Stakeholder Engagement Protocol

Subsequent sections outline the protocol/guide used during each interview. This covers all aspects, from Preface through to Conclusion. Tthe core focus of these interviews is to better understand current approaches to cyber incident response and recovery practices within an OT context. More specifically, how are cyber incidents broached by key stakeholders.

1 Preface

The following question-set and associated notes will be applied during the preface phase.

- Reiterate the purpose of the interviews based on the interview guide, and the expected timescale.
- Confirm the participant knows the full interview will be recorded, and that they will be told when the recording is due to begin, and when it is due to end.
- Turn ON the recording now.
- Confirm the consent to participation, that recorded has begun, and their rights in regard to participation.

2 Establishing Demographics

The following question-set and associated notes will be applied to the demographics phase.

- Please can you tell us your job title, and provide a brief overview of your core roles and responsibilities?
  Probe: Ask for clarity on any terms that are not clear.
- How many years of experience do you have working in this role?
  Probe: How many years of experience do you have working in this field?
  Probe: How many years of experience do you have working in this sector?
- At a very high level, please can you explain to us what you understand the term Response and Recovery to mean within the context of an Operational Technology (Industrial Control Systems) cyber security incident?

Definition: Decisions and actions for the rapid implementation of a coordinated,multidisciplinary process,to manage the direct effects of an incident through protection of operational systems, human life, and the environment, creating the conditions required for a return of service.
Definition: The process of rebuilding and restoring services to normal operation following an incident. Although distinct from response, recovery forms an integral part of response processes, as actions taken during the response activities can influence longer-term outcomes.

3 Scenario Familiarisation

The following question-set and associated notes will be applied during the scenario familiarisation phase.

- Please review the following infrastructure diagram (See Figure 1, a description will also be provided).
  Probe: Are there any aspects of the diagram which are unclear, or that you would like additional information on?
- Please review the following cyber incident diagram (See Figure 2, a description will also be provided).
  Probe: Are there any aspects of the diagram or attack which are unclear, or that you would like additional information on?

4 Response and Recovery Analysis

The following question-set and associated notes will be applied during the response and recovery analysis phase.

- Given your role in the organisation, at a high level, what are the core steps you would go through as part of response and recovery operations in the example scenario?
  Probe: Explore unusual terms and elaborate on anything that is unclear.
  Probe: Explore identified phases/processes.
  Probe: Is there anything unusual in this scenario that would cause you to deviate from a standard response process?
- How many individuals within the organisation would work directly with you on these steps, i.e. performing the same role as you and under your management?
- Who else would you have direct engagement with during response and recovery operations?
- How many individuals across the organisation would be involved in response and recover operations more generally speaking?
  Probe: Explore the use of any third-parties.

- When undertaking a response and recovery operation to this scenario, what do you consider the primary goal to be?
- When you are undertaking individual response and recovery actions, how do you factor in risk evaluation as part of the decision-making process?
  Definition: Evaluating risk associated with the executing of specific actions, and thus the potential for unintended consequences arising as a result of those actions.
- Typically, what are the expected outputs post incident? So, once you have appropriately recovered from an incident and everything is back to normal?
  Definition: Reporting internally/externally, documenting, etc.
  Probe: Explore unknown/unclear post-incident outputs.
- Please review this second cyber incident diagram (See Figure 3, a description will also be provided). Would anything be done differently compared to the first scenario?
  Probe: Are there any aspects of the diagram or attack which are unclear, or that you would like additional information on?

5 Guidance Analysis

The following question-set and associated notes will be applied during the external guidance analysis phase.

- In your opinion, which standards or guidelines best cover response and recovery in relation to Operational Technology cyber-attacks targeting the nuclear sector?
  Probe: Why effective/not effective?
- As a final question, what is your opinion on currently available standards and guidelines within the context of cyber incident response and recovery?
  Probe: Why effective/not effective?

6 Conclude

The following question-set and associated notes will be applied during the conclusion phase.

- Confirm that the interview questions have been completed, and ask the interviewee if they would like to add anything in addition which may be relevant.
- If supporting documentation has been described and offered throughout the process, politely remind the interviewee to forward it on via E-Mail.
- Turn OFF the recording now.
- Thank the interviewee for their time and input into the project.

- Inform the interviewee that if at any time they recall any additional points deemed relevant to the discussed topic area, that one would greatly appreciate them being sent via E-Mail.
- Reiterate the options for withdrawal as described in the participant information sheet.

