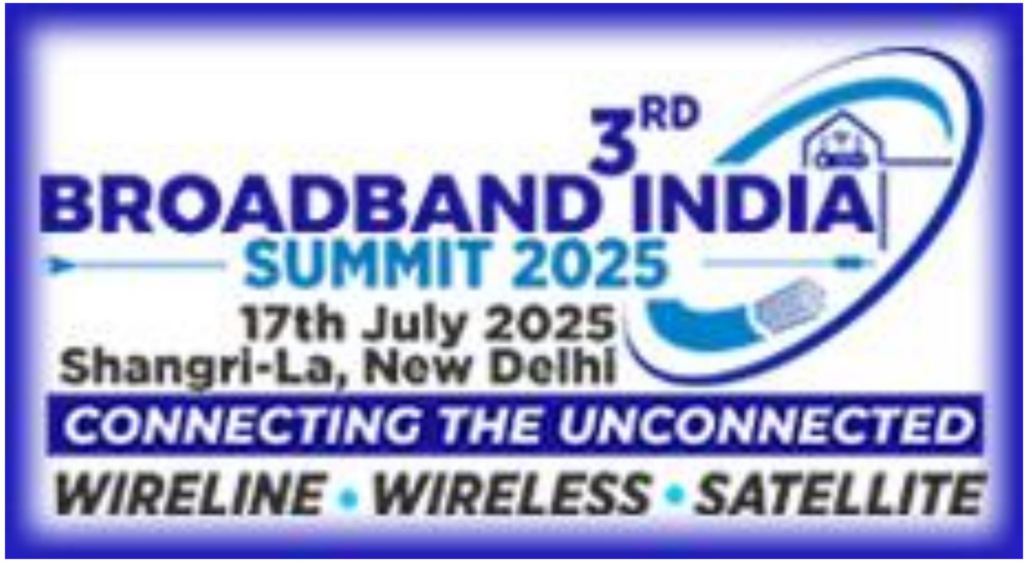
Critical Infrastructure Protection: The New Frontline in National Security

17th July 2025



3RD BROADBAND INDIA SUMMIT 2025

17th July 2025

Shangri-La, New Delhi

CONNECTING THE UNCONNECTED

WIRELINE • WIRELESS • SATELLITE

BIF™

BROADBAND INDIA FORUM

"Think Tank for Digital Transformation"

PYRAMID®

NexGen Cyber Security & Forensics

Thoughts from Alok Gupta

Principal Advisor & Co-Chair Cyber Security Committee, BIF

Founder & CEO Pyramid Cyber Security & Forensic

A bit about me

Alok Gupta

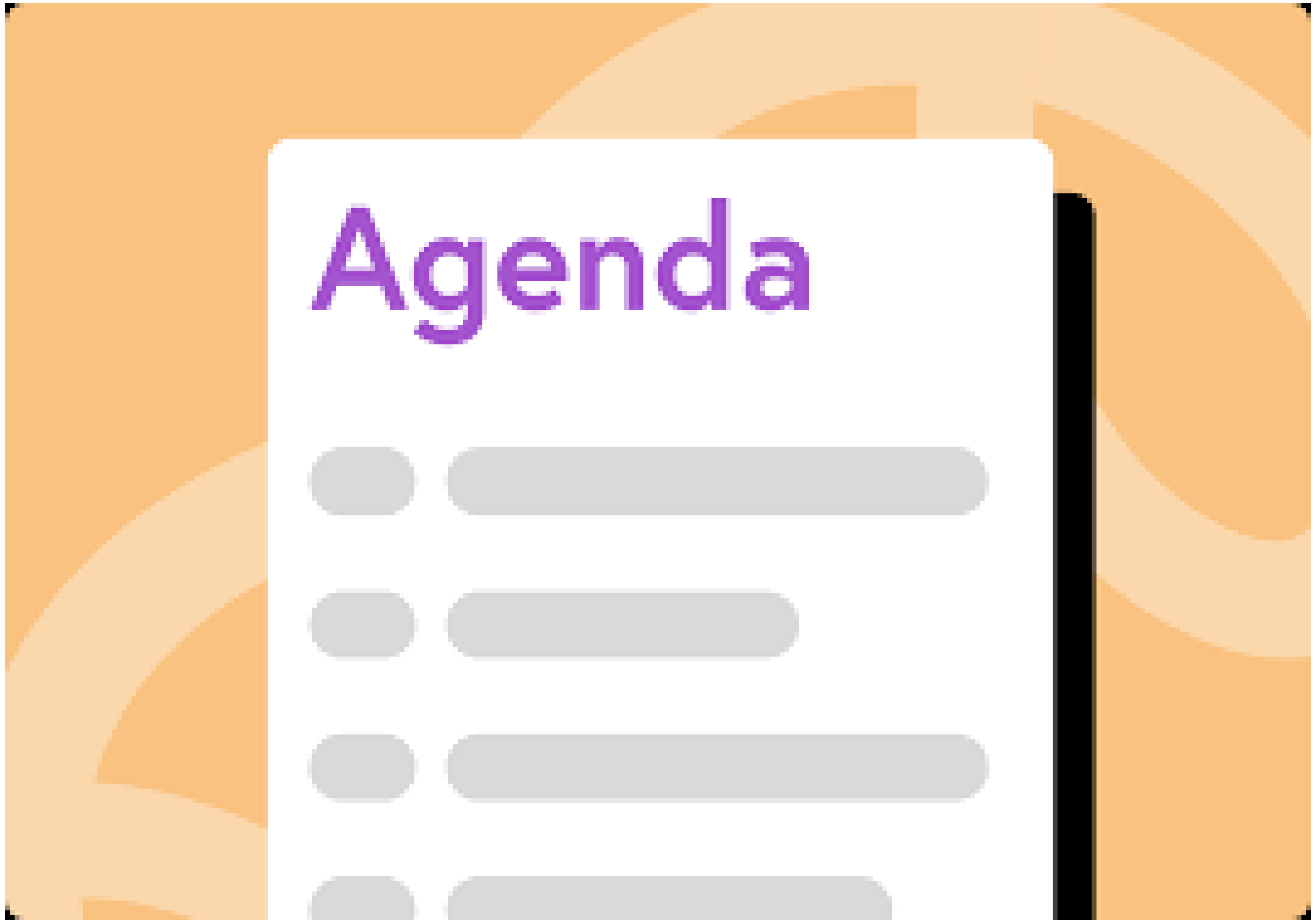
- Experience: 32+ years in the Information and Communications Technology (ICT) industry Serial Entrepreneur , Founder & CEO, Pyramid Cyber Security & Forensic, a boutique Digital Forensic and specialised Information Security solution and services provider
- Member of the regional committee on Digital Transformation for Confederation of Indian Industries (CII)
- Advised several Enterprises and Government agencies leverage use of ICT and Information Security to compete and grow in the global economy.
- Principal Advisor & Co-Chair Cyber Security Committee of Broadband India Forum
- Member Board of Governors Birla Institute of Management Technology
- Faculty FAFD, Institute of Chartered Accountants of India (ICAI)
- Writes Columns, frequently quoted in IT, Security & Forensic media , regularly speaks at several events, workshops, seminars and forums in India and Internationally

