

Task. Respond to a Category 3 Incident.

Purpose. The organization must be able to respond to the risk introduced by Category 3 incidents, otherwise known as “unsuccessful activity attempts,” to protect the usability and defensibility of its enterprise.

Conditions.

- **Incident Response Team.** The organization is staffed with personnel who possess the knowledge, skills, attributes, processes, and technology required to perform in the following DoD Cybersecurity Workforce Framework (DCWF) Work Roles: Information Systems Security Manager (ISSM), Incident Responder, Infrastructure Support Specialist, System Administrator, and Network Administrator.
- **Stakeholders.** The organization is able to call and email the following stakeholders: Information Owner, Information System Owner, commander, and Tier III (Installation) Cyber Security Service Provider (CSSP).
- **Incident Criteria.** The organization suspects the following activity has occurred: there were deliberate attempts to gain unauthorized access to an Information System (IS) (i.e., someone attempted valid or potentially valid username and password combinations) that were defeated by normal defensive mechanisms.
 - NOTE: this does not include exploratory scanning or “run-of-the-mill” viruses defeated/deleted by antivirus software.

Standard. The organization was able to contain the incident, determine the root cause, eradicate the threat/vulnerability, restore operations, implement lessons learned, and communicate with its stakeholders throughout each phase.

Analysis Phase

Bridge the gap between what was perceived and what actually happened. Using the Data Sources suggested, search for answers to the Questions listed below. If enough evidence suggests a Category 3 incident occurred, create a report with the information available and execute Containment procedures immediately (see next page). Otherwise, re-categorize the event as Category 8 “Investigating” or Category 9 “Explained Anomaly.” At the end of every incident response phase, update your report with any new Reportable Details collected and/or generated.

Data Sources

- Network: IDS alerts, NetFlow records, transactions (e.g., HTTP, DNS, SMB queries), statistics, and PCAP files.
- Host: memory artifacts (e.g., network connections, processes, services, scheduled tasks, etc.) and disk artifacts (logs, accounts, files, Windows Registry keys, etc.).

Questions

- Which IS did the culprit attempt to access?
- Which account on the IS in question did the culprit attempt to access?
- During what time periods did the culprit attempt to access the account and IS in question?
- How did the culprit attempt to authenticate (e.g., physically, remotely, etc.)?
- Were there any successful logins immediately after the failed login attempts?
- Are there any other ISs and/or accounts someone attempted and/or successfully authenticated with during the time of interest?

