Incidence response playbook- Identity- Based attacks

I. Preparation

* Create a comprehensive incident response plan that explains each team member's roles and responsibilities, as well as the measures to be done in the event of an occurrence.
* Establish security rules to protect important assets and apps that could be targeted in an attack.
* Employees should receive frequent security awareness training to educate them on the dangers of identity-based attacks and privilege abuse.

 II Detection

Examine logs and audit trails for any odd behavior involving privileged accounts, such as unlawful access or modifications to system configurations.

* To detect and prevent attacks involving privilege abuse, deploy intrusion detection and prevention systems.
* Use user behavior analytics (UBA) technologies to detect unusual user behavior and identify potential insider threats.

III. Response

1. Identify the incident:

* Gather and evaluate the facts at your disposal to ascertain the extent and gravity of the occurrence.
* Determine which programs and systems were impacted by the attack.
* Check to see if any private information was compromised.

1. Contain the incident:

* To stop additional harm, isolate the damaged systems and disconnect them from the network.
* Change the passwords on any hacked accounts and disable them.
* To stop further abuse of privileges, implement access controls and limit permissions for privileged accounts.

1. Investigate the incident

* Conduct a careful investigation to find out what caused the occurrence in the first place and to find any weaknesses that were misused.
* Gather and save evidence for potential legal or disciplinary action in the future.
* To coordinate the investigation and ensure adherence to any regulatory obligations, communicate with the pertinent stakeholders, including IT, legal, and management.

1. Resolve the situation

* Create a plan to address the vulnerabilities that the assault exploited.
* Patch or upgrade impacted apps and systems.
* Put security measures in place to stop similar instances from happening again.

1. Report the event

* Notify the appropriate parties about the occurrence and its effects, including clients, partners, and regulatory organizations.
* Provide frequent updates on the investigation and the steps being taken to stop similar events in the future.
* Review the incident response plan and make any necessary updates in light of the incident's lessons learned.

IV. Recovery

* Restore the systems and applications that were affected to normal operation.
* Check to make sure that all access and security measures are set up and working correctly.
* To assess the success of the incident response strategy and pinpoint areas for improvement, conduct a post-event evaluation.