Critical Infrastructure Protection: The New Frontline in National Security

Session Takeaways

Today we will address

- Examples of Critical Infrastructure Protection
- Critical Telecommunications Infrastructure
- Key aspects of Telecom Cyber Security Rules
- Cyber threats & Risk faced by Telecom Sector
- How to Prevent & Protect
- Zero Trust: Never Trust Always Verify

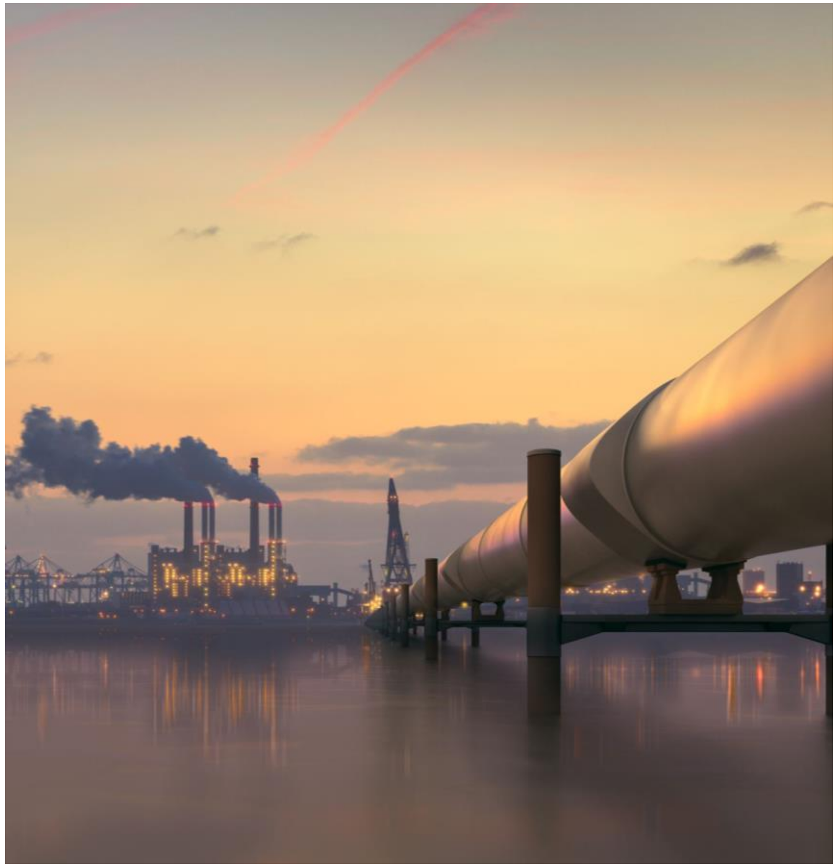


Critical infrastructure protection (CIP)

Critical infrastructure protection (CIP) are measures taken to safeguard the essential systems and assets of a nation or organization, ensuring their continued operation and preventing disruptions that could have severe consequences on security, economy, public health, or safety

Examples

- **Energy:** Power grids, oil and gas facilities, nuclear reactors
- **Transportation:** Airports, railways, highways, maritime systems
- **Communications:** Telecommunications networks, internet infrastructure
- **Water:** Drinking water treatment and distribution, wastewater treatment
- **Financial Systems:** Banking and financial market infrastructure
- **Public Health:** Hospitals, medical facilities, emergency services
- **Food:** Production, processing, and distribution of food
- **Public Administration:** Government services and infrastructure

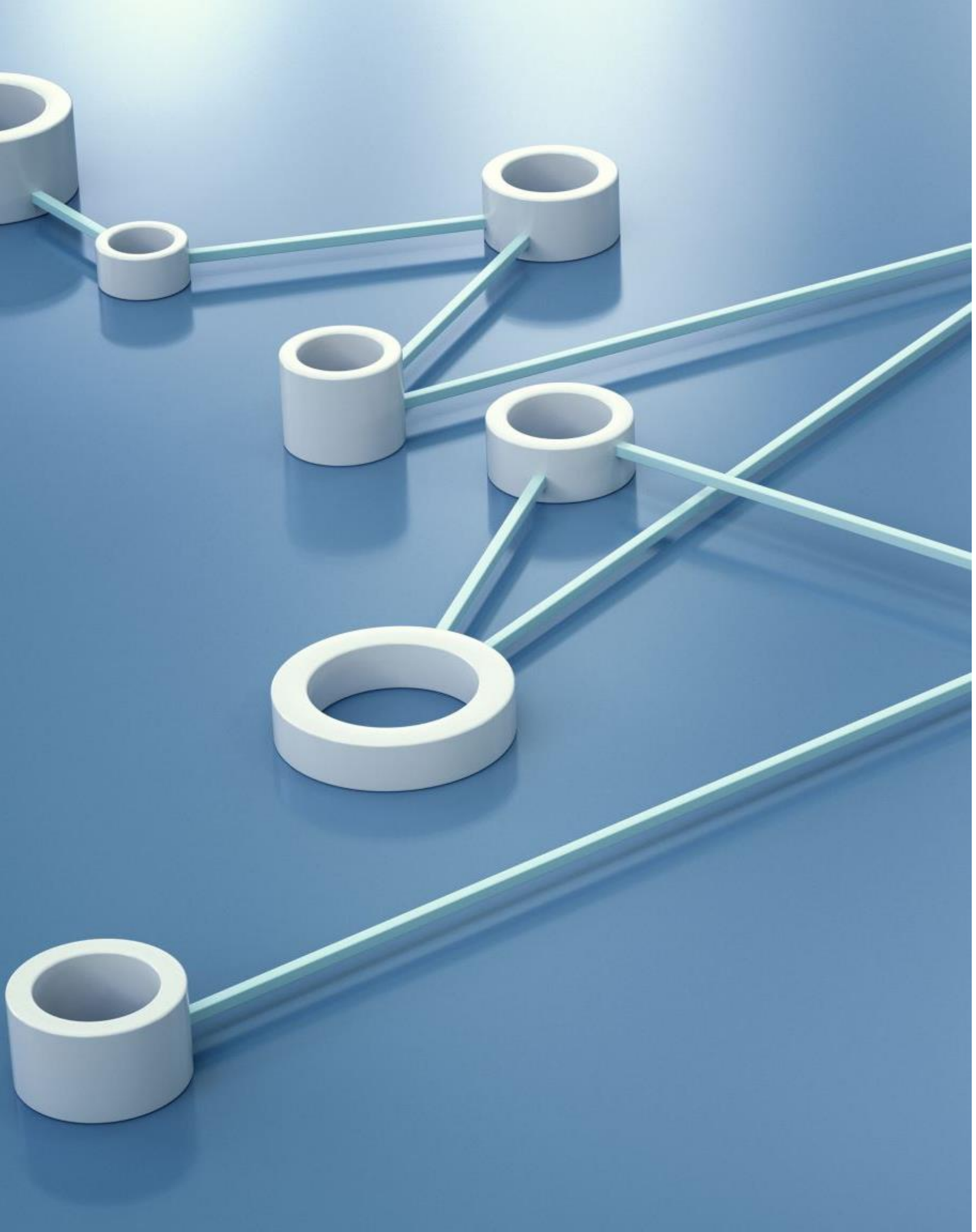


Critical Telecommunication Infrastructure (CTI)

Involved safeguarding essential telecommunication networks and systems from disruptions

The Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024, in India, are a key example of such measures, focusing on designated networks whose disruption could have significant impacts

Key aspects



Designation of Critical Infrastructure

The Central Government designates specific telecommunication networks or parts thereof as Critical Telecommunication Infrastructure (CTI) based on their potential to impact national security, the economy, public health, or safety

Compliance and Security

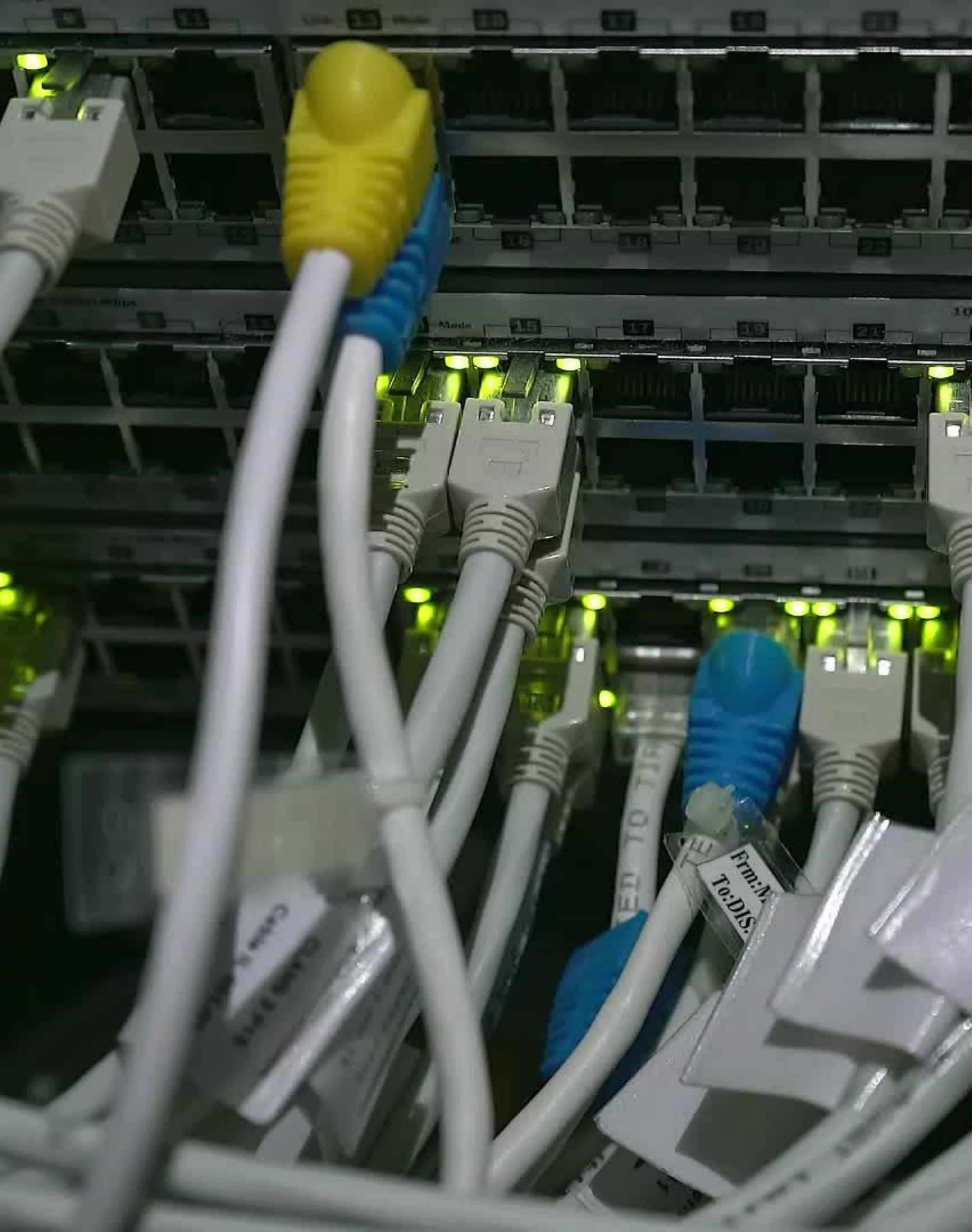
Telecommunication entities operating CTI are required to comply with specific standards and regulations, including those related to hardware, software, and security protocols

Chief Telecommunication Security Officer (CTSO)

Telecommunication entities must appoint a CTSO to oversee compliance with CIP rules and ensure the implementation of necessary security measures

Security Incidents

The Telecommunications (Telecom Cyber Security) Rules, 2024 define and address security incidents that could affect telecommunication systems



Network Segmentation

Telecom operators are encouraged to segment their networks to isolate critical infrastructure from less sensitive systems, limiting the potential impact of security breaches

Real-time Threat Detection

Implementing systems for real-time threat detection and monitoring is crucial for identifying and responding to potential security incidents

Interdependencies

Recognizing the interconnectedness of critical infrastructure sectors is vital, as disruptions in one area can have cascading effects on others

Cybersecurity Frameworks

Telecom operators are encouraged to adopt robust cybersecurity frameworks based on industry best practices, such as ISO 27001 and NIST, to enhance their resilience against evolving threats

NIST

ISO 27001

Cyber threats faced by Telecom Sector

Telecom companies store a lot of sensitive data, making them an attractive target for cyberattacks.

Malware and ransomware: These attacks can disrupt services and affect many consumers

Social engineering and phishing: These attacks can compromise subscriber credentials or devices

DDoS attacks: These attacks can disrupt services

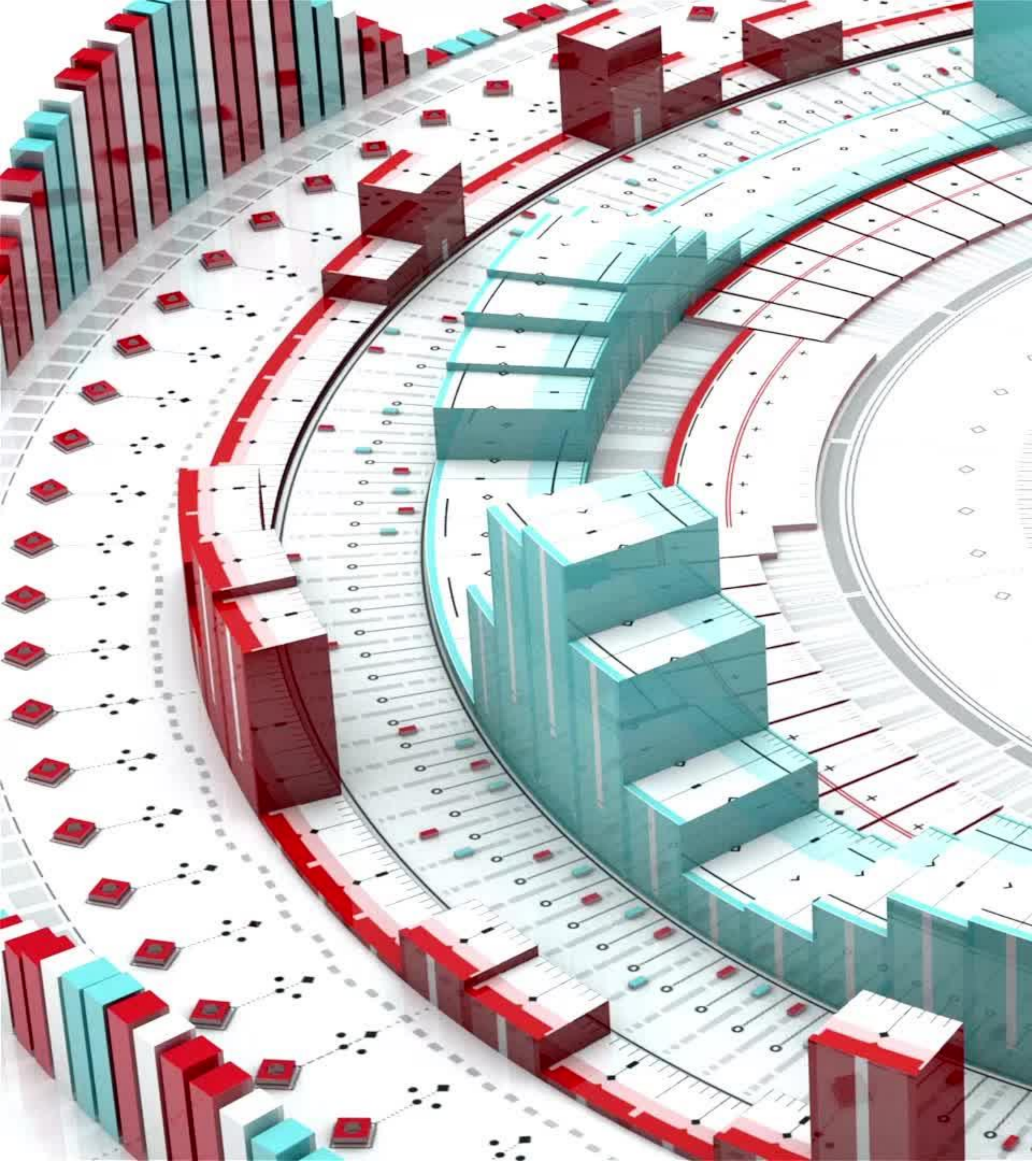
How to prevent and Protect

The Importance of Cybersecurity Awareness

How much end-users know about the cyber security threats their networks face, the risks they introduce and mitigating security best practices to guide their behavior

Cyber Hygiene

- Cybersecurity best practices that an organization's security practitioners and users need to undertake similar to having personal hygiene practices to maintain your own health,
- Cyber hygiene best practices help protect the health of your organization's network, assets & sensitive data



Cyber Range

Cyber range is a virtual environment that simulates real-world networks and cyberattacks.

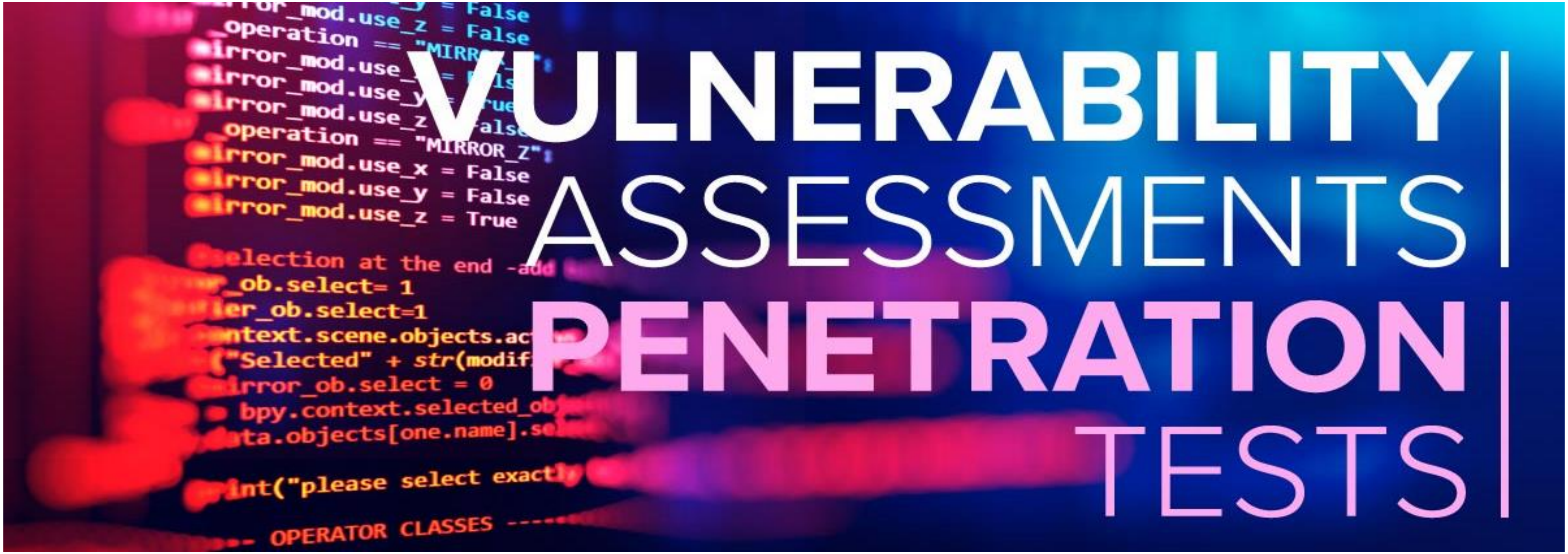
It provides a safe and controlled environment for training, testing, and research in cybersecurity

Cyber range can be used to simulate various network setups, including target infrastructures

IT & Security Audit & Assessment

Get current system's internal control design and effectiveness against relevant standards, best practices and remote working including design, architecture, implementation, performance, efficiency, security protocols and IT governance.

Experts should be engaged to design and review incident response plan and check the organization’s preparedness and readiness for a revised cyber insurance



- Vulnerability Assessment scans should be performed on your network, applications, web infrastructure and end points to check critical and exploitable vulnerabilities.
- Thereafter Penetration tests exploitation is conducted to determine whether unauthorized access or other malicious activity is possible and identify which flaws pose a threat.

Red Team Exercise

Red Teaming is the process of using tactics, techniques, and procedures to emulate real-world adversaries to train and measure the effectiveness of the people, processes, and technology used to defend organizations

Enable Multifactor Authentication:

- Social engineering remote privileged employees will allow hackers to know and steal credentials allowing them to access business critical information as insiders.

- Multifactor Authentication System allows remote employees to leverage convenient & flexible tokens for secondary authentication of all end points, trusted devices, VPN, on-premise and cloud applications, to prevent credential theft and unauthorized access while meeting the regulatory needs

Multifactor authentication
Time
Something you have
Something you are
Something you know
Location
*****
55984
TechTarget

YKYTA/ADOBE STOCK, ALEXDNDZ/ADOBE STOCK

©2019 TECHTARGET. ALL RIGHTS RESERVED

24x7 Continuous Monitoring & Threat Intelligence

- 24x7 Log & network monitoring correlated with threat feeds to not only meet the compliance requirements of continuous monitoring at the same time giving you instant alerts and intuitive dashboard for governance as well as remediation via Managed Security Services Platform

Secure Configuration Management

Misconfigurations can lead to breaches and cyber incidents

Compliance requires organizations to continuously check and remediate configuration issues in physical servers and VM's and provide audit-ready reports

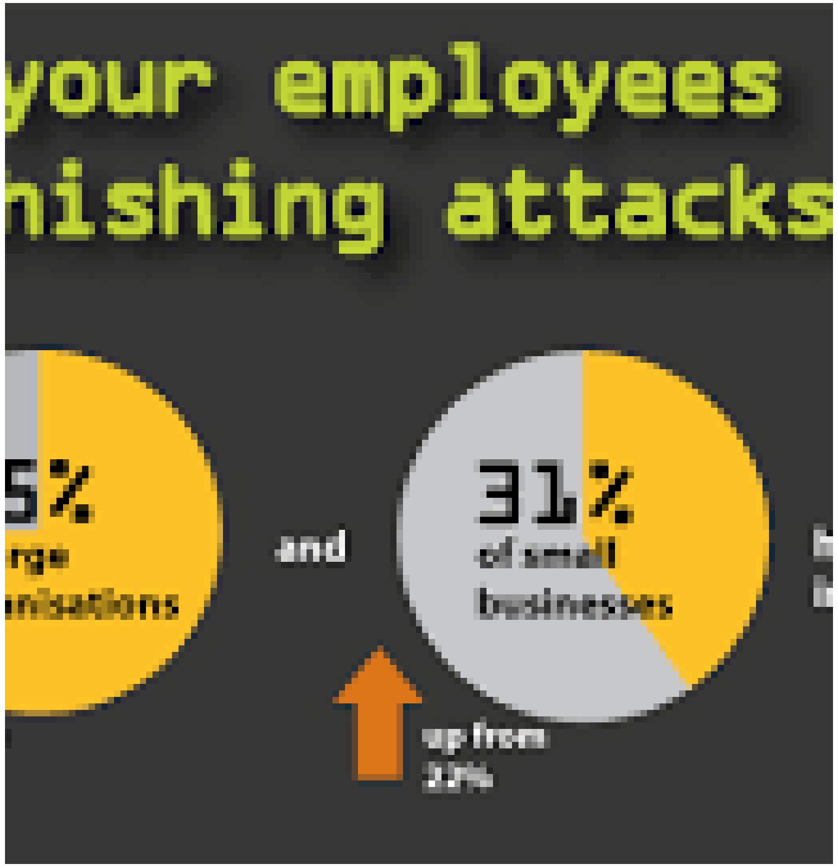
Continuously and comprehensively identify and automatic remediation

Phishing Campaign Assessment

- Sophisticated threat actors mostly target senior leadership, privileged users, and those with payment authority.

