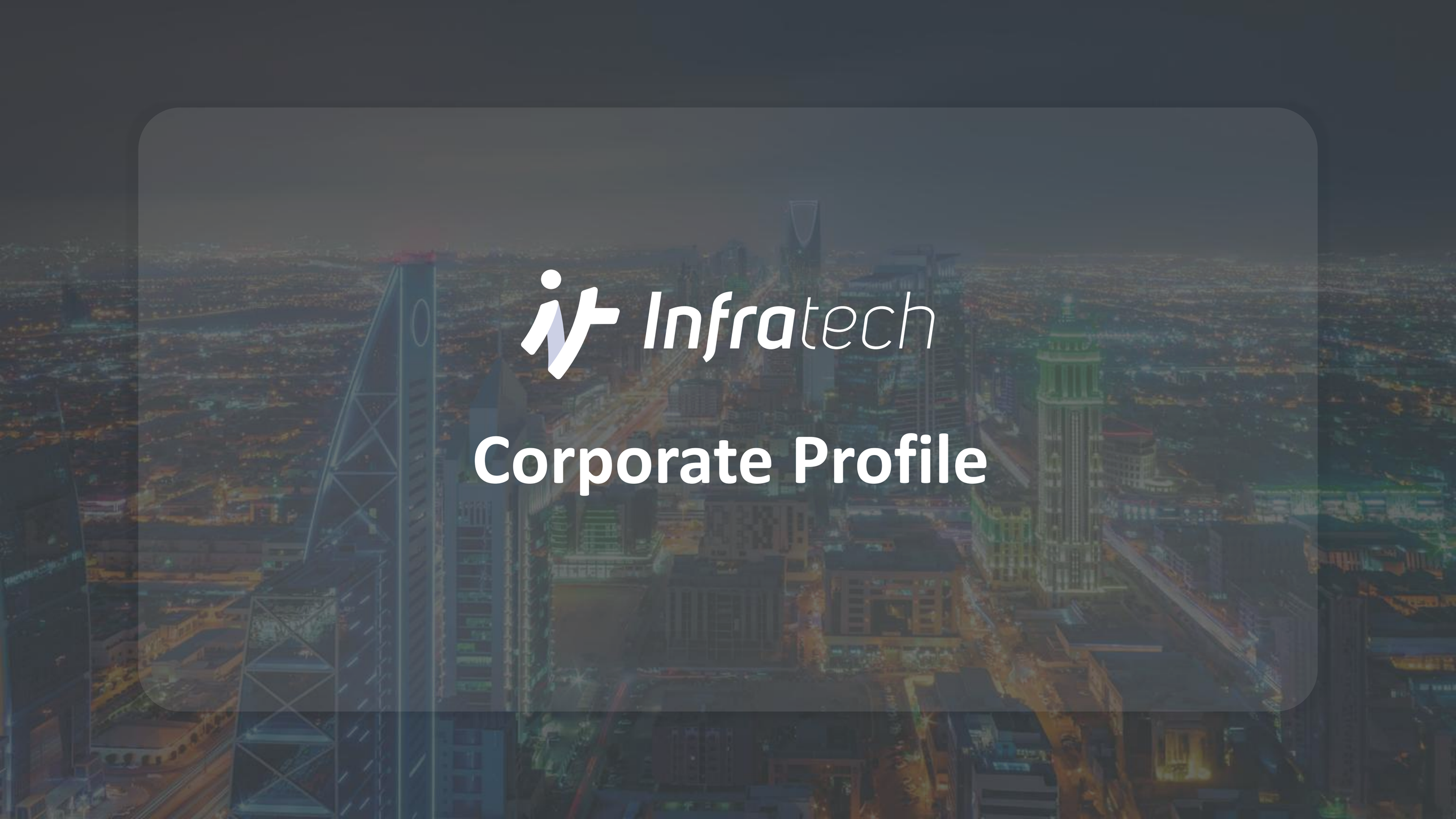
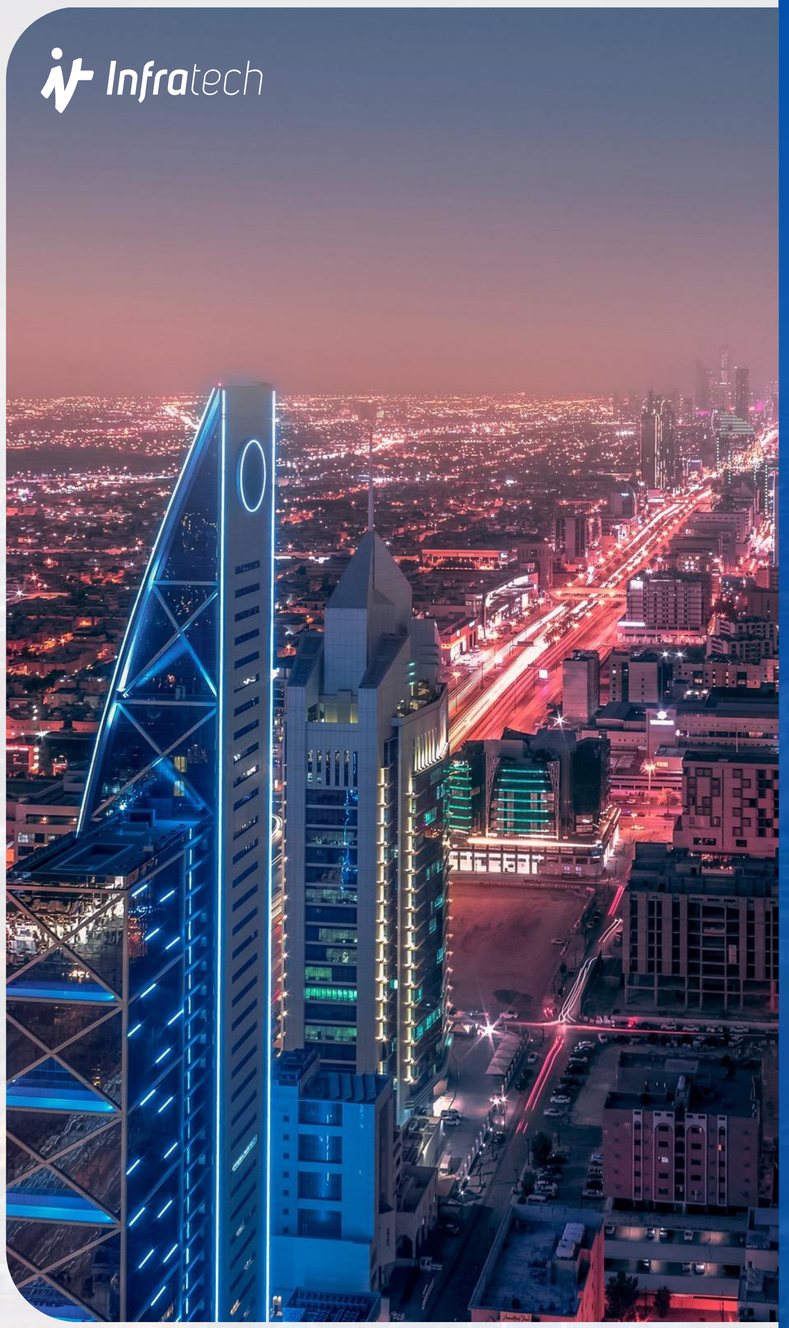


