CYBER RANGES

Customer Success Stories

A Selection of Project Implementations

About the Company

CYBER RANGES is the ISO27001 certified next-generation military-grade full-content lifecycle platform for the validation of threat-informed defense capability and cyber resilience. Built on cloud technology, CYBER RANGES is available as subscription, as managed service, as On-Premise, also with a Portable rugged deployment option. Our TOAR-based ecosystem combines up-to-date threat intelligence, next-gen cyber ranging and incident response systems.

CYBER RANGES applies high automation, high orchestration and high scalability to the delivery of even complex large-audience deep-dive tabletop and technical drills based on high-fidelity IT/OT infrastructure replicas. CYBER RANGES fully supports MITRE (PRE-)ATT&CK® across its entire cyber range architecture. Through its proprietary Injector Engine CYBER RANGES emulates the latest-intel attacks, APTs and specific tactics and exploits from the MITRE ATT&CK® Matrix™.

CYBER RANGES powers the international CyberStars™ initiative run in collaboration with national focal points and regulatory authorities from around the world. CyberStars provides a turnkey project package for participating countries to organize national cybersecurity competitions and to participate in international ones, while at the same time meeting the objectives of national cybersecurity strategies.

CYBER RANGES actively participates as a key member organization in the European Cyber Security Organization (ECSO), where Dr. Al Graziano CEO is the co-chair of the Working Group WG5 on Education, Training, Awareness and Cyber Ranges, advancing best practices in the domain of cyber ranges, cyber exercises, cybersecurity education and competency development.

CYBER RANGES is also an active Partner of the Global Cyber Alliance – GCA (New York, Brussels, London) in its worldwide mission to sustain a trustworthy Internet by reducing cyber risk. CYBER RANGES is a founding member of the Canada-based Cyber Security Global Alliance (CSGA) and a partner of the Virginia-based Cyber Bytes Foundation.

CYBER RANGES Corp.
Quantico Cyber Hub, Suite 305, 1010 Corporate Drive, Stafford, VA 22554 (USA)

For all queries please write to us at: **contact@cyberranges.com**
or call us toll-free (North America): **1-800-959-0163**
or visit: **www.cyberranges.com**

CASE STUDY

Threat-Informed Defence

Domain	**Military**
Year	**2020-2021**
Audience	**Security analysts, supervisors**
Number of Users	**Classified information**
Use Cases	**· Attack & Defend training** **· MITRE ATT&CK bespoke scenarios** **· Knowledge Assessment**

Customer Requirements

An elite military unit of a NATO country wanted an environment where its security analysts could train as well as create realistic complex infrastructures in which complex attack-defence scenarios could be run with the aim of validating security technologies and current vulnerabilities in a controlled environment.

The environment aimed at supporting Red Team, Blue Team, Grey Team and White Team activities against attacks available in the platform to be based on the MITRE ATT&CK® Matrix with various degrees of complexity and difficulty. Additionally, the simulations in the library had to address the specifications of the latest known vulnerabilities.

The platform was required to execute the same attacks available in the then-current polygon and on other virtual machines that emulate work machines or servers configured as those in production, virtualized and available in the virtualization platform. The attacks had to be carried out in their raw form with the goal of determining resilience to the respective exploits. For each scenario the Customer requested the ability to modify easily the network features (such as source or destination IP addresses) and applications installed on the virtual machines involved in the scenario.

The platform had to automatically determine whether the evaluated person could manage to stop the attack launched against the resource being protected. The same if an offensive scenario was being played, in which the candidate had to exploit a previously unknown vulnerability. An activity report was then produced for the two types of scenarios (offensive and defensive). The range platform was expected to track several compromise indicators at the same time so that the administrator could assess the path undertaken by the person assessed throughout the scenario period and generate evaluation reports on the basis of the compromise indicators pursued.

Market Gap

The Client required an on-prem cyber range that allowed its personnel to create bespoke simulations of situations and attacks. When looking at available solutions in the market, all of them were either lacking of the required ease of use, could not be used by the operators autonomously, or the available attack simulations were too simple and lacking of realism. Also, no other range vendors could provide content authoring functionality, nor the ability to dynamically configure the attack injections, as required for designing classified simulations.

CYBER RANGES Value Choice

CYBER RANGES implements different roles with different privileges and a fully independent authentication module, which can be extended to integrate with external active directory services.

The CYBER RANGES dashboard and scoreboard allow full visibility of scenario execution and assessment. CYBER RANGES scoring and reporting functionalities supports the generation of a number of reports. Evaluation is carried out by the Exam Engine and the Scoring Engine and it reflects the parameters defined in the scenarios being used, for instance NIST NICE. New evaluation reports can be created by editing the evaluation parameters in the scenario definition and through the Scoring Engine.

