

INSIDE Cybersecurity in realm of AI

AUTOMATION • ARTIFICIAL INTELLIGENCE • CLOUD

# Enterprise

## CHANNELS

### MEA

PAGES 68  
VOLUME 11 | ISSUE 09  
APRIL 2024  
WWW.EC-MEA.COM

ENTERPRISE SOLUTIONS ADVISORY FOR CHANNEL PARTNERS



**TRUST BUT  
VERIFY**

As our reliance on digital technologies grows, the synergy between AI and cybersecurity becomes increasingly critical

#ZeroTrust

GLOBAL  
CISO  
FORUM



PRESENTS



POWERED BY



16 APRIL - **UAE** | 17 APRIL - **PAKISTAN**  
18 APRIL - **KSA** | 22 APRIL - **QATAR**  
APRIL - **EU** | APRIL - **US**



BROUGHT TO YOU BY

**GEC  
MEDIA  
GROUP**

OFFICIAL MEDIA PARTNERS

**CYBER SENTINELS**

**Enterprise**  
CHANNELS MEA

**BUSINESS  
TRANSFORMATION**



Dear Readers,

**I**n this issue of the Enterprise Channels Magazine, we are focussing on cybersecurity in realm of AI. With AI technology experiencing an explosive surge across various sectors, it's not just revolutionizing industries but also fundamentally altering how we approach cybersecurity.

However, this AI revolution isn't without its challenges. As AI becomes more sophisticated, so too do the cyber threats it can enable. From the proliferation of convincing deepfakes to the emergence of AI-powered cyberattacks, the landscape of digital security is constantly evolving.

To tackle this issue, We've assembled a treasure trove of insights and expertise from top industry leaders to guide you through this complex landscape. Whether you're a seasoned cybersecurity professional or just beginning to navigate these waters, our coverage offers something for everyone.

And that's not all! This month boasts not one, but two major events that are essential for anyone concerned about cybersecurity. First up is the Global Security Symposium on April 16th, where experts will convene to share cutting-edge strategies for protecting digital assets. Following closely is the highly anticipated GISEC 2024 from April 23rd to 25th, offering a prime opportunity to connect with leaders in the field and stay abreast of the latest developments.

So, stay tuned as we unpack the latest trends, provide actionable tips, and arm you with the knowledge you need to safeguard yourself and your organization in this exciting yet challenging era of AI-driven cybersecurity.

**RONAK SAMANTARAY**

ronak@gecmediagroup.com

**PUBLISHER**

TUSHAR SAHOO  
tushar@gecmediagroup.com

**CO-FOUNDER & CEO**

RONAK SAMANTARAY  
ronak@gecmediagroup.com

**GLOBAL HEAD, CONTENT  
AND STRATEGIC ALLIANCES**

ANUSHREE DIXIT  
anushree@gecmediagroup.com

**ASSISTANT EDITORS**

SEHRISH TARIQ  
sehrish@gecmediagroup.com

**GROUP SALES HEAD**

RICHA S  
richa@gecmediagroup.com

**PROJECT LEAD**

JENNEFER LORRAINE MENDOZA  
jennefer@gecmediagroup.com

**SALES AND ADVERTISING**

RONAK SAMANTARAY  
ronak@gecmediagroup.com  
Phone: + 971 555 120 490

**Content Writer**

KUMARI AMBIKA

**IT MANAGER**

VIJAY BAKSHI

**DESIGN TEAM**

**CREATIVE LEAD**

AJAY ARYA

**SENIOR DESIGNER**

SHADAB KHAN

**GRAPHIC DESIGNERS**

JITESH KUMAR  
SEJAL SHUKLA

**PRODUCTION, CIRCULATION, SUBSCRIPTIONS**

info@gecmediagroup.com

**DESIGNED BY**



**SUBSCRIPTIONS**

info@gecmediagroup.com

**PRINTED BY**

Al Ghurair Printing & Publishing LLC.  
Masafi Compound, Satwa, P.O.Box: 5613,  
Dubai, UAE

**GEC  
MEDIA  
GROUP**

**(UAE)** Office No #115  
First Floor , G2 Building  
Dubai Production City  
Dubai, United Arab Emirates  
Phone : +971 4 564 8684

**(USA)** 31 FOXTAIL LAN,  
MONMOUTH JUNCTION,  
NJ - 08852  
UNITED STATES OF AMERICA  
Phone :+ 1 732 794 5918

**A PUBLICATION LICENSED BY**

International Media Production Zone, Dubai, UAE  
©copyright 2013 Accent Infomedia. All rights reserved.  
while the publishers have made every effort to ensure the  
accuracy of all information in this magazine, they will not be  
held responsible for any errors therein.





TRANSFORMATION IN  
**SECURITY**

TRANSFORMATION IN  
**NETWORKING**

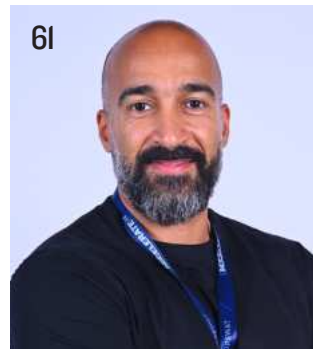
TRANSFORMATION IN  
**BUSINESS APPLICATIONS**

TRANSFORMATION IN  
**IT & COMPUTING**

02 MAY - **UAE**

09 MAY - **KSA**

# CONTENTS



03  
EDITORIAL

23-26  
CHANNEL

37-63  
GUEST COLUMN

06-18  
EVENTS

27-31  
REAL LIFE

64-65  
SOCIALLY SPEAKING

19-22  
VIEWPOINT

32  
PRODUCTS



# Successful conclusion of the women leadership symposium

**G**EC Media Group is thrilled to announce the successful conclusion of the second edition of the Women Leadership Symposium. Held on 7th of March the symposium brought together industry leaders, professionals, and aspiring individuals for a day of celebration, inspiration, and authentic conversations.

## Celebrating Women's Achievements in Leadership

The Women Leadership Symposium served

as a platform to celebrate the remarkable achievements of women in leadership roles across the tech, business, and marketing industries. Attendees were inspired by the diverse contributions of women leaders and gained valuable insights into the challenges and opportunities facing women in the workforce.

## Confronting the “Elephant in the Room”

One of the highlights of the symposium was the discussion on embracing difficult conversations and addressing the “elephant in the room.”

Through open and honest dialogue, attendees explored sensitive topics and learned strategies for fostering authenticity, trust, and collaboration in the workplace.

## Empowering Authentic Leadership

Authenticity emerged as a central theme throughout the symposium, with speakers emphasizing the importance of genuine interactions, vulnerability, and courage in leadership roles. By embracing authenticity, attendees were empowered to lead with integrity,





inspire their teams, and drive positive change within their organizations.

### Various Panel Discussions included

**Women Driving Innovation in Technology: Insights from the Women Leadership Symposium**  
The panel discussion was expertly moderated by Somy Varghese, a prominent advocate for women's empowerment and Head of Digital Transformation & Technology. With her insightful questions and engaging facilitation, Somy guided the conversation towards exploring the challenges and opportunities faced by women in the tech industry.

### Panelists

1. K.U Shankri | Managing Director,

2. Luckystar Computer LLC
2. May El Barachi | Director of Computer Science and IT, University of Wollongong in Dubai
3. Sona Saha Das | Head - Data Strategy and Governance, M.H Alshaya Co.
4. Pragyan Priyadarshani | CTO, Landmark Group
5. Oma Martins | Associate Director and Head, IT GRC, IHS Towers

### Insights and Perspectives

Throughout the discussion, panelists shared their personal experiences, insights, and strategies for driving innovation in technology. From leveraging data and technology for business transformation to fostering a culture of diversity and inclusion, the panelists provided valuable

perspectives on how women are leading the way in shaping the future of technology.

### Women in Communication and Marketing Leadership

The panel discussion was skillfully moderated by Aisha Abdalla Al Marzooqi, a distinguished Corporate Communication Expert. With her deep industry knowledge and insightful questioning, Aisha guided the conversation towards exploring the challenges and opportunities faced by women in communication and marketing leadership roles.

Panelists:

1. Vidya Subramanian | Senior Marketing Specialist, Amiviz
2. Dhvani Sejpal | VP Treasury



- Transformations, Finesse Global
3. Hima Karanath Renandranadhan | Head of Sales and Marketing, Sudo Consultants
4. Sandy Issa | Marketing Manager Middle East at ISS, Intelligent Security Systems
5. Sonal Dawda | Head of Marketing & Corporate Communications, Dubai National Insurance & Reinsurance P.S.C

### Insights and Perspectives

Throughout the discussion, panelists shared valuable insights and experiences from their diverse backgrounds in communication and marketing leadership. From leveraging digital platforms for brand engagement to navigating cultural nuances in global marketing campaigns, the panelists provided invaluable perspectives on how women are driving innovation and excellence in their respective roles.

### Building a Supportive Ecosystem for Women Entrepreneurs

The panel discussion was moderated by Sheeba Hasnain, a respected Chairperson and Chief Information Officer. With her insightful questions and facilitation, Sheeba guided the conversation towards exploring strategies for building a supportive ecosystem that empowers women entrepreneurs to succeed.

### Panelists

1. Dr. Mary Jane Alvero | Group Chief Executive Officer, Prime Group
2. Tatiana Novikova-Yamshchikova | CEO, Xiongmao Digital. The Leading China E-commerce Solution in UAE
3. Nataliia Kobzar | CEO | Skin Coach
4. Yasmin Juma Almheiri | Doctor in Social Relationships at Workplace, ADNOC
5. Chada El Islam Benmahcene | CEO & Founder, ENTROGX Ventures

### Insights and Strategies for Success

Throughout the discussion, panelists shared valuable insights and strategies for creating a supportive ecosystem for women entrepreneurs. From providing access to mentorship and funding opportunities to fostering a culture of collaboration and inclusivity, the panelists highlighted the importance of addressing the unique challenges faced by women in entrepreneurship.

### Gratitude to Our Partners and Attendees

We extend our heartfelt gratitude to our partners, sponsors, speakers, and attendees for their unwavering support and participation in making the Women Leadership Symposium a resounding success. Your commitment to diversity, inclusion, and empowerment has truly made a difference, and we are grateful for your contributions. 🏡





## DRIVING OPERATIONS AND PERFORMANCE EXCELLENCE

YOUR PARTNER FOR



Cloud & Digital  
Transformation



Enterprise  
Applications



Analytics &  
Automation AI &  
ML as a Service



Cyber  
Security  
Solutions



Management Consulting,  
Advisory and Quality Assurance

An unit of



“Delivery centres in US, Middle East and India”

# Leap 2024 breaks its own record with 215,000 visitors, 25% jump in YoY attendance



**L**EAP 2024, the four-day technology conference and exhibition in Riyadh, shattered its attendance records after organisers Tahaluf revealed more than 215,000 visitors descended on Riyadh Exhibition and Convention Centre in Malham for this year's event – surpassing the attendance figure of Glastonbury festival.

Already the world's most-attended technology event, LEAP 2024 witnessed a staggering 25 per cent year-on-year rise in visitors – up from 172,000 last year – to further consolidate the Kingdom of Saudi Arabia's world-leading status as a game-changing accelerator propelling the global technology ecosystem.

And with more than US\$14 billion in public and private sector technology sector investments and collaborations announced on-event this year, the long-lasting impact of LEAP – known as the 'Digital Davos' – will significantly boost domestic technology infrastructure and propel multi-vertical upskilling and talent incubation opportunities for the country's youth in support of Saudi Vision 2030.

Speaking at the event's closing ceremony, His Excellency Faisal Al Khamisi, Chairman of Saudi Federation for Cybersecurity, Programming and Drones (SAFCSP), said: "LEAP 2024 has provided over US\$ 500m in economic impact to Saudi Arabia. Of course, none of this would have been possible without the visionary leadership of HRH Crown Prince and Prime Minister Prince Mohammed bin Salman."

Michael Champion, CEO of Tahaluf – the strategic joint venture

between Informa, the Events Investment Fund, and SAFCSP, which organises LEAP alongside Saudi's Ministry of Communications and Information Technology, added: "The world has spoken, and the volume is deafening. With a 25 per cent year-on-year increase in footfall, LEAP is playing a critical role in enabling and propelling Saudi Arabia's position as the world's undisputed accelerator for holistic technology sector transformation.

"From blockbuster double-digit billion-dollar investments to pioneering technologies, products, and services that are fast-tracking the wholesale adoption of Generative AI, deep tech, and an array of associated verticals across every industry imaginable, LEAP 2024 is the living embodiment of the unparalleled vision and scale of Saudi Arabia's technology sector ambitions," added Champion.

During LEAP 2024's closing ceremony, Champion, who announced LEAP 2025 will take place from 10-13 February at Riyadh Exhibition and Convention Centre in Malham, promised an even larger event next year.

"We are already finalising plans to expand LEAP into Riyadh city centre next year with a new LEAP NIGHTS concept, with more than 100 major activations by the world's largest tech brands and leading Saudi entities," added Champion. "With Saudi Arabia recently announcing it has already achieved its aim of attracting 100 million tourists, we're not stopping at the event's show floor – we want LEAP to contribute to the multi-faceted magnetism of this dynamic country." 🏹

# STC GROUP announces partnerships at LEAP including Oracle Alloy, Cisco, Huawei, Ericsson physical esport



**S**tc Group, a global leader in digital transformation, successfully concluded its participation in LEAP 2024, the world's most-attended tech event, as its primary strategic partner and exhibitor.

At the event, stc Group reaffirmed its commitment to digital innovation beyond connectivity, by demonstrating advanced technological solutions in health, logistics, megaprojects and sports. The Group also showcased its expanding scale and scope through announcing strategic agreements and partnerships with some of the most prominent actors in the industry, including:

- **Oracle Alloy:** stc Group announced a new sovereign cloud platform offering more than 100 Oracle cloud services to support enterprises in capitalizing on hyperscale cloud services, while addressing data residency and data sovereignty requirements.
- **Ericsson:** The partnership showcased the world's first physical esport "HADO", combining (AR) and physical movement, to highlight the potential of 5G technology and cloud gaming.
- **Huawei:** Propelling stc Group's growth ambitions this strategic alliance focuses on developing new business portfolios underpinned by trailblazing solutions in fintech and app development.
- **GalaxySpace:** The collaboration will see the two companies explore the building of a space-to-ground integrated network. Both parties will also cooperate on Non-Terrestrial Networks

(NTN), exploring direct-to-device satellite technologies.

- **Bolttech:** the partnership will explore embedding IoT-enabled solutions beyond mobile devices into other aspects of a customer's digital lifestyle, including protection for home appliances, health electronics, and cyber assets
- **Cisco:** stc and Cisco signed multiple agreements with Cisco to modernize and unify its existing Network Operations Center (NOC) and to elevate stc Academy services such as participating in knowledge sharing and developing learning programs.

Locally, stc Group has multiple strategic agreements including PSDSARC, Prince Sultan Center for Defence Studies to instill digital thinking and develop analytical capabilities, an Air to Ground agreement with Flynas and Skyfive which seeks to equip Flynas's entire A320 fleet of 120 aircraft with advanced A2G solutions, offering passengers seamless access to in-flight Wi-Fi services. stc Group is planning to roll out the A2G network for specific flight routes across Saudi Arabia starting in 2024.

During the event, stc Group presented a wide array of remarkable exhibitions, promoting an impressive and thriving technological ecosystem. The Digital Stadium showcase conveyed the future of sports stadiums and optimized fan experiences through 360 camera views, its state-of-the-art command control centers, and remote clinics. 🏏



# ACES, Aramco Digital announce deals at LEAP 2024, multiple partnerships are signed



**Bryan Harris,**  
CEO, TikTok

**L** EAP 2024, the world's most attended technology event, continued its trailblazing transformational impact on the global technology ecosystem as numerous local and international technology companies recommitted their dedication to Saudi Arabia as the regional hub for technology and innovation with more than US\$ 764 million in ongoing investments.

The deals were headlined by Advanced Communications & Electronic Systems (ACES), a Saudi-based ICT solution provider and equipment innovator, which announced it would invest US\$ 618 million to localise special GSM and smart towers as part of its ambitions to expand operations and infrastructure equipment development and innovation.

Elsewhere, Aramco Digital announced a US\$ 46 million collaboration with LTIMindtree, a global technology consulting and digital solutions company based in India, to establish an information technology services hub in Saudi Arabia, while Chinese consumer electronics brand HONOR announced regional expansion plans with an investment of US\$ 100 million.

Revealed on the penultimate day of the event, which is taking place at Riyadh Exhibition & Convention Centre in Malham, the new announcements ensure on-event investment commitments now exceeds US\$ 13.5 billion

## **TikTok CEO: AI will Benefit Future Content Creators and Moderation Efficiency**

In a lively fireside chat that drew a capacity audience at LEAP 2024's Main Stage, Shou Chew, the enigmatic CEO of TikTok, announced the platform – which now has more than one billion monthly users – reiterating the company's support for over 175,000 small businesses in the Kingdom across a wide range of industries.

## **Investments for Good: When Profit Meets Potential**

Speaking on LEAP 2024's Main Stage, HRH Prince Khaled bin Alwaleed bin Talal Al Saud, the Founder & CEO of KBW Ventures, outlined the importance of balancing profit-first investment approaches with the transformative potential of VC funds to propel technology-driven innovations that will help solve the critical challenges facing humanity.

