Incident Response Playbook
Large Scale Compromise

Phase 1: Preparation

Create an incident response plan that outlines each team member's roles and responsibilities as well as the steps to take in the event of a large-scale compromise attack.

Create an incident response team, which should include a team leader, technical professionals, communication experts, and legal counsel.

Identify the critical systems and services that are crucial to business operations. To guarantee that these assets are safeguarded in the event of an assault, identify and rank them.

Use tools and systems to monitor network traffic and spot any strange activity as you implement monitoring and alerts. Establish alerts to inform the incident response team of any questionable activities.

Phase 2: Detection and Analysis

Determine the attack's scope by evaluating its effects and identifying the users, services, and systems that were impacted.

Data collection and analysis Gather information about the attack, such as the originating IP addresses, traffic patterns, and attack type. To create a strategy for your reaction, use this information.

Choose an assault vector: Decide whether phishing emails, unpatched vulnerabilities, or other methods were used by the attackers to gain access to the systems.

Identify the number and types of compromised systems, the data accessed, and the attack techniques employed to determine the scope of the compromise.

Phase 3: Containment, Eradication, and Recovery

To stop the attack, isolate the impacted services and systems to limit future harm. This can entail turning off impacted systems, banning traffic from particular IP addresses, or configuring network capacity restrictions.

Eliminate the attack by locating and eradicating any malware or malicious code that might be to blame. To stop upcoming threats, update your software and patches.

Rebuild systems as necessary after restoring them from clean backups. Make sure that the most recent antivirus definitions and patches are installed on all systems.

Conduct a post-event review: Examine the occurrence and pinpoint any flaws in the security controls or incident response plan. Utilize this knowledge to make future incident response efforts better.

Phase 4: Communication and Reporting

Notify all stakeholders: Share information about the incident and the actions taken to contain and stop the attack with all relevant parties, including management, staff, customers, and law enforcement agencies.

Provide updates: Inform all parties involved of the incident's status and its development.

Establish incident reports: Create an incident report detailing the incident's cause, effects, and resolution. Utilizing this report will help future incident response efforts and regulatory compliance.

Identify areas for improvement and revise the incident response strategy as necessary by holding a lessons-learned session with the incident response team.