Scenario 4 - Disconnection of detectors:

Purpose:

- **Technical:**
  - Increase competence of distinguishing a cyber attack from technical faults
  - Increase competence on how to troubleshoot the disruption of detectors
- **Procedure:**
  - Practice procedures around events that may be either technical errors or cyber attacks
  - Increase the competence for cyber related incidents

Description of scenario:

Part 1:

Three technicians working the night shift in the control room observe that the gas detectors suddenly stop responding. The disruption happens simultaneously for all of the gas detectors. All other detectors are still working as intended, and no other changes in the system are noticed.

Part 2:

A technician uses a diagnosis software trying to find the error. The technician contacts the detectors to retrieve a diagnosis, but the detectors are not responding. The technicians can not find any technical faults when troubleshooting and start to suspect that a cyber attack may be in progress.

Part 3:

The technicians receive a phone call from SOC that they have been compromized and that they currently are under cyber attack.

Justification of scenario:

One of the operators from the interviews had this scenario as an example from a real event. In that example, the gas detectors had been disconnected for 17 hours, before measures were initiated. The reason behind that specific event was indeed a technical error, but could also have been caused by a cyber attack. Increasing the awareness that “technical errors” actually can be a result of a cyber attack amongst the control room operators is evidently necessary. There are several possible causes for such an event, e.g. fog, technical error, electrical error or it can be a result of a cyber attack.

Exercise plan:

Time duration	Total of 2 hours including introduction and first evaluation.
Prerequisites	- Training of employees on log analysis

Participants	- First line personnel:
	  - Control room operators
	  - Maintenance personnel
	- Platform management
	- IT security experts

Example questions	*Part 1:*

	Technical: - When should the error be manually checked? Could it wait until the morning? - Is this a serious event? *Procedure:* - When should other personnel be informed? - When should the emergency response team be contacted? - Is this a serious event? *Part 2:* *Technical:* - What other components should be investigated for infection? *Procedure:* - What are the procedures for the first line personnel? - Who should be contacted now? - What other components should be investigated for infection? - Are there any procedures for this? - If suppliers are involved, what is the response time stated in the contract? *Part 3:* *Technical:* - How should we avoid that other areas get infected as well? - How can this situation be solved? *Procedure:* - Who should be contacted? - What are the procedures for the first line personnel? - Who has the responsibility for contacting the media, PSA, etc.? *Discussion and reflection:* - How can you distinguish whether it is a cyber attack or if it is just a technical error without saying that it is not likely? - How should the correspondence between the technicians working the night shift and the SOC-personnel be organized?
Variations	- Other sensors or detectors can be disconnected. - Involve the emergency response team. - Fog may lead to detectors not responding, and this can be added to the exercise if there is a need for a more complex scenario.

Suggestions to playbook	*Further input to the scenario:* - The scenario can develop after the disconnection is discovered. More severe consequences can be added by the facilitator as the scenario is played out.