

# Eradication of OT-based Security Incidents Checklist

**Note:** Prior to starting the eradication 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 Eradicating OT-based Security Incidents	
Actions	Completed
Check whether all compromised systems in the OT environments are remediated.	<input type="checkbox"/>
If the incident involves rootkits, rebuild the hardware.	<input type="checkbox"/>
Check whether patches are installed and network configuration is restored.	<input type="checkbox"/>
Check whether access to compromised accounts and systems in the OT environment is restricted.	<input type="checkbox"/>
Check whether passwords on all compromised accounts are reset.	<input type="checkbox"/>
Check whether the compromised files are replaced with clean and updated versions.	<input type="checkbox"/>
Check whether the latest PLC program and HMI program are installed.	<input type="checkbox"/>
Check whether the affected OT systems are reimaged from backup sources or rebuild systems from scratch.	<input type="checkbox"/>
Check whether backup of historian data is retrieved.	<input type="checkbox"/>
Ensure to monitor for any signs of the attacker's response to containment activities.	<input type="checkbox"/>
Check whether multifactor authentication is enforced for all remote access to OT networks and devices.	<input type="checkbox"/>
Check whether anti-malware software or next-generation antivirus (NGAV) is utilized to scan compromised systems and ensure all malicious content is removed.	<input type="checkbox"/>
Check whether continuous analysis and logging of network traffic are performed with SIEM.	<input type="checkbox"/>

Check whether a zero-trust security model is applied in the OT environment to restrict unwanted devices, insecure PLCs, sensors, and controllers.	<input type="checkbox"/>
Check whether access control lists (ACLs) are applied on the OT network to filter port input packets.	<input type="checkbox"/>
Check whether jump boxes are utilized on the OT platform to isolate and monitor access to systems.	<input type="checkbox"/>
Check whether deep packet inspection (DPI) is performed to monitor the OT network behavior and identify compromised devices.	<input type="checkbox"/>