Incident Response Checklists

Preparation Checklist

Your incident response checklist for the preparation phase sets the stage for other phases during the IR journey. It’s important that your team pays close attention to this area as it focuses on how the IR team will identify and respond to incidents.

* Have you developed security policies for the organization?
  + If so, are employees aware of the policy and can the security team enforce it?
* What is the organizational definition of a security incident?
* Do you have a process in place to prioritize and document security incidents?
* Who is responsible for each phase of the incident response process (identification, containment, eradication, recovery, and lessons learned)?
* Does the IR team have all the tools and a “jump bag” required to handle incidents?
  + An Incident Responder journal
  + A contact list of everyone on the IR team
  + USB drives
  + A bootable USB drive or CD with all software needed to repair file systems and eradicate threat(s)
  + A laptop or other device to complete forensics
  + Endpoint protection and anti-malware software utilities
  + Network and endpoint toolkits to add/remove components.
* Who communicates important updates from incident response?
* Who will work with law enforcement officials, if necessary?
* Who will bring systems back online in the event of an impactful data breach?

Identification Checklist

During the identification phase of incident response, your security team needs to thoroughly investigate and record all details related to the security incident. The incident responder should record all details within the IR journal. Here are some checklist questions that can be used during the identification phase.

* **Who** discovered or reported the incident?
* **When** was the incident discovered or reported?
* **Where**was the incident discovered or located?
* **What**impact does the incident have on business operations?
* **What**is the extent of the incident with the network and applications?

Containment Checklist

In the containment phase of incident response, the IR team should stop any threat(s) from creating any additional damage as well as save any data related to the incident. This data may be used in reporting or notifying legal authorities. Here are a few common questions to ask during this phase.

* Can the incident be isolated?
  + If the incident can be isolated, what steps will be taken to isolate?
  + If not, explain why the system(s) can’t be isolated and work with the owners to resolve the problem.
* Are the affected systems isolated from non-affected systems?
* Have backups been created to protect critical data?
* Have copies of infected machines been made for forensic analysis?
* Have all malware and other threats been removed from the infected systems?

Eradication Checklist

The eradication phase includes a more permanent fix for infected systems. Here are some checklist items to run through during this phase in the incident response process.

* Have infected systems been hardened with new patches?
* Do any systems or applications need to be reconfigured?
* Have all possible entry points been reviewed and closed?
* Have all processes to eradicate the threat(s) been covered?
* Are any additional defenses needed to support the eradication of the threat(s)?
* Has all malicious activity been eradicated from affected systems?

Recovery Checklist

The recovery phase allows the responder to bring back systems into production after the eradication phase is completed. Here are some common questions to include in your incident response checklist.

* **Where** will responders pull recovery and backups from?
* **How** will infected systems be deployed back into production?
* **When** will infected systems be deployed back into production?
* **What** operations will be restored during the recovery phase?
* **What** testing and verification should be done on infected systems?
* **Have** responders included documentation on how the recovery was completed?

Lessons Learned Checklist

Documentation is key during the lessons learned phase of incident response. A detailed report should cover all aspects of the IR process, the threat(s) that were remediated, and any future actions that need to take place to prevent future infection. Consider these questions when entering the lessons learned phase.

* Has all necessary documentation been recorded throughout the IR phases?
* Has the responder prepared an incident response report for the lessons learned meeting?
* Does the report cover every aspect of the incident remediation process?
* When can the IR team hold the lessons learned meeting?
* Who will deliver the lessons learned meeting?
* Are there areas for improvement in the incident response process?

These incident response checklists can help keep the IR team stay on track throughout each phase of responding and remediating security incidents. What other important questions does your team ask during the IR process?

https://cipher.com/blog/5-helpful-incident-response-checklists