## **Seedford Partners Announces First-Ever Saudi Space Fund**

LEAP 2024's status as propellant for Saudi Arabia's blossoming space industry has been further enhanced by Seedford Partners, a leading international VC firm run specialising in Deep Tech investments, announcing the establishment of the country's first-ever private investment fund.

With a decade-plus track record in space technology startup investments, Seedford's portfolio includes Axiom Space, Voyager Space, SpaceX, Elroy Air, Skydweller, and numerous other space . 🔴

# LEAP records \$11.9 B new investments from AWS, Datavolt, IBM, Dell and Datadog



**L**EAP 2024, the world's most attended global technology conference, unveiled a massive US\$11.9 billion in new investments to support deep and emerging technologies, innovation, and cloud computing in Saudi Arabia and worldwide.

The investments further consolidate the Kingdom's position as the largest market and digital economy in the Middle East and North Africa (MENA) for leading technology companies, such as Amazon Web Services (AWS), IBM, DataVOLT and ServiceNow. The investments will also go to developing Saudi digital skills and supporting tech start-ups.

HE Eng Abdullah Alswaha, the Saudi Minister of Communications and Information Technology (MCIT), announced the record value of investments on the opening day of LEAP 2024's four-day run at Riyadh Exhibition & Convention Centre in Malham. The event ends on March 7, with expectations the third annual instalment will surpass its own record attendance of 172,000 visitors, set in 2023.

Minister Alswaha also highlighted the unwavering support that

HRH Crown Prince and Prime Minister Mohammed bin Salman has provided for the Saudi and global tech sectors and for the growth and prosperity of the digital economy, as part of the Kingdom's Vision 2030. The investments are part of the Crown Prince's empowerment of Saudi's burgeoning technology sector amid unprecedented growth in the country's digital economy, Generative AI, biological and healthtech, quantitative science, space, satellites, fintech, and open sources.

## LEAP 2024 Record Investments

On the first day of LEAP 2024, AWS announced a US\$5.3 billion investment in a new cloud zone in Saudi Arabia. Datavolt also announced a US\$5 billion investment for new data centres in the Kingdom with a capacity of more than 300 megawatts.

IBM plans to invest US\$250 million for a global software development centre in the Kingdom, while ServiceNow will invest US\$500 million to localise its regional services in Saudi Arabia with training and development programs to upskill and train Saudi talent. 🏹



# Redington re-imagines the digital future at LEAP 2024



**R**edington, the leading technology integrator and innovation powerhouse, will make a quantum leap in empowering digital transformation journeys at Leap 2024 taking place in Riyadh from 4th to 7th March 2024.

In its third edition, LEAP 2024 is a global tech event with over 172,000 attendees coming from more than 183 countries and will feature 1000 plus speakers, all talking about advanced technologies and solutions shaping the digital future.

The distributor will unveil a captivating showcase themed: Re-imagining the Digital Future: Where Tradition Meets Technology in the Kingdom, during the four-day technology show.

Attendees to the Redington booth – H1A, E50 at LEAP 2024 will witness innovations across technologies, learn new use cases for advanced solutions, gain insights to on ground experiences, success stories, market trends, and connect with technology experts to re-imagine the digital future.

Redington's The Bridge initiative will forge seamless connections across our channel ecosystem. Vendors, partners, and customers alike will talk about their experiences and learnings on Redington's dedicated podcast channel – Technogram – now available on Spotify, Apple Podcasts, Google Podcasts and Amazon Music.

Redington's focus for the technology show is to play a key role in empowering and enabling digital transformation journeys across industries in the Kingdom.

Dharshana Kosgalage, Head of Technology Solutions Group, Redington Middle East and Africa, said, "We look forward to making meaningful connections while also strengthening our existing relationships at LEAP 2024. We are leveraging our vast technology expertise to fuel innovation and foster a collaborative ecosystem that empowers businesses across Saudi Arabia to thrive and achieve business outcomes. Through cutting-edge solutions and a partnership-driven approach, we are re-imagining the digital future, unlocking the Kingdom's full potential for a brighter future."

Rawad Ayash, President, Saudi Arabia, Redington, said, "Saudi Arabia represents a strategic and growing market for Redington, and we are fully invested in supporting the Kingdom's ambitious Vision 2030. Events like LEAP are instrumental in this journey, providing an invaluable platform to stay at the forefront of technological advancements. We are playing a key role in accelerating digital transformation, empowering our partners to evolve into trusted advisors for their customers. Our collaborative approach helps businesses to navigate the evolving digital landscape with confidence and success." 🏡



# Future IT Summit (FITS) in Saudi Arabia culminates in success, spearheading technological advancements



**T**he eagerly awaited Future IT Summit (FITS) in the Kingdom of Saudi Arabia (KSA) concluded, marking a significant milestone in the realm of technology and artificial intelligence (AI). The summit, held at Le Méridien Riyadh brought together leading industry experts, policymakers, and innovators to explore the transformative

potential of AI and IT governance in the modern era.

The summit commenced with an enlightening keynote address by Dr. Jassim Haji, President of IGOAI, who delved into “The Future of Leadership in an AI-Driven Era: Navigating Opportunities and Challenges.” Dr. Haji’s insights set the stage for robust discussions throughout the event.



A distinguished panel of experts, including Mohammed Ali Shalan and Dr. Maad Alowaifeer, engaged in thought-provoking discussions on AI leadership and the challenges posed by the evolving technological landscape. Moderated by Dr. Jassim Haji, the panel provided valuable

insights into navigating the complexities of AI integration and optimization in various sectors. The summit also showcased exemplary achievements in the IT domain with the presentation of awards such as the Top Ten Happy

Companies To Work For 2024, the CIO Catalyst 2024, and the Badge of Honor 2024. These awards recognized organizations and individuals who have demonstrated excellence and innovation in leveraging AI and IT strategies. Key sessions on CIO strategies for harnessing





the power of AI in enterprise IT and AI governance in government sectors, moderated by industry stalwarts Mohammed Alshobani and Mohammed Manashi, provided attendees with actionable insights and best practices. The event concluded with networking sessions,

providing attendees with valuable opportunities to connect, collaborate, and forge partnerships for future endeavors. As Saudi Arabia continues its journey towards digital transformation and technological advancement, FITS emerges as

a pivotal platform for fostering innovation, collaboration, and sustained growth in the IT sector. With its commitment to driving AI-driven innovation, FITS is poised to shape the future of technology in Saudi Arabia and beyond. 🔥



# Salam leads the way at LEAP 2024 with a 'Human Inspired, Business Focused' vision for digital transformation



Eng. Ahmed Al-Anqari,  
CEO of Salam

**S**alam, acclaimed as the fastest growing and most innovative Saudi telecommunications brand at the 2023 Global Brands Awards, is proud to announce its strategic sponsorship of LEAP 2024. This landmark event, taking place at the Riyadh Exhibition and Convention Center from March 4-7, 2024, and known as the "Digital Davos," represents the zenith of global tech gatherings.

Positioned prominently with stand No. H1.K80 in the main hall, Salam is set to shine alongside the world's tech elite at LEAP 2024. The event promises to be unparalleled in scale, with expectations of over 450 startups, more than 1,000 speakers, and over 170,000 exhibitors from across the globe.

Eng. Ahmed Al-Anqari, CEO of Salam, conveys his anticipation for the event: "LEAP 2024 serves as a lighthouse for technological innovation and marks a pivotal moment in the Kingdom's journey toward the KSA 2030 vision. Salam's strategic sponsorship reflects our commitment to this transformative journey. We are excited to unveil how our innovative solutions in connectivity, mobility, cybersecurity, cloud services, and emerging technologies like IoT and AI are setting new benchmarks in telecom and empowering businesses

to become futureproof and agile. Our participation this year is driven by a 'Human Inspired, Business Focused' ethos, ensuring our leadership in delivering technology that is accessible and transformative."

This year's theme, "Human Inspired, Business Focused," emphasizes Salam's commitment to spearheading digital transformation efforts that are both innovative and inclusive. Salam's booth will provide an immersive experience into a future where technology is designed around human needs and business objectives, showcasing Salam's blueprint for a digitally empowered Kingdom through the lenses of connectivity, cybersecurity, cloud management, and emerging technologies.

Al-Anqari further states, "Standing alongside the global telecom and tech giants at LEAP 2024, we reaffirm our mission to forge an innovative and inclusive future. We invite attendees to discover the new worlds we are shaping, where technology and human potential converge to unlock infinite possibilities."

Salam looks forward to welcoming visitors, partners, and technology enthusiasts from around the world to their booth at LEAP 2024, where the future of digital transformation will be unveiled. 🏹

# New white paper defines the 10 Gbps campus network architecture for intelligent cities



Campuses, the fundamental components of our cities, play a crucial role in bringing together people and industries. Huawei's enterprise business market insights indicate that more than 90% of urban residents work and live inside campuses. Additionally, over 80% of a country's Gross Domestic Product (GDP) and 90% of innovations are generated within these campus environments.

As digital transformation takes root, smart campuses have emerged. A smart campus requires an "everything-aware" converged network so that people, things, and services on campus are no longer isolated. Instead, they unite as a whole, interacting with and affecting each other. Furthermore, inter-system collaboration, information interaction, and service convergence have become the norm. Such interaction and convergence create added value.

The smart campus is the foundation of the smart city. This city of the future leverages

advanced technology for efficient services, sustainable energy, transportation, and governance. Smart infrastructure, data analytics, and citizen engagement are deployed by stakeholders to drive progress in urban centers.


During the Ultra-Broadband Forum 2023 (UBBF 2023) in Dubai, Huawei, together with the UAE Telecommunications and Digital Government Regulatory Authority (TDRA), Omdia, etisalat by e&, MTN South Africa unveiled the 10 Gbps City Initiative, the next evolution in smart cities. This initiative calls for the construction of fully connected 10 Gbps cities to provide ubiquitous network experience, accelerate the digital-intelligent transformation of industries, and boost digital productivity.

The 10 Gbps City is a new type of infrastructure critical to implementing national digital strategies and boosting the digital economy. The construction of 10 Gbps cities involves delivering 10 Gbps to individuals, homes, enterprises, and campuses. It also requires 400GE/800GE converged transport networks and AI DCNs related to the preceding

four 10 Gbps access scenarios.

Many cities around the world have released their 2030-oriented digital economy strategies. Cities such as Riyadh are actively exploring ways to implement 10 Gbps City and 10 Gbps Society to unleash the new momentum of the digital economy.

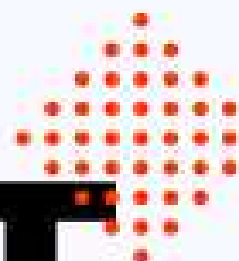
To help define the future of campus networks, Huawei released the High-Quality 10 Gbps Campus Network Construction White Paper supported by WBA (Wireless Broadband Alliance) at MWC Barcelona 2024, themed "Huawei Intelligent Cloud-Network, Accelerating Industrial Intelligence".

This white paper puts forward the philosophy of experience-centric campus network construction; it also delves into how Huawei's High-Quality 10 Gbps CloudCampus Solution offers three types of experience upgrade — wireless experience upgrade, application experience upgrade, and Operations and Maintenance (O&M) experience upgrade — to accelerate enterprises' digital and intelligent journey. 

Under the High Patronage of His Majesty King Mohammed VI



29 - 31 MAY 2024 MARRAKECH

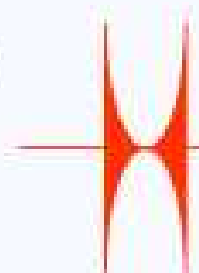


# VISIT THE LARGEST TECH & STARTUP SHOW IN AFRICA

## Creating A Bold Future For Africa

- Discover **MORE** tech solutions
- Hear **MORE** ground-breaking opinions
- Meet **MORE** tech brands
- Network with **MORE** tech professionals
- ... than anywhere else on the entire African continent

- AI Everything (AI x Cloud x IoT x Data)
- Digital Finance
- Digital Cities
- Cybersecurity
- Telecoms & Connectivity
- Digital Health
- Consumer Tech
- North Star Africa



UNLOCK AFRICA'S DIGITAL FUTURE AT GITEX AFRICA  
MAY 29-31, MARRAKECH, MOROCCO



gitexafrica.com

Book to secure  
your Early Bird  
Ticket today.  
Expires 18 April 2024





# Regulation remains the strongest multiplier to cybersecurity growth, according to report from Frost & Sullivan



Newly released report ahead of GISEC Global 2024 offers deep dive into current conditions of the region's cybersecurity industry



**Bashar Bashaiah,**  
Managing Director,  
Cloudflare

In 2023, the United Arab Emirates (UAE) actively repelled more than 50,000 cyberattacks daily, according to the UAE Cybersecurity Council. In the first three quarters of the same year, the country successfully prevented over 71 million attempted attacks in total.

These findings, highlighted in a report from

analysts Frost & Sullivan (F&S), show the exponential growth of the region's cybersecurity landscape – and serve as a sobering reminder of the rising threats that accompany it.

As the GCC (Gulf Cooperation Council) cybersecurity industry continues to grow – with F&S estimating it to triple in value by 2030 to reach US\$13.4 billion – countries like the UAE and Saudi Arabia continue to reduce their dependence on oil exports and are instead opting

for digital tools and technologies.

This shift in economic agenda has made businesses increasingly prone to escalating cyber threats, with regional geopolitical instability further driving vulnerability across key sectors.

The detailed report, titled 'Middle East Cybersecurity: Exploring the Middle East Cybersecurity Market Potential', was released ahead of GISEC Global 2024 – the Middle East and Africa's largest and most impactful cybersecurity super-congregator, which returns to Dubai World Trade Centre from 23-25 April. In collaboration with Frost & Sullivan, it aims to identify the challenges and opportunities facing the region's expanding industry.

## The Middle East braces for escalating cyber threats

In the UAE and Saudi Arabia, specifically, there has been a dramatic uptick in the adoption of technology across the finance, healthcare, and manufacturing sectors, further boosting the need for cybersecurity and robust regulatory frameworks.

Contributing to the existing challenges with increased reliance on technology are issues around awareness and a scarcity of skilled professionals, as well as a lack of clarity among businesses regarding proactively combating cyberattacks.

In response to these industry-wide shortcomings, and as the region continues to navigate the global overhaul of technology, countries in the Middle East are taking measurable steps to



**Kenneth D'Souza,**  
Marketing Manager,  
Spire Solutions

enhance their cybersecurity posture.

Setting up cyber-specific departments and innovation centres, driving awareness through educational campaigns and training programmes, and promoting entrepreneurship through cybersecurity conferences are just some of the ways that the region is equipping the next generation and bridging the existing skills gap.

In fact, as per the ITU Global Cybersecurity Index 2020 highlighted in

the report, Saudi Arabia has ranked second, and the UAE fifth, among 194 participating countries, indicating that both countries have taken extensive measures in terms of regulatory approaches.

As a result, they have become destinations of choice for academics, businesses, research, and innovation, with the UAE government launching the first national Cyber Pulse Innovation Centre aimed at upskilling professionals at Abu Dhabi Polytechnic.

## GCC Countries take confident steps towards building cyber resilient posture

In the UAE and Saudi Arabia, specifically, there has been a dramatic uptick in the adoption of technology across the finance, healthcare, and manufacturing sectors, further boosting the need for cybersecurity and robust regulatory frameworks.

Contributing to the existing challenges with increased reliance on technology are issues around awareness and a scarcity of skilled professionals, as well as a lack of clarity among businesses regarding proactively combating cyberattacks.

In response to these industry-wide shortcomings, and as the region continues to navigate the global overhaul of technology, countries in the Middle



**Parminder Kaur,**  
Director and Head  
of Security Advisory,  
MEASA, Frost &  
Sullivan

East are taking measurable steps to enhance their cybersecurity posture.

Setting up cyber-specific departments and innovation centres, driving awareness through educational campaigns and training programmes, and promoting entrepreneurship through cybersecurity conferences are just some of the ways that the region is equipping the next generation and bridging the existing skills gap.

In fact, as per the ITU Global Cybersecurity

Index 2020 highlighted in the report, Saudi Arabia has ranked second, and the UAE fifth, among 194 participating countries, indicating that both countries have taken extensive measures in terms of regulatory approaches.

As a result, they have become destinations of choice for academics, businesses, research, and innovation, with the UAE government launching the first national Cyber Pulse Innovation Centre aimed at upskilling professionals at Abu Dhabi Polytechnic.

# Will AI's potential be realised in 2024?



**Bryan Harris,**  
Chief Technology Officer, SAS

Artificial intelligence is everywhere, and stories about its promise and threat are rampant. Will AI's potential be realized in the year ahead? SAS, the leader in AI and analytics, asked executives and experts across the company to predict trends and key business and technology developments in AI for 2024.

Below are some of the predictions they shared.

## **Generative AI will augment (not replace) a comprehensive AI strategy**

"Generative AI technology does a lot of things, but it can't do everything. In 2024, organizations will pivot from viewing generative AI as a stand-alone technology to integrating it as a complement to industry-specific AI strategies. In health care, that means the generation of individualized treatment plans. In manufacturing, generative AI can simulate production to identify improvements in quality, reliability, maintenance, energy efficiency and yield."

– Bryan Harris, Chief Technology Officer, SAS

## **AI will create jobs**

"In 2023, there was a lot of worry about the jobs that AI might eliminate. The conversation in 2024 will focus instead on the jobs AI will create. An obvious example is prompt engineering, which links a model's potential with its real-world application. AI helps workers at all skill levels and roles to be more effective and efficient. However, they will also spark many new jobs and roles that will help drive economic growth."

