penthertz

INNOVATIONS & SERVICES

CATALOG 2024

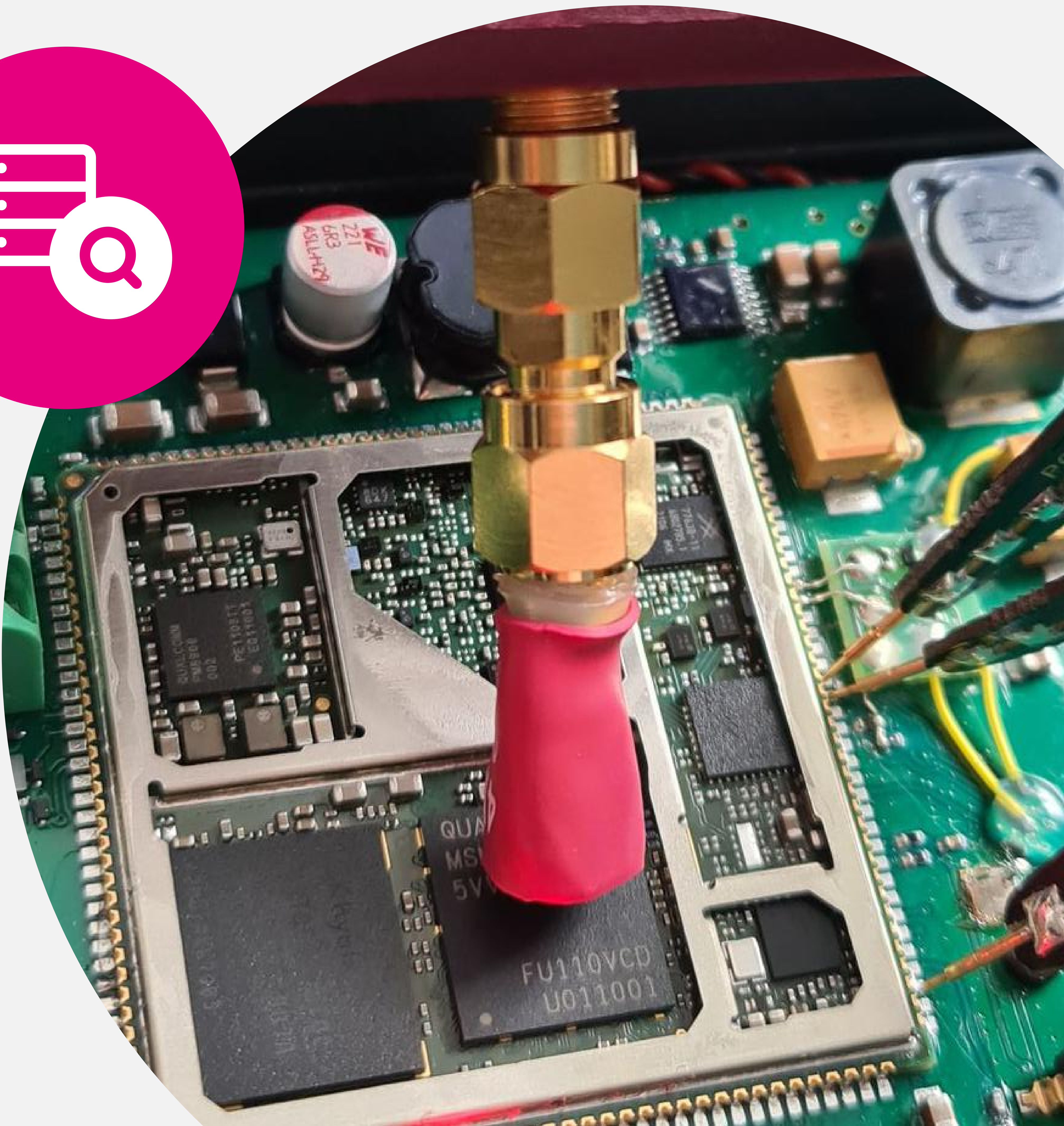


Table of Contents

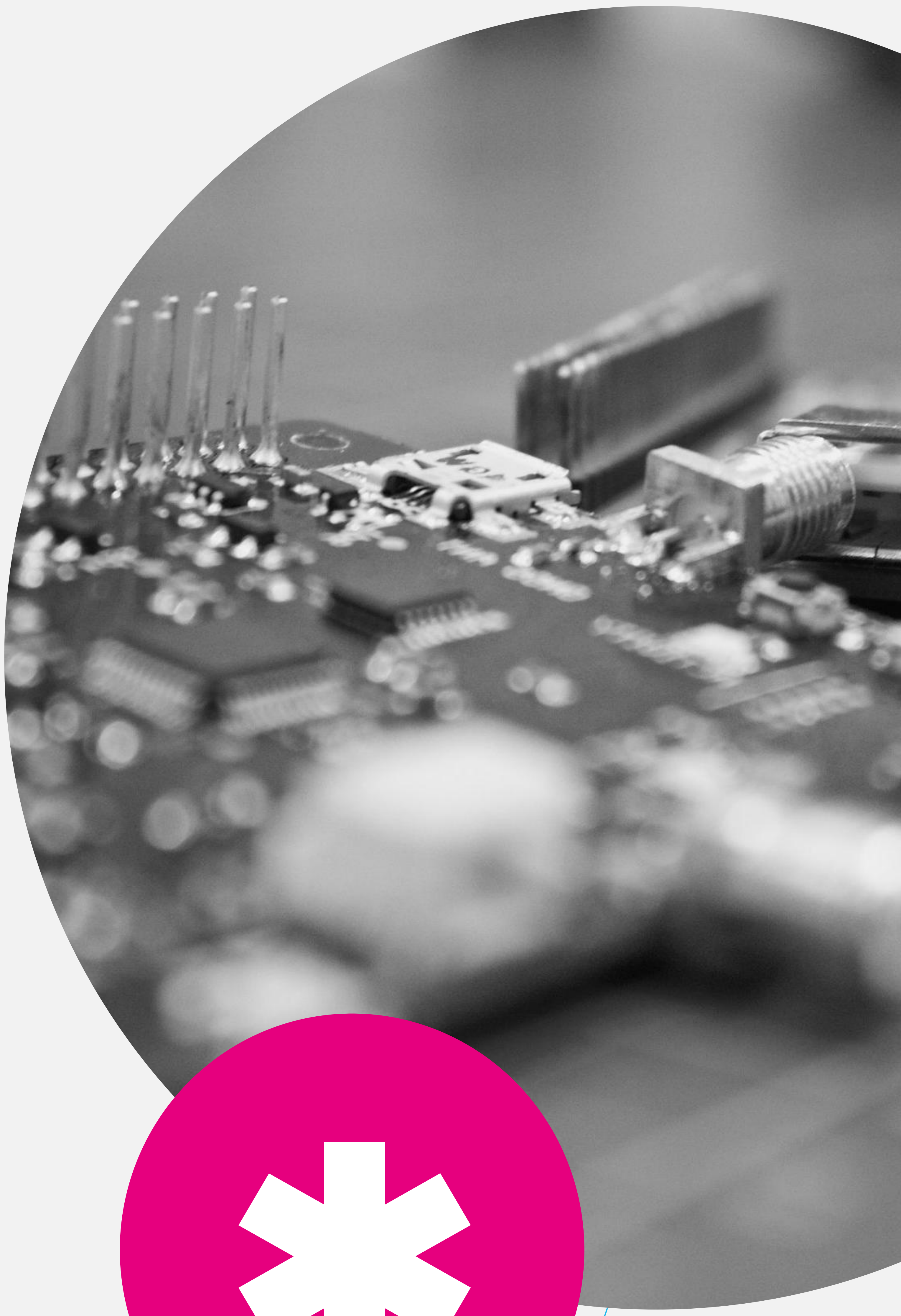
1 Introduction
P. 02

2 Technical Courses
P. 03

3 Vulnerability research
P. 14

4 Pentest, Red Team tests & expertises
P. 15

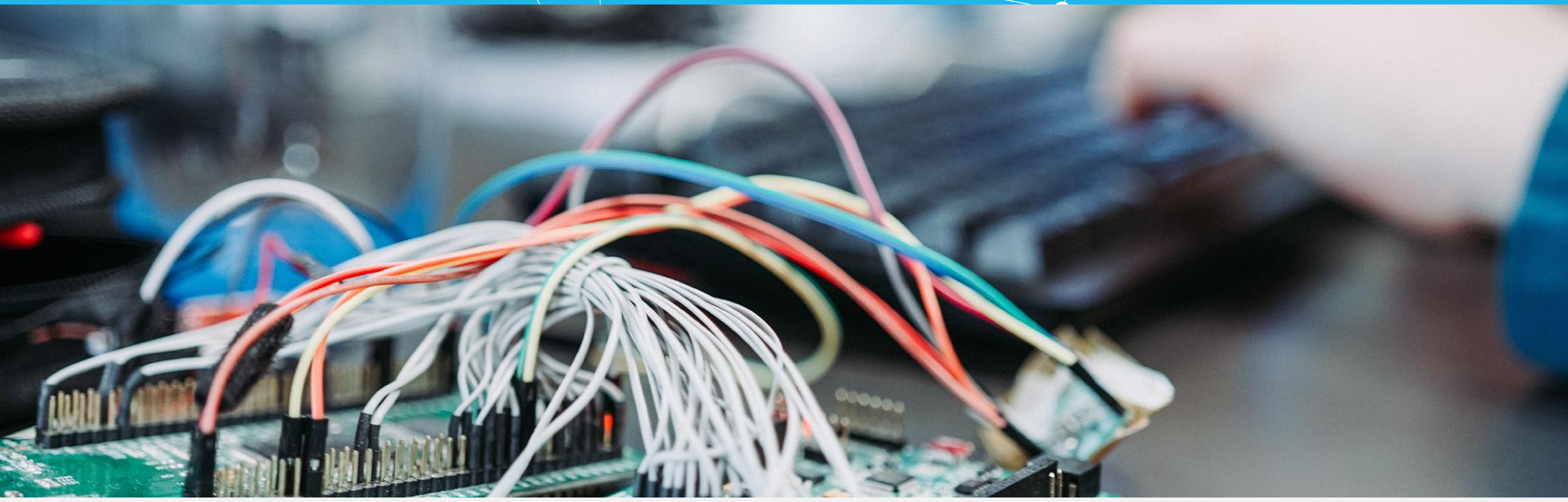
5 R&D & Tools
P. 18



Introduction

We specialize in wireless communications and hardware security to help you solve new challenges.

- Trainings & skills transmission
- Vulnerability research
- Hardware attacks
- Research & Development
- Pentest & Red Teams
- Tools development



