Checklist for a Streamlined Incident Response Plan

With cybercrime growing in sophistication and frequency, it would be no surprise if an attack managed to sneak past your organization's defenses. That's why having a well-organized incident response plan is vital to limiting the damage in the wake of an attack and bringing normalcy back to operations.

To determine the robustness of your incident response plan, we've created a checklist to help your cybersecurity team ascertain its efficiency and effectiveness.

PREPARATION

The preparation phase sets the stage for other phases in the incident response cycle. Pay attention to the following questions to establish whether your incident response team has the necessary tools and processes to detect and prevent an incident.

- [ ] *Do you have security policies in place? If so, is every employee aware of them?*
- [ ] *Do you have a clear definition of a security breach?*
- [ ] *Have you performed a risk assessment to find vulnerabilities in your systems?*
- [ ] *Have you implemented the necessary technology solutions to detect and prevent cyberattacks?*
- [ ] *Have you assigned responsibilities for the effective execution of each phase of the incident response process?*
- [ ] *Do you have the personnel to inform law enforcement agencies, if necessary?*
- [ ] *Do you have a communication channel to share essential updates during and after an incident?*

IDENTIFICATION

In this phase, your incident response team needs to thoroughly investigate and record all details related to the security incident in an incident response journal. Here are some questions for the identification phase.

- [ ] *How was the incident discovered and reported?*
- [ ] *How long did it take to detect the incident?*
- [ ] *What vulnerabilities did the cybercriminals exploit?*
- [ ] *What is the impact of the incident on routine operations, systems and networks?*

CONTAINMENT

In the containment phase, the incident response team mitigates the threat and prevents hackers from inflicting further damage. Here are some pertinent questions for this phase.

- [ ] *Can the incident be isolated? If yes, what steps can be taken? If not, then why can't it be isolated?*
- [ ] *Are the compromised systems isolated from the uncompromised systems?*
- [ ] *Is there a backup in place to protect critical data?*
- [ ] *Have experts performed a forensic analysis of the affected systems?*
- [ ] *Have all malware and other threats been removed from the compromised devices?*

ERADICATION

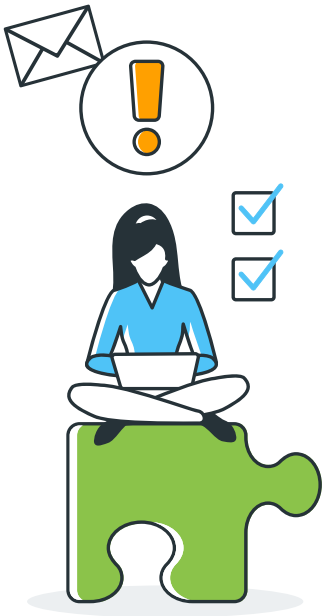
This phase consists of a more stable fix for compromised systems. Here are some questions to run through during the eradication phase.

- [ ] *Have you patched the affected systems with new updates?*
- [ ] *Do any systems or applications need reconfiguration?*
- [ ] *Have all the vulnerabilities been eliminated?*
- [ ] *Has the malicious payload been removed from the affected devices?*

RECOVERY

After the completion of the eradication phase, the recovery phase allows organizations to restore normal operations. Here are some questions to consider during this phase.

- [ ] *Where will the responders pull recovery and backups from?*
- [ ] *How and when will the compromised systems be deployed back to work?*
- [ ] *What operations need to be restored?*
- [ ] *Have the affected systems been tested and verified?*
- [ ] *Is there proper documentation of the entire incident response process?*



IMPLEMENT MANAGED SOC FOR RAPID INCIDENT RESPONSE

A security operations center (SOC) can help organizations respond effectively after an incident. Once the incident is confirmed, the SOC acts as the first responder, performing actions like shutting down or isolating compromised systems, terminating harmful processes, deleting files and more. However, having an in-house SOC is not feasible for organizations with limited resources.

With Kaseya's Managed SOC in your corner, you can launch effective incident response without implementing expensive hardware or hiring additional workforce. Our experts monitor your critical attack vectors 24/7, and if an attack happens, they respond to the extent necessary and minimize the damage while ensuring minimum impact on business continuity.

LEARN MORE