

Timeline of Events

Security Breach Investigation Report

Date & Time	Event	Description	Responsible Party
2024-05-12 08:10	Initial Alert	Intrusion detection system triggered on server S-02.	IT Security Team
2024-05-12 08:18	Attack Confirmed	Unusual login activity observed; unauthorized access confirmed.	Network Admin
2024-05-12 08:30	Containment Initiated	Compromised accounts disabled and affected systems isolated.	IT Security Team
2024-05-12 09:05	Investigation Begins	Logs and affected files retrieved for analysis.	Incident Response Team
2024-05-12 11:20	Stakeholder Notified	Management and legal team informed of breach incident.	Security Lead
2024-05-13 09:45	Root Cause Identified	Attack exploited unpatched vulnerability (CVE-2024-XXXX).	Security Analyst
2024-05-13 13:10	Remediation	Systems patched, credentials reset, and monitoring intensified.	IT Operations
2024-05-14 10:30	Post-Incident Review	Debrief session held; incident response procedure evaluated.	Incident Response Team

Important Notes

- Ensure all entries in the timeline are precise, factual, and time-stamped.
- Timeline should be updated in real-time or as soon as information becomes available.
- Maintain objectivity; avoid speculation or unverified information.
- Store this document securely to protect sensitive details during and after investigation.
- Timeline can be referenced for legal, compliance, and post-mortem review.