Courses - part 1

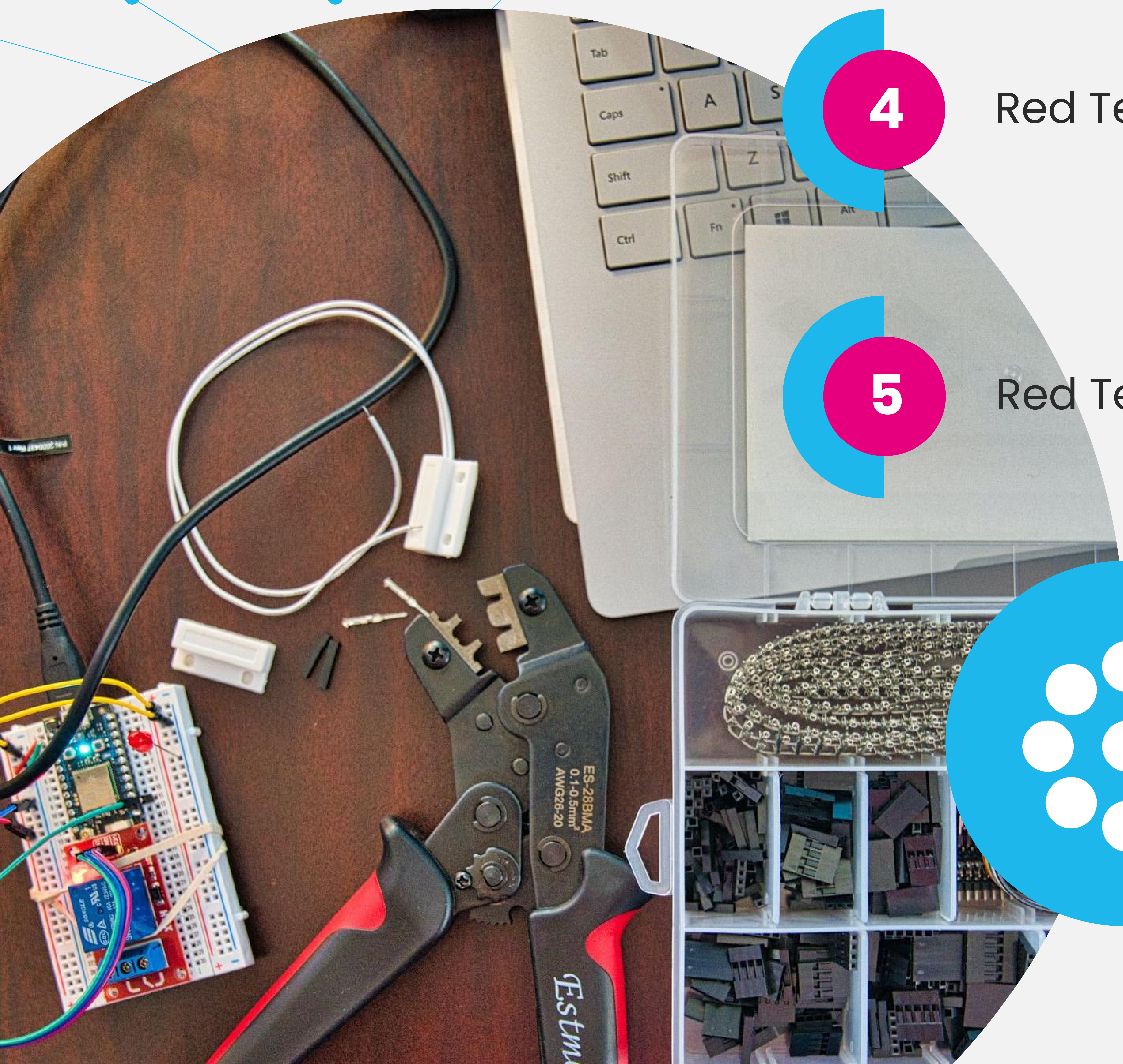
1 RF Hacking with SDR

2 Mobile Hacking with SDR

3 5G Devices & New core security and Open RAN

4 Red Team OTA

5 Red Team Wi-Fi

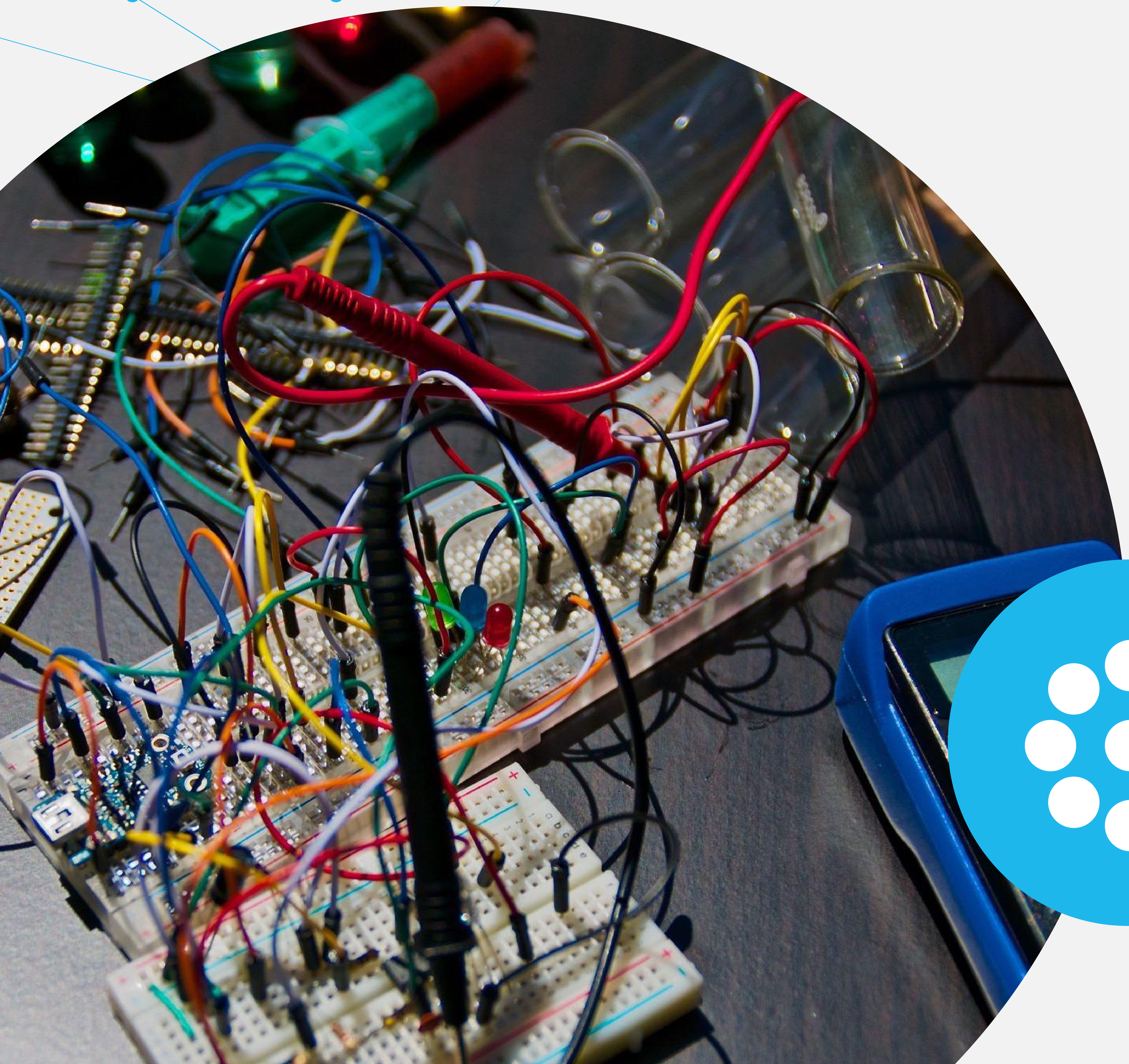


Courses - part 2

1 Red Team RFID

2 Practical Core network, Telecom Hacking

3 Tailored program



RF Hacking with SDR

Intrude most RF systems with Software-Defined Radio

TRAINER

Sébastien Dudek
Founder of Penthertz

OBJECTIVES

Learn essential concepts of radio, low-level Software-Defined Radio with GNU Radio, and methods to deal with most RF systems, including the exotic ones.