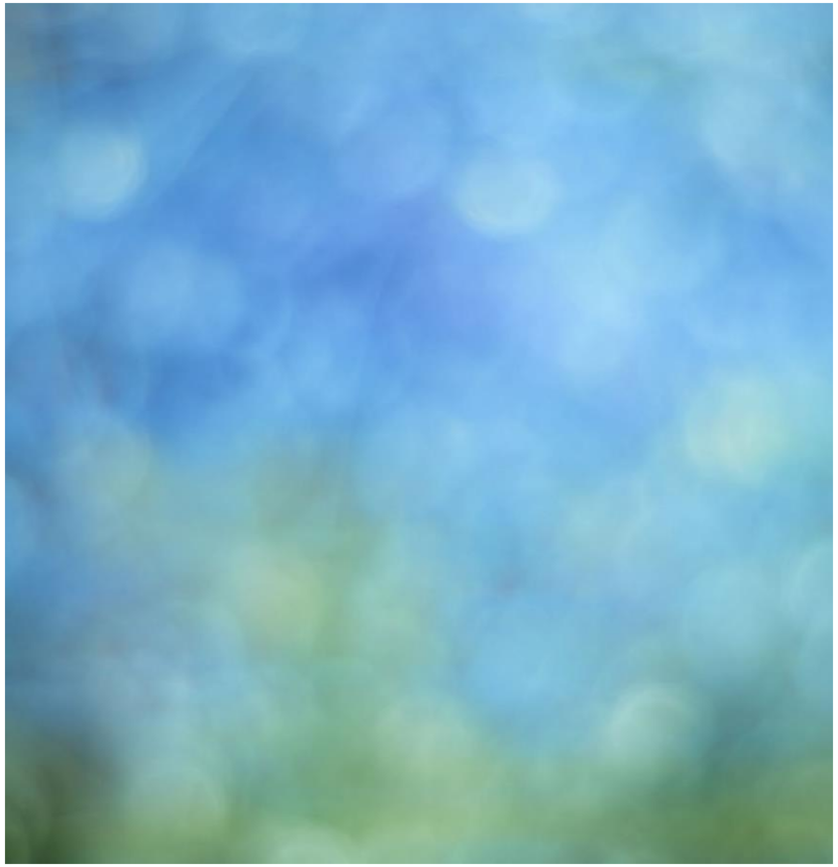
- Very convincing campaigns and phishing attacks are launched to lure such users.

- Launch scenario based simulated campaigns for phishing assessment and employee awareness



Ensure Compliance to Data Privacy

Manage	Manage access to sensitive and regulated data
Follow	Follow proper compliance requirements
Monitor and detect	Monitor and detect suspicious behavior on sensitive data

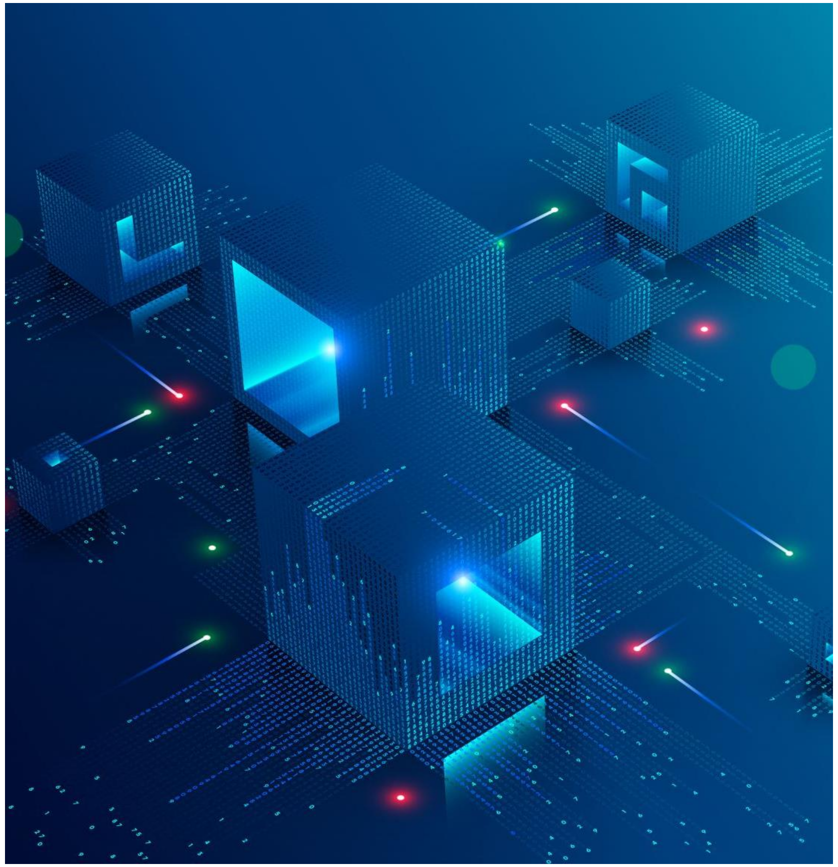


Go for Cyber Insurance

- Cyber insurance help businesses hedge against the potentially devastating effects of cybercrimes such as malware, ransomware, distributed denial-of-service (DDoS) attacks, or any other method used to compromise a network and sensitive data

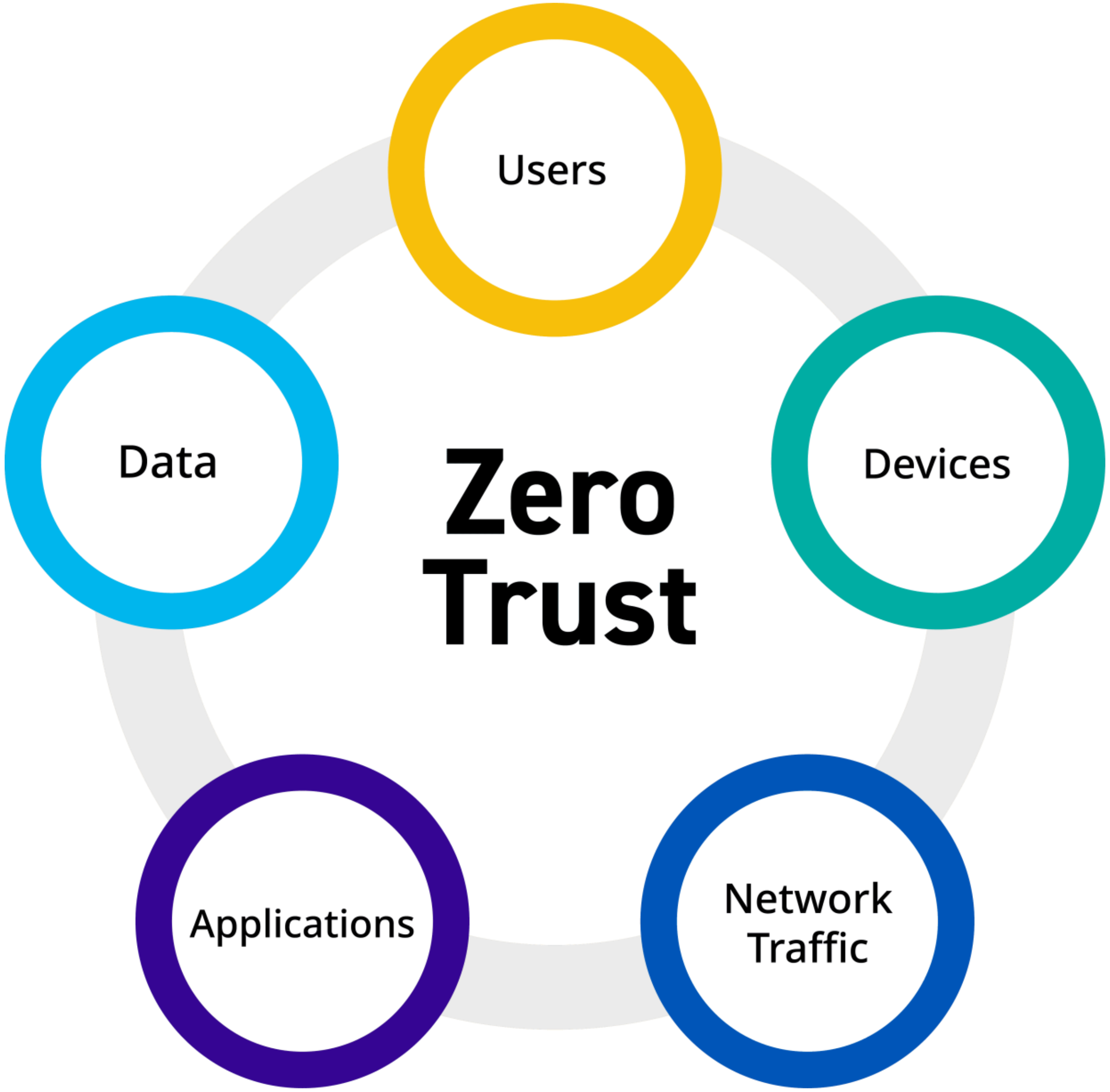
Cyber Security Essentials

- Prediction, prevention, detection, resolution & protection from cyber attacks, breaches and threats
  - Design & Architecture (Zero Trust)
  - Audit & Assessment
  - VA-PT
  - Policy & Process
  - Compliance, Adoption of Standards
  - Data Leak prevention
  - Information Rights Management
  - Multifactor Authentication
  - Continuous Configuration Management
  - Security Information Event Management (SIEM)
  - Threat Intelligence & Security Analytics
  - Managed Security Service



Zero Trust

Zero trust is a cybersecurity strategy that assumes no entity should be trusted by default. It's based on the principle of "never trust, always verify" and aims to prevent unauthorized access to data and services



Thank You!

Alok Gupta,
Founder & CEO
Pyramid Cyber Security & Forensic
alok.gupta@pyramidcyber.com
9999189650

Questions?