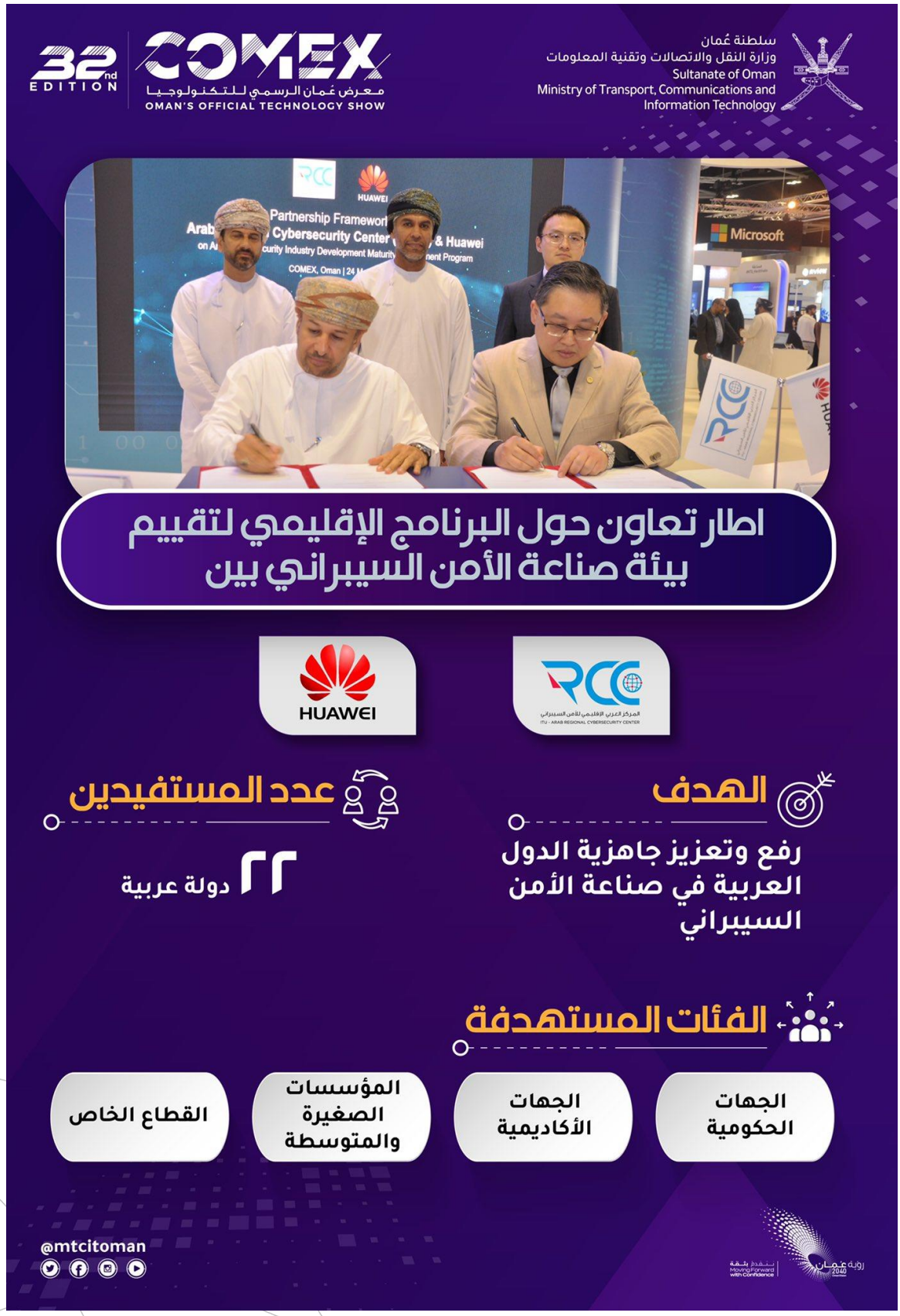
البرنامج الإقليمي لتقييم بيئة صناعة الأمن السيبراني

بالتعاون مع شركة هواوي



البرنامج يهدف إلى رفع وتعزيز جاهزية الدول العربية والاسلامية في صناعة الأمن السيبراني، ويستهدف البرنامج الجهات الحكومية والأكاديمية، كما تشمل القطاع الخاص والمؤسسات الصغيرة والمتوسطة.

نبذة عن البرنامج

أطلق المركز العربي الإقليمي للأمن السيبراني التابع للاتحاد الدولي للاتصالات(ITU-ARCC) ، بالتعاون مع شركة "هواوي"، برنامجاً جديداً بعنوان "نموذج نضج استراتيجيات تطوير قطاع الأمن السيبراني". ويهدف البرنامج إلى رفع وتعزيز جاهزية الدول العربية و الاسلامية في صناعة الأمن السيبراني، ويوفر دليلاً شاملاً لمساعدة الجهات الحكومية والجهات الأكاديمية والمؤسسات الصغيرة والمتوسطة والقطاع الخاص في الدول العربية والاسلامية على تقييم وتعزيز قدراتهم في مجال الأمن السيبراني .

