CYBERBIT
TRAIN FOR REAL

Cyber Range for Enterprise - Build or Buy?

White Paper

Overview

An increasing number of enterprise leaders are adding cyber range training to their annual SOC team training regimen ensuring that their cyber practitioners can train in realistic, simulated IT environments and scenarios. The approach of using a cyber range poses numerous benefits to enterprises. A key decision in the establishment of a cyber range is whether to build it internally or buy a ready-made cyber range product. This white paper elaborates the pros and cons of building your own cyber range versus buying one off-the-shelf.

What is a Cyber Range?

A Cyber Range is a virtual SOC simulation platform aimed at training and assessing cybersecurity practitioners while also providing a testbed for new tools and processes in a real-world virtual environment that simulates attacks, benign traffic, and scalable networks. Cyber Ranges provide hands-on training using commercial security products, enabling trainees to practice detecting, investigating and responding to cyberattacks. A Cyber Range simulates a multitude of cyber threats in varying levels of difficulty and offers a selection of network structures and security tools that mirror the trainee's production environment.

Benefits of including Cyber Range Sessions in Annual Cybersecurity Training

Cyber ranges serve as a hands-on cyber simulation labto train cybersecurity practitioners in an advanced, simulatedenvironment. Enterprises all over the world increasingly include cyber range sessions in their annual training to gain valuable experience against real cyberattacks, ensuring that their SOC team is prepared when a malicious attacker attempts to breach the network they have been hired to protect. Since most SOC team members do not experience their first attack until it is occurring, providing a real-world experience is paramount to ensuring success.

Benefits of Cyber Range sessions

- Train cybersecurity practitioners
- Assess SOC team candidates
- Test processes and technologies

All in a true-to-life environment that simulates attacks, scenarios and networks.

Should I Build my Cyber Range, or Buy One?

To be effective, a cyber range should at least include the following key components:

Component	Objective	Comments
Virtualized Networks	Provide a realistic environment mirroring an enterprise network	The range should emulate a variety of network topologies to accommodate multiple types or organizations, such as financial institutions, corporate networks and industrial control networks (such as those deployed in a manufacturing facility, electric grid or utility company).
Training Scenarios	Execute a wide range of repeatable training sessions simulating multiple attack scenarios for multiple roles.	Training scenarios should be automated and repeatable to maintain consistency and provide an unbiased assessment of trainees' capabilities and achievements.
Attack Machine	Design new training scenarios in a straightforward manner and execute them in the simulated network.	To create new threat scenarios that mirror recent attacks, simulated attacks should consist of building blocks that are easy to assemble and edit. These scenarios should be easily injected into the simulated network.
Traffic Generator	Generate benign traffic in the simulated network to optimize the training experience.	The Range should generate a variety of traffic protocols and types of communication such as emails, web browsing, SYN flooding and more.
Training Setup Tools	Easily and rapidly set up a new training session.	The range should offer a straightforward setup tool or wizard to enable instructors to select the network topology and scenario, allocate team members, and modify scenarios and levels of difficulty on-the- fly.
Debriefing Tools	Provide effective post-training debriefing.	The platform should support session recording and replay, and should seamlessly integrate with predefined scenarios to display or skip to significant events.
LMS Integration	Share qualification data between Learning Management Systems and the Cyber Range, allowing trainees to independently go through LMS-based training and participate in related hands-on Range-based training.	The Platform should preferably combine theoretical LMS-based training with hands-on training in a cyber range, with data sharing between both systems supported for trainee assessment and tracking.
Assessment Tools	Assess individual and team performance.	Provide automated assessment and ranking of trainee performance and skills, as well as free-text comments for tracking.

Main Pros and Cons of Building Your Own Cyber Range

Pros:

- **Customization -** Custom design, according to the specific needs of your SOC team
- **Training Alignment -** Scenarios can be completely aligned with the curriculum, pending the investment in building, customizing and testing attack scenarios
- **Budget management -** No need to pay for extra features which may not be used

Cons:

- **Maintenance Overhead -** Creating and maintaining a homegrown range carries substantial costs, which are not always evident in the planning stage. These involve managing 3rd party tools and the effort required to modify scenarios and maintain networks. These costs are detailed in the following section, The Cost of Building Your Own Range.
- **Attack Scenario Setup -** Maintaining, updating, adding, and testing attack scenarios is one of the most significant overhead contributors of using a homegrown range. A single scenario may take weeks to tailor and test. Furthermore, aligning scenarios with the various network topologies simulated in the range is a time-consuming process. For example, the vulnerability being exploited in an attack scenario must be present (planted) in the simulated network components.
- **Network Topology Modification -** A commercial range comes with a set of virtual networks that can be fired up quickly and reset in a click of a button after the training session ends. A homegrown range involves significant efforts in launching and resetting networks, often requiring direct modification of the virtual machine.
- **Functionality and Feature Set -** A commercial range integrates multiple capabilities such as setup, attack scenarios, benign traffic simulation, recording, replay, and ranking, which all work in tandem as a single integrated offering. A homegrown range typically does not include this set of capabilities. This significantly reduces training quality.
- **Quality Assurance -** A home-grown range would require ongoing debugging and would have to be supported by the faculty. In contrast, a commercial range would be tested on an ongoing basis and its support would be offloaded to an external service provider, reducing maintenance overhead.

