Black Hat MEA Highlights Importance of Cross-Industry Collaboration and Spotlights Next Gen Cybersecurity Talent

RIYADH, RIYADH, KINGDOM OF SAUDI ARABIA, November 15, 2023 /EINPresswire.com/ -- Black Hat MEA 2023 is not only shining a light on Saudi Arabia's burgeoning cyber industry, it is also showcasing how international security leaders are working closer than ever to tackle data breaches and the collaborative steps are necessary to ensure organisations are as prepared as possible in the event of an attack.

The three-day event, which is organised by Tahaluf, the Informa LLC joint venture with SAFCSP, and taking place at Riyadh Front Exhibition and Convention Centre until November 16, is also providing a platform for the next generation of cyber professionals, with 13-year-old Marco Liberale, the event's youngest-ever speaker, taking centre stage with a session on ransomware.

Liberale, who developed an interest in malware and ransomware at a young age but is now seeking to make a difference as an ethical hacker, told delegates how his interest for "picking locks" aged three or four evolved into the creation of his first piece of malware "around the age of five."

During a live demo, he showed how a ransomware attack works and how to prevent it, highlighting the need for companies to "regularly update operating systems, back up data, and use reliable cybersecurity software."

Elsewhere, with demands ramping up on cyber professionals to protect their organisations from increasing threats, Sam Curry, a career cybersecurity leader and current Chief Information Security Officer (CISO) at US-based cloud security company Zscaler, shared his insights into what makes a successful CISO.

In his keynote How Not to Lose Your Job in 13 Months – a reference to the average global tenure of a CISO – Curry said the role should not be to try to prove you are the "smartest cyber person in the room". In contrast, he said, the role is one of logistics and social skills – to identify the person on the board who can be the smartest cyber person in the room.

"Have your metrics, have your objectives, but find the person who can be that alpha and talk them through the metrics, so they become the most knowledgeable person," Curry said. "When the time comes, and questions are asked, you are nodding and not giving the answers."

He also offered sage advice to CISOs and those striving to one day hold the role in case they should find themselves in an elevator with their CEO. "Try not to use the word 'risk' because that is what they will expect you to say," he said. "It can't be something technical. Instead, mention how you [as a CISO] affect revenue, margins and costs, customer satisfaction, employee efficiency, strategy... Try limiting yourself to those. It means you have to pay attention in meetings and understand your impact on those things. You have to evolve as CISOs. You're no longer the smartest cyber person in the world, you are grooming the next generation to take over."

Speaking on day two of the event, which has attracted more than 60,000 registrations, Dr Pascal Andrei, Chief Security Officer at Airbus, stressed the fundamental need to ensure aircraft electronic systems are fully protected against unauthorised access at all times.

"When we are talking about security, you, as cyber security experts, need to understand the full spectrum from physical security, crisis management, and business continuity planning, because

when you want to save yourself from cyberattacks, it is imperative to understand the overall picture of the company because you are all a part of the same fight," said Andrei.

"Protecting aircraft systems involves mapping and assessing the worldwide and industry relationships in place across the cyber ecosystem, identifying risks, and assessing these risks as part of a holistic plan to process information in a safe and secure manner. It also involves entering into productive relationships with external parties and government agencies to leverage collective intellectual capacity, skills, and knowledge."

In an eye-opening session on the Deep Dive Stage, John Staniforth, CISO of the UK's Royal Mail Group, took delegates through the lessons he and his organisation learned following a ransomware attack earlier this year. Staniforth explained how Royal Mail was hit by the cybercriminal group LockBit, who penetrated the firm's cybersecurity and accessed hundreds of zipped data files, which equated to more than one million individual files when unzipped.

Staniforth described it as "knowing your house has been burgled because it's a mess, but trying to understand how they got in." He added: "We had to piece together whether they had smashed a window to get in, had someone dropped the key on the way out, or had they just picked the lock?"

He described the challenges of dealing with multiple stakeholders, from the CEO, who wants to know when it will be over and at what cost, to staff, media, and national crime organisations. Staniforth outlined the importance of engaging with the threat actors, and fully comprehending the risks of paying or not paying the ransom, which in this case was US$80 million, including being on the wrong side of terror financing regulations because you are "dealing with criminals."

He talked about how some companies might agree on a deal with their attackers, such as paying the ransom in exchange for not being targeted for a set period of time. In this case, after a month-long negotiation with the threat actor, Staniforth revealed the group did not pay the ransom, and the upset hackers published some of the data and transcripts of their negotiations. He concluded that "time, balance, and patience" are key to dealing with a cyberattack.

Elsewhere, an inspiring panel discussion at the Executive Summit focused on women in cybersecurity, titled 'Driving Bigger Impact', featuring a high-calibre quartet of female cyber experts, looked at what must be done to get more women into the industry to meet the growing demand for talent and the steps being taken by Saudi Arabia to move the needle.

Aseel Al Fehaid, a data protection and privacy director, outlined how 40,000 men and women in the Kingdom have been "trained in digital skills, including cyber," leading to the creation of 20,000 jobs. She added the more women who get involved, the more will be inspired to enter the sector, insisting the increasing number of females in the industry in Saudi Arabia is "a reflection of the commitment to inclusivity and the valuable contribution women bring to the industry".

Rasha Abu AlSaud, Chief Technology Officer at Saudi National Bank, pointed to the various national efforts to improve cybersecurity across all levels. She added the Government had established a strong ecosystem in the Kingdom and made skillsets available, not just for the academic sector, but across all sectors. She predicted the country will soon see a “50-50” split of men and women working and studying in the Saudi Arabian cyber industry, which will “empower more and more women into this very important domain”.

Black Hat MEA 2023 is running from November 14-16 in Riyadh. For registration and further information, please visit www.blackhatmea.com.

Pragati Malik
MCS Action FZ LLC
email us here
Visit us on social media:
Other
