SISEN: Instructor Guide

Security-Informed Safety

Dr Ayman El Hajjar
University of Westminster

Purpose of this Guide

This guide supports instructors who are preparing and delivering the SISEN practical activities. It assumes that the instructor has already selected the relevant scenario and now needs detailed guidance on preparation, sequencing, supervision, evidence, troubleshooting, recovery, and assessment.

The shorter SISEN Teaching and Integration Guide explains how the resource pack can be adopted within a module. This Instructor Guide focuses on how to deliver the activities reliably and consistently.

1 Documents Used During Delivery

Before the practical session, ensure that students have access to:

- the SISEN Student Guide;
- the relevant Medical IoT, Smart Building, or 6LoWPAN scenario guide;
- the SISEN Attack and Disruption Guide;
- the SISEN Hazard Analysis and Evidence Sheet; and
- any local module instructions or assessment requirements.

The Student Guide, scenario guides, attack guidance, capture guidance, and activity worksheet are available from the SISEN project site and the repository. The main scenario documentation is stored under `docs/`. Manual wireless and infrastructure guidance is provided in `docs/manual-attacks.md`, while the separate hardware access-point activities are documented under `ap/hw-ap/docs/`.

2 Instructor Preparation

2.1 Environment Checks

Before each teaching session:

- use a tested copy of the current SISEN repository;
- run `sudo ./setup/setup-dependencies.sh` and confirm that the required operating-system, networking, wireless, MQTT, capture, and analysis dependencies are installed;
- run `./setup.sh` as the normal user and confirm that the local `.env` file and project-local Python environment are created;
- confirm that students do not need to activate `.venv` manually;
- confirm that the MQTT broker, read-only dashboard, namespace, wireless, and capture dependencies are available;
- run the selected scenario from startup to cleanup;

- confirm the available attack names using `python3 attacks/run_attack.py -list`;
- run the selected bounded observation, attack, or disruption activity from a separate terminal;
- confirm the expected technical and dashboard effect;
- confirm that packet capture and evidence collection work as documented;
- test the stopping and recovery procedure; and
- reset the environment before students begin.

All commands in the SISEN documentation assume that the instructor and students are working from the root folder of the repository unless stated otherwise.

2.2 Delivery Scope

Select the activity before the session. Students should perform only the bounded activity specified for the class. The scenario guides explain the system context, while the Attack and Disruption Guide provides the technical procedure and evidence-inspection guidance. Launcher-managed telemetry attacks and manual wireless infrastructure activities should remain clearly separated during delivery.

3 Recommended Delivery Sequence

3.1 Opening Briefing

Explain:

- the purpose of the selected scenario;
- the distinction between a security event, operational effect, unsafe condition, hazard, and harm;
- the evidence students are expected to collect and how filenames, interfaces, topics, timestamps, and packet references should be recorded;
- the selected bounded activity;
- how the activity will be stopped or reversed; and
- how the worksheet will be used during the session.

3.2 Establish Normal Operation

Students should first confirm that the scenario is operating normally. Require evidence of:

- successful scenario startup;
- active sensors or nodes;
- current telemetry;
- dashboard updates;
- expected MQTT topics, UDP traffic, gateway logs, or wireless frames; and
- the normal communication path relevant to the selected activity.

Students should not perform the attack or disruption until a baseline has been recorded.

3.3 Capture and Observation

Where packet capture is required, students should first identify the active host and namespace interfaces using the commands documented in `docs/captures.md`. They should run `tcpdump` in a separate terminal and leave it running while the activity is performed. They should stop the capture using `Ctrl+C` and then open the resulting `.pcap` file in Wireshark using the filters provided in the capture and activity guidance.

Capture files should be written under `captures/`. Students should record the selected interface, capture filename, relevant MQTT topic or protocol, and the packet number or time range used as evidence.

Additional terminals may be required for MQTT observation, log monitoring, the read-only dashboard, monitor-mode capture, or the bounded activity itself.

3.4 Perform the Selected Activity

Students should run one bounded activity at a time. Helper-based telemetry attacks normally refresh the injected condition for approximately ten seconds and then exit, while legitimate scenario telemetry continues and should restore the dashboard afterwards. Ask students to record:

- the command used;
- the targeted component or data path;
- the immediate technical effect;
- the visible effect on telemetry, logs, captures, or the dashboard; and
- whether the system recovers automatically or requires intervention; and
- the evidence showing that recovery occurred.

3.5 Safety Analysis

Students should not describe the attack itself as the hazard. Require them to distinguish:

1. the initiating security event;
2. the affected component, data, or communication path;
3. the immediate operational effect;
4. the resulting unsafe condition;
5. the possible harm;
6. relevant preventive, detective, fail-safe, and recovery controls;
7. the evidence that would demonstrate that a proposed control works; and
8. residual risk.

3.6 Stopping and Recovery

Before ending the session:

- stop the bounded activity using the documented procedure;
- stop any running packet capture;

- remove any temporary monitor-mode interface where it was used, for example with `sudo iw dev mon-sisen del`;
- confirm that telemetry has resumed where recovery is expected;
- stop launcher-managed scenarios using `python3 launch_sisen.py -stop`;
- confirm that namespaces, interfaces, dashboards, publishers, and helper processes have been removed; and
- reset the environment for the next group.

