CYBERANGE SMART CITY SIMULATION
Learning cyber security on real world scenarios

About ISAC

The logo of ISAC is a form of an abstract watchful eye with a dot that represents Individual, Information, Intelligence and India.

Information Sharing and Analysis Center (ISAC) is a non-profit organization dedicated to information sharing, awareness, capacity building and analysis for critical sectors in cyber space.
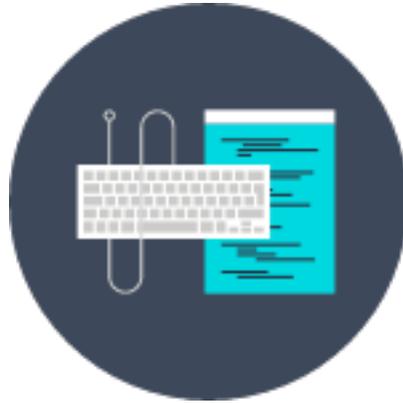
What is Cyberange?

Cyberange is a scaled model of the real world. Organizations can be simulated to better understand the state of cyber security.

Watch Cyberange Promo Video

How is Cyberange designed?

An industry/organization is thoroughly researched and scaled model is constructed by bringing field experts.

How Real is Cyberange?

Care is taken to accurately deploy real world software's and hardware where applicable and possible.

Real SCADA / ICS technologies are used to control Cyberange

The vulnerable software reflect real world deployments!

How can we use Cyberange?

- Cyber Range allows you to practice latest attack vectors by using special virtual machines that are intentionally designed with vulnerabilities and technical challenges reflecting real world deployments. These vulnerabilities and challenges are updated periodically to stay current.

- The delegates can be trained in this lab on various subjects such as Penetration Testing, Reverse Engineering, Web Application Security, Mobile Application Security, Exploitation, Crime Prevention through Environment Design and Smart Cities Security.

Need of Government

- With 26/11 and the latest **Uri Attacks**, cyber intelligence plays even a bigger role in protection of our country. Gone are the days of spying physically – today it's all about intelligence from mobiles, social media, emails and hard-drives to prevent terrorist attacks.

- The government needs over **300,000** security experts in all Critical Information Infrastructures such as Railways, Aviation, Transport, Nuclear, Space, Oil and Gas etc. to protect Industrial controls from cyber warfare and economic loss

- **With over 109 planned Smart Cities,** the Government needs to train key stakeholders in various aspects of safe cities and protection of Information Infrastructures.

Need of Corporate

- As per a market research report, the global Cyber Security Industry will be worth $202.36 billion by 2021 growing at a CAGR of 10.6%.

- From a current $1.23 billion in 2016, Indian market is expected to grow at a CAGR of 8% during this period.

- At present, there is a shortfall of close to a million cyber security professionals in India.

- If we fail to find the right people soon, India will be at risk on losing foreign direct investments and technology projects due to concerns of economic loss, data theft and privacy by cyber attacks from state sponsored hackers

- The sole aim of our adversaries is to destroy the reputation of India as technology super power for outsourcing, data processing and software development.

*compound Annual Growth Rate

Need of LEA

- With Digital India push, there is an anticipation in huge rise in Financial cyber crimes

- India is currently ranked as Number 1 country targeted for Cyber crimes in the world

- The Law Enforcement Agencies are the first respondents to cyber crimes as they have to handle investigations under IT Act Law 2000

- The LEA is ill-equipped with skills to handle the rising issues of cyber crimes including corporate espionage, data thefts, privacy breaches and banking frauds.

- The sole aim of our adversaries is to destroy the reputation of India as technology super power for outsourcing, data processing and software development.

How Cyberange Helps

Sections in the Solution

1. Cyberange Model Lab
2. Building Simulation
3. Hands-on Training
4. Exam and Certification

Cyberange Model Lab Building Simulation Hands-on Training Exam and Certification

Example Layout of Cyberange Lab

- Simulated Physical Smart City
- Consists of model train tracks and switching networks using real SCADA Industrial controls
- Consists of traffic lights and software simulating real world use
- Consists of a hospital and bank that simulates industry process
- Has Government building and school with scenarios of physical security and crime prevention in event of terrorist attack
- Will cover Aviation security, Dam Security and more!
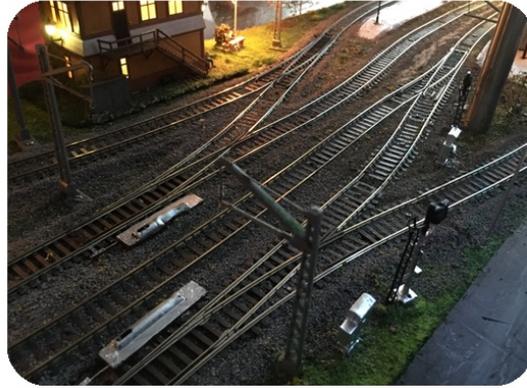- Consists of over 100+ Industry challenges on Cyber security
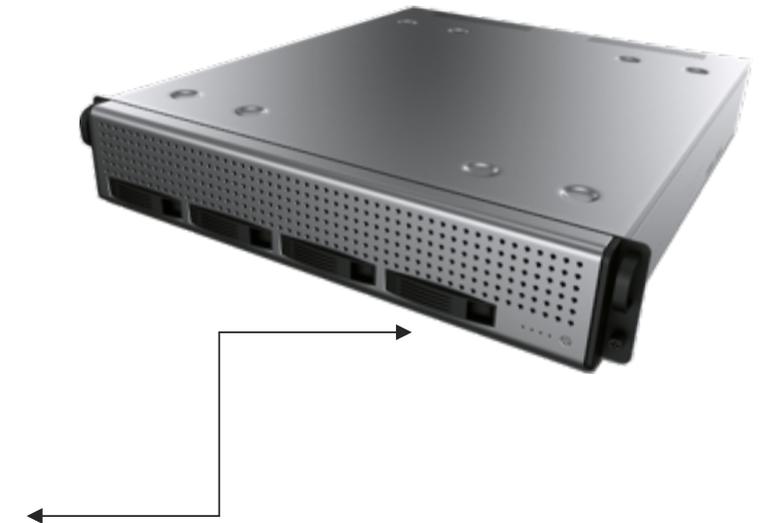
Cyberange Model Lab   Building Simulation   Hands-on Training   Exam and Certification

