Incident Response Policy, Plan, and Procedure Creation

Policy Elements:

- Statement of management commitment
- Purpose and objectives of the policy
- Scope of the policy (to whom and what it applies and under what circumstances)
- Definition of computer security incidents and related terms
- Prioritization or severity ratings of incidents
- Performance measures
- Reporting and contact forms.

Plan Elements

- Mission
- Strategies and goals
- Senior management approval
- Organizational approach to incident response
- How the incident response team will communicate with the rest of the organization and with other organizations
- Metrics for measuring the incident response capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization

Procedure Elements

- Procedures should be based on the incident response policy and plan.
- Standard operating procedures (SOPs) are a delineation of the specific technical processes, techniques, checklists, and forms used by the incident response team.
- SOPs should be reasonably comprehensive and detailed to ensure that the priorities of the organization are reflected in response operations.
- SOPs should be tested to validate their accuracy and usefulness.

SIX STEPS FOR EFFECTIVE INCIDENT RESPONSE

The SANS Institute provides six steps for effective incident response:

1. **Preparation:** Developing policies and procedures to follow in the event of a cyber breach. Key to this process is effective training to respond to a breach and documentation to record actions taken for later review.
2. **Identification:** This is the process of detecting a breach and enabling a quick, focused response.
3. **Containment:** One of the first steps after identification is to contain the damage and prevent further penetration.

Contd…

4. **Eradication:** This stage involves neutralizing the threat and restoring internal systems to as close to their previous state as possible. This can involve secondary monitoring to ensure that affected systems are no longer vulnerable to subsequent attack.

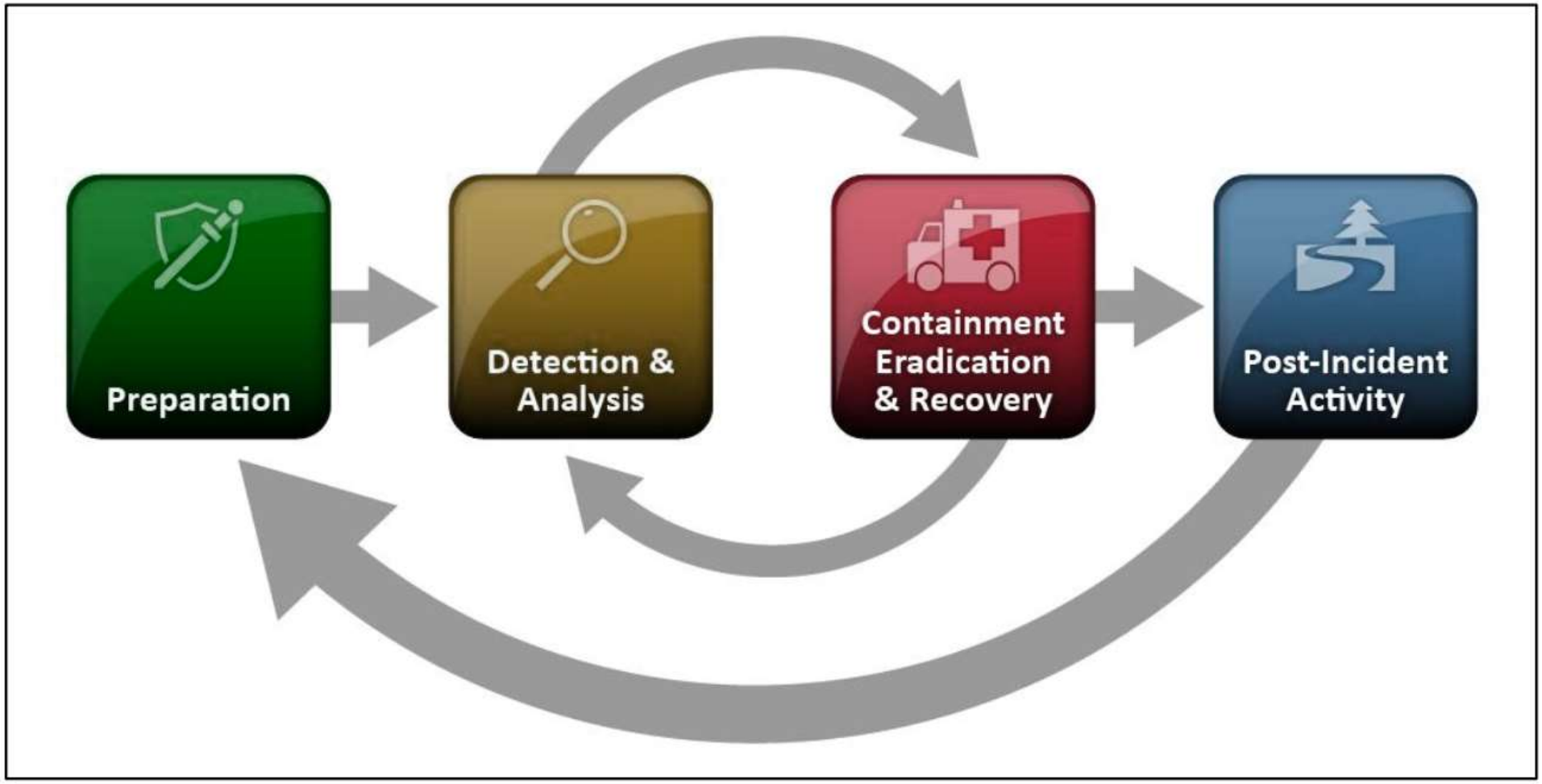
5. **Recovery:** Security teams need to validate that all affected systems are no longer compromised and can be returned to working condition.

