

Eradication of IoT-based Security Incidents Checklist

Note: Prior to starting the eradication of IoT-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 IoT-based Security Incidents	
Actions	Completed
Check whether strong usernames and passwords are used for IoT devices and change the default passwords.	<input type="checkbox"/>
Check whether multifactor authentication mechanism is enabled on the IoT devices for identity confirmation while accessing an IoT device.	<input type="checkbox"/>
Check whether a dedicated IoT manager is used to manage the IoT network for continuous monitoring, managing alerts, updating, and reporting incidents.	<input type="checkbox"/>
Check whether machine learning technology is used to analyze and identify IoT-based security incidents as quickly as possible.	<input type="checkbox"/>
Check whether intrusion detection and intrusion prevention systems are used to defend IoT-based attacks.	<input type="checkbox"/>
Ensure to perform a factory reset and reconfigure the device settings of the affected IoT devices.	<input type="checkbox"/>
Check whether the network activity of the device is mapped to eradicate the malware completely from the network.	<input type="checkbox"/>
Check whether the SSL certificates of the websites are verified before they interact with the IoT device.	<input type="checkbox"/>
Check whether the registry file(s) of malware is deleted from the device firmware.	<input type="checkbox"/>
Check whether IoT devices' access privileges to high-risk features such as location, camera, and microphone are denied.	<input type="checkbox"/>
Check whether unnecessary communications are restricted between IoT devices and the Internet.	<input type="checkbox"/>
Check whether unusual data access privileges are removed for IoT devices to eliminate risks of data exposure.	<input type="checkbox"/>
Check whether the network backdoors are detected and removed, such as Telnet on the IoT device firmware.	<input type="checkbox"/>

Check whether a port scan is running on the IoT devices and close unsecured and unused ports.	<input type="checkbox"/>
Check whether the IoT devices are updated with the latest application software and firmware to patch the identified vulnerabilities.	<input type="checkbox"/>
Check whether automation is used to continuously discover new IoT devices connecting to the network and then apply appropriate security controls.	<input type="checkbox"/>