مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

< التهديدات السيبرانية في عصر الرقمنة والذكاء الاصطناعي\>

بناء القدرات في مجال الذكاء الاصطناعي،
يجسد روح الريادة التي تتميز بها دولة الإمارات

صاحب السّمو
الشيخ محمد بن زايد آل نهيان
رئيس دولة الإمارات العربية المتحدة

لم تكن التحديات سوى عتباتٍ
تجاوزناها في مسيرة تحقيق طموحاتنا،
ولن توقفنا عن مواصلة السير

صاحب السّمو
الشيخ محمد بن راشد آل مكتوم
نائب رئيس الدولة رئيس مجلس الوزراء - حاكم دبي

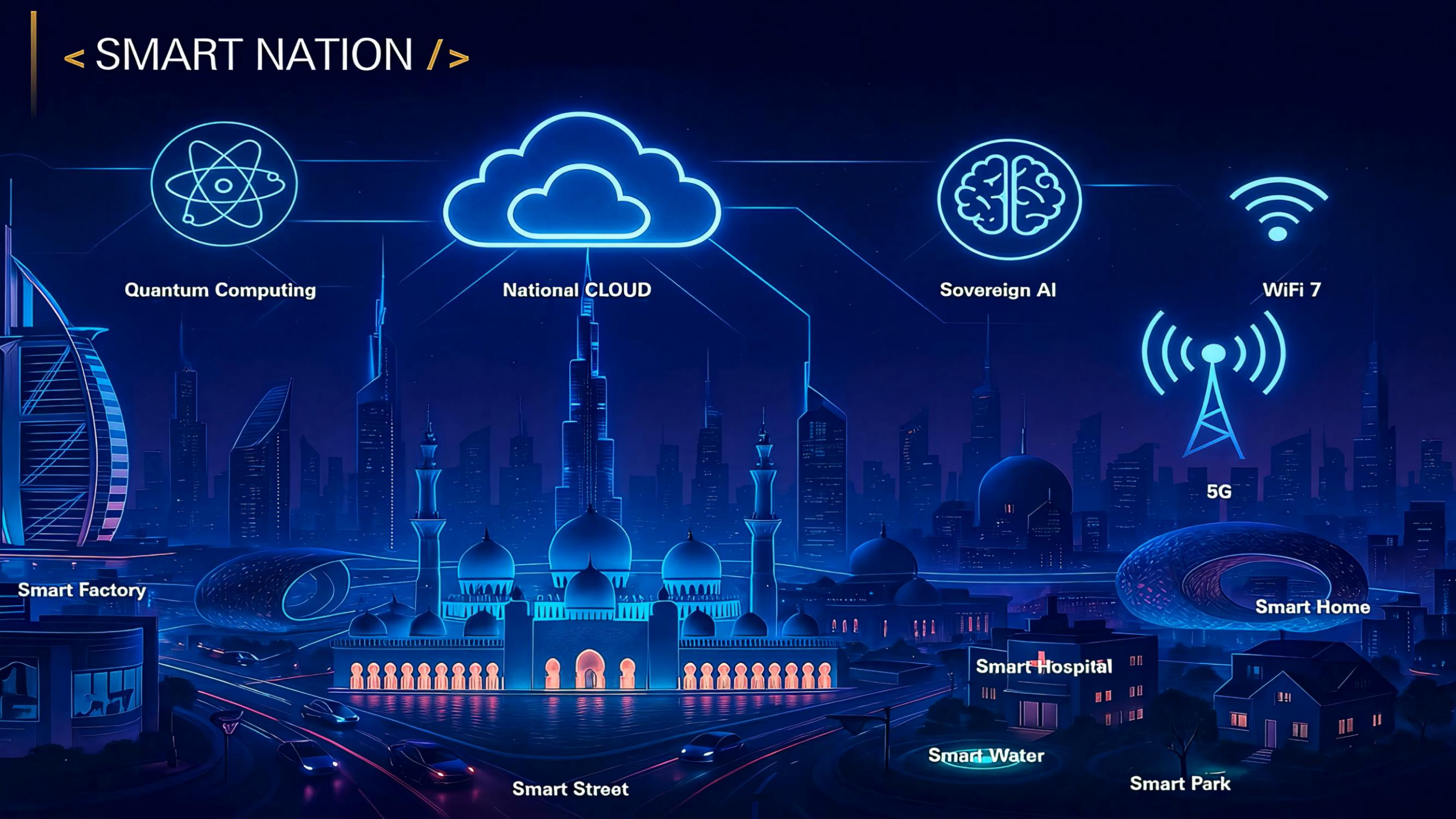
< الإمارات الأولى عالميا في مؤشر الأمن السيبراني \>

Global Cybersecurity Index

يقيس التقرير البنية التحتية في الأمن السيبراني بناء على خمسة محاور هي:

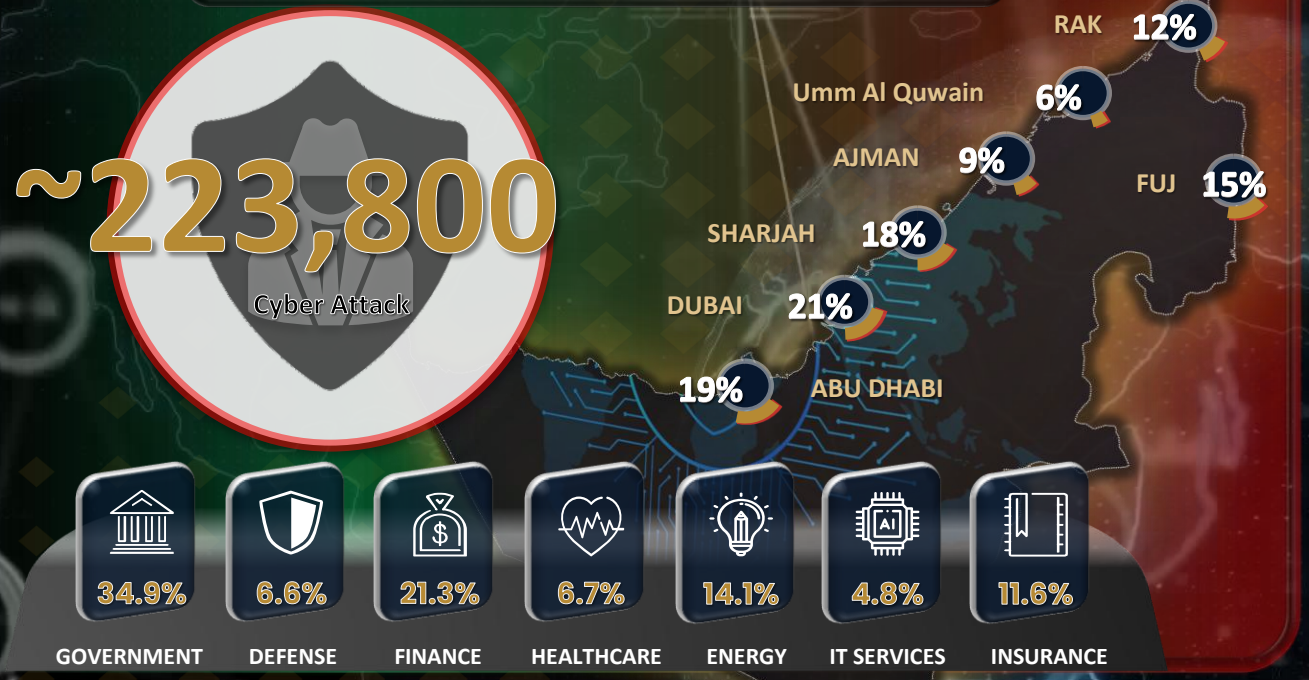
- إجراءات تطوير القدرات
- الإجراءات الفنية/التقنية
- الإجراءات التنظيمية
- الإجراءات القانونية
- إجراءات التعاون

< SMART NATION />



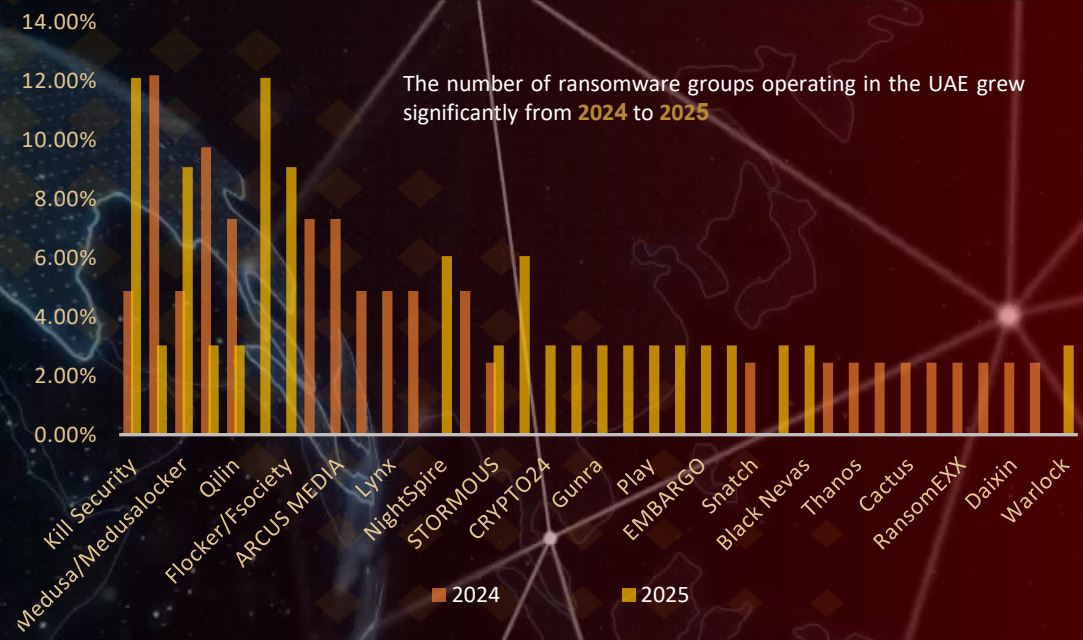
<UAE Cyber Threats Statistics (2024 – 2025) - Key Insights and Statistics />

UAE ATTACK SURFACE EXPOSURE



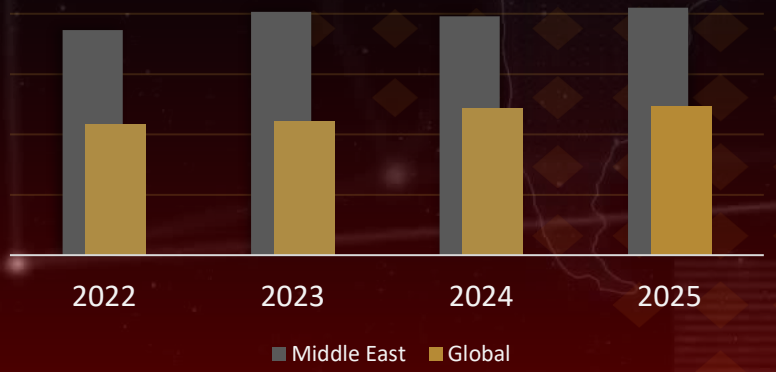
ACTIVE RANSOMWARE GROUPS IN THE UAE IN 2024 - 2025

The number of ransomware groups operating in the UAE grew significantly from **2024** to **2025**



Data Breach Cost By Region (USD)

The average cost of a data breach reached **US$4.94** million globally, driven by factors such as lost business, customer response costs, and data visibility gaps.



Distributed Denial of Service (DDoS) Attacks

	Max Bandwidth (Peal Volume)	Avg. Attack Duration	Top Targeted Industries	Total DDoS Attack
UAE	85.92 Gbps	18.53 Min.	Wired Tele. Carriers	2,301
Globally	960.397 Gbps	60 Min.	Wired Tele. Carriers	7.96 M

Incident Breakdown By Type – Threat Hunt Data

- 61% E-Mail Fraud/Phishing /Spoofing
- 8% Scans/Probes/ Attempted Access
- 24% Improper Usage & Unlawful Activity
- 4% Vulnerabilities /Web Application Attacks
- 1% Compromised Information
- 1% Malicious Code

< أبرز التهديدات السيبرانية \>

الحروب السيبرانية

الإرهاب السيبراني

الجرائم السيبرانية

الجهات التي تقف وراء الهجمات

مجموعات الجريمة الإلكترونية

قراصنة النشطاء (Hacktivists)

الجهات المدعومة من الدول

التهديدات الداخلية

< الجريمة السيبرانية: المشهد الجديد للتهديدات – التهديدات والتحديات \>

التحول الإجرامي: انتقال الجريمة المنظمة إلى الفضاء السيبراني (Cybercrime-as-a-Service)كنموذج عمل متكامل

استهداف البنى الحيوية: التركيز المتزايد للمجرمين على تعطيل خدمات البنية التحتية الحيوية (المواصلات، الخدمات الأمنية)

إخفاء الهوية الرقمية: التحديات المتصاعدة في تتبع المعاملات غير المركزية (كالعملات المشفرة والبلوكتشين) في سياق مكافحة الجريمة وغسيل الأموال.

التحديات القضائية العابرة للحدود: صعوبة تتبع وملاحقة مرتكبي الجرائم السيبرانية وتحديد الولاية القضائية في بيئة رقمية تتجاوز الحدود الدولية

<الذباب الإلكتروني (الحسابات الوهمية)/>

شبكات من الحسابات المزيفة او التي يتم التحكم بها بشكل آلي ممنهج على منصات التواصل الاجتماعي وتستخدم لنشر آراء وأفكار معينة بشكل مكثف للتأثير على الرأي العام وتنفيذ أجندات مظللة

التأثير السياسي

التأثير الإقتصادي

توجيه الرأي العام

الدعايات والإشاعات

المؤشرات التي تدل على الحسابات الوهمية

1. نشاط مكثف غير طبيعي
2. المحتوى المتكرر
3. قلة التفاعل الحقيقي
4. **النتيجة:** قلة الوعي عند بعض مستخدمي منصات وسائل التواصل الاجتماعي تجعله ضحية تنطلي عليه هذه الإشاعات

< آليات التمكين الإجرامي: التشفير المتقدم والتمويل اللامركزي \>

تكنولوجيا التشفير

استخدام تطبيقات التشفير من طرف إلى طرف لحماية الاتصالات بين البائع والمشتري من الرصد

العملات المشفرة والمعاملات

الاعتماد على العملات المشفرة كعمليات دفع لضمان إخفاء الهوية وتجنب التتبع المالي التقليدي

الترويج بالذكاء الاصطناعي

استخدام أدوات الذكاء الاصطناعي لإنشاء محتوى ترويجي جاذب أو مضلل، واستهداف دقيق للمتابعين

اتصالات خفية

تحويل الاتصالات إلى قنوات مغلقة (محادثات خاصة، مجموعات مشفّرة) بعد جذب الضحية

< قيادة التحقيق الجنائي: تمكين الذكاء الاصطناعي في الاستