CYBER RANGES
LEARN
TEAM UP
COMPETE
www.cyberranges.com

About Silensec

- ISO27001 certified by the British Standardization Institute (BSI) since 2014
- Re-certification audit in July 2020 to include CYBER RANGES product and services.

bsi.

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2013

This is to certify that: G & N Silensec LTD
G & N Court
41 Pafou Street
Limassol

Holds Certificate No:

and operates an Inform
27001:2013 for the foll

The Information Security Management System applies to the provision of the Silensec CYBER RANGES products and services, information security training and consultancy services and 24/7 SOC and managed security services including the support functions of IT, Sales, Finance and Administration in accordance with the Statement of applicability, SIL REC-008_v1.6 Date 25/06/2020.

The Information Security Management System applies to the provision of the Silensec CYBER RANGES products and services, information security training and consultancy services and 24/7 SOC and managed security services including the support functions of IT, Sales, Finance and Administration in accordance with the Statement of applicability, SIL REC-008_v1.6 Date 25/06/2020.

For and on behalf of BSI:

Andrew Launn, EMEA Systems Certification Director

Original Registration Date: 2020-07-13
Latest Revision Date: 2020-07-27

Effective Date: 2020-07-13
Expiry Date: 2023-07-04

Page: 1 of 2

...making excellence a habit.™

silensec™
ISO27001 Certified

Limassol (CY) - HQ
Sheffield (UK)
Nairobi (KE)

Services

- Security Audit and Compliance
- Security Systems Integration
- 24x7 SOC
- Managed Security
- Security Training

About us

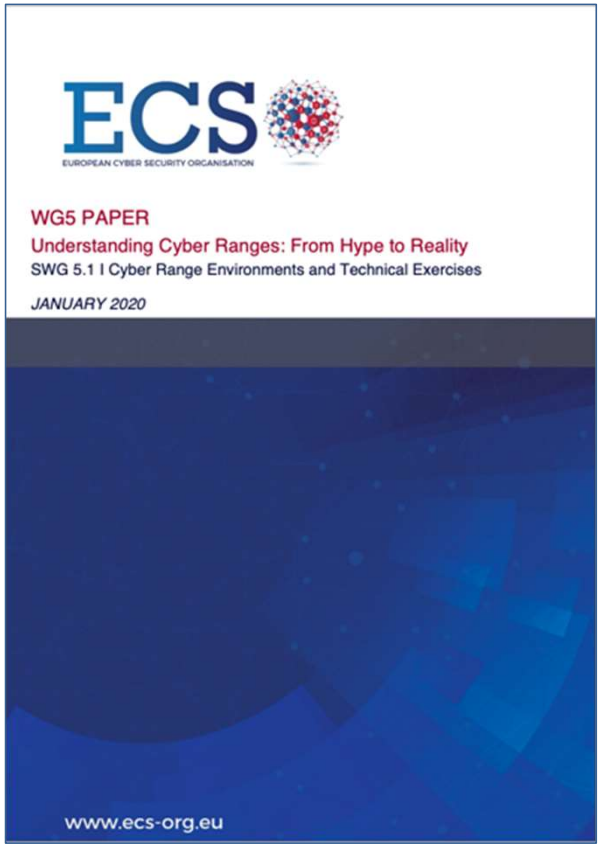
- Est. in May 2006 in Sheffield
- Privately owned
- 55 people ... *and growing*

Leadership in Cyber Range Domain

CYBER RANGES

Leading the WG 5 of European Cyber Security Organisation (ECSO), and also specifically on Cyber Ranges SWG 5.1 and Education & Training SWG 5.2

Editor and main author of the **ECSO Paper on Cyber Ranges** (rel. on 30-Mar-2020)

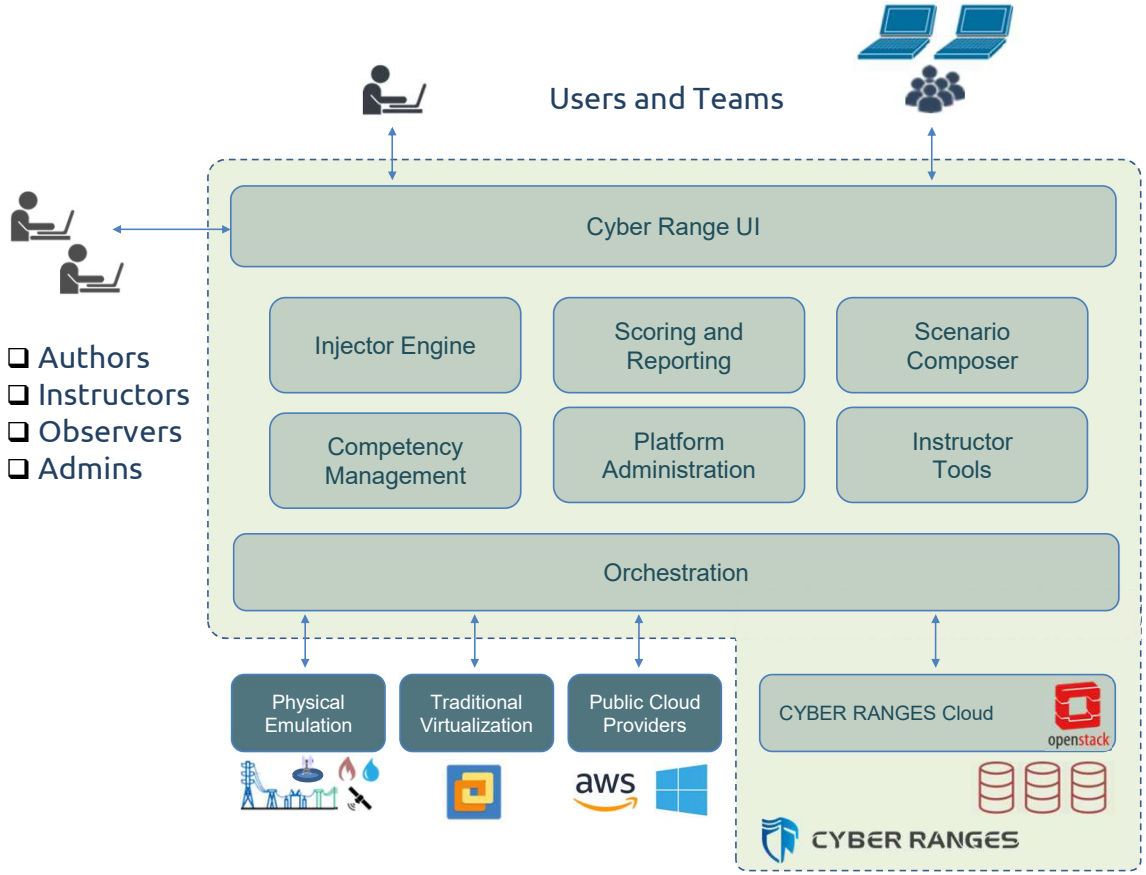


Official platform being used by the UN for the organization of regional and national cyber drills since 2017 – powered up the **ITU 2020 Global Cyber Drill** with 213 participants (58 countries)

Awarded several EU research grants related to cyber ran[illegible] their application

COMPACT INFRA STRESS ENSURESEC

Next-generation Architecture



CYBER RANGES

NEXT-GENERATION CYBER RANGE

- Full Stack Technology on bare-metal servers
- Fully owned IPR
- Flexible deployment options
- Powerful orchestration
- Scenario composition
- Library of Scenarios, attacks and assessments
- Library of infrastructure assets and integration of 3rd party technologies
- Attack and user traffic simulation
- Multi-user events automation
- Multiple user roles

Deployment Options

Cyber Range as a Service

Hosted

On Premise

Portable

CYBER SPACE, ENGAGED.

CYBER RANGES

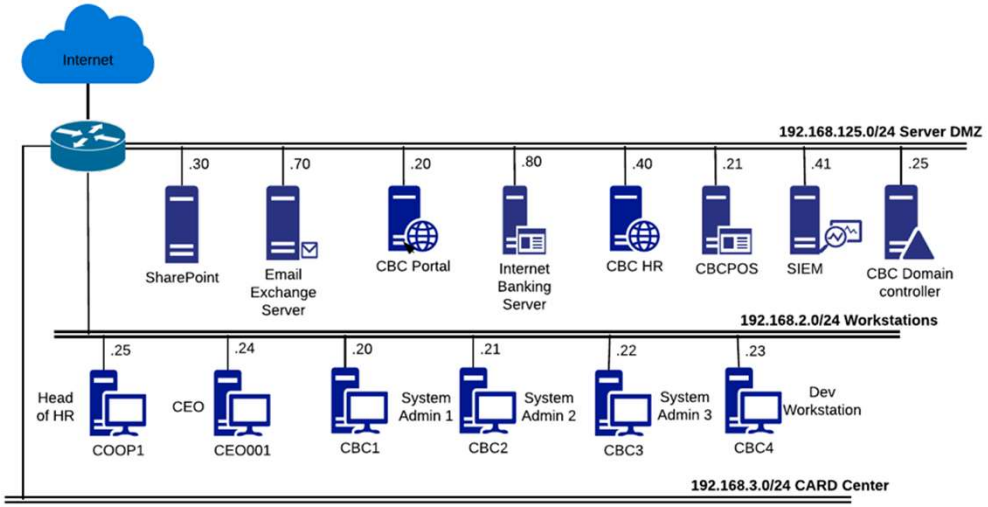
CYBER RANGES PORTABLE

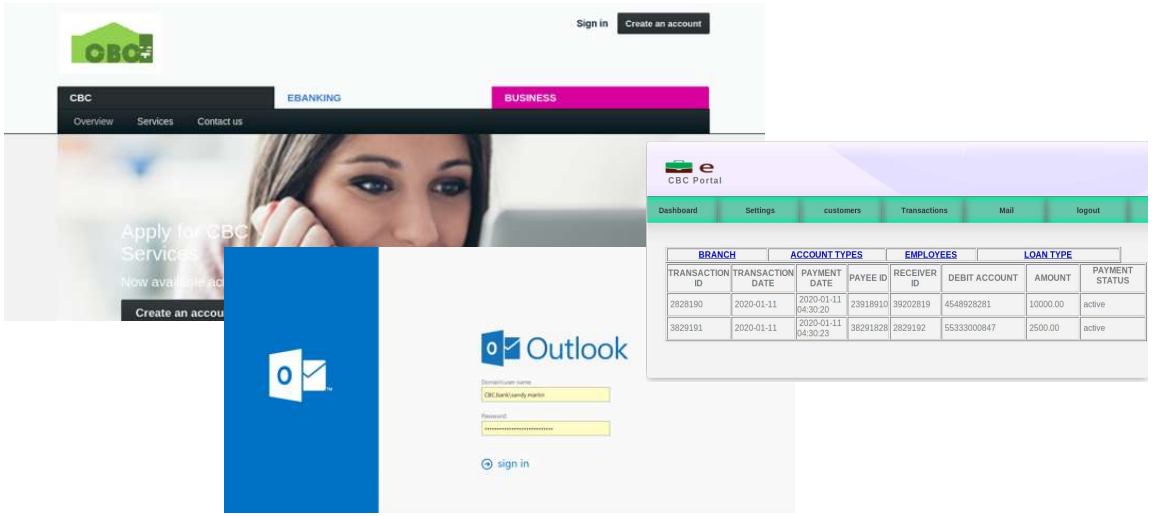
- Pelican case, ruggedized carry-on
- Five-minute deployment
- 3 x Custom Laptops with CYBER RANGES Installed
- 1 x Wireless Access Point with Internet access module
- 1 x Network Switch and cabling
- Injector Engine for user traffic and attacks simulation
- Library of pre-loaded CYBER RANGES Scenarios