DURATION

4 days

CONTENT

- Introduction to radio & preliminaries
- Hands-on radio Analogic and Numeric with GNU Radio
- Attacking physical intrusion systems
- Unexpected implants, industrial systems, and arsenals
- And more.

trainings@penthertz.com

Scan me for more info!

Mobile Hacking with SDR

Assess mobile devices & networks using SDR

TRAINER

Sébastien Dudek
Founder of Penthertz

OBJECTIVES

Use Software-Defined Radio to cover the maximum attacks that could apply to mobile phones, IoT modules, connected cars, and other infrastructures.

DURATION

3 days

MORE

- Introduction to mobile networks and protocols (2G/3G/4G/5G)
- Security & attack surface
- Set up a fake mobile station & making a testbed for pentests
- Fuzzing stacks
- And more.

trainings@penthertz.com

Scan me for more infos

5G Devices & Networks security and Open RAN

Pentest 5G devices and core networks And the new Open RAN

TRAINER

Sébastien Dudek
Founder of Penthertz

OBJECTIVES

Learn how to hack 5G devices connected over the air with RF and SDR. Discover methods to intrude core networks and scale up your accesses.

DURATION

3 days

CONTENT

- Introduction to mobile networks and protocols
- 5G NSA and SA
- Security mechanisms on the radio
- Set up a testbed for RF pentests
- Attacking the 5G NGC
- Open RAN practical attacks
- And more.

trainings@penthertz.com

Scan me
for more infos

Red Team OTA: Physical intrusions with RF

Intrude premises being unseen

TRAINER

Sébastien Dudek
Founder of Penthertz

OBJECTIVES

Discover new opportunities for attacks targeting RFID, nRF, Bluetooth, and Sub-GHz systems, and enter to premises stealthily.

DURATION

3 days

CONTENT

- RFID & NFC systems
- Attacking current technologies with the Proxmark3
- MITM Bluetooth LE, cracking and injection
- Turning mouses & keyboards into RF implants
- Opening garage doors
- And more.

trainings@penthertz.com

Scan me
for more info!

Red Team Wi-Fi: Modern techniques

The ultimate course to uncover modern Wi-Fi offensive attacks

TRAINER

Sébastien Dudek
Founder of Penthertz

OBJECTIVES

Save time and assess Wi-Fi networks with modern techniques against current targets.

DURATION

2 days

CONTENT

- Introduction & evolutions
- Monitoring networks
- Analyzing frames
- Opened to WPA3 attacks
- Attacking companies to get access to the Active Directory
- Red Team tips
- Defense

trainings@penthertz.com

Scan me
for more info!

Red Team RFID

Open doors stealthy with concrete techniques

TRAINER

Sébastien Dudek
Founder of Penthertz

OBJECTIVES

This training is about showing current technologies we can face during a pentest or Red Team assessment, and how to be efficient with the right techniques.

DURATION

2 days

CONTENT

- The differences between several RFID and NFC systems
- The difference between RFID and NFC
- How to attack identification badges
- Attacks against classical HF tags
- Attack against systems we can also encountered in cars
- How to proceed with secure tags

trainings@penthertz.com

Scan me
for more info!

2G-5G Practical Core network, Telecom Hacking

Learn about risks and opportunities to intrude core networks

TRAINER

Sébastien Dudek
Founder of Penthertz

OBJECTIVES

Get good basics of core network fundamentals in order to understand the weaknesses that could be found during an internal penetration test, or to open doors during a red team attack from the outside.

DURATION

3 days

CONTENT

- 2G, 3G, 4G, and 5G infrastructures
- Security mechanisms
- Exposed services
- The different protocols and interfaces
- Hunting for external vulnerabilities
- Steal secrets and information of subscribers
- Privoting internally
- Security measures

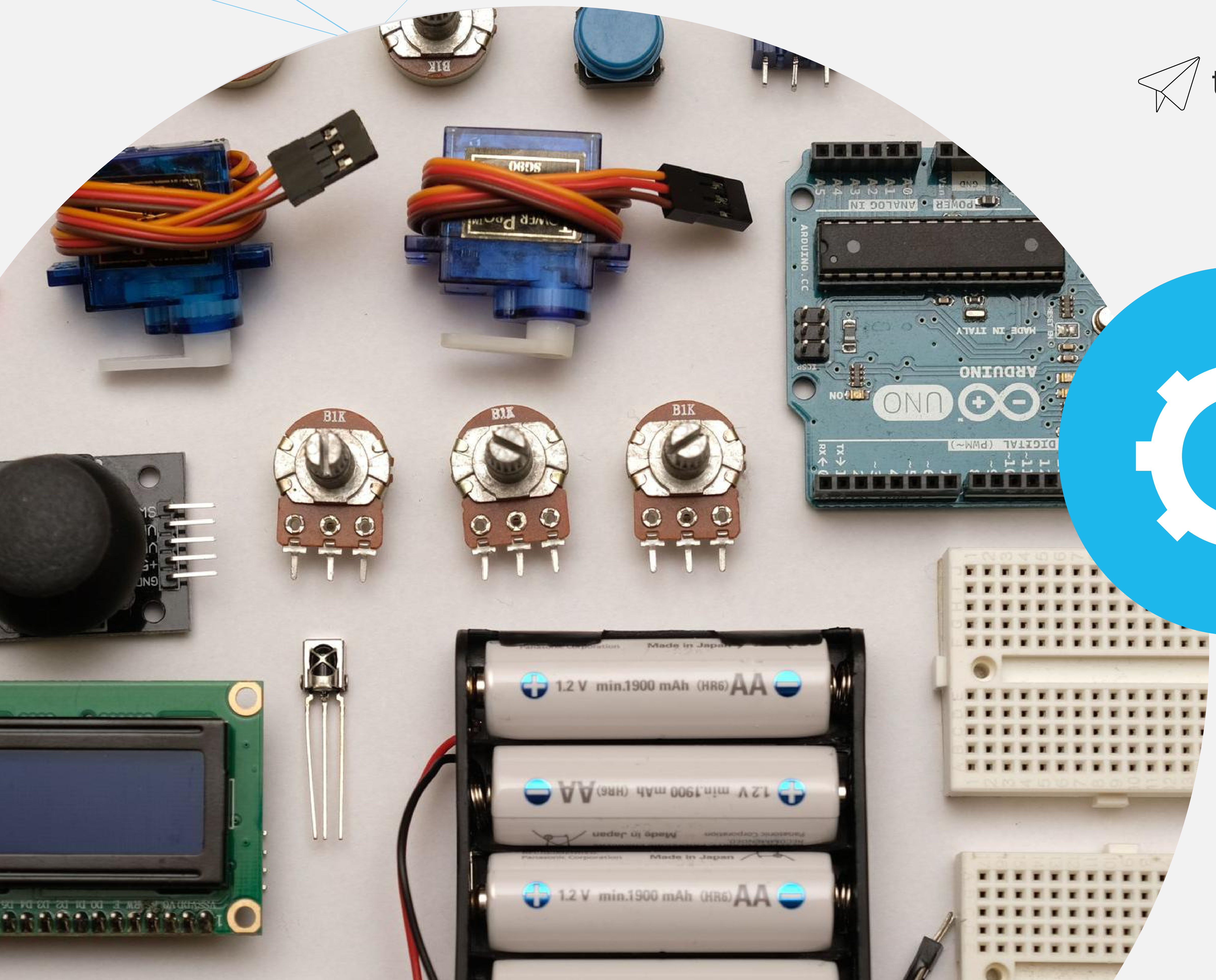
trainings@penthertz.com

Scan me
for more info!

Tailored sessions

Make your own recipe by customizing an existing training, or building your program with us to fit clear expectations:

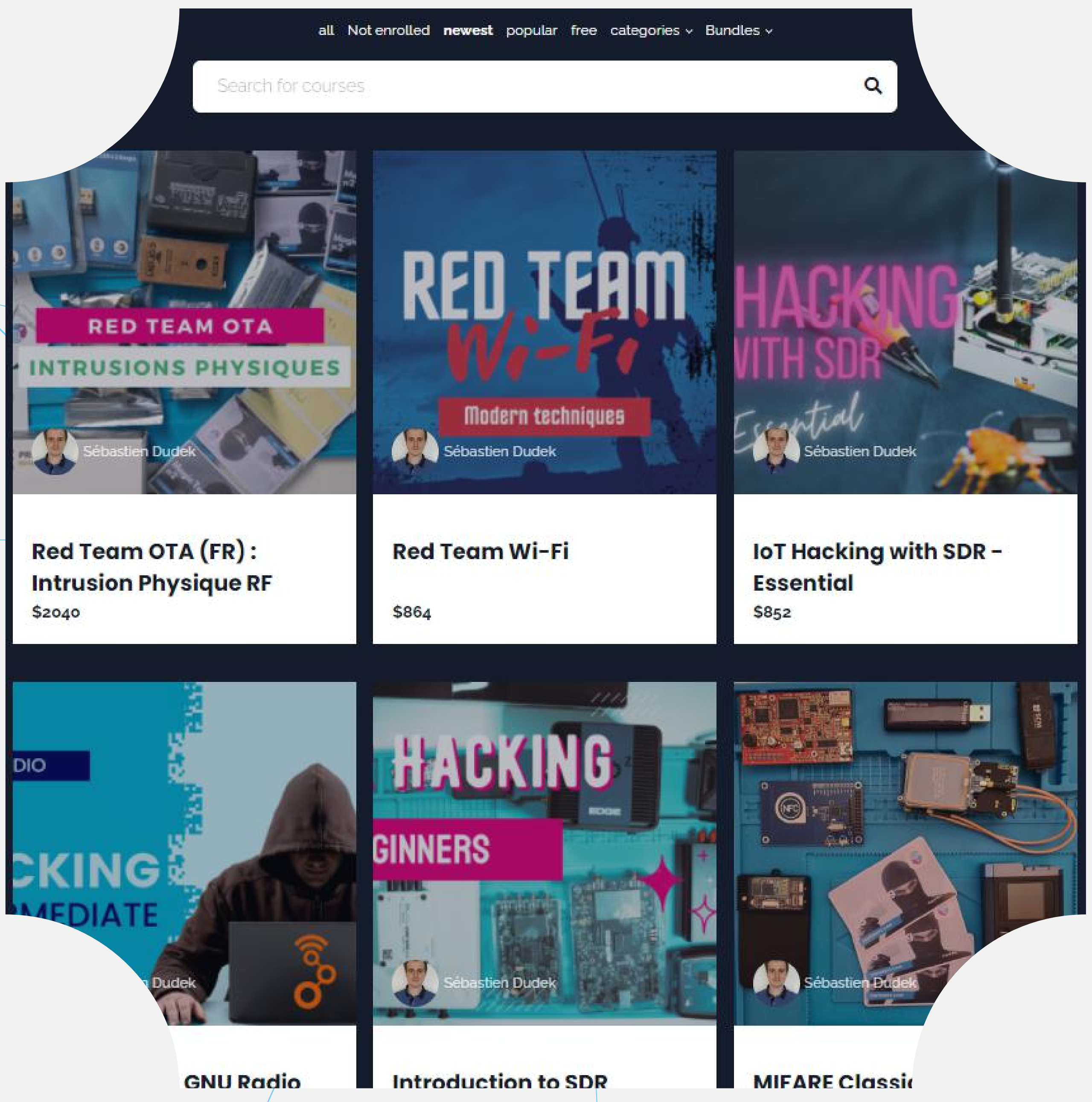
- **Mobile technologies**: attack of basebands, hunt for application vulnerabilities, fuzzing, core network attack, and defenses
- **GPS**: decoy attacks, limits, and defenses
- **Bluetooth**: attacks, fuzzing, and defenses
- **Wi-Fi**: attacking the different protocols, fuzzing the protocol stack, and analyzing the radio signal
- **RFID/NFC**: additional content and advanced techniques with SDR
- **Hardware**: additional content in hardware and practice to attack embedded systemsà
- And other technologies.