– Udo Sglavo, Vice President of Advanced Analytics, SAS

## **AI will enhance responsible marketing**

"As marketers, we must consciously practice responsible marketing. Facets of this are awareness of the fallibility of AI and alertness to possible bias creeping in. Whether you create or apply AI, you are responsible for its impact. That's why all marketers, regardless of technical know-how, can review the model cards, validate that their algorithms are effective, fair, and adjust as needed."

– Jennifer Chase, Chief Marketing Officer, SAS

## **Financial firms will embrace AI amid a Dark Age of Fraud**

"Even as consumers signal increased fraud vigilance, generative AI and deepfake technology are helping fraudsters hone their multitrillion-dollar craft. We are entering the Dark Age of Fraud, where banks and credit unions will scramble to make up for lost time in AI adoption – incentivized, no doubt, by regulatory shifts forcing financial firms to assume greater liability for soaring APP [authorized push payment] scams and other frauds."

– Stu Bradley, Senior Vice President of Risk, Fraud and Compliance Solutions, SAS

## **Shadow AI will challenge CIOs**

"CIOs have struggled with 'shadow IT' in the past and will now confront 'shadow AI' – solutions used by or developed within an organization without official sanction or monitoring by IT. Well-intentioned employees will continue to use generative AI tools to increase productivity. And CIOs will wrestle daily with how much to embrace these generative AI tools and what guardrails should be put in place to safeguard their organizations from associated risks."

– Jay Upchurch, Chief Information Officer, SAS. 🔗



# Outdated data can spell AI's doom, but real-time Streaming will help AI live up to its promise



**Fred Crehan,**  
Area Vice President, Emerging Markets  
at Confluent

**W**hile the promise of AI has been around for years, there has been an unprecedented resurgence thanks to breakthroughs across reusable large language models (LLMs), more accessible machine learning models, more data than ever, and more powerful GPU capabilities. This has given organisations the impetus they needed to accelerate their AI investments. After all, it is an unmissable opportunity with economists estimating the impact of AI in the Middle East to be US\$320 billion by 2030, and contributing as much as 13.6% of the GDP in some regional nations.

While this newfound focus on AI can be directly linked to a single event that took place in the last quarter of 2022 – the public availability of ChatGPT – fast forward over a year on and we see that despite their best intentions, most organisations have struggled to implement a successful AI strategy. The 2023 global trends in AI report by S&P that surveyed over 1,500 AI decision-makers unsurprisingly highlights that one of the biggest barriers to AI innovation is access to clean and trustworthy data. The truth is while you can have a great AI/ML model, these models cannot stand alone. If the data powering these models is not high-quality, reliable, or fresh, there isn't much value that will come out of these models.

Connecting AI models to enterprise data in real time has been one of the most challenging problems data-dependent teams have been trying to solve. Addressing this challenge has become even more pressing with the emergence of GenAI. For businesses to succeed in this new era of AI, they

have to avoid the challenges that legacy data-at-rest architectures impose and build the modern AI stack on a foundation of data in motion.

## **What's holding back true artificial intelligence innovation**

Imagine a world where your AI applications can make instantaneous decisions based on the freshest, most relevant data. Now snap back to your current enterprise reality: a labyrinth of data silos and varying cloud services, connected by a spaghetti-like mess of point-to-point integrations. This makes it a formidable task to actualise the seamless real-time connections that AI applications need for timely and accurate responses.

The root of the issue lies in your outdated data integration methods, which are built on slow, batch-based pipelines. These cumbersome systems take far too long to deliver data, rendering it stale and inconsistent by the time it arrives to feed your AI applications. Compounding these data problems are issues with poor governance and scalability.

The reality is your AI strategy is deeply interrelated to your data strategy. Outdated data infrastructure and integration methods aren't just a technical hurdle; they can be a roadblock to AI innovation. If you don't solve the foundational data infrastructure challenges for real-time AI, they will stifle developer agility and put the brakes on the pace of AI advancement. Until you tackle this challenge, your AI capabilities will remain constrained, always waiting for outdated data that has lost relevance. ↩

# Five trends dictating the future of networks



**Prashil Gareeb,**  
Vice President of Managed Networks  
from Dimension Data

Below are five ways in which we're seeing this shift taking place.

## The rise of the multi-cloud

A significant aspect of this transformation is the increasing shift towards companies implementing a multi-cloud approach. In these cases, organisations are strategically deploying applications and workloads both on-premises and off-premises, driven by the purpose and nature of their operations.

Data sovereignty, especially in sectors like government and financial services, plays a pivotal role here in determining where sensitive data is hosted. To help achieve this, organisations and service providers are separating network functions among various service providers. This approach allows them to achieve scalability and optimise multi-cloud networking architecture.

## Network-integrated security

In this era of dynamic change, network security has rightfully taken centre stage. With a distributed workforce creating more opportunities for potential attack, enterprises are compelled to transition to centralised, cloud-based security solutions, such as the secure access service edge (SASE) and a managed endpoint security model.

Network-integrated security is also emerging as a linchpin, with technologies like proactive detection and response, zero-trust networking, and identity-based security fortifying communication across networks. This end-to-end, secure-by-design approach is the bedrock of the future network.

## Spread of WAN

The WAN (Wide Area Network) has undergone a substantial evolution in recent times, with the acceptance of the Internet as WAN becoming more widespread. The pandemic experience has sped this process up, demonstrating that the internet can serve as a reliable and cost-effective enterprise transport mechanism, reducing the demand for more expensive connectivity options.

## Software-defined Networking

Software-defined networking (SDN), a long-standing buzzword, has now matured into a transformative force. It allows for a business-outcome-based network, aligning infrastructure with business policies and rules. Intelligent networking, or intent-based networking, has become the rallying cry for networks of the future. These networks incorporate automation, programmability, predictive analytics, and orchestration to proactively adapt and optimise.

## Intelligent Networks

The future promises self-healing and self-optimising networks leveraging AIOps, automation, and orchestration. The agility of intelligent networks positions organisations to adapt swiftly to market changes and cultural shifts, ensuring resilience and competitiveness.

The changing face of campus and branch networks reflects this ongoing transformation. Legacy infrastructures are giving way to more automated and intelligent networks fuelled by SDN practices. Proactive monitoring and measurement through detailed and predictive analytics are enhancing user experiences, while the adoption of automation helps bridge the skills gap caused by trends like "the great resignation."

Yet, amidst this promising future, enterprises grapple with operational concerns. The inherent complexity and intelligence of modern networks pose challenges for internal operations teams with limited programming skills. AIOps and automation, while simplifying ongoing network operations, present complexities in deployment and configuration.

As we gaze toward the future, one thing is clear: the networks of tomorrow are not just technological infrastructures; they are strategic assets shaping the destiny of enterprises. Navigating this requires a commitment to continuous innovation, adaptability, and the embrace of intelligent networking solutions that promise not just connectivity but resilience, security, and agility in the face of an ever-evolving digital landscape. 🔴

## Cisco to transform du's SOC into advanced Cyber Defence and Intelligence Centre

Cisco announced a landmark collaboration with du, from Emirates Integrated Telecommunications Company (EITC), signaling the beginning of a major cybersecurity transformation initiative. The initiative focuses on revolutionizing du's Security Operations Center into an advanced Cyber Defense and Intelligence Center, leveraging artificial intelligence and automation to enhance security and operational efficiency.

The agreement signifies Cisco's commitment to supporting du's aspiration to lead digital transformation in the United Arab Emirates (UAE) ensuring robust cybersecurity measures that align with the nation's digital transformation strategy. This transformative partnership demonstrates how Cisco's innovative solutions can be a catalyst in



Adele Trombetta, SVP & GM CX EMEA at CISCO

securing an entire region's digital infrastructure.

Saleem Alblooshi, CTO at du, said: "Through this strategic collaboration, Cisco is reinforcing our dedication to supporting the digital transformation journey of our customers. By leveraging Cisco's advanced security operations and AI capabilities, du is empowered to lead the way in cybersecurity defense, ensuring that our customers' digital platforms are fortified against evolving threats. This integration propels du to the cutting edge of digital trust, enabling safe and intelligent organizations to thrive in the digital era."

With the rapid evolution of cyber threats, it's imperative for service providers like du to prioritize cybersecurity. Cisco's CX Services teams will play a crucial role in ensuring that du's

## Orange Business to provide Palo Alto's Prisma SASE with service provider interconnect

Orange Business, Orange Cyberdefense and Palo Alto Networks have further strengthened their partnership to deliver Palo Alto Networks Prisma Secure Access Service Edge (SASE) with Service Provider (SP) Interconnect. Orange Business is the first service provider worldwide to make this solution available via its Evolution Platform, allowing customers to compose a roster of services to meet evolving business requirements.

Orange is uniquely and jointly pioneering with Palo Alto Networks to propose on-net connectivity using an innovative SP interconnection infrastructure service. Orange Business uses its existing global carrier network facilities to enable its customers' networks to connect to Palo Alto Networks Prisma SASE and back to the Orange internet backbone. This network topology optimizes network utilization, improves traffic performance and ensures end-to-end traffic visibility.

Building on trusted next-generation connectivity solutions, Orange Business has developed Evolution Platform as



the foundation for a secured, flexible and virtualized ecosystem to orchestrate networks, cloud and cybersecurity by Orange Cyberdefense, aligning customers' business strategy with their infrastructure

strategy. Evolution Platform leverages Orange Cyberdefense's threat intelligence backbone, complemented with state-of-the-art capabilities and expertise, including detection and response.



## Kyndryl now Veeam Accredited Service Partner through recent strategic alliance

Kyndryl, the world's largest technology infrastructure services provider, and Veeam Software, the #1 leader by market share in Data Replication and Protection Software, announced a global strategic alliance focused on providing customers with resiliency services supported by innovative technology, expert infrastructure management and incident recovery services. Under the alliance, Kyndryl will now be a Veeam Accredited Service Partner.

Kyndryl offers professional services and technical implementation integrated with Veeam solutions, providing customers with options for:

**Comprehensive Cyber Resilience:** Using an integrated approach to help customers strengthen their stakeholder confidence with strategies to effectively recover from adverse conditions,



John Jester,  
CRO at Veeam.

including cyber incidents, human error and hardware failures.

**Simplified Vendor Transitions:** Provide customers with a seamless transition to modern, security and compliance rich cloud-based infrastructure with scalable and customizable options for hybrid and multi-cloud backup and recovery.

**Modern Data Protection Solutions:** Help customers modernize and protect data across their enterprise with a simplified, holistic approach on a single platform for effective and reliable data protection with robust defense for modern SaaS applications, data and systems.

**Enhanced Operational Efficiencies:** Integrated automation to drive operational efficiency, enabling customers with the flexibility to adapt to changing business needs and industry standards.

## Mindware to make available Microsoft 365 Copilot, AI integrated with Microsoft 365, to channel partners

Following closely on the recent launch of its new business unit dedicated to Artificial Intelligence, Mindware, a leading value-added distributor (VAD) in the Middle East and Africa, has announced that it is now making Microsoft 365 Copilot available to regional enterprises through its expansive partner ecosystem. Copilot is an AI tool integrated into Microsoft 365, that combines the power of large language models with enterprise data in the Microsoft 365 apps, to turn words into a powerful productivity tool.

Microsoft and Mindware have established a strong partnership that has thrived for over 25 years, dating back to the inception of Mindware. Throughout this time, the two companies have closely collaborated to provide a comprehensive suite of Microsoft offerings, including Azure, Dynamics 365, Enterprise Mobility & Security, Exchange, Microsoft 365, Office 365, Power BI, SQL, SharePoint, Teams, and Windows. Their joint efforts have empowered regional organizations, across various domains, to leverage cutting-edge technology solutions for enhanced digital transformation, productivity and growth.



(L-R) Philippe Jarre, President, Mindware Group and Tamer Elhamy,  
Microsoft Middle East's Chief Partnership Officer.

## IFS partners with Artificial Intelligence Global Company in Saudi Arabia, targeting oil and gas, utilities

IFS, the global cloud enterprise software company, signed a strategic partnership with Artificial Intelligence Global Company in Saudi Arabia. As an industry specialized solution provider, IFS is in a strong position to drive digitization in key Oil and Gas and Utilities markets while AIGC's deep-rooted local experience and capabilities will provide a solid platform to tap into this growing market.

AIGC will help accelerate the uptake of IFS solutions that resonate with the Oil & Gas and Utilities companies. These include IFS Cloud, IFS Cloud Enterprise Asset management to overcome operational challenges, IFS Cloud EAM's AI-embedded maintenance planning and scheduling and Field Service Management solution to support 360 degree end-to-end service lifecycle.

Speaking on the new collaboration, Vijay Jaswal, Chief Technology Officer, APJ&MEA, at IFS said, "Saudi Arabia plays a vital role in our Middle East expansion plans, and it



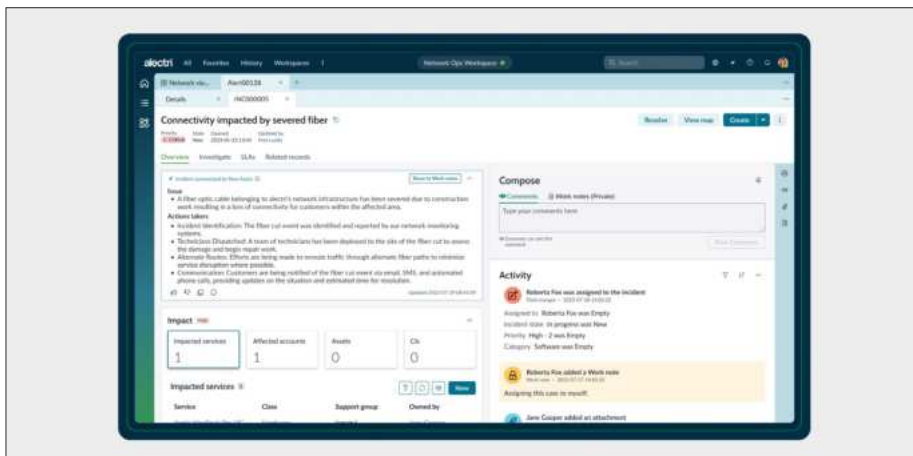
is important for us to have a sturdy and well-connected partner to enable us to meet local business needs, help them drive growth and support the country's digitization goals. We truly believe that AIGC has a strong network

and market insights that will help us accelerate the goals of businesses that are focused on embracing digitization to attain operational efficiency, sustain long term growth, and lessen their carbon footprint."

## Now Assist for Telecommunications Service Management from Servicenow using NVIDIA AI to raise agent productivity

ServiceNow announced that they are broadening their relationship with the introduction of telcospecific generative AI solutions to elevate service experiences. The first solution, Now Assist for Telecommunications Service Management, is built on the Now Platform and uses NVIDIA AI to help boost agent productivity, speed time to resolution, and enhance customer experiences. As telcos look to reduce costs and uncover new business opportunities, they're turning to AI and automation. In a survey from IDC, 73% of global telecommunications service providers identified AI/ML investments to support operations as their top transformation priority.

"GenAI is a gamechanger for telcos looking to boost productivity, improve customer experiences, and drive cost savings with its ability to learn and improve with each use," said Rohit Batra, general manager and vice president for telecom, media, and



tech at ServiceNow. "Together, ServiceNow and NVIDIA will help telcos realize unprecedented business value and impact, fast. This is just the beginning of a large scale transformation for the industry, and we're excited to be at the forefront."

"The telco industry is rapidly evolving

as AI makes its mark on enterprises everywhere," said Chris Penrose, global head of business development for telco at NVIDIA. "Our partnership with ServiceNow will help telcos leverage GenAI to tackle their unique challenges and build better, stronger, more efficient experiences."

## IBM redesigns Al-Futtaim Group's Blue Rewards including user experience, technology stack, business teams

IBM Consulting has been selected by Al-Futtaim Group to redesign its Blue Rewards' customer experience journey and transform the Group's Digital core through large scale data migration projects.

IBM Consulting implemented a redesign of the Blue Rewards digital platform which includes the user experience, technology stack, and business teams. This resulted in an integrated lifestyle platform that anticipates user needs and preferences, generating personalized rewards and seamless alignment across nine diverse markets. Leveraging its expertise and partnerships with Microsoft and SAP, IBM Consulting implemented a robust, modern digital core, unifying data from diverse sectors like automotive, retail, real estate, and finance. IBM Consulting experts undertook this transformation journey using IBM tools like IBM HANA Impact Assessment, IBM



HANAtization, and Data Reconciliation to minimize risk and speed up transformation. In collaboration with IBM's partners SAP and Microsoft, IBM Consulting streamlined SAP S4HANA migration and modernized its solutions on Microsoft Azure to leverage its cost efficiency, agility, and environmental sustainability benefits.

"We are excited to collaborate with IBM Consulting as we embark in our digital

transformation journey to unlock new possibilities and ensure our digital future is defined by excellence and customer centricity. Together, we are poised to reshape the landscape of Al-Futtaim Group's digital operations, setting a benchmark for industry standards and enriching the overall customer experience," said Himanshu Shrivastava, Chief Technology Officer of Al-Futtaim Group.

## Law enforcement by UK, US to disrupt LockBit ransomware is positive news for enterprises

The global law enforcement operation, led by the UK and US, to disrupt LockBit ransomware operations is a positive development for cyber defenders and impacted organizations. It compromised and disrupted a significant portion of LockBit's infrastructure used for encryption and data leaks. The arrest of two alleged LockBit members is expected to lead to long-term disruption and reveal more about the criminal operation.

