INVESTIGATION AND RECOVERY CHECKLIST

Detection & Verification

- Analyze suspicious email with links and attachments emails.
- Perform analysis on outdated softwares for vulnerabilities.
- Collect and analyze system, application, network, firewall, security logs.
- Examine system artifacts like registry changes, file system modifications, installed applications and services.
- Perform static, dynamic analysis and reverse engineering of samples.
- Conduct memory forensic by analyzing RAM dumps.
- Monitor alerts from security tools like antivirus software or network intrusion detection sensors.
- Look for unusual filenames with random characters, evidence of auditing configuration changes, or failed login attempts from unfamiliar remote systems.
- Correlate signals from security lanes to confirm a breach.
- Search for host artifacts such as unusual services, scheduled tasks, unfamiliar parent-child process trees, or tampering with antivirus/EDR solutions.
- Investigate identity anomalies, including first-time login locations, bursts of MFA fatigue, or ad-hoc administrative grants.
- Monitor for backup anomalies like sudden surges in change rates, tampering with retention policies, failed replications, or positive results from restore-time malware scans.

- Determine which systems have been compromised and what data has been accessed or affected.
- Mobilize the incident response team, which may include IT security staff, IT ops, forensic specialists, legal counsel, communications, management, and HR.
- Assign an incident manager to coordinate efforts.
- Do not immediately shut down systems. This can erase crucial forensic evidence like volatile system logs and memory dumps.
- Create a bit-for-bit duplicate of the original evidence file through drive imaging.
- Block all compromised accounts immediately.
- Force logout on all devices and accounts.
- Setup up MFA on all accounts and optional use of authenticator apps.
- Maintain detailed audit logs that record who accessed, modified, and transferred the evidence.
- Generate a unique hash value during the imaging process to verify the integrity and authenticity of the digital evidence.
- Store digital evidence in a secure repository with strong access controls and password protection.
- Encrypt all stored digital evidence, both at rest and in transit.

Containment & Eradication

- Isolate affected systems by shutting down ports, disabling network connections, or using automated tools to quarantine devices.
- Prioritize the isolation of critical assets and high-value data first.
- Create a physical or logical air gap to completely disconnect a network or system from external networks.
- Use virtualization to create independent, sandboxed environments to isolate systems, applications, or network segments on the same hardware.

- Implement network segmentation to limit the lateral movement of ransomware or other malicious activity.
- Restrict access to sensitive data or systems by tightening firewall rules or restricting user access.
- Delete malware, disable breached accounts, and fix the vulnerabilities that allowed the breach.
- Automate security updates using tools like unattended-upgrades or dnf-automatic to ensure consistency and continuous protection.
- Prioritize patching high-severity patches and those directly related to the breach.
- Maintain a central list of Indicators of Compromise (IOCs), which can include file hashes, IP addresses, and domains.
- Use updated antivirus or Endpoint Detection and Response (EDR) tools to scan and remove malicious code.
- Thoroughly eliminate any web shells or hidden backdoors.
- For heavily compromised systems, re-image them from a known-good backup instead of trying to clean them in place.
- Harden system configurations by disabling unused services, closing open firewall ports, and tightening access permissions.

Recovery & Restoration

- Provision a "clean room" or a sandboxed environment to test and validate restored data and applications.
- Verify that your backups are clean and uncompromised by reviewing access and change history and performing IOC scans on the backup data.
- Collect all identified IOCs like files, IP addresses, domain names, URLs, hashes, etc.
- Compile a list of all endpoints, systems, networks that have signs of IoCs.

- Collect and analyze ransomware artifacts like files with ransomware notes.
- Restore systems from clean, immutable, and air-gapped backups.
- Use backup logs and visibility tools to pinpoint the exact time and vector of the initial infection to ensure the recovery point predates any compromise.
- Thoroughly test and verify the integrity and functionality of restored systems before reconnecting them to the production network.
- Use IOC filtering to prevent the reintroduction of threats during the recovery process.
- Require strong passwords and Multi-Factor Authentication (MFA) to prevent unauthorized access.
- Limit user privileges by adhering to the principle of least privilege and utilizing Role-Based Access Control (RBAC).
- Disable unnecessary services, protocols, and remove unused accounts to reduce potential attack vectors.
- Whitelist critical applications to ensure only approved software can run.
- Encrypt local storage and network traffic to protect data at rest and in transit.
- Implement network segmentation to limit the lateral movement of threats.
- Establish appropriate firewall rules and deploy Intrusion Detection/Prevention Systems (IDPS).
- Ensure server backups are encrypted and tested regularly.
- Implement enhanced logging and continuous threat detection to watch for any anomalies after systems are back online.