CYBER & SECURITY SOLUTIONS

LX RANGE

Leonardo Cyber Range

LEONARDO

The definition and implementation of an optimal cyber security strategy for national ecosystems implies the development of defense capabilities, including training and exercising for security teams and technical staff working in both governmental and critical infrastructure sectors.

Institutions and operators of national industries and utilities — such as defense, energy providers, transport, and telecom operators — must be fully aware of cyber risks. They also need to promptly test and coordinate effective countermeasures to mitigate these risks and minimize their impacts.

Realistic training and testing are essential to support effective cyber protection and response. However, the most advanced cybersecurity teams face challenges such as ensuring training focuses on the most relevant and sophisticated threats specific to their operational context, assessing the effectiveness of their incident response procedures, and performing thorough post-mortem analyses to identify and correct weaknesses in defense strategies. Furthermore, collaboration among specialists is often hindered by the lack of efficient information sharing and dedicated tools for testing cyber resilience.

While real production systems would theoretically offer the best training environment, exposing them to dangerous situations is neither feasible nor safe due to potential operational disruptions and costs. Advanced digital ecosystems for real-world infrastructure modeling address this issue by leveraging state-of-the-art cloud provisioning and virtualization techniques. These infrastructures enable the creation of immersive scenarios where cybersecurity personnel can learn, train, and exercise, while supporting detailed analysis and debriefing on current cyber threats.

This capability is essential to ensure service continuity and operational resilience at the desired levels. Cyber Range environments also enable deep testing activities on new software and network components, as well as on organizational strategies and procedures, guaranteeing optimal protection and resilience against malicious cyber activities.

WHERE THREATS MEET READINESS

LX Range simulates highly realistic hybrid federated theaters to provide advanced training environments for cyber experts, test the cybersecurity of products and technologies, and assess the resilience of complex infrastructures. It implements complex multi-domain digital twins and offers highly configurable, reusable theaters and scenarios that can operate concurrently.

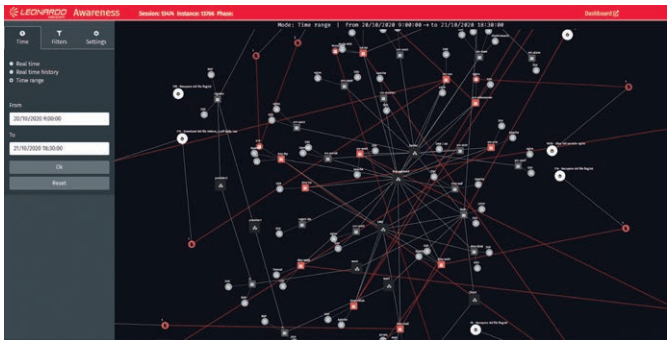
Live Exercise Phase

Theater Design:
the process begins by creating a theater that is the digital twin of the target infrastructure, replicating both the digital and physical systems of the organization. This includes systems, networks, applications, relevant documents, and automated attack/defense platforms. The theater is built from a modular library, allowing high customization and reusability to support multiple scenarios.

Scenario Definition:
on the theater, a training scenario is defined by specifying the type and objectives of the cyber game, event scheduling rules, and team composition. Depending on available resources, up to hundreds of virtual machines can simulate target systems along with their applications and network elements.

Gaming Session:
after deploying the scenario and instantiating virtual machines, the cyber exercise begins. Trainees, typically divided into Red (attack) and Blue (defense) Teams, practice techniques on a dynamic and partially known theater. Using specialized tools (e.g., attack workstations and SIEM), teams pursue goals while reporting actions, collaborating via intelligence platforms, and messaging tools. The White Team (supervisors) monitors the exercise during its execution through aggregated visualizations of tactics and participant behavior, supported by administrative tools for scoring.

Evaluation & Debriefing:
participant performance is assessed using automated and semi-automated tools throughout the exercise. After the session, full action tracking enables detailed analysis at both individual and team levels. The information gathered by the White Team supports a continuous improvement cycle, allowing identification of vulnerabilities and the optimization of defensive strategies and procedures.



Visual awareness module interface example

Logical Model

LX Range manages the design, implementation, and orchestration of theaters, scenarios, and simulation sessions through the integration of specialized architectural modules:

Theater Module Design creates digital twins of target infrastructures using a modular library of networks, OS, apps, and artifacts. It supports graphic configuration and models attack/defense tools and interconnections. Modules are reusable, adaptable, and upgradable for evolving training scenarios.

Automated Attack (Defense) Execution enables automatic deployment, orchestration, and execution of attack and defense tactics using FOSS and COTS tools covering the full attack chain. It supports reusable tactics with conditional execution, automatic or semi-automatic operations, and provides real-time feedback for evaluators and scoring.

Exercise Management & Orchestration, supports theater composition, exercise configuration, deployment, management, and orchestration. Supports monitoring, event data capture, scoring evaluation, and gaming awareness. Allows multiple parallel sessions on the same theater with remote access for Blue, Red, and White Teams.

Visual Awareness provides a portal for the White Team to monitor team activities during live exercises, access performance data and reports, and support scoring and evaluation. Features interactive navigation across networks, nodes, and services, with visual correlation of team actions and simulated infrastructure elements.

Scoring Management permits dynamic visualization of progress and results from both automated and manual attack and defense activities. It generates detailed, comprehensive reports on team actions and performance during exercises, supporting thorough evaluation, scoring, and debriefing processes.

Traffic Generator simulates user activities and generates related network traffic within the environment. Injects background traffic using over one hundred simulated protocols. Supports measurement of usability, Quality of Service (QoS), and Quality of Experience (QoE) metrics during exercises.

Identity & Access Management ensures secure and controlled access to the LX Range environment through centralized user enrollment and strong authentication mechanisms. It supports flexible access policies and fine-grained control over user roles and permissions. Identity management is streamlined across all LX Range modules, enabling participants to interact only with the components relevant to their assigned tasks

Attack / Defence execution platform interface example

Test and Evaluation

Leveraging its capabilities for automatic generation and configuration of complex theaters and scenarios, LX Range can simulate an infrastructure by accurately replicating both the digital and physical systems of an organization. This capability allows testing of IT and cybersecurity technologies in isolated environments against realistic real-world threats. Additionally, the system enables the identification of vulnerabilities in assets and security systems, supporting the definition and validation of effective containment and mitigation procedures.

KEY FEATURES

- → Continuous updates on the most advanced and relevant threats to mission-critical digital infrastructures, enabled by collabora tion with the Leonardo Global Cybersec Center.
- → Capability to integrate complete digital twins, modeling complex infrastructures and technologies in highly realistic scenarios.
- → Highly configurable scenarios with automated deployment, requi ring no further intervention.
- → Automated attack and defense modules, configurable during the initial setup phase of scenarios.
- → Collaborative, competitive, and technology evaluation processes integrated with external virtual and physical environments.
- → Federation-ready architecture for integration with third-party cyber ranges.

For more information:
cyberandsecurity@leonardo.com

Leonardo Cyber & Security Solutions Division
Via R. Pieragostini, 80 - Genova 16151 - Italy

MM08974 07-25

leonardo.com