

OT-based Security Incidents Detection and Analysis Template

Note: Prior to starting the OT-based Security Incidents detection and analysis, Section 1 and Section 2 must be filled with required information.

Section 1: Details of the Organization

Organization Name:	
Contact Number:	
Website:	
Address:	
<i>Additional Contact Information:</i>	

Section 2: Details of the Incident Responder

Date Report Received:		Date Report Processing Began:	
Name:		Report Number:	
Title:		Department:	
Email Address:			
Phone Number and, If Applicable, Extension:			

Section 3: OT-based Security Incidents Detection and Analysis

❑ Incident ID _____

Details of the incident

❑ Indicators of the Attack _____

OT device affected due to the incident _____

Details of the indicators:

❑ Detecting OT-based Network Anomalies

Tools/techniques used _____

Results obtained:

☐ **Capturing OT-based Network Traffic**

Tools/techniques used _____

Results obtained:

☐ **Analyzing OT-based Network Traffic**

Tools/techniques used _____

Results obtained:

☐ **Analyzing OT-based Logs**

Tools/techniques used _____

Results obtained: