معرض و مؤتمر الخليج العالمي لأمن المعلومات
GISEC GLOBAL

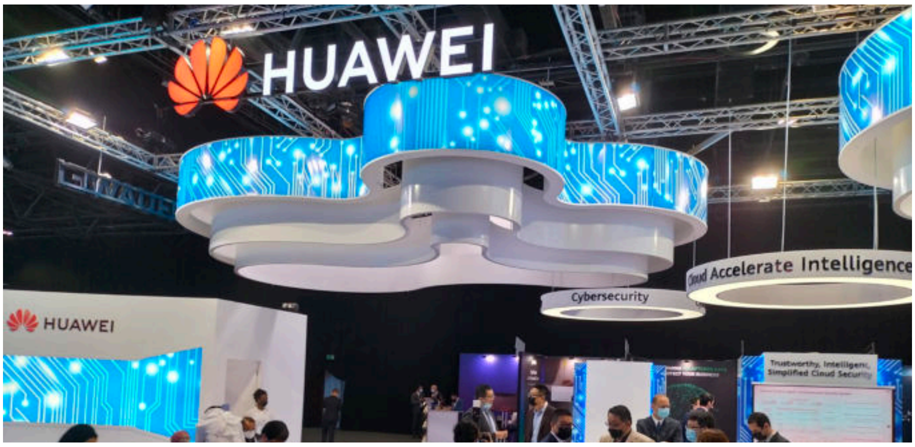
times

GISEC 2022 SPECIAL DAILY

BROUGHT BY
Enterprise CHANNELS MEA

21 MARCH – 23 MARCH 2022

Day Three


HUAWEI
Cloud Accelerate Intelligence
Cybersecurity
HUAWEI
Trustworthy, Intelligent, Simplified Cloud Security

UAE's Cybersecurity Council signs MoU with Huawei

The UAE's Cybersecurity Council signed a Memorandum of Understanding with Huawei to collaborate in the strengthening of local strategies and efforts related to cybersecurity. The agreement was signed at Gisec.

As per the memorandum, both parties will work towards strengthening strategic collaboration in cybersecurity based on the Public-Private-Partnership model. This will help promote cybersecurity innovation, drive development in cybersecurity capabilities, and nurture a strong cybersecurity ecosystem.

As part of the memorandum, both parties have agreed to work together in building visibility and promoting thought leadership in the area of cybersecurity, cooperating in the field of cybersecurity research and development through an independent think tank that both parties will establish, and jointly establishing a Cybersecurity Center of Excellence to deliver talent training that addresses the cybersecurity capacity-building needs for Emiratisation.

The partnership comes as spending on security including hardware, software, and services is also on the rise across the region, predicted to grow 7% to $3.76 billion in 2022 according to IDC.

In addition, the agreement aims to create an open, transparent, and trustworthy environment between the UAE Government, Huawei, and other technology vendors.

HE Dr Mohammad Hamad Al Kuwaiti, Head of Cybersecurity, UAE Government, said: "We are excited to be signing this agreement with Huawei in line with our mission of developing a comprehensive cybersecurity strategy and creating a safe and strong cyber infrastructure in the UAE. This step will also help drive our efforts to establish the UAE as a leading global hub for cybersecurity for the benefit of the nation."

During the opening day of Gisec 2022 (Pix by GEC Media).

"We are here to collaborate, partner with public and private sectors for different perspectives"

HE Dr Mohamed Al Kuwaiti, Head of Cyber Security, UAE Government.
The 10th edition of Gisec which opened on 21 March, hosted a second day defined by the signing of transformational partnerships and global cybersecurity experts sharing their unique expertise.
A number of high-level memorandum of understandings were signed on day two of Gisec Global, covering business-critical cybersecurity solutions and promises of enhanced collaboration.
The UAE Cybersecurity Council signed partnerships with Huawei, Amazon Web Services and advisory firm Deloitte to increase cloud adoption and knowledge sharing.

Huawei and CSC will work towards strengthening strategic collaboration in cybersecurity based on the Public-Private-Partnership model. This will help promote cybersecurity innovation, drive development in cybersecurity capabilities, and nurture a strong cybersecurity ecosystem. In addition, the agreement aims to create an open, transparent, and trustworthy environment between the UAE Government, Huawei, and other technology vendors.
AWS will work with the CSC to enable faster adoption of AWS cloud services by the UAE's public sector and regulated industries – including healthcare and financial – by leveraging AWS's global cloud infrastructure.

