

Connecting attack simulation to defensive action

Public portfolio recreation of training work in a simulated industrial environment.



Adapted from my industrial cybersecurity training work | Conceptual system overview.

A sample training structure

New, non-operational teaching outline based on the documented training approach.

Scenario and learning goal

A simulated workstation produces unusual network discovery traffic. Learners must distinguish observations, hypotheses, and evidence needed for escalation.

Observe and investigate

Review synthetic logs and a timeline. Identify the affected assets, relevant telemetry, and missing context before proposing a response.

Explain the defence

Describe which monitoring, segmentation, or filtering controls could help, what they would observe, and how to validate the change in the lab.

Assess understanding

Ask the learner to justify the conclusion and repeat the exercise with altered evidence. Success is reasoned investigation, not memorising a command.

Illustrative exercise outline | Designed to connect system behaviour, evidence, and defensive decisions.