zettawise consulting

Zettawise' Cyber Range
The Trusted Tool To Test Enterprise' Digital Immunity

Endorsed by

SECURITY AND SCIENTIFIC TECHNICAL RESEARCH ASSOCIATION

Ministry of Home Affairs, Govt of India

These days, organizations rely on a wide variety of security solutions to protect their networks from cyber-attacks and traffic anomalies. But the more tools deployed, the more complex a security infrastructure becomes. These complex system interactions pose a serious risk to security performance and network resiliency.

Cyber Range is used to validate the security posture of client's networks with real applications and a complete range of threat vectors. By simulating real-world legitimate traffic, distributed denial of service (DDoS), exploits, malware, and fuzzing, Zettawise's Hybrid Cyber Range validates an organization's security infrastructure, reduces the risk of network degradation by almost 80%, and increases attack readiness by nearly 70%.

It not only provides a secure environment to test the enterprise' immune system against the latest cyber threats but also enables organization to evaluate the appropriate security products or solutions, manage incidents and perform Red Team – Blue Team exercises.

zettawise consulting

Key Functions of Cyber Range

Realistic Simulations

The platform offers realistic scenarios for cybersecurity posture assessment , allowing professionals to practice defending against sophisticated attacks.

Dynamic Test Environments

Dynamic environments let users experience different cyber scenarios in a hybrid environment by applying various attack strategies and evasion mechanism. Testing of equipment are best done in this bed.

Interactive Training

Interactive exercises enable hands-on learning, ensuring teams are well-prepared to handle real-world cyber threats.

zettawise consulting

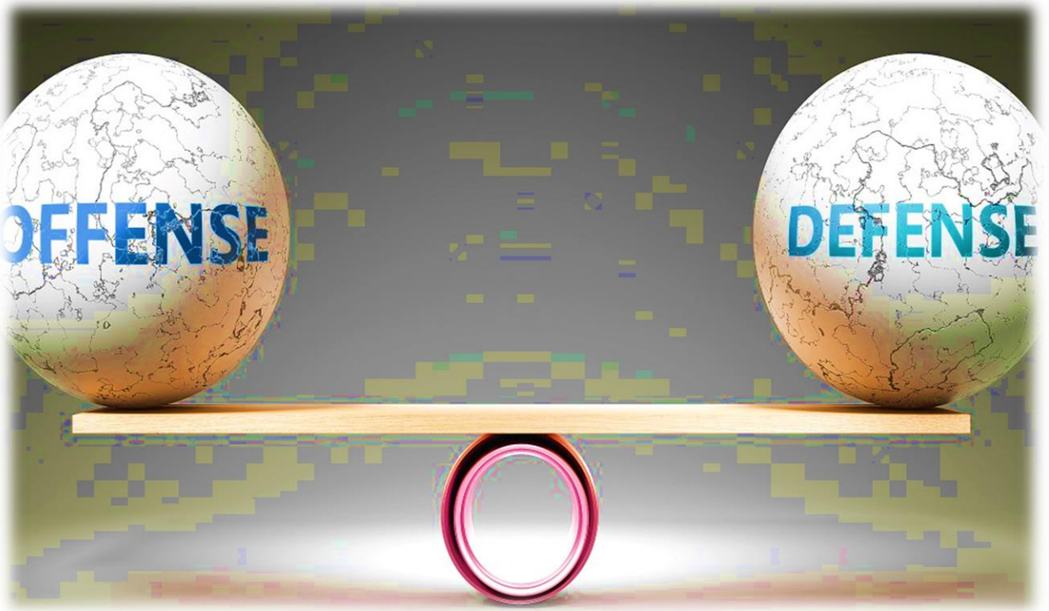
Cyber Range Helps Enterprises to Develop

Offensive Tactics

Opportunities to develop offensive strategies, allowing professionals to understand the mindset and techniques of cyber attackers.

Defensive Maneuvers

Exercises to strengthen defensive capabilities, enabling teams to identify and neutralize cyber threats effectively. It also helps critical sector organizations to conduct performance and security test of their ICT equipment before commissioning.