Infratech

Corporate Profile



CONTENT

Message from CEO

Technology is revolutionizing how consumers and businesses operate, enabling faster and better performance. Businesses that adapt quickly to these changes remain leaders, while slow adaptors lag far behind.

The MENA region, rich in human and natural resources, holds immense potential to improve lives through innovative technologies like Cyber security, Big data, AI, blockchain, IoT, and Fin-tech.

Infratech's mission is to empower the region with innovative integrated solutions, driving digital transformation to enhance KPIs, transparency, competitiveness, investments, and living standards. We continue to invest in technology and human capital to lead the region's technological revolution.

Ayman Al Suhaim
CEO

Who are we?

Infratech, based in Riyadh, Saudi Arabia, excels in information security, IT/OT infrastructure, and digital transformation, supported by a global team, R&D centers, and financial stability for seamless project delivery.

Trusted for its values of credibility, transparency, and customer focus, Infratech serves strategic clients across sectors like defense, oil & gas, health, telecom, and banking.

With solutions designed to global standards, Infratech ensures
efficiency, integration, and business alignment at the lowest total cost of ownership (TCO).

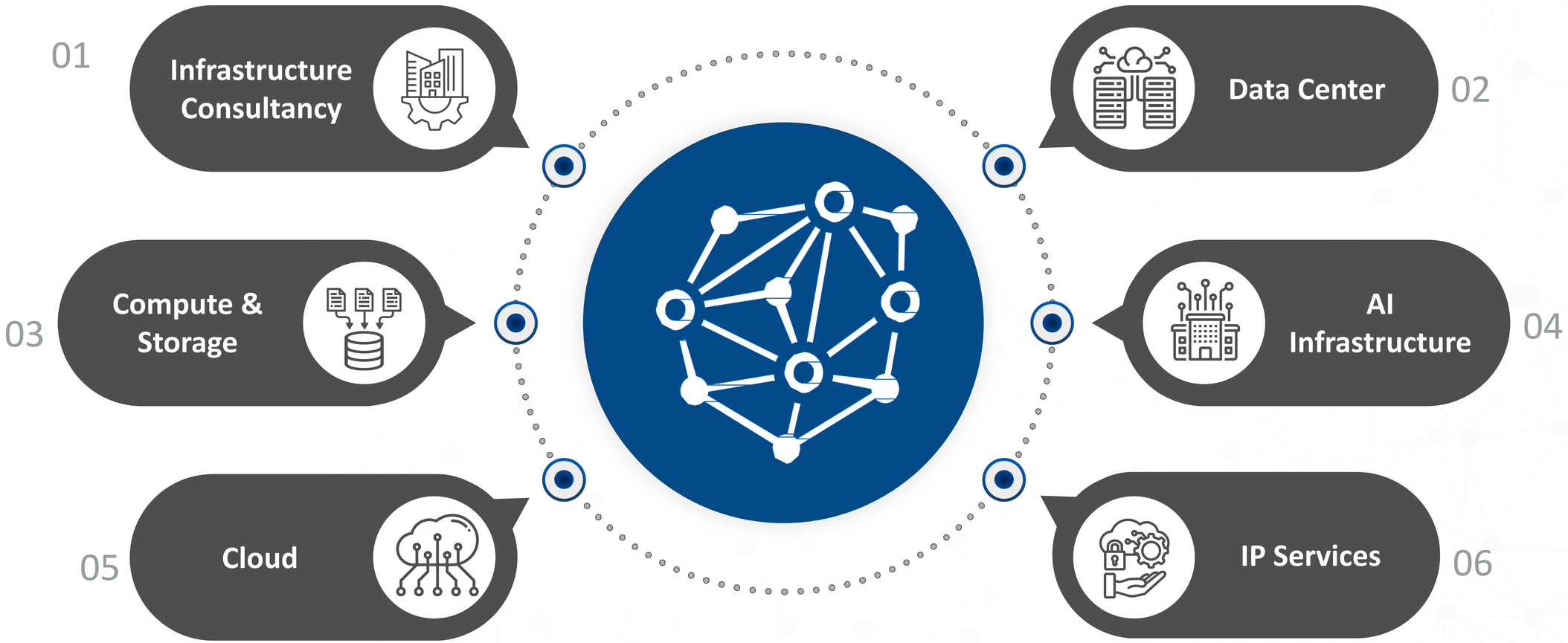
Some of our Clients

Some of our Clients

Infratech

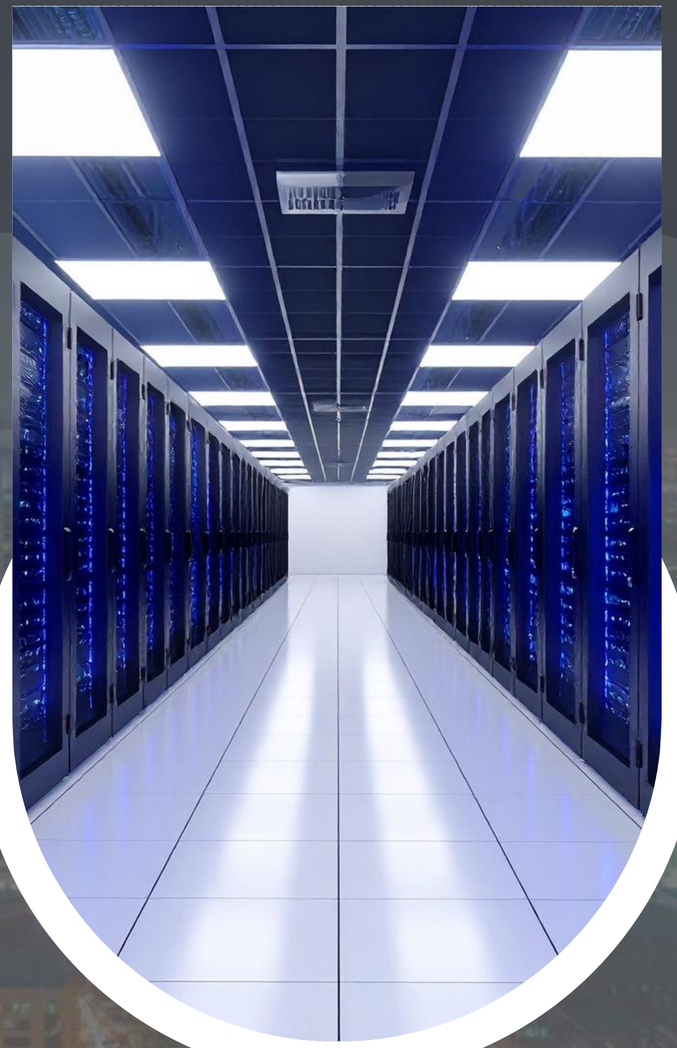
IT INFRASTRUCTURE

IT INFRASTRUCTURE



Infratech

INFRASTRUCTURE LOB MAIN PILLARS / OFFERING



Infrastructure LOB Main Pillars / Offering

DATA Center Preparation	Network & Network Security	Computing, Storage & Backup	Software	Low Current & Paaive	Co-location & Cloud Services	OT Infrastructure & OT Cyber Security
Cooling & Environmental Solutions	Wired & Wireless Networks	Servers & HCI	Virtualization	Copper & fiber Solutions	Co-location Services	Industrial Switches & Routers IP66/IP67
Power Solutions	SD-Networks & SASE	SAN & NAS Storage	Operation Systems	IPT & VC Solutions	Infratech Cloud Services	Industrial Wireless connectivity WIFI, P2P, P2MP, & LoRaWAN
Passive Solutions	NAC, NDR & Firewalls	Backup Solution & Backup Storage	Containers SW	IOT Solutions	Global Cloud Provider Servies	CS Solution Patch Management, FW, IPS, Asset Discovery, data diode , Remote Access, & backup
Monitoring & Management	Optical Networks	Super Computers & GPU	EDR	AV, CCTV & Access Control	SaaS & IaaS	
Compliance & Standards	Monitoring & Management	Monitoring & Management	Solution SW & Cloud Applications	BMS. Fire Fighting & Master Clock	Cloud Cyber Security Solution	OT GRC Services

