

Containment of IoT-based Security Incidents Checklist

Note: Prior to starting the containment 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 Containing Mobile-based Security Incidents	
Actions	Completed
Check whether the infected IoT devices are disconnected from the network and isolate the devices for analysis.	<input type="checkbox"/>
Check whether IoT devices with remote access features are disabled.	<input type="checkbox"/>
Check whether access passwords have been changed for all IoT devices connected to the network after identification of a security incident.	<input type="checkbox"/>
Check whether the IP address from where the attack traffic originated is blocked.	<input type="checkbox"/>
Ensure to immediately update and patch all compromised devices' software.	<input type="checkbox"/>
Check whether the Wi-Fi network password is changed to disconnect suspicious wireless IoT devices from the network.	<input type="checkbox"/>
Check whether the specific sub network is isolated from the compromised IoT devices using VLANs.	<input type="checkbox"/>
Check whether remote access, file-sharing, and universal plug and play features on IoT devices are disabled.	<input type="checkbox"/>
Check whether the IoT devices are blocked from unnecessary communication with other networked devices.	<input type="checkbox"/>
Check whether unauthorized data access, storage, and transmission are blocked from IoT ecosystems.	<input type="checkbox"/>
Check whether tools such as Nmap, Shodan, and Masscan are implemented for IoT device discovery and management purposes.	<input type="checkbox"/>
Check whether the compromised IoT devices are isolated safely without exposure to any data theft or business loss.	<input type="checkbox"/>
Check whether the affected devices are shifted to a sandbox environment without shutting down or rebooting them.	<input type="checkbox"/>

Check whether existing usernames and passwords are changed with unique, complex characters for devices having remote login capability.	<input type="checkbox"/>
Check whether outbound requests or commands to establish connections with IoT devices are blocked.	<input type="checkbox"/>
Check whether the IP address range of IoT devices are limited to only necessary connections and gateways.	<input type="checkbox"/>
Check whether the compromised devices are blacklisted to facilitate incident response investigation and prevent future attacks.	<input type="checkbox"/>
Check whether vulnerable IoT network services and access to critical resources are blocked.	<input type="checkbox"/>
Check whether all rogue devices and access points present in the IoT network are removed.	<input type="checkbox"/>