Cybersecurity & Data Privacy in GCC's"

GLOBAL CAPABILITY CENTRES

GCC SUMMIT 2025

FROM LEDGERS TO GLOBAL LEADERSHIP

CHARTERED ACCOUNTANTS SHAPING GCCs

27th -28th June 2025
The Grand Hotel, Vasant Kunj, New Delhi

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

Disclaimer!

- Everything I state here is my opinion and is based on my research and experiences
- I am sure that some of you will already know most of it so do not get angry!

Session Outcome

Take away from today's Sessions

By the end of this session, you will be able to learn about:

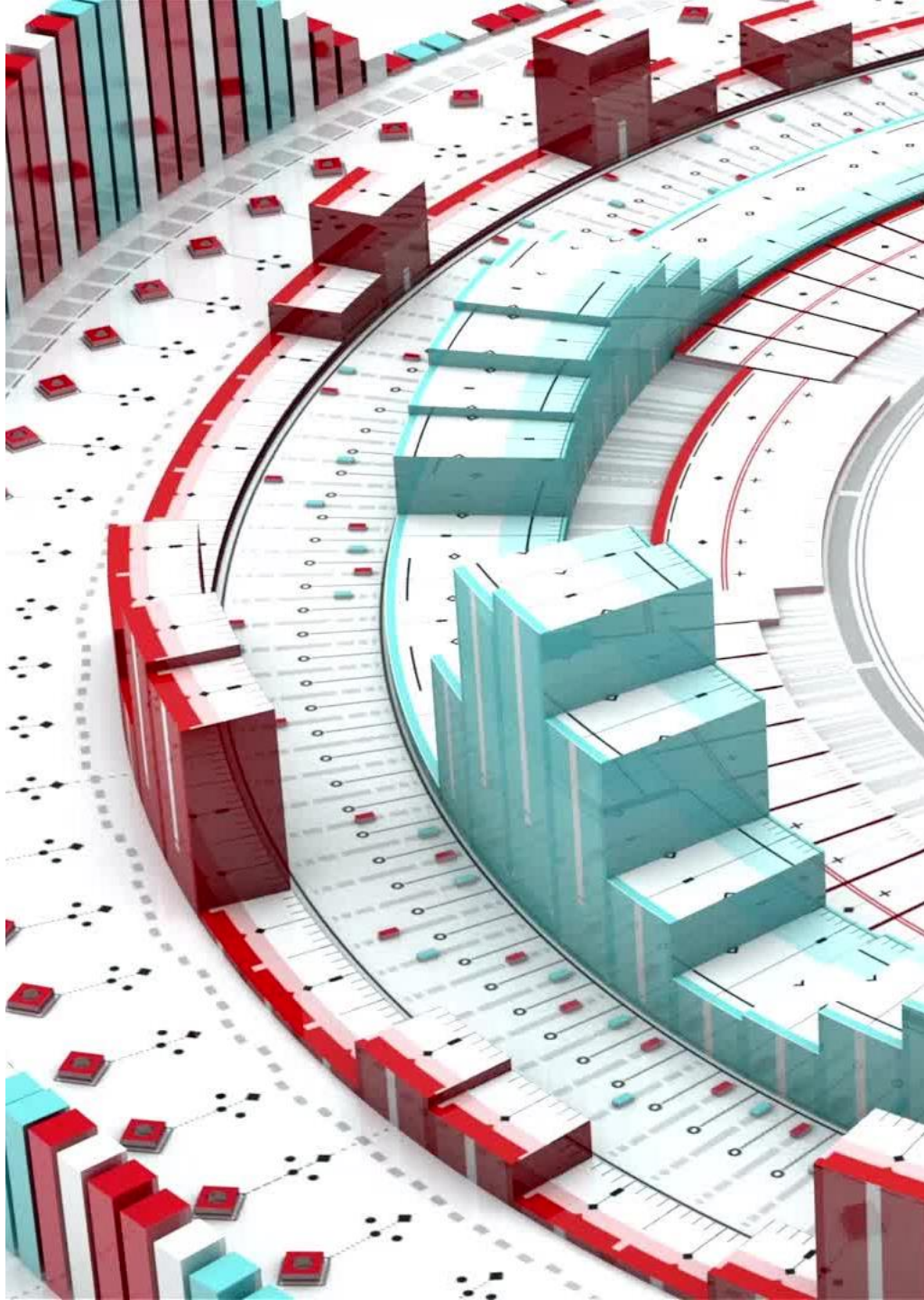
Challenges: Cyber Security & Data Privacy in GCC

How to prevent & Protect

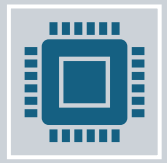
Best is to start Now!

