

Forum: [Hack Forums](#)

Thread: [incident response playbook design question](#)

kykychand - October 16, 2025, 5:20 am

How do you design an incident response playbook that minimizes lateral spread from an initial virus infection?

Bastille - October 16, 2025, 8:27 am

An incident response is usually composed of 7 steps :

- 1 - Preparation
- 2 - Detection
- 3 - Analysis
- 4 - Containment
- 5 - Eradication
- 6 - Recovery
- 7 - Post event (lessons learned, surveillance, etc)

Depending on the threat, the playbook you'll use will be different, but it always uses the steps above.

STEP 1 : PREPARATION

Before going straight into the incident response, you **MUST** be pro-active and reduce the surface attack or go through hardening. For example, running an audit on your Active Directory servers, going with remediation to fix flaws / vulnerabilities, so in case the server is compromised, the attacker will have more difficulties with lateral movements and you'll slower him.

Few examples : running PingCastle on a Domain Controller, whitelisting only the necessary traffic with the dedicated ports, vlans, follow the principle of least privileges, use dedicated accounts on the AD to run services such as backups, installing an EDR/XDR on every machine, etc.

You also need to prepare your team to counter an attack, let them know about the Incident Response procedure (the 7 steps), you need to train them like to be able to conduct an analysis and so on.

STEP 2 : DETECTION

This part depends on your budget, if you have a SOC or not for example, if you've configured alerts on your email services, and so on.

STEP 3 : ANALYSIS

Relies the team's knowledge and skills to be able to find if the threat is real or not.

STEP 4 : CONTAINMENT

That's also where you can avoid lateral movements from the attacker. Think about :

- Changing passwords
- Shutting down NIC (useful if you have physical access)
- Shutting down IPSec VPNs between other sites / offices / customers / supply chain / ...

STEP 5 : ERADICATION

Explicit, be sure to spend enough time on the analysis to understand how the attacker proceeded

so you'll fix the vulnerabilities / flaws he used.

STEP 6 : RECOVERY

Explicit

STEP 7 : POST EVENT

Take a look at what worked well, what didn't work very well, try to improve your process, and don't forget to monitor the activity in case it could happen again.

obama carlos - October 16, 2025, 10:03 am

no lo se.

mohamedtaher - November 6, 2025, 2:28 pm

splunk

victorvictor - November 9, 2025, 3:49 am

(Oct 16, 2025 08:27 AM) Bastille Wrote: [CITE](#) An incident response is usually composed of 7 steps :

- 1 - Preparation
- 2 - Detection
- 3 - Analysis
- 4 - Containment
- 5 - Eradication
- 6 - Recovery
- 7 - Post event (lessons learned, surveillance, etc)

Depending on the threat, the playbook you'll use will be different, but it always uses the steps above.

STEP 1 : PREPARATION

Before going straight into the incident response, you MUST be pro-active and reduce the surface attack or go through hardening. For example, running an audit on your Active Directory servers, going with remediation to fix flaws / vulnerabilities, so in case the server is compromised, the attacker will have more difficulties with lateral movements and you'll slow him.

Few examples : running PingCastle on a Domain Controller, whitelisting only the necessary traffic with the dedicated ports, vlans, follow the principle of least privileges, use dedicated accounts on the AD to run services such as backups, installing an EDR/XDR on every machine, etc.

You also need to prepare your team to counter an attack, let them know about the Incident Response procedure (the 7 steps), you need to train them like to be able to conduct an analysis and so on.

STEP 2 : DETECTION

This part depends on your budget, if you have a SOC or not for example, if you've configured alerts on your email services, and so on.

STEP 3 : ANALYSIS

Relies the team's knowledge and skills to be able to find if the threat is real or not.

STEP 4 : CONTAINMENT

That's also where you can avoid lateral movements from the attacker. Think about :

- Changing passwords

- Shutting down NIC (useful if you have physical access)
- Shutting down IPSec VPNs between other sites / offices / customers / supply chain / ...

STEP 5 : ERADICTION

Explicit, be sure to spend enough time on the analysis to understand how the attacker proceeded so you'll fix the vulnerabilities / flaws he used.

STEP 6 : RECOVERY

Explicit

STEP 7 : POST EVENT

Take a look at what worked well, what didn't work very well, try to improve your process, and don't forget to monitor the activity in case it could happen again.

awesome, thx

Bastille - November 10, 2025, 10:51 am

(Nov 9, 2025 04:49 AM)victorvictor Wrote: [\[CITE\]](#) awesome, thx

You're welcome, if you have other questions feel free !