CYBER RANGES

CYBER RANGES
Functionalities at Glance

Library of Scenarios

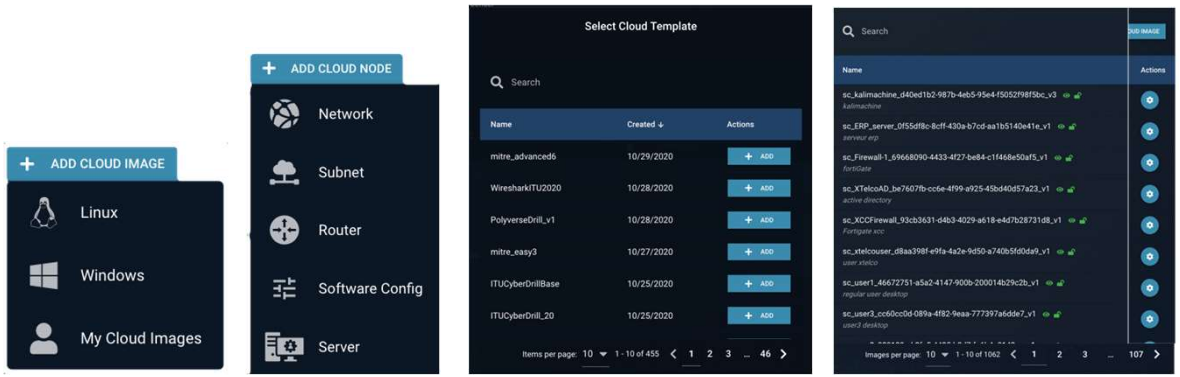




CYBER RANGES

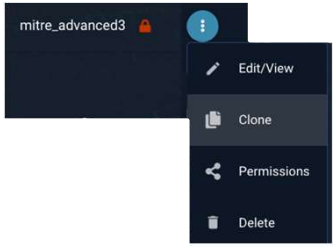
- Learning Paths
  - ❑ SOC Analyst
  - ❑ System administration
  - ❑ Penetration testing
  - ❑ Malware analysis
  - ❑ … and many more
- Corporate Scenarios
  - ❑ Red Team
  - ❑ Red vs Blue Team
  - ❑ Incident Response
- MITRE ATT&CK Scenarios
  - ❑ Multiple attack techniques
  - ❑ Multiple CVEs

Scenario Composition



Build multi-segment Networks From Scratch

Reusable Library of VMs and Simulation Environments



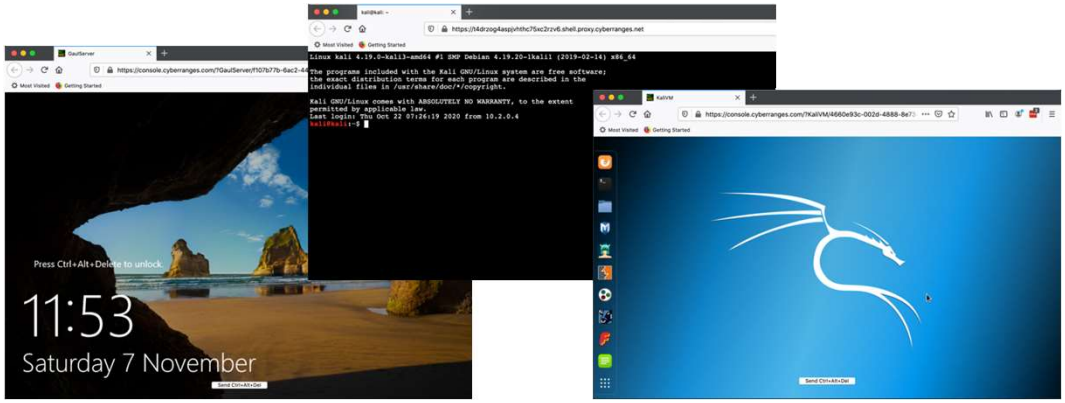
One-Click Cloning and Repurposing of Any Scenario

Full ACL Support for Authors Collaboration

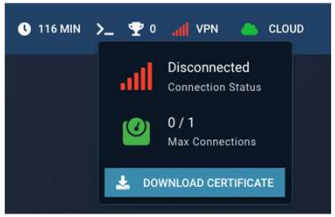
CYBER RANGES

- Library of Content
  - ❑ Virtual Machines
  - ❑ Simulation Environments
  - ❑ Assessments
- Scenario Repurposing
  - ❑ Cloning of Scenarios
  - ❑ Cloning of simulation environments
- Full ACL Support
  - ❑ Scenarios
  - ❑ Simulation Infrastructures