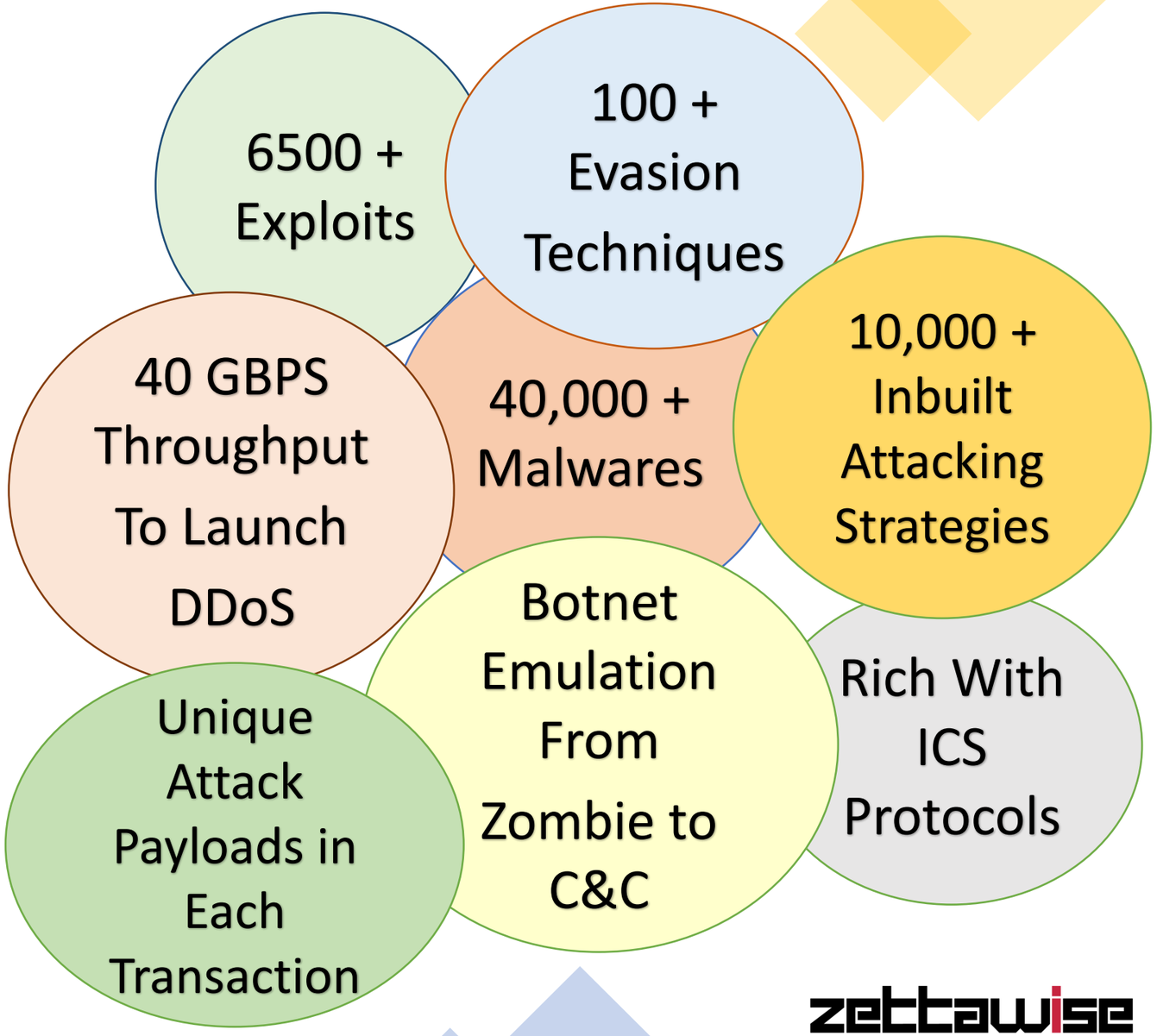


Capabilities of Zettawise' Cyber Range

How might a particular configuration or security setup withstand a cyber-attack ?

Zettawise' Hybrid Cyber Range addresses that by simulating both good and bad traffic to validate and optimize networks under the most realistic conditions. Security infrastructures (IT & OT) can also be verified at high scale, ensuring ease of use, greater agility, and speedy network testing.

