CYBER RANGES

CYBER EXERCISES
Resilience, Enhanced

Powering up your Cyber Drills with CYBER RANGES by Silensec

What is a Cyber Drill?

A Cyber Drill is a planned event of various formats, during which an organization simulates cyber attacks, information security incidents and other types of disruption.

With a Cyber Drill your organization can test its cyber capacity, capability and resilience by measuring its ability to detect, respond to and stand against security incidents of all types, minimizing any related impact.

Cyber Drill Simulations are delivered through different **experiential scenarios** that run in a secure environment that replicates, to a chosen degree of fidelity, the live or desired infrastructure of your organization.

A scenario is a self-contained piece of interactive content, which combines a storyline, a virtual infrastructure and applications, competency objectives, user activity, tasks to perform and challenges to deal with, ancillary contextual information assets, and much more. Scenarios may engage single or many users, be time-constrained and mapped against a number of criteria, such as competencies and performance indicators.

Since 2017 CYBER RANGES by Silensec has been supporting the delivery of all the Regional Cyber Drills organized by the United Nations' International Telecommunication Union (ITU) in collaboration with national regulatory authorities all over the world.

These Cyber Drills have engaged hundreds even thousands of delegates from national CERTs/CSIRTs, critical infrastructure operators, financial and telecom institutions.

The 6 scenario-based Exercises of the ITU 2020 Global Cyber Drill, engaging over 210 participants from 57 countries, have been on the CYBER RANGES platform.

silensec™
iso27001 Certified

Information Security Professionals

England | Kenya | Cyprus (HQ)

Benefits of CYBER RANGES

- Testing your organization's ability and validating its plans to respond to security incidents.
- Testing your organization's cyber resilience
- Assessing the cyber capacity and capabilities of a SOC team
- Assessing the competence of your organization's Red Team
- Complying with regulatory and best-practice requirements, e.g. from a Central Bank
- Testing the cyber proficiency of other Teams, e.g. Blue Team, DevOps, Comms, Legal
- Testing your team's current skill set and identifying any gaps and areas for improvement
- Evaluating your team's readiness and response reflexes against cyber attacks, when needed in combination of table-top, in-theatre or kinetic exercises
- Testing the coordination, communications and information sharing of internal and external teams, stakeholders, ecosystem partners, third parties and other entities
- Team building opportunities.

Cyber Drill Design

Choose from a wide range of realistic simulation environments, from simple environments with just a few systems (VMs) to more complex environments with dozens of systems to allow teams with different roles to collaborate and/or compete against one another.

Customize your simulation environment, by choosing from an exhaustive library of commercial security systems and applications, from pre-set environments to customizing these or even replicating your full infrastructure.

Choose the attacks you want to simulate, from simple attacks exploiting a single vulnerability, to more complex, sophisticated attacks simulating advanced threat vectors and exploiting both human and technical vulnerabilities.

Choose the difficulty level, by turning each chosen attack into a search for the "needle in the haystack" by adding background user traffic, thousands of realistic event logs, multiple parallel attacks from different countries and much more, depending on the skill levels of the participants.

CYBER SPACE, ENGAGED.

Silensec specializes in the delivery of **Cross Cyber Drills (C2 Drills)**, where hands-on and table-top scenarios are simultaneously delivered to Operations and Management teams to simulate the overall effectiveness of information security processes, communications and responsibilities.

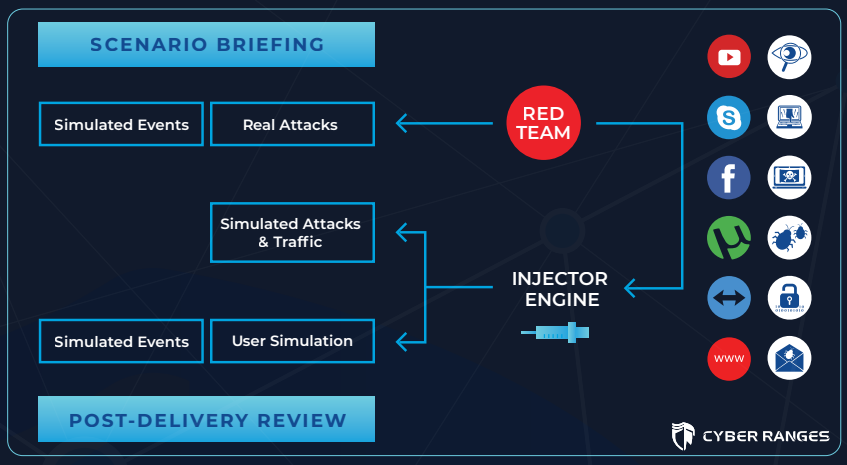
Cyber Drill Delivery

In a typical execution of a Cyber Drill powered by CYBER RANGES, the CYBER RANGES Injector Engine is responsible for the simulation and automation of a wide range of cyber attacks, user activities and background traffic.

The CYBER RANGES Injector Engine is also used by the White Team to inject live attacks and traffic during an active scenario.

This increases the difficulty of the scenario against the performance of the participants. Real attacks can be even carried out by an external Red Team connected to the CYBER RANGES simulation environment.

