Incidence Response playbook: Insider Threat- Privilege misuse

1. Initial response:
    - Inform the incident response team and other essential stakeholders, such as legal and human resources.
    - To prevent future harm, isolate the affected systems or devices.
    - Gather and save evidence linked to the occurrence, such as system logs, user activity records, and any other relevant data.
2. Investigation:
    - Determine the scope and effect of the incident, including the extent of the insider's data or system access.
    - Determine the person(s) responsible for the incident and their motivation.
    - Analyze activity logs and other pertinent data to comprehend the sequence of events and any other indicators of malicious activity.
    - Determine the organization's possible effect, including any sensitive or secret data that may have been accessed or exfiltrated.
3. Mitigation:
    - Remove insiders' access to all systems and data that aren't required for their job function.
    - To avoid such events in the future, implement extra security controls such as two-factor authentication or data loss prevention.
    - Increase monitoring and detection capabilities to detect similar instances and patterns of behavior.
4. Remediation:
    - Review and update system and data access policies and procedures to verify they are adequate to prevent repeat events.
    - Increase staff understanding of the hazards of insider threats and how to identify and report them by providing additional training.
    - As appropriate, consider legal and disciplinary action against the insider responsible for the occurrence.
5. Notification:
    - Determine whether the situation necessitates informing consumers, partners, or other stakeholders.
    - Notify affected parties in accordance with applicable laws or organizational policies.
    - To retain stakeholder trust, provide clear and accurate information about the incident, including the efforts done to mitigate and remediate it.
6. Post-incident Review:
    - Examine the incident response process to discover opportunities for improvement.
    - Examine whether the incident response strategy was effective and whether any changes are required.
    - Record the incident and reaction activities for future use and reference.