Using Gamification for Cyber Exercises and Security Competence Building

Almerindo Graziano
CEO, Silensec
al@silensec.com

ITU Cyberdrill, 4-5 Oct 2018
Grand-Bassam, Côte d'Ivoire

silensec™ iso27001 Certified

About Silensec

- Information Security Management Consultancy Company (ISO27001 Certified)
  - Security compliance, Security Audits
  - Security System Integration (SIEM, DAMs, WAFs, etc.)
  - Managed Security Services
- Independent Security training provider

About Me

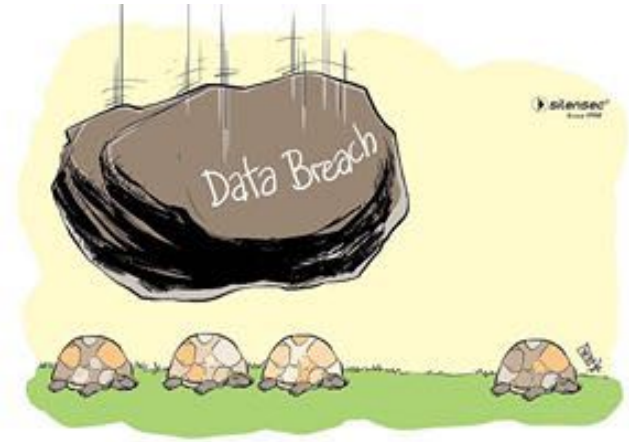
Almerindo Graziano

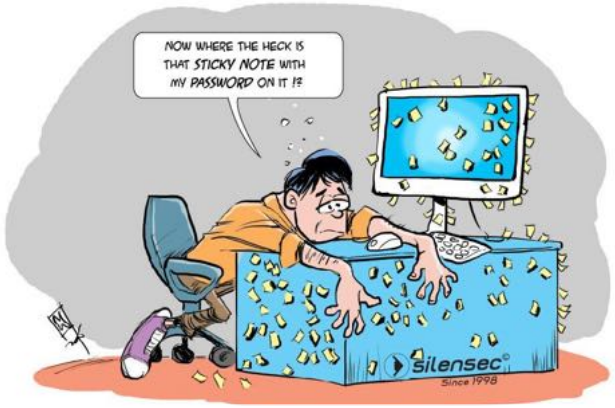
- CEO of Silensec
- PhD in mobile computer security from the University of Naples, Italy.
- Founder and course Leader for the MSc in Information Systems Security at Sheffield Hallam University
- Author of numerous security training courses
- Cyber security expert for International Telecommunication Union (ITU)
- Airmiles collector

silensec™ iso27001 Certified

Silensec on Social Media

Free Security Awareness Resources





Follows us on our social media channels for regular security cartoons, editorials and weekly newsletter

Silensec Silensec @Silensec Silensec @Silensec

ITU Cyberdrill, 4-5 Oct 2018
Grand-Bassam, Côte d'Ivoire

silensec™ ISO27001 Certified

The Security Skills Gap

The Size of The Problem

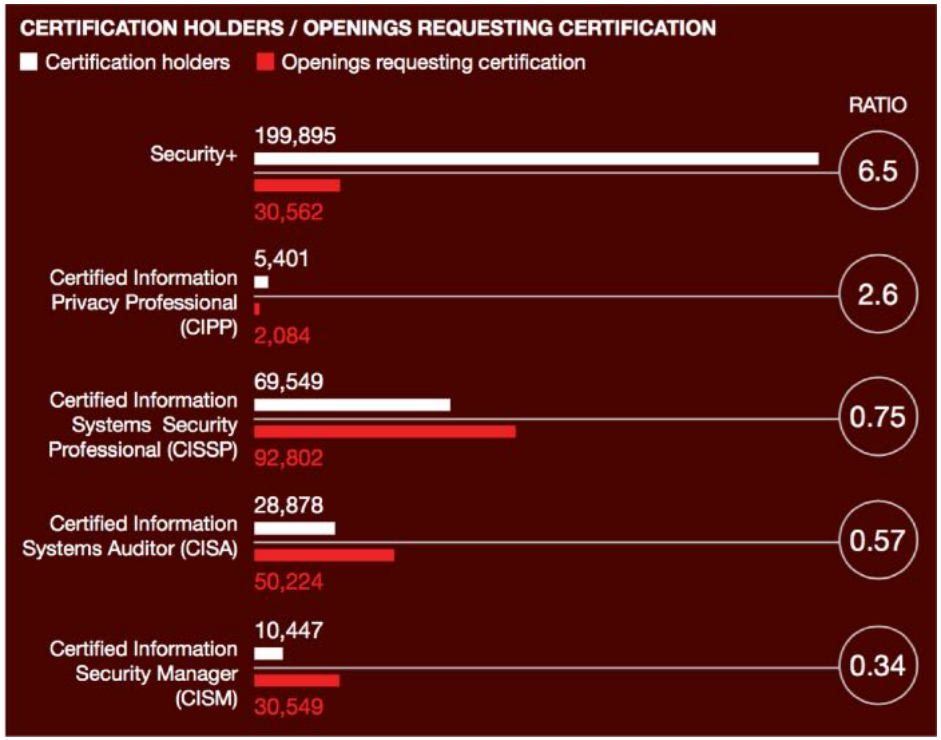
At least 3.5 million cyber security jobs will be left vacant by 2021

1 in 5 organization receives fewer than 5 candidates for each advertised security position and 37% of the organisations lament that fewer than 1 in 4 of the candidates they do receive are actually qualified for the job!

