Data Sheet

DTS SOLUTION
CYBER SECURITY REDEFINED

Cyber Security Response

DTS Solution can support your organization build complete cyber response capabilities by developing enterprise wide incident response and management framework. The incident response framework includes everything from incident triage to chain of custody to deep forensic analysis.

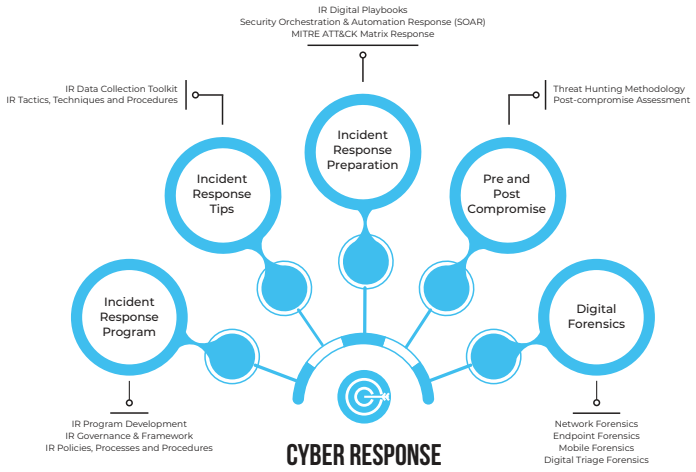
Incident response is an organized approach to addressing and managing the aftermath of a security breach or cyberattack, also known as an IT incident, computer incident, or security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

Ideally, incident response activities are conducted by the organization's computer security incident response team (CSIRT), a group that has been previously selected to include information security and general IT staff as well as C-suite level members. The team may also include representatives from the legal, human resources and public relations departments. The CSIRT response should comply with the organization's IR Plan, a set of written instructions that outline the organization's response to a cyberattack.

Any incident that is not properly contained and handled can, and usually will, escalate into a bigger problem that can ultimately lead to a damaging data breach or system collapse. Responding to an incident quickly will help an organization minimize losses, mitigate exploited vulnerabilities, restore services and processes, and reduce the risks that future incidents pose.

Incident response enables an organization to be prepared for the unknown as well as the known and is a reliable method for identifying a security incident immediately when it occurs.

DTS Solution – Cyber Response



Incident Response Plan

An IRP should include procedures for detecting, responding to and limiting the effects of a data security breach. Incident response plans usually include instructions on how to respond to potential attack scenarios, including data breaches, denial of service/distributed denial of service attacks, network intrusions, virus, worms or malware outbreaks or insider threats.

Without an incident response plan in place, an organization may not detect the attack, or it may not follow proper protocol to contain the threat and recover from it when a breach is detected. According to the SANS Institute, there are six key phases of an incident response plan which we at DTS follow when designing and developing the IR framework:

Preparation: Preparing users and IT / security staff to handle potential incidents should they should arise
Identification: Determining whether an event is, indeed, a security incident
Containment: Limiting the damage of the incident and isolating affected systems to prevent further damage
Eradication: Finding the root cause of the incident, removing affected systems from the production environment
Recovery: Permitting affected systems back into the production environment, ensuring no threat remains
Lessons learned: Completing incident documentation, performing analysis to learn from the incident and potentially improve future response efforts

An **incident response plan** can benefit an enterprise by outlining how to minimize the duration of and damage from a security incident, identifying participating stakeholders, streamlining forensic analysis, hastening recovery time, reducing negative publicity and ultimately increasing the confidence of corporate executives, owners and shareholders.

The plan should identify and describe the roles and responsibilities of the incident response team members who are responsible for testing the plan and putting it into action. The plan should also specify the tools, technologies and physical resources that must be in place to recover breached information.

DTS SOLUTION
CYBER SECURITY REDEFINED

DUBAI: Office 4, Oasis Center, Sheikh Zayed Road, Dubai, United Arab Emirates
T: +971 4 338 3365 | **E:** info@dts-solution.com

800 HACKED

ABU DHABI: Office 253, Al Bateen C6 Tower - Bainunah, King Abdullah Bin Abdulaziz Al Saud Street | **T:** 971 2 2076777
LONDON: 160 Kemp House, City Road, London, EC1V 2NX, United Kingdom | **T:** +44 2081230 387 (DTS)
www.dts-solution.com