trainings@penthertz.com

On-demand

If you do not have time, Penthertz also provides on-demand trainings that are already pre-recorded:



Red Team OTA (FR) : Intrusion Physique RF
$2040

Red Team Wi-Fi
$864

IoT Hacking with SDR - Essential
$852

GNU Radio

Introduction to SDR

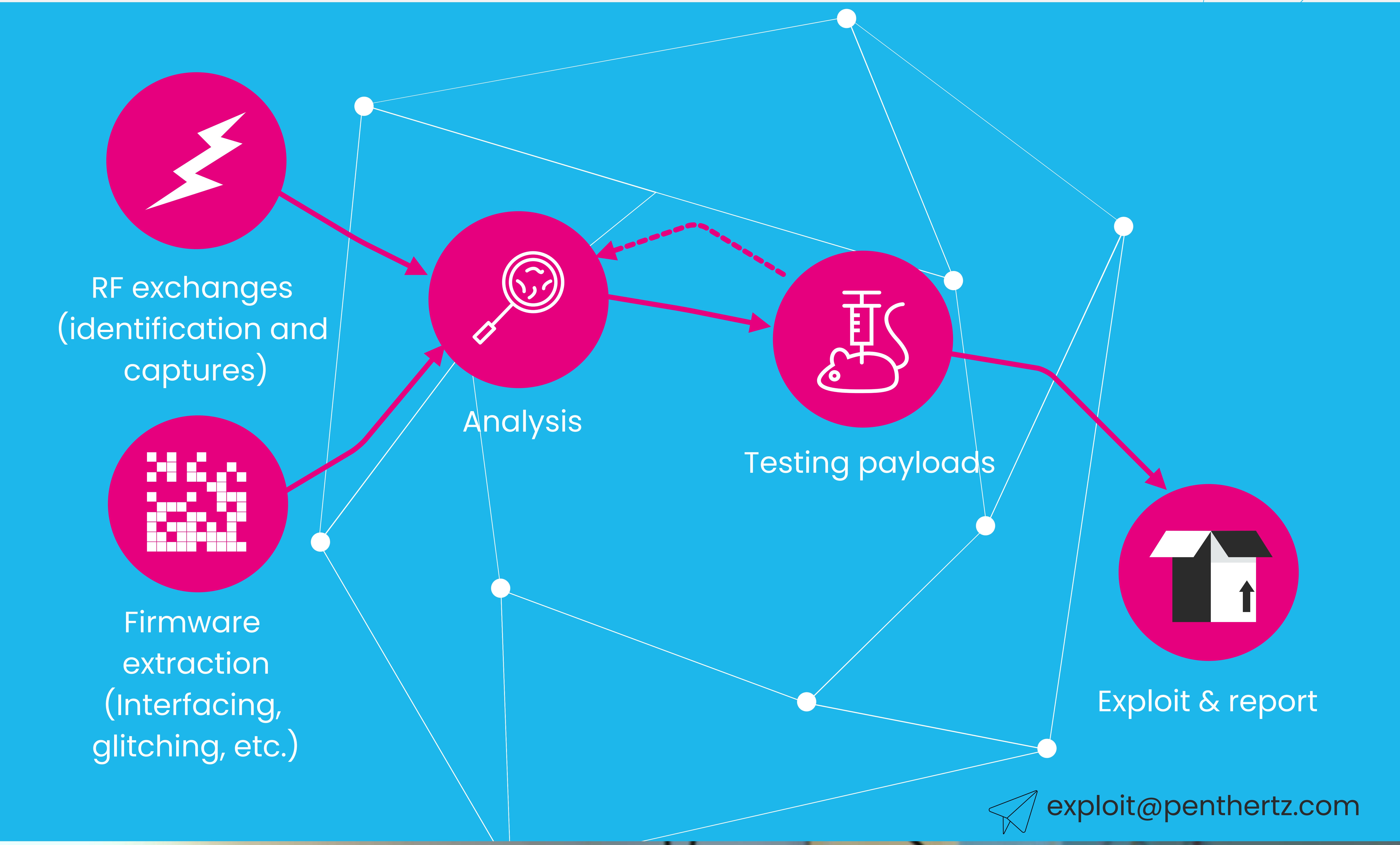
MIFARE Classic

If you need a custom program, you can also contact us at: trainings@penthertz.com

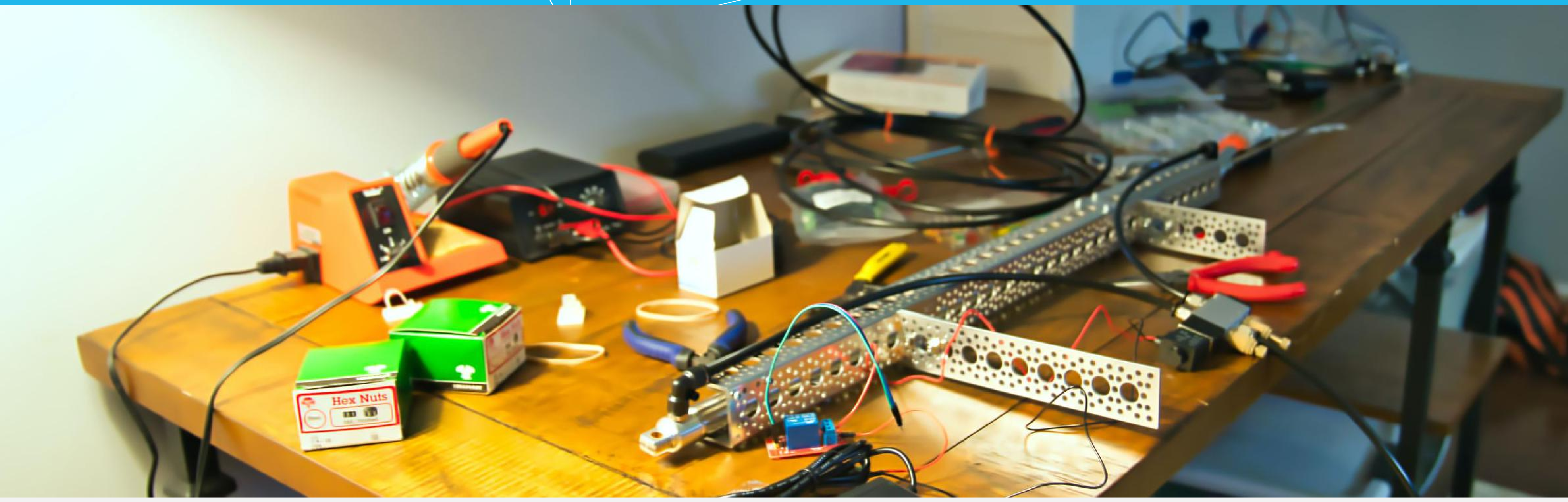
Get also a look on our YouTube channel!

