Do's and Don'ts

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's	Don'ts
Use forensic tools to collect volatile data and other critical artifacts from the system.	Do not panic. It makes things worse.
Collect external intelligence based on identified Indicators of Compromise (IOC).	Do not shut down compromised systems.
Secure systems and other media for forensic collection.	Do not discuss the incident with others unless otherwise directed.
Collect the appropriate logs at both the network and endpoint level.	Do not use domain admin credentials to access the systems environment.
Communicate promptly with potential customers and stakeholders.	Do not execute any non-forensic software on compromised systems.

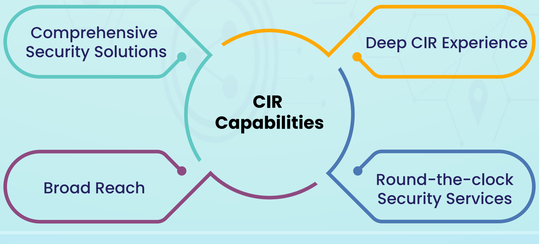
Why Organizations Need Incident Response?

A robust cyber incident response plan helps you stay ahead of the cybersecurity adversaries. The key benefits of the IR plan include:

1. Respond to the threat with ease and confidence
2. Mitigate the impact of the incident
3. Improve overall cybersecurity posture
4. Strengthen customer trust
5. Solidify brand reputation
6. Ensure compliance
7. Prepare, respond, and react with speed and resilience
8. Contain the threat from spreading
9. Maintain business continuity

Why StealthLabs?

StealthLabs delivers a powerful blend of technical skills, business experience, and industry insights when helping clients build effective CIR capabilities.



Want to Know How to Begin Developing CSIRP?

Contact Us Directly

+1 817-415-1200
https://t.me/learnlabsts
info@stealthlabs.com