Zettawise' Cyber Range is endorsed by SASTRA (RRU, Ministry of Home Affairs, Govt of India) for its capabilities to deal with ICS security.



zettawise consulting

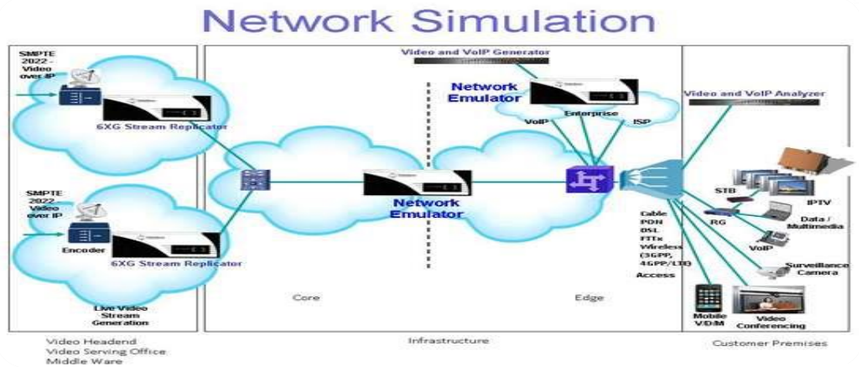
IXIA
Enabling a Converged World™

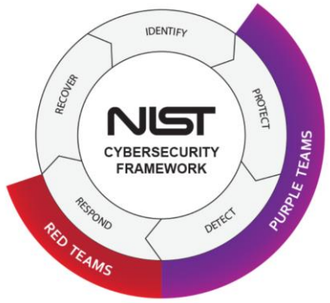
BreakingPoint™
Find it before they do.™

DARKTRACE

FORTINET

SOPHOS
Cybersecurity made simple.





splunk>

HPE aruba networking

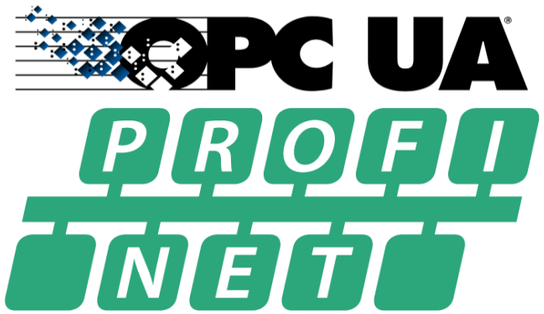
CISCO

MISP
Threat Sharing

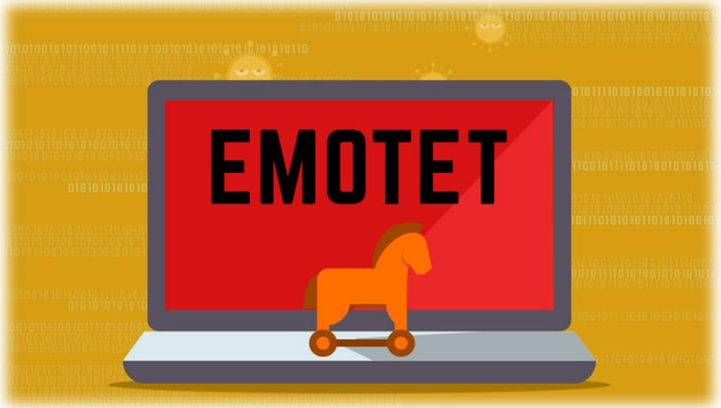
Major Components of Zettawise' Cyber Range

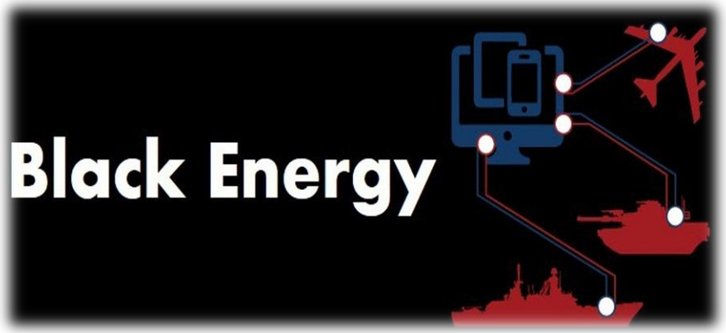
ADAPT —AND— ATTACK

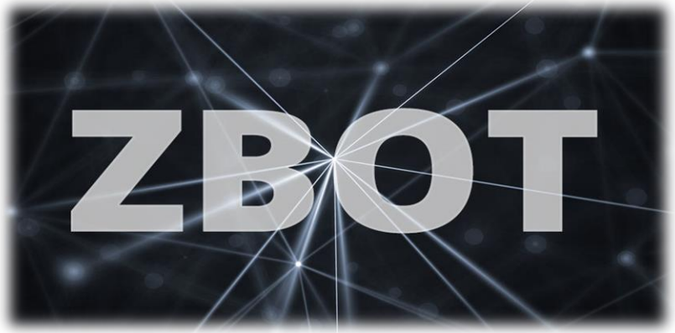
The Cyber Range is Rich With ICS Protocols

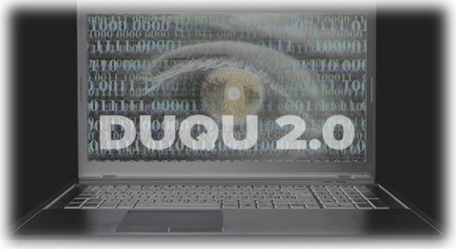


Cyber Range Can Emulate Botnets Like …









zettawise consulting

www.zettawise.in

Zettawise Helps Customers Combat With Modern Cyber Threat By:

1. Security Architecture / Design Validation
2. Incident Response Playbook Creation / Validation
3. War Game / Table-Top Exercise
4. Hands-on Training on Cyber Defense Mechanism
5. Threat Mitigation Process Verification
6. Simulating Advanced Attacks To Check Resilience
7. Performance Testing Of Security Equipment (RFC2544 Standard)

Services Offered

www.zettawise.in

zettawise consulting

Key Test Cases of Zettawise' Cyber Range

- Mitigate existing and future risks through testing of different normal and abnormal scenarios (both for applications and hardware equipment)
- Build highly realistic labs using simulation techniques at a substantially lower cost
- Run customized traffic and attacks replicating the uniqueness of your network without compromising security
- Run regression tests with updated application and attack scenarios to continuously validate the dynamic world of SCADA security and fast-track patch management and updates
- Build SCADA cyber defence training curriculum to train security professionals with scenarios like application traffic management, deploying security policies, and handling breach incidences

Cyber-attack Models Tested on A Digital Twin

- Port and Network Security
- Eavesdropping
- Jammers
- Denial of Service
- Packet Modification
- Stimulate Intrusion Detection System
- Signal Intelligence
- Vulnerability Exploitation
- Virus Attacks
- Worm and Virus propagation
- Backdoors, Rootkits
- Botnets
- Coordinated Attacks
- Adaptive Attacks
- Ransomware
- Data Exfiltration

Services Best Fit For Critical Sectors

zettawise consulting

www.zettawise.in

Use Case 1: DDOS Protection

Problem Statement:

Today, distributed denial of service (DDoS) attack is a big risk to any business with an online presence. Organizations need to know if their networks can fend-off the flood of traffic coming from hundreds of thousands of compromised systems while still accepting normal business traffic. Since every update in the network may impact the efficacy of your DDoS mitigation solution, validation must be a continual process

Solution Approach:

Zettawise' Hybrid Cyber Range simulates both normal application traffic and security threats at scale so you can validate critical data points like number of packets dropped by your DDoS mitigation solution, how your solution functions in a real attack, what level of service you can provide while under attack, and how your people and process react to and withstand an attack.

zettawise consulting

Use Case 2: SCADA Network Security Test

Problem Statement :

With SCADA operating over IP networks, the line between IT and OT has blurred...however, many OT teams are not prepared to handle threats in ICS networks.

Organizations are taking notice of the threats to SCADA networks and the possible impacts of breaches. It is also clear that, despite being much farther from the standard network security demarcation zones, SCADA networks continue to be exceptionally vulnerable to cyber-attacks.

Solution Approach:

Validation in the lab with Zettawise' Hybrid Cyber Range's real-world application traffic and security attacks can ensure SCADA networks are resilient and secure. Increasing the attack readiness of both your ICS networks and people will go a long way in increasing the resiliency of the SCADA/ICS systems of today and in the future.

Why Do We Need to Test?

SCADA networks are exceptionally vulnerable Many traditional SCADA systems now contain extensions to operate over TCP/IP to connect to and access distributed, remote systems. Using TCP/IP means these systems have the reliability and sophistication of a data transfer protocol that keeps the Internet running. However, this has also exposed SCADA networks to the vulnerabilities targeted at TCP/IP over the course of many years. On top of this, we need to consider the fact that many SCADA applications were not designed with IP network-level security in mind. Coupled with the fact that SCADA is implemented in many critical infrastructures, state and non-state actors may have special interest in such networks.

