Task. Respond to a Category 1 Incident.

Purpose. The organization must be able to respond to the risk introduced by Category 1 incidents, otherwise known as "root-level intrusions," 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: an Information System (IS) was accessed by a privileged account (e.g., domain administrator) without authorization and/or malicious software that provides remote, interactive control was installed.

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.

Search for answers to the questions below to bridge the gap between what the organization thinks happened and what actually happened. If enough evidence suggests a Category 1 incident occurred, create a report and execute Containment procedures immediately. Otherwise, re-categorize the event as Category 8 "Investigating" or Category 9 "Explained Anomaly."

Questions

- What account was used to access the IS?
- Does this account have administrator privileges?
- Which ISs did the account access and at what time/day did they access these ISs?
- Who had access to the account and were working during these time periods?
- Did they have authorization to access the account and/or ISs during these time periods?

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).

Security Manager

Start

Information Systems

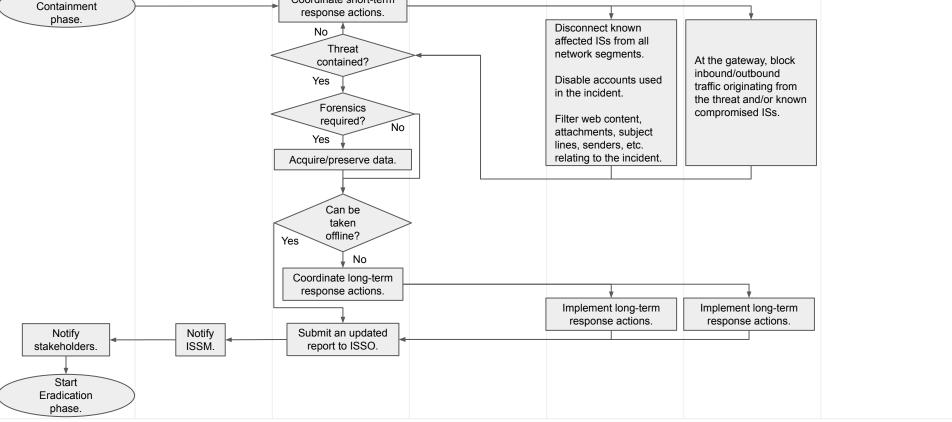
Security Officer

References

Category 1 Incident Response Plan Containment Phase

Network System Incident Responder Administrator Administrator Coordinate short-term Disconnect known affected ISs from all Threat network segments.

Page 3/6



References

NIST SP 800-61

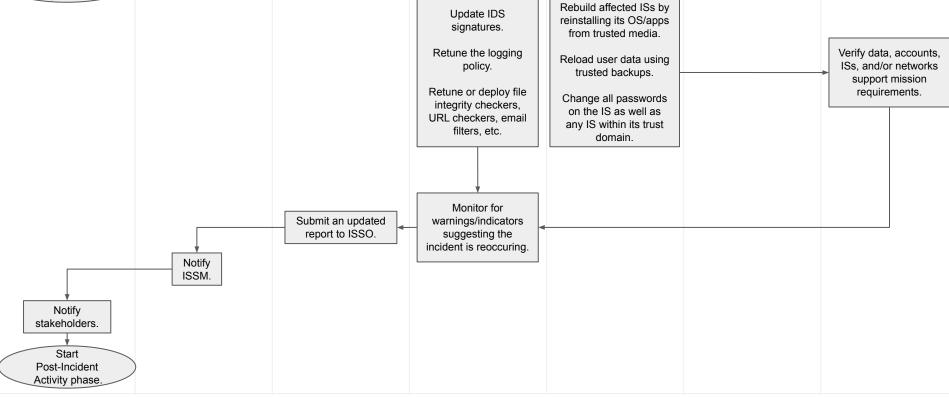
Category 1 Incident Response Plan Eradication Phase

Page 4/6

CJCSM 6510.01B DA PAM 25-2-14 DA PAM 25-2-17 Network Information Systems Information Systems Infrastructure System Incident Responder Security Manager Security Officer Support Specialist Administrator Administrator Start Eradication phase. Determine the root cause.

Develop mitigation strategies (patch, Patch vulnerable ISs reconfigure, etc.). and the baseline image (or implement a compensating control). Coordinate Remove other Correct Access mitigation strategies. access mechanisms Correct IS and Control List used by the baseline image misconfigurations. adversary. misconfigurations. Remove compromised accounts. Threat removed? No Yes Root cause Notify removed? stakeholders. No Yes Start Notify Submit an updated Recovery ISSM. report to ISSO. phase.

References



Security Manager

Start Post-Incident

Activity phase.

Notify

stakeholders.

Start Preparation phase.

Information Systems

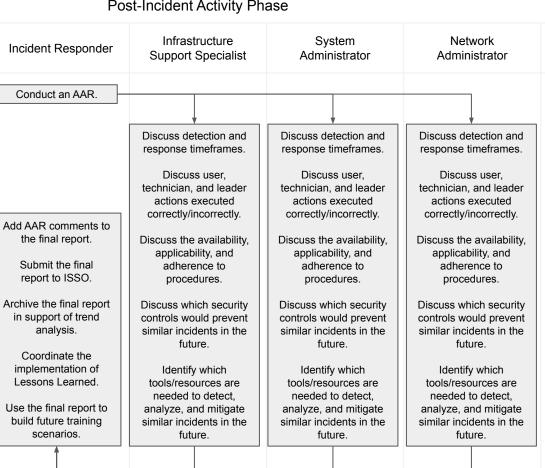
Security Officer

Notify

ISSM.

Category 1 Incident Response Plan Post-Incident Activity Phase





Page 6/6