

Cyber Security Incident Response



A robust Cyber Security Incident Response (CSIR) is imperative for IT organizations to build a secure, vigilant, and resilient landscape.

Here are five Do's and Don'ts for Effective Incident Response





Do not panic. It makes things



Use forensic tools to collect volatile data and other critical artifacts from the system.

Collect external intelligence

of Compromise (IOC). Secure systems and other media for forensic collection.

based on identified Indicators

Collect the appropriate logs at both the network and endpoint level.

potential customers and stakeholders.

Communicate promptly with

worse.

Don'ts

Do not discuss the incident

compromised systems.

Do not shut down

directed.

Do not use domain admin credentials to access the systems environment.

with others unless otherwise

Do not execute any non-forensic software on compromised systems.

Why Organizations Need Incident Response? A robust cyber incident response plan helps you stay ahead of

the cybersecurity adversaries. The key benefits of the IR plan include:

and confidence

Respond to the threat with ease





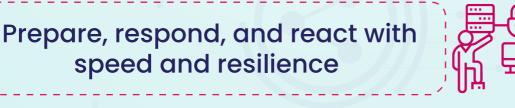
Mitigate the impact of the incident

cybersecurity posture





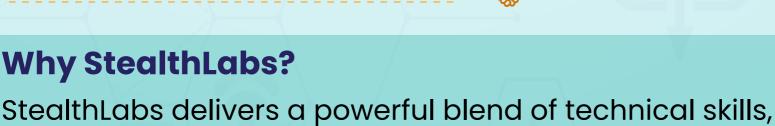






Why StealthLabs?

Maintain business continuity



business experience, and industry insights when helping clients

build effective CIR capabilities. Comprehensive **Deep CIR Experience Security Solutions**

CIR



Capabilities

Want to Know How to Begin Developing CSIRP?

Round-the-clock

Security Services



Contact Us Directly