The recovery and release of decryption keys by law enforcement will provide immediate relief to LockBit victims trying to recover their encrypted data. Freezing over 200 cryptocurrency accounts linked to LockBit will limit the actors' access to funds, hindering their operations. U.S. Treasury sanctions might influence organizations' choices regarding future ransomware payments.

It's too early to gauge the broader impact. Disrupting cybercrime operations helps victims and costs adversaries, but doesn't solve the issue entirely. For instance, the August 2023 disruption of the Qbot botnet



Selena Larson, senior threat intelligence analyst at Proofpoint.

didn't halt TA577's activities; they switched to different malware. Initial Access Brokers (IABs) are becoming more creative and sophisticated in their attack chains.

This includes everything from improved social engineering, unusual file types, CVE exploitation, chaining scripting files, and so much more. IAB and ransomware actors are also leaning into 0-day and

n-day vulnerabilities, developing new and aggressive social engineering techniques, and using publicly available hacking tools to access organizations.

Any significant disruption to large-scale cybercriminal activities is something to celebrate. But the fight against cybercrime that costs millions of dollars per year continues.



## Group-IB attributes 523 attacks to nation-state actors across the globe, MEA organisations accounted for 77

Group-IB, a leading creator of cybersecurity technologies to investigate, prevent, and fight digital crime, has presented a comprehensive overview of the cyber threat landscape in the Middle East and Africa (MEA) for the years 2023/2024 with the release of its annual Hi-Tech Crime Trends report. The report provides a thorough analysis of how cybersecurity challenges in the MEA region have evolved. The Gulf Cooperation Council (GCC) countries, South Africa, and Turkey were the most frequently targeted locales by Ransomware-as-a-Service (RaaS) affiliates. Information stealers pose a significant concern, impacting 297,106 infected devices in the MEA region whose logs were made available on Underground Clouds of Logs, and an additional 903,002 hosts, logs from which were put up for sale on underground markets. Additionally, 152 new data leaks were detected in the MEA region in 2023.

Nation-state sponsored hackers target MEA



Group-IB researchers discovered that the Middle East and Africa was a significant target for advanced persistent threats (APTs), also known as nation-state sponsored groups, last year. Overall, Group-IB attributed 523 attacks to nation-state actors across the globe in 2023.

Attacks on MEA organizations accounted for 15% of the global total, numbering 77, with Group-IB experts asserting that this may be due to ongoing geopolitical conflicts in the region, along with MEA's importance to the global energy market.

## SAP launches Innovation Hub in Saudi Arabia and Experience Center in Khobar

SAP announced it is increasing its investment in Saudi Arabia, a critically important market for the global technology company. To enable further co-innovation with new and existing customers and partners, SAP has launched a first-of-its-kind regional SAP Innovation Hub in the Kingdom and will also open an SAP Experience Center in Khobar this month.

His Excellency Eng. Haitham ALOhali, "As Saudi Arabia increasingly diversifies its economy and strategically deploys technology to transform key industries, it is vital that organizations such as SAP invest further in their operations and training across the Kingdom.

### SAP Experience Center and Innovation Hub

AlFaifi explained that the SAP Innovation Hub will serve as a pivotal platform for fostering a vibrant community of innovation and co-creation in Saudi Arabia. Designed to



Ahmed AlFaifi, SVP & MD, Middle East Africa – North, SAP.

empower individuals and organizations to collectively tackle operational challenges and drive incremental business value across various industries, custom-tailored to the Saudi market, the hub will bring together SAP global and regional experts, local businesses, startups, and partners in a collaborative environment.

SAP has reiterated its commitment to Saudi Arabia's digital transformation by supporting the Ministry of Communication and Information Technology Center of Digital Entrepreneurship, (CODE) startup program as part of the SAP Innovation Hub, fostering cross-company learning and collaboration to drive innovation in the region.

## Major shift in phishing landscape due to adoption of GenAI and GAN predicts Trend Micro

Trend Micro released its Security Predictions Report for 2024 titled "Critical Scalability". The report emphasizes the crucial need for organizations to adopt an advanced multilayered security approach to counter the growing attack surface.

The report underscores that in 2024, a growing number of enterprises will adopt artificial intelligence and machine learning (AI/ML) technologies. It notes that approximately 69% of IT leaders view the integration of machine learning as a critical operational priority. Although these technological advancements are anticipated to drive organizational growth, they also pose substantial risks, with bad actors exploiting these innovations to orchestrate attacks.

Furthermore, the report also predicts a major shift in the phishing landscape due to the widespread adoption and enhanced



Dr. Moataz Bin Ali, Regional Vice President and Managing Director, MMEA, Trend Micro

capabilities of Generative AI (GenAI) and Generative Adversarial Networks (GANs). This shift allows for the use of highly realistic audio and video content at a lower cost, leading to an increase in sophisticated scams such as business email compromise (BEC), virtual kidnapping, and similar frauds.

Additionally, the 2024 landscape is expected to see heightened vulnerabilities in cloud environments, along with targeted attacks on software supply chains and blockchain technology, which could result in ransom demands or attempts to encrypt entire blockchains.

## e& and Huawei sign MoU to build green and energy efficient networks in UAE

e& and Huawei signed a Memorandum of Understanding during MWC 2024 to collaborate on building green and energy-efficient networks in the UAE to significantly reduce carbon emissions and contribute to sustainable environmental practices.

e& will continue to work with Huawei to achieve network decarbonisation across its ICT infrastructure, including radio, core and transport networks, and data centers. The effort to decarbonise the network will adopt a mix of Huawei's energy-efficient technology innovations and intelligent software features, as well as maximising the use of renewable energy. The companies will also collaborate in hosting a series of knowledge-sharing sessions to exchange insights on climate change and the latest technological advancements and adapt and align network strategies accordingly.

In a pioneering move, e& launched its region's first net-zero 5G Massive MIMO site using Huawei technology during COP 28 in December 2023, showcasing a tangible commitment to eco-friendly technology deployment.



Sabri Albreiki, Chief Technology Officer of e& International, remarked, "Through our strategic partnership with Huawei, we aim to accelerate the decarbonisation of our ICT infrastructure by deploying their energy-efficient network equipment combined with energy-saving software features, advanced machine learning capabilities, and renewable

energy sources. Signing this MoU with Huawei reinforces our joint commitment to a greener, more sustainable future."

Echoing this sentiment, Gavin Wang, President of Huawei e& Global Key Account, stated, "The combined efforts of e& and Huawei exemplify a strong commitment to climate change and sustainable technology."

## Delinea announces definitive agreement to acquire Fastpath for identity governance and identity access

Delinea, a provider of solutions that seamlessly extend Privileged Access Management (PAM), announced a definitive agreement to acquire Fastpath, a leader in Identity Governance and Administration (IGA) and identity access rights. This strategic move follows Delinea's recent acquisition of Authomize and marks a significant expansion in Delinea's capabilities to enhance privileged access, controls, and governance, reducing organizational cybersecurity risk and ensuring compliance.

By incorporating Fastpath's expertise, Delinea is poised to offer a robust, AI-driven authorization security platform making Delinea the definitive source for managing authorization across infrastructure, applications, and data, providing unmatched insights and control over user access and privileges.

"This strategic acquisition by Delinea heralds a new era in identity security, establishing



Art Gilliland, CEO, Delinea

pioneering standards for Privileged Access Management in an increasingly digital and interconnected world, where cybersecurity challenges are constantly evolving," said Art Gilliland, CEO of Delinea. "The addition of Fastpath will empower the Delinea Platform to dynamically control authorizations by assessing user risk. This advanced approach is crucial for securing modern, distributed environments across infrastructure, applications, and data."

In today's landscape, dominated by Infrastructure-as-a-Service and SaaS applications, organizations face a growing attack surface and challenges in managing data and identity sprawl. The combination of Fastpath with Delinea is timely, addressing these challenges head-on. It equips Chief Information Security Officers (CISOs) and their teams with advanced tools for managing the complex interactions between privileged users and corporate data.

## Dell Technologies announces solutions to help CSPs facilitate network cloud and operations

Dell Technologies announces new solutions to help communications service providers facilitate network cloud and operations transformation to achieve improved economics and agility, while maintaining network reliability.

Dell is using its decades of experience in digital transformation and deep industry partnerships to design telecom solutions that reduce risk, so CSPs can ease the deployment, automate the operation and simplify the support and lifecycle management of disaggregated network cloud infrastructure.

"The first step in network cloud transformation is installing the cloud infrastructure platform, both architecturally and operationally," said Dennis Hoffman, senior vice president and general manager, Telecom Systems Business, Dell Technologies. "It takes a team to successfully address the people, process and technology aspects of these programs. We're contributing not only our technology, but our years of cloud transformation experience to ecosystem



partnerships with communication service providers around the world."

As CSPs integrate a broad ecosystem of technologies to build open, cloud-native networks, they need a simple way to deploy and manage infrastructure from multiple vendors across geographically distributed areas, without compromising network reliability or adding increased costs.

Dell announces the Dell Telecom Infrastructure Automation Suite, software designed to automate the orchestration and lifecycle management of multi-vendor, network cloud infrastructure at scale. The Automation Suite, based on open standards and APIs, integrates seamlessly into the network and offers CSPs the flexibility to deploy and manage their choice of infrastructure across distributed, multi-vendor environments.



AMPLIFY YOUR VOIZE  
WITH US AND EXPLORE  
OUR SERVICES.



DESIGN  
SERVICES



PHOTOGRAPHY &  
VIDEOGRAPHY



2D & 3D  
ANIMATION



TELE-  
CALLING



EVENT  
MANAGEMENT



MEDIA  
BUYING



DIGITAL  
MARKETING



CORPORATE  
GIFTS



SOCIAL  
MEDIA



BRAND  
ACTIVATION



BOOTH  
BUILDING



CONTENT  
GENERATION

“

We combine leading technologies with highly skilled security analysts to deliver a proactive and predictive approach

**Jasim Al Awadi**

Chief ICT Officer, du

# STAYING UPDATED WITH EMERGING QUANTUM HACKS AND ADVERSARIAL MACHINE LEARNING TECHNIQUES IS CRUCIAL

Enterprise Channel MEA had an exclusive interview with Jasim Al Awadi, Chief ICT Officer, du and got an overview of the cybersecurity around GCC with a focus on AI and machine learning

## **How do you envision the GCC Cybersecurity market evolving in response to the projected tripling in size by 2030, considering the escalating capabilities of AI-driven threats?**

The GCC Cybersecurity market is on track to experience significant expansion by 2030, with a projected tripling in size. This growth is primarily driven by factors such as increasing digitalization, cloud adoption, and the need to secure automated processes. Firstly, there is increased investment in AI-driven threat detection solutions that can analyse vast amounts of data, identify anomalies, and predict potential threats. This enables organisations to enhance their defence against evolving cyber threats.

Secondly, the adoption of behavioural analytics, powered by AI algorithms, allows for the detection of patterns and anomalies in user behaviour, making it possible to identify insider threats or compromised accounts quickly. Moreover, organisations are embracing AI-driven automation to enhance their incident response capabilities. This allows for real-time threat mitigation, adaptive access controls, and automated patch management, enabling organisations to respond swiftly and efficiently to cyber threats.

The integration of AI algorithms with biometric authentication methods, such as facial recognition and behavioural biometrics, is strengthening identity verification, adding an extra layer of security to protect against unauthorized access. Collaboration between GCC organisations and AI research institutions is also contributing to the growth of the cybersecurity market. This collaboration enables the development of customized solutions tailored to regional threats, ensuring that organisations have the necessary tools to defend against specific challenges they face.

## **In light of malicious actors using AI for sophisticated cyber threats such as deepfakes and social engineering, what strategies and technologies are organisations in the GCC region implementing to bolster their defenses against these evolving threats?**

Organisations in the GCC region are proactively implementing strategies and technologies to strengthen their defenses against AI-driven cyber threats, such as deepfakes and social engineering. In order to enhance cyber-resilience and capacity building, organisations need to take several steps. Firstly, they need to upgrade their infrastructure and enhance their incident response capabilities. This involves implementing the latest technologies and tools to detect and respond to cyber incidents effectively. Additionally, organisations should focus on fostering skilled cybersecurity professionals, either through training initiatives or partnerships with educational institutions, to address the shortage of talent in this field.



Promoting collaboration and cooperation among organisations is also crucial for improving cyber resilience. By sharing information, conducting joint exercises, and developing expertise together, organisations can collectively strengthen their defences against cyber threats. Participating in global threat intelligence networks enables organisations to stay informed about emerging threats and defend against evolving cyber-attacks. Public-private partnerships are also essential in enhancing information exchange, sharing best practices, and coordinating responses to cyber incidents.

Given the ever-changing threat landscape, organisations in the GCC region must continue to adapt and invest in cutting-edge technologies and practices to safeguard critical infrastructure and sensitive data. Overall, it is important for organisations to not only invest in next-generation security solutions but also develop comprehensive incident response plans and conduct regular drills and simulations to improve readiness. By focusing on areas such as phishing, social engineering, and secure practices, organisations can reduce the risk of falling victim to cyber-attacks.

### **With the growing menace of quantum hacks and adversarial machine learning, what proactive measures should organisations in the GCC region take to mitigate the risks posed by these advanced cyber threats?**

To safeguard digital enterprises against cyber-attacks, deploying next-generation cyber security services and solutions is crucial. This includes establishing an enterprise Security Operations Centre (SOC) that offers end-to-end advisory, protection, and security monitoring. This SOC should be equipped with innovative and advanced cyber security platforms that can adapt and evolve to counter new security threats.

Operating a dedicated team of security experts within the SOC ensures 24x7 Security Monitoring Incident Detection, and Response. By combining leading technologies with highly skilled security analysts, organisations can achieve a proactive and predictive approach to securing critical areas such as users, applications, endpoints, and infrastructure. Rapidly detecting and responding to security events through a proven process-driven approach is essential in mitigating threats effectively.

Staying updated with emerging quantum hacks and adversarial machine learning techniques is crucial. Organisations should invest in ongoing research and development to counter these threats effectively. Regular security assessments and threat intelligence help identify vulnerabilities promptly and mitigate risks. Collaboration with industry peers and trusted partners facilitates the acquisition of expertise, knowledge sharing, and staying informed about the latest advancements in cyber security. Finally, continuously monitoring advancements in quantum computing and adversarial machine learning enables organisations to adapt security measures accordingly.

### **As the GCC Cybersecurity landscape becomes increasingly complex, how is your organisation dealing with the challenges of data poisoning and ensuring the integrity of their data against potential manipulation by malicious actors?**

We operate the Enterprise Security Operations Centre (SOC) that employs some of the most innovative and advanced cyber security platforms hosted in the UAE. These platforms have been built to adapt, learn, and evolve to counter new security threats, including data poisoning. Our dedicated team of security experts within the SOC provides 24x7 Security Monitoring, Incident Detection, and Response.

We combine leading technologies with highly skilled security analysts to deliver a proactive and predictive approach to securing and managing critical areas such as users, applications, endpoints, and infrastructure. Our enterprise SOC rapidly detects and responds to security events using a process-driven approach aimed at detecting, qualifying, investigating, and mitigating threats.

By leveraging these innovative platforms and highly skilled professionals, we can effectively monitor and detect any potential data poisoning attempts and address them promptly. We continuously evolve our capabilities and stay informed about emerging threats to ensure the integrity of our data and protect against manipulation by malicious actors.

### **Considering the inevitability of regulatory responses to combat AI risks, how are organisations in the GCC region preparing to comply with emerging cybersecurity reg-**


### **ulations while maintaining operational efficiency and innovation?**

Organisations need to stay informed about emerging cybersecurity regulations to understand their impact on operations. They should establish dedicated teams or departments responsible for managing compliance and conducting regular assessments to identify gaps and make necessary improvements. Collaborating with regulatory bodies and industry associations helps understand requirements and seek guidance. Investing in technology solutions for efficient compliance monitoring and reporting is crucial.

Implementing robust security measures and controls that align with regulations while maintaining operational efficiency is necessary. Updating policies, procedures, and training programs educates employees on compliance obligations. Ongoing risk assessments and a culture of compliance ensure proactive vulnerability management. Continuously monitoring and adapting to evolving cybersecurity regulations ensures ongoing compliance and minimizes risks.

### **In the face of AI-driven cyber threats, how crucial is collaboration and information sharing among organisations in the GCC Cybersecurity community to enhance collective defense and resilience?**

Collaboration is essential for effective cybersecurity defence in the era of AI threats. Organisations can pool their resources, expertise and threat intelligence for a stronger collective defence through the practice of collective defence, sharing threat intelligence, utilizing AI for collective defence, sharing knowledge and resources, and reducing the risk landscape. These approaches enable organisations to stay ahead of emerging threats, detect anomalies, and respond in real-time.

Real-world applications of collaboration in the GCC Cybersecurity community include industry collaborations, joint exercises, and partnerships with academia and research institutions. These collaborations enable the development of tailored machine learning models and the sharing of resources and expertise to enhance cybersecurity resilience. 