Global Capability Centres (GCC) growth story

- With India's strong talent pool, digital infrastructure, and government policies, GCCs today are transforming from cost-centric offshore units to strategic hubs driving global innovation and digital transformation
- With over 2,200 GCCs employing 2.8 million professionals, the market is projected to reach US $110 billion by 2030
- Chartered Accountants are in a unique position to leverage this growth story since they not only understand their domain of accounting, taxation, audits etc. but they understand how a business works



Why cybersecurity is crucial for GCC’s?



Global Capability Centres (GCCs) manage sensitive data and critical business functions

GCCs face significant cyber threats and require strong security measures to protect themselves and their parent organizations

Challenges

WHAT'S THE GREATER CYBERSECURITY THREAT?

Protecting Sensitive Data!

GCCs handle vast amounts of sensitive data, including customer information, financial data, intellectual property, and more

A breach could lead to severe financial losses, reputational damage, and legal repercussions

Maintaining Business Continuity!

GCCs are integral to the core operations of their parent companies

A cyberattack could disrupt their ability to provide services, impacting the entire organization

Ensuring Compliance!

GCCs operate under various regulatory frameworks, including data privacy laws like GDPR and HIPAA

Cybersecurity measures are essential for meeting compliance requirements and avoiding penalties

Preventing Financial Losses!

Cyberattacks, such as ransomware and phishing scams, can lead to significant financial losses through ransom demands, recovery costs, and business disruptions

Protecting Reputation!

A cyberattack can severely damage a company's reputation, eroding customer trust and impacting future business prospects

Remote Work Risks!

With the rise of remote work, GCCs face new cybersecurity challenges.

Secure remote access protocols and robust endpoint security are crucial.

Data Privacy!

Compliance with country specific data privacy and data protection regulations

Global Data Privacy Regulations

General Data Protection Regulation (GDPR) (EU)
California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) (US)
UK Data Protection Act 2018 (the "Data Protection Act") (UK)
Privacy Act 1988 (Australia)
Personal Data Protection Act (PDPA) (Singapore)
Digital Personal Data Protection (DPDP) (India)
Personal Information Protection Law (PIPL) (China)
Lei Geral de Proteção de Dados (LGPD) (Brazil)

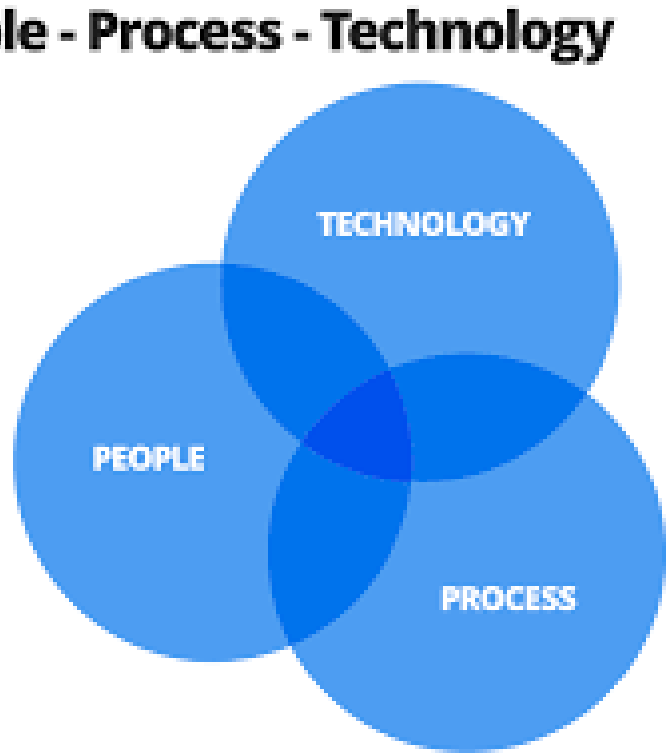
Cyber Security & Data Privacy: Strategic & Proactive

Cybersecurity is not just an IT concern for GCCs

It's a critical business imperative that requires a strategic and proactive approach

How to prevent and Protect

Relevance of PPT in Cyber Security



Build a Security-First Culture

How much end-users know about the cyber security threats their networks & IT assets 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

Implement Risk Management Framework

Develop and implement comprehensive risk management frameworks, such as NIST CSF/ISO 27001 including threat detection, incident response, and business continuity plans

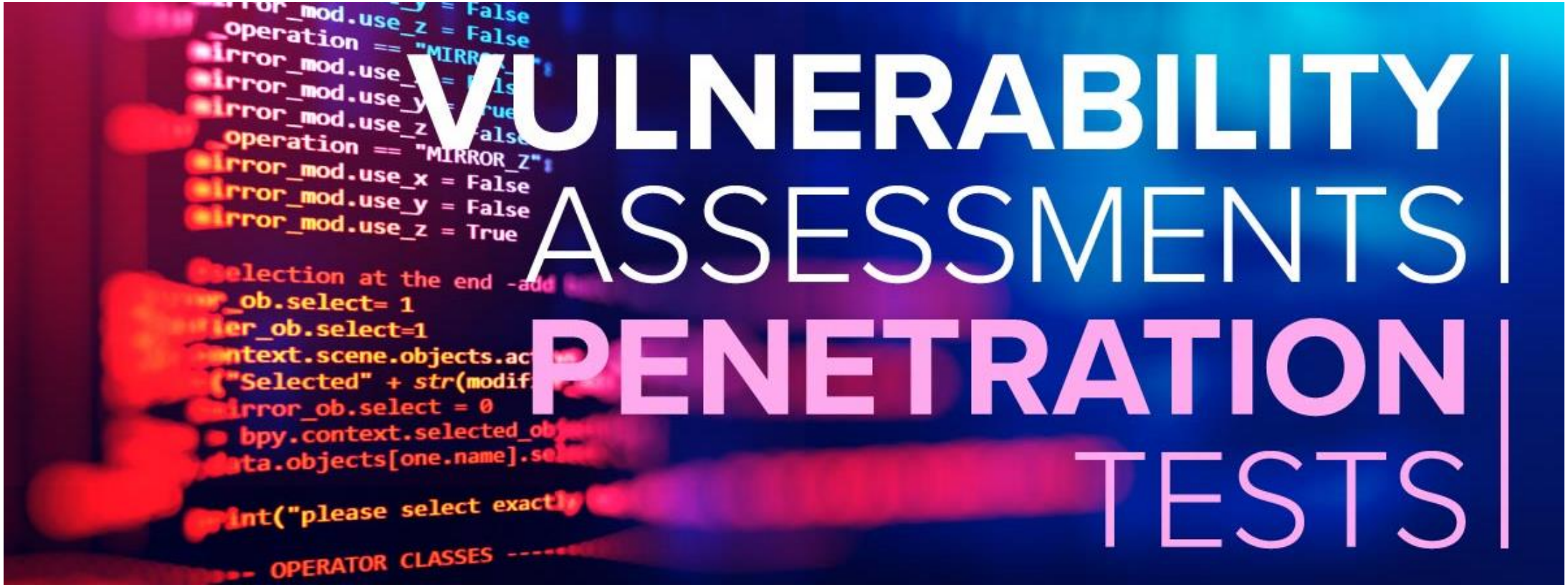
Implement Zero Trust Architecture

Implement zero-trust principles, where access is granted based on least privilege and continuous verification

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

Security Operations Centre (SOC)

Establish SOC for 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 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

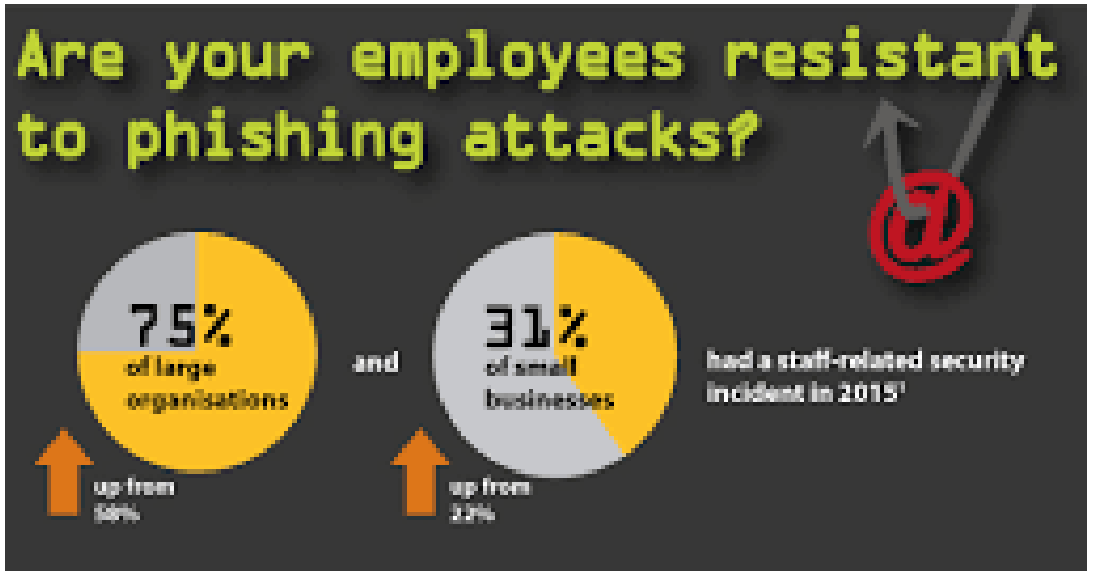
Continuously and comprehensively identify and automatic remediation

Phishing Campaign Assessment

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

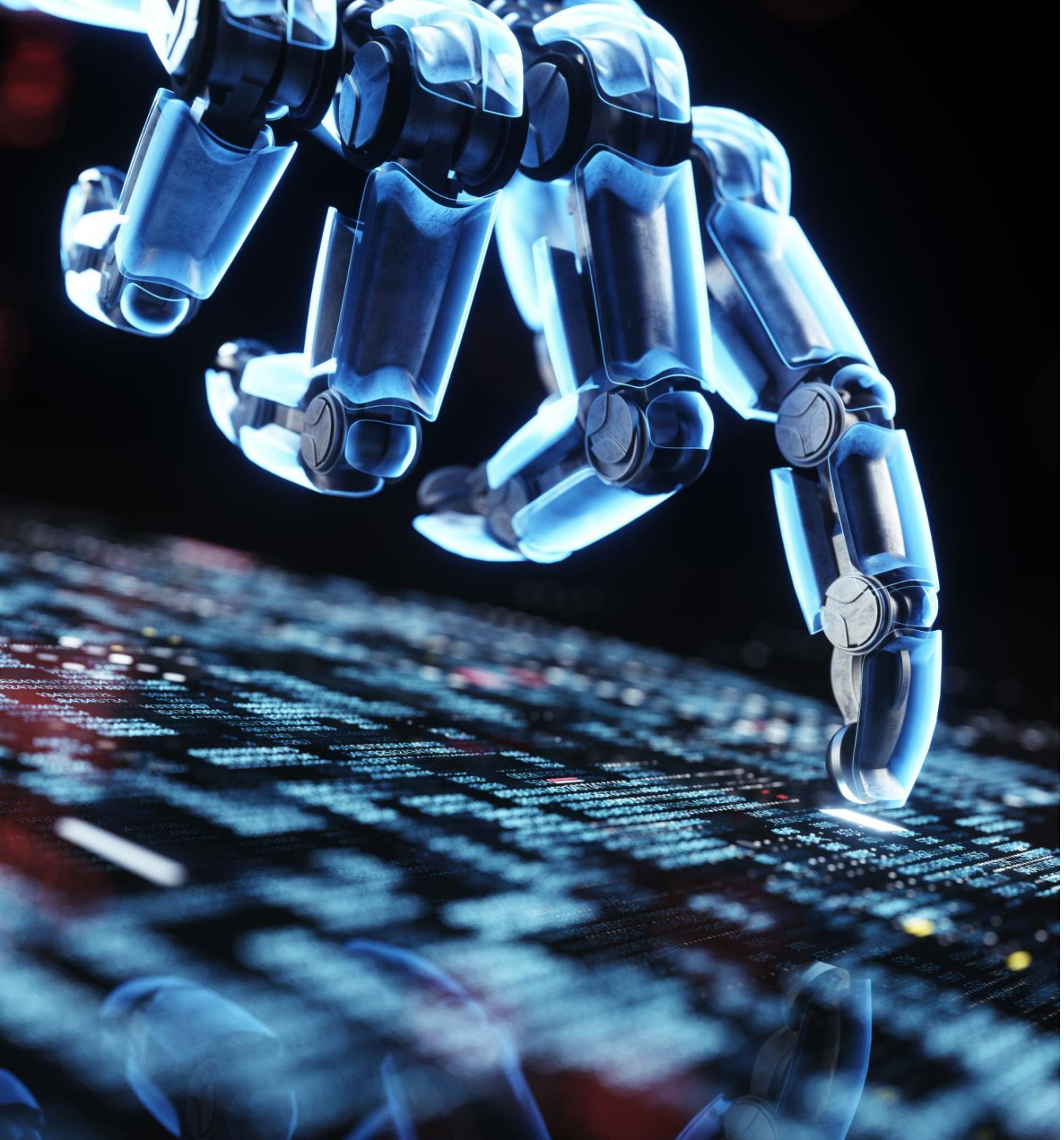
Very convincing campaigns and phishing attacks are launched to lure such users.

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



Get Cyber Insurance!

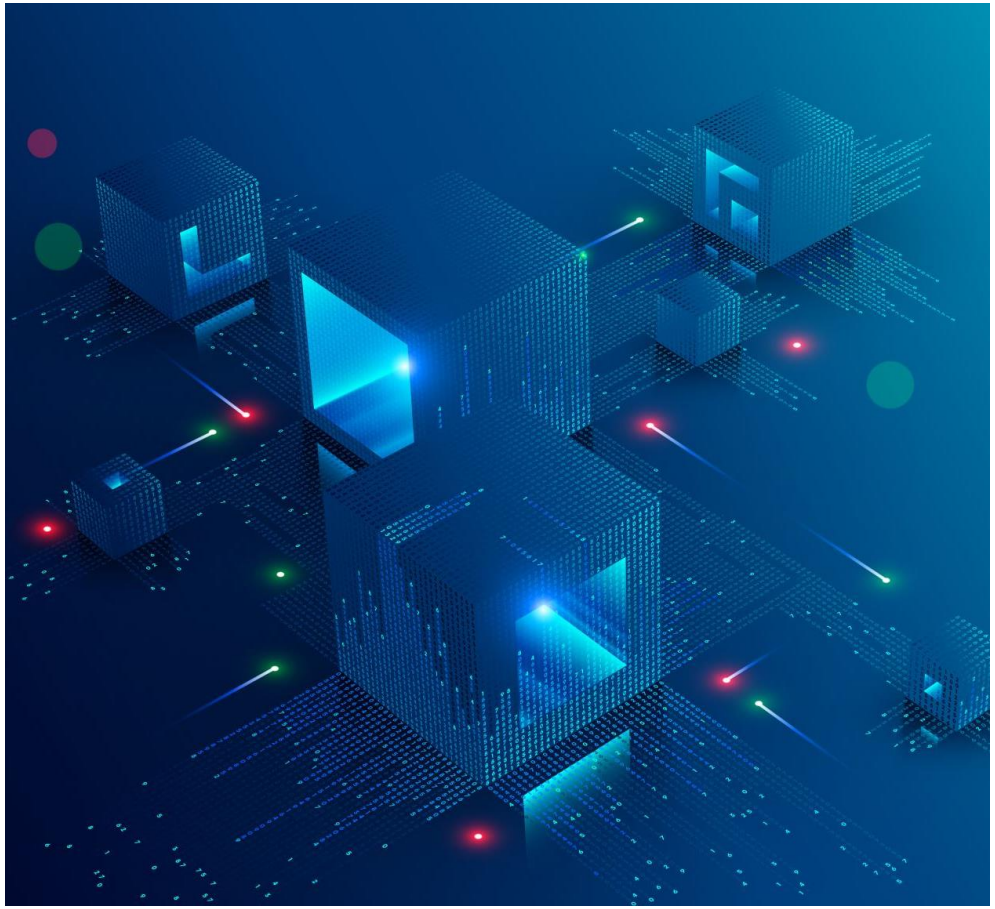
Cyber insurance help businesses hedge against the potentially devastating effects of cybercrimes such as malware, ransomware, distributed denial-of-service (DDoS) attacks, or any other method used to compromise a network and sensitive data