Cyberange Lab Pictures

Lab of Smart City connected with Cyberange Simulation Server

Sample representation only. Models are frequently updated and may look different depending on the scale, size and specification of Cyberange deployment.

Cyberange Model Lab · Building Simulation · Hands-on Training · Exam and Certification

Part 2 – Building Simulation

- The Simulation is the **Brain of Cyberange** that makes the whole physical model alive and interactive for learning on scenarios.

- Over 1 Million lines of code **(Patent Pending)** has been written to create a gamified architecture interconnected with the Physical Cyberange model.

- **The simulation software is constantly updated and built and comes with built-in 30 missions (and over 100+ sub missions) for interacting with the physical model.**

Cyberange Simulation Dashboard

Allows you to see progress of each individual and team!

Scoreboard is updated Automatically!

Solution to challenges are Submitted in the Dashboard!

Updated every month with new challenges!

Cyber Range

Blue Team Scoreboard

#	Team	Country	Points
1	demo1	🇮🇳	20
2	demo3	🇮🇳	0
3	demo2	🇮🇳	0

Red Team Scoreboard

#	Team	Country	Points
1	Iron Man	🇮🇳	0
2	demo4	🇮🇳	0
3	demo99	🇮🇳	0
4	Jaya surya kommireddy	🇮🇳	0
5	demo6	🇮🇳	0
6	Harsh	🇮🇳	0
7	demo5	🇮🇳	0

Challenges

Level 1	Points	Solved by	First solvers
Red Team - Recon1	20	33%	⭐demo1

Level 2	Points	Solved by	First solvers
Red Team - Recon2	40	0%	*Unsolved*
Red Team - Recon3	40	0%	*Unsolved*

Level 3	Points	Solved by	First solvers
Red Team - Recon4	100	0%	*Unsolved*
Red Team - Recon5	100	0%	*Unsolved*

2

Cyberange Model Lab   Building Simulation   Hands-on Training   Exam and Certification

Hands-on Training

- Various delegates can be nominated from multiple sectors on Cyberange

- The training will meet the following objectives:

    - Give orientation on National Security and importance of the Information Infrastructure
    - Give BASELINE knowledge of cyber security that is universally applicable
    - Build up on their sector specific experience to give cyber security skills

Cyberange Model Lab Building Simulation Hands-on Training Exam and Certification

Course Content – Missions Covered

FINDING TARGETS AND GATHERING INFORMATION

Mission 01: Finding the IP address of the city's Municipal Corporation office.

Mission 02: Finding the SCADA master control device controlling Billboards.

Mission 03: Finding the NOC center for traffic light and accident relief system

Mission 04: Finding the City's Central Fire Alarm Management System

Mission 05: Finding the SCADA PLC master control of the DAM Project

NETWORK, PORT RECON AND CCTV HACKING

Mission 06: Scanning the network for IP Cams.

