Szenarien Überlegungen

1. Beschränkung von Benutzeraktionen

- **Deaktivierung kompromittierter Benutzerkonten:**
  Sperren Sie ein Konto, das ungewöhnliche Aktivitäten aufweist.

  ```
  yaml
  ```

  ```
  - name: Disable suspicious user account
    hosts: all
    tasks:
      - name: Lock user account
        user:
          name: "{{ suspicious_user }}"
          state: absent
  ```

- **Passwortänderung erzwingen:**
  Ändern Sie ein Passwort und informieren Sie den Benutzer über die notwendigen Schritte.

---

2. Monitoring und Protokollierung

- **Erhöhte Protokollierungsstufe aktivieren:**
  Setzen Sie die Log-Level höher, um verdächtige Aktivitäten zu überwachen.

  ```
  yaml
  ```

  `- name: Enable debug logging hosts: all tasks: - name: Increase log level lineinfile: path: /etc/software.conf regexp: '^log_level' line: 'log_level=DEBUG' notify: - restart_service handlers: - name: restart_service service: name: software state: restarted`

- **Logs zu einem zentralen System senden:**
  Nutzen Sie eine zentrale Log-Verarbeitung (z. B. ELK oder Graylog), um verdächtige Muster zu analysieren.

---

3. Netzwerkaktionen

- **Firewall-Regeln anpassen:**
  Blockieren Sie IP-Adressen oder Ports, die mit verdächtigen Aktivitäten in Verbindung stehen.

  ```
  yaml
  ```

  ```
  - name: Block suspicious IP hosts: all tasks: - name: Add IP to firewall iptables: chain: INPUT source: "{{ malicious_ip }}" jump: DROP
  ```

- **Quarantäne-Netzwerk zuweisen:**
  Verschieben Sie einen Host in ein isoliertes VLAN für weitere Untersuchungen.

---

4. Datenaktionen

- **Ereignisdaten sammeln:**
  Sichern Sie kritische Protokolle und Speicherabbilder zur späteren Analyse.

  ```
  yaml
  ```

  ```
  - name: Collect logs for forensic analysis hosts: all tasks: - name: Archive logs command: tar -czvf /tmp/logs.tar.gz /var/log/ - name: Transfer logs to analysis server copy: src: /tmp/logs.tar.gz dest: /path/to/analysis_server/logs/
  ```

- **Sicherung sensibler Daten:**
  Bewegen Sie sensible Daten von einem gefährdeten System an einen sicheren Ort.

---

5. Systemaktionen

- **Automatische Schwachstellenbehebung:**
  Identifizieren und patchen Sie bekannte Schwachstellen.

  ```
  yaml
  ```

`- name: Apply security updates hosts: all tasks: - name: Update all packages apt: upgrade: dist`

- **Neustart oder Shutdown:**
  Fahren Sie ein System herunter, wenn ein schwerwiegendes Risiko besteht.

  ```
  yaml
  ```

  `- name: Shutdown compromised system hosts: compromised_node tasks: - name: Shut down system command: /sbin/shutdown now`

---

6. Benachrichtigungen und Integrationen

- **Automatische Benachrichtigungen:**
  Informieren Sie Admins über Vorfälle via Slack, E-Mail oder PagerDuty.

  ```
  yaml
  ```

  `- name: Send notification hosts: all tasks: - name: Send Slack alert uri: url: https://slack.com/api/chat.postMessage method: POST headers: Authorization: "Bearer YOUR_SLACK_TOKEN" Content-Type: "application/json" body: | { "channel": "#security-alerts", "text": "Suspicious activity detected on {{ inventory_hostname }}" } status_code: 200`

- **Service-Desk-Tickets erstellen:**
  Automatisieren Sie die Erstellung von Tickets in Systemen wie Jira oder ServiceNow.

---

7. Reaktionen für spezifische Bedrohungen

- **Ransomware-Angriff:**
  Trennen Sie betroffene Dateien oder verschieben Sie sie in einen quarantänebezogenen Speicher.
- **DNS-Spoofing:**
  Überschreiben Sie DNS-Cache oder aktualisieren Sie DNS-Servereinstellungen.
- **DoS-/DDoS-Angriff:**
  Nutzen Sie Ratenbegrenzung oder IP-Blacklist, um Angriffe zu entschärfen.