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de **trois ans d'emprisonnement** et de **100 000 € d'amende**.*

Man in the Middle Attack



DEMONSTRATION – BLE Man in the Middle Attack



```
seignobm@seignobm-Precision-7560:~$
```

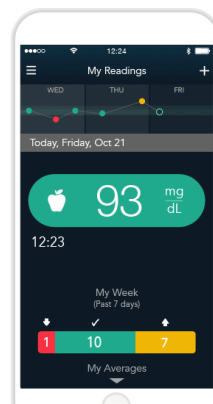
Les équipements médicaux sont-ils vulnérables aux cyberattaques ?



Drug dispenser pump

CVE-2021-33885 (Score de sévérité 10/10)

Impact : Accès complet (Incluant la modification des valeurs des données)



Blood Glucose Meter

CVE-2018-18975 (Score de sévérité 7.5/10)

Impact : Fuite de données à caractère médical



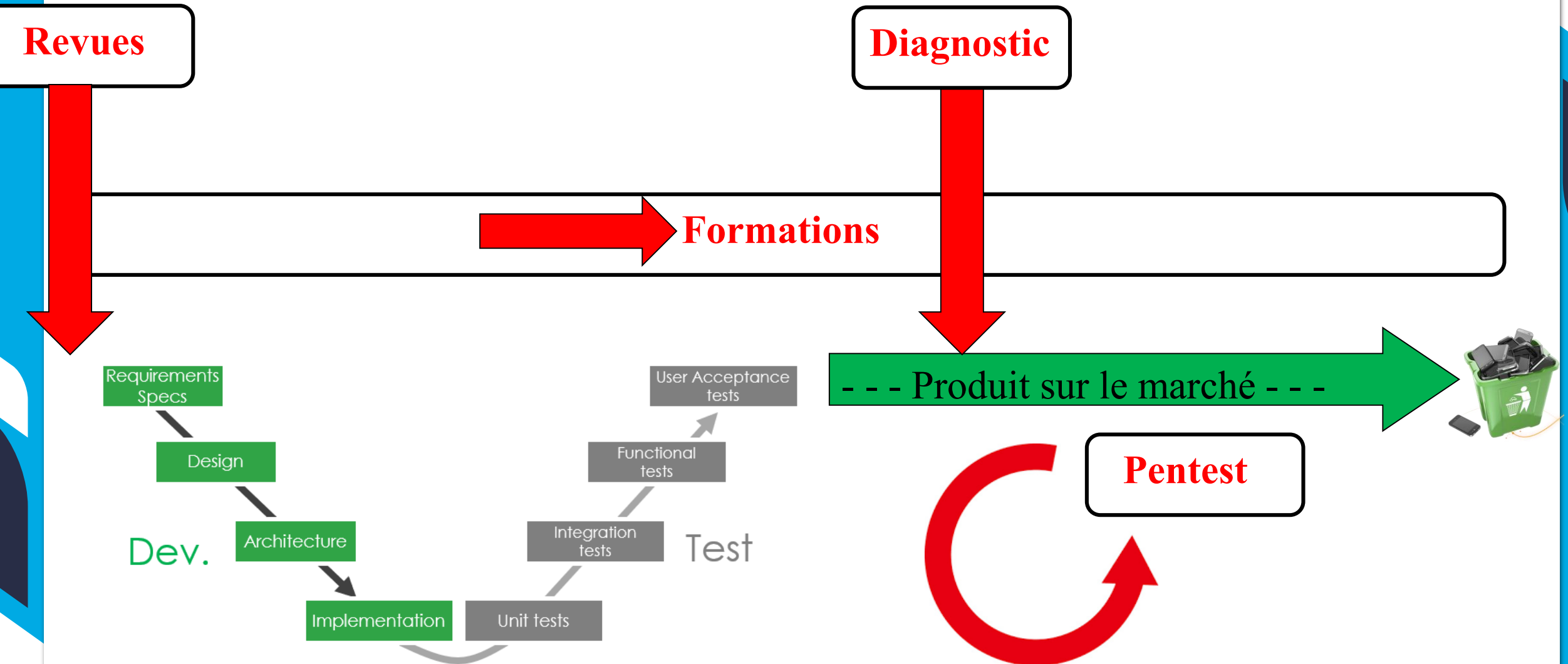
Syringe Infusion Pump

CVE-2017-12718 (Severity Score 8.1/10)