The Cost of Building Your Own Range

When considering to build a cyber range in-house, the following are some of the costs that should be factored in:

1. **Network design –** The foundation for a cyber range is a virtual network, and often even a set of virtual networks. The network includes components such as databases, web servers, email servers, AC server, user endpoints, and industrial control system (ICS) components. The networks are designed to support the needs of organizations across various industries, to which the range may be offered for training. Before setting out on a Cyber Range project, an enterprise should consider the training use cases it expects to accommodate, and evaluate the scenarios it wishes to simulate, including the design and testing of network architectures. This phase takes 2-3 months of a full-time staff member.
2. **Scenario development –** Designing and implementing effective attack scenarios, particularly complex attacks, using the latest attack methods seen in the wild, may take 1-2 months, and requires expertise in threat and attack analysis. An effective curriculum should include dozens of attack scenarios with varying levels of difficulty, which may take more than a year for an organization to create.
3. **Network maintenance –** Adding new network topologies or adapting an existing network for a customer in a specific industry, such as a financial institution or a manufacturing company, would require a skilled and dedicated staff member, with network architecture expertise.
4. **Scenario modification –** Training scenarios must be adapted to the network in use, requiring significant expertise in threat and attack analysis.
5. **Third party tools –** An effective range integrates dozens of security tools, allowing trainees to train in an environment that mirrors their own. These licenses require additional procurement overhead and may require an additional lead time of 3-5 months for license negotiations, while a commercial range includes these systems "out-of-the-box."
6. **Context management –** Initiating a training session requires setting up the appropriate network, scenarios and levels of difficulty. All these are pre-configured in a commercial range and are automatically set up with a single click of a button when a session is initiated. However, in a homegrown range, these are managed manually and require an IT administrator's time.
7. **Trainee monitoring, ranking and debriefing –** A key to an effective training session is the instructor's ability to monitor the session, play it back for student feedback, and rank trainees. A lack of these capabilities may result in the need to hire additional staff members.
8. **Auto-Scoring** - Providing your staff with the ability to train on their own, requires a set of tools and techniques to automatically evaluate the knowledge and accomplishments of the trainee participating in the scenario. Such techniques can be an evidence evaluation application or sensors to be built into both the tools and endpoints on your system. These sensors will ensure that your trainees are performing the right actions in the network. Building these sensors into your network will require significant work as each sensor must be configured to the correct stage of each attack scenario.

Costs of Building a Cyber Range In-House

Item	Duration and cost	Total Cost	Comments
Range network design	2-3 months' time of a dedicated staff member	$12K	
Scenarios	$20K-$40K per scenario x 10 scenarios	$200K-$400K	
Network modification	2-4 weeks	$8K	Medium size network adaptation: 2-3 segments, 30 endpoints
Scenario modification	$10K for an external expert 70-150 hours for an in-house expert	$10K	Adaptation to a different network of ~100 endpoints
Managing 3rd party tools	3-5 weeks of initial negotiations, then bout 1 week of work a year. Cost - $20K initially, hen $5K-$10K annually	$50K	
Context management	1-2 hours daily of an IT administrator	$20K-$30K	Per annum
Debriefing and training session monitoring	Increase in number of instructors	$50K-$70K	Per annum
Auto-Scoring Mechanism	$20k per scenario x12	$240K	
Fresh & Updated Auto Scoring	$20k per scenario x3	$60k	Per annum
TOTAL		**$718k - $723k** **$280k - $310K**	**For the first year** **Per annum for each consecutive year**

Cyberbit Range

Cyberbit Range is a cybersecurity training and simulation platform that enables trainees to experience true-to-life cyberattack scenarios and practice responding to them. Trainees operate in a hyper-realistic environment which includes a configurable corporate network, commercial security tools, emulated traffic and simulated attacks with various levels of difficulty. Scenarios simulate the latest online threats, such as ransomware, web server shutdown and denial of service (DoS) attacks. Diverse network topologies can be deployed as required by the training program to replicate those found in financial institutions, industrial control networks and other sensitive enterprises. These network blueprints include specific components and architectures tailored for the training program, allowing adaptation of existing scenarios and networks. Cyberbit Range has an advanced training management system that provides instructors with a live view of the trainees' screens, and offers drag-and-drop creation of new training sessions, post-training debriefings and trainee evaluation. Cyberbit Range offers over 40 out-of-the-box scenarios, constantly being updated to ensure your team is equipped to handle any known attack type.

ABOUT CYBERBIT™

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.

sales@cyberbit.com | www.cyberbit.com

CYBERBIT
TRAIN FOR REAL