Use Emerging Technologies to bullet proof Cyber Security & Data Privacy

- Artificial intelligence (AI)
- Blockchain
- Quantum Computing & Cryptography

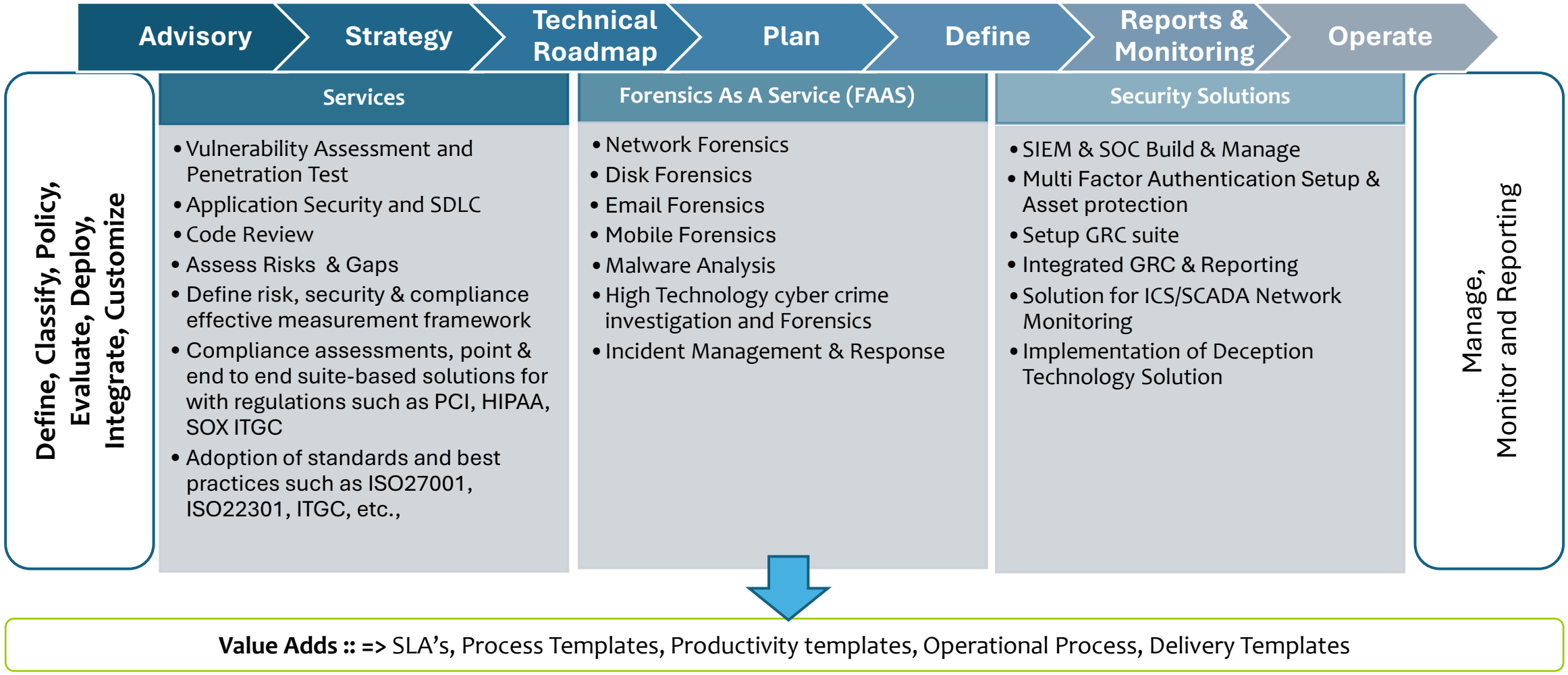
Cyber Security Essentials



Prediction, prevention, detection, resolution & protection from cyber attacks, breaches and threats

- Design & Architecture with a Zero Trust Approach
- Policy & Process consulting
- Audit & Assessment, VA-PT
- Firewalls, IDS, IPS, Anti Malware
- Multifactor Authentication
- Quantum Cryptography
- Data Leak prevention
- Information Rights Management
- Automated Configuration Management
- EDR,MDR, XDR, MDM
- Security Information Event Management (SIEM)
- Threat Intelligence & Security Analytics
- Managed Security Service

Cyber Security Landscape



Questions?

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