معرض و مؤتمر الخليج العالمي لأمن المعلومات
GISEC GLOBAL

times

GISEC 2022 SPECIAL DAILY

BROUGHT BY
Enterprise CHANNELS MEA

21 MARCH – 23 MARCH 2022

Day Two

Future IT Summit 2022 attracts close to 200 enterprise and industry executives

Carrying forward its legacy of the past eight years, The Future IT Summit and Catalysts Awards 2022 was successfully held at Conrad Hotel, Dubai on 17th March 2022. The event brought together some of the major names of technology and included a series of insightful presentations, round table meetings, and incisive panel discussions.

The event was started with an opening keynote by Ronak Samantaray, Co-founder and CEO, GEC Media Group and he extended a warm welcome to all the honourable guests and speakers with utmost gratitude for joining him in-person at FITS 2022.

The event saw the participation of high profile industry and enterprise executives including Hanan Huwair; Arul Jose Vigin, Charbel Zreiby, Samer Semaan, Ehab Eid, Sheridan Moodley, Mohammad Qattash, Taufiq Rahman, Dinesh Chandra, Mohammad Al-Jallad, Basil Ayass, Maya Zakhour, Awais Bin Imaran, Damir Jaksic, Kashif Rana, Ahmad Alabbi, Loubna Imenchal, Thomas Gigi Mathew, Mario Veljovic, Shameema Parveen, Salma Awwad, Veronica Ustinova, Yasmin Al Rawi, Debbie Botha, Zaid F Ghattas, Manal Allam, Ali El Kontar, Shrenik Jain, Pratap Patjoshi, Binita Prasad, Sridhar Rajagopal, and Mario Foster, amongst others.

The Future IT Summit 2022 event partners included:

Platinum Partners: Dell Technologies and Mindware, Zero & One and AWS, Epicor.

Gold Partners: Automation Anywhere, Freshworks and VAD Technologies, HPE and Emitac Enterprise Solutions, Netapp and Ingram Micro, Logitech and Ingram Micro, Pure Storage and Teksalah, AMD, Securenet.

Exhibiting Partners: HTP, Virsec, Nakivo, Scality.

Supporting Partners: Infoblox, Raqmiyat, Finesse, ASBIS and Sherpa Communications.

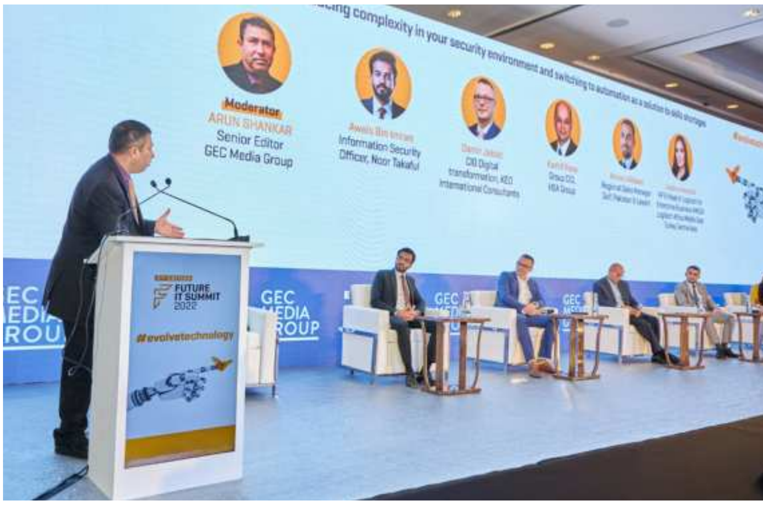
GEC MEDIA'S FUTURE IT S

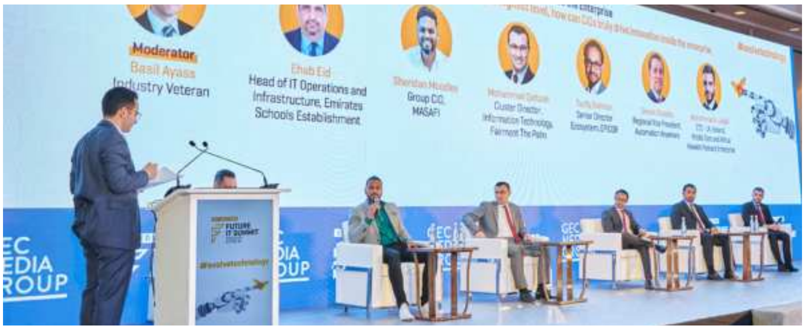
Expert Panel : Reducing complexity in your security environment and switching to automation as a solution to skills shortages
Moderator
ARUN SHANKAR
Senior Editor
GEC Media Group
Awais Bin Imran
Information Security Officer, Noor Takaful
Damir Jaksic
CIO Digital transformatio KED
International C ltants
Kashif Rana
Group CIO, HSA Group
Ahmad AlAbbadi
Regional Sales Manager Gulf, Pakistan & Levant
Loubna Imenchal
VP & Head of Logitech for Enterprise Business AMECA Logitech Africa Middle East Turkey Central Asia
GEC
FUTURE IT SUMMIT 2022