CYBER RANGES Features



- End-to-End Cyber Drill workflow management
  - User registration and creation of teams
  - Design, development and delivery of the Cyber Drill Scenarios
  - Assessment of skills, cyber capabilities and cyber resilience
  - Learning paths to skills gap and cyber capability shortage remediation
- Library of Cyber Drill Scenarios, design and development of Customer-specific Scenarios
- Library of Attack Simulations to replicate the latest cyber threats
- Seamless integration and support of Scenarios from Value-Added Third Parties.

CYBER RANGES for National Cyber Drills

National Cyber Drills are usually organized by a National Focal Point that brings together organizations from across the Nation's critical infrastructure.

With CYBER RANGES the organizing of Cyber Drills becomes streamlined and National Authorities leverage on the ability to easily plan the cost-effective execution of Cyber Drills at desired regular time intervals (every year down to every term or less) and to even organize multiple Cyber Drills by theme or industry sector.

CYBER RANGES offers Authorities the opportunity to obtain measurable outcomes and actionable assessment towards the continuous development of skills, cyber power and ultimately improvement of your stakeholders' cyber resilience.

Through CYBER RANGES PORTABLE a Cyber Drill can be delivered to accommodate any location requirements (such as an oil rig, a military outpost, or a vessel at sea).

Benefits of National Cyber Drills

Evaluating readiness and response abilities to coordinated cyber attacks across the Nation
Assessing national cyber capabilities
Raising awareness of the latest cyber threats
Improving coordination, communications and sharing of cyber threat intelligence among national stakeholders.

Corporate Cyber Drills and Training

CYBER RANGES can be used to address the security training needs of any organization through corporate Cyber Drills, and to deliver company-specific hands-on training scenarios over a highly realistic replica of its live or desired IT, OT, ICS, IoT infrastructure.

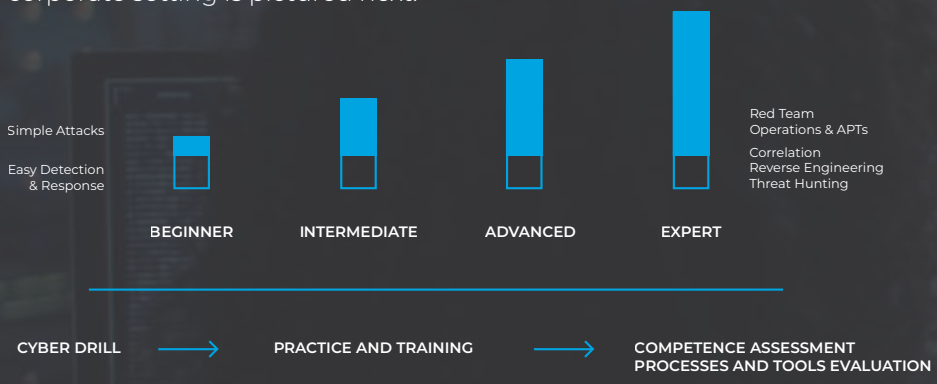
Cyber Drills are used to assess the organization's cyber capabilities and cyber resilience at regular intervals while also identifying gaps in specific security domains.

Sample scenario formats include:

RED TEAM vs BLUE TEAM	In this corporate scenario type players are divided into two teams, simulating respectively the attackers (red team) and the defenders (blue team). This scenario type is ideal for testing and improving the communication and collaboration between an organization's cyber defence and offensive teams.
LIVE FIRE	In this scenario format participants are exposed to live attacks simulating different types of threat actors. The attacks are simulated automatically or live through the CYBER RANGES Injector Engine. This scenario is ideal for testing the detection and response capabilities of the SOC Team or for assessing the organization's cyber resilience against specific cyber attacks.
CAPTURE THE FLAG	This scenario type can be used to assess a wide range of hands-on security skills by targeting different security roles within the organization. Suck key roles being: Penetration Tester, SOC Analyst, Malware Analyst, Threat Hunter and more.

Each Scenario Type can be easily built on the replica of a specific corporate environment in order to train teams for identifying and responding to specific attack vectors.

The typical application of a CYBER RANGES-powered Cyber Drill to a corporate setting is pictured next:



CYBER RANGES has proudly powered up the United Nations' ITU 2020 Global Cyber Drill

Virtual Cyber Drills

A Virtual Cyber Drill is an online Cyber Drill with no need for a physical venue to hold activities in.

CYBER RANGES is the ideal platform for the delivery of Virtual Cyber Drills with a great number of participants, well above the typical industry average of 10-20 participants each time, and while ensuring a high-fidelity simulation experience.

The Planner's "Magnificent 7" Reasons to Host a Virtual Cyber Drill on CYBER RANGES:

1. CYBER RANGES HOSTED for the secure private access to the Cyber Drill scenarios and data
2. Customized Secure Cyber Drill Registration Page
3. Design and development of custom Cyber Drill scenarios
4. Integrated Webinar Technology for online Cyber Drill delivery and Expert Moderator tools
5. Live interactive experience of Scenarios and hands-on practice of the Cyber Drill scenarios, led and supervised by field-hardened cyber security experts
6. Secure recording of the Cyber Drill Sessions for post-delivery playback
7. Expert Evaluation Report and Follow-on Consultancy.

CYBER RANGES
CYBER SPACE, ENGAGED.

For more information on how and when to organize your next Cyber Drill contact us or our Value-Added Partners at:
info@cyberranges.com