More than 40,000 Cybersecurity Professionals Expected in Riyadh as Black Hat MEA 2024 Officially Opens

RIYADH, SAUDI ARABIA, November 27, 2024 /EINPresswire.com/ -- The highly anticipated Black Hat MEA officially opened its doors today in Saudi Arabia, marking a global record as the largest cybersecurity expo by space with an overall floor space of over 53,000 square meters.

Running from November 26-28 at the Riyadh Exhibition and Convention Centre in Malham, the three-day mega-event launched with an engaging Executive Summit addressing critical topics such as the transformative impact of AI on cybersecurity, the rapidly shifting cyber threat landscape, and the challenges of hacking in outer space.

The opening ceremony was officially inaugurated by His Excellency Eng. Faisal Al-Khamisi, the Chairman of the Saudi Federation for Cybersecurity, Programming & Drones. In his opening remarks, Al-Khamisi underscored the event's growth and importance.

“We take great pride in announcing that Black Hat MEA has officially become the world’s largest cybersecurity event by area, reflecting its remarkable growth and global stature,” he said. “Four years ago, we demonstrated the readiness of the Saudi market with the inaugural edition, and by Black Hat MEA 2023, it had grown to become the most-attended cybersecurity event globally. Over the next three days, attendees will experience a truly unique event featuring more than 350

speakers, 450 exhibiting companies, and participation in 10 diverse features."

Black Hat MEA 2024 promises to set a new benchmark for innovation, collaboration, and knowledge-sharing within the global cybersecurity community.

Exploring Cutting-Edge Cybersecurity Trends and Innovations

Opening the Executive Summit was Kirsten Davies, Founder and CEO of Institute for Cyber Civics, who conducted a session called 'Guarding the Ballot'. Davies said that while there were enormous measures for securing the votes in the ballots, there were still quite a few cybersecurity headlines.

"We had issues in software systems with duplication ballots, where the registrations hadn't been cleaned up before election day, meaning there were people voting who shouldn't have been eligible to," she said. "In some states, there were even cases where thousands of votes had no signatures or ID attached to them.

"As an industry, we are charged with protecting the most sensitive and critical data, and even in the most sacred parts of our governments and election processes, we need to be unafraid to look where the gaps are, where we should be doing risk analysis. With the adoption of artificial intelligence in its many forms, we could see the use of blockchain when it comes to voting, whether we want to transition to a fully digital platform or use mobile phone face scans to verify the ID of said voter."

Key Discussions: AI, Cyber Threats and Digital Resilience

Discussing the complexities of cybersecurity and its multifaceted domain involving systems, people, and processes, Gary Hayslip, CISO at Softbank Advisors, highlighted the importance of

understanding a company's purpose, data usage, and stakeholder relationships to build resilient security programs. Hayslip shared his experiences from various roles, including the US Navy, the City of San Diego, Webroot, and Softbank Investment Advisors, detailing how he adapted different frameworks to fit each organization's culture and needs.

“When I left the federal government and joined the city of San Diego as their first CISO, what was unique in this environment was the sheer scale of smart city projects and networks sprawling across the city, supplying services to over four million citizens,” Hayslip said. “When I first started, no one had any idea what a framework or system was, but they just knew they needed someone to manage everything.

“Even though we were handling things such as credit card transactions, what I learned pretty quickly was that it was all about relationships. Many of the stakeholders had known each other for years, so it was extremely important for me to take – what I call – the ‘fish taco’ approach, which is to invite them for lunch and get an understanding of their needs. I faced a lot of pushback, but occasionally, I would find someone who would be willing to take my help and do a project together, finding my champions. Once you do a few assessments around baseline risk and results start to show, that’s when things start to happen, and the net gets cast wider.”

Expert Insights on Data Security and Global Cyber Challenges

In an insightful and slightly terrifying session surrounding deepfakes and the impact of such malicious AI attacks, Bilal Baig, Technical Director, Mediterranean, Middle East, and Africa, for Trend Micro, pondered how it is possible to keep up with what is happening with so much data, AI systems, and models being created and circulated.

“The current threat landscape can be divided into three factors: Ransomware, data theft, and phishing. We have platforms such as YouTube, which are the perfect places for bad actors to use AI programs to scan the faces of a CEO or Chief Legal Officer [CLO] in videos, which are then used as tools to gain valuable company information,” said Baig.

“We have seen instances where a targeted email is sent to an employee requesting a Zoom call with the CEO and CLO, and the deepfake video is played during the call requesting the employee to upload sensitive financial company information ahead of a last-minute and important meeting with a client or government partner. To the untrained eye, it is hard to tell the difference, and these types of attacks work all the time.”

Secure-By-Design: Ensuring Cyber Safety in Space Exploration

Day One of Black Hat MEA also heard from cybersecurity expert Umar Khan, who shed light on hacking satellites, rockets, and more at the Executive Summit. Khan, who is Chief Information Officer and Senior Vice President at Relativity Space, has worked with industry giants such as SpaceX and MaxLinear and highlighted the different components of satellites and rockets,

explaining how they function and communicate. Highlighting the increasing accessibility of information due to the use of commercially available parts and open-source software, Khan argued how this public access has fed into new attack vectors for malicious actors.

"Satellites are no longer these mysterious black boxes," Khan said. "Many are built with components we already know, such as smartphone processors and Linux operating systems. This makes it easier than ever for attackers to exploit weaknesses in the software and hardware. The rise of low-cost ground station technology means anyone with a US$35 software-defined radio and an internet connection can potentially eavesdrop on satellite communications or even take control of a spacecraft."

Khan concluded his session with a call to action for the cybersecurity community, emphasising the urgent need for secure-by-design principles in space systems, regular vulnerability scanning, and robust incident response plans.

“The resounding success of the first day of Black Hat MEA has surpassed all expectations. The energy, innovation, and collaboration on display have set a powerful tone for the days ahead,” said Annabelle Mander, Senior Vice President of Tahaluf. “It’s enlightening to see industry leaders, experts, and enthusiasts come together to address today’s most pressing cybersecurity challenges while shaping the future of digital resilience. This is more than an event – it’s a movement towards a safer, more connected world."

Nour Ibrahim
MCS Action FZ LLC
+971 544250187
email us here