Cyberbit is the industry’s leading hyper-realistic simulation platform, allowing organizations to simulate networks, traffic and attack scenarios, to test people, procedures and technologies in a safe and controllable environment.

Out of the Box Attacks and Networks
Cyberbit offers out of the box content packages for a large variety of cybersecurity attacks. In addition to these packages, you can build new attack scenarios or customize existing scenarios. The platform includes also pre-configured virtual network architectures with many network segments, machines and services. Attack scenarios can be used to simulate the exploitation of vulnerabilities and verify the impact of the attack on this controlled virtual environment.

Cyberbit is in line with industry standard “Best Practices” in including the NIST Incident Response Framework, NICE Cybersecurity Framework and MITRE ATT&CK Enterprise Framework.

Hyper-realistic Virtual Network
Cyberbit comes with pre-configured networks including 60+ components simulating operational environments. In addition to IP-based networks, Cyberbit can integrate sections of SCADA networks, such as physical MODBUS controllers and other SCADA components, to simulate complex networks of critical infrastructure sites. Standard network security tools, such as firewalls, routers, Network Management Systems (NMS), antivirus, SIEM, and more are incorporated into the network, thereby simulating a real-world cyber environment.

Use Cyberbit to Provide:
- Test response playbooks and security tools
- Verify your security posture
- Tailor to your needs

Network Customization
Cyberbit provides the option to import customized networks into the environment and integrate them with the attack server, traffic generator, scenario builder and more. Using Network importer, you can import new network architectures and build a dedicated Cyber Lab to test specific tools, processes, skill level and incident response methodologies.

Drag and Drop Customization
Scenario Builder is a visual designer that provides you with the ability to build scenarios and run them inside Cyberbit. Using Scenario Builder, you can easily create new threat scenarios to be used throughout your training exercises.
ICS Attack scenarios
ICS training scenarios include a hybrid combination of a virtual network, customized attack scenarios and a hardware cabinet of SCADA components. The ICS module allows you to perform penetration tests in the SCADA\ICS environment and observe the effects of an attack on real machines and SCADA equipment.

Benign Traffic Generator
Cyberbit includes an advanced network traffic generation module (TG) that allows the instructor to create specific traffic flows and inject them into the training network to mask the hostile activities that take place during a scenario. Benign traffic includes among others: web surfing, FTP requests, user authentication and other activities that represent real network traffic (HTTP, HTTPS, FTP, POP3, SMTP, SSH etc.).

Furthermore, Scenario Builder allows for easy adaptation of the included Cyberbit scenarios to additional networks.

Attack Server
The Attack Server is an automatic attack machine responsible for executing the attack scenarios and inserting malware into the network. It automatically operates from various network segments, according to the scenario configuration.

The automatic attack machine requires a single click from the instructor application to start executing the full attack scenario.

ABOUT CYBERBита™
Cyberbit addresses one of the most acute cybersecurity problems: preparing the human element for attacks. Its flagship product, Cyberbit Range, is the market leading cyber range for training cybersecurity professionals, preparing cybersecurity teams for attacks by delivering a hyper-realistic experience that immerses them in a virtual SOC, where they use real-world security tools to respond to real-world, simulated cyberattacks. As a result, it dramatically increases SOC team performance, improves teamwork, and improves evaluation, hiring, and certification processes. The Platform delivers over 100,000 training sessions annually across 5 continents. Customers include Fortune 500 companies, MSSPs, system integrators, higher education institutions, governments and militaries. Cyberbit is headquartered in Israel with offices in the US, Europe, and Asia.