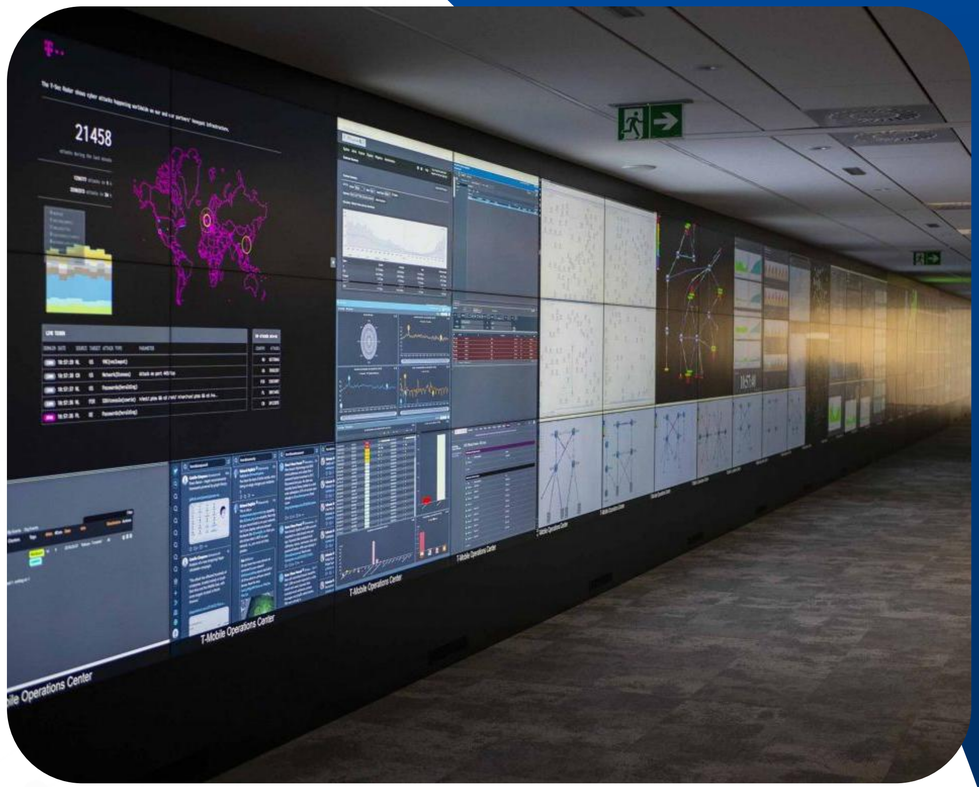
Infratech

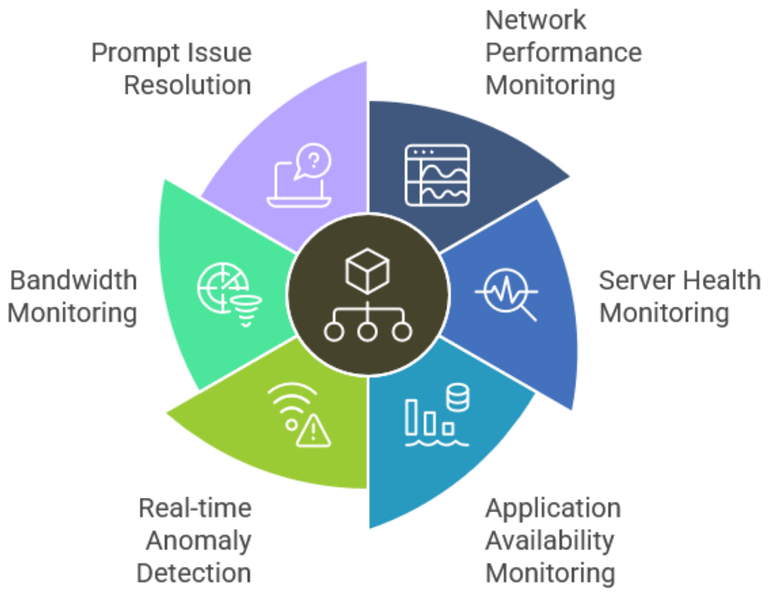
NOC SERVICES

What is a NOC responsible for?

A network operations center (NOC) is a centralized place from where our NOC team supervises, monitor and maintain a customers' network and IT infrastructure

- 24x7x365 network, application, servers monitoring
- Monitor any IT Device or application be it on-prem or on cloud
- First level of troubleshooting and resolution
- Proactive monitoring and taking action to prevent any potential network outage
- Uninterrupted network operations to ensure smooth business continuity.
- Faster network incident detection and response leading to minimized damage.
- Report on network performance and incidents.





“Our NOC is not just a reactive entity; it's a proactive partner that ensures our clients' IT infrastructure operates smoothly and securely. By proactively addressing issues, we minimize disruptions, enhance performance, and allow our clients to focus on their core business objectives."

