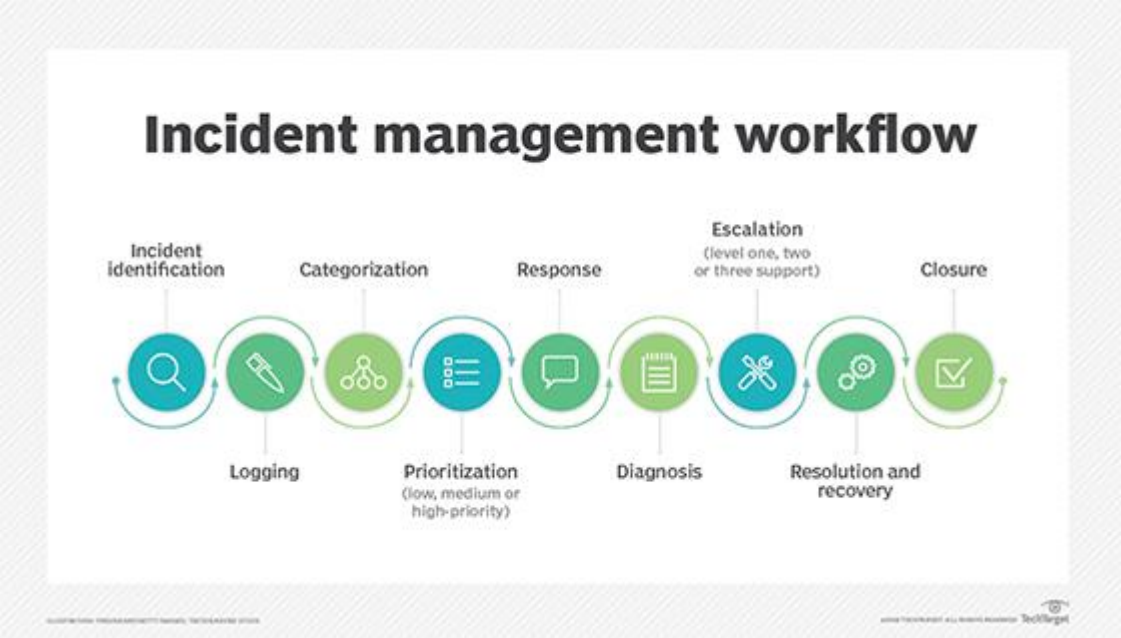

SANS Incident Response Plan

1. **Preparation**—review and codify an organizational security policy, perform a risk assessment, identify sensitive assets, define which are critical security incidents the team should focus on, and build a Computer Security Incident Response Team (CSIRT).

2. **Identification**—monitor IT systems and detect deviations from normal operations, and see if they represent actual security incidents. When an incident is discovered, collect additional evidence, establish its type and severity, and document everything.

3. **Containment**—perform short-term containment, for example by isolating the network segment that is under attack. Then focus on long-term containment, which involves temporary fixes to allow systems to be used in production, while rebuilding clean systems.

4. **Eradication**—remove malware from all affected systems, identify the root cause of the attack, and take action to prevent similar attacks in the future.

5. **Recovery**—bring affected production systems back online carefully, to prevent additional attacks. Test, verify and monitor affected systems to ensure they are back to normal activity.

6. **Lessons learned**—no later than two weeks from the end of the incident, perform a retrospective of the incident. Prepare complete documentation of the incident, investigate the incident further, understand what was done to contain it and whether anything in the incident response process could be improved.

Step 1: Preparation

The goal of the preparation stage is to ensure that the organization can comprehensively respond to an incident at a moment's notice.

In a SANS incident response plan, these are critical elements that should be prepared in advance:

- **Policy**—define principle, rules and practices to guide security processes. Ensure the policy is highly visible both to employees and users, for example by displaying a login banner that states all activities will be monitored, and clearly stating unauthorized activities and the associated penalties.

- **Response Plan/Strategy**—create a plan for incident handling, with prioritization of incidents based on organizational impact. For example, organizational impact is higher the more employees are affected within the organization, the more an event is likely to impact revenues, or the more sensitive data is involved, such as salaries, financial or private customer data.

- **Communication**—create a communication plan that states which CSIRT members should be contacted during an incident, for what reasons and when they can be contacted. For example, there may be operations staff on call at all hours, everyone in the organization should know, which incident responders to contact to help bring

systems back up. The communication plan should state the policy for contacting law enforcement, and who should make contact.

- **Documentation**—documentation is not optional and can be a life saver. If the incident is considered a criminal act, your documentation will be used to press charges against suspects. Any information you collect about the incident can also be used for lessons learned and to improve your incident response process. Documentation should answer the questions: Who, What, When, Where, Why, and How?.