Impact : Execution de code à distance (incluant le Déni de Service)

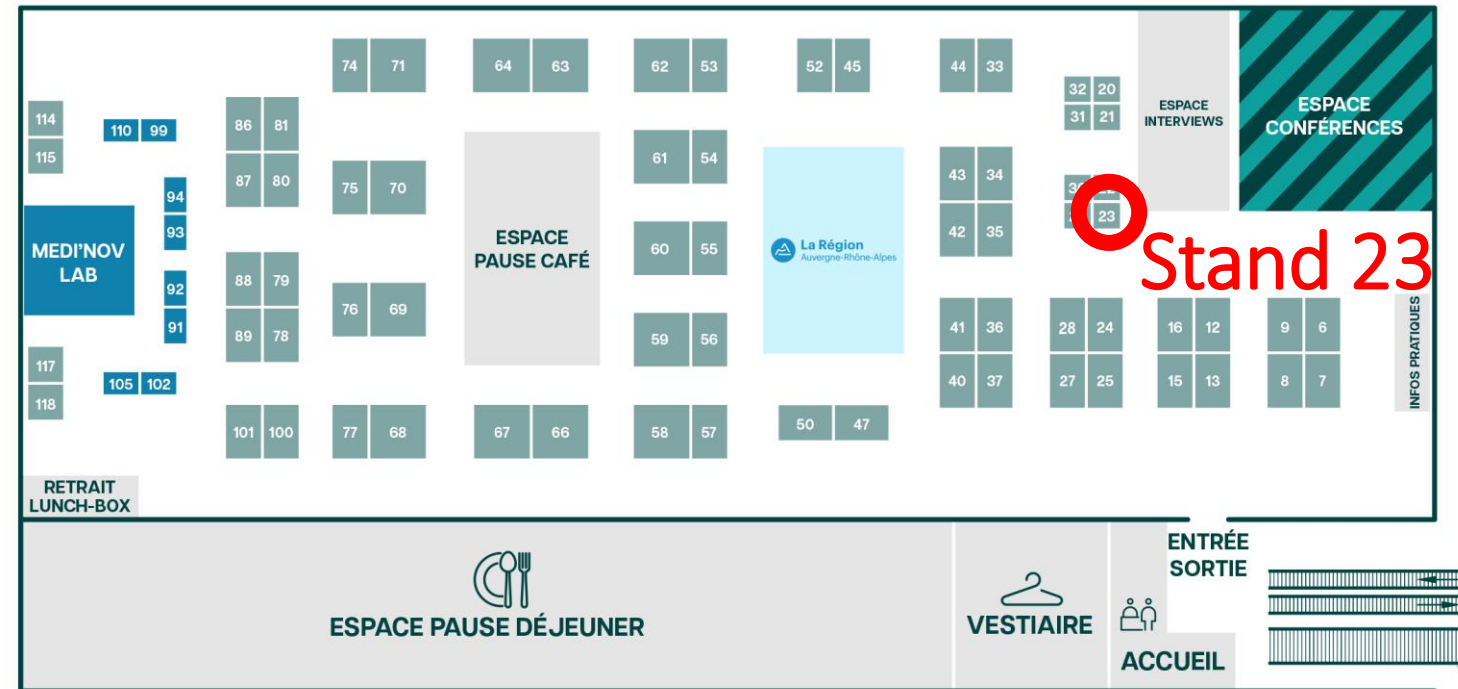
Exploit disponible librement <https://www.exploit-db.com/exploits/43776>

Comment intégrer la cybersécurité ?





contact@esynov.fr



■ Conférences plénières ■ Conférences flash ■ Tables rondes

Mickaël SEIGNOBOS
Ingénieur Cybersécurité Produit