UMMIT 2022

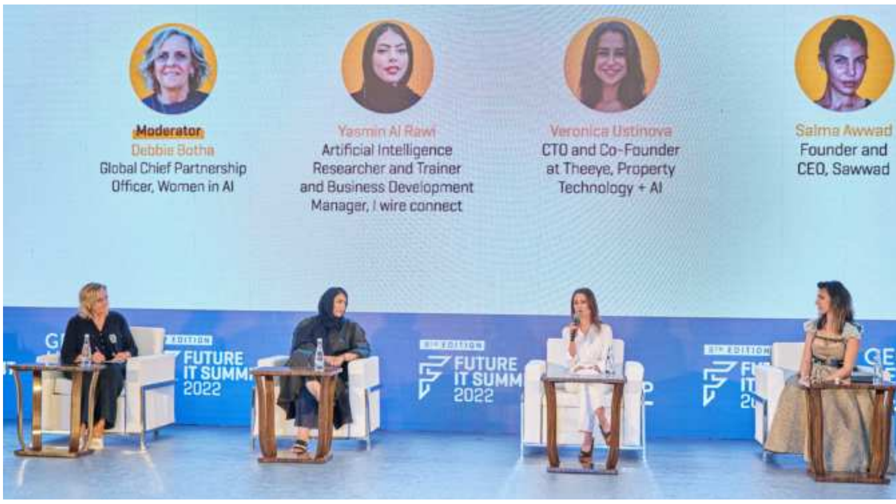
GLOBAL CIO
MANUFACTURI
FORUM
GCMF
FUTU
IT SU

FUTURE
IT SUMMIT
2022
GEC MEDIA GROUP


Moderator
ARUN SHANKAR
Senior Editor
GEC Media Group
Information Security
Officer, Noor Takaful
CIO Digital
transformation, KEO
International Consultants
FUTURE IT SUMMIT 2022
#evolvetechnology
GEC MEDIA GROUP


Moderator
Basil Ayass
Industry Veteran
Ehab Eid
Head of IT Operations and
Infrastructure, Emirates
Schools Establishment
Sheridan Moodley
Group CIO,
MASAFI
Mohammad Qattan
Cluster Director
Information Technology,
Fairmont The Palm
FUTURE IT SUMMIT 2022
#evolvetechnology
GEC MEDIA GROUP

Basil A
ndustry


Moderator
Debbie Botha
Global Chief Partnership
Officer, Women in AI
Yasmin Al Rawi
Artificial Intelligence
Researcher and Trainer
and Business Development
Manager, I wire connect
Veronica Ustinova
CTO and Co-Founder
at Theeye, Property
Technology + AI
Salma Awwad
Founder and
CEO, Sawwad
FUTURE IT SUMMIT 2022

8TH EDITION
FU
IT S
20
GEC MEDIA GROUP
FUTURE IT SUMMIT

BTX
2022
ROAD SHOW
AND TRANSFORMATION AWARDS
RIYADH
23rd MAY
SECURITY
NETWORKING
BUSINESS APPLICATIONS
IT & COMPUTING

CATALYSTS AWARDS 2022
Honoring the best
BEST IT COMPANIES TO WORK FOR 2022
TOP 10
HAPPY COMPANIES CREATE HAPPY EMPLOYEES
GEC MEDIA GROUP
COMMITTED. PASSIONATE. RESPONSIBLE
MIDDLE EAST | AFRICA | ASIA | USA
www.gecmediagroup.com

HE Abdullah Khalifa Obaid Al Marri opens Gisec 2022.