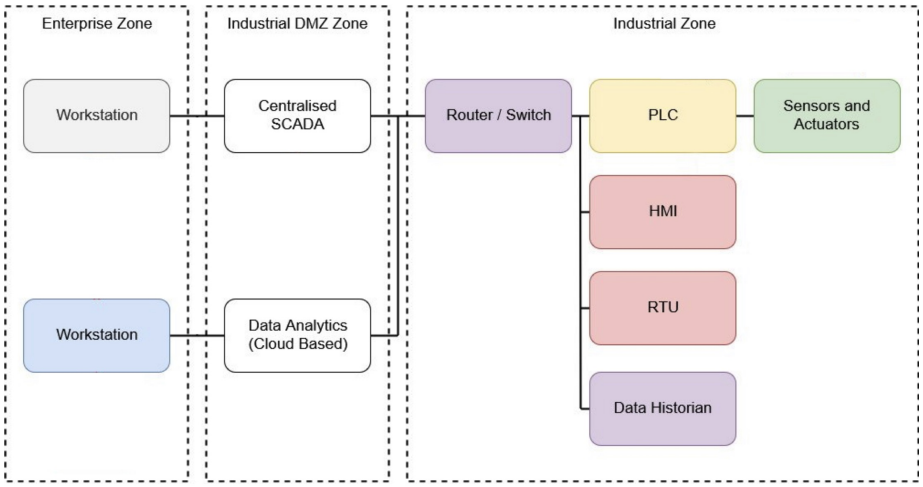

Figure 1: Core Infrastructure

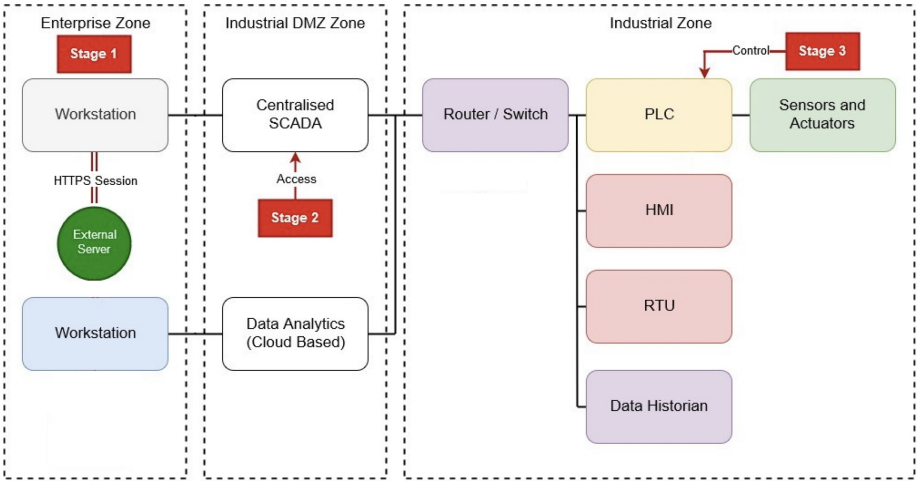

Figure 2: Scenario 1 - Operational Process Manipulation (Post Social-Engineering)

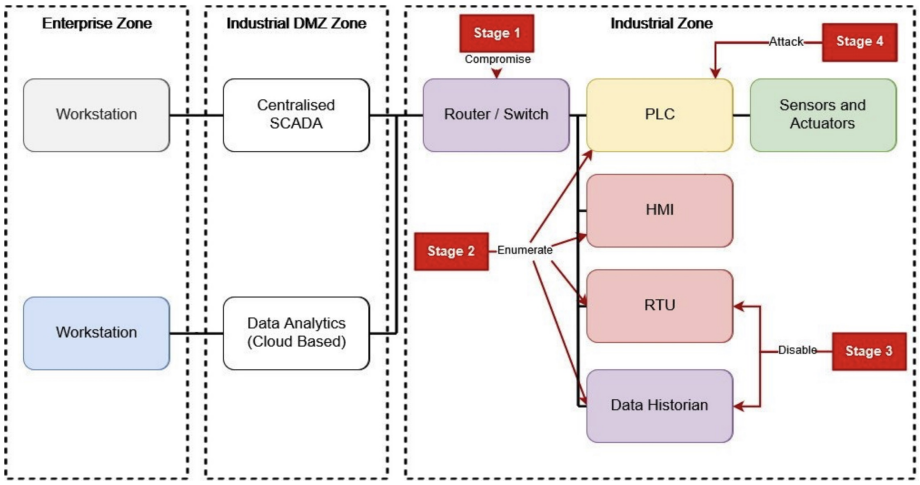

Figure 3: Scenario 2 - DoS Attack