This opens opportunities for government entities and other strategic industries to accelerate innovation and digital transformation in line with the UAE's economic and national agendas.

Deloitte's MoU will enable the firm and the CSC to collaborate and leverage Deloitte's experience in the field of cybersecurity and expertise in the UAE, as well as drawing on and implementing internationally recognised good-industry practices as part of the UAE cybersecurity agenda.

HE DR MOHAMED AL KUWAITI
Head of Cyber Security, UAE Government discussed the importance of cyberspace on international peace and security.

MESFER ALMESFER
Chief Information Security Officer, NEOM.

Gisec also hosted the Global Cybersecurity Congress – an annual gathering aimed at unifying efforts on local, national and global cross-sector levels and organsied in collaboration with the UAE CSC. The congress intends to help shape national security and defence strategies to combat evolving threats.

Addressing topics such as Cloud Security and Compliance and Threat Intelligence and Cyber-Defence for Military and Law Enforcement, the congress was opened by HE Dr Mohamed Al Kuwaiti, Head of Cyber Security, UAE Government, who discussed the importance of cyberspace on international peace and security.

"We are not here to compete, but we are here to collaborate, build on these relationships and partner with the public and private sectors for different perspectives and to share knowledge, and we have seen this through the MoU's we have signed over the last two days with international entities," said Dr Al-Kuwaiti.

Running across the three-day event, Gisec Global is hosting a number of content sessions designed to spotlight best practice in cybersecurity across the region, with a specific focus on Africa, Israel, Qatar, and Saudi Arabia.

The event also featured discussions regarding how Saudi Arabia's new mega-project and smart city, NEOM, has approached and developed built-in cybersecurity programmes to repel cyberattacks

Mesfer Almesfer, Chief Information Security Officer at NEOM, said there exists no black and white approach to integrated cybersecurity platforms at the design stage of a project.

"If you are starting a new green environment, it is a very good opportunity for entities to build something from scratch with no legacy systems to try and manoeuvre around, which can cause issues," he said. "You should always keep cybersecurity as default from day one, work with your architects and planners to ensure enhanced resident experience is factored in from the outset."

Ibrahim Mohammed Alshamranie, Chief Cybersecurity and Privacy Officer, Saudi Arabia, Huawei, meanwhile looked at how artificial intelligence has the ability to profoundly change industry and organisations.

SUJOY BANERJEE
Associate Director, Sales and Business Development for UAE, ManageEngine.

ManageEngine finds demand for extended reality, hyper-automation, conversational AI

There has been a significant rise in demand for tools that help manage remote workforce and fight the many security risks involved in this new way of working. ManageEngine's discussions with visitors at the booth during Gisec 2022, indicate that this trend is likely to continue in the coming years as well. We expect to see a steady rise in adoption of technologies that help organisations effortlessly migrate to cloud-delivered and service-led products.

Most importantly, we believe organisations are more likely to develop a strong interest in adopting innovations like extended reality, hyper-automation, conversational AI and more that are emerging in the cybersecurity and cloud space.

ManageEngine's key focus this year at the event was the recently launched cloud access security broker component of ManageEngine's SIEM solution, Log360, and discuss how the rapid growth of cloud infrastructure services is driving increased interest in securing data, applications and workloads in cloud computing environments.

The vendor also spoke about the endpoint data loss prevention and anti-ransomware capabilities of ManageEngine's unified endpoint management solution, Desktop Central.

ManageEngine's discussions mainly involved combating the evolving cybersecurity threats in the region and how ManageEngine's suite of IT security products can help organisations in this aspect. In particular, the vendor discussed advanced ML-powered threat mitigation capabilities offered by ManageEngine's SIEM tool, Log360.

