
# A quick look at Incident response

By Ryan Nolette
The man of many titles

- Security Operations Lead
- Senior Security Engineer
- Senior Threat Researcher
- Incident Response Consultant



CARBON BLACK
ARM YOUR ENDPOINTS

Agenda

1. What is Incident response?
2. What are the steps to respond to an incident?
3. What do I do after an incident?

CARBON BLACK

## What is Incident Response?

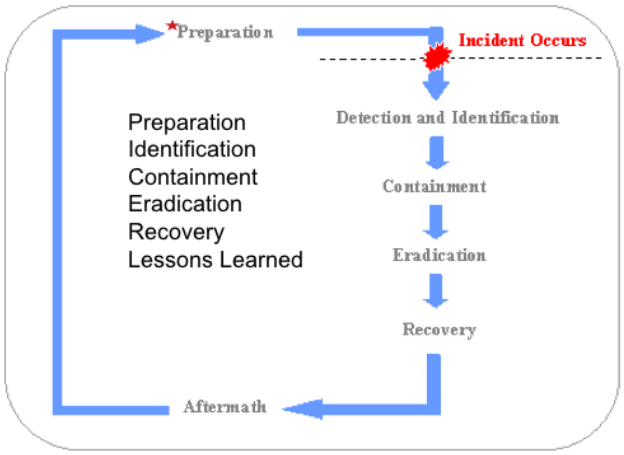
Incident Response (IR) is an **systematic** approach to addressing and managing the **consequences** of a security breach or attack.

The objective is to handle the situation in a manner that limits **damage** and reduces **recovery** time and costs.

CARBON BLACK

## What are the steps to respond to an incident?

According to the SANS Institute, there are six steps to handling an incident most effectively






CARBON BLACK

Preparation

The organization **educates** users and IT staff of the importance of updated security measures and **trains** them to respond to computer and network security events quickly and correctly.

5

CARBON BLACK

Identification

The response team is initiated to **confirm** whether a particular event is, in fact, a security **incident**.



CARBON BLACK

## Containment

The team determines how far the problem has spread (**Scope**) and provides a plan to stop the propagation (**containment**).



CARBON BLACK

Eradication

The team investigates to discover the origin of the incident (**catalyst event**). The **root cause** of the problem and all traces of malicious code are **removed**.



CARBON BLACK

Recovery

Data and software are restored from **clean** backup files. Steps are taken to ensure vulnerabilities are lessened (**hardening**). Systems are monitored for any sign of **weakness** or **recurrence**.



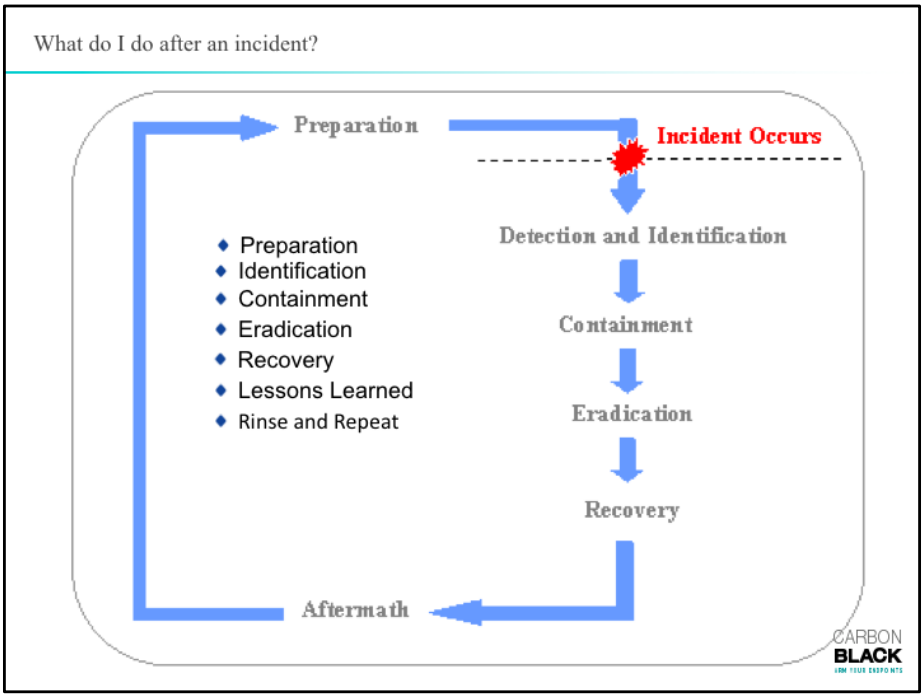
CARBON BLACK

Lessons learned

The team **analyzes** the incident and how it was handled, making **recommendations** for better future response and for **preventing** a **recurrence**.



CARBON BLACK


What do I do after an incident?
Preparation
Incident Occurs
Detection and Identification
Containment
Eradication
Recovery
Aftermath
Preparation
Identification
Containment
Eradication
Recovery
Lessons Learned
Rinse and Repeat
CARBON BLACK

references

- http://www.sans.org/reading-room/whitepapers/incident/incident-handling-process-small-medium-businesses-1791?show=incident-handling-process-small-medium-businesses-1791&cat=incident
- http://www.infosec.gov.hk/english/images/sihc_en.gif

12

CARBON BLACK