6. **Lessons Learned:** During this stage, the incident response team and partners meet to determine how to improve future efforts. This can involve evaluating current policies and procedures, as well specific decisions the team made during the incident. Final analysis should be condensed into a report and used for future training.

Incident Response Team Services

1. **Intrusion Detection**
2. **Advisory Distribution** : A team may issue advisories within the organization regarding new vulnerabilities and threats.
3. **Education and Awareness :** Education and awareness are resource multipliers—the more the users and technical staff know about detecting, reporting, and responding to incidents, the less drain there should be on the incident response team.
4. **Information Sharing**

Incident Response Life Cycle



Preparation

1. Preparing to Handle Incidents

- Incident Handler Communications and Facilities:

- ✓ **Contact information**
- ✓ **On-call information**
- ✓ **Incident reporting mechanisms**
- ✓ **Issue tracking system**
- ✓ **Smartphones**
- ✓ **Encryption software**
- ✓ **War room**
- ✓ **Secure storage facility**

Contd…

- Incident Analysis Hardware and Software:

- ✓ Digital forensic workstations and/or backup devices
- ✓ Laptops
- ✓ Spare workstations, servers, and networking equipment, or the virtualized equivalents
- ✓ Blank removable media
- ✓ Portable printer
- ✓ Packet sniffers and protocol analyzers
- ✓ Digital forensic software
- ✓ Evidence gathering accessories

Contd…

- Incident Analysis Resources:

✓ Port lists
✓ Documentation
✓ Network diagrams and lists of critical assets
✓ Current baselines
✓ Cryptographic hashes

- Incident Mitigation Software:

Preparation Contd…

2. Preventing Incidents

- Risk Assessments.
- Host Security
- Network Security
- Malware Prevention
- User Awareness and Training.

Detection and Analysis

- ➢ Attack Vectors
- ✓ External/Removable Media
- ✓ Attrition
- ✓ Web
- ✓ Email
- ✓ Impersonation
- ✓ Improper Usage
- ✓ Loss or Theft of Equipment

Contd…

➢ Signs of an Incident

- ✓ Incidents may be detected through many different means, with varying levels of detail and fidelity.
- ✓ Automated detection capabilities include network-based and host-based IDPSs, antivirus software, and log analyzers.
- ✓ Incidents may also be detected through manual means, such as problems reported by users. Some incidents have overt signs that can be easily detected, whereas others are almost impossible to detect.
- ✓ The volume of potential signs of incidents is typically high—for example, it is not uncommon for an organization to receive thousands or even millions of intrusion detection sensor alerts per day.
- ✓ Signs of an incident fall into one of two categories: **precursors and indicators.** A *precursor* is a sign that an incident may occur in the future. An *indicator* is a sign that an incident may have occurred or may be occurring now.

Contd…

- Incident Analysis

- ✓ Incident detection and analysis would be easy if every precursor or indicator were guaranteed to be accurate.
- ✓ Profile Networks and Systems
- ✓ Understand Normal Behaviors
- ✓ Create a Log Retention Policy
- ✓ Perform Event Correlation
- ✓ Maintain and Use a Knowledge Base of Information
- ✓ Run Packet Sniffers to Collect Additional Data
- ✓ Filter the Data

Contd…

- Incident Documentation

- ✓ The current status of the incident
- ✓ A summary of the incident
- ✓ Indicators related to the incident
- ✓ Other incidents related to this incident
- ✓ Actions taken by all incident handlers on this incident
- ✓ Chain of custody, if applicable
- ✓ Impact assessments related to the incident
- ✓ Contact information for other involved parties (e.g., system owners, system administrators)
- ✓ A list of evidence gathered during the incident investigation
- ✓ Comments from incident handlers
- ✓ Next steps to be taken (e.g., rebuild the host, upgrade an application).