silensec™ ISO27001 Certified

The Security Skills Gap

Lack of Certified Professionals



The security job market has big gaps with regards to security certifications

The cost of training and certificaition is one of the underlying causes of the cybersecurity skills gap

silensec™ ISO27001 Certified

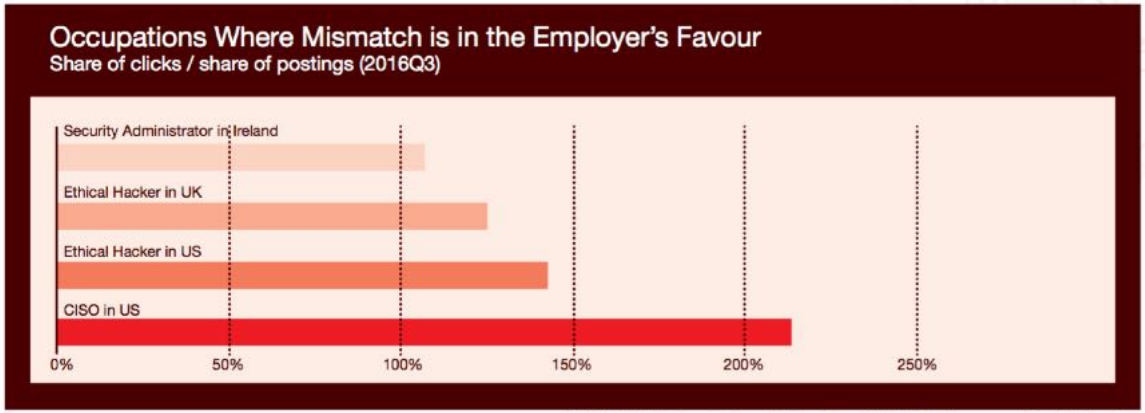
High-value skills in critically short supply

- Intrusion detection
- Secure software development
- Attack mitigation

ITU Cyberdrill, 4-5 Oct 2018
Grand-Bassam, Côte d'Ivoire

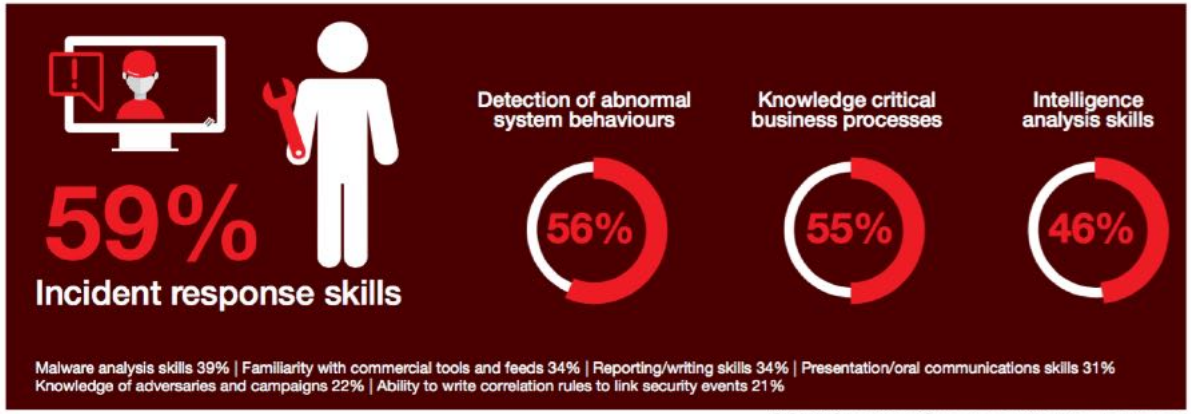
The Security Skills Gap

The Gap Between Offer And Demand



SOURCE: Indeed Spotlight: The Global Cybersecurity Skills Gap

"Other desired skills include malware analysis skills, familiarity with commercial tools and feeds, knowledge of adversaries campaigns and the ability to write correlation rules to link security events.



SOURCE: 2017 Cybersecurity Trends Report

silensec™ ISO27001 Certified

The Challenges

Companies Do Not Invest Enough In Staff Training

- Companies prefer to invest in systems rather than competences
- ROI on security spending alone is difficult to justify
- Companies fear staff may leave once trained
- Training costs money, period!

> after salary, opportunities for training are the second highest motivating factor in recruitment and staff retention followed by the reputation of the employer's IT department and potential for advancement.

