Incidence Response Playbook- system intrusion (Malware)

Preparation :

1.1. Create a detailed incident response plan outlining the measures your team should follow in the event of a malware incursion before it occurs. Ensure that all stakeholders are aware of and have access to the plan.

1.2. Form a response team: Determine key persons who will be in charge of coordinating emergency response operations. Members of the IT security team, IT operations, legal, and senior management should all be present.

1.3. Establish clear communication channels and protocols: In the case of an incident, establish clear communication channels and protocols. Ascertain that all team members have current contact information for one another.

1.4. periodically backup data: Create a backup schedule and make sure that important data is periodically backed up.

1.5.Establish security measures within your firm, including firewalls, antivirus software, intrusion detection systems, and access controls.

Detection

2.1. Locate the malicious software: Determine out what kind and how much malware is infected. A comprehensive system scan utilizing antivirus software or other malware detection technologies can be used to do this.

2.2. Isolate the compromised system: To stop the malware from spreading further, disconnect the compromised system from the network.

2.3. Identify the infection's extent: Find out which systems are impacted and how much harm has been done.

Containment:

3.1 Disable all remote access to the compromised system in order to stop the malware from spreading.

3.2. Implement network segmentation: To stop malware from propagating, isolate the affected system from the rest of the network.

3.3. Turn off or quarantine infected devices: To stop the malware from spreading further, turn off all network connections and confine affected devices.

Eradication

4.1. Remove the malware: To remove the malware from the infected system, use antivirus software or other malware removal solutions.

4.2. Fix vulnerabilities: Determine whatever vulnerabilities the virus took use of and fix them.

4.3. Keep an eye on the system: Keep an eye on the system to make sure that the malware has been entirely eliminated and that no new infections have appeared.

Recovery

5.1. Restore from backup: Restore any information or computer systems that were harmed by malware from the most recent backup.

5.2. Test the system: Check the system to make sure it is operating properly and that the malware infection has not left any residual effects.

5.3. Conduct a post-event review to identify any areas that could want improvement and then revise the incident response plan as necessary.