# SPECIAL REPORT - CYBERSECURITY



**Morey Haber,**  
Chief Security Advisor,  
BeyondTrust



**Vishal Pala,**  
Senior Solutions Engineer  
– META, Barracuda



**Irina Artioli,**  
Cyber Protection  
Evangelist at Acronis



**Jos Beernink,**  
Vice President of EMEA  
at Milestone Systems



**Roman Flepp,**  
Marketing Director,  
Threema



**Dr Waël Kanoun,**  
Managing Director of  
Cyber Solutions, Thales  
Middle East and KSA



**Abrar Ullah,**  
Associate Professor,  
Mathematical and  
Computer Sciences,  
Heriot-Watt University  
Dubai



**Emad Fahmy,**  
Systems Engineering  
Manager, Middle East,  
NETSCOUT



**Alexey Lukatsky,**  
Managing Director,  
Cyber Security Business  
Consultant, Positive  
Technologies



**Hasanian Alkassab,**  
Security Business Unit  
Director at GBM



**Rami Nehme,**  
Regional Sales Director,  
OPSWAT



**Emile Abou Saleh**  
Senior Director of  
Proofpoint Middle East,  
Turkey & Africa



**Samer Diya,**  
the President of Sales  
Emerging Markets,  
Forcepoint.

# Ensure deepfake AI communications is identified



**I**n an exclusive interview with Enterprise Channel MEA, Morey Haber, Chief Security Advisor, BeyondTrust states that GCC region finds itself at the nexus of evolving challenges posed by AI. With malicious actors increasingly leveraging AI to orchestrate sophisticated cyberattacks, organizations across the GCC face a pressing imperative: fortify their defenses against these emerging threats. From deepfakes to quantum hacks, the proliferation of AI-driven risks necessitates a multifaceted approach rooted in collaboration, innovation, and regulatory compliance.

The GCC's demographic mosaic, characterized by a diverse populace comprising both citizens and expatriates, presents a unique cybersecurity landscape. This diversity, while enriching, amplifies the complexity of defending against AI-driven threats. AI-powered deepfake technology, capable of targeting any nationality, language, culture, or religion, poses an unprecedented risk of misinformation and social engineering attacks. In this context, a comprehensive defense strategy tailored to the region's cultural and linguistic nuances becomes indispensable.

To mitigate the risks posed by AI-driven threats, organizations in the GCC must adopt proactive measures across multiple fronts. One

such measure is the implementation of robust web content filtering mechanisms. By subjecting all forms of digital communication to rigorous scrutiny, organizations can detect and neutralize malicious content while ensuring adherence to cultural norms and legal requirements. Additionally, prioritizing identity security emerges as a cornerstone of the GCC's cybersecurity posture. By authenticating communications and mitigating the risks of deepfake impersonations, organizations can enhance their resilience against AI-driven attacks.

The principle of least privilege (PoLP) assumes paramount importance in bolstering the GCC's cyber defenses. By adopting a proactive approach to reduce, monitor, and manage privileged accounts, organizations can thwart cyberattacks that exploit unmonitored administrative access. This not only enhances security but also aligns with emerging regulatory frameworks aimed at safeguarding sensitive data and preserving privacy rights.

Amidst the looming specter of quantum hacks and adversarial machine learning, organizations must remain vigilant. While these threats currently reside in the realm of theory, investing in preemptive defenses is imperative. Quantum-safe encryption solutions offer a



“

For organizations concerned about the future of these attacks, they should consider quantum safe encryption (quantum unhackable) solutions for communications

### KEY HIGHLIGHTS

- **AI Threats:** GCC faces evolving cyber challenges with AI, including deepfakes.
- **Defense Tactics:** Proactive measures like filtering and identity security are crucial.
- **Innovative Solutions:** Quantum-safe encryption aids in preemptive defense.
- **Regulatory Adherence:** Compliance ensures efficient navigation of regulations.
- **Collaborative Approach:** Sharing information enhances resilience across GCC.

**Morey Haber,**  
Chief Security Advisor,  
BeyondTrust



proactive defense against future vulnerabilities, particularly for critical sectors such as government and defense. By embracing these technologies, organizations can mitigate the potential risks associated with nation-state warfare and safeguard sensitive information from quantum-enabled adversaries.

Regulatory compliance serves as another linchpin in the GCC's cybersecurity resilience strategy. As global regulatory frameworks evolve to address AI risks, organizations must adapt while preserving operational efficiency and innovation. Aligning with both global standards, such as GDPR, and locally crafted regulations enables organizations to navigate the complex regulatory landscape effectively. By upholding cultural norms and legal requirements, organizations can mitigate the risks posed by AI-driven cyber threats while fostering trust and accountability in digital transactions.

Collaboration and information sharing

emerge as critical pillars in the GCC's collective defense against AI-driven cyber threats. In an interconnected digital ecosystem, no organization operates in isolation. The rapid dissemination of threats and vulnerabilities necessitates a collaborative approach that transcends geographical boundaries. By fostering a culture of collaboration, the GCC cybersecurity community can enhance its collective resilience and respond effectively to emerging threats.

Safeguarding the GCC against AI-driven cyber threats demands a concerted effort grounded in collaboration, innovation, and regulatory compliance. As organizations navigate the complexities of a rapidly evolving threat landscape, a proactive stance is imperative. By embracing advanced technologies, adhering to regulatory requirements, and fostering collaboration, the GCC can bolster its cyber defenses and ensure a secure digital future for all. 🔴

# Next generation threats require next generation solutions



**W**ith the projected tripling in size of the GCC cybersecurity market by 2030, organisations face a pressing imperative: fortifying their defenses against escalating AI-driven threats. As organisations across the GCC grapple with these challenges, Hasanian Alkassab, Security Business Unit Director at GBM, offers insights into the evolving cybersecurity landscape and the proactive measures being taken to mitigate emerging threats.

The GCC is witnessing a remarkable surge in demand for AI-driven solutions, driven by organisations' recognition of the need to enhance efficiency and decision-making processes in a rapidly evolving business landscape. Alkassab highlights the pivotal role of AI in contributing to the region's GDP, with the UAE, Saudi Arabia, and the broader GCC poised to reap substantial benefits. Against this backdrop, the GCC cybersecurity market is primed for significant expansion, with AI-powered defenses expected to become standard practice. Alkassab underscores the indispensable role of human expertise in tandem with AI, emphasizing the need for a skilled cybersecurity workforce to navigate evolving threats effectively.

As malicious actors increasingly wield AI for sophisticated cyber threats like deepfakes and social engineering, organizations in the GCC are ramping up their defenses. Alkassab details the implementation of advanced threat detection systems powered by AI, along with employee training programs to equip staff with the skills to recognize social engineering tactics. Security awareness campaigns and investments in AI-powered deception technology further bolster defenses, underscoring the multi-pronged approach adopted by GCC organizations to stay ahead of the curve.

Alkassab highlights the growing menace of quantum hacks and adversarial machine learning, urging organizations to take proactive measures to mitigate these advanced cyber threats. With enterprise complexity on the rise and the attack surface expanding, traditional cybersecurity solutions may prove inadequate. Alkassab advocates for the adoption of next-generation Managed Detection and Response (MDR) solutions powered by machine learning and orchestration, empowering cybersecurity teams to combat evolving threats effectively. At GBM, Alkassab emphasizes the importance of prioritizing robust measures against data threats, including rigorous access controls,

“

GBM Shield helps by taking a holistic approach to mitigate security risks by focusing on people, processes, and technology

### KEY HIGHLIGHTS

- **Market Growth:** The GCC cybersecurity market is poised to triple by 2030, driving demand for AI-driven solutions.
- **Defense Strategies:** GCC organisations employ multi-layered approaches, including advanced threat detection and AI-powered deception, to combat malicious AI threats.
- **Proactive Measures:** Next-gen solutions like MDR, powered by machine learning, mitigate risks posed by quantum hacks and adversarial machine learning.
- **Data Security Focus:** GBM emphasizes robust measures to safeguard data integrity, including strict access controls and continuous threat intelligence updates.
- **Compliance and Innovation:** GCC organizations prepare for stricter regulations while fostering innovation, ensuring alignment with evolving cybersecurity standards.



**Hasanian Alkassab,**  
Security Business Unit Director  
at GBM

authentication mechanisms, and continuous threat intelligence updates. Collaborative efforts within the industry further bolster collective resilience, enabling organizations to maintain a secure environment for their operations.

In light of the inevitability of regulatory responses to combat AI risks, Alkassab outlines proactive measures being taken by organizations in the GCC. Conducting thorough compliance audits, implementing robust governance frameworks, and prioritizing data privacy and security throughout the AI lifecycle are crucial steps. Alkassab underscores the importance of open communication and collaboration with regulators, facilitating early adaptation to evolving regulations while maintaining operational efficiency and fostering innovation.

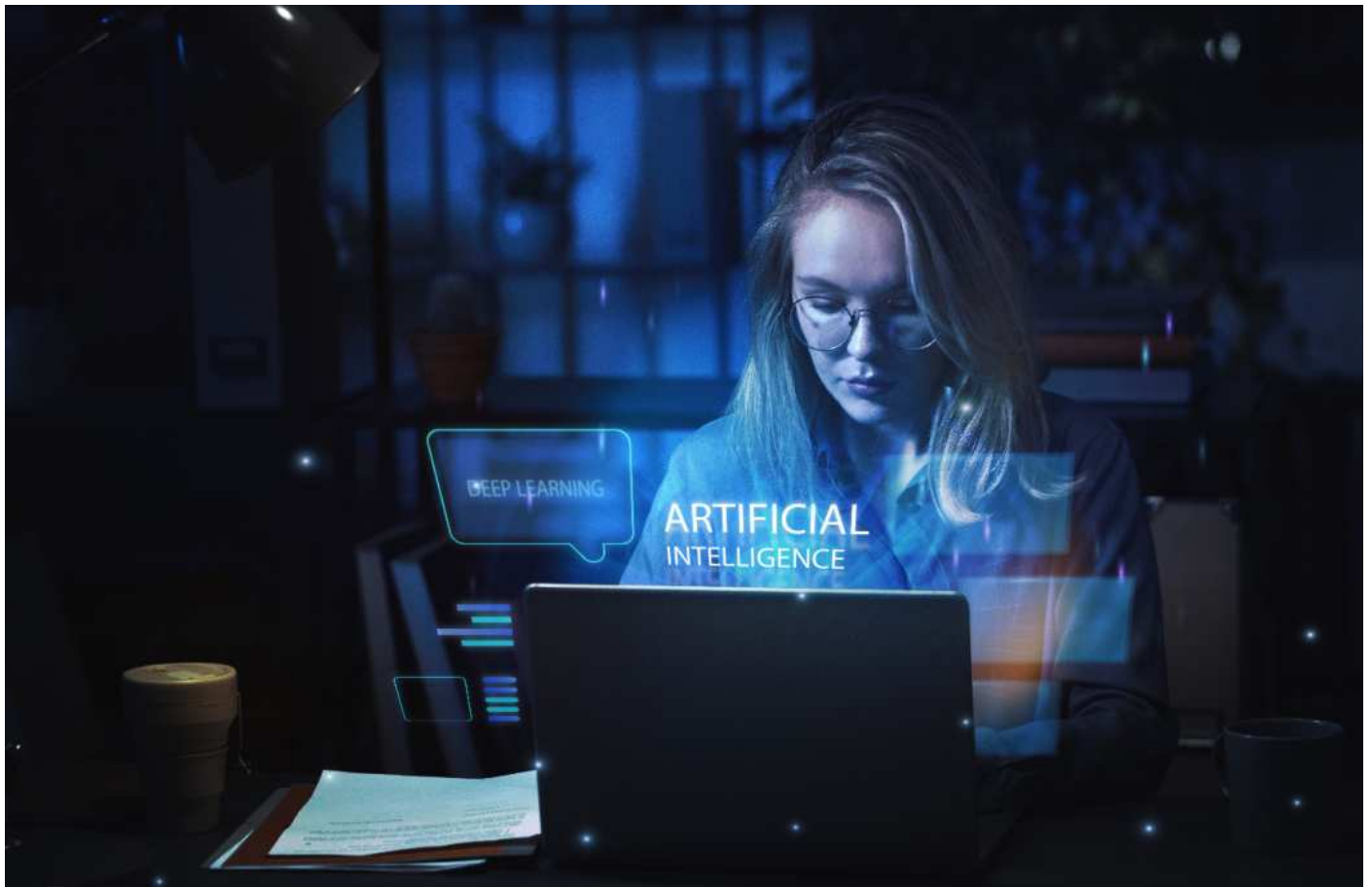
In anticipation of regulatory responses aimed at combating AI risks, Alkassab

outlines proactive measures being undertaken by organizations in the GCC. Conducting thorough compliance audits, implementing robust governance frameworks, and prioritizing data privacy and security throughout the AI lifecycle are deemed critical. Alkassab stresses the significance of open communication and collaboration with regulators, facilitating early adaptation to evolving regulations while sustaining operational efficiency and fostering innovation.

As the GCC navigates the complex landscape of AI-driven cyber threats, collaboration, innovation, and proactive measures emerge as indispensable tools for enhancing collective defense and resilience. Through strategic investments in technology, workforce development, and regulatory compliance, organizations can effectively safeguard against emerging threats and secure the future of cybersecurity in the GCC. 🔥



# AI-driven cyber threats transcend boundaries



**A**s the GCC Cybersecurity market experiences exponential growth, Beernink emphasizes the critical need for dynamic responses to the surge in AI-driven threats. The integration of advanced AI technologies within cyber threats necessitates a paradigm shift towards sophisticated AI-driven defense systems capable of swift threat detection and adaptive responses. Beernink underscores the importance of multi-layered security frameworks, akin to the Cyber Kill Chain, to identify and counter threats at various stages. This approach reflects the region's commitment to staying ahead in a rapidly evolving digital landscape.

In response to malicious actors leveraging AI for sophisticated cyber threats like deepfakes and social engineering, GCC organizations are adopting multifaceted defense strategies. Beernink advocates for the deployment of AI-driven threat detection systems aligned with the Cyber Kill Chain framework, alongside continuous employee training programs to address human factor vulnerabilities. Collaboration between physical and cybersecurity domains intensifies, emphasizing the importance of securing video systems. This proactive stance reflects the region's recognition of the evolving threat landscape and its commitment to safeguarding critical assets.

Facing the growing menace of quantum hacks and adversarial machine learning, GCC organizations must adopt proactive measures to safeguard their cybersecurity. Beernink highlights the importance of continuous investment in research and development for AI-driven threat detection systems, alongside regular cybersecurity training for employees. Collaboration with cybersecurity experts and sharing threat intelligence within the region enhances collective defense capabilities. This forward-thinking approach underscores the GCC's commitment to staying ahead of emerging threats and maintaining resilience in the face of evolving cyber challenges.

Milestone Systems places a strong emphasis on safeguarding against data poisoning challenges in the complex GCC Cybersecurity landscape. Beernink details stringent data validation protocols, advanced anomaly detection algorithms, and continuous monitoring to counter potential manipulations. Regular employee training underscores the importance of vigilance against social engineering attempts, while strategic collaborations with cybersecurity experts strengthen defenses against data integrity threats. This comprehensive defense strategy reflects the region's proactive stance towards ensuring the integrity of critical data assets in an increasingly interconnected digital environment.

As regulatory responses to combat AI risks loom on the horizon,

“

In this digital age, where threats evolve, cybersecurity becomes not just a necessity but an invaluable investment for the future.

### KEY HIGHLIGHTS

- GCC's cybersecurity market rapidly evolves, demanding dynamic responses to AI threats, as outlined by Milestone Systems' VP, Jos Beernink.
- Multi-layered defense, aligned with the Cyber Kill Chain, combats deepfakes and social engineering in GCC, stressing collaboration and secure video systems.
- Proactive measures, like AI threat detection and training, mitigate quantum hacks and machine learning risks in GCC.
- Milestone Systems ensures data integrity through strict validation and collaborations, combating data poisoning in GCC.
- GCC organizations prepare for compliance with robust governance, education, and AI solutions, balancing regulation and efficiency.



**Jos Beernink,**  
Vice President of EMEA at  
Milestone Systems

GCC organizations are proactively preparing to comply with emerging cybersecurity regulations. Beernink highlights investments in robust governance frameworks, continuous education, and training programs, alongside collaborations with regulatory bodies to foster a mutual understanding of technological advancements. Implementing advanced AI-driven cybersecurity measures becomes a focal point, allowing organizations to strike a balance between compliance and operational agility. This proactive approach reflects the region's commitment to maintaining regulatory compliance while fostering innovation and technological advancement.

In the face of AI-driven cyber threats, collaboration and information sharing among organizations in the GCC Cybersecurity community are crucial for enhancing collective defense and resilience. Milestone Systems

actively participates in initiatives like the CVE Program, contributing to identifying and cataloging known cybersecurity issues. This collaborative approach ensures a quicker response to emerging risks and fosters the development of innovative defense mechanisms. It highlights the GCC's recognition of the interconnected nature of cyber threats and the importance of a unified approach to defending against them.

As the GCC navigates the AI-driven cyber threat landscape, collaboration, innovation, and proactive measures emerge as key pillars for securing the future of cybersecurity in the region. By adopting dynamic defense strategies, fostering collaboration, and staying ahead of regulatory requirements, GCC organizations can effectively mitigate emerging threats and maintain the trustworthiness of evolving technologies in an increasingly digital world. ➔

# Focus on the mechanisms for protecting biometric information



**A**lexey Lukatsky, Managing Director, Cyber Security Business Consultant, Positive Technologies gives the brief insights stating that before organizations can effectively combat AI-driven threats, they must address fundamental challenges within their cybersecurity infrastructure. This includes bolstering expertise within cybersecurity teams to ensure they are equipped with the necessary skills and knowledge to identify and respond to emerging threats. Additionally, implementing robust multi-factor authentication mechanisms is essential to enhance the security of access to critical systems and data. Understanding the IT landscape and mapping out company assets is crucial for organizations to identify potential vulnerabilities and prioritize security measures effectively. Moreover, improving security event registration and vulnerability management processes enables organizations to detect and respond to threats in a timely manner, minimizing the impact of cyber attacks.

