



# Cyberbit Range

Powering the world's leading cybersecurity training and simulation centers

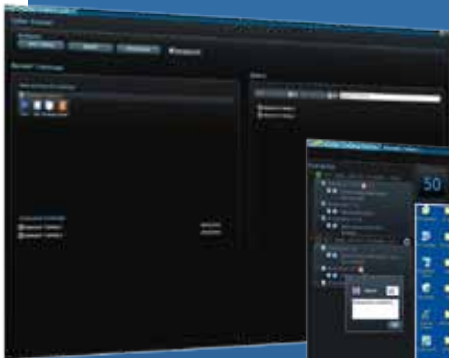
## Cyberbit Range

Powering the world's leading cybersecurity training and simulation centers

A skilled cyber-security workforce is a key element of enterprises and governments efforts to combat the serious threat to organizations operation posed by cyber attacks, including cyber-espionage, cyber-crime and cyber-warfare. To meet this need, CYBERBIT, a leader in the defense industry, has introduced its comprehensive Cyberbit Range. The field proven solution offers a virtual cyber defense environment designed to train cyber-security professionals and decision makers in securing national military and civilian networks against all forms of cyber attacks. The system is an integral component of CYBERBIT's comprehensive cyber defense solutions.



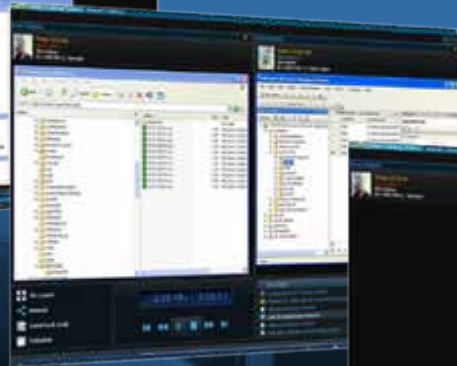
Training Set Up



Scenario Running



Training Review Panel



Trainee Evaluation



## Simulated security attacks, maximizing the awareness and improving the skills of the cyber workforce

Conducted in a generic, isolated and secured environment, the Cyberbit Range offers a scalable and realistic training experience where trainees are exposed to various attack scenarios and security breaches to improve their hands-on skills. The solution enables to run automated scenarios which can be run repeatedly through each training session to promise consistency and continuous improvement. The Cyberbit Range can simulate large-scale virtual networks (IT, SCADA, tactical communications, etc.) and attacks based on previous real-world incidents, including SCADA attack scenarios. It can also pinpoint system vulnerabilities and help security professionals develop countermeasures and improved protocols for dealing with cyber attacks on critical network systems – such as communications networks and utility grids

## Fully customizable simulations of real-world applications

The Cyberbit Range is supported by proprietary architecture and applications, advanced software and large-scale COTS

hardware. Its semi-automatic (manned and unmanned) environment utilizes live network and traffic simulation to train users in real-time. Easily adapted to the customer's actual work environment, the Cyberbit Range offers a range of security tools and systems. These include risk assessment tools, monitoring systems, security information and event management (SIEM) systems, forensic tools and supporting databases, as well as other network, security and cyber components.

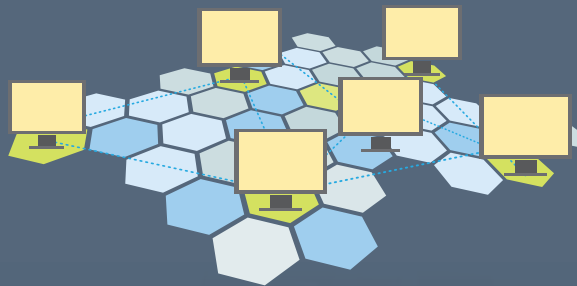
## Performance evaluation and debriefing

The Cyberbit Range also features an advanced training management system, where the training manager defines, builds, deploys and runs the training methodology and scenario for each training session. The trainees' activities are tracked and recorded – along with all logs from the network components and security information events – to be fully analyzed during a debriefing and after action review (AAR). The Cyberbit Range is available with a choice of implementation options. The system can be implemented as a comprehensive turnkey solution – backed with unique cyber training methodology – or delivered on a fee-for-service basis by CYBERBIT.

## Network Simulation Attack Simulation | Traffic Simulation



Blue Team



Red Team Simulation  
(Attack Machine)



White Team



## Key Features

- High-fidelity virtual defense training and simulation environment
- Simulation of multiple automatic and repeatable cyber attack scenarios
- Simulation of diverse networks from small-medium businesses up to large-scale enterprise /government networks
- Virtualization and emulation of any network device and protocol
  - Network appliances
  - SCADA controllers
  - Servers and applications
- Advanced network traffic generator engine
  - Supports a wide range of protocols and applications
  - Simulates attacks, legitimate traffic and normal user behavior
- Built in attack scenarios for both IT and OT (SCADA) networks
- Real-time training on multiple security systems and tools
- Fully scalable and modular in design
- Skill assessment analysis and debriefing in AAR stations
- Cost efficient with maximum use of COTS hardware and software
- Ability to integrate any third party or customer application and hardware
- Advanced training, auditing and analysis tools

## Training for a broad range of cyber security personnel



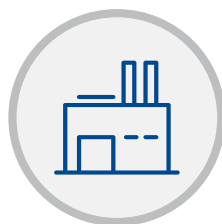
**Government  
cyber defense**



**Military cyber  
defense**



**IT and SCADA  
security workforce**



**Energy, gas, electricity  
and water utilities**



**Telecommunication  
service providers**

## ABOUT CYBERBIT™

CYBERBIT provides advanced cyber security solutions for high-risk, high-value enterprises, critical infrastructure, military and government organizations. The company's portfolio provides a complete product suite for detecting and mitigating attacks in the new, advanced threat landscape, and helps organizations address the related operational challenges. Cyberbit's portfolio includes advanced endpoint detection and response (EDR), SCADA network security and continuity, security incident response platform, and security team training and simulation. Cyberbit's products were chosen by highly targeted industrial organizations around the world to protect their networks.

CYBERBIT is a wholly-owned subsidiary of Elbit Systems Ltd. (NASDAQ and TASE: ESLT)

[sales@cyberbit.net](mailto:sales@cyberbit.net) | [www.cyberbit.net](http://www.cyberbit.net)

**US Office:**

CYBERBIT Inc.  
3800 N. Lamar Blvd. Suite 200  
Austin, TX 78756  
Tel: +1-7377170385

**Israel Office:**

CYBERBIT Commercial Solutions Ltd.  
22 Zarhin St. Ra'anana  
Israel 4310602  
Tel: +972-9-7799800

**PROPRIETARY INFORMATION**

The information here in is proprietary and includes trade secrets of CYBERBIT Commercial Solutions Ltd. It shall not be utilized other than for the purpose for which it has been provided.



**CYBERBIT**  
PROTECTING A NEW DIMENSION