

CALL TO ACTION ABU DHABI 2023

REGIONAL CYBERSECURITY WEEK

9 - 12 OCTOBER 2023

Participants of the Regional Cybersecurity Week, organized by the Arab Regional Cybersecurity Centre in Sultanate of Oman (ARCC) and hosted by the UAE Cyber Security Council.

RECOGNIZING THAT: the Regional Cybersecurity Week 2023 provided an exceptional platform for 70+ countries, various international organizations, and industry leaders to collectively address pressing cybersecurity concerns, foster open dialogue, develop tailored solutions, and collaborate on regional cybersecurity challenges.

Acknowledging the following key considerations:

1600⁺
DELEGATES

70⁺
COUNTRIES

50⁺
SPEAKERS

07
DRILLS

05
GUINNESS
WORLD RECORDS

11
INTERNATIONAL
ORGANIZATIONS



Regional Cybersecurity Week
الأسبوع الإقليمي للأمن السيبراني
ABU DHABI 2023



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



OIC-CERT
Computer Emergency Response Team

FIRST
Middle East Security Center



The escalating global cyber-attacks that threatens the smooth functioning of socio-economic operations and national environments.



The pivotal role of Computer Incident Response Teams (CIRTs) in identifying, defending against, responding to, and managing cyber threats, thereby enhancing the security of cyberspace within sovereign nations.



The necessity of strengthening relations between member states within the regions to facilitate enhanced cybersecurity cooperation, collaboration cybersecurity, ensuring societal continuity during crises, and safeguarding the provision of essential services and resiliency of the critical national infrastructure.



The need for increased investment to effectively secure cyberspace. This includes promoting CIRT-to-CIRT collaboration, developing human capacity, sharing information and knowledge, and fostering teamwork to fully harness the benefits of Information and Communication Technologies.



The imperative to cultivate a culture of cybersecurity for the future This begins with integrating cybersecurity-related curricula at all levels of the national education system, from primary schools to higher education, fostering a generation of digital citizens.



The substantial advantages derived from cooperation among stakeholders.



The need to promote cyber security innovation and industry development to further strength countries readiness in cyber security.



Emerging Technologies security Guidelines: Recognizing the impact of emerging Technologies in the Cybersecurity, we advocate to address the importance of the Security Guidelines and best practices. These Guidelines should encompass the responsible add secure development, deployment and management of emerging technologies to safeguard against cyber threats and vulnerability.



Enhance Critical Infrastructure Cyber Protection: Implementing specialized measures which enhance the protection of critical infrastructures. It includes isolation from compromised networks, redundancy and advanced monitoring to safeguard against large scale cyber threats.



In light of these critical considerations, we must now take decisive action to address the pressing challenges we face. We hereby propose the following cybersecurity call to action.



COMMITMENT

We pledge our dedication to fostering confidence and security in the use of Information and Communication Technologies (ICTs).



EMBRACE CYBER RESILIENCE

We strongly urge industries to adopt frameworks that not only repel threats but also ensure uninterrupted operations even during cyberattacks.



SHARING

We will actively share our experiences and best practices concerning cyber threats and cybersecurity.



HARMONIZATION

We will actively pursue harmonization and integration, as necessary, with other relevant organizations, benefiting from their experiences and preventing duplication of efforts.



RESEARCH & DEVELOPMENT

We encourage governments, academia, and the private sector to increase their investment in cybersecurity Research & Development (R&D).



STRENGTHEN CYBER STRATEGIES

We will collaborate with all relevant stakeholders to establish and update cyber strategies that strategically approach cybersecurity development, implementing policies to enhance preparedness and resilience.



CYBER INCLUSION

We advocate for the introduction of cybersecurity education at foundational levels and its continuation through higher education and ongoing professional development.



ETHICAL AI ADOPTION

We will promote ethical AI adoption by encouraging businesses and organizations to prioritize ethical considerations in AI development and deployment, fostering a culture of responsible AI use to ensure its benefits for all of humanity.

In adopting this cybersecurity call to action, we aim to fortify our collective efforts in securing our digital future, fostering collaboration, and enhancing our resilience against cyber threats. Together, we can build a safer and more secure cyberspace for all.

THE LARGEST CYBER SECURITY EVENT IN THE REGION IN NUMBERS

70+ Countries



3 Board Meetings

CSC Board meeting which addressed concerns and discussed future collaborations



the Board of Directors of the Organization of Islamic Cooperation delved into shared priorities and initiatives.

The 11th Arab Cybersecurity Cooperation Team (ACCT) meeting, in the esteemed presence of the Chairs, Heads, and CEOs of National Cybersecurity Centers across Arab Nations.



5 GUINNESS WORLD RECORDS

★★★★★

- 01 MOST NATIONALITIES IN A CYBERSECURITY AWARENESS LESSON
- 02 MOST NATIONALITIES IN A CYBER DRILL COMPETITION
- 03 LARGEST CYBER DRILL COMPETITION
- 04 LARGEST CYBER-CITY THREAT SIMULATION MODEL
- 05 LARGEST CYBER-CITY THREAT SIMULATION MODEL (DEVICES)



7 Cyber Drill Scenarios

1 A HOLISTIC CYBER DEFENSE TACTICS



3 CAPTURE THE FLAG (CTF)



2 LOG ANALYSIS WEB APPS HACKED AND CRYPTO MINING



4 LOG ANALYSIS WEB APPS HACKED AND CRYPTO MINING



5 A HOLISTIC CYBER DEFENSE TACTICS



6 LOG ANALYSIS WEB APPS HACKED AND CRYPTO MINING



7 A HOLISTIC CYBER DEFENSE TACTICS



Regional Cybersecurity Week
الأسبوع الإلكتروني للأمن السيبراني
ABU DHABI 2023



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



OIC-CERT
Computer Emergency Response Team



Cyber Security Call to Action Report in



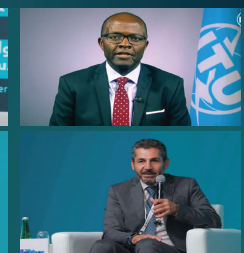
7+ Languages Endorsed by the ITU



1600+ Delegates



50+ Speakers, 6 Panel Discussions



THE PULSE:

For the first time ever experiencing how a city is secured from cyber attacks, how the power of data and real-time simulation is leveraged to build insight-driven decisions



5 MoUs



3 OIC-CERT Global Cyber Security Awards



11 International Organisations:
UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCT)