silensec™ iso27001 Certified

The Market Solution

The Commoditization of Security Training

Certified Ethical Hacking Training Course

CompTIA Security+ Training

Using Python For Offensive Pentesting

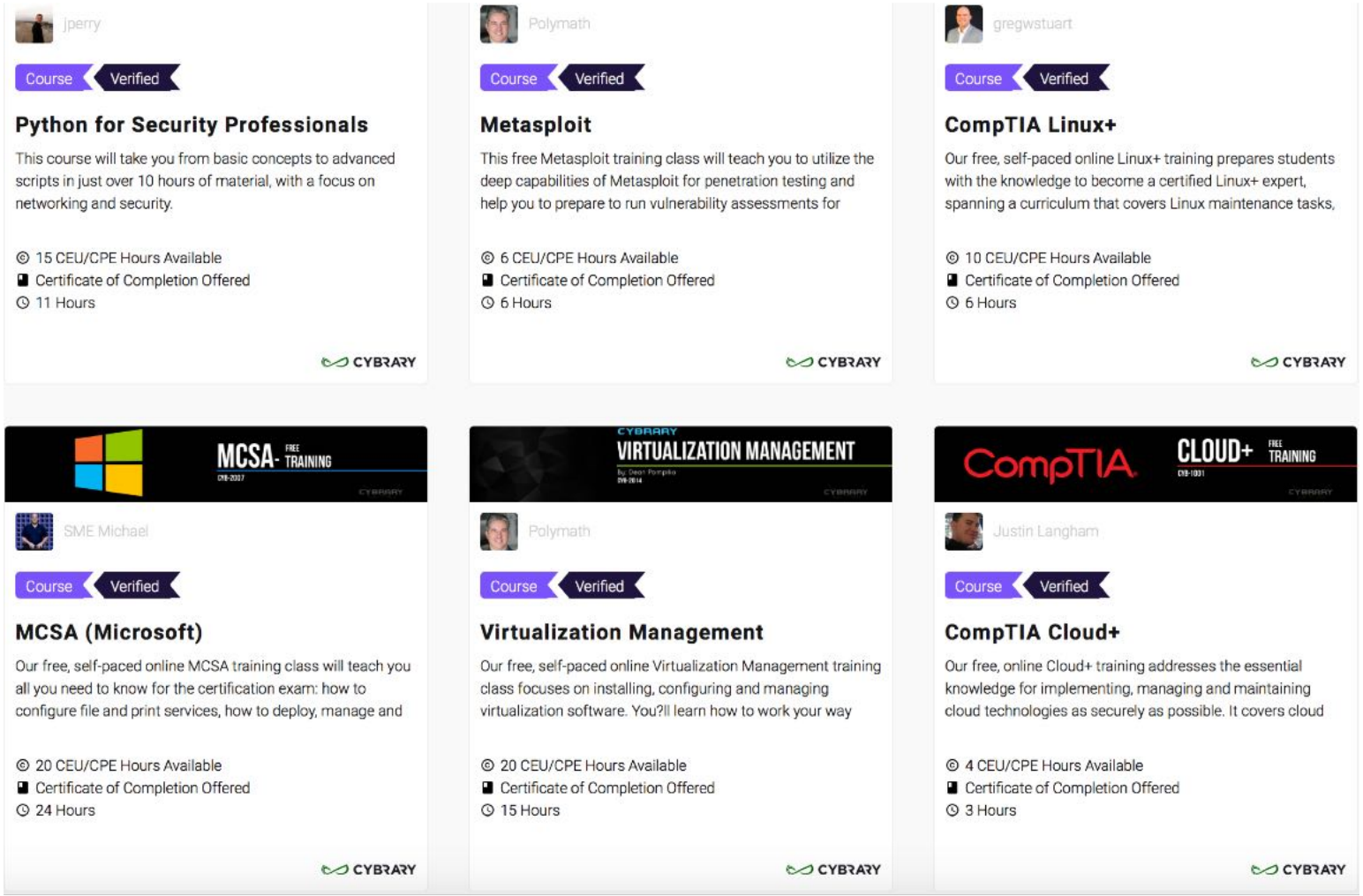
Learn WiFi Hacking & Pentesting

Hacking Android Using Kali Linux

Certified Information Systems Security Professional CISSP

The Market Solution

Welcome to Cybrary, Where Every Training is Free!



ITU Cyberdrill, 4-5 Oct 2018
Grand-Bassam, Côte d'Ivoire

silensec™ ISO27001 Certified

After All..

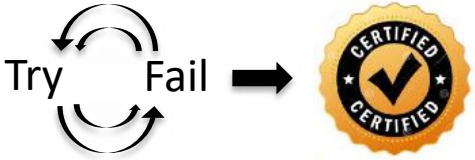
Welcome To Google University – Free Admission Daily

silensec™ ISO27001 Certified

What is Really Happening?

The True Cost of Commoditization

Which certification? Which training? Where can I practice?...



Emphasis is put on the achievement and not in the acquisition of competences

Paper Certifications and Certificates of Completion!

Finding the right security professional gets harder

silensec™
iso27001 Certified

Security Gamification

Gamification Principles

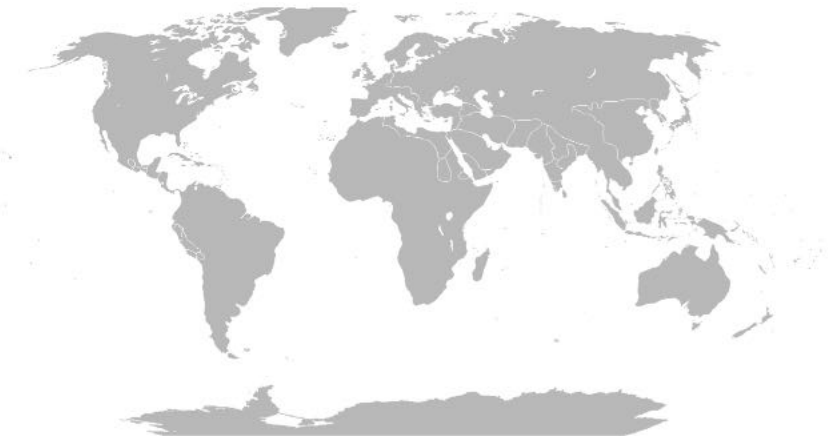
- Gameplay
- Re-playability
- Co-operation/competition between players
- Allegion
- Graphics power
- Artistic and sound aspects
- Plot

silensec™ iso27001 Certified

ITU Cyberdrills Experience

Sample Activities

- Development of Cyberdrill workshops and training for Computer Emergency Response Teams
- Events run by the International Communication Union (ITU) worldwide



Past Cyberdrills

- Zambia
- Egypt
- Montenegro
- Mauritius
- Tunisia
- Ecuador
- Oman
- Qatar
- Suriname
- Tanzania
- Moldova
- Argentina