Key Benefits of NOC Services

- **Proactive issue detection and resolution:** Minimizing downtime and business disruption.
- **Improved system performance and reliability:** Ensuring smooth operations.
- **24/7 support:** Providing continuous availability and peace of mind.
- **Reduced IT costs:** Preventing costly outages and optimizing resource utilization.
- **Focus on core business:** Allowing clients to concentrate on their strategic goals.

Infratech

CYBER SECURITY SERVICES

Cybersecurity Solutions – Summary

Unified Security Framework

Data & Information Security: DLP, DSPM, encryption, IRM, insider threat defense

Governance, Risk & Compliance: ISO/NIST alignment, regulatory adherence, TPRM

OT/IoT Security: ICS/SCADA visibility, segmentation, anomaly detection

Threat Management & SOC: SIEM, SOAR, threat intel, MDR, red teaming

Network Security: NGFW, segmentation, SWG/SEG, DDoS & DNS protection

Cryptography & Key Management: HSM, KMS, PKI, tokenization, FIPS-compliant controls

Application Security: Secure SDLC, DevSecOps, WAF/RASP, API protection

Endpoint Security: EDR/XDR, zero-trust access, vulnerability & mobile management

Cloud Security: CSPM, CWPP, CASB, SSE/SASE for multi-cloud governance

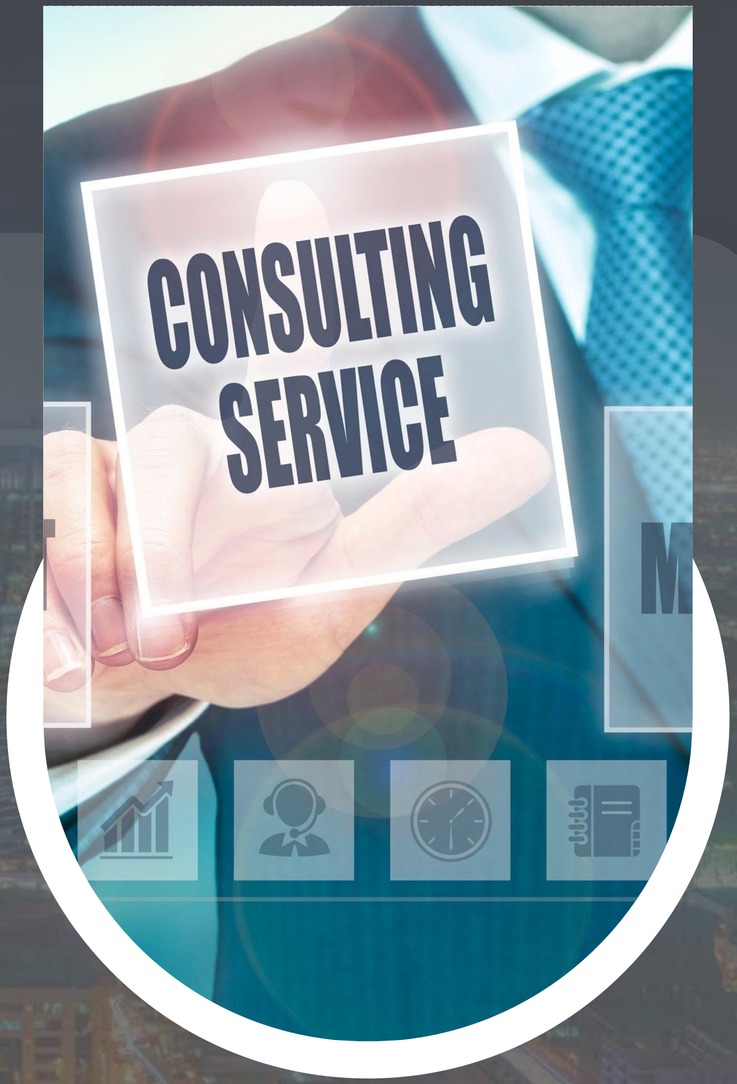
Identity & Access: MFA, SSO, PAM, IGA ensuring least privilege and adaptive control

OUTCOME:

A cohesive, adaptive, and compliant cybersecurity ecosystem enabling **resilient digital operations** and **business continuity**.

Infratech

CYBER GRC
CONSULTING SERVICES



CYBER GRC Consulting services

Governance

- Strategy & Roadmap Development
- CS Operating Model
- CS Policies, Standards, Procedures Development
- CS Awareness Program

Risk

- Cybersecurity Threat Profiling
- Risk Management Framework Development
- Risk Assessments
- Risk Register
- Risk Treatment Plans
- Data Protection & Privacy Assessments

Compliance

- Cybersecurity Maturity Assessment
- Unified Controls Frameworks Development
- Compliance Assessments and Implementation (NCA, SAMA, NDMO, PDPL, Aramco, SABIC, ISO, PCI etc.
- Pre-Audit and Compliance Readiness Checks

Design, Execute And Change

- NCA ECC-2
- NCA CSCC
- NCA CCC
- NCA TCC
- NCA OSMACC
- NCA DCC
- SAMA CSF
- SAMA ITGF
- SAMA CTIP
- SAMA CFF
- SAMA BCMF
- SAMA FEER
- PCI DSS
- NIST CSF
- ISO27001

Initial structure of unified cybersecurity control framework (uccf)

Meetings, information gathering, assessment for each control area

Capability & maturity analysis & reporting

IMPLEMENTATION ROADMAP

MONITORING & ENHANCEMENT

GOVERN → **STRATEGY** → **DESIGN** → **EXECUTE** → **CHANGE** → **ASSURE**

Infratech

OT/IOT SECURITY SERVICES

OT/IoT Cybersecurity Services

DETECT

Empower your industrial operations with our comprehensive suite of services and solutions, addressing key industry challenges.