Mission 07: Gain access to the city's central surveillance system

Mission 08: Move the cameras away from the buildings 1,3 and 5

TRAFFIC CONTROLLER LIGHTS AND MANIPULATING SYSTEMS

Mission 09: Establish connection to Traffic Controller System

Mission 10: Gain access to Modbus Relay Switching Program

Mission 11: Manipulate the program to gain access from external network

NETWORK EXPLOITATION AND BANKING SYSTEM

Mission 12: Find the gateway to central bank system

Mission 13: Gain access to the bank's security system

Mission 14: Manipulate the bank's alarm system

SCADA SWITCHING, HACKING RAILWAY NETWORKS

Mission 15: Find the Northern Railway Networks system

Mission 16: Obtain access to NRN Network

Mission 17: Gain access to switching system

Mission 18: Switching tracks - controlling Modbus Relay

AUTOMOBILE, WIFI AND HOSPITAL HACKING

Mission 19: DDOS'ing alarm systems

Mission 20: Hacking ECU causing total vehicle immobilization

Mission 21: Taking over Wi-Fi network at the local coffee shop

Mission 22: Manipulating medical records of patients admitted in hospital

SECURE POWER GRID AND DEFEND NETWORKS

Mission 23: Writing Firewall Rules for city's Power Grid

Mission 24: Snort Configuration for detecting attacks

Mission 25: SCADA Security for city's power grid

Mission 26: Setting Up Honeypots for defending networks

Mission 27: Policy Management to minimize risk

FORENSIC OPERATIONS OF SYSTEM AND NETWORK

Mission 28: GSM interception and handling PCAP Files

Mission 29: Handling file system images

Mission 30: Log analysis of attack on a telecom system

For Universities

Step 3: 8 Hour Lab Exam and Certification

Professional Level

Step 2: 5 Day Hands-on Cyberange Training | 1 Day Sector Specific Training

Associate Level

Step 1: Metasploit Online Training | Fellowship Online Training | 3 Day Baseline Security Training

3

Cyberange Model Lab | Building Simulation | Hands-on Training | Exam and Certification

For Corporate

5-Day Bootcamp for Corporate / Industry training

1. Portable version of Cyberange is deployed at Corporate site
2. Delegates are trained in bootcamp style (8 hours per day)
3. All sessions are hands-on, engaging and interactive
4. Certification is optional
5. The Lab is dismantled and removed after training

Deploying Cyberange in your premises

You can also buy the Cyberange program and deploy it at your campus for regular training.

Benefits of deploying Cyberange:

- Delegates can practice 24/7
- Get latest attack vectors simulated in Cyberange
- Your team never gets obsolete and is always prepared to handle latest cyber attacks
- Ideal for Universities (B.Tech / M.Tech), Law Enforcement, Organizations aiming ISO 27001 Compliance, Government agencies, Managed Services, Companies that deal in critical sectors (Banking/Telecom/Transport/Nuclear etc)

Cyberange Model Lab   Building Simulation   Hands-on Training   Exam and Certification

Part 4 – Exam and Certification

This is the most crucial part where the candidates will be tested for their skills in cyber security and certified!

To ensure only the best make it, a practical lab exam of 8 hours is conducted, consisting of various hands-on challenges in a time-bound environment.

ISAC has pioneered lab exams on cyber security in India with it's National Security Database program since 2011 and uses its phenomenal experience in certification process to deliver a world-class certification program for smart cities on Cyberange.

Exam Structure

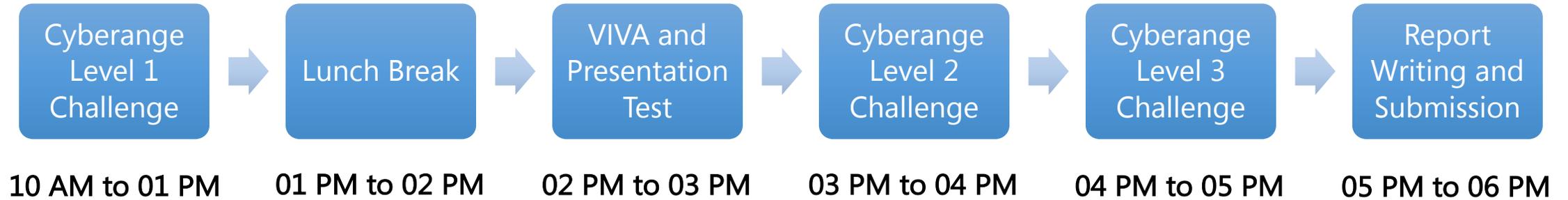| Cyberange Level 1 Challenge		Lunch Break		VIVA and Presentation Test		Cyberange Level 2 Challenge		Cyberange Level 3 Challenge		Report Writing and Submission

10 AM to 01 PM   01 PM to 02 PM   02 PM to 03 PM   03 PM to 04 PM   04 PM to 05 PM   05 PM to 06 PM

Sample Challenges:

1. Exploit the Android Phone remotely to get SMS and Contacts
2. Secure the Firewall and identify loopholes in the ACLs
3. Analyze the logs and identify the attack methods used by the attacker
4. Reverse Engineer a small binary to find the C&C of a botnet
5. Find problems in the in-flight system of an Airplane to spoof navigation

4

Certification Structure

Associate Level → Professional Level → Specialist Level

Associate Level

- Awarded to delegates who attend training
- Prove basic knowledge and cyber security skills
- Can help create awareness and handle level 1 security tasks

Professional Level

- Requires passing the **Cyberange 8-hour LAB exam**
- Must have hands-on experience and proven skills for security jobs
- Can handle level 2 and level 3 security tasks

Specialist Level

- **Requires Professional Level**
- Must have minimum 5 years of sector specific experience
- Can be a National Asset for handing a critical information infrastructure

Don't get obsolete. Get trained on Cyberange.

For further details, please reach us:

Information Sharing and Analysis Center
319A, Logix Technova, Next to Adobe Corporation
Sector 132, Noida – 201301

Email: support@isac.io
Contact: +91 8882-560-560

Rajshekhar Pullabhatla
Director - ISAC
+91 85274 65252 | +91 98738 69121
rajsm@isac.io