

Containment of OT-based Security Incidents Checklist

Note: Prior to starting the containment of OT-based security incidents, 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: Checklist for Containing OT-based Security Incidents	
Actions	Completed
Check whether the indicators of compromise (IoCs) are blocked based on prior analysis of the attack or malware.	<input type="checkbox"/>
Check whether communication with the external network and suspicious IP addresses across the OT network environment is blocked.	<input type="checkbox"/>
Check whether the DNS sinkhole technique is used to contain the incident on the OT systems.	<input type="checkbox"/>
Check whether the network processes are terminated based on prior analysis of the attack.	<input type="checkbox"/>
Check whether the access control lists (ACL) on firewalls are changed with the assistance of ICS engineers and network architects.	<input type="checkbox"/>
Check whether the critical components of the ICS/OT network and systems are isolated.	<input type="checkbox"/>
Check whether any unused system or network services are disconnected.	<input type="checkbox"/>
Check whether safety instrument systems are isolated.	<input type="checkbox"/>
Check whether access to suspected industrial OT protocols is blocked.	<input type="checkbox"/>
Check whether the detected suspicious IPS signatures of ICS/OT protocols are restricted.	<input type="checkbox"/>
Check whether any physical network device connected to the instrumentation networks in the OT environment is removed.	<input type="checkbox"/>
Check whether unauthorized cross-level communications are blocked.	<input type="checkbox"/>
Check whether unauthorized and remote access to the OT system is deactivated.	<input type="checkbox"/>
Ensure to use SCADA/ICS simulators in the sandboxing process.	<input type="checkbox"/>
Ensure to revoke the changes made in the system, such as logic changes, firmware downloads, corrupted OT packets, online edits to PLC projects, etc.	<input type="checkbox"/>
Check whether any removable device/USB access to the OT network is disabled or blocked.	<input type="checkbox"/>