About Zettawise

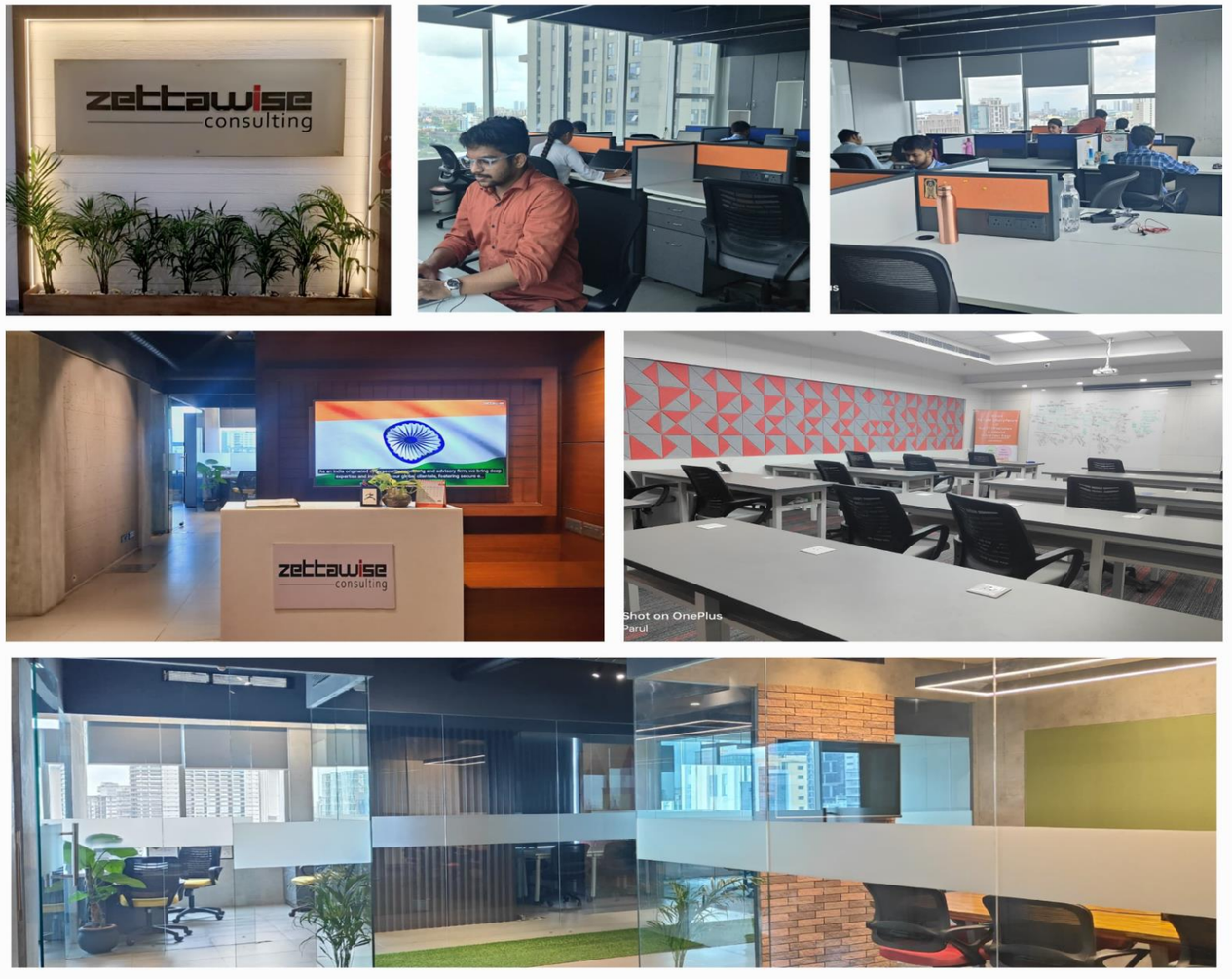
Zettawise Consulting Pvt. Ltd (www.zettawise.in) is an ISO 27001, ISO 9001 and ISO 20000-1 certified technology firm which has established its position prominently in national critical infrastructure protection. It assists governments & large enterprises in strengthening their cyber security posture, ensuring compliance with international best practices, improving their cyber attack resilience and enhancing incident handling capabilities.