OT/IoT Continuous Monitoring

24/7 monitoring of OT/ IoT networks and systems to detect and respond to threats in real-time.

OT Compliance

Navigate complex regulatory landscapes effortlessly with our tailored OT compliance services.

ICS Security Roadmap

Chart a clear path to ICS security excellence with our roadmap solutions.

IoT Remediation Complexity

Ensure robust and effective remediation strategies, safeguarding your network and maintaining operational continuity.

OT Cyber Threats

Defend against evolving OT cyber threats with our proactive defense strategies.

Cyber Security Solutions

Empower your OT systems with our cutting-edge cybersecurity solutions, ensuring your systems remain fortified against evolving threats.

OT/IoT Cybersecurity Services

Comprehensive Coverage from Identification to Recovery Our Services Ensure Your Needs Are Met

- Risk Assessment
- Asset Visibility
- Architecture Design & Review
- Regulatory Compliance
- Vulnerability Assessment
- Asset Inventory
- Configuration Review

- Consultancy
- Vulnerability Management
- Training & Awareness
- Asset Hardening
- Network Segmentation
- OT Penetration Testing

- Threat Detection
- SIEM
- OT SOC

- Table Top Exercise (TTX)
- Incident Response
- Digital Forensics

Infratech

NCA COMPLIANCE SERVICES

NCA Compliance Services

NCA Periodic Requirements:

→ Penetration testing
→ Vulnerability Assessments
→ Gap Assessment
→ Risk Assessments
→ Architecture Review
→ Configuration Review
→ IR Retainer
→ Tabletop Exercise
→ OT SOC - Security Monitoring

Infratech offers a range of periodic services designed to meet the requirements set forth by the National Cybersecurity Authority (NCA). These services are tailored to enhance your resilience against cyber threats while ensuring compliance with NCA regulations.

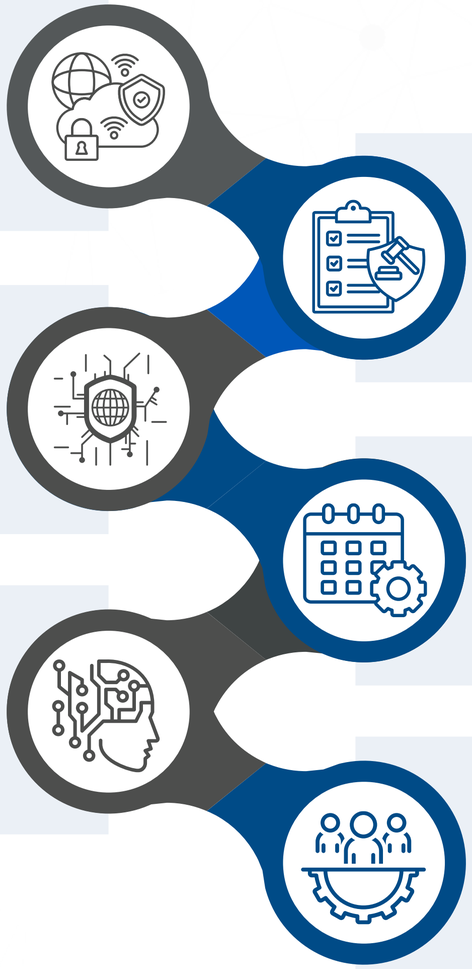
OT / IoT Cybersecurity Offering

How Infratech Can Empower Your Cybersecurity Journey

Infratech Security Services
Infratech partners with customers throughout their OT/IoT security journeys, offering comprehensive services from the Identify phase to the Recover phase.

OT/IoT Cybersecurity Solutions
Infratech offers cutting-edge solutions tailored to meet your needs, including advanced threat detection, Secure Remote Access, SIEM, Data Diodes, Industrial Patch management etc..

OT & IoT Threat Intelligence
Enable threat-informed defense with information about threats and advisories for your sector.



NCA Compliance Services
Infratech offers a range of periodic services designed to meet the requirements set forth by the National Cybersecurity Authority (NCA).

Preventive maintenance
Enhance the resilience and security of your operational technology with our vendor-grade OT cybersecurity preventative maintenance services.

Staff Augmentation
Boost your operational efficiency with our expert staff augmentation services, providing highly skilled professionals who seamlessly integrate into your team.