ITU Cyberdrill, 4-5 Oct 2018
Grand-Bassam, Côte d'Ivoire

Cyber Exercise

Example

- Log Analysis and Incident Response
- Computer/Mobile forensics
- Cyber Threat Intelligence
- Ethical Hacking
- Table-top exercises

silensec™ ISO27001 Certified

Cyber Ranges

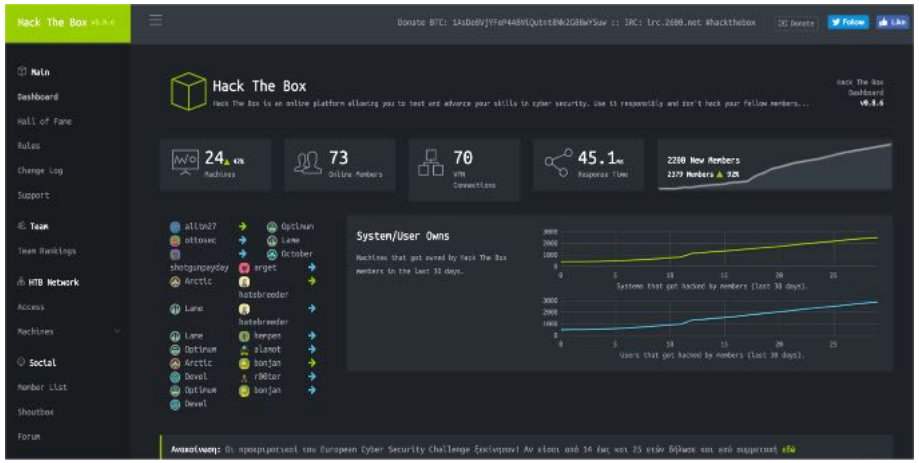
Definition

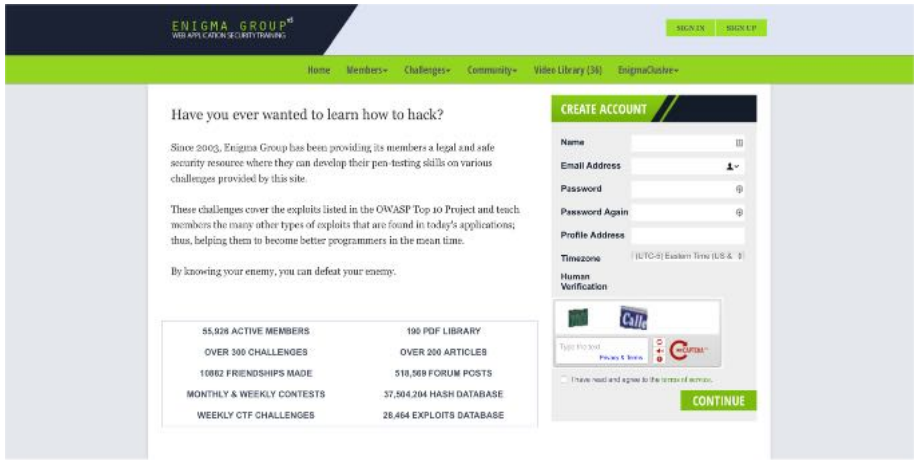
> An interactive, simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment. National Initiative for Cyber security education (NIST)

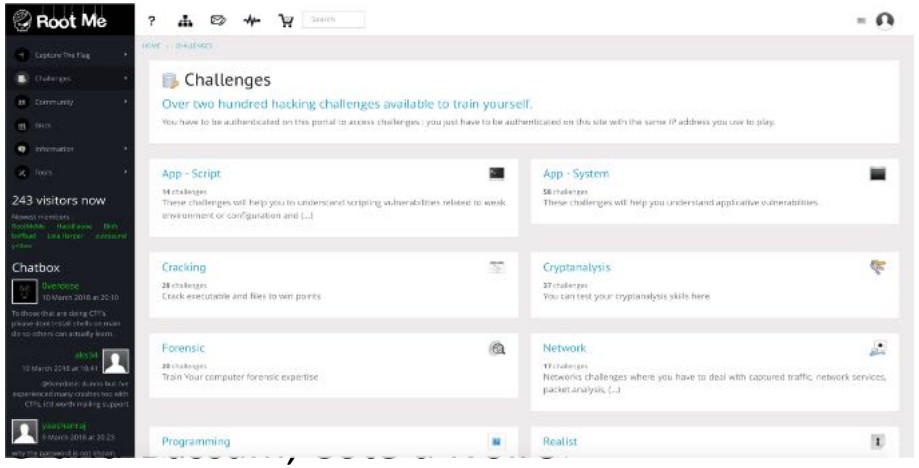
silensec™ ISO27001 Certified

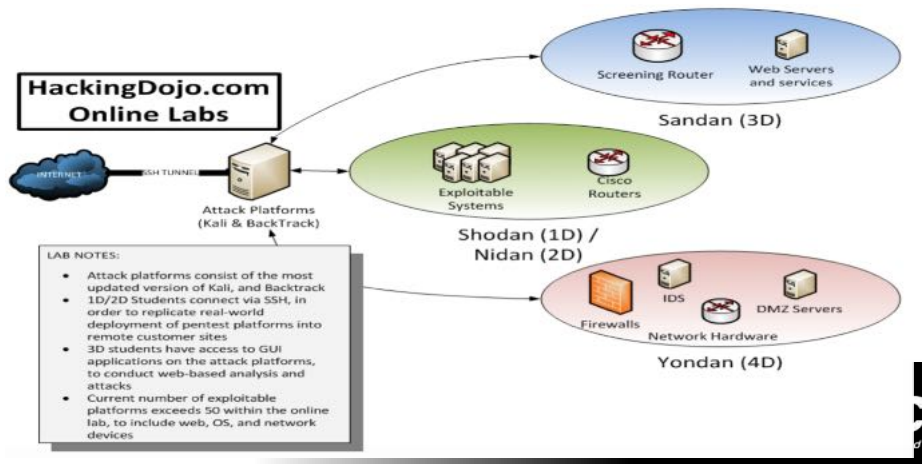
CTF2013
THEGAME THERULES THESCORE THEPRIZE THEBLOG
Teams
My Team
My Fortress
IRC
All Teams
Fortress
You are using 1 of 99 servers
Server State Statistics Actions
test22 (ACTIVE, RUNNING) Soon
New Server