It offers both in-depth cloud security analytics as well as real-time active directory auditing. Customers came to know that the product is available both on-premise and on-cloud.

emt
TECHNOLOGY DISTRIBUTION
emt TECHNOLOGY DISTRIBUTION a rhipe company
SECURITY | CLOUD | ICT MANAGEMENT | IOT
WATCHER
eEngine

ARMIS
Our Portfolio
Data Security
netwrix
SECLORE
People Identity & Security
Attivo NETWORKS
ilantus
IMMERSIVELABS
Device Security
CROWDSTRIKE
Lookout
ARMIS.
Network Security
BLUECAT
IronNet
appgate
Workloads & Application Security
illumio
Checkmarx
Visibility & Analytics
REDSEAL
GROUP-IB
ARISTA
solarwinds
Automation & Orchestration
CYWARE
seceon
STRIKE READY

NATION STAGE
F23
F22
F20
F37
Ammune
API Security Solution
L7DEFENSE
ISRAEL CYBER ALLIANCE
Cyber Israel
Radiflow

CREDENCE SECURITY
D3 SECURITY
exterro
ENTRUST
Lookout
HumanFirewall
RISK MANAGEMENT/ COMPLIANCE
INCIDENT RESPONSE AUTOMATION FOR EVERYONE
Securing the Future of Data
EmailAuth
exterro
The Industry's Only Unified
Legal GRC Software Platform
E-Discovery Software
Privacy
ENTRUST

HAVELSAN
TURKISH CYBER SECURITY CLUSTER
HAVE
TR7
Logsign

ITB
IT BELT COMPANY
www.itb.com.sa
ITB

EXIT
EDGE
بدج
BEACON RED
بيكن رد

Shif
Delinea

CHANNEL PARTNERS AT GISEC 2022

SANS
The most trusted source for cybersecurity training, certifications, degrees and research
DFIR
cyberstart

"Preventing a breach can prove to be an extremely rigorous exercise leaving organisations' SOC teams overwhelmed with noisy security alerts and a high cost of threat intelligence. Most cybersecurity companies that claim predictive threat detection are not able to foresee an attack," said Wael Jaber, Vice President Technology and Services, CyberKnight.

"The predictions we make are over 97% accurate, and more importantly, they produce an extremely low rate of false positives, 0.01%. This means that organisations can trust our predictions enough to act and even automate enforcement," commented Abdullah Beshtawi, Regional Manager MEA, Seclytics.

Value distributor CyberKnight partners with Seclytics for SOC visibility solutions

As organisations continue to struggle with visibility into advanced cyberthreats, SOC teams are left overwhelmed with seemingly never-ending security alerts and false positives, leaving IT Security leaders doubtful of their attack readiness.

CyberKnight announced at Gisec that it has signed a distribution agreement with Seclytics, the pXDR platform that aligns and streamlines SOC workflow. Seclytics' Augur gives organisations exceptional visibility on threats providing smart automation and orchestration to help beat alert overload and take back control of a SOC.

The platform does not rely on blocklists, or malware signatures based on past attacks: Augur's predictive intelligence is proactive, seeking out and identifying threats long before attacks are launched.
Predictions are over 97% accurate, and more importantly, they produce an extremely low rate of false positives, 0.01%. This means that organisations can trust predictions enough to act and even automate enforcement.

Dragos to focus on improving OT security skills in UAE and Saudi Arabia

ROBERT M LEE
Chief Executive Officer and Co-Founder of Dragos.

Dragos, a global vendor in cybersecurity for industrial control systems and operational technology environments, announced the opening of its UAE office in Dubai during its debut appearance at Gisec.

The announcement closely follows Dragos's expansion in both the UAE and Saudi Arabia in November 2021 and sends a strong signal of the company's commitment to UAE. Dragos's focus on protecting the industrial sector in the region supports UAE initiatives such as Operation 300bn, which calls for the sector's GDP contribution to leap from $36 Billion to $82 Billion, or AED 300 Billion, by 2031.

Included in Dragos's new office, located in Dubai Internet City Innovation Hub, is space for the company's OT cybersecurity talent, including incident response, penetration, and threat intelligence professionals. Also included is a training centre to upskill talent for OT cybersecurity readiness.

The company has a team of OT risk analysts, threat researchers, and incident responders, and codifies their expertise into scalable technology that delivers the most effective protection against industrial threats

In parallel, the company has partnered with key government entities to provide training and threat intelligence and is in the midst of building an advanced, future-ready ecosystem with OEM manufacturers and channel resellers.

Dragos offerings include:

- Platform – combines ICS, OT network sensors, a scalable data architecture, and expert analysis modules for asset inventories, vulnerabilities, threats, and streamlined response.
- Intelligence – ICS, OT specific news, research, and analysis on industrial cyber threats, industry targeting, vulnerabilities, and actionable defence recommendations.
- Services – experienced professionals delivering OT security assessments, risk management, threat hunting, and incident response services.

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