Exercise planner

Package 3, exercise 1

'Actor has conducted reconnaissance'

Version 1.0

Table of contents

1 Introduction

1.1 Background and scope

Facilities and installations in the petroleum sector are required to have preparedness plans in place for managing serious incidents. The industry is subject to various scenarios involving ICT incidents, but the Norwegian Ocean Industry Authority (Havtil) has, through audits, noted that little or no training is carried out related ICT security in the industrial control and security systems. Considering this, Havtil has commissioned a set of training and exercise scenarios. These exercises have been prepared by Proactima together with Netsecurity and was adapted by Havtil.

The Activity regulation § 23 stipulates that: «necessary training and necessary drills are conducted, to ensure that the personnel are always able to handle operational disturbances, hazard, and accident situations in an effective manner». The Technical and Operational regulation stipulates the same in § 52. This means that the requirements for training and exercise are the same for onshore and offshore facilities.

Training enhances personal skills and knowledge, while exercises test collaboration and response capabilities during an emergency. In addition, exercises can reveal organisational and structural strengths and weaknesses and prepare management for dealing with various crises.

1.2 Structure of this guide

The exercise planner contains several scenarios. Each scenario includes suggestions on which functions are relevant to the exercise. The scenarios can be used for training, tabletop exercises, or incident response simulation exercises.

Part 3 of the guide contains additional information to aid in preparation and implementation. This includes:

- a possible sequence of events prior to exercise start-up
- a sequential incident flow chart
- relevant technical material

2 Scenario

The scenario described in this guide starts with the detection of a suspicious gathering of information related to the SAS networks and the industrial control systems.

2.1 Overview of the scenario

The responsible personnel for SAS/IACS discover a file area on a server located in the demilitarised zone (DMZ). In the file area, there are files that appear to contain information about networks and credentials for industrial networks.

Table 1. Summary of roles/functions that can be trained using the various modules.

Task	Stage	Personnel responsible for SAS/IACS	Local operations managers	Personnel responsible for systems operation	ICT department
2.2	Initial events – file area detection	x	?	x	
2.3	Escalation – malware detection			x	x
2.4	Malware activation attempt			x	x

2.2 Initial events – file area detection

Closer examination shows that the files appear to contain information, usernames, and passwords, as well as other information that can provide an overview of networks and functions in the industrial networks.

2.2.1 Initial questions

Personnel responsible for SAS/IACS

- What are the immediate actions that must be taken?
- How to collaborate with the ICT department?
- How to collaborate with personnel responsible for system operation?
- How to verify the information in the file area with your own system documentation?

ICT department

- What are the immediate actions that must be taken?
- How to collaborate with personnel responsible for system operation?
- Is it possible to define an indicator from the identified findings?
- Are there any indications that the file area is established by a legitimate user?
- Who must be notified?

Personnel responsible for system operation

- How to collaborate with the ICT department?
- Who have responsibilities in the situation?

Local operations managers

- Should the local operations managers be involved?

2.2.2 Advisory questions

The ICT department suspects that an external actor has gained foothold in the office network.

ICT department

- Who have responsibilities in this situation?
- Who must be notified?
- How can we know if the actor has done more than just gather information?
- Access control
    - How is the access management set up?
    - Who administrates the access controls in the organisation, and how?
- Are the usernames and passwords used in other systems?
    - Are there procedures in place for password renewals and system back-ups?
- How long could the actor have had access?
- How can we remove the actor's access?

- Should the access be revoked or should we continue to monitor the activities?
- Do we need external support?

Personnel responsible for system operation

- How can we uncover if the actor has affected the control system or the SAS network?
  - What resources do we need and how should these be utilised?
  - Do we need support from the supplier/external resources?
- Are the usernames and passwords in the industrial networks used in other systems?
  - Are there procedures in place for password renewals and system back-ups?

Personnel responsible for SAS/IACS

- Should personnel responsible for SAS/IACS be involved?

Local operations managers

- Should the local operations managers be involved?

2.2.3 Additional action points (dependent on the outcome of discussions/decisions)

- The firewall for the control systems does not contain any logs related to the incident.
  - Do we need support from the ICT supplier in the investigation/evaluation of the incident?
- The firewall logs contain traces of unknown activity
  - Which disciplines (internal or external) can be contacted for support?

2.3 Escalation – malware is detected

Closer examination reveals that the overview of usernames and passwords corresponds with those being used in parts of the control network. There are no attributes in the file area or files that can support the identification of the one who established the files.

The IT administrator detects indicators of malware that refers to the same type of firewalls the organisation utilises in the industrial networks.

2.3.1 Initial questions

ICT department

- What measures can be established to protect the firewall?
  - Are there any pending software updates?
  - How can we identify and share indicators (IoC)?
- How to collaborate with personnel responsible for systems operation?
- Who must be notified?

Personnel responsible for systems operation

- How to collaborate with the ICT department?
- Who is responsible during the situation?

Personnel responsible for SAS/IACS

- What are the potential consequences of isolating the firewall?
  - …. for the operation of the control systems?
  - …. for the operation of the facility or installation?
- How to collaborate with the local operations managers?

2.3.2 Additional action points (dependent on the outcome of discussions/decisions)

- The firewall for the control systems does not contain any logs related to the incident.
  - Do we need support from the ICT supplier in the investigation/evaluation of the incident?
- The firewall logs contain traces of unknown activity
  - Which disciplines (internal or external) can be contacted for support?

2.4 Malware activation attempt

To protect the firewall and uncover information about the actor, the firewall is updated and closely monitored.
It is detected that the malware is activated, but it is unsuccessful in its attempt to cause any damage.