HACKTHIS!!
THE HACKERS PLAYGROUND
Want to learn about hacking and network security? Discover how hacks, dumps and defacements are performed and secure your website against hackers with HackThis!!
Challenges
Community
Articles
Login
Register
Featured articles
Website Security
Blind SQL Injection
One-Time Pad
Steganography & encryption
How to hide messages in audio files


Hack The Box
Hack The Box
24 Machines
73 Online Members
70 VPN Connections
45.1ms Response Time
2288 New Members
2379 Members
System/User Owns
Machines that got owned by Hack The Box members in the Last 30 days.
Systems that got hacked by members (last 30 days).
Users that got hacked by members (last 30 days).


ENIGMA GROUP
WEB APPLICATION SECURITY TRAINING
Home Members Challenges Community Video Library (36) EnigmaClusive
Have you ever wanted to learn how to hack?
Since 2003, Enigma Group has been providing its members a legal and safe security resource where they can develop their pen-testing skills on various challenges provided by this site.
These challenges cover the exploits listed in the OWASP Top 10 Project and teach members the many other types of exploits that are found in today's applications; thus, helping them to become better programmers in the mean time.
By knowing your enemy, you can defeat your enemy.
55,928 ACTIVE MEMBERS
OVER 300 CHALLENGES
10862 FRIENDSHIPS MADE
MONTHLY & WEEKLY CONTESTS
WEEKLY CTF CHALLENGES
100 PDF LIBRARY
OVER 200 ARTICLES
518,569 FORUM POSTS
37,504,204 HASH DATABASE
28,464 EXPLOITS DATABASE
CREATE ACCOUNT
Name
Email Address
Password
Password Again
Profile Address
Timezone
Human Verification
CONTINUE


Root Me
Challenges
Over two hundred hacking challenges available to train yourself.
App - Script
App - System
Cracking
Cryptanalysis
Forensic
Network
Programming
Realist
243 visitors now
Chatbox


HackingDojo.com
Online Labs
INTERNET
SSH TUNNEL
Attack Platforms
(Kali & BackTrack)
Screening Router
Web Servers and services
Sandan (3D)
Exploitable Systems
Cisco Routers
Shodan (1D) / Nidan (2D)
IDS
DMZ Servers
Firewalls
Network Hardware
Yondan (4D)
LAB NOTES:
Attack platforms consist of the most updated version of Kali, and Backtrack
1D/2D Students connect via SSH, in order to replicate real-world deployment of pentest platforms into remote customer sites
3D students have access to GUI applications on the attack platforms, to conduct web-based analysis and attacks
Current number of exploitable platforms exceeds 50 within the online lab, to include web, OS, and network devices

Silensec Cyber Range

Specifications

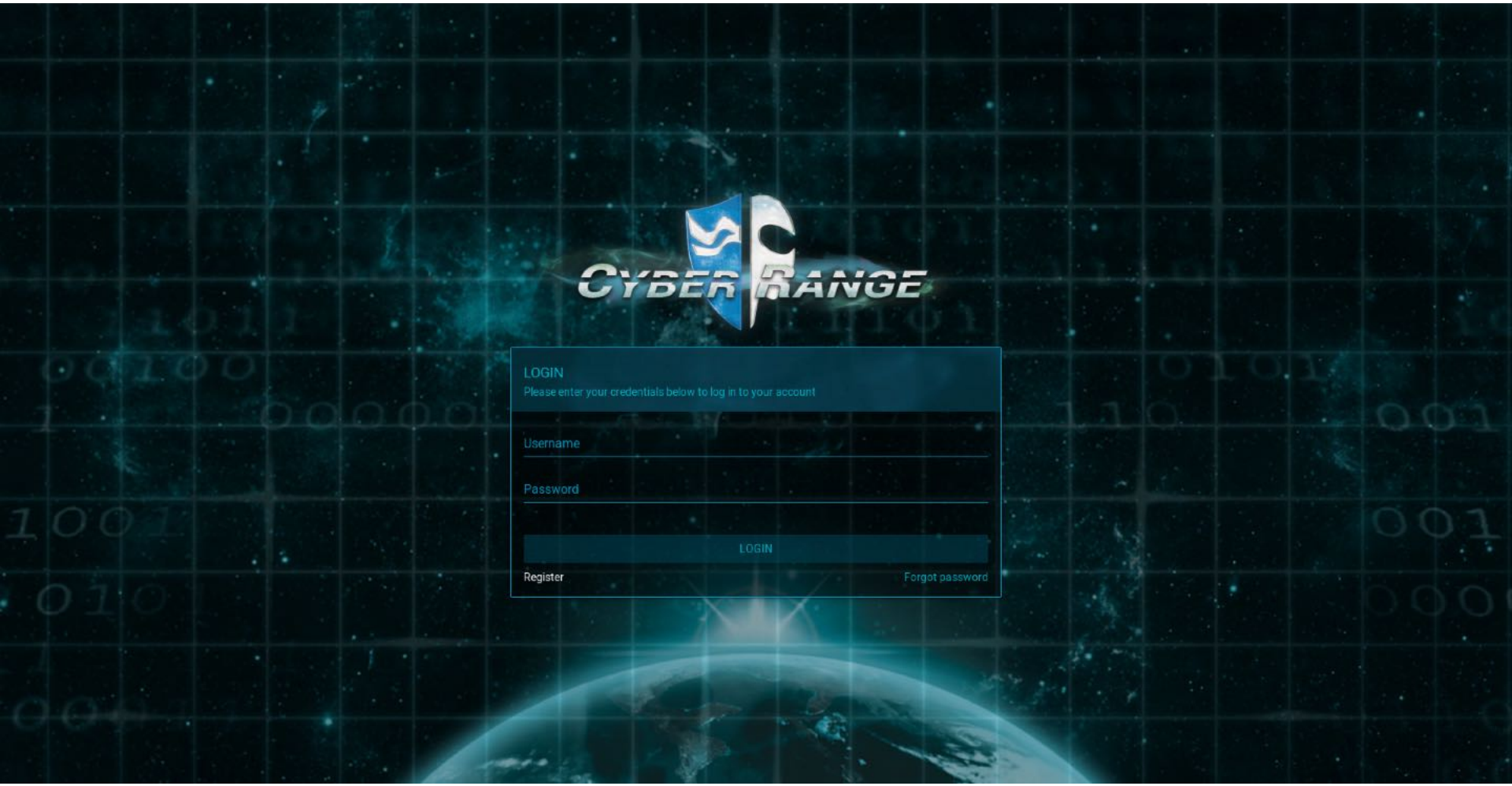
- Portable cyber range
  - 192GB Ram
  - 24 CPU cores
  - 6TB storage)
- Online cyber range
  - Scalabale to thousands of simultaneous users