Infratech

MANAGED SECURITY SERVICES (MSSP)

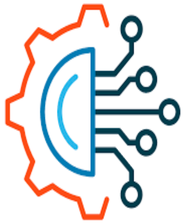
MDR Services

SOC monitoring

SIEM implementation /operation

TH/TI

DFIR



Automation

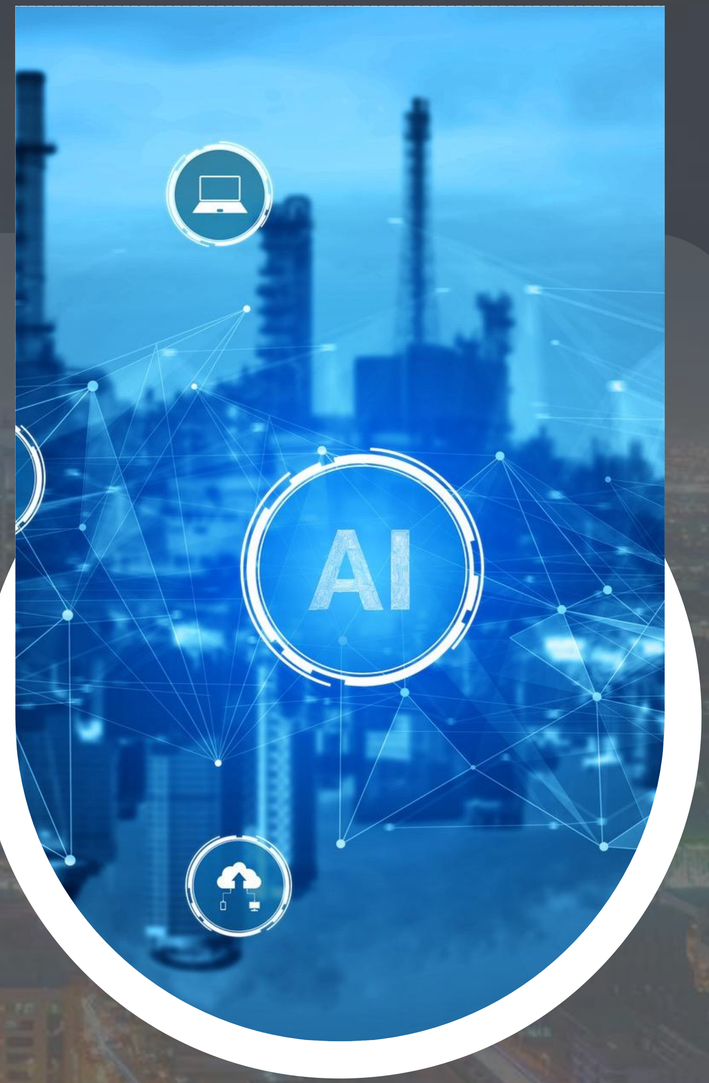
Compromise assessment

Phishing simulation and awareness

Security Administrator

Infratech

SOC AS A SERVICE BUSINESS MODELS



Three Business Models

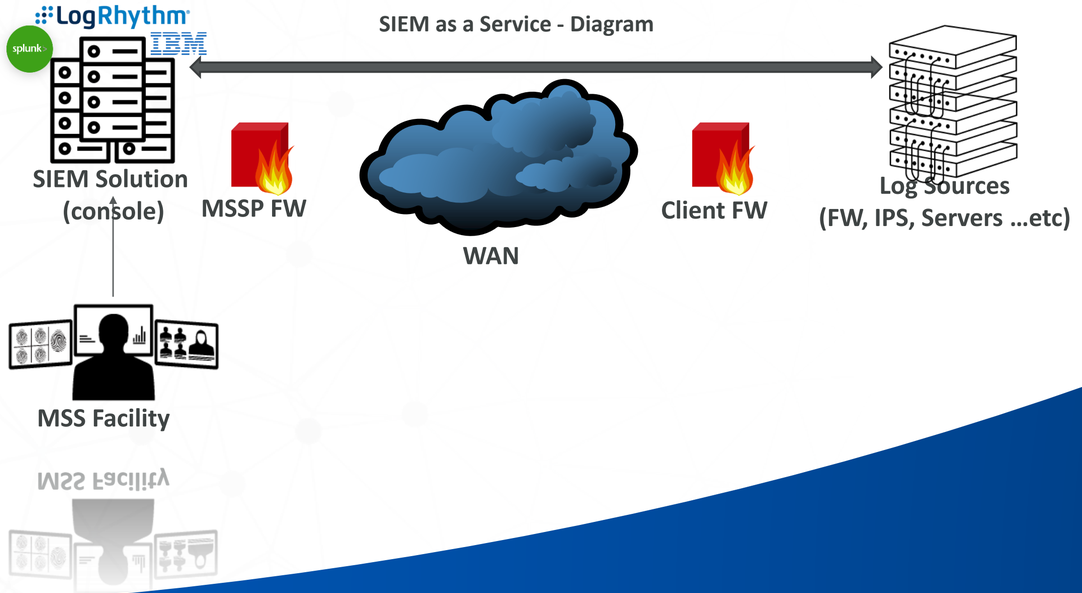
	Full Remote Resources Model (Shared)	Full Remote Resources Model (Dedicated)	Hybrid Model (Onsite Resources + Remote Resources)
SLA	MSSP SLA applied	Dedicated SLA	MSSP SLA applied (Agreed on with Client)
Resolution Time	Remediation Done by Client Teams	Remediation Done by Our Team	Remediation Done by Onsite Team
Resource Management	Resource Selection/Management Totally by MSSP	Resources Selection with the support of Client if required	Partial Selection/Management by Client for Onsite Resources

