Incident Response Plan

Security Operations and Policy

2022-08-16

Coleton Sanheim & D’Artagnan Boocock

Table of Contents

[**Incident response plan**](#_gy2gmvx01ffa) **2**

[**Actions Required**](#_nhs4bljuf4o0) **2**

[Triage Phase:](#_pf1lyn6972z8) 2

[Investigative Phase:](#_kzau9ots34c3) 3

[Containment Phase:](#_we03bbbj4cp9) 3

[Analysis and Tracking Phase:](#_d6fxcjr94e9e) 3

[Recovery Phase:](#_bt3ma39j9v9y) 3

[**Tools**](#_6gvtfg7iqqji) **4**

# Incident response plan

Incident response is a reactive approach which begins when a security problem is detected. Quick and decisive action is necessary to determine the cause of the issue and resolve it before more damage is done.

Thorough documentation can be a vital learning tool to ensure known vulnerabilities are accounted for and mitigated. Thus, any lessons learned can be applied to the current security controls, preventing future incidents.

Incident response typically includes the following steps:

1. Planning and creating a response protocol
2. Responding to the incident
3. Document findings and recover data

It is important to ensure malware is contained and all unaffected parts of the network remain unaffected. The quickest way to isolate an incident is to physically disconnect the affected device(s) from the network. Alternatively, the security officer may choose to shut down the corrupted system. Unfortunately, this will clear the RAM and make it more difficult to analyze the root cause of the incident.

When creating a good containment strategy, the following must be considered:

* Forensic evidence should be preserved
* Service availability
* Potential damage elsewhere on the network
* Containment time
* Containment resources

# Actions Required

## Triage Phase:

The triage phase is the first step that an incident response team will perform once an incident has been detected. At this phase the team will determine if the event that triggered the response is real or a false positive. This stage needs to be completed with utmost urgency, as every second you are spending on checking whether this is a legitimate breach is less time to investigate and contain the attack.

The team should check for evidence for the existence of the problem that triggered the event. The team should have up to date information on the security world, checking IP addresses against known attackers. Finally, the team should analyze the network to check for irregular traffic that would indicate propagation of malicious code.

## Investigative Phase:

This phase is where the main investigation takes place, the team need to gather as much information as they can on the event, such as:

* When did the event occur
* How did it get discovered / Who discovered it
* How many areas were impacted
* What is the effect of the event
* How did the event occur

After the team gathers this (and more) information and has compiled it into a report, they will analyze the findings and determine the best way to proceed. They can now move on to the next phase.

## Containment Phase:

Now that the event has been analyzed, the next step is to contain it for future analysis. The team should scan the entire network and determine which machines, if any, have been infected. Once this is done all connections from the infected machine(s) to the rest of the network needs to be severed to prevent propagation. Once the infected machines are properly isolated, analysis of how the incident happened can begin to take place.

## Analysis and Tracking Phase:

This phase is split into two parts, first analysis needs to be performed to determine the scope of what was affected and what damage was done. The second is tracking, where the incident response team needs to track the attack back to where the breach started, and update and harden systems accordingly.

## Recovery Phase:

Finally, in this phase the team will make sure all solutions have been put in place to ensure this incident does not repeat itself. Then the process of restoring affected systems back to full activity can begin. The incident response team should compile their entire process of all 5 phases into a final report to file and submit to the higher ups in the company for review and to keep records.

# 

# Tools

CM Tools

SIEM

Log files within the affected computer will be a trove of data the analysts will need to comb through during the investigation.

Documentation of previous incidents within the company will help analysts recognize any similarities with past incidents

Documentation of known malware (CVEs) will be useful to identify the problem and address it properly