Usability



In-Browser Access to the Simulation Environment



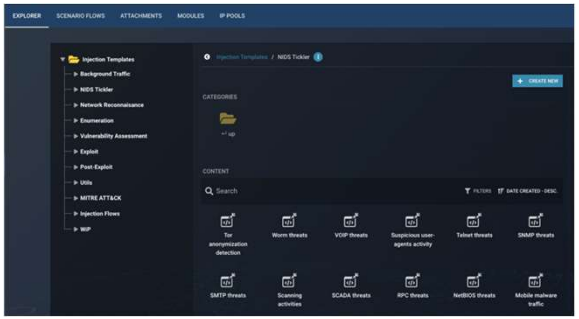
Access via VPN for
for
BYOD Engagements

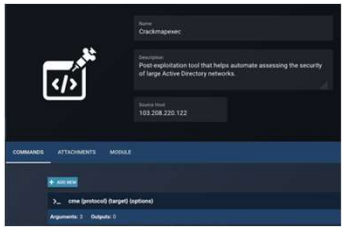
Individual access
to the VMs

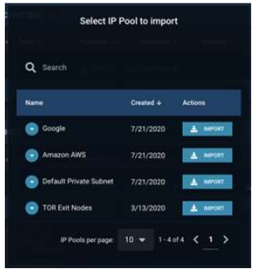
CYBER RANGES

- Per-VM Access Modes
  - ❑ VPN
  - ❑ Web Shell
  - ❑ Remote Console
  - ❑ Web Proxy
- Individual Access to VMs
  - ❑ Restart
  - ❑ Reset