Vulnerability research

We analyze RF communications and extract firmware to find vulnerabilities.


RF exchanges (identification and captures)
Firmware extraction (Interfacing, glitching, etc.)
Analysis
Testing payloads
Exploit & report

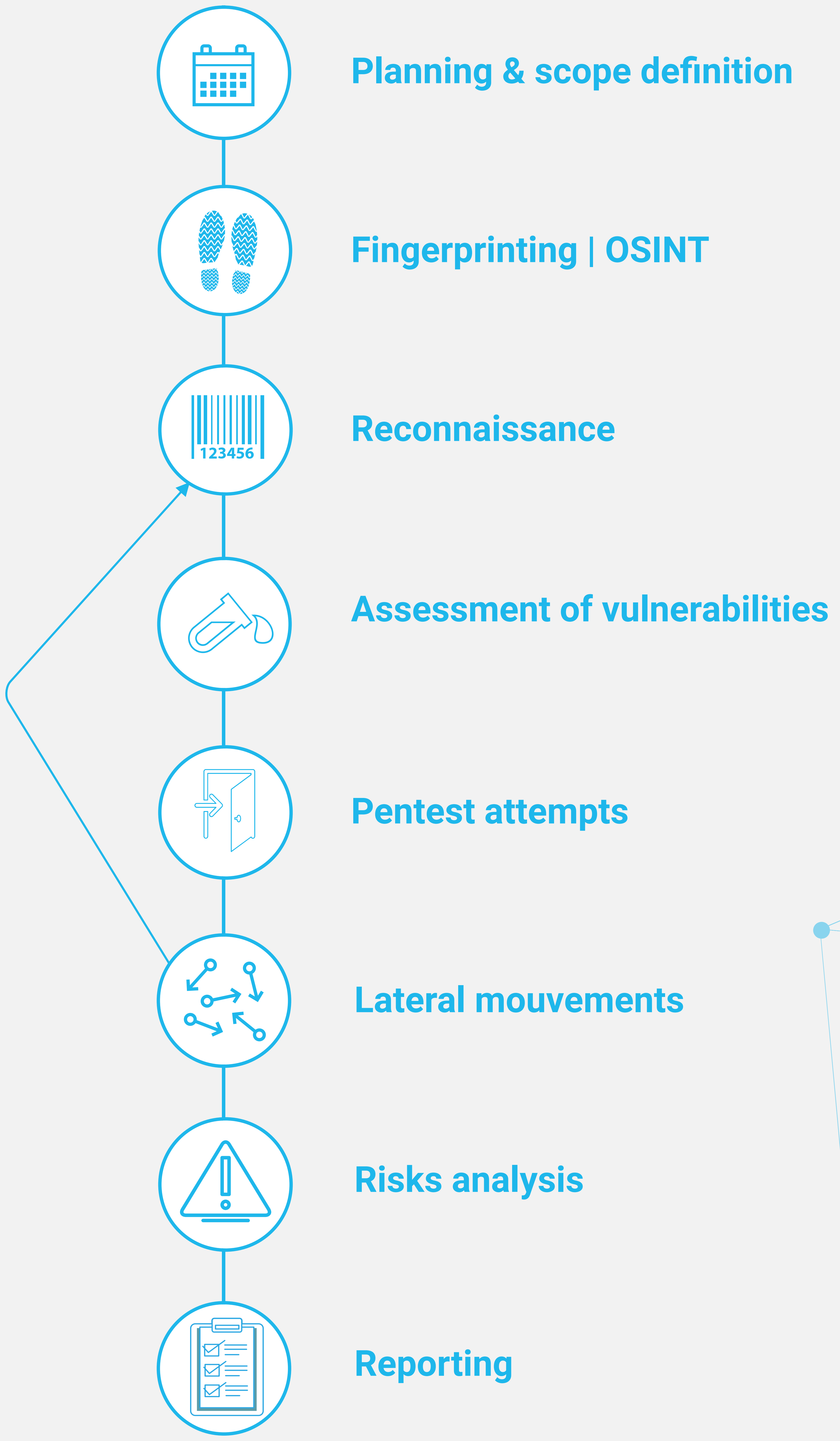
exploit@penthertz.com



Pentest & Red team tests

Most security tests are specific to your product, so we **avoid you wasting time** reading and fixing unrelated bugs by focusing on important ones. We also help you get your **product certified**.

Moreover, we offer Red Team assessments giving you a **real-world** based on our **various attack scenarios**.



- Planning & scope definition
- Fingerprinting | OSINT
- Reconnaissance
- Assessment of vulnerabilities
- Pentest attempts
- Lateral mouvements
- Risks analysis
- Reporting

pentest@penthertz.com

Connected cars expertise

We have experience assessing cars communications performed between the different ECUs over CAN/LIN/FlexRay, especially IVI/IVCs or even T-Boxes using Mobile/Bluetooth/Wi-Fi exchanges, immobilizers, V2X, Charging stations on Power-Line Communication, and are curious to find new challenges

CAN/LIN/FLEX/100BASE-T1

- Discovery of UDS, XCP, DCM, DoIP, SoIP
- Dumping UDS services, DIDs,
- Testing sessions accesses & writing access
- Looking for secrets
- Checking seeds
- Fuzzing tests
- Etc.