HE Abdullah Khalifa Obaid Al Marri opens Gisec 2022

HE Lieutenant General Abdullah Khalifa Obaid Al Marri, Commander-in-Chief of Dubai Police, opened Gisec 2022. His Excellency toured the three-day event accompanied by dignitaries including His Excellency Dr Mohamed Al-Kuwaiti, Head of Cyber Security, UAE Government and His Excellency Hamad Al Mansoori, Director General, Dubai Digital.

With more than 300 global cybersecurity brands showcasing technologies, Gisec is hosting leading international and regional innovators such as Huawei, Spire Solutions, Microsoft and Etisalat on how to tackle increasing threats resulting from a rise in remote working and rapidly accelerated digitalisation.

Gisec is organised in close partnership with UAE's influential cyber entities, including UAE Cyber Security Council, Dubai Electronic Security Centre, Dubai Police, Telecommunications and Digital Government Regulatory Authority, and will curate and prioritise the region's strategic cybersecurity agendas.

Gisec is organised in close partnership with UAE's influential cyber entities.

The UAE Cyber Security Council will host the Global Cyber security Congress and the first ever National Bug Bounty programme.

The UAE Cyber Security Council will host the Global Cyber security Congress and the first ever National Bug Bounty programme, hosting over 100 international ethical hackers, while dedicated conference tracks will probe the cybersecurity landscapes in Saudi Arabia and Africa.

HE Dr Mohamed Al Kuwaiti, Head of Cyber Security, United Arab Emirates Government.

Stephen Kavanagh, Executive Director of Police Services at Interpol.

MK Palmore, former Head of the FBI's San Francisco Cybersecurity Investigative Branch.

Awareness and collaboration are key to building culture of cybersecurity readiness

The 10th edition of Gisec opened at Dubai World Trade Centre as industry leaders unite to uncover the latest in global cybersecurity trends and discuss ever-increasing digital challenges.

Delivering the keynote speech on the first morning of the three-day show, HE Dr Mohamed Al Kuwaiti, Head of Cyber Security, United Arab Emirates Government, discussed the shared responsibility required to tackle the volatility of cyberspace and how collaboration is essential to successfully protecting against global cybercrime.

"If we look at the current landscape, awareness and collaboration are key to building a culture of cybersecurity readiness," said Al Kuwaiti. "We need to innovate and work towards building the next generation of cyber security professionals. The UAE Cybersecurity Council has a timeline, and the plan is to export the UAE's cybersecurity model across the region.

That collaboration can be epitomised by the UAE Cyber Security Council's National Bug Bounty Programme, where 100 ethical hackers will work in real-time at Gisec to hack, identify, and solve software flaws discovered across different scenarios and mainframes, including electric cars, mobile phones, and drones.

Among the speakers on opening day, Stephen Kavanagh, Executive Director of Police Services at Interpol, delivered his address to the industry discussing how the public and private sectors must play collaborative roles in the response to cybercrime.

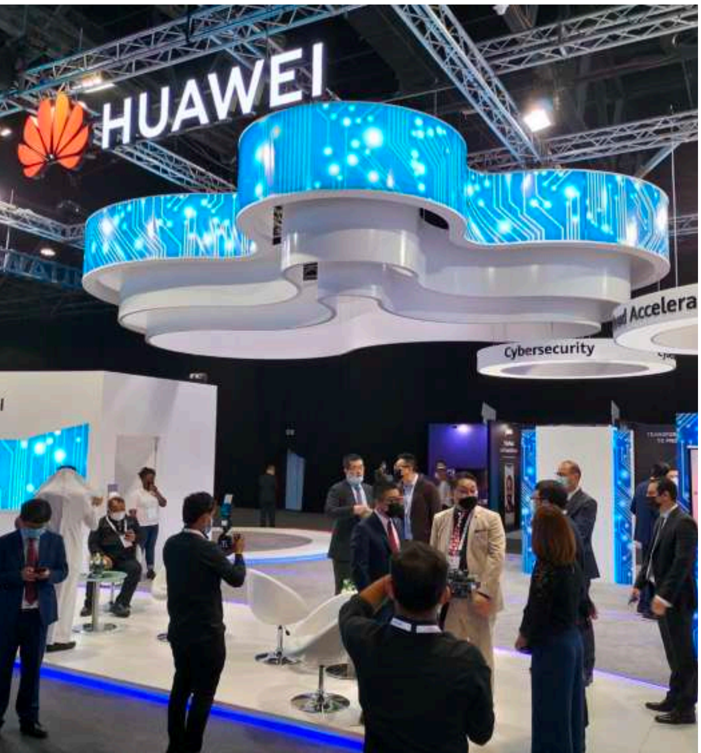
"Today, we find ourselves in a new world," said Kavanagh, the former Chief Constable of Essex Police in the United Kingdom. "We need a clear vision where all parties work together. Interpol is increasingly bringing data and expertise from the private sector to assist law enforcement. It is unrealistic to think law enforcement can recruit and retain the best brains, so that is where they turn to the private sector."