4 Scenario Delivery Notes

4.1 Medical IoT

Core safety focus: Trustworthy and timely patient telemetry.

Main communication path: Wearable simulator, BLE-to-Wi-Fi gateway, MQTT broker, and patient monitoring dashboard.

Useful activities:

- MQTT topic observation;
- gateway-log observation;
- spoofed patient telemetry;
- extreme or malformed values;
- replayed telemetry;
- safety-critical patient conditions such as critical vitals, suppressed fall alerts, suppressed panic-button events, and falsely normal battery state.

Key teaching points:

- false but plausible telemetry may be more dangerous than visible loss of data;
- broker access does not by itself prove the authenticity of patient data;
- the gateway is an important trust boundary;
- freshness, plausibility, and continuity checks have direct safety value; and
- students should distinguish simulated BLE behaviour from over-the-air Bluetooth capture.

4.2 Smart Building

Core safety focus: Trustworthy environmental and occupancy telemetry.

Main communication path: Simulated sensors, wireless access point, MQTT broker, and building monitoring dashboard.

Useful activities:

- MQTT topic observation;
- telemetry spoofing;

- extreme or malformed values;
- replay and message freshness;
- telemetry noise;
- single-client disconnection;
- sensor blackout; and
- scenario-focused cases such as hidden gas leaks, suppressed fire alarms, and hidden blocked exits.

Separate HW-AP activities may be used where physical wireless infrastructure is available. These include open-AP observation, hidden-SSID observation, MAC filtering and spoofing, WEP IV collection, WPA2 handshake capture, rogue access-point observation, and targeted deauthentication. These activities are documented under `ap/hw-ap/docs/` and are not launched through the main SISEN scenario launcher.

Key teaching points:

- one infrastructure failure may affect several telemetry streams simultaneously;
- occupancy and environmental data may influence ventilation, evacuation, and building-control decisions;
- missing data and misleading data require different fail-safe responses;
- shared infrastructure can create common-mode failure; and
- wireless management behaviour can be observed independently of MQTT payloads.

4.3 6LoWPAN

Core safety focus: Trustworthy and timely telemetry across a constrained wireless path.

Main communication path: IEEE 802.15.4 devices, 6LoWPAN adaptation, IPv6, UDP telemetry, border-router or relay behaviour, MQTT, and dashboard presentation.

Useful activities:

- low-power wireless and protocol-path observation;
- node-specific spoofed telemetry;
- extreme values;
- replayed telemetry;
- incomplete or missing telemetry fields; and
- safety-critical industrial conditions such as masked boiler pressure, hidden emergency-stop state, and hidden machine overheat.

Key teaching points:

- the border router is both a trust boundary and a potential single point of failure;
- IEEE 802.15.4, 6LoWPAN, IPv6, UDP, MQTT, and the dashboard are distinct layers;
- security at the MQTT stage does not protect the complete end-to-end path; and
- constrained devices may limit the controls that can be deployed locally.

5 Expected Student Evidence

Students should collect only evidence that supports their analysis. Appropriate evidence may include:

- scenario startup and normal-operation output;
- dashboard state before, during, and after the activity;
- relevant MQTT, UDP, wireless, or namespace traffic;
- gateway, publisher, relay, or attack-helper logs;
- the selected bounded activity command;
- the observed technical and operational effect;
- the completed security-to-safety chain;
- the completed hazard analysis;
- clear separation between direct observation, inference, and assumptions;
- recovery evidence;
- mitigation, assurance evidence, and control status; and
- initial and residual-risk discussion where required.

Screenshots and extracts should be accompanied by a short explanation of what they demonstrate.

6 Assessment Guidance

Assessment should prioritise:

- accurate technical observation;
- correct distinction between attack, system effect, hazard, and harm;
- evidence-based reasoning with precise filenames, interfaces, topics, timestamps, and packet references;
- clear separation between direct observation, inference, and assumptions;
- appropriate mitigation and resilience controls;
- testable assurance evidence for proposed controls;
- recognition of recovery behaviour and residual risk; and
- clear explanation of evidence.

The practical may be used formatively, as part of a laboratory portfolio, or as a structured assessed exercise. Local submission requirements and marking criteria should be provided separately by the module team.

7 Troubleshooting Principles

When an activity does not produce the expected effect:

1. confirm that the correct scenario and access-point mode are running;

2. confirm that the expected nodes, namespaces, interfaces, and processes exist;
3. confirm that the dashboard and baseline telemetry are operating normally;
4. verify the target, topic, interface, port, category, scenario key, attack name, and command options;
5. inspect the relevant logs and capture traffic;
6. stop the scenario and activity cleanly;
7. rerun the setup or scenario cleanup where necessary; and
8. restart from a known clean state.

Do not improvise alternative targets or interfaces during a taught session. Use the tested commands and identifiers provided in the SISEN documentation.

8 Instructor Close-Out Checklist

Before the material is delivered or reused:

- confirm that the installation, launcher, attack, capture, monitor-mode, and cleanup commands match the current repository;
- confirm that all links and filenames are current;
- test the selected scenario from startup to cleanup;
- test the selected bounded activity and expected evidence;
- confirm that no placeholder text remains in student-facing material;
- confirm that the scenario guide, activity guide, worksheet, and local assessment instructions are consistent; and
- record any known issue that students may encounter.