- **Team**—build a CSIRT team with all relevant skills, not just security. Include individuals with expertise in security but also IT operations, legal, human resources, and public relations—all of whom can be instrumental in dealing with and mitigating an attack.

- **Access control**—make sure that CSIRT staff have the appropriate permissions to do their job. It is a good idea to have, as part of the incident response plan, network administrators add permissions to CSIRT member accounts, and then remove them when the incident is over.

- **Training**—ensure initial and ongoing training for all CSIRT members on incident response processes, technical skills and relevant cyberattack patterns and techniques. Carry out drills at regular intervals to insure that everyone in the CSIRT knows what they need to do and is able to perform their duties during a real incident.

- **Tools**—evaluate, select and deploy software and hardware that can help respond to an incident more effectively. All of the tools should be packaged in a "jump bag" that can be quickly accessed by CSIRT members when an incident occurs.

Step 2: Identification

This step involves detecting deviations from normal operations in the organization, understanding if a deviation represents a security incident, and determining how important the incident is.

The SANS incident response identification procedure includes the following elements:

- **Setting up monitoring** for all sensitive IT systems and infrastructure.
- **Analyzing events** from multiple sources including log files, error messages, and alerts from security tools.
- **Identifying an incident** by correlating data from multiple sources, and reporting it as soon as possible.
- **Notifying CSIRT members** and establishing communication with a designated command center (for example this could be senior management, IT operations)
- strong{Assigning at least two incident responders to a live incident, one as the primary handler who assesses the incident and makes the decision, and the other to help investigate and gather evidence.
- **Documenting everything** that incident responders are doing as part of the attack—answering the Who, What, Where, Why, and How questions.
- **Threat prevention and detection capabilities** across all main attack vectors.

Step 3: Containment

The goal of containment is to limit damage from the current security incident and prevent any further damage. Several steps are necessary to completely mitigate the incident, while also preventing destruction of evidence that may be needed for prosecution.

The SANS containment process involves:

- **Short-term containment**—limiting damage before the incident gets worse, usually by isolating network segments, taking down hacked production server and routing to failover.
- **System backup**—taking a forensic image of the affected system(s) with tools such as Forensic Tool Kit (FTK) or EnCase, and only then wipe and reimage the systems. This will preserve evidence from the attack that can be used in court, and also for further investigation of the incident and lessons learned.

- **Long-term containment**—applying temporarily fixes to make it possible to bring production systems back up. The primary focus is removing accounts or backdoors left by attackers on the systems, and addressing the root cause—for example, fixing a broken authentication mechanism or patching a vulnerability that led to the attack.

Step 4: Eradication

Eradication is intended to actually remove malware or other artifacts introduced by the attacks, and fully restore all affected systems.

The SANS eradication process involves:

- **Reimaging**—complete wipe and re-image of affected system hard drives to ensure any malicious content is removed.
- **Preventing the root cause**—understanding what caused the incident preventing future compromise, for example by patching a vulnerability exploited by the attacker.
- **Applying basic security best practices**—for example, upgrading old software versions and disabling unused services.
- **Scan for malware**—use anti-malware software, or Next-Generation Antivirus (NGAV) if available, to scan affected systems and ensure all malicious content is removed.

Step 5: Recovery

The goal of recovery is to bring all systems back to full operation, after verifying they are clean and the threat is removed.

The SANS recovery procedure involves:

- **Defining time and date to restore operations**—system owners should make the final decision on when to restore services, based on information from the CSIRT.
- **Test and verifying**—ensuring systems are clean and fully functional as they go live.
- **Monitoring**—ongoing monitoring for some time after the incident to observe operations and check for abnormal behaviors.

- **Do everything to prevent another incident**—considering what can be done on the restored systems to protect them from recurrence of the same incident.

Step 6: Lessons Learned

No later than two weeks from the end of the incident, the CSIRT should compile all relevant information about the incident and extract lessons that can help with future incident response activity.

The SANS lessons learned process includes:

- **Completing documentation**—it is never possible to document all aspects of an incident while it is going on, and achieving comprehensive documentation is very important to identify lessons for next time.
- **Publishing an incident report—**the report should provide play-by-play review of the entire incident, and answer the Who, What, Where, Why, and How questions.
- **Identify ways to improve CSIRT performance**—extract items from the incident report that were not handled correctly and can be improved for next time.
- **Establish a benchmark for comparison**—derive metrics from the incident report that you can use to guide you in future incidents.
- **Lessons learned meeting**—conduct a meeting with the CSIRT team and other stakeholders to discuss the incident and cement lessons learned that can be implemented immediately.