User Traffic & Attack Simulation

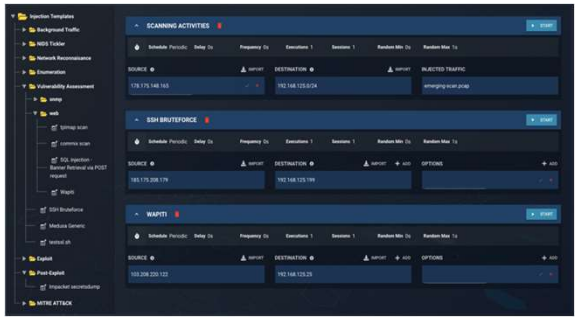


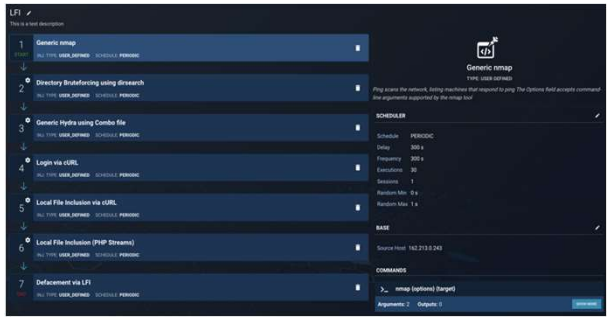




Configurable Attack Library

Configurable IP Address Pools





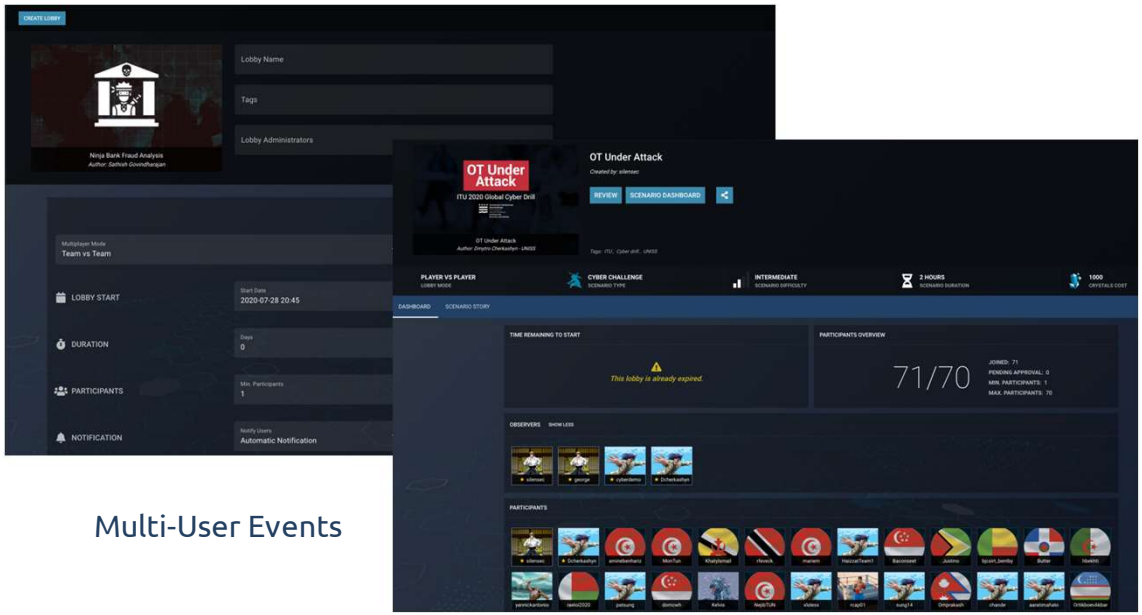
Configurable Live Injections

Per-Scenario Attack Flows

CYBER RANGES

- Agent-based attack and user traffic simulation engine
- Background Traffic Simulation
- Stateful attack injection
- Simulation of false-positive attacks
- Red Team Automation
- Configurable Attack Library
- Live injections during scenarios
- Configurable IP Address Pools
- Automatic orchestration of attacks

Orchestration



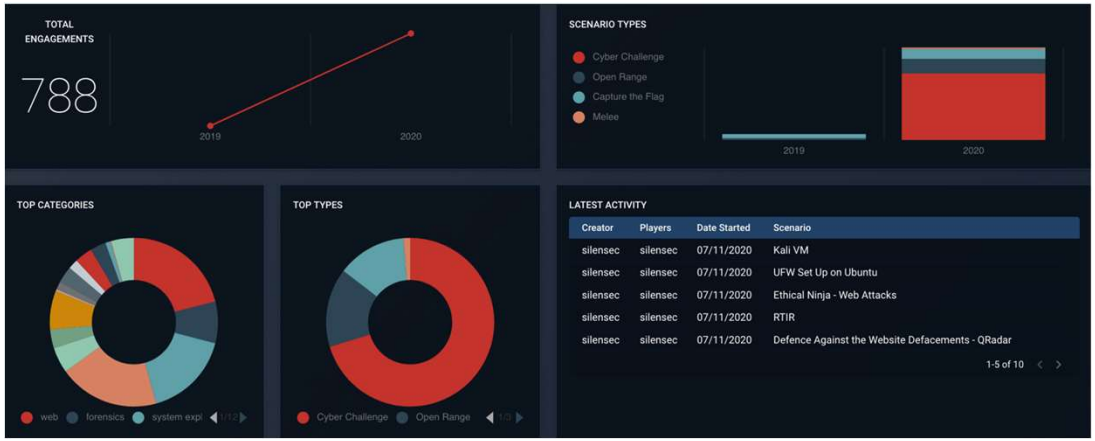
Multi-User Events

Events Calendar

CYBER RANGES

- One Click to Create Multi-User Events
  - ❑ Multiple isolated networks or Shared networks
  - ❑ Automatic orchestration of attack simulation
- Numerous Applications
  - ❑ Red vs. Blue teams exercises
  - ❑ Security Training
  - ❑ Competence Assessment
  - ❑ Staff Recruitment
- Events Calendars
- Invite Users to Join Events

