Data Sheet

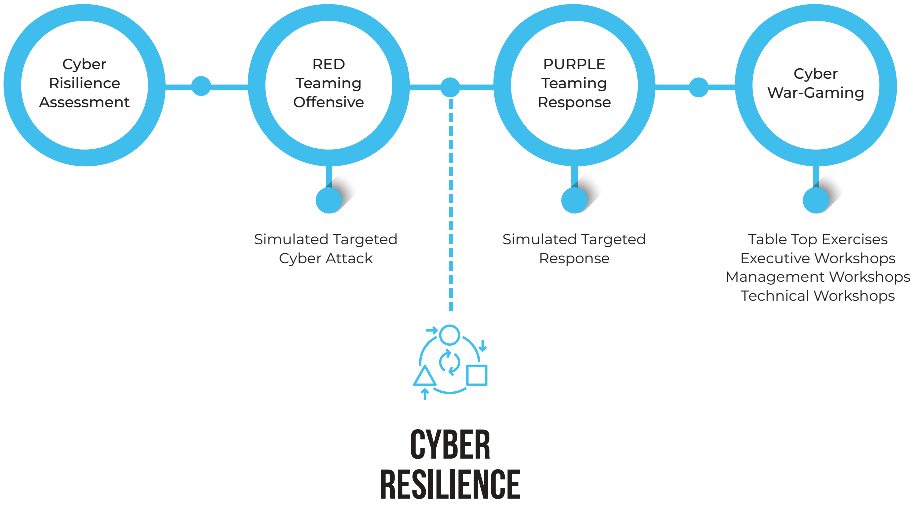
Cyber Security Resilience

Cyber Resilience refers to an entity's ability to continuously deliver the intended outcome and sustain business operations despite adverse cyber events. **Cyber Resilience** is an evolving perspective that is rapidly gaining recognition. The concept essentially brings the areas of information security, business continuity and (organizational) resilience together.

Entities with potential need of cyber resilience abilities include, but is not limited to; IT systems, critical infrastructure, business processes, organizations, societies and nation-states. Adverse cyber events are those that negatively impact the availability, integrity or confidentiality of networked IT systems and associated information and services. These events may be intentional (e.g. cyber-attack) or unintentional (e.g. failed software update) and caused by humans or nature or a combination thereof.

The objective of cyber resilience is to maintain the entity´s ability to deliver the intended outcome continuously at all times. This means even when regular delivery mechanisms have failed, such as during a crisis and after a security breach. The concept also includes the ability to restore regular delivery mechanisms after such events as well as the ability to continuously change or modify these delivery mechanisms if needed in the face of new risks. **Backup and disaster recovery operations** are part of the process of restoring delivery mechanisms.

DTS Solution advisory team can help your organization build cyber resiliency by conducting different types of assessment based on the level of maturity of the organization. We initially start with a cyber resilience assessment which identifies the gaps across your environment, this could be missing policies, processes and instructions such as crisis management, external media communication, breach notification policy etc. We may also find gaps on key critical business processes across people, process or technology that do not meet cyber resilience requirements. These findings would then be presented in a report and management presentation would be conducted.


Cyber Risilience Assessment

RED Teaming Offensive

PURPLE Teaming Response

Cyber War-Gaming

Simulated Targeted Cyber Attack

Simulated Targeted Response

Table Top Exercises
Executive Workshops
Management Workshops
Technical Workshops

CYBER RESILIENCE

DTS Solution Approach to Cyber Resilience

DTS Solution can also perform **Simulated Targeted Cyber Attacks (STCA)** using our **Red Teaming approach** to test the capability of the organization to detect and deflect any attacks we throw at the organization. This approach really identifies the level of maturity across various aspects. We can also perform Purple Teaming exercises where in coordination with the Red Team the effectiveness of the **CSOC - security analytics, monitoring and incident detection and containment** is measured.

To further strengthen Cyber Resilience understanding. we can also engage various key stakeholders by performing war-gaming exercises and simulations to give the participating members hypothetical scenarios of a cyber-attack and the actions they would take. This is all played out by preparing a role-based scenarios and then presenting these simulated scenarios to the stakeholders involved for them to solve as they go through the different challenges. This not only raises awareness but makes the stakeholders realize the level of preparedness they have in place.