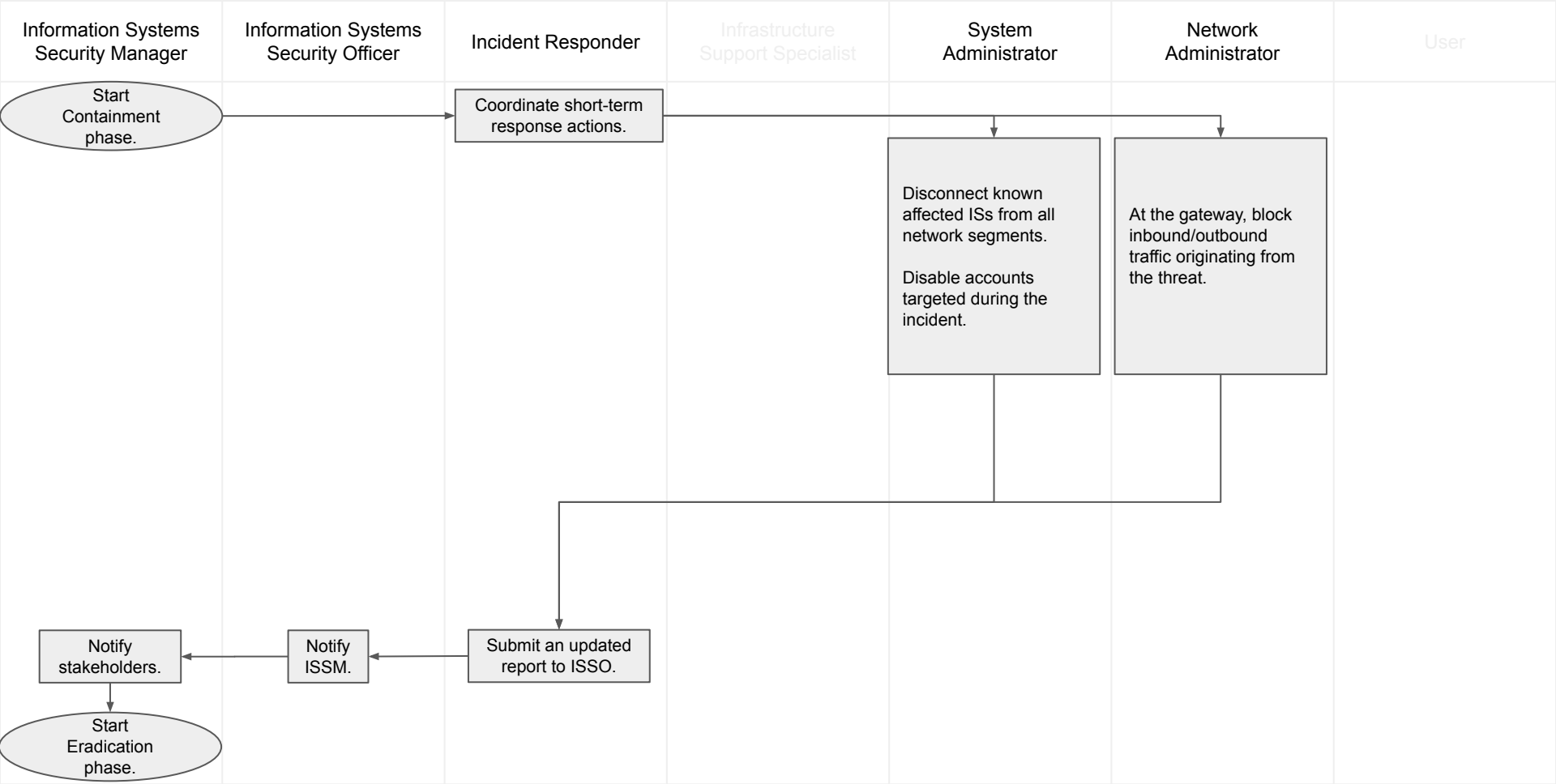
How to Investigate

- Select one of the Data Sources above, pick a field within it, and search other data sources for the value it contains. Repeat until you collect enough findings to suggest an incident has occurred.

Reportable Details

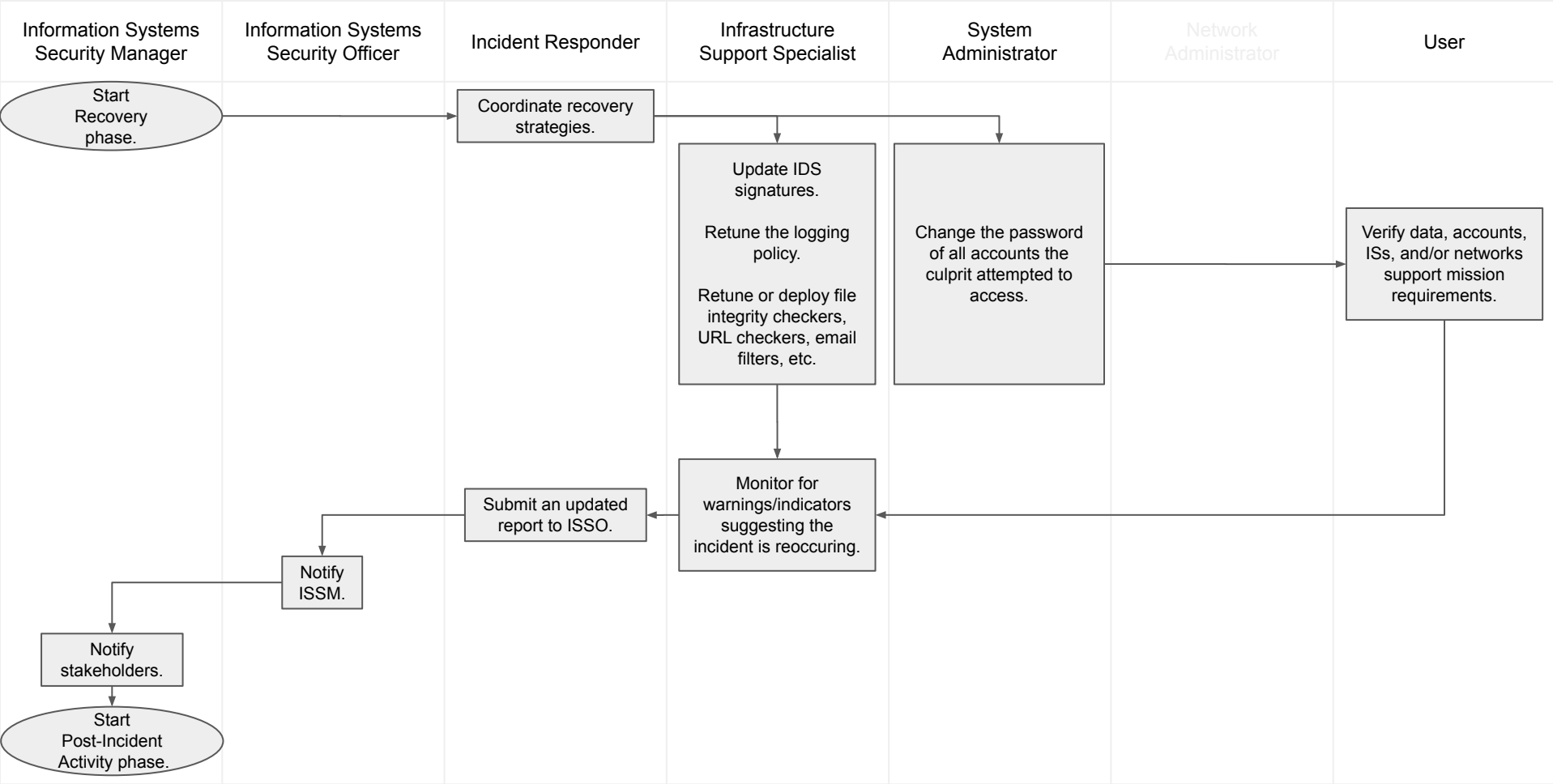
- Date-Time Groups (DTG) of when the incident started and was detected, contained, and resolved.
- Primary Point-of-Contact (POC) and alternate POC for incident.
- Category, summary, and root-cause of incident.
- Hostname, IP address, MAC address, make/model, serial number of devices affected.
- All actions taken (include the 5 Ws).

Category 3 Incident Response Plan
Containment Phase



Category 3 Incident Response Plan

Eradication & Recovery Phase



Category 3 Incident Response Plan

Post-Incident Activity Phase

