Incident Timeline

This document details the timeline of events and actions taken during the simulated security incident.

Timestamp	Event	Action Taken	Status
Feb 13 06:15:01	First failed login attempt for victim_user recorded.	None (initial detection phase)	Detected
Feb 13 06:15:36	Tenth failed login attempt for victim_user recorded.	None (initial detection phase)	Detected
Feb 13 06:15:38	Successful login by victim_user (simulated unauthorized access).	None (initial detection phase)	Confirmed
Feb 13 06:16:29	Analysis of journalctl logs initiated.	Log analysis to identify suspicious activity.	In Progress
Feb 13 06:16:33	Incident classified as Brute-Force / Unauthorized Access (High Severity).	Incident classification completed.	Completed
Feb 13 06:16:35	victim_user account locked and active sessions terminated.	Containment measures applied.	Completed
Feb 13 06:16:37	Investigation for malicious files/artifacts initiated.	Remediation efforts.	In Progress
Feb 13 06:16:40	victim_user account and home directory removed.	Threat removed and root cause (compromised account) addressed.	Completed
Feb 13 06:16:42	System checked for remaining artifacts.	System restoration and verification.	Completed