CYBER1: Growing need for cyber security in the Middle East, with market estimated to double in the coming years

Digitisation in the Middle East has progressed, but this development also means increased risk exposure. The region has experienced a huge increase of cyber-attacks in recent years. The threat also rises as Europe shifts from Russia, as a supplier of oil and natural gas, to other nations. The heightened security threat means growth opportunities for CYBER1, to provide cyber resilience solutions.

The nations in the Middle East region all strive for an environment that is digitally secure. But efforts both from companies and from the government are reactive and fragmental in nature, even though it has been increased in the last years. The response therefore often has a hard time catching up with the ever evolving and changing threat from cybercrimes.

The increase of digitalization increases the exposure to cyber threats

One of the Middle East's largest economies, the United Arab Emirates, witnessed a 250 % increase in cyberattacks and cybercrimes during the COVID-19 pandemic. Another example is Saudi Arabia, which stopped more than seven million cyberattacks in the first three months of 2021. The number of these attacks has risen by 104% over the past year. There are cyber-attacks from both other nation-states and criminal organizations seated around the world.

The increase in threats is also reflected in the projection for the cybersecurity market in the Middle East. The size of the market today is estimated to be USD 20.3 billion and is projected to grow to USD 44.7 by 2027. The need for operational security is steadily increasing to safeguard the supply of oil and gas to different countries around the world.

Increased need for applied cyber security solutions

Credence Security, which is the dominant distribution arm of CYBER1, headquartered in Dubai and offers solutions to both public and private sector across India and the Middle East.

"We can see an increased awareness of digital threats and risks in the Middle East. We also notice the growing demand for not only responding to threats but increasing preparedness for breaches in cyber security. This is also reflected in the market projection for 2027", says Garreth Scott, Managing Director of Credence Security.

The company operates from six pillars of business.
· **Digital Forensics & Incident Response:** Focuses on the identification, investigation, and remediation of cyberattacks. Some of the leading vendors in this field include Exterro, Oxygen Forensics, Teel Technologies, and Sumuri.
· **Privacy, Security & Data Governance:** Providing solutions both at the end-user level and in corporate networks, servers, databases, and the cloud to protect business-critical data with automated security solutions that help you stay ahead of today's ever-changing threats. Some leading vendors in this pillar are HelpSystems, Digital Guardian, Lookout
· **Continuous Adaptive Risk & Trust Assessment:** CARTA similarly to Zero Trust is a strategic

approach to IT security that favors continuous cybersecurity assessments and contextual decision-making based on adaptive evaluations of risk and trust. Some key solutions in this pillar are SOAR from D3 Security, Digital Risk Protection from ZeroFox and Breach & Attack Simulation from Picus Security

· **Anti-Phishing & Security Awareness:** Security measures that individuals and organizations can take to prevent a phishing attack or to mitigate the impact of a successful attack. Vendors in this pillar include EmailAuth and HumanFirewall

· **Identity, Payments & Data Security:** Enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. The leading vendors in this pillar are Entrust, Forentix and Randtronics, NetIQ and Futurex

· **DevSecOps:** Automates the integration of security at every phase of the software development lifecycle. Leading vendors in this pillar include CheckMarx.

The above collobrations with leading industry vendors, demonstrates that CYBER1 is well placed to cater for the current and projected growth of cyber security provisions required in the region.

For further information, please contact:

Public Relations Contact:
Christer Lundin : E-mail: christer@cyber1.com

Mangold Fondkommission AB is the Company's Certified Adviser.
Phone: +46 (0)8 503 015 50 E-mail: ca@mangold.se

About CYBER1

CYBER1 is engaged in providing cyber resilience solutions and conducts its operations through presences in Sweden, South Africa, United Arab Emirates, Kenya and the UK. Listed on Nasdaq First North Growth Market (Nasdaq: CYB1.ST), the Group delivers services and technology licenses to enhance clients' protections against unwanted intrusions, to provide and enhance cyber resilience and to prevent various forms of information theft. CYBER1 had revenues of €37.22m in 2021.

For further information, please visit www.cyber1.com/investors.

For all company filings and reports, please visit: https://cyber1.com/cyber1-investor-information/

Attachments

CYBER1: Growing need for cyber security in the Middle East, with market estimated to double in the coming years