

# Eradication of Cloud Security Incidents Checklist

**Note:** Prior to starting the eradication of cloud security incidents checklist, 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:			
<i>Additional Details (If Any):</i>			

Section 3: Eradication of Azure Security Incidents Checklist	
Actions	Completed
Whether Microsoft Azure Sentinel is used to analyze the threat kill chain and respond through built-in orchestration	<input type="checkbox"/>
Whether the allowlist rules in the adaptive application control policy in the cloud defender mechanism is updated to identify new legitimate user behavior and avoid false positives	<input type="checkbox"/>
Whether the access to the compromised Azure accounts is revoked	<input type="checkbox"/>
Whether the anti-malware database is updated with the hashes and other information of the identified malware	<input type="checkbox"/>
Whether the vulnerabilities are patched and the configuration in the Azure environment is changed	<input type="checkbox"/>
Whether multi-factor authentication is implemented by blocking legacy authentication	<input type="checkbox"/>
Whether administrative access to the account that runs the ADFS service is prevented	<input type="checkbox"/>
Whether the inbound SMB access to the systems is restricted	<input type="checkbox"/>
Whether a group-managed service account (gMSA) is shifted from a service account; or a complex password for a service account is implemented	<input type="checkbox"/>
Whether unnecessary accounts from domain admins, backup operators, and enterprise admin groups are removed	<input type="checkbox"/>
Whether the krbtgt account is reset twice	<input type="checkbox"/>
Whether conditional access, such as location-based access, to all user and service accounts is implemented	<input type="checkbox"/>
Whether Azure MFA, Microsoft Authenticator App, and Windows Hello are used to eliminate attack vectors based on passwords	<input type="checkbox"/>
Whether anti-malware vendor updates are installed	<input type="checkbox"/>
Whether Azure DDoS protection along with a web application firewall are implemented to block malicious traffic	<input type="checkbox"/>
Whether Azure policy is enforced to block key vault creation and encryption operations illegitimately	<input type="checkbox"/>
Whether the database firewall rules are modified to restrict access	<input type="checkbox"/>

Section 4: Eradication of AWS Security Incidents Checklist	
Actions	Completed
Whether collaboration is made with the organization's leaders, including stakeholders and legal counsel, to obtain access to the environment and resources for eradication	<input type="checkbox"/>
Whether AWS Support is used to reduce the risk; it can handle requests, patches, backups, etc.	<input type="checkbox"/>
Whether automated incident response mechanisms with ThreatResponse suite such as AWS_IR CLI are developed for common security incidents	<input type="checkbox"/>
Whether security incident response simulations (SIRS) is implemented to practice incident response plans on internal events and create runbooks that guide during incident eradication	<input type="checkbox"/>
Whether the original access keys are deactivated and the secret/access keys and CLI commands are modified	<input type="checkbox"/>
Whether root user account access keys are removed	<input type="checkbox"/>
Whether the IAM users created by attackers are deleted and their passwords are changed	<input type="checkbox"/>
Whether the IAM role temporary security credentials are revoked	<input type="checkbox"/>
Whether the "Deny Policy" is enforced to deny all actions	<input type="checkbox"/>
Whether the spilled files from EBS volumes are removed	<input type="checkbox"/>
Whether the encrypted s3 objects are deleted	<input type="checkbox"/>

Section 5: Eradication of Google Cloud Security Incidents Checklist	
Actions	Completed
Whether the suspected compromised user accounts are temporarily suspended	<input type="checkbox"/>
Whether two-step verification with security keys in the Google Cloud environment are enabled	<input type="checkbox"/>
Whether all VMs and containers are updated	<input type="checkbox"/>
Whether the administrator account is set with recovery options	<input type="checkbox"/>
Whether account activity alerts are enabled to identify suspicious sign-ins or service setting changes by other administrators	<input type="checkbox"/>
Whether a defense-in-depth network strategy is implemented on the Google Cloud environment	<input type="checkbox"/>
Whether strong API key generation, storage, and management is implemented in the Google cloud environment	<input type="checkbox"/>
Whether VPC service controls (VPC SC) are used to restrict unauthorized access	<input type="checkbox"/>
Whether the principle of least privileges is implemented, and passwords on all compromised accounts are reset	<input type="checkbox"/>
Whether network traffic analysis tools are used to track and resolve abnormalities	<input type="checkbox"/>
Whether unauthorized use of user-managed service account keys is blocked	<input type="checkbox"/>
Whether it is ensured that Google cloud storage buckets are not publicly accessible	<input type="checkbox"/>
Whether Google Cloud Armor is used to stop unusual traffic flow	<input type="checkbox"/>
Whether zero-trust environment is implemented	<input type="checkbox"/>
Whether WAF and granular security policies are implemented	<input type="checkbox"/>

Section 6: Eradication of Google Kubernetes Engine Security Incidents Checklist	
Actions	Completed
Whether access to the Kubernetes cluster control plane is restricted	<input type="checkbox"/>
Whether the affected VM is quarantined from internal and external traffic	<input type="checkbox"/>
Whether the external IP address is detached from the affected VM and an intermediate VM is used to access it from another VM in the same network	<input type="checkbox"/>
Whether a fresh copy of the container is deployed, and the infected container is removed	<input type="checkbox"/>
Whether the infected container is transferred into the sandbox environment, in case the security incident is not controlled	<input type="checkbox"/>
Whether the workload and host VM are deleted if the impact is large	<input type="checkbox"/>
Whether the cloud platform is isolated using subnetworks, firewall rules, and IAM	<input type="checkbox"/>
Whether the proxy-based load balancer is enabled to limit other instances from exposer	<input type="checkbox"/>
Whether the HTTPS load balancer is enabled to mitigate future attacks such as SYN flood, IP flood, etc.	<input type="checkbox"/>
Whether access to Google Cloud Storage resources is disabled for all users	<input type="checkbox"/>
Whether Google Cloud data security tools are used to mitigate enterprise data loss and leakage	<input type="checkbox"/>
Whether encryption is enabled for data at rest and transit	<input type="checkbox"/>