As malicious actors increasingly leverage AI for sophisticated cyber threats, organizations must deploy strategies to counter these evolving risks. A key focus area is enhancing cybersecurity culture and raising staff awareness to empower employees to recognize and mitigate AI-based social engineering attacks. This involves providing comprehensive training programs and encouraging a culture of vigilance and skepticism

towards suspicious communications. While technical solutions for detecting deepfakes are still evolving, organizations can implement measures such as regular cybersecurity awareness training and robust email filtering systems to mitigate the risk of falling victim to AI-driven phishing attacks.

Quantum hacks and adversarial machine learning pose significant challenges to cybersecurity, requiring organizations to adopt proactive measures to mitigate these risks. Lukatsky recommends leveraging post-quantum encryption algorithms to safeguard communications against potential quantum attacks. Additionally, organizations can invest in developing in-house expertise or partner with specialized vendors to deploy advanced solutions capable of detecting and mitigating adversarial machine learning attacks. By staying abreast of emerging threats and investing in cutting-edge technologies, organizations can enhance their resilience against evolving cyber threats.

**Protecting Data Integrity:** Maintaining the integrity of data is critical to safeguarding against manipulation by malicious actors. Lukatsky emphasizes the importance of deploying sophisticated tools such as Network Traffic Analysis (NTA), Security Information and Event Management (SIEM), and Endpoint Detection and Response (EDR) to protect datasets from poisoning. These tools enable organizations to detect and respond to anomalous activities that may indicate attempts to



“

It is necessary to solve more fundamental issues such as the lack of expertise in corporate cybersecurity teams, the lack of multi-factor authentication, the lack of understanding of companies' assets and their IT landscape

### KEY HIGHLIGHTS

- GCC organizations should prioritize addressing expertise gaps and authentication deficiencies before confronting AI-driven threats.
- Strategies focus on raising cybersecurity awareness to counter evolving risks like deepfakes and social engineering.
- Proactive measures include leveraging post-quantum encryption and developing in-house expertise against quantum hacks.
- Sophisticated tools like NTA and SIEM are deployed to protect data integrity from manipulation by malicious actors.
- Collaborative defense strategies enhance collective resilience through constant communication and information sharing within the GCC cybersecurity community.



**Alexey Lukatsky,**  
Managing Director, Cyber  
Security Business Consultant  
Positive Technologies

manipulate data. Additionally, implementing robust access controls, cryptographic protection mechanisms, and anomaly detection systems helps organizations ensure the integrity of data throughout its lifecycle, from transmission to storage and analysis.

**Navigating Regulatory Compliance:** With regulatory responses to AI risks on the horizon, organizations must prepare to comply while fostering innovation. Lukatsky advises organizations to adopt a cautious approach and await final regulatory frameworks before adapting their strategies. In the interim, organizations can focus on achieving a balance between operational efficiency, security, and innovation by implementing best practices and industry standards. This includes conducting regular risk assessments, implementing robust security controls, and staying informed about emerging regulatory requirements to ensure readiness to comply

with evolving cybersecurity regulations.

**Fostering Collaboration and Information Sharing:** Collaboration and information sharing are essential for enhancing collective defense and resilience against AI-driven threats. Lukatsky underscores the importance of constant communication between cybersecurity professionals and organizations to share threat intelligence and best practices. By establishing formal channels for information sharing within the GCC cybersecurity community and internationally, organizations can leverage collective expertise to stay ahead of emerging threats and bolster their cybersecurity posture. This collaborative approach enables organizations to pool resources, share insights, and coordinate responses to cyber threats, ultimately enhancing the overall resilience of the cybersecurity ecosystem. 🔥

# Trust is good, but control is better



**I**t is quite obvious now that the proliferation of AI-driven technologies poses significant risks to the integrity and confidentiality of organisational communications. As cybercriminals leverage AI advancements to manipulate content and exploit vulnerabilities, the need for robust security measures has never been more critical. Threema OnPrem emerges as a beacon of trust and control, offering organisations a comprehensive solution to safeguard their communication channels against emerging threats while ensuring absolute data ownership and confidentiality.

Threema OnPrem stands out as a pioneering solution, allowing organisations to host their business messaging securely on their own servers. By adopting Threema OnPrem, organisations gain complete control over their data and software, eliminating reliance on third-party service providers. This self-hosted approach empowers organisations to establish a closed communication environment, where data privacy and security are prioritized above all else. With Threema OnPrem, companies can rest assured that their sensitive data remains within their IT infrastructure, enhancing control and minimizing cybersecurity risks.

The rise of AI-driven threats underscores the importance of safeguarding organisational communications against manipulation and exploitation. Threema OnPrem addresses these challenges by providing a closed communication channel exclusive to authorized internal users. By restricting external access to internal

communication, Threema OnPrem mitigates the spread of AI-manipulated content, reducing the likelihood of data breaches and ensuring the confidentiality of sensitive information. This proactive approach to cybersecurity empowers organisations to stay ahead of emerging threats and maintain the integrity of their communication channels.

Threema OnPrem offers organisations unparalleled data ownership and confidentiality through its self-hosting capabilities. By hosting the solution on their own servers, organisations maintain total control over every aspect of the communication tool. This level of control establishes a secure environment that protects against CEO frauds, smishing, and other cyber threats targeting sensitive data. With Threema OnPrem, organisations can confidently safeguard their data, knowing that they retain full control over their communication channels and infrastructure.

#### Adapting to Emerging Cybersecurity Threats

Threema OnPrem's security architecture is designed to adapt to the evolving threat landscape, ensuring ongoing protection against AI-driven risks. By enabling organisations to set up a closed communication channel restricted to authorized internal users, Threema OnPrem minimizes the vulnerability to external threats. This proactive stance against cybersecurity threats empowers organisations to stay ahead of emerging risks and safeguard their sensitive data effectively. With Threema OnPrem, organisations

“

Threema OnPrem is a closed communication channel where only authorised internal users can communicate with each other.

### KEY HIGHLIGHTS

- Robust end-to-end encryption protocols safeguard all Worganizational communications from unauthorized access or interception.
- Multi-factor authentication adds an extra layer of security, reducing the risk of unauthorized access.
- Regular security audits and updates bolster the organization's resilience against evolving threats.
- Comprehensive employee training enhances awareness and equips staff to recognize and respond to security incidents effectively.



**Roman Flepp,**  
Marketing Director  
Threema

can navigate the complexities of the digital landscape with confidence, knowing that their communication channels remain secure and protected.

Threema OnPrem offers a range of features and protocols tailored to maintain a self-contained chat environment, particularly in sectors where data privacy is paramount. With pre-built Docker images and configuration examples, installing updates is streamlined, requiring minimal effort and resources. The use of container technology simplifies the setup process, necessitating only a few open ports and a single DNS record to commence operations. In an era defined by cybersecurity threats, safeguarding

organisational communications is paramount. Threema OnPrem offers organisations a comprehensive solution to protect their communication channels against emerging risks while ensuring absolute data ownership and confidentiality. By empowering organisations with trust, control, and proactive security measures, Threema OnPrem enables them to navigate the complexities of the digital landscape with confidence. As organisations continue to prioritize data security and privacy, Threema OnPrem stands as a trusted partner in safeguarding their communication channels against evolving threats. 🔑



# GCC Unites for Faster AI Cybersecurity Adoption



**S**amer Diya, President of Sales Emerging Markets at Forcepoint, shed light on the evolving cybersecurity landscape and the imperative for collaborative innovation to fortify defenses against emerging threats.

With the proliferation of generative AI, malicious actors are empowered to create sophisticated cyber threats such as deepfakes and social engineering attacks. Samer Diya envisions an evolutionary response from the GCC cybersecurity market, characterized by increased adoption of advanced AI-driven cybersecurity solutions. These solutions leverage generative AI not only for threat detection but also for developing robust defense mechanisms capable of identifying and neutralizing AI-generated threats in real-time. The collaboration between cybersecurity firms and AI researchers is poised to play a crucial role in enhancing the region's cybersecurity posture against evolving threats.

To combat the evolving threat landscape, organizations in the GCC are implementing multifaceted strategies that encompass employee education and the deployment of advanced technologies for threat detection and mitigation. Recognizing the inevitability of human error, organizations prioritize preparing their workforce to safely and securely use AI tools. Additionally, the adoption of comprehensive cybersecurity frameworks such as Zero Trust, coupled with technologies like Data Loss Prevention (DLP) and Risk-Adaptive Protection (RAP), is becoming

increasingly common to safeguard against data breaches originating from AI-generated content.

In response to the growing menace of quantum hacks and adversarial machine learning, organizations in the GCC are embracing proactive measures encompassing employee awareness, technological solutions, and strategic planning. This includes investments in quantum-resistant encryption technologies and the implementation of robust anomaly detection systems capable of identifying and mitigating adversarial attacks on machine learning models. Collaboration with leading research institutions and cybersecurity experts further enhances the region's resilience against emerging threats.

Forcepoint, a leader in cybersecurity solutions, is steadfast in addressing the challenges posed by data poisoning and ensuring the integrity of data against potential manipulation by malicious actors. Leveraging advanced AI-driven anomaly detection systems, Forcepoint proactively identifies and neutralizes data poisoning attempts in real-time, safeguarding the integrity of critical data assets. Additionally, the adoption of Data Loss Prevention (DLP) solutions extends robust policies across web and cloud environments, reinforcing security against AI tools while allowing safe experimentation with new technologies.

As regulatory responses to combat AI risks become inevitable, organizations in the GCC are preparing to comply while maintaining operational efficiency and fostering innovation. By integrating

“

we are seeing more companies turn to advanced AI-driven cybersecurity solutions, leveraging technologies that secure data wherever it resides.

### KEY HIGHLIGHTS

- GCC cybersecurity market anticipates rapid growth, driving adoption of AI-powered defenses against evolving threats.
- Organizations focus on employee education and advanced tech to counter deepfakes and social engineering.
- Proactive measures, including quantum-resistant encryption and anomaly detection, tackle emerging risks.
- Forcepoint's AI-driven solutions safeguard data integrity, preempting manipulation by malicious actors.
- Collaborative efforts among GCC cybersecurity stakeholders strengthen collective defense against AI threats.



**Samer Diya,**  
the President of Sales  
Emerging Markets, Forcepoint.

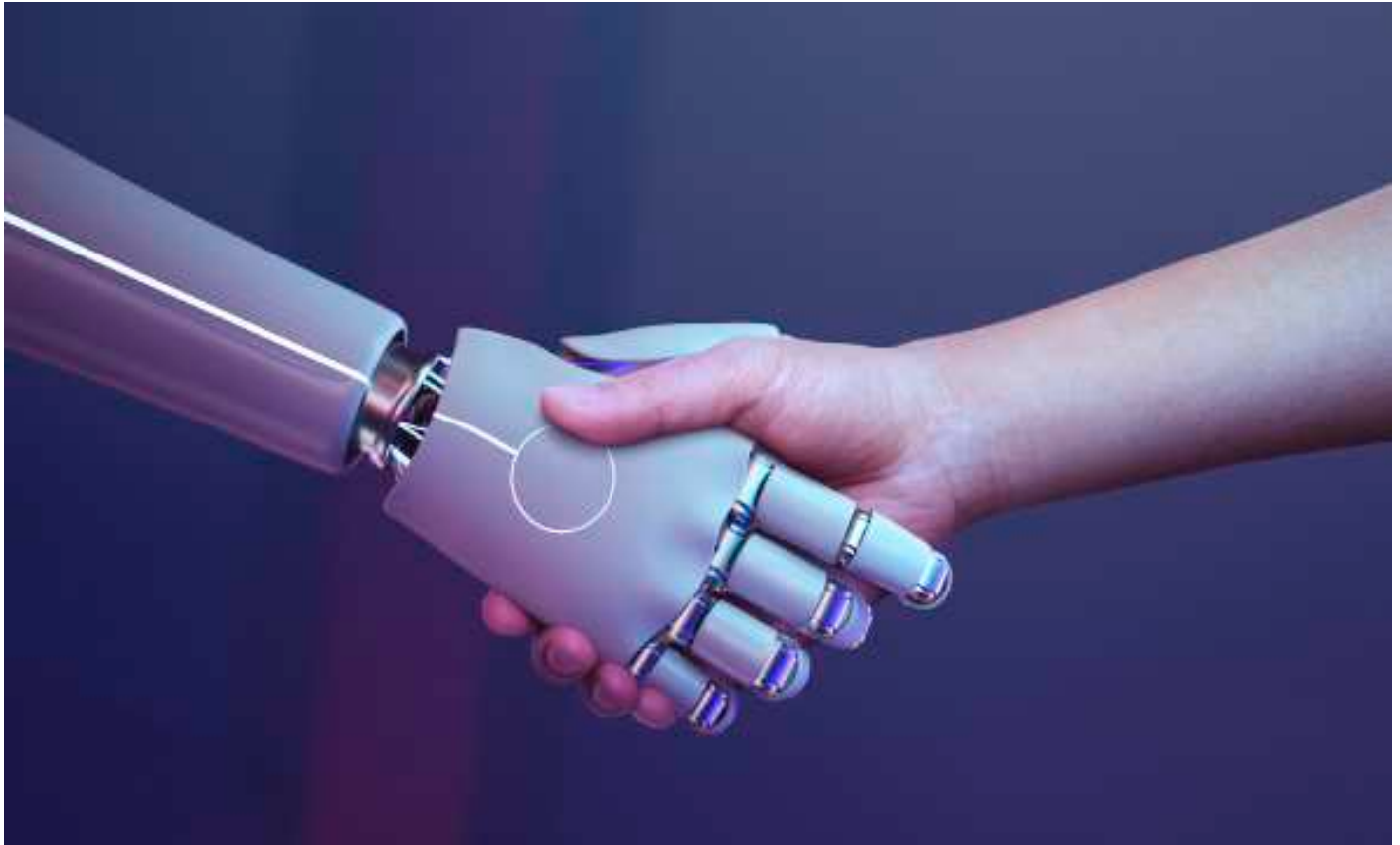
compliance into operational frameworks and investing in solutions that automate regulatory reporting, organizations ensure adherence to emerging cybersecurity regulations without sacrificing efficiency. Forcepoint's Data Security Everywhere capabilities streamline compliance processes by enforcing a single set of policies across managed and unmanaged devices, ensuring data protection and regulatory compliance seamlessly.

In the face of AI-driven cyber threats, collaboration and information sharing among organizations in the GCC cybersecurity community are crucial for enhancing collective defense and

resilience. By pooling insights, experiences, and intelligence, organizations create a formidable barrier against malicious actors, developing unified defense mechanisms and coordinated responses to cyber incidents. Through collaborative initiatives and joint efforts, the GCC cybersecurity community shapes the future of cybersecurity, ensuring sustained resilience against evolving threats.

By embracing advanced technologies, fostering collaboration, and prioritizing cybersecurity awareness, organisations in the GCC navigate the complex threat landscape with confidence, ensuring the security and integrity of digital assets in an increasingly digital world. 🔴

# Generative AI presents a double-edged sword



**G**CC region is witnessing a significant transformation in its cybersecurity landscape, driven by the projected tripling in the size of its cybersecurity market by 2030. This growth is occurring amidst the escalating capabilities of AI-driven threats and the looming menace of quantum hacks. To address these challenges, organizations in the GCC region are adopting proactive measures and innovative strategies to bolster their cybersecurity defenses. This feature explores the evolving cybersecurity landscape in the GCC region and the strategies organizations are employing to navigate the future of cybersecurity.

The GCC cybersecurity market is undergoing rapid evolution in response to the rise of AI-driven attacks. Governments across the region are investing heavily in AI-powered technologies for smart initiatives, necessitating a comprehensive approach to cybersecurity. An agile defense strategy is paramount to effectively refine and deploy AI tools, while robust third-party cybersecurity risk management is essential to safeguard against potential vulnerabilities within the broader ecosystem. Initiatives like the Dubai Cyber Security Strategy and the Saudi Vision 2030 exemplify the region's commitment to building a secure and resilient digital future.

Malicious actors are increasingly leveraging AI for sophisticated cyber threats such as deepfakes and social engineering, posing significant challenges to organizations in the GCC region. In response, organizations

are adopting human-centric cybersecurity approaches, recognizing the importance of human oversight alongside AI automation. Proficiency in data science, machine learning, and programming has become a priority, enabling organizations to develop and deploy AI-driven security solutions effectively. Responsible and ethical design of AI tools is emphasized, with collaboration among governments, businesses, and cybersecurity experts playing a crucial role in addressing AI-enabled cyber threats. Integrating AI and machine learning into security strategies enables organizations to streamline operations, automate tasks, and mitigate potential risks before they escalate into security incidents. Collaboration among GCC countries further strengthens defenses through shared intelligence and the establishment of region-wide cybersecurity standards.