www.cyberranges.com

ITU Cyberdrill, 4-5 Oct 2018
Grand-Bassam, Côte d'Ivoire

silensec™ iso27001 Certified

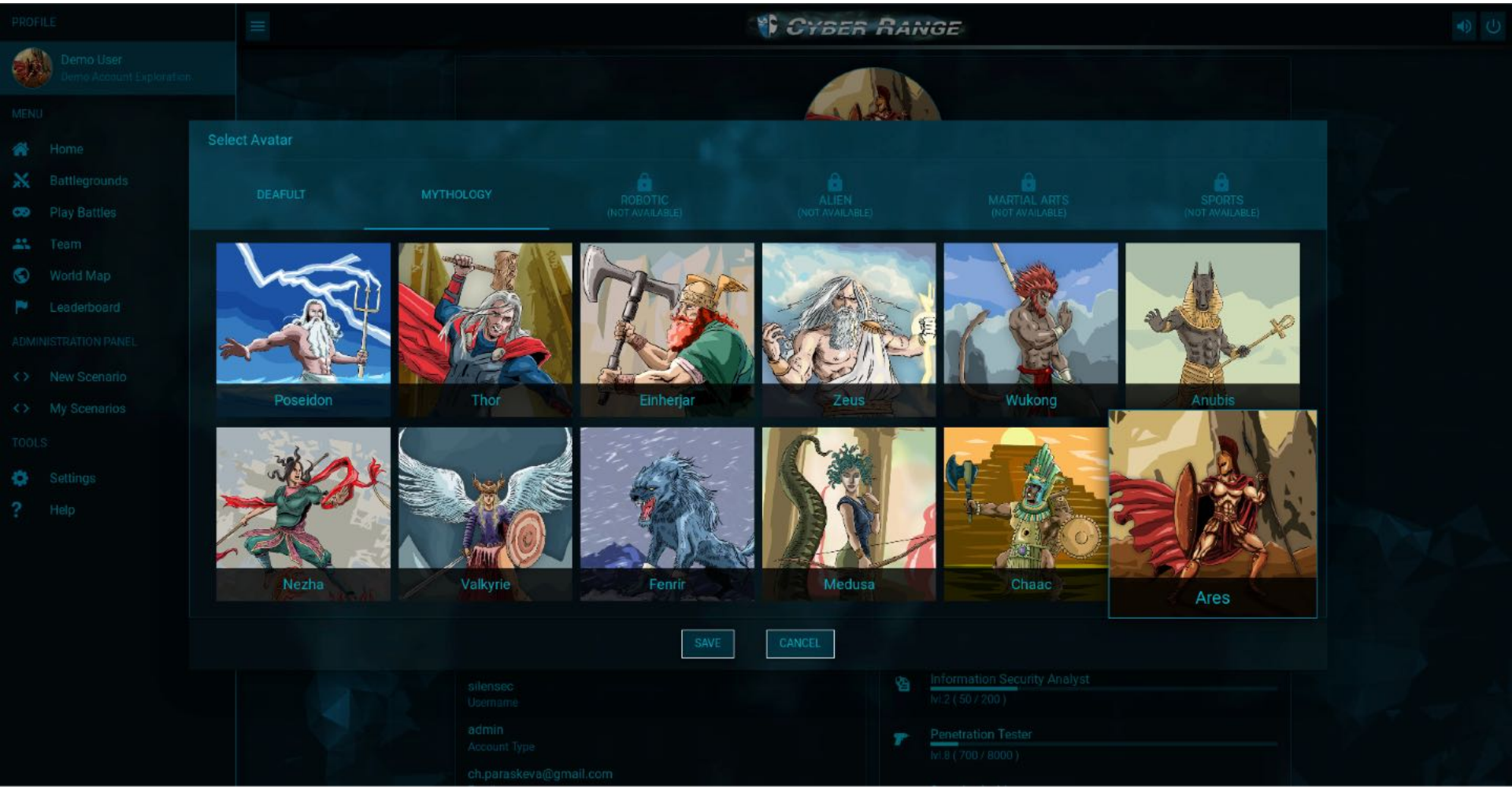
Silensec Cyber Range



ITU Cyberdrill, 4-5 Oct 2018
Grand-Bassam, Côte d'Ivoire

silensec™ iso27001 Certified

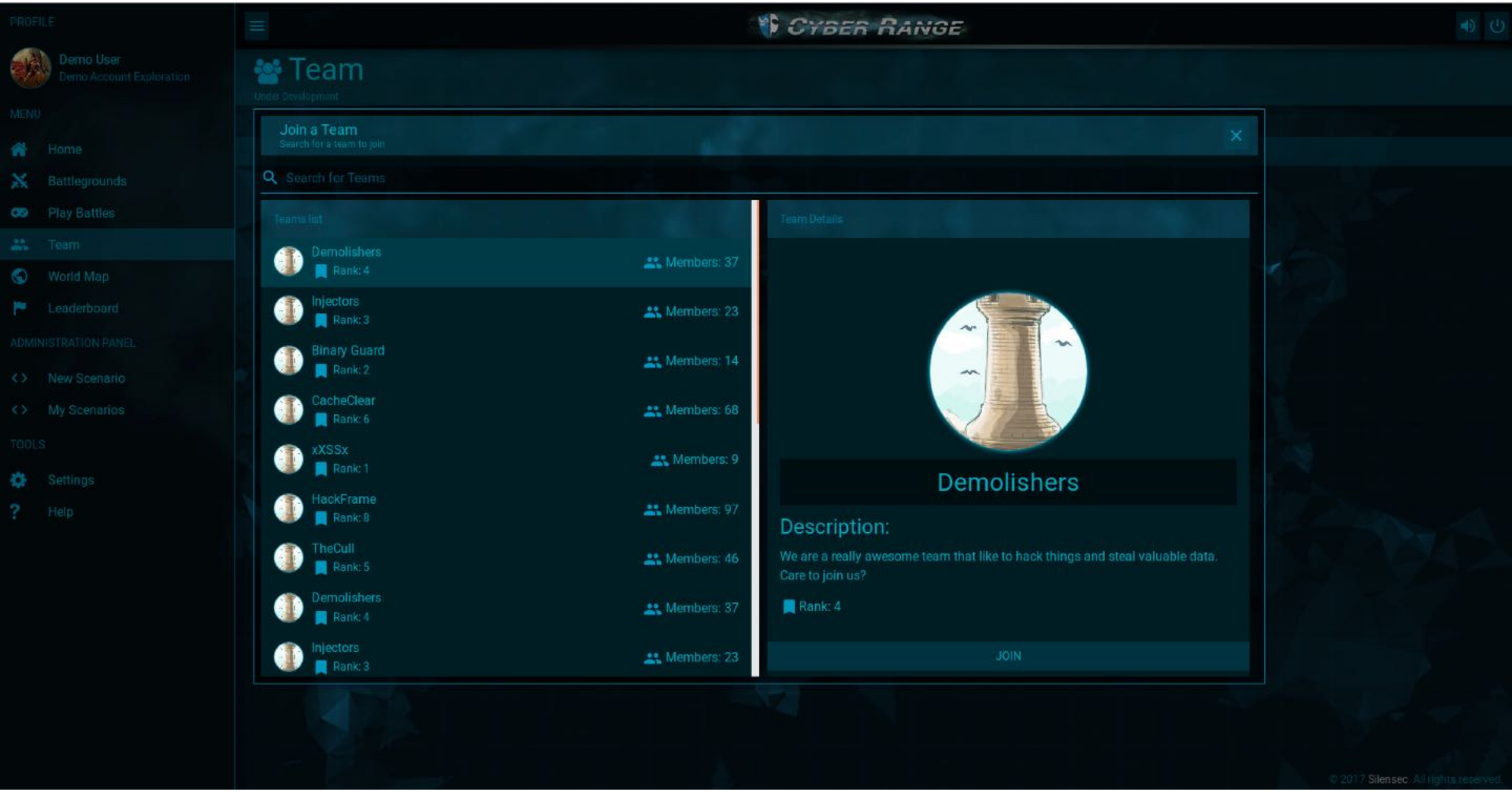
Online Persona



ITU Cyberdrill, 4-5 Oct 2018
Grand-Bassam, Côte d'Ivoire

silensec™ iso27001 Certified

Join a Team



ITU Cyberdrill, 4-5 Oct 2018
Grand-Bassam, Côte d'Ivoire

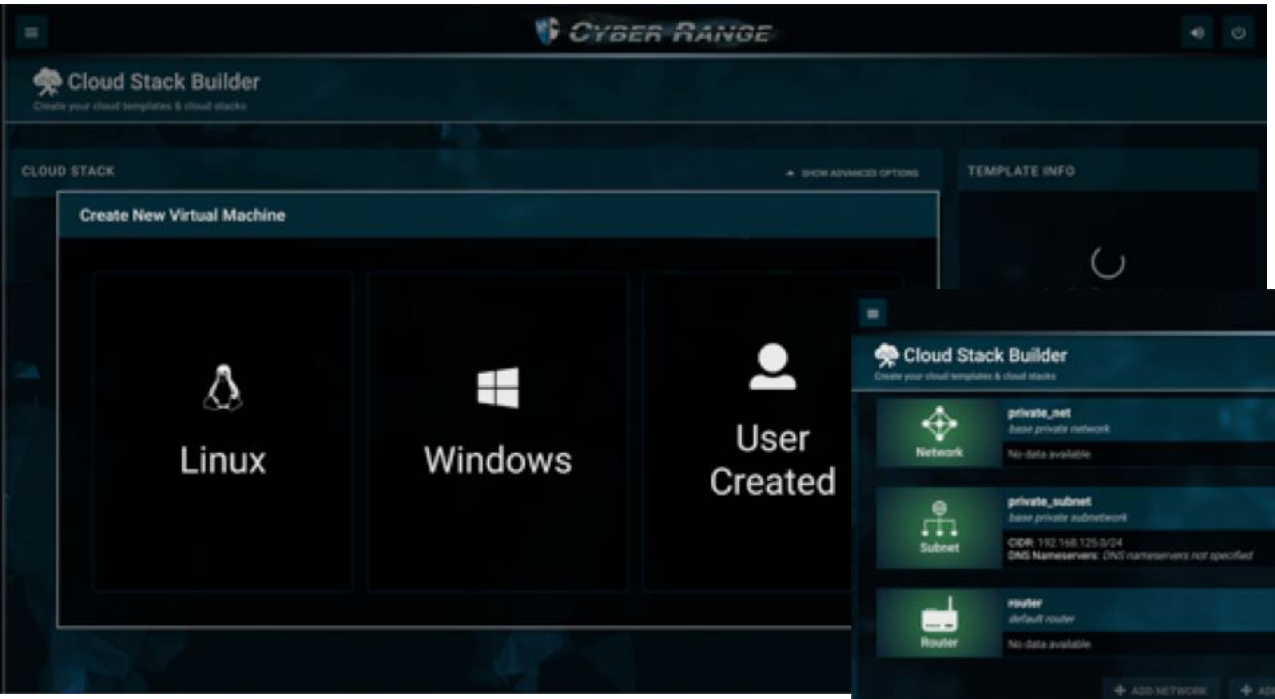
