Incident Response

Process:

1. Preparation -> Training personnel, conducting regular security assessments, and have all necessary resources to handle a security incident
2. Detection -> Identifying potential security incidents (network monitoring, IDS and security audit)
3. Analysis -> Understand its nature and scope (type of attack, systems affected, data compromised, attack tactics/techniques/procedures (TTPS))
4. Containment -> Limit the scope and magnitude of the incident
5. Eradication -> Removing malware, closing security gaps, implementing patches
6. Recovery -> Ensure all systems are cleaned and secure before bringing back online
7. Lessons learned -> Post-incident review, lessons learned are documented and used to improve the incident response plan

Tabletop exercise -> Walk through various incident scenarios in a structured manner (validate the effectiveness of the incident response plan)