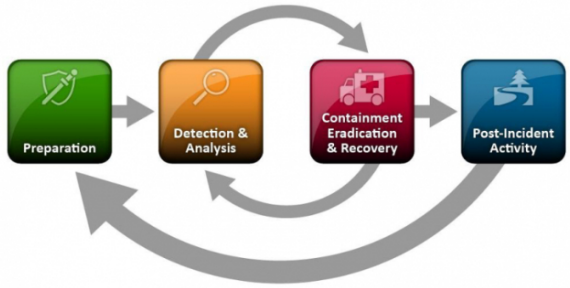
Incident Response Lifecycle (NIST SP 800 61r2)

Many organizations have procedures for handling computer-security incidents, and this is known as having an Incident Response Plan (IRP). Many of these plans are based on the NIST SP 800 61r2 guidelines. While different organizations have put forward other types of incident response lifecycles, like SANS, the one guided by NIST has shown to be the most popular. The Incident Response Lifecycle is split into four different categories and this document will be going over each one individually. One thing to keep in mind is that the cycle is an ongoing process and all four parts are used to help prevent the same incident from recurring in the future.



Source: NIST

PREPARATION

Being prepared is one of the most important aspects of incident response. If you do not have the right teams, resources, or documentation then the incident response process is being set up for failure. With the right amount of preparation, you can prevent attacks before they even happen. Being prepared consists of two major groups, being prepared for incidents and actively preventing incidents.

Some activities that involve being **prepared for incidents** are:

- Contact Information for all stakeholders
- Having a war room for central communication and coordination
- Documentation
- Baselines on running systems
- Equipment that can be used in an IR scenario, such as digital forensic toolkits

Activities that involve actively **preventing incidents** would be:

- Having current risk assessments
- Utilizing Client and Server security
- Having a user awareness and training program established

While there is no perfect preparation phase of the incident response process, it is the first line of defense of an attack that could have catastrophic damage.

DETECTION & ANALYSIS

The Detection & Analysis phase of IR involves two distinct sub-phases that if properly implemented, will be able to alert the CSIRT team at the company or organization of an active event taking place. For the detection sub-phase, many SOCs, internal security teams, and organizations have tools such as intrusion detection and prevention systems (IDPS), antivirus/antispam/antimalware software, and log monitoring solutions set up to alert the appropriate team when incidents are detected. Having members of the IR team know what systems are in place, can be beneficial in knowing how to enter in the next sub-phase, analysis. Analysis can often be one of the most complex steps in the IR lifecycle because it involves finding how the initial attack took place and how it moves throughout the network. Many organizations utilize network profiles and baselines, knowledge bases and policies for log retention, in order to make this phase easier for the incident responder.

Three other things to note, is that the responder needs to be able to effectively document their finding when analyzing the attack, as well as prioritizing actions that need to be taken place, and then the IR team needs to notify the proper authorities. This notification is often outlined ahead of time in what is typically called a Communication Plan that exists within various organizational policies. This includes managers, computer leaders, Human Resources, and the Legal department to name a few and then those parties would alert third parties or the public, depending on the type of organization that the attack occurs in. With those two sub-phases completed, the responder can continue to the next phase of the IR process.

CONTAINMENT, ERADICATION & RECOVERY

The Containment, Eradication & Recovery phase of the IR Lifecycle contains two sub-phases that are extremely important to ensure that the organization can successfully recover from the attack. The first sub-phase is containment, and this can come in many different forms. For example, the way to contain a mass-spear phishing campaign, would be a lot different than a Sodinokibi ransomware attack. There are a few key criteria that NIST established to determine what the containment strategy should be:

- Potential damage to and theft of resources
- Need for evidence preservation
- Service availability
- Time and resources needed
- Effectiveness
- Duration of the solution

During the containment sub-phase, it is also important, like the Detection & Analysis phase, to keep a detailed log of all evidence that you find regarding the attack. This could be information that could be used for further prevention tactics, as well as knowledge that could be shared with the cybersecurity community. The second sub-phase is eradication & recovery and this phase is the act of returning your systems back to normal. Actions for eradication could consist of rebuilding machines from known good backups, deleting malware, or resetting credentials on compromised accounts. Actions for recovery consist of restoring those systems to their pre-attack state. This could also include eliminating any vulnerabilities that were exploited in the attack, as well as changing passwords, installing patches, tightening network security, etc.

LESSONS LEARNED

The most important part of the Post-Incident Activity phase is learning and improving the existing systems. Incident response teams are supposed to be an ongoing and ever-growing effort to prevent threats before they happen and respond to new threats as they emerge. NIST recommends holding a "lessons learned" meeting that could address the following questions:

- Exactly what happened and when did it happen?
- How well did staff and management perform in dealing with the incident?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can be taken?
- What indicators should be watched for in the future?
- What additional tools or resources are needed to mitigate future incidents?

After this meeting is conducted, it is important to implement answers to those questions, back to the Preparation phase in order to learn from the attack and use it to their advantage in defending the company or organization.

Previous Topic
Mark Complete
Next Topic
Back to Lesson