** Infratech SOC Team provides detailed incident ticket includes recommendation and all details*

Connection from MSSP to Clients (SIEM as a Service)

Second Connection Model:

- At each client they will have collectors to collect logs/flows from log sources
- SIEM solution on different tenant will be implemented at cloud.
- Collectors will send logs to SIEM through WAN
- Analysts from MSSP, will get an access to only SIEM solution servers (Console)



Pros	Cons
GUI is extremely fast	Huge traffic over WAN (In Megabytes/Gigabytes)
Stability as per the SLA between MSSP & Client with their ISP (internet Service Provider)	Logs are stored at cloud
In Case WAN is down: Logs that not delivered to SIEM will be stored locally till connectivity is back again	

RPA automation

Build and deliver innovative process automation to Reduce the SLA and automate the SOC operation

Mission

Automate the full MDR service process

Vision

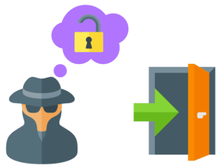
Infratech

OFFENSIVE CYBER SECURITY

What we do !

Offensive security services catalogue !

Vulnerability Assessments	Penetration Testing	Vulnerability & Attack Surface Management	Red-Teaming Assessment	Purple-Teaming Assessment
				

Config review & Benchmarking	Physical Security Assessment	Compromise Assessment (Threat Hunting)	Breach-Attack Simulation(BAS)	Source Code Review (SAST + DAST+SCA)
				

Our Services Offering

A full-fledged end-end technologies testing capabilities

APPLICATION PENTESTING
- Web Application
- Mobile Application
- Thick Application
- Virtual Application
- API

NETWORK PENTESTING
- Internal Network
- External Network
- Wireless Network
- Host-Based
- Mainframe

CLOUD PENTESTING
- AWS
- Azure
- Google Cloud
- Kubernetes

IOT PENTESTING
- ATM
- Automotive
- Medical Device
- OT
- Embedded

BLOCKCHAIN PENTESTING
- Private, Public, Hybrid, Permissioned, Consortia
- Consensys, Codefi, R3 Corda, Hyperledger Fabric, and more!

SOCIAL ENGINEERING
- Phishing
- Vishing
- Physical Pentest
- On-Site Assessment

RED TEAM
- Assumed Breach
- Black Box

STRATEGIC ADVISORY
- Security Assessment
- Threat Modeling
- Benchmarking & Config Review

SECURE CODE REVIEW
- SAST & SCA
- DAST

Purple TEAM
- Attack-Defense exercise.
- Detective controls validation

Vulnerability Management
- Vulnerability Management implementations.
- Vulnerability Management operations.

Compromise Assessment
- Threat Hunting.

BREACH & ATTACK SIMULATION
BREACH & ATTACK SIMULATION PLATFORM
- Continuous Detective Control Testing at Scale
- Build Customized Procedures
- Track & trend security posture over time
- Map to MITRE ATT&CK framework
- Industry benchmark

ATTACK SURFACE MANAGEMENT
ATTACK SURFACE MANAGEMENT PLATFORM
- Continuous Testing
- Identify Unknown Assets
- Evaluate Risk of Exposures
- Manual Exposure Triaging

CYBER WARFARE TRAINING
DARK SIDE OPS
- Malware Dev
- Adversary Simulation

Infratech

DIGITAL TRANSFORMATION

Digital Transformation

01

IOT
“Internet of things”

02

AI & Cognitive
Decision Making

03

Legacy System
Modernization

04

Customer Experience
Consultancy

05

Blockchain

06

Big Data &
Data Analytics

07

Digital Transformation
Consultation

Partners


f5
vmware
Entrust Datacard
VECTRA
MSAB
LogRhythm
The Security Intelligence Company
kaspersky
Netwrix Auditor
Akamai
Recorded Future
IBM
Gold Partner
TREND MICRO
Trellix
LINKSHADOW
BeyondTrust
Belkasoft
forensics made easier
arcon
paloalto NETWORKS
FORTINET
DELL
SentinelOne
CISCO
opentext
X-Ways
FORCEPOINT
ManageEngine
hp
COMMVAULT
SailPoint
MAGNET FORENSICS
splunk>
BROADCOM
Digital Intelligence
ACCESSDATA
CYBER RANGES
nexthink
change your perspective
Infoblox
THALES
TEELtechnologies
Vound Intella
Delinea
Qualys
NETSCOUT
CUBIC
MotionDSP
COFENSE
AMPED FIVE
ivanti
KnowBe4
Human error. Conquered.
OXYGEN FORENSICS
ExtraHop
ZIMPERIUM
NUTANIX
OPSWAT.
ANOMALI

THANK YOU!

infratech.com.sa

7266 Uthman Ibn Affan Rd - At Taawun,
Riyadh 12476 - 4407, Kingdom of Saudi Arabia

+966 92 000 9988