يعدّ هذا البرنامج الأوّل من نوعه في المنطقة والعالم، وتم تصميمه خصيصاً لمواكبة متطلبات الأمن السيبراني في المنطقة العربية. وهو أحد ثمار الشراكة التي وقعها المركز العربي الإقليمي للأمن السيبراني مع شركة"هواوي" في مايو ٢٠٢٢ بهدف تعزيز تبادل المعارف وبناء القدرات والتعاون في قطاع الأمن السيبراني في العالم العربي.

يحرص المركز على تبادل الخبرات مع شركائه ضمن منظومة الأمن السيبراني بهدف خلق فرص جديدة لهم، والمساهمة في بناء منظومة سيبرانية داعمة للجميع. كما يؤمن بأن الأمن السيبراني هو مسؤولية مشتركة تتطلب تعاون جميع أصحاب المصلحة. وتعدّ الشراكة بين القطاعين العام والخاص ضرورة أساسية لتحديد المخاطر ومنع الهجمات الإلكترونية وحماية البيانات والأصول؛ إذ تتيح مثل هذه الشراكات المجال لتبادل المعلومات، والتطوير المشترك لحلول الأمن السيبراني، واعتماد أفضل الممارسات. وبالاستفادة من مكامن القوة لكلا القطاعين، يمكن للحكومات والشركات تعزيز قدراتها الدفاعية، والكشف الاستباقي عن التهديدات والاستجابة لها، وضمان حماية البُنى التحتية الحيوية.

أهداف البرنامج

ويهدف "البرنامج الاقليمي لتقييم بيئة صناعة الأمن السيبراني" إلى توفير:

١ .دليل إرشادي لقياس وتعزيز نضج بيئة صناعة الأمن السيبراني لمختلف المؤسسات المنضوية ضمن المنظومة الرقمية؛ ويشمل ذلك مثل حماية البنية التحتية الرقمية، وأمن البيانات، وأمن الحوسبة السحابية، والتكنولوجيا الناشئة، وأمن الاتصالات، وما إلى ذلك .

٢ .معلومات دقيقة وفعالة للمساعدة في تطوير استراتيجية طويلة المدى لصناعة الأمن السيبراني

٣ .تحديد أفضل الممارسات من البلدان الأخرى لاستخلاص الدروس والاستفادة منها في التحسين الذات.

٤ .خارطة طريق وطنية لبناء قدرات الأمن السيبراني.

٥ .تحفيز الطلب على الخدمات والمنتجات المتعلقة بالأمن السيبراني مما يسهم في زيادة نمو القطاع.

Foundational Characteristics Shaping the Comprehensive Program

We summarized and generalized the good practices of each from existing cybersecurity assessment models, and synthesized the objectives of this project to arrive at the following:

Structure	Coverage	Questionnaire Granularity Design	Assessment Method	Result Presentation
Category-Element-Aspect-Indicator-Checklist	**Generic and Scenario-based Assessment**	**Binary Answer with Evidence Collection**	**Self-assessment and Cooperation**	**Maturity Level, Heatmap and Radar Chart**
The **five-layer** structure is the basis for the development of this Program, and the division and disassembly of each layer makes the Program more **specific** and **comprehensive**.	Both **generic and scenario-specific** elements are used as part of the Program, aiming to address the customization for the increasingly changing cybersecurity environment	**Binary** responses are used to determine if the indicator requirements are satisfied in the checklist. And checklists are with **samples of materials** that can be provided as **supporting documentation** for the indicators.	**Flexible** assessment methods incorporating **self-assessment** and **cooperation**, combined with easy-to-understand checklists, increase the **flexibility** of Program assessments.	The Program provides a more **intuitive representation** of maturity level results through the three charts mentioned above, which **assist in making decisions**, which is a rare representation of existing models in the market.

Introduction to Category - Summary

The categories CIDSMM include all assessment content of these 5 industry-renowned models

CIDSMM Categories
Category 1. Policy and Strategy
Definition: This category explores the national capacity to develop and deliver cybersecurity strategy and enhance its cybersecurity resilience while maintaining the benefits of cyberspace vital for government, international business, and society.
Category 2. Legal and Regulatory
Definition: This category refers to the capacity of the government to develop and enact national legislation directly or indirectly related to cybersecurity, including primarily the capacity of law enforcement, prosecution, regulatory agencies, and courts.
Category 3. Standard, Organization and Technology
Definition: This category examines the development and implementation of cybersecurity standards and best practices, the establishment of cybersecurity agencies and mechanisms, as well as the implementation of processes and technical controls in order to reduce cybersecurity risks.
Category 4. Culture and Knowledge
Definition: This category explores the creation of a strong culture of cybersecurity for the population, the public and private sectors, which will lead to increased awareness of cybersecurity, the development of professionals, and the accumulation of research outcomes in the field of cybersecurity.
Category 5. Commercial Gain and Cooperation
Definition: This category examines the growth and development of the cybersecurity industry, as well as the multi-dimensional cooperation approach of government organizations, public welfare institutions, and enterprises.