Security Incident Management Runbook

Credential Stuffing

Revision:1
Date: August 14th, 2024

*Group: **3***
Ananthu Krishna Vadakkeppatt
Ramachandra Muralidhara
Syed Mujahid Hamid Ali
Yannish Kumar Ballachander Sreedevi

Table of Contents

Introduction

A particular type of cyberattack known as "credential stuffing" allows attackers to access accounts without authorization by using compromised usernames and password pairs that they obtained through former data breaches. The procedure to handle such events, includes the phases of detection, analysis, containment, eradication, recovery, and post-incident, is provided in this runbook.

Data Classification

The Organization's Data Classification Standard is used to determine the overall impact.

Classification	Definition	Example
Confidential	Data that may cause harm to the company and/or public if compromised.	• Access to Personal Identifiable Information (PII)
Internal	Data that is owned by the organization that may result in financial loss if compromised.	• Access to organization's sensitive records.
Public	Data that is made available to the public consumption.	• Contact information • Business hours

Technologies, Systems, Services, Process

Name	Definition	Capabilities
Security Incident and Event Management (SIEM)	A centralized log repository.	• Unifies the process of threat detection and investigation that increases productivity. • Logs collected are analyzed to create alerts, dashboards or reports. • Can be used for monitor or respond to security incidents based on various predefined rules.
Multi-Factor Authentication	Multiple factors for secure access.	• Acts an extra layer of security over your accounts. • Takes away risk associated with using the same password.

User & Entity Behavior Analytics	A security technology that uses machine learning and analytics to detect abnormal behavior in users and entities.	• Identifies potential insider threats, compromised accounts, and advanced persistent threats by analyzing deviations from normal behavior patterns. • Provides risk scoring and prioritization of threats based on behavioral anomalies.

Response Procedures

Detection Phase

Role/Team/System	Description	Objectives	Action
User	An employee who works within the same organization and identifies multiple logins attempts on his or her account.	To report incident through channels recommended such as email.	Send an email to the Service Desk informing them about the malicious attempts by the attacker.
Security Analyst	Analyzes the logs related to the activity described by the user and sends it to the UEBA.	To investigate about the incident and assess its impact as well as legitimacy.	Analyze the evidence and proceed to send the same to the User and Entity Behavior Analytics if necessary.
User and Entity Behavior Analytics	It is a system that is used to analyze or monitor user behavior to detect anomalies.	Carry out further tests to indicate a pattern used by the attacker that can pinpoint a security threat.	Flags login attempts considered to be malicious and provides the security analyst with additional information.

Analysis Phase

Role/Team/System	Description	Objectives	Action
Security Analyst	Is responsible for analyzing logs or	Determines the impact, scope and nature of the	Analyzes logs as well as alerts to look for patterns in order

	examining security alerts.	security risk and provides remediation methods.	to identify vital information.
Threat Intelligence Analyst	Receives important threat intelligence data that needs to be analyzed to come up with answers.	Provides detailed explanation about the impact of the attack on the organization.	Uses Indicators of compromise collected by the security analyst to figure out the type of attack used.
Forensic Analyst	Performs detailed analysis focused on the physical section of the security incident.	Goal is to discover technical details that are related to the security incident.	Determine the surface area which was affected by the attack.
Incident Response Lead	The personnel responsible for responding to these security incidents.	Ensure that there is a response drafted with accurate information.	Oversee the process of incident response and document every action as well as findings.

Containment Phase

Role/Team/System	Description	Objectives	Action
System Administrator	Responsible for managing and maintain IT infrastructure.	To prevent further risk of unauthorized access by the attacker.	- Block the account of the victim until they verify it manually using a call or something else. - Ask the user to implement the use of multi-factor authentication systems to strengthen the

			security of their account.
Network Administrator	Responsible for managing and maintaining the network infrastructure.	To prevent security risks from such sources.	- Block the IP addresses used by the attacker. - Also employ other techniques such as rate limiting or throttling that diminish the amount of requests that can be made by a single IP.

Eradication Phase

Role/Team/System	Description	Objectives	Action
Security Analyst	Responsible for analyzing the logs and alerts.	Verify that all indicators of compromise are addressed.	Make sure that there are no other logs or alerts that remain which can increase the chances of residual threats.
IT Support Team	Provides technical support and troubleshooting.	To assist in applying necessary patches and updates.	Relay effective countermeasures to the victims such as that they do not fall prey to do the same attack.
System Administrator	Manages and maintains IT systems and infrastructure.	To remove malicious access and restore normal operations.	Remove any unauthorized user accounts or access credentials that were created or compromised during the attack.

Recovery Phase

Role/Team/System	Description	Objectives	Action
System Administrator	Manages and maintains IT systems and infrastructure.	To restore normal operations and ensure system stability.	Restore affected systems from clean backups, and verify that systems are functioning correctly and securely.
Security Analyst	Responsible for analyzing the logs and alerts.	To verify that the threat has been fully eradicated and that systems are secure.	Conduct post-recovery validation to ensure that all systems are free from vulnerabilities and that no traces of the attack remain.
IT Support Team	Provides technical support and troubleshooting.	To assist users and systems during the recovery process.	Support affected users by resetting passwords, verifying account security, and aiding as needed to ensure smooth operations.

Post-Incident Phase

Role/Team/System	Description (optional)	Objectives	Action
CISO	Responsible for the organization's overall information security strategy.	To keep stakeholders informed and ensure strategic alignment.	Communicate the outcome of the incident to the senior leadership team (SLT) and provide recommendations for future security enhancements.
Incident Response Lead	The personnel responsible for responding to these security incidents.	To finalize the incident response process and ensure	Document the incident response efforts, including timelines, actions

		all actions are documented.	taken, and outcomes, and prepare a final report.
IT Support Team	Provides technical support and troubleshooting.	To ensure all systems are functioning properly post-incident.	Verify that all systems have returned to normal operation and that any residual issues are resolved.