WIRELESS

- Hijacking Wi-Fi and BT/BTLE communications
- Testing exposed services from Wireless, 2G/3G/4G/5G interfaces
- Testing mobile modules security mechanisms
- Fuzzing the mobile modules
- Testing backends in use by the mobile connectivity
- Testing immobilizers
- Etc.

HARDWARE

- Testing I2C, SPI, JTAG/SWD, DAP, etc...
- Dumping the firmware
- Analyzing firmware (Linux like QNX/Android, AUTOSAR depending on time, etc.)
- Glitching attacks (EMFI, power, etc.) & side-channels, ...

pentest@penthertz.com

Mobile network expertise

Since its creation, Penthertz is doing assessing mobile equipments such as cars, intercoms, and robots, but also pentests on Core-Networks, especially attacking EPCs and 5G NGCs from the outside as inside for operators and private networks.

CORE NETWORKS

- Finding and exploiting exposed GTP, S1-MME, AMF/NRF, N3, etc.
- Tests on SIGTRAN (SS7) and DIAMETER
- Pentesting on UPFs
- Routing informations
- Internal tests
- Fuzzing stacks
- Etc.

RANS

- Checking for capabilities
- Attacks from RAN and X2 tests
- Fuzzing stacks from a UE
- Open RAN pentests
- Hunting for fake 2G-5G stations

USER EQUIPMENTS

- Location
- Downgrading, Jamming and hijacking
- Analyzing communication from 2G-5G
- Rooting mobile modules and dumping memory
- Glitching attacks
- Fuzzing basebands
- Attacking M2M infrastructures

pentest@penthertz.com

Physical Intrusions

We go beyond internal & external tests to intrude your gates!

Social Engineering
To test employees' awareness

Lockpicking
Challenging physical security mechanisms

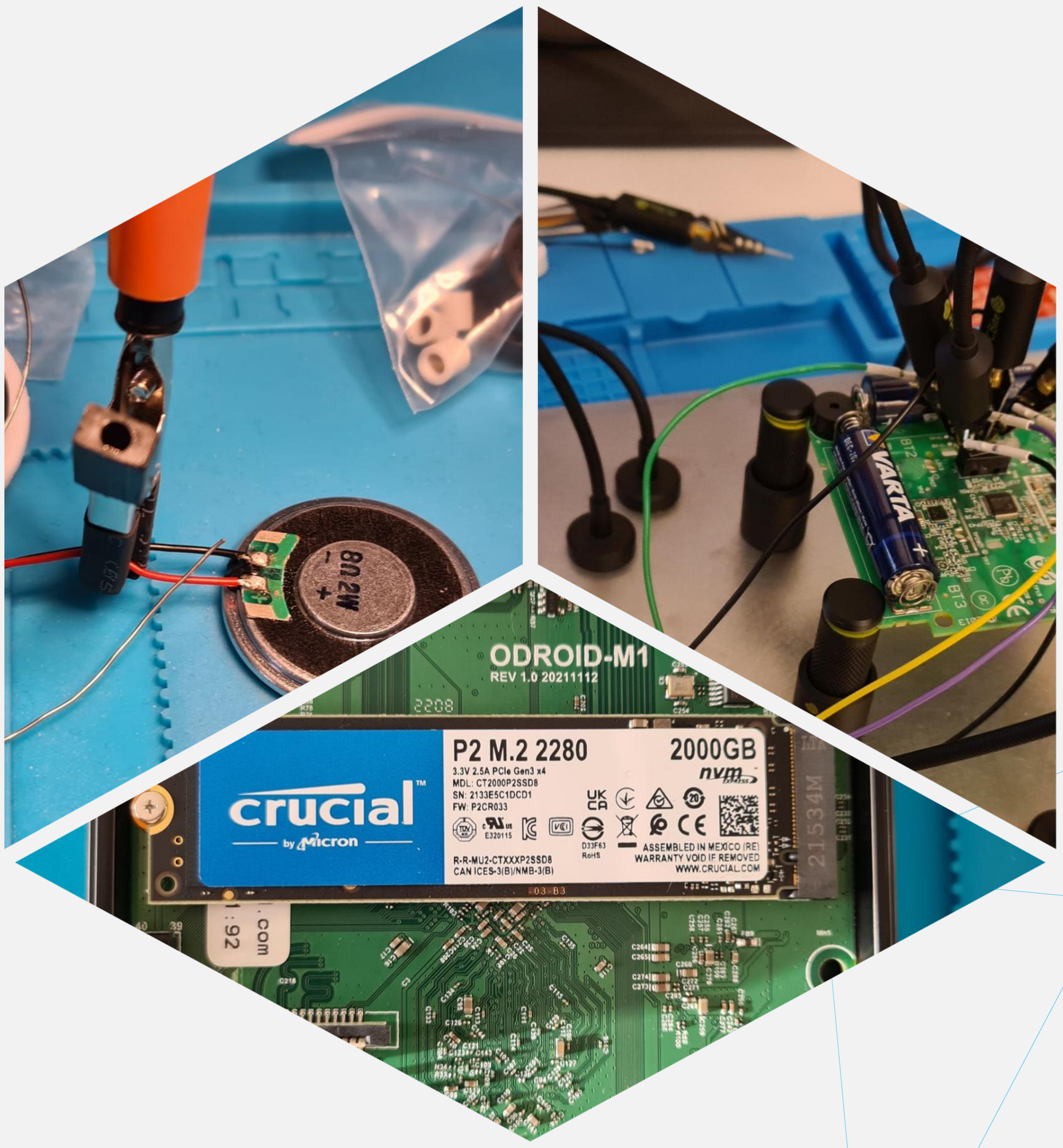
RF/Smart Mechanisms
Opening gates that use tags, remotes, etc.

pentest@penthertz.com

Research & Development

We are constantly developing **new methods and tools** to handle **future technologies** for our assessments and research.

These prototypes & tools can be reused or extended for your needs to **perform redundant tests automatically, saving you time and money and focusing on new and complex challenges**.



products@penthertz.com

GitHub

We also publish free tools on GitHub!

Are you interested in working with us?

We would love to hear about your projects and help you grow safely!

Website
penthertz.com

Mail
contact@penthertz.com

LinkedIn
/penthertz

/penthertzlab

@PentHertz

@Penthertz@infosec.exchange

/c/Penthertz