silensec™ iso27001 Certified

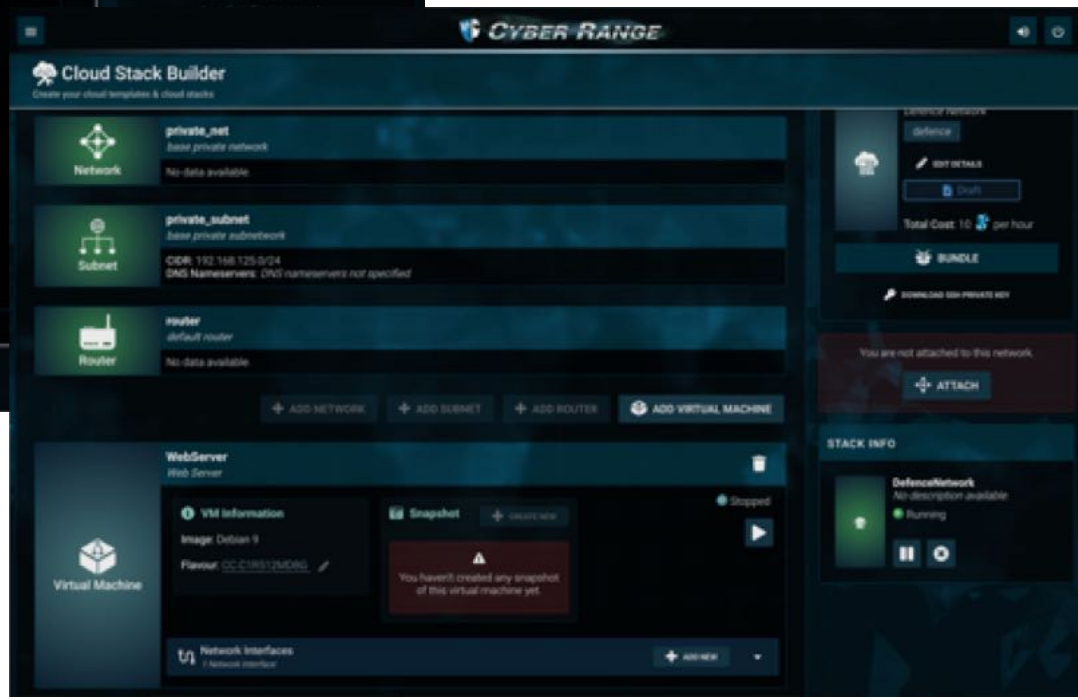
Cooperation

Game Mode

PROFILE
Demo User
Demo Account Exploration
MENU
Home
Battlegrounds
Play Battles
Team
World Map
Leaderboard
ADMINISTRATION PANEL
New Scenario
My Scenarios
TOOLS
Settings
Help
CYBER RANGE
Scenarios
Search and select a scenario to start a battle
Select Battle Mode
Select Battle Mode
Select Battle Type
Select Scenario
Single Player
Play versus virtual machines or AI
Multiplayer
Play versus or co-op with other players against virtual machines and AI
BACK
NEXT
© 2017 Silensec. All rights reserved.

Creating the Game/Scenario





ITU Cyberdrill, 4-5 Oct 2018
Grand-Bassam, Côte d'Ivoire

silensec™ ISO27001 Certified

Starting The Game

ITU Cyberdrill, 4-5 Oct 2018
Grand-Bassam, Côte d'Ivoire

silensec™ ISO27001 Certified

Scoring

silensec™ iso27001 Certified

Cyber Range Use Today

National Cybersecurity Competitions – www.cyberstars.pro

Arab Regional Cyberstars Threat Hunter Edition

ITU Cyberdrill, 4-5 Oct 2018
Grand-Bassam, Côte d'Ivoire

silensec™ iso27001 Certified

Thank you