Zettawise Consulting is a part of the joint workforce of SASTRA (RRU, Ministry of Home Affairs, Govt of India) under the aegis of "AtmaNirbhar and AtmaSurakshit Bharat Mission" of Govt of India.

zettawise consulting

zettawise
consulting

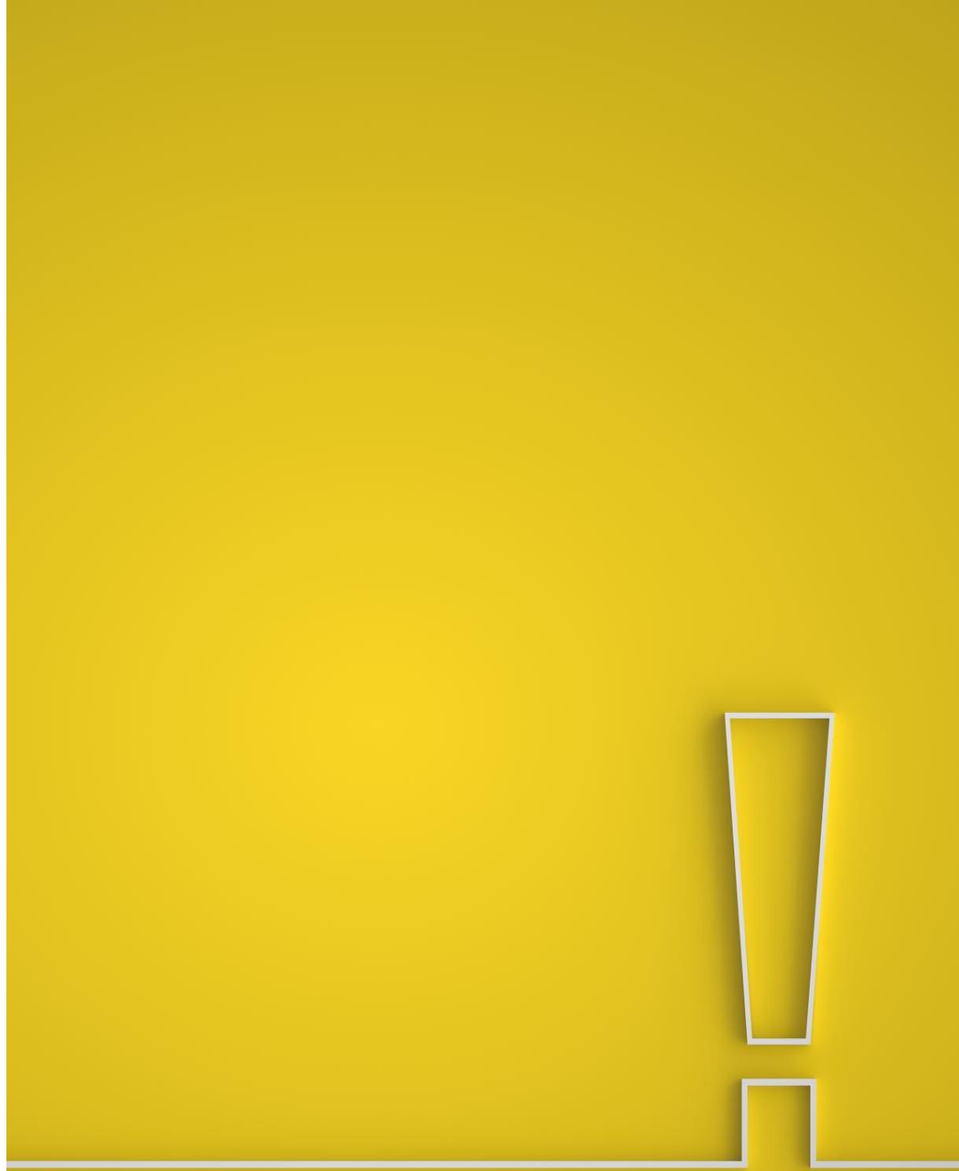
www.zettawise.in



Zettawise’ State of The Art Cyber Command Centre

Other Services of Zettawise

- Information Security Audit, Consulting & Advisory
- Enterprise and Third-Party Risk Assessment
- ICS Security (Fully Loaded OT Lab, Focused on Critical Infrastructure)
- Security Assessment (Vulnerability Assessment & Penetration Test)
- Dev-Reg-Sec-Ops
- Skill Development



zettawise consulting

Zettawise Consulting Pvt. Ltd.
11th Floor, Godrej Genesis.
EP & GP Block
Suit No. 1102. Sector – 5
Salt Lake Electronics Complex.
West Bengal 700091. India.
Call: +91 9830089446 / +91 7980889376
Web: www.zettawise.in

zettawise consulting

Thanks.