The growing menace of quantum hacks and adversarial machine learning presents significant challenges to cybersecurity in the GCC region. Quantum computing, although still in its nascent stage, poses a substantial threat to current encryption algorithms. As quantum computing progresses, the potential for these machines to break existing encryption methods poses a real concern for businesses. To mitigate these risks, organizations in the GCC region must adopt proactive measures to enhance cybersecurity preparedness. Leadership engagement and clear directives are crucial for developing and implementing effective quantum cyber strategies. By preparing for quantum-resilient cryptographic standards and investing in defending



“

To mitigate the risks of quantum hacks and adversarial machine learning, organizations in the GCC region must adopt proactive measures to enhance cybersecurity preparedness

### KEY HIGHLIGHTS

- GCC cybersecurity market set to triple by 2030, driven by AI threats and tech investments.
- Emphasis on AI integration and collaboration to tackle evolving cyber threats.
- Proactive measures taken to mitigate quantum hacks and adversarial machine learning risks.
- Balancing regulatory compliance with operational efficiency and innovation in GCC cybersecurity.
- GCC's commitment to a secure digital future through collaboration, innovation, and compliance



**Emad Fahmy,**  
Systems Engineering Manager,  
Middle East, NETSCOUT

against quantum threats, organizations can navigate the challenges posed by evolving cyber threats effectively. Additionally, staying ahead of threats becomes vital as the rise of remote work extends the network edge to home environments, making all internet-connected devices susceptible to quantum attacks.

GCC governments have devised long-term strategies to steer their economies away from predominant energy industries and toward technology and innovation. As part of these digitalization initiatives, significant investments have been made in cybersecurity, particularly following the unprecedented Shamoon cyberattack in Saudi Arabia and Qatar in 2012. In response to regulatory responses aimed at combating AI risks, organizations in the GCC region are implementing measures to strengthen their defenses against cyber threats. The ITU Global Cybersecurity Index ranks GCC nations as leaders in cybersecurity

preparedness, reflecting their dedication to cybersecurity. However, concerns remain about the reliability of self-assessment by states, emphasizing the need for continued vigilance and investment in cybersecurity.

**Conclusion:** In conclusion, as organizations in the GCC region navigate the complexities of the evolving cybersecurity landscape, collaboration, innovation, and proactive measures are essential to ensure resilience against emerging threats. By embracing AI and machine learning, preparing for quantum hacks, and complying with emerging regulations, organizations can safeguard their digital assets and contribute to a secure and resilient digital future in the GCC region. Through concerted efforts and strategic investments, the GCC region can continue to lead the way in cybersecurity readiness and pave the path for sustainable growth and prosperity in the digital age. 🔴

# Embrace multi-faceted cybersecurity strategies

With the rapid advancement of AI capabilities, the strategies employed by cybercriminals are poised to become increasingly sophisticated. Anticipating this trend, we can anticipate a surge in AI-driven attacks targeting vulnerabilities within AI-powered systems themselves.

In 2023 Over 12,000 respondents were asked to select the five most significant risks facing their country within the next two years from a list of 35 risks, with “Risk 1” representing the most commonly chosen risk in each economy. In the UAE, Saudi Arabia and Qatar, highlighted countries in the GCC, cybersecurity measures failure ranks fifth and fourths accordingly among global risks, according to the WEF Global Report.

Now, attention has turned towards addressing challenges related to artificial

occupy the fifth place in the UAE and misinformation and disinformation rank fifth in Saudi Arabia for the year 2024. Over 11,000 respondents were tasked with selecting the five most significant risks facing their respective countries in the next two years from a list of 36 risks

## For Qatar the risk has shifted to digital inequality

The shift towards addressing artificial intelligence (AI) challenges signifies a recognition of the evolving cyber threat landscape. In the UAE and Saudi Arabia, the elevation of adverse AI outcomes to top concerns reflects a growing awareness of AI-related risks, including bias and misuse. Concurrently, the prominence of cybercrime in the UAE and misinformation in Saudi Arabia underscores the continued relevance of traditional cybersecurity issues alongside emerging threats. These rankings indicate a nuanced understanding of cybersecurity

Ultimately, this highlights the ongoing efforts to adapt to and combat the diverse nature of cyber threats.

Nevertheless, this impending challenge also presents an opportunity to harness the potential of AI in fortifying our cyber defenses. Today, we’re at the forefront of innovation, diligently crafting AI-powered security solutions that possess the agility and discernment to swiftly detect and respond to threats. By leveraging the prowess of AI, our solutions transcend conventional methods, enabling proactive mitigation and safeguarding against emergent cyber risks. Through our relentless commitment to innovation and cybersecurity resilience, we aim to empower organizations to navigate the dynamic threat landscape with confidence and resilience.

The utilization of AI by malicious actors to fabricate deepfakes and orchestrate intricate social engineering attacks is an escalating concern in today’s digital landscape. Particularly in the GCC region, where organizations are witnessing a surge in such tactics, entities must remain vigilant and fortified against these evolving threats.

IA: For instance, the rise of deepfake technology presents a challenge, as seen in scenarios where business executives or regular employees may unknowingly interact with AI-generated deepfakes during routine video calls. Additionally, the prevalence of QR-based phishing, or “quishing,” underscores the need for proactive measures, especially considering the increasing frequency of such attacks. The number of quishing attacks showed that one out of eight emails with a QR code is malicious. In the second half of 2023, 15% of all emails that contain QR codes were quishing attacks according to Acronis Cyberthreat Report H2 2023. We also are facing the fact that 91.1%



intelligence (AI), resulting in a shift in the highest-ranked risks. In the UAE and Saudi Arabia, adverse outcomes of AI now hold the third-place position, while cybercrime and cyber insecurity

challenges and the need for comprehensive strategies. Organizations and policymakers are urged to prioritize cybersecurity investments, enhance awareness, and foster collaboration to mitigate evolving cyber risks effectively.

“

The looming specter of quantum computing dismantling existing encryption standards poses a significant and pressing concern for cybersecurity practitioners worldwide.

### KEY HIGHLIGHTS

- Advanced AI-driven threat detection ensures real-time identification and mitigation of security risks.
- Robust end-to-end encryption protocols safeguard all organizational communications from unauthorized access or interception.
- Multi-factor authentication adds an extra layer of security, reducing the risk of unauthorized access.
- Regular security audits and updates bolster the organization's resilience against evolving threats.
- Comprehensive employee training enhances awareness and equips staff to recognize and respond to security incidents effectively.



**Irina Artioli,**  
Cyber Protection Evangelist at  
Acronis

#### Saudi Arabia

- 1 Cost-of-living crisis
- 2 Interstate conflict
- 3 Rapid and/or sustained inflation
- 4 Severe commodity price shocks
- 4 Breakdown of critical infrastructure
- 4 Failure of cybersecurity measures

of organizations have already faced AI-enhanced phishing.

To effectively combat these threats, organizations are adopting a multifaceted cybersecurity approach. This includes implementing robust defense mechanisms across multiple layers of their IT infrastructure. For example, organizations should focus on stopping phishing threats at the time of

delivery, but also investing in detection technologies capable of identifying and neutralizing malware in the later stages of the attack cycle. Furthermore, processes need to be adapted and followed through. For example payment transaction should not be authorized by a video call only, but should require the person to sign it off in the online system as well.

Additionally, fostering a culture of cybersecurity awareness through comprehensive user education programs is critical. By educating employees about various social engineering techniques employed by cybercriminals, organizations can strengthen their human firewall and reduce the risk of falling victim to deceptive schemes.

Moreover, deploying cutting-edge threat detection solutions equipped with AI capabilities is indispensable. These sophisticated systems possess the adeptness to discern anomalies indicative of deepfake manipulation, enabling organizations to swiftly identify and



neutralize fraudulent content before it can wreak havoc.

The looming specter of quantum computing dismantling existing encryption standards poses a significant and pressing concern for cybersecurity practitioners worldwide. Although quantum computers are still in nascent stages of development, the potential ramifications of their exponential computational power on encryption protocols cannot be understated. In the GCC region, organizations are urged to adopt a proactive stance in addressing this emergent threat.

To effectively mitigate the risks posed by quantum computing, organizations must embrace a multi-faceted approach to cybersecurity. Firstly, it is imperative to transition towards quantum-resistant cryptography, which involves the deployment of encryption algorithms immune to the computational prowess of quantum machines. By embracing these quantum-safe cryptographic techniques, organizations can fortify their data protection measures and preemptively safeguard against the impending threat of quantum-based attacks.

Additionally, organizations should invest in security solutions equipped with the capability to detect and counter adversarial machine learning attacks. As AI-driven cyber threats continue to proliferate, it becomes paramount to deploy advanced security mechanisms capable of discerning and mitigating sophisticated attacks orchestrated by malicious actors leveraging machine learning algorithms.

Data poisoning represents an escalating threat landscape wherein nefarious actors manipulate datasets with the intent to compromise the integrity and efficacy of AI models. This insidious tactic not only undermines the reliability of AI-driven systems but also poses significant risks to organizational security and decision-making processes. In response, organizations operating within the GCC region must adopt a proactive approach to mitigate the perils associated with data poisoning.

Central to addressing the menace of data poisoning is the implementation of robust data provenance solutions. These sophisticated systems are instrumental in tracing the lineage and historical

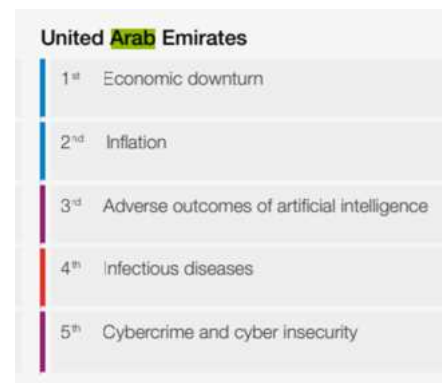


trajectory of data, thereby facilitating comprehensive visibility into its origin, evolution, and usage. By leveraging data provenance technologies, organizations can establish a stringent accountability framework, enabling them to pinpoint and rectify instances of data manipulation or tampering effectively.

Moreover, organizations must bolster their defense mechanisms by employing anomaly detection techniques tailored to identify aberrant patterns or deviations within datasets. These anomaly detection algorithms serve as vigilant sentinels, swiftly flagging suspicious alterations or anomalies indicative of potential data poisoning attempts. Through the integration of anomaly detection methodologies, organizations can proactively fortify their data integrity defenses and preemptively thwart malicious data manipulation endeavors.

As the digital landscape evolves, the emergence of stringent cybersecurity regulations stands as a pivotal step towards elevating the standards of data protection and safeguarding sensitive information against an increasingly sophisticated threat landscape. For organizations operating within the GCC, compliance with these evolving regulations should not be perceived merely as a regulatory burden, but rather as a strategic imperative to fortify their security posture and engender trust among stakeholders.

By adhering to cybersecurity regulations, organizations can establish a robust framework that not only mitigates the risk of data breaches and cyber-attacks but also fosters a culture of accountability and transparency. Compliance serves as a cornerstone for bolstering organizational



resilience, enabling entities to proactively identify and address vulnerabilities, and fortify their defense mechanisms against evolving cyber threats.

In the increasingly interconnected and dynamic digital landscape, the proliferation of complex cyber threats underscores the indispensable need for collaboration and information sharing within the GCC cybersecurity community. Recognizing the collective nature of the cyber threat landscape, it is imperative for stakeholders across the region to unite efforts, share insights, and collectively fortify their defenses against evolving cyber adversaries. This allows organizations to react quickly to new emerging threat waves.

Collaboration serves as a linchpin for enhancing cybersecurity resilience, enabling the GCC cybersecurity community to pool resources, expertise, and intelligence to effectively combat emerging threats. By fostering an ecosystem of collaboration, stakeholders can leverage collective wisdom and experience to stay ahead of cyber adversaries, identify emerging threat vectors, and devise proactive defense strategies.🔥

## A Strategic Imperative

### TechOps

Streamline their IT infrastructure and improve operational efficiency, which can result in lower costs and increased productivity.



### Competency Framework

Assess your current capabilities architecture and identify areas for improvement, helping you to make informed decisions about where to invest your technology resources



### TechSust Align

Optimize and improve your technology systems, ensuring they are operating at peak efficiency and effectively supporting your business goals.



### Biz Insights

Provide advanced analytics services, leveraging the latest technologies and techniques to help you turn your data into actionable insights.



### DXT

Develop a digital strategy that aligns with your business objectives, enabling you to stay ahead of the curve in a rapidly changing digital landscape.



# Organisations must grasp Quantum Computing's encryption threat



Organisations in the GCC region are facing unprecedented challenges posed by advanced threats leveraging AI and quantum computing. As malicious actors continue to innovate their tactics, GCC organizations are adopting proactive strategies and collaborative measures to fortify their defenses and ensure the integrity of their data.

The advent of AI has ushered in a new era of cyber threats, with malicious actors leveraging its capabilities for sophisticated attacks such as deepfakes and social engineering. Recognizing the potency of AI in both offense and defense, organizations in the GCC are embracing AI-driven security solutions to bolster their resilience.

Intelligent AI-driven email security systems are being employed to identify phishing patterns, analyze content for malicious intent, and spot unknown threats. Additionally, AI is enhancing application security by detecting anomalies, adjusting machine learning models, and accelerating threat detection and intelligence.

Furthermore, AI-enabled incident response mechanisms empower security teams to swiftly detect, contain, and neutralize attacks, mitigating human error and accelerating incident triage. By leveraging AI, organizations in the GCC are equipping themselves with the tools needed to counter the evolving threat landscape effectively.

The emergence of quantum computing poses a formidable challenge to traditional encryption schemes, necessitating proactive measures from GCC organizations. Understanding the potential vulnerabilities, organizations are evaluating their encryption technologies and considering replacements to mitigate the risk of quantum hacks.

While quantum computing remains a nascent technology with limited applications, GCC organizations are adopting a cautious approach, recognizing the importance of ongoing vigilance and preparedness. By staying informed and prioritizing cybersecurity initiatives, organizations are positioning themselves to adapt to emerging threats effectively.

The rise of threats such as data poisoning and ransomware underscores the importance of safeguarding data integrity in the GCC cybersecurity landscape. Organizations are investing in robust backup and recovery solutions to mitigate the impact of data manipulation attacks.

Utilizing solutions that offer immutable backups and secure recovery mechanisms, organizations can ensure the integrity of their data against malicious actors. By implementing multifactor authentication and secure interfaces, organizations enhance their resilience against data manipulation threats, safeguarding critical assets and ensuring business continuity.



“

As an immediate action, organisations must approach security as an ongoing endeavour, starting with easily achievable tasks and steadily enhancing defences rather than focusing on threats that are still on the horizon.

### KEY HIGHLIGHTS

#### **AI Defense Adoption:** GCC

organizations are increasingly adopting AI-driven cybersecurity solutions to counter advanced threats like deepfakes and social engineering, bolstering their defense mechanisms.

**Quantum Threat Preparedness:** With quantum computing on the horizon, GCC entities are proactively evaluating encryption technologies to address potential vulnerabilities, ensuring data security in the face of evolving cyber risks.

**Data Integrity Safeguarding:** Robust backup and recovery solutions are being implemented by GCC organizations to protect against data manipulation threats such as ransomware and data poisoning, ensuring business continuity and data integrity.

#### **Collaborative Defense Frameworks:**

Collaboration and information sharing among GCC cybersecurity stakeholders are paramount, enabling collective defense strategies to effectively confront emerging cyber threats and mitigate risks.

#### **Regulatory Advocacy and Compliance:**

GCC organizations are advocating for regulatory frameworks and standards tailored to the region's cybersecurity landscape, fostering an environment conducive to innovation and compliance while addressing unique challenges.



**Vishal Pala,**

Senior Solutions Engineer  
– META, Barracuda

In the face of AI-driven cyber threats, collaboration and information sharing have emerged as essential pillars of collective defense in the GCC cybersecurity community. By fostering collaborative efforts, organizations can exchange threat intelligence, stay abreast of evolving tactics, and enhance their collective resilience.

Collaborative initiatives enable early detection and response to cyber incidents, leveraging pooled resources and advanced detection capabilities. Moreover, sharing best practices and lessons learned elevates cybersecurity awareness and education, empowering stakeholders to mitigate risks effectively.

Furthermore, collaborative efforts pave the way for the development of robust

cybersecurity policies and regulations tailored to the GCC region's unique challenges. By advocating for regulatory frameworks and standards, organizations foster an environment conducive to cybersecurity innovation and compliance.

In conclusion, as GCC organizations navigate the complex cybersecurity landscape, they are leveraging AI-powered defense mechanisms, mitigating quantum threats, safeguarding against data manipulation, and embracing collaborative measures to enhance collective defense and resilience. By harnessing the power of AI and fostering collaboration, GCC organizations are poised to confront emerging cyber threats with agility and effectiveness, safeguarding their digital assets and ensuring a secure future. 🔥

# GCC firms gear up for cyber regulations with strategic moves



In recent years, the Middle East has witnessed a surge in interest in Artificial Intelligence (AI) adoption, with several GCC countries prioritizing emerging technologies in their national strategies. Emile Abou Saleh, Senior Director of Proofpoint Middle East, Turkey & Africa, sheds light on the evolving GCC cybersecurity landscape and the strategies organisations are adopting to combat escalating AI-driven threats.

The GCC cybersecurity market is poised for significant growth, projected to triple in size by 2030. With AI playing a pivotal role in both offensive and defensive cyber operations, the demand for sophisticated cybersecurity solutions is on the rise. End-user spending on security and risk management in the MENA region is expected to reach \$3.3 billion by 2024, reflecting a 12.1% increase from the previous year. As organisations grapple with a fast-paced evolution in the threat landscape, comprehensive cybersecurity strategies that encompass people, processes, and technology are imperative.