Contd…

➢ Incident Prioritization

Incidents should not be handled on a first-come, first-served basis as a result of resource limitations. Instead, handling should be prioritized based on the relevant factors, such as the following:

- ✓ *Functional Impact of the Incident*
- ✓ *Information Impact of the Incident*
- ✓ *Recoverability from the Incident*

Category	Definition
None	No effect to the organization's ability to provide all services to all users
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users
High	Organization is no longer able to provide some critical services to any users

Functional Impact Categories

Contd…

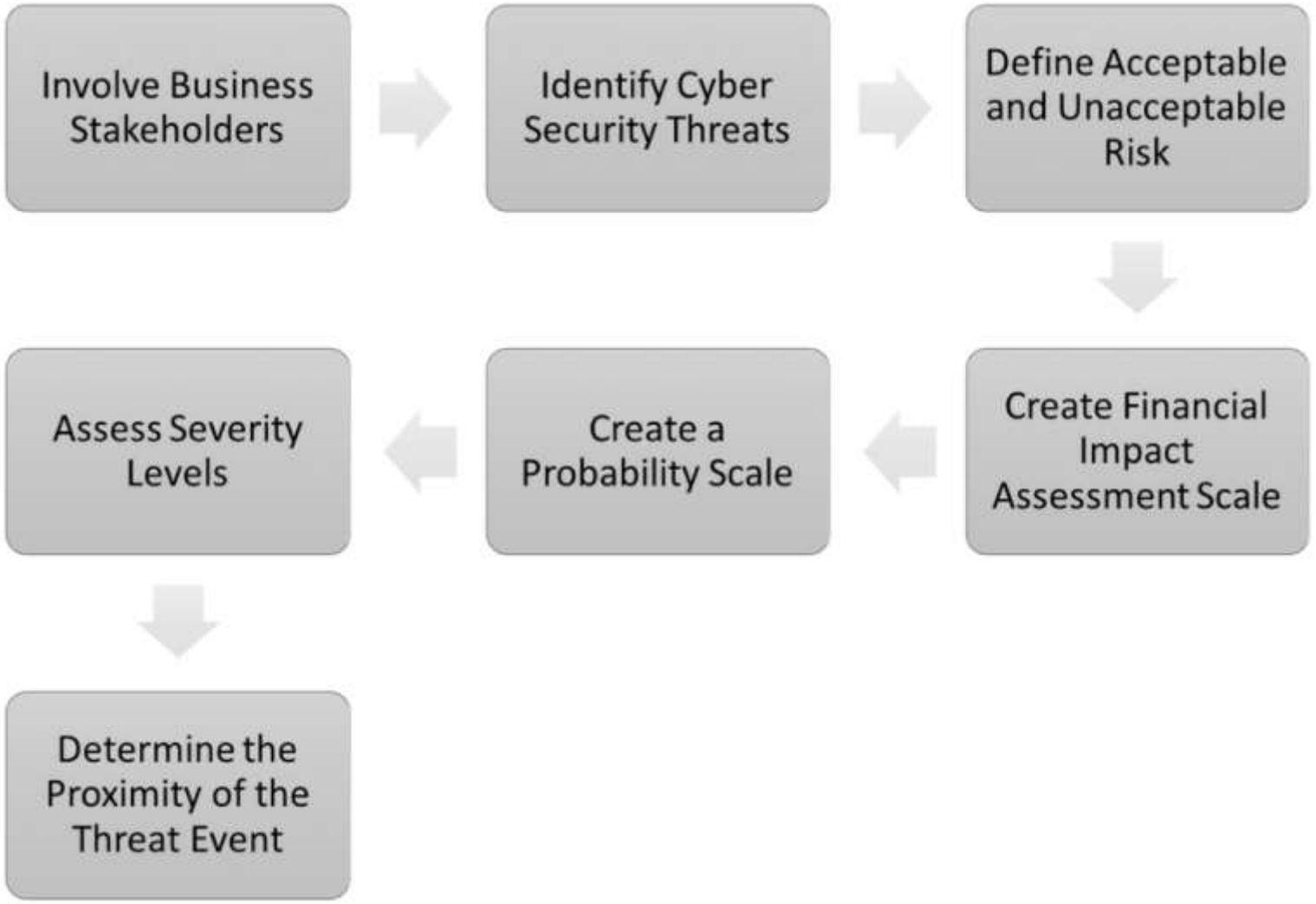
Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

Information Impact Categories

Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation

Recoverability Effort Categories

Incident Prioritization



Contd…

- ➢ Incident Notification
- ✓ CIO
- ✓ Head of information security
- ✓ Local information security officer
- ✓ Other incident response teams within the organization
- ✓ External incident response teams (if appropriate)
- ✓ System owner
- ✓ Human resources (for cases involving employees, such as harassment through email)
- ✓ Public affairs (for incidents that may generate publicity)
- ✓ Legal department (for incidents with potential legal ramifications)
- ✓ US-CERT (required for Federal agencies and systems operated on behalf of the Federal government)
- ✓ Law enforcement (if appropriate)