Also speaking on the main stage was MK Palmore, the former Head of the FBI's San Francisco Cybersecurity Investigative Branch. Palmore outlined how global development is forcing businesses to reassess their priorities to prevent large-scale cyber-attacks.

"By 2025, 42 billion devices will be connected to the internet," Palmore said. "This is a huge expanded digital surface area to protect, so offers huge opportunities for cyber criminals. It is no surprise then that, from an infrastructure and security standpoint, our reliance on digital services as we look to maintain society and business operations has become the No1 issue for organisations."

During the next two days, conference attendees will continue to hear from a host of prominent speakers, including renowned hacker Jayson E Street; Mesfer Almesfer, Chief Information Security Officer, NEOM; Professor Isa Ali Pantami, Federal Ministry of Communications and Digital Economy, Nigeria; and His Excellency Amir Hayek, Israeli Ambassador to the UAE and Ministry of Foreign Affairs, Israel, among others.

CYBERSECURITY VENDORS AT GISEC 2022



CISCO
SECURE
CISCO

ITB
IT Cyber Security
OT Cyber Security
DRAGOS
DRAGOS

Qualys
Continuous Security
Qualys
One Platform
Qualys
One Platform.
One Agent.
One View.
Now bringing the unified power of the Qualys Cloud Platform to EDR

tenable
tenable
tenable.sc
SEE EVERYTHING
PREDICT
tenable.ep

der in
OT & IoT Security and Visibility
nozominetworks.com
D32
The Leader in OT & IoT Security and Visibility
Leadership in Key Industries
The Leader in OT & IoT Security and Visibility

Microsoft
Microsoft
GESTURE

Healthcare top targeted sector throughout 2021 according to Cisco report

On the occasion of Gisec, Cisco released its predictions on emerging trends, based on research from the company's threat intelligence group Talos. The report details cybersecurity trends, highlighting the most common attacks, biggest targets and 2022 predictions.

Healthcare was the top targeted sector throughout the majority of 2021. The main reason adversaries are continuing to target this industry is due to healthcare providers' often underfunded cybersecurity budgets and extremely low downtime tolerance, the latter of which has been intensified by the pandemic.

Ransomware dominated the threat landscape in 2021. Cisco Talos researchers observed two trends emerging in ransomware engagements: a proliferation of adversaries, and an increased reliance on commercially available and open-source tools. Throughout 2020 and in the beginning of 2021, Ryuk was the primary ransomware family observed. As the year went on, it began to gradually disappear, similar to several other well-known ransomware types. What followed was a greater variety of actors culminating in the last quarter of the year.

Regarding attack vectors, Cisco Talos found that the adversaries most commonly exploited internet-facing applications and used phishing and business email compromise attacks to target end users.

For 2022, Cisco Talos is monitoring the situation around Log4J vulnerabilities, supply chain and third-party risks, the potential revival of Emotet, and the environment around ransomware.

Log4J vulnerabilities have caused widespread concern among customers and the security community at large, and we could easily see an increase in related incidents in 2022. As many researchers have pointed out, this incident has far-reaching implications based on Log4J's wide use within enterprises, and the difficulty some organisations might have in finding and patching everything that is vulnerable.

The past year was an indicator of things to come in terms of supply chain and third-party risk. When adversaries target a large Managed Service Provider MSP or open-source software incorporated into countless enterprise products, they greatly expand the potential pool of victims. It is expected that supply chain and third-party risk will continue to pose significant threat to enterprise security, as numerous actors such as ransomware groups leverage these attacks to pivot to high-value targets.

The company is demonstrating the inherent security strengths of Microsoft Cloud.

Microsoft generates $15B in security revenue in 2021, making it the biggest security company

Microsoft reiterated its commitment to securing the hybrid workplace of the future through its participation at Gisec. “Security has never been more critical for our customers given the evolving threat landscape and the move to hybrid work that so many companies are now forced to navigate,” said Sayed Hashish, General Manager, Microsoft UAE.