Malicious actors are leveraging AI to intensify cyber threats such as phishing and malware, presenting significant challenges to existing cybersecurity defenses. Saleh emphasizes the importance of human-centric cybersecurity strategies, including comprehensive employee training and the adoption of advanced technologies such as AI-powered email security and behavioral analysis platforms. By empowering employees to recognize and resist threats,

organisations can fortify their security posture against evolving AI-driven attacks.

To combat the rising threat of adversarial machine learning, organisations in the GCC region must adopt proactive cybersecurity measures. Saleh outlines key strategies, including robust and preemptive email security, user education, cloud security implementations, and multi-factor authentication. By embedding a culture of continuous cybersecurity awareness and shared responsibility across the organisation, GCC organisations can enhance their defense posture against evolving cyber threats.

Proofpoint employs a comprehensive strategy to address the complexities of the GCC cybersecurity landscape, particularly the challenges of data poisoning and safeguarding data integrity. Leveraging innovations across threat protection, identity defense, and information protection platforms, Proofpoint offers advanced email security measures, identity protection, and data loss prevention strategies to secure sensitive data from theft, loss, and insider threats.

As regulatory scrutiny increases, organisations in the GCC must prioritize compliance with emerging cybersecurity regulations while fostering innovation and maintaining operational efficiency. Saleh discusses proactive measures organisations can take, such as implementing best practices in AI development and deployment and staying vigilant about policy changes to adapt proactively to

“

Staying vigilant about developments in the cybersecurity landscape, including policy changes and draft regulations specific to AI will enable organizations to adapt proactively to emerging requirements.

### KEY HIGHLIGHTS

- GCC cybersecurity market is projected to triple by 2030, with \$3.3 billion expected in end-user spending by 2024, driven by escalating AI-driven threats.
- Human-centric cybersecurity strategies, including comprehensive employee training and advanced AI-powered defenses, are prioritized by GCC organizations to counter malicious AI-driven attacks.
- Proactive measures such as robust email security, user education, and multi-factor authentication are adopted by GCC organizations to mitigate risks of quantum hacks, adversarial machine learning, and data poisoning.
- GCC organizations prepare to comply with emerging cybersecurity regulations by implementing AI best practices and staying vigilant about policy changes.
- Collaborative defense and information sharing among GCC cybersecurity stakeholders are crucial for enhancing collective resilience against AI-driven cyber threats.



**Emile Abou Saleh**

Senior Director of  
Proofpoint Middle East,  
Turkey & Africa

regulatory requirements.

In the face of AI-driven cyber threats, collaboration and information sharing among organisations in the GCC cybersecurity community are critical. Saleh emphasizes the importance of sharing threat intelligence and coordinating responses to enhance collective defense measures. By fostering collaboration between government agencies and private sector organisations, the GCC cybersecurity community can better protect itself against the increasing risk of AI-driven cyberattacks.

As organisations in the GCC navigate the evolving cybersecurity landscape amidst

AI-driven threats, proactive measures and collaborative efforts are essential to safeguarding digital assets and ensuring operational resilience. By adopting comprehensive cybersecurity strategies, leveraging advanced technologies, prioritizing regulatory compliance, and fostering collaboration, GCC organisations can mitigate emerging threats effectively and strengthen their defense posture against evolving cyber risks. Through collective action and continuous vigilance, the GCC cybersecurity community can confront the challenges posed by AI-driven threats with confidence and resilience. 🔥



# Proactive cyber regulation compliance with efficiency is the need of hour

**A**I and operational technology (OT) presents both immense opportunities and significant challenges for organizations across various industries. As malicious actors increasingly leverage AI for sophisticated cyber attacks such as deepfakes and social engineering, organizations must adopt proactive strategies and technologies to bolster their defenses against these evolving threats.

One of the primary applications of AI in cybersecurity lies in threat detection and analysis. AI algorithms excel at processing large volumes of data quickly, allowing organizations to analyze patterns and detect anomalies that may indicate a cybersecurity threat. Whether it's unusual network traffic or suspicious user behavior, AI-powered systems can identify potential threats in real-time, enabling organizations to respond swiftly and effectively.

Furthermore, AI plays a crucial role in phishing detection, a prevalent method used by cybercriminals to infiltrate organizations. By analyzing email content, AI algorithms can identify potential phishing attempts, preventing end-users from falling victim to convincing AI-generated phishing emails. This proactive approach significantly reduces the risk of data breaches and financial losses associated with phishing attacks.

Moreover, AI contributes to vulnerability management by continuously scanning and analyzing an organization's software and infrastructure for potential weaknesses. By identifying vulnerabilities promptly, organizations can take proactive measures to patch or mitigate these risks, strengthening their overall cybersecurity posture.

In addition to threat detection and vulnerability management, AI enables automated threat response, empowering organizations to automate responses to identified threats. Whether it's isolating affected systems, blocking suspicious IP addresses, or patching vulnerabilities, AI-driven automation streamlines response efforts and minimizes the impact of cyber attacks.

Despite the significant benefits AI brings to cybersecurity, organizations must also address the risks posed by advanced

threats such as quantum hacks and adversarial machine learning. Adopting a defense-in-depth approach is crucial, involving multiple layers of defense, including network segmentation, intrusion detection systems, and endpoint protection. This multi-layered approach mitigates the impact of advanced threats and reduces the likelihood of successful cyber intrusions.

Furthermore, organizations must invest in enhanced threat intelligence and monitoring to detect and respond to emerging threats effectively. By monitoring networks for suspicious activities and indicators of compromise, organizations can detect and mitigate threats before they escalate, enhancing overall cybersecurity resilience.

As regulatory responses to combat AI risks become inevitable, organizations in the GCC region must proactively prepare to comply with emerging cybersecurity regulations while maintaining operational efficiency and innovation. This involves establishing dedicated teams or departments tasked with monitoring regulatory developments and ensuring organizational compliance. By implementing cybersecurity frameworks and adopting best practices, organizations can proactively safeguard against AI-related risks while fostering innovation.

Collaboration and information sharing among organizations in the GCC cybersecurity community are paramount to enhancing collective defense and resilience against AI-driven cyber threats. By building partnerships, participating in joint exercises, and leveraging technologies such as threat intelligence platforms, organizations can exchange insights, threat indicators, and best practices, strengthening the overall cybersecurity ecosystem in the region.

Looking ahead, the future of AI-powered digital twins in OT environments holds significant promise and challenges. While digital twins offer a virtual replica of OT environments for testing and optimization, organizations must exercise caution when applying AI technology in real-world production environments. Striking the right balance between innovation and risk management

“

The first step is to put checks and balances in place for AI, limiting adoption to lower impact areas to ensure that availability is not compromised

### KEY HIGHLIGHTS

- AI-driven cybersecurity enhances threat detection and response, fortifying defenses against evolving cyber threats.
- Proactive defense strategies, such as network segmentation and threat intelligence, mitigate the impact of advanced threats like quantum hacks.
- Compliance readiness ensures organizations in the GCC region align with emerging cybersecurity regulations while fostering innovation.
- Collaboration among GCC cybersecurity stakeholders strengthens collective defense capabilities against AI-driven threats.
- AI's role in red team & blue team exercises improves cyberattack simulations, enhancing overall defense and response strategies.



**Rami Nehme,**  
Regional Sales Director  
OPSWAT

is essential to ensure the safe and secure adoption of AI in OT.

In conclusion, navigating the evolving landscape of AI in cybersecurity and operational technology requires a proactive approach, leveraging AI-driven technologies to enhance threat detection, vulnerability management, and automated

response capabilities. By adopting a defense-in-depth approach, complying with emerging regulations, and fostering collaboration within the cybersecurity community, organizations can effectively mitigate the risks posed by advanced cyber threats while embracing the transformative potential of AI in the digital age. 🏹

# Efficient cyber regulation compliance is the need of the hour



**D**r. Wael Kanoun, Managing Director of Cyber Solutions at Thales Middle East and KSA, explores the evolving landscape of cybersecurity in the GCC region. Dr. Kanoun shares insights into the projected growth of the GCC cybersecurity market, strategies to combat AI-driven threats, proactive measures against emerging risks, and the importance of collaboration for collective defense.

With the GCC cybersecurity market poised to triple by 2030, Dr. Kanoun envisions a stronger sector bolstered by comprehensive laws and regulations. The UAE's Cybersecurity Council and KSA's National Cyber Agency are pivotal in thwarting increasingly sophisticated threats. Investments in cybersecurity education and training programs are crucial to address talent shortages, ensuring a skilled workforce capable of dissolving potential threats.

Organizations in the GCC are ramping up efforts to combat AI-driven threats, including deepfakes and social engineering. Dr. Kanoun highlights the deployment of artificial intelligence to prevent security incidents, with significant investments planned in the UAE. Quantum computing is also on the horizon, offering advanced encryption capabilities. Collaborations with

government entities, such as Thales' partnership with the Dubai Electronic Security Centre, underscore the commitment to strengthening cybersecurity infrastructure.

As the menace of quantum hacks and adversarial machine learning grows, Dr. Kanoun emphasizes a Defense-in-Depth approach. Thales is actively developing security measures against adversarial machine learning and Quantum Computing enabled attack techniques, including the Falcon algorithm for post-quantum cryptography. Protecting data integrity against manipulation by malicious actors is paramount, with a holistic approach encompassing technical solutions, governance processes, and comprehensive training programs.

In an era where data is likened to oil, safeguarding data integrity is imperative. Dr. Kanoun underscores the importance of employing state-of-the-art technologies for encryption and key management. Thales' cybersecurity portfolio, enhanced by the addition of Imperva, offers solutions to protect applications, data, and identities. Collaboration with Intel Trust Authority enables end-to-end data security using confidential computing, ensuring compliance with emerging regulations while maintaining operational efficiency.



“

Falcon algorithm, a post-quantum cryptography standard that can withstand attacks from future powerful quantum computers.

### KEY HIGHLIGHTS

- GCC cybersecurity sector witnessing comprehensive regulatory advancements to combat evolving threats.
- Rising demand for skilled cybersecurity workforce amidst talent shortages in the UAE and Saudi Arabia.
- Emphasis on Defense-in-Depth approach to mitigate risks posed by data poisoning and manipulation.
- Compliance with emerging cybersecurity regulations crucial, with Thales providing solutions for regulatory adherence.
- Collaboration and information sharing vital for GCC cybersecurity community to stay ahead of sophisticated adversaries.



**Dr. Waël Kanoun,**  
Managing Director of  
Cyber Solutions, Thales  
Middle East and KSA

Dr. Kanoun highlights the significance of compliance with emerging cybersecurity regulations, akin to GDPR requirements. All GCC states have developed national cybersecurity strategies and introduced regulations to combat cybercrime and ensure data privacy. Thales' collaboration with Intel Trust Authority facilitates compliance with data protection regulations while retaining control over cryptographic key material, eliminating the need to place complete trust in cloud providers.

In the face of AI-driven cyber threats, collaboration and information sharing are paramount. Dr. Kanoun stresses the need for a united approach to enhance collective defense and resilience. By pooling resources, expertise, and threat intelligence, organizations in the GCC cybersecurity

community can identify emerging threats faster and develop robust defense strategies. Fostering a culture of cooperation ultimately bolsters the region's cybersecurity resilience against sophisticated adversaries.

As the GCC cybersecurity landscape evolves, collaboration, innovation, and proactive measures are essential for safeguarding digital assets. Dr. Kanoun's insights shed light on the strategies and innovations employed by organizations in the GCC region to combat AI-driven threats and navigate the complex cybersecurity landscape. With a united approach and a focus on collaboration, the GCC is poised to enhance collective defense and resilience against emerging cyber threats, ensuring a secure future for all. 🏹

# Collaborative efforts enable quicker identification



**T**he projected tripling in size of the GCC cybersecurity market by 2030 signifies a significant shift in the region's approach to cybersecurity. As the size of the market expands, organisations are recognising the need to adapt to the escalating capabilities of AI-driven threats. Projections suggest a substantial growth rate, indicating a market volume of US\$1.98 billion by 2028. This growth is driven by the proliferation of AI technologies and their adoption by malicious actors to launch sophisticated cyber-attacks. To address these challenges, the GCC cybersecurity market is witnessing increased investment in AI-powered security solutions. According to a survey by Gartner, 34% of organisations are presently utilising or implementing AI application security tools. Moreover, collaboration and information sharing among GCC countries are becoming essential to combat AI-driven threats effectively. By exchanging threat intelligence and best practices, governments and organisations can enhance their cybersecurity posture and mitigate potential risks.

Organisations in the GCC region are implementing advanced strategies and technologies to bolster their defences against AI-driven threats such as deepfakes and social engineering attacks. This includes investments in AI-driven threat detection systems, behavioural analytics tools, and employee training programmes. The adoption of multi-

faceted approaches aims to strengthen defences against evolving cyber threats. Employee education and awareness programmes are crucial to empowering personnel to recognise and respond to suspicious activities effectively. Additionally, collaborations with cybersecurity vendors and AI researchers are facilitating the development of innovative security solutions tailored to the region's specific challenges.

To mitigate the risks posed by quantum hacks and adversarial machine learning, organisations in the GCC region are adopting proactive measures. This includes investments in robust encryption techniques resistant to quantum computing attacks and the deployment of advanced anomaly detection systems. Collaboration with leading research institutions and cybersecurity experts is enabling organisations to stay ahead of emerging threats and develop innovative countermeasures. By fostering collaboration and information sharing, GCC countries can develop comprehensive strategies to combat these evolving cyber threats effectively.

Organisations in the GCC region are implementing comprehensive security policies and frameworks to safeguard against data poisoning and ensure data integrity. This involves deploying robust encryption techniques, AI-driven anomaly detection systems, and regular audits to proactively identify and neutralise data poisoning attempts. Compliance with regulatory requirements, such as data protection laws, is essential to

“

Organisations should enhance their AI defences by deploying advanced anomaly detection and adaptive security measures to effectively detect and respond to adversarial machine learning attacks.

### KEY HIGHLIGHTS

#### **GCC Cybersecurity Market Growth:**

The GCC cybersecurity market is projected to triple in size by 2030, reaching a volume of US\$1.98 billion by 2028, driven by increasing AI-driven threats.

#### **AI-Powered Defence Strategies:**

Organisations in the GCC are adopting AI-driven security solutions to counter deepfakes and social engineering, with 34% already utilising AI application security tools.

#### **Proactive Measures Against Emerging Threats:**

Investments in quantum-resistant encryption and anomaly detection systems are being made to mitigate risks posed by quantum hacks and adversarial machine learning.

#### **Comprehensive Data Protection:**

Organisations are implementing robust security policies and frameworks to safeguard against data poisoning and ensure data integrity, with compliance becoming increasingly vital.

#### **Collaborative Defence Approach:**

Collaboration and information sharing among GCC cybersecurity communities are essential for enhancing collective defence and resilience against evolving cyber threats, fostering a united front in cybersecurity efforts.



**Abrar Ullah,**

Associate Professor, Mathematical and Computer Sciences, Heriot-Watt University Dubai

maintaining data integrity and trust. Moreover, collaborations with regulatory authorities and industry peers are integral to staying informed about evolving regulations and best practices.

As regulatory responses to combat AI risks become inevitable, organisations in the GCC region are proactively preparing to comply with emerging cybersecurity regulations. This includes investments in comprehensive cybersecurity frameworks, employee training programmes, and collaborations with regulatory authorities. By integrating compliance into their operational frameworks and innovation strategies, organisations can navigate regulatory challenges effectively while maintaining operational efficiency and

innovation.

Collaboration and information sharing among organisations in the GCC Cybersecurity community are crucial for enhancing collective defence and resilience. By sharing threat intelligence and best practices, organisations can stay ahead of emerging threats and bolster their cybersecurity posture. Collaborative efforts enable quicker identification and mitigation of cyber threats, reducing the impact of attacks on individual organisations and the broader community. Moreover, collaborations with national CERTs and industry associations facilitate the exchange of insights and experiences, fostering a united front against evolving cyber threats in the GCC region. 🔥





# What's trending







معرض و مؤتمر الخليج العالمي للأمن المعلومات

**GISEC**  
GLOBAL

**23-25 APR 2024**  
DUBAI WORLD TRADE CENTRE

**THE SUPER CONNECTOR**  
EVENT FOR

**CYBERSECURITY**  
**COMMUNITY**

SCAN HERE



**EMPOWER THE**  
**CYBER-SECURED FUTURE**

Enquire about Exhibiting, Sponsorship,  
Speaking Opportunities & more!

gisec@dwtc.com | tel: +971 4 308 6469

#gisecglobal | gisec.ae

HOSTED BY

مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL

OFFICIAL GOVERNMENT  
CYBERSECURITY PARTNER

مجلس الأمن الإلكتروني  
CYBERSECURITY COUNCIL

OFFICIALLY SUPPORTED BY



شرطة دبي  
DUBAI POLICE



TDR  
هيئة تنظيم الاتصالات  
والتجارة الإلكترونية  
DUBAI WORLD TRADE CENTRE

ORGANISED BY



DUBAI WORLD TRADE CENTRE

POWERED BY

**BOTS** | **GLOBAL  
CIO  
FORUM**



THE  
WORLD  
CIO 200  
SUMMIT

**2024 ROADSHOW**

MAY-SEPTEMBER 2024

# UNLEASH THE MIGHT



50  
COUNTRIES

4000  
C-LEVEL EXECS

300+  
SESSIONS

200+  
EXHIBITORS