

# 6

## Six Steps of Incident Response Plan

Incident Response Plan represents a pre-planned action strategy to respond to the security threats in an event of a cyber-attack. Following are the important steps of an Incident Response Plan of an organization:

01

**PREPARATION:** Creating a policy that includes a set of written principles, processes, and a communication strategy.

02

**IDENTIFICATION:** Analysing log files, scan findings, system alerts, and other data to determine whether or not a malicious act has occurred.

03

**CONTAINMENT:** Containing the damage and preventing it to escalate.

04

**ERADICATION:** Contaminated systems are removed from the network and replaced with new, unaffected systems.

05

**RECOVERY:** Damaged work should be recovered, and systems that were impacted should be cleaned.

06

**LESSONS LEARNED:** Analyzing the root cause of the breach.

[www.centextech.com](http://www.centextech.com)

Centex Technologies



13355 Noel Road,  
Suite # 1100, Dallas, TX 75240

Phone: (972) 375 - 9654

501 N. 4th Street,  
Killeen, TX 76541

Phone: (254) 213 - 4740

1201 Peachtree St NE,  
Suite 200, Atlanta, GA 30361

Phone: (404) 994 - 5074

Capital Factory, 701, Brazos  
Street, Austin, TX 78701

Phone: (512) 956 - 5454