Scenario Composer and Injector Engine are built in the CYBER RANGES platform, which can scale up to support scenarios and virtual infrastructures totalling 1,000's of simultaneous virtual machines.The CYBER RANGES architecture implements native redundancy and back-up of its scenarios. CYBER RANGE implements TOAR with native orchestration at its core, which means a limited number of steps and actions are required to managed the lifecycle of scenario virtualization, in most cases being fully automated. Through the Injector Engine it is possible to reproduce many different attack types.

This was an air-gapped cyber range deployment during the COVID-19 pandemic. The system had to be fully operational in three months from the tender award. The project team to appoint had to show suitable expertise and credentials. We demonstrated strong empathy with the Customer's operational requirements, a solid trust relationship with our local market partner, together with an up-to-date understanding of the MITRE ATT&CK Matrix. The subscription to the CYBER RANGES Threat-Informed Scenarios, guaranteed that every month the organization would receive up-to-date attack simulations reflecting active threat actors. A process was developed to ensure that the monthly updates could be safely transferred onto the CYBER RANGES isolated environment. ■

CASE STUDY

Threat-Informed Defence

Domain	**Banking**
Year	**2021**
Audience	**Security Team**
Number of Users	**40+**
Use Cases	**· Skills Development** **· Assessment of Cyber Resilience** **· Threat Emulation**

Customer Requirements

One of the largest banks in the GCC region wanted to acquire a cyber range for the upskilling of their security personnel and for the continuous assessment of cyber resilience. The Bank wanted the cyber range to address the following needs:

- **Continuous Professional Development** – The cyber range needed to have up-to-date skills development scenarios which could be used autonomously by the security team to upskill
- **Replica Environment** – The bank wanted to set up a replica environment onto the cyber range and use it to run regular threat simulations to practice and assess the security team's incident response skills
- **Assessment of cyber resilience** – The bank wanted to run regular assessments of cyber resilience to measure their response capabilities to a number of cyberattacks.
- **Private Cloud Deployment** – The cyber range had to be deployed on the bank's private cloud environment on Azure.

Market Gap

Most of the products that the Bank investigated, focused on offering training scenarios but had no threat emulation capabilities, no support for tabletop delivery and no assessment of cyber resilience. Last but not least, the Bank found very few options which could be deployed on the bank's private cloud infrastructure.

CYBER RANGES Value Choice

CYBER RANGES was able to meet the Bank's needs through its unique cyber resilience assessment features and functionalities, which enable to combine tabletop and operational exercises, bringing both the management and technical teams together for responding to the simulated attacks. The cyber exercises were conducted regularly on the Bank's infrastructure with an isolated replica environment. The members of the security team were able to easily access the deployed CYBER RANGES platform for independent learning and upskilling throughout the year. ■

CASE STUDY

United Nations

Domain	**Intergovernmental Agency**
Year	**2021 and 2022**
Audience	**National CERTs**
Number of Users	**500+**
Use Cases	**· Online delivery of Large-scale cyber exercise** **· Threat Emulation**

Customer Requirements

The United Nations' International Telecommunication Union (ITU) has been responsible over a decade for the organization of national and regional cyberdrills aimed at national CERTs to help them further develop their response capabilities and strengthen international collaboration and coordination. When the COVID-19 pandemic broke out in 2020 all in-presence events were cancelled and ITU decided to deliver a worldwide capability event, the Global Cyberdrill, entirely online. The ITU needed a cyber range platform that would meet the following requirements:

- **Large-scale cyberdrill** – The Global Cyberdrill was going to be open to all the United Nations member-States and therefore the platform would need to support thousands of virtual machines.
- **Web-based Delivery** – The Global Cyberdrill was to be delivered online and web-based access was key to ensure the participation of CERTs from around the world.
- **Remote Facilitation** – The cyber range platform would need to offer capabilities to provide remote technical support and supervision to participants.
- **Threat Emulation** – Many of the cyberdrill scenarios challenged the incident response process of CERT teams and the ability to simulate real threats was crucial to successful realism.
- **Collaborative Scenario Development** – The cyberdrill scenarios were to be developed by multiple ITU partners who would need remote access to the platform to develop their scenarios

Market Gap

The ITU needed a solution that was flexible, could run with minimal back-stage and on-stage resources, and could accommodate a substantial number of requirements. However, current solutions were either not scalable or the scalability was only limited to the simulation environment and not to the management of large-scale events. Furthermore, multiple separate solutions would have needed to be set up and integrated to deliver the Global Cyberdrill.