“At Microsoft, we have been hard at work to empower our customers to defend themselves against cyber threats, and we have earned their trust: we generated $15 billion in security revenue in 2021, up nearly 45% from the prior year. This makes Microsoft the biggest security company in terms of revenue and allows us to further strategically invest in our security offering: in 2020, we committed to invest $20 billion over five years, a four-fold increase from previous rates, to speed up its cyber security work.”

The company continues to safeguard the hybrid workplace by providing organisations of all sizes with a host of solutions, such as Microsoft’s Defender for Cloud, which is the only cloud provider with native multi-cloud protection for the industry’s top three platforms, and Microsoft Defender for Business, which helps companies with up to 300 employees defend against cybersecurity threats, including malware, phishing, and ransomware in environments with Windows, macOS, iOS, and Android devices.

The company is demonstrating the inherent security strengths of Microsoft Cloud, as well as how regional stakeholders can use Microsoft’s Zero Trust approach to create safer environments for themselves, their employees, and their customers.

Cryptomining attacks in UAE doubled in 2021 over 2020 finds Kaspersky

According to the Kaspersky Security Network findings released at Gisec 2022, cryptomining attacks in the UAE doubled in 2021 as compared to 2020. The country also witnessed an increase in financial malware attacks on Android by 42% in the same time period. The Middle East overall paints a similar picture, wherein cryptomining attacks increased by 7% and financial malware on Android increased by 6% in 2021 as compared to 2020.

On the bright side, all malware attacks in the country saw a decrease by 22%, and ransomware attacks too dropped by 25% in 2021 as compared to 2020. While the plummeting numbers are a promising sign, experts are noticing a change in tactics used by cybercriminals targeting the UAE. More complex and targeted cyberattacks are being devised and launched, suggesting that cybercriminals are focusing more on quality than quantity.

Cryptominers steal computing power by exploiting all applications, servers, and platforms that can support their mining operations. Such attacks result in organisations experiencing IT infrastructure performance lags and high electricity bills, which are less noticeable than the usual red flags in cybersecurity such as disruption of services, financial losses or file encryption due to a ransomware attack.

During the second half of 2021, Kaspersky reported that almost 40% of all ICS computers were attacked by malicious software at least once. Cyberattacks on these systems can impact production operations, result in financial losses and affect people’s lives. The goal of such attacks can be both cyber sabotage and cyber espionage.

Huawei highlighting secure digital transformation solutions and strategies for enterprises

At Gisec 2022, Huawei is demonstrating use cases and discussing best strategies to protect Middle Eastern enterprises in the current digital era. Huawei will demonstrate its resilient communications networks, scenarios and latest use cases in enabling industrial digitisation, intelligent cloud solutions, smart low-carbon datacentre, smart campus solutions, end-to-end cyber security assurance system, 5G security, cloud security, secure digital power solutions, and secure networks at the leading cybersecurity event. During the event, Huawei regional and global experts will participate in various panel discussions and deliver keynotes on trending security topics.

122% increase in malware in UAE according to Acronis

Acronis revealed that daily malware detections in UAE have been on the rise in the month of March, a worrying trend that exposes the critical need for cybersecurity in the region, especially for small business size companies.

Over the last two weeks we have seen a rapid increase in new cyber threats, which could be a concern. The latest data indicates malware detections alone have increased by 122%. This goes to show that cybercriminals are working overtime to develop tools and tricks that enable them to counter-fight the solutions being put in place.

During Q4 of 2021 over 12,640 ransomware attacks were successfully blocked on average per month by Acronis, a 0.2% jump from Q3 2021. In the same period, Acronis' cyber protection solutions also blocked 1,156,773 malware attacks on average per month representing a 74% jump from Q3. Acronis also successfully blocked over three million malicious URLs on average per month further demonstrating the effectiveness of strategic approach and technology.

CANDID WUEST
Acronis VP, Cyber Protection.

CYBER SENTINELS

PRESENTS

GCC SECURITY SYMPOSIUM AND CISO AWARDS 2022

SEC_RITY IS NOT COMPLETE WITHOUT U!

17 MAY 2022 | UNITED ARAB EMIRATES

REGISTER NOW

BROUGHT TO YOU BY

GEC MEDIA GROUP

OFFICIAL MEDIA PARTNERS

Enterprise CHANNELS MEA

BUSINESS TRANSFORMATION