C Tech Bilişim Teknolojileri San. ve Tic. A.Ş.

CYBER RANGE

"FOR DEVELOPING, TESTING, ANALYZING AND STUDYING CYBER TOOLS AND TECHNIQUES"

"AN ANALYTICAL PLATFORM DESIGNED FOR MODELING AND SIMULATION OF COMPLEX TASKS AND ADVANCED THREATS"

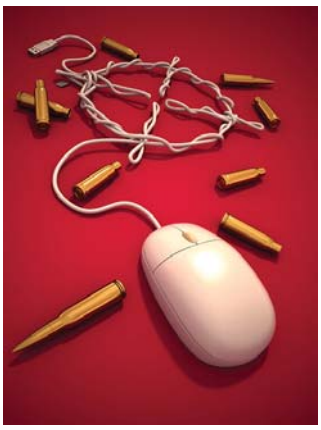
C Tech Bilişim Teknolojileri San. ve Tic. A.Ş.

OVERVIEW

Even if millions of dollars are spent on IT infrastructures, they are still weak and fragile to cyber threats, yet new threats are emerging everyday. In order to simulate the effects of these threats on IT infrastructures, experimental platforms composed of reusable virtual systems and always up-to-date threat libraries are required. Today, existing platforms are insufficient. In addition, lack of qualified human resources and required experience on cyber defense are still the biggest issues. However, by using proven methods, advanced cyber scenarios and comprehensive training programs, elite cyber defense (or warrior) teams can be built to gain in required experience.

An Internet scale experimentation platform with realistic cyber conditions supported by various attack vectors is a key component for training these cyber warriors. CTech Cyber Range is a high fidelity analytical platform designed for modeling and simulation of complex tasks and advanced threats to experiment, develop, test, analyze and study cyber tools and techniques.

USE CASES



- Develop proof of concept cyber tools, counter measures and techniques.
- Model large-scale cyber and non-cyber physical scenarios.
- Study and analyze efficiency of proposed or in use network security architectures and related components.
- Mitigate risks of migrating to a new network architecture or using a brand new network component.
- Improve security policies and procedures using various testing methodologies.
- Execute training and cyber exercises involving adversary elements and war games.

FEATURES

- A multi user platform
- Network components with desired fidelity;
  - Physical
  - Virtual
  - Emulated
  - Simulated
- Customizable and flexible infrastructure
- Easy to use graphical interface
- Built-in, highly reusable cyber scenarios
- Rich attack/threat content
- Scalable and modular architecture