CASE STUDY

United Nations

cyberranges.com

CYBER RANGES Value Choice

CYBER RANGES provided ITU with a turnkey solution from user registration and onboarding to the management of the entire cyberdrill lifecycle, bringing together CERTs from around the world and enabling other ITU cyberdrill partners to collaboratively work on a single range platform for the design and development of their scenarios. ■

CASE STUDY

National Financial Drill

Domain	**Financial Sector**
Year	**2021**
Audience	**CISOs, SOC analysts, Incident responders**
Number of Users	**400+**
Use Cases	**· Online delivery of Large-scale cyber exercise** **· Assessment of cyber resilience** **· Threat Emulation**

Customer Requirements

The Central Bank of an East Asian country wanted to organize a national industry-wide cyberdrill to assess the cyber resilience of all its financial institutions: banks, insurance companies and payment providers. Furthermore, the Central Bank wanted to test the incident response and threat-sharing collaboration among institutions.

The Central Bank was looking for a cyber range solution that would meet the following requirements:

- **Large-scale cyber exercise** – Being a national event, the platform would need to support hundreds of users and 1,000+ virtual machines.
- **Life-like Threat Emulation** – The cyber range platform would need to include real attacks simulating current threat actors and associated attacks campaigns.
- **Observer Capabilities** – A number of different stakeholders wanted to observe the execution of the cyber exercise and needed spectator access to the platform.
- **Tabletop and operational cyber exercises** – The platform needed to simulate real-life interaction between management and operational personnel in handling the incident response.
- **Realistic Simulation Environment** – The platform needed to provide each participating organization with access to a realistic simulation environment replicating a corporate infrastructure of a typical financial institution.
  Online Delivery – The platform needed to be able to support online only delivery of the cyberdrill.

Market Gap

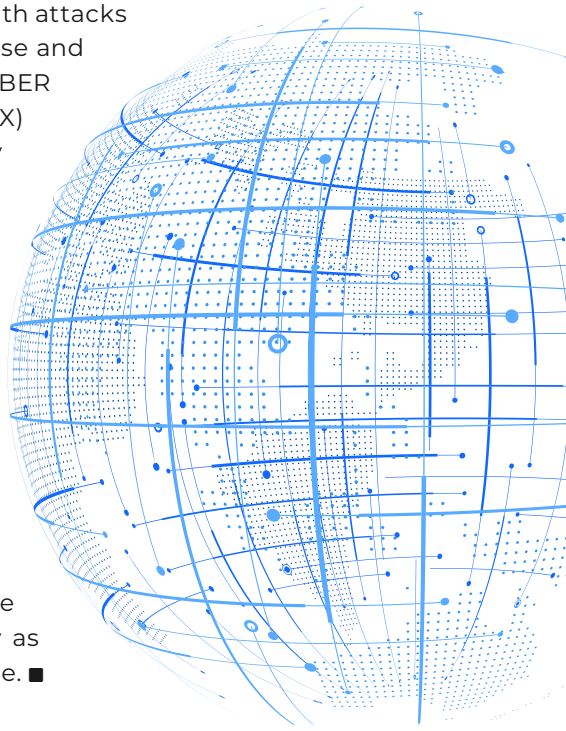
When researching the market, the Central Bank identified a number of potential vendors and consulting companies with similar capabilities. However, all of them presented one or more limitations. Firstly, none was designed to support the large-scale online delivery of the cyberdrill, beyond the access to the simulation environment. With hundreds of professional participants from nearly 40 organizations, the platform needed to provide support tools and functionalities, which were not available with any of the platforms the Central Bank reviewed.

None of the identified platforms offered the ability to integrate tabletop and operational exercises and none integrated threat emulation functionalities capable of generating the life-like attacks necessary to challenge the incident response capabilities of the participating organizations.

A couple of platforms were identified, which could simulate attacks, however their threat emulation capabilities were very limited and primarily aimed at small 20-person training classes, eventually offering no scalable solution.

CYBER RANGES Value Choice

CYBER RANGES provided the Central Bank with a turnkey solution capable of meeting all the requirements including the set-up of a large-scale simulation environment with nearly 2,000 virtual machines. Each organization was given access to a separate simulated infrastructure, with access to a range of security monitoring controls to detect attacks and intrusions. Based on the latest cyber threat intelligence, CYBER RANGES developed a lifelike threat emulation targeting the simulated environment with attacks such as phishing, ransomware, internal compromise and more. The exercise was delivered as a CYBER RANGES-powered Cross-Cyber eXercise (C2X) combining tabletop /TTX) and cybersecurity exercises (CSX).



