TLP-CLEAR

**Master Scenario and Event List**

MSEL Template supporting Planners’ Preparation phase

February 2026

Table of Contents

1. Exercise Purpose & Objectives 2

2. Exercise Practical Details 4

3. Scenario Overview 5

4. Master Events and Injections Table 6

5. Group and Player Information 10

5.1 Group Information 10

5.2 Player Information 10

5.3 Simulated Entities 10

# Exercise Purpose & Objectives

|  |  |
| --- | --- |
| *Purpose* | What is the overall purpose or mission of the exercise? Why do you want to organise it? |
| 1. **WHY 1**: 2. **WHY 2**: 3. **WHY 3:** |
| *Objectives* | What are the specific objectives of this exercise (*max 5*)? Enter description.   1. **Objective 1**: 2. **Objective 2**: 3. **Objective 3**: 4. **Objective 4**: 5. **Objective 5**: |

# Exercise Practical Details

|  |  |
| --- | --- |
|  | |
| Exercise type | [Functional Exercise / Full-Scale Exercise / etc.] |
| **Exercise Format** | [In-person / Virtual / Hybrid] |
| **Exercise Duration** | [Total hours/days] |
| **Exercise Start Time (CET)** | [Date and Time - T-0] |
| **Exercise End Time (CET)** | [Date and Time] |
| **Exercise Location(s)** | [Physical/Virtual locations] |
| **Exercise success criteria** | How to measure - e.g., [Response time under 30 minutes"] |

# Scenario Overview

Provide 2-3 paragraph summary of the scenario, including the threat actor, attack type, affected systems, and general storyline.

Example: [This exercise simulates a coordinated cyberattack by APT-TransStrike targeting European transportation infrastructure. The attack begins with a supply chain compromise of railway signaling equipment, followed by escalating disruptions to port operations, aviation systems, and logistics networks. Players will respond to a 48-hour crisis affecting multiple EU member states...]

# Master Events and Injections Table

This table below is offering a structured approach to defining events, incidents and injects. The table can therefore be duplicated, as there can be multiple events and events could have several incidents.

|  |  |
| --- | --- |
| **Event 1: TITLE** | |
| [Enter event 1 description] | *[Enter incidents related to event 1]* |
| **Incident 1: TITLE** | |
| [Enter Incident 1 description] | *[Enter injects related to incidents 1]* |
| *Inject 1* | |
| *Inject Title* | *[Enter inject title]* |
| *Status* | *[Enter status]* |
| *From* | *[Enter entity]* |
| *Sent at* | *[Enter date and time]* |
| *Recipients* | *[Enter recipients]* |
| *Subject* | *[Enter subject]* |
| *Description* | *[Enter description]* |
| *Content* | *[Enter content of the inject]* |
| *Links* | *[Enter link]* |
| *Evaluation Criteria* | [Criterion 1 - e.g., "Response Time"] - [Success = <15 min / Partial = 15-30 min / Failure = >30 min].  [Criterion 2 - e.g., "Correct Procedure"] [Did they follow SOP? Yes/Partially/No].  [Criterion 3 - e.g., "Communication"] [Notified stakeholders? Yes/No].  [Criterion 4 - e.g., "Technical Action"] [Blocked threat? Yes/Partially/No] |
| *Inject 2* | | |
| *Inject Title* | | *[Enter inject title]* |
| *Status* | | *[Enter status]* |
| *From* | | *[Enter entity]* |
| *Sent at* | | *[Enter date and time]* |
| *Recipients* | | *[Enter recipients]* |
| *Subject* | | *[Enter subject]* |
| *Description* | | *[Enter description]* |
| *Content* | | *[Enter content of the inject]* |
| *Links* | | *[Enter link]* |
| *Evaluation Criteria* | | *[Criterion 1 - e.g., "Response Time"] - [Success = <15 min / Partial = 15-30 min / Failure = >30 min].*  *[Criterion 2 - e.g., "Correct Procedure"] [Did they follow SOP? Yes/Partially/No].*  *[Criterion 3 - e.g., "Communication"] [Notified stakeholders? Yes/No].*  *[Criterion 4 - e.g., "Technical Action"] [Blocked threat? Yes/Partially/No]* |

# Group and Player Information

## Group Information

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Group ID** | **Group Name** | **Role in the Exercise (e.g. Primary**  **Responder)** | **Number of participants** | **Physical Location** | |
| 01 | *IT Support* | *Responders* | *5* | *Athens/Greece* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Player Information

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Name** | **Email** | **Organisation** | **Group ID** |
| 01 | *John Doe* | *John.doe@itsupport.com* | *Agency* | *IT Support* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Simulated Entities

These entities are SIMULATED by the ExCon and will interact with players:

|  |  |  |  |
| --- | --- | --- | --- |
| **Entity** | **Type** | **Simulated By** | **Contact Method** |
| *[National Media]* | *News Organization* | *[Controller name]* | *Email, fake news website* |
| *[Regulatory Authority]* | *Government* | *[Controller name]* | *Official letters, phone calls* |
| *[Vendor/Partner]* | *Third Party* | *[Controller name]* | *Email, phone* |
| *[Law Enforcement]* | *Police/FBI/Europol* | *[Controller name]* | *Phone, email* |
| *[Customer/Public]* | *Stakeholder* | *[Controller name]* | *Social media, email* |