Reporting



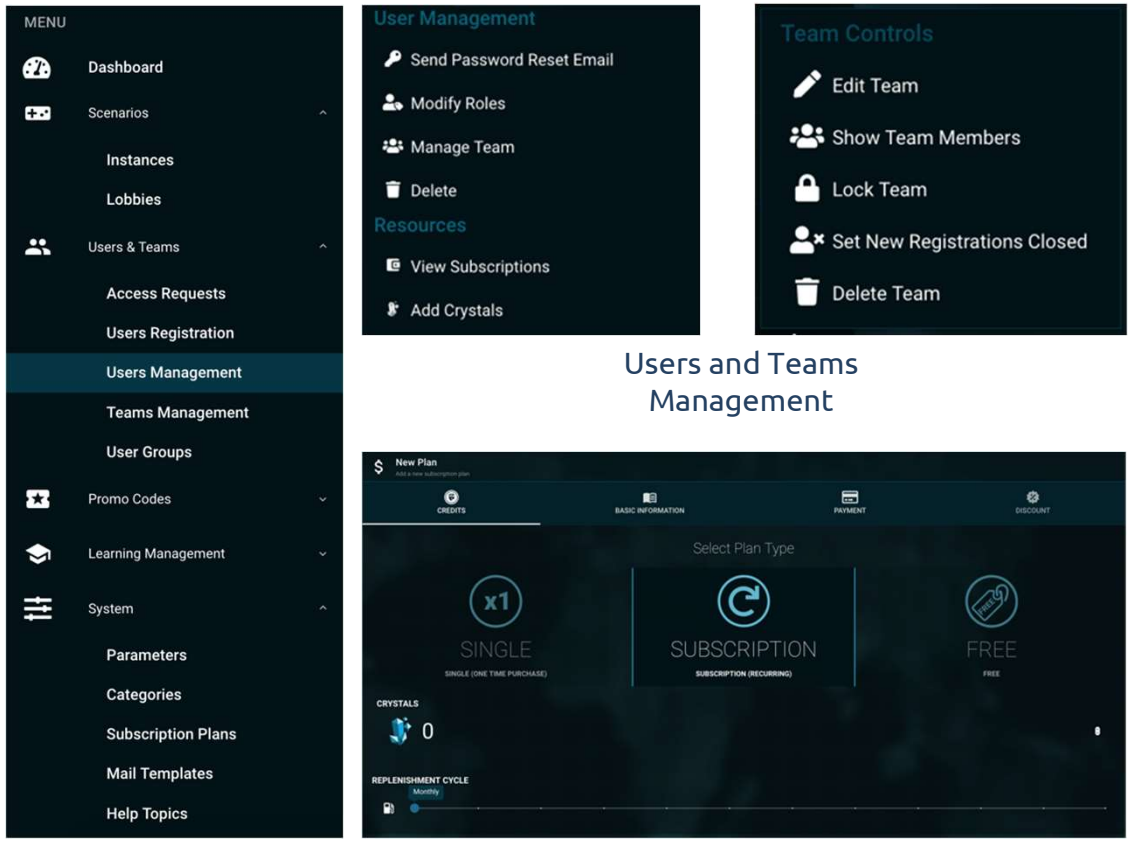
Organizational View

Tracking User/s Progression

CYBER RANGES

- Manage Organizations
  - ❑ Manage teams and staff
  - ❑ Assign users to scenarios
- Track User/s Progression
  - ❑ Engagement
  - ❑ Competency areas
- xAPI Compliance
  - ❑ Integrate with third-party LMS

Administration and MSSP



Users and Teams Management

CYBER RANGES

- CYBER RANGES Administration
  - ❑ Manage Scenarios and Events
  - ❑ Manage Users and Teams
  - ❑ Manage Permissions
  - ❑ Manage Competency Frameworks
- MSSP Functionalities
  - ❑ Manage Subscription Plans
  - ❑ Issue Promo Codes
  - ❑ Create and Manage Organizations

Why CYBER RANGES by Silensec

- Leading the Cyber Range Technology Innovation
- Delivered also on-premise, built to scale

- Start using CYBER RANGES for security training and continue using it for:

  - competence-based recruitment
  - development of cyber capabilities
  - profiling skills at national level
  - improving cyber resilience
  - proof of concept, product testing

  … and much more

CYBER SPACE, ENGAGED.