The simulated environment further included user emulation, including browser and desktop activities, reading of e-mails and clicking on e-mail attachments. Thanks to its powerful orchestration and automation CYBER RANGES could run the Bank's large-scale event with just a handful of back-stage technical engineers and on-stage facilitators. The final report extracted from CYBER RANGES effectively informed the Central Bank's programme executive team about the baseline response capabilities across the country as well as identified both gaps and areas of excellence. ■

CASE STUDY

Higher Education

Domain	**Education**
Year	**2019**
Audience	**Academic staff and students**
Number of Users	**1,000+**
Use Cases	**· Delivery of Security Training** **· Role-based Skills Assessment** **· National CTFs** **· Delivery of tabletop exercises**

Customer Requirements

This US University was looking for a cyber range to support its teaching and learning programmes.

Specifically, the University was interested in the following features and functionalities:

- **Library of scenarios** – The university wanted security scenarios, which could be used to complement the teaching resources and to help in the directed learning activities.
- **Running CTF** – The academic staff wanted to develop and host CTF events within the university and with students from other universities.
- **Computing workspace** – The academic staff wanted to provide each student with access to computing resources on the cyber range for coursework, assignments and research work, including remote access to comply with the COVID- 19 social distancing requirements.
- **Support for BeSpoke Teaching Resources** – The Academic staff wanted to use the cyber range to develop custom teaching materials and learning resources for enrolled students.

Market Gap

When researching the market, the University mostly found two options:

1. the majority of current cyber range providers are based on public cloud and they primarily offer subscriptions to a library of scenarios to cater for the large consumer/corporate market;
2. cyber range vendors that would provide more customization capabilities would be prohibitively expensive for an academic institution as more tailored for corporate or rather military applications.

CYBER RANGES Value Choice

CYBER RANGES helped the University in many ways. Firstly, the University was able to leverage on existing computer servers, which were quickly repurposed for the installation of CYBER RANGES ON-PREM. Then, the CYBER RANGES platform delivered exactly what the university needed: each student, researcher and faculty member was allocated a quota on CYBER RANGES and could use the allocated computing resources through the Scenario Composer, accessible remotely from off-campus.

The CYBER RANGES scenario library was accessible to the students for independent and directed learning. Finally, the academic staff was happy to use the Scenario Composer to create experiential scenarios, exams, other learning materials and resources for their work. ■

CASE STUDY

Large-Scale Human Capital Development

Domain	**Government / Law Enforcement**
Year	**2021**
Audience	**SecOps / Technical and Management**
Number of Users	**10,000+**
Use Cases	**· Delivery of Security Training** **· Role-based Skills Assessment** **· National CTFs** **· Delivery of tabletop exercises**

Customer Requirements

A government entity was looking for a solution to deliver a multi-year large-scale nation-wide capacity building programme to train thousands of individuals with different job roles, skill levels and experience, in different security domains.

This government entity was looking for a solution that would meet the following requirements:

- **A Rich training content library** – The training programme was aimed at different job roles and different levels of experience, thus there was the need for a large library of training content.
- **On-Premise deployment** – The organization wanted to maintain control over the training data and wanted to run everything on premises within their network security perimeter.
- **Scalable deployment** – As the training programme would be rolled out over time, the platform would need to easily scale up to support the growing number of participants, while minimizing service disruption at the same time.
- **Web-based platform** – The platform would be web-based and allow the online delivery of the training sessions to comply with COVID-19 health management policies.
- **Instructor tools** – The platform needed to include instructor tools that would facilitate both the in-presence and virtual delivery of the training sessions.
- **Ease of use** – The platform needed to be cost-effective and easy to use to enables trainers to operate it in full autonomy and efficiency.
- **Tabletop delivery** – The platform needed to support the delivery of tabletop exercises (TTX) to a management audience.
- **Support of competency frameworks** – The platform needed to support competency frameworks and map all the assessments to such frameworks (standard, bespoke) in order to track national baseline competencies, competency gaps and areas of excellence.

CASE STUDY

Large-Scale Human Capital Development

cyberranges.com

Current Market Gap

The current market offered no solutions that would meet the organization's requirements. Some solutions would offer a good library of scenarios but they were not available on premises, or would not include instructor tools for the delivery of live training sessions. The on-premise cyber range products to avail did not feature a good level of orchestration and automation to be easily used without the heavy need for administrators or technical engineers and would not include support for tabletop exercises.

Finally, many of the available on-premise products were designed to require physical access to training venues and would not support remote delivery. The only available alternative had seemed to source different components and somehow integrate them.

This organization proved very ambitious and future-minded for what the market had to offer.

CYBER RANGES Value Choice

CYBER RANGES was installed on the Customer's existing bare-metal hardware infrastructure, leveraging system resources to avail instead of having to source new equipment thus adding costs and supply chain delays.

CYBER RANGES provided the Customer with a turnkey solution, meeting all the project hard and soft requirements. The project team was ready to roll out the training programme just one month after the handover of the entire CYBER RANGES deployment, which it took less than 2 weeks to complete. ■