

New Cyberbit Range Release Offers Hyper-Realistic Training for Multidimensional Approach to Cyberdefense

Upgraded cyber range gives companies access to dynamic, real-world environments; offsets skills shortage concerns; and offers cross-departmental training for IT and business executives

Austin, Texas – October 26, 2016 – [Cyberbit](#), whose cybersecurity solutions protect the world's most sensitive systems, today announced the expansion of its [Cyberbit Range](#) security training and simulation platform, offering dynamic, hands-on training for IT security teams and business executives so they can be operationally-ready for cyberattacks. The Cyberbit Range lets enterprises, universities and governments address skill shortage concerns and dramatically improves security team responsiveness and effectiveness by providing the industry's most engaging approach to cybertraining.

The upgraded version of the Cyber Range platform includes dynamic range modeling that is highly customizable, so trainees can practice in near real-life settings. Companies can now replicate their own network setup, use their actual security tools and simulate their typical network traffic so trainees can receive the most effective and realistic training available. Additional new features include virtual and physical SCADA training, cross-functional executive training, and new attack scenarios (including ransomware variants). The Cyberbit Range platform leverages the expertise of the world's leading military simulation systems provider Elbit Systems Ltd., Cyberbit's parent company.

As advanced threats evolve to outsmart even the most experienced security teams, a company's approach to cybersecurity training has to mirror the types of multidimensional attacks they are facing today. Current offerings don't offer respite, as they are traditionally based on theoretical training approaches and a predefined set of tools. The Cyberbit Range changes this industry method by giving business leaders and security analysts a hyper-realistic virtual training environment complete with complex incident simulation, a massive library of attack scenarios and next-generation training tools.

“Security analysts are expected to both master and operate dozens of new tools continually against threats they have never seen, so organizations that put people first will succeed and thrive in today’s ever-evolving threat landscape,” said Adi Dar, CEO of Cyberbit. “By making real-life simulated training more accessible, Cyberbit Range ensures teams – from SOC staff to executives – are best equipped to manage these targeted attacks.”

“Every day, cyber criminals are developing new means of infiltrating networks in government, in the private sector, and in organizations across the globe,” said Col. Ken McCreedy, USA (Ret.), senior director of cybersecurity and aerospace for the Maryland Department of Commerce. “The flood of new types of cyber threats has, in turn, created a tremendous demand for cybersecurity professionals. Thanks to ETA’s selection of the Cyberbit Range for its new cybersecurity training center in Baltimore, Marylanders will have access to lifelike simulations and interactive training, ensuring a new wave of cyber sleuths will be able to effectively strategize and combat evolving cyber-attacks.”

A complete organizational ecosystem that gives users real-world simulations of threats and traffic on multiple network types, Cyberbit Range provides individuals and teams the training to assess and fine-tune their capabilities. This helps managers enforce best practices and make smarter decisions based on network activity. Together, security analysts and managers receive practical training on how to collaborate and approach various attack types.

New features include:

- **Dynamic range** – Provides the tools for companies to replicate their network setup in a virtualized environment so trainees can practice in realistic settings.
- **Training for business executives** – Expands training outside the security operation to the business level, so security and business teams can collaborate and flawlessly execute organizational best practices.
- **Custom scenario builders** – Customers can create specific attack scenarios based on their organizational needs, and expand the extensive scenario library included with the Cyberbit Range.
- **SCADA training** – Security staff tasked with protecting critical infrastructure facilities can utilize actual SCADA hardware and unique ICS/SCADA protocols to best simulate their physical environment and improve team effectiveness during an attack.
- **Updated scenario package** – the Range will include new and updated attacks scenarios such as ransomware.

The new updates for the Cyberbit Range are available immediately. For pricing and more details, please contact sales@cyberbit.net.

Additional resources:

- Read the blog: [The Cyber Range – Addressing the “Security Tools Fatigue”](#)
- [Request a demo.](#)

About Cyberbit

Created to protect the most high-risk organizations in the world, Cyberbit secures enterprises and critical infrastructure against advanced cyberthreats. The company's battle-hardened cybersecurity solutions detect, analyze and respond to the most advanced, complex and targeted threats. Cyberbit employs a formidable and diverse team from both the public and private sector including PhDs, hackers, former CISOs and SOC managers, as well as seasoned veterans of the intelligence and military communities. With offices in Texas and Israel, Cyberbit is a subsidiary of Elbit Systems Ltd. (NASDAQ: ESLT) and has more than 500 employees in the United States, Europe and Asia. To learn more about how Cyberbit maximizes protection against today's signature-less threats, visit www.cyberbit.net.

Contacts:

Dalia Rosen, VP, Head of Corporate Communications

Tel: 972-4-831-6784

Fax: 972-4-831-5420

E-mail: dalia.rosen@elbitsystems.com

Dana Tal-Noyman, Corporate Communications

Tel: 972-4-831-8809

Cell: 972-54-9998809

E-Mail: dana.tal@elbitsystems.com

Justine Boucher, Metis Communications

Tel: +1 617-236-0500

E-Mail: cyberbit@metiscomm.com