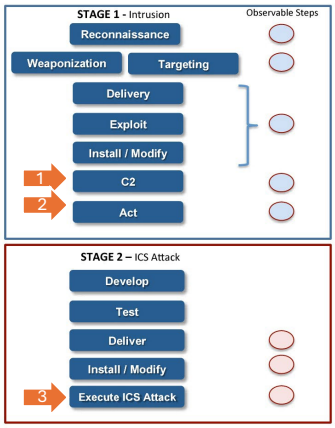
2.4.1 Initial questions

ICT department

- What are the immediate actions?
- How can tactics, techniques, and procedures (TTP) be uncovered?
    - How to identify and share indicators (IoC)?
- How to collaborate with the sector CERT?

3 Additional information for preparation and implementation

This chapter contains background information about targeted cyber-attacks against industrial ICT systems. Digital attacks often adhere to fixed patterns, often referred to as 'kill chains'. The diagram on the right illustrates the various stages making up this exercise, as well as the exercise items incorporated into the guide.



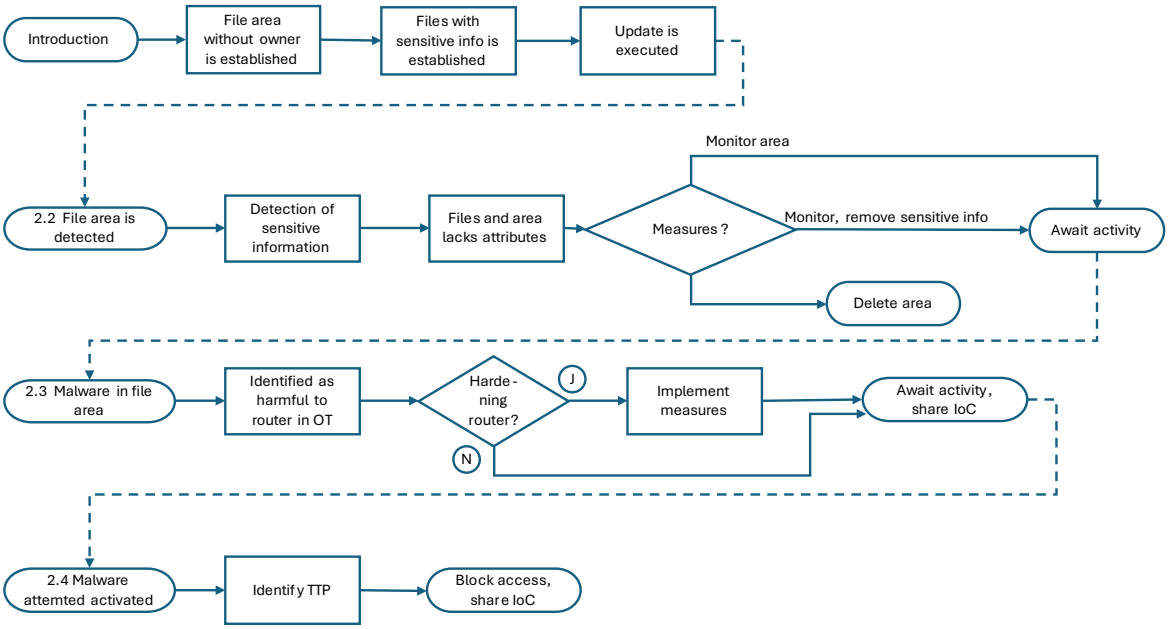
- Actor has passed the barriers for stage 1 and gathers information locally
- Attack
  - 1) Information gathering
  - 2) Reconnaissance of OT interface
  - 3) Malware activation
- Exercise points
  - Clarify responsibilities
  - Information sharing
  - Investigation/forensic

3.1 Introduction to the incident

A file area that contains files with sensitive information is detected. It is unclear who has established the area or the files.

3.2 The incident

It is possible that the file area was established, and the information is gathered by an actor who illegitimately has gained access to the system through a legitimate remote access or user.



3.3 Lessons learned

Review of procedures, improvement of systems to prevent new attacks, etc.

Discussion leader

- How are the participants involved to provide feedback to the final report from the exercise?

ICT department

- Are roles and responsibilities adequately described?
- How does existing procedures support the incident management?
- Were the procedures adhered to? What changes should be made?
- How is the management documentation protected?

Personnel responsible for systems operation

- Are roles and responsibilities adequately described?
- How does existing procedures support the incident management?
- Were the procedures adhered to? What changes should be made?

Personnel responsible for SAS/IACS

- Are roles and responsibilities adequately described?
- How does existing procedures support the incident management?
- Were the procedures adhered to? What changes should be made?
- How to ensure learning across all shifts?

Local operations managers

- How does existing procedures support the incident management?
- How to ensure learning across all shifts?

3.4 Relevant reference material

The example utilised in this exercise where it is detected that sensitive information is gathered and saved locally, is unlikely to occur. Most actors attempt to remain invisible, and if possible, utilise functions that are available in the network.
The American government, together with the Canadian, Great Brittain, Australian, and New Zealand government developed the guide *Identifying and Mitigating Living Off the Land Techniques*[1]. The abstract of the report is three pages long and contains points with best practices for detection and hardening.

The attack on the electrical supply in Ukraine in December 2015, started during the spring of 2015. It is likely that there were several possibilities to detect the activities before the

[1] [1] https://media.defense.gov/2024/Feb/07/2003389936/-1/-1/0/JOINT-GUIDANCE-IDENTIFYING-AND-MITIGATING-LOTL.PDF

incident (*Analysis of the Cyber Attack on the Ukrainian Power Grid*[2] p. 23). This report is also referenced in exercise 1, package 1.

[2] https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf