

Containment of Cloud Security Incidents Checklist

Note: Prior to starting the containment of cloud 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 Cloud Security Incidents	
Actions	Completed
Make sure communication with the external network is blocked until the incident is detected and resolved	<input type="checkbox"/>
Check if the incident has affected backups, and route the services through backup systems	<input type="checkbox"/>
Make sure the accounts, files, hosts, devices, servers, and other affected resources are disconnected from the network in case of a malware attack	<input type="checkbox"/>
Check whether the attacker's IP addresses and compromised accounts used to perform the attack are blocked	<input type="checkbox"/>
Make sure the services that are vulnerable to the attack are stopped in case of an application attack	<input type="checkbox"/>
Check whether the VM instances affected or connected to the affected host are isolated	<input type="checkbox"/>
Check whether the access to databases is revoked	<input type="checkbox"/>
Check whether the access is disabled to the infected VM while keeping important forensic evidence, such as active network connections and memory contents	<input type="checkbox"/>
Send suspicious processes or accounts to the sandbox environment to monitor their activities	<input type="checkbox"/>
Check whether the compromised resources are isolated from the network	<input type="checkbox"/>

Section 4: Checklist for Containing Azure Security Incidents	
Actions	Completed
Check whether the global administrative access is limited to critical resources	<input type="checkbox"/>
Make sure unknown communication channels are blocked using both internal and external security controls	<input type="checkbox"/>
Review and disable suspicious Azure accounts	<input type="checkbox"/>
Check whether the critical data from public storage is removed, such as blobs, and clear the cached content	<input type="checkbox"/>
Establish number matching for MFA	<input type="checkbox"/>
Check whether the permissions of managed identities are restricted	<input type="checkbox"/>
Check whether the unnecessary roles or permissions for resource management are deleted	<input type="checkbox"/>
Check whether the unnecessary policies from key vault access policies are audited and removed	<input type="checkbox"/>
Check whether a zero-trust model is implemented for continuous validation of Azure accounts	<input type="checkbox"/>
Check whether the Next Security Groups (NSGs) and host-based firewalls are used to filter and block malicious traffic	<input type="checkbox"/>
Frequently validate existing security controls for effective containment of incidents	<input type="checkbox"/>
Check whether an automation feature in Azure Security Center and Sentinel is enabled to run a playbook, which can disable problematic network connections	<input type="checkbox"/>
Discard unused virtual machines and subnets	<input type="checkbox"/>
Check whether a proper network segmentation is implemented to stop the spreading of infections to other Azure networks	<input type="checkbox"/>
Check whether the Microsoft Defender for Cloud is configured to predict and block threats in advance	<input type="checkbox"/>

Section 5: Checklist for Containing AWS Security Incidents	
Actions	Completed
Check whether the sandbox environment is implemented to test and isolate the affected systems	<input type="checkbox"/>
Protect Amazon EC2 instance from accidental termination by enabling termination protection	<input type="checkbox"/>
Build containment procedures based on alerts, resources, environment, data, etc.	<input type="checkbox"/>
Check whether your containment plans are tested regularly	<input type="checkbox"/>
Make sure you Isolate the Amazon EC2 instance by switching the VPC security group	<input type="checkbox"/>
Make sure the failure plans are developed in case of ineffective containment techniques	<input type="checkbox"/>
Identify the security group associated with the affected instance and delete all the existing rules	<input type="checkbox"/>
Make sure a dedicated "Isolation" security group rule is implemented for applications	<input type="checkbox"/>
Create a custom route table and identify the subnet related to the instance; then, associate the custom route table with the subnet of the AWS instance	<input type="checkbox"/>
Detach all Internet gateway routes from the tables	<input type="checkbox"/>
Check whether a custom route table is implemented with no interconnection routes within the VPC	<input type="checkbox"/>
Check whether options for containment are available based on the requirements and the situation	<input type="checkbox"/>

Section 6: Checklist for Containing Google Cloud Security Incidents	
Actions	Completed
Check whether unauthorized access to the Google Cloud Platform is blocked	<input type="checkbox"/>
Check whether the suspicious IP addresses are blocked and unused network services are disconnected	<input type="checkbox"/>
Create a snapshot of the virtual machine disk for forensic investigation after the workload is redeployed or deleted	<input type="checkbox"/>
Inspect the virtual machine while the workload is running to identify and contain emerging threats	<input type="checkbox"/>
Start a fresh copy of the container and delete the compromised container	<input type="checkbox"/>
Limit ongoing damage using cloud-integration tools and fix the underlying issue	<input type="checkbox"/>
Check whether the compromised VM's and containers are isolated in the Google Cloud environment	<input type="checkbox"/>
Continuously manage access controls and enforce the principle of least privileges	<input type="checkbox"/>
Check whether the compromised cloud instance is removed from the Google Cloud environment	<input type="checkbox"/>
Check whether the compromised cloud accounts and user accounts are deleted	<input type="checkbox"/>
Update policies and anti-malware signatures	<input type="checkbox"/>
Use VPC Service Controls (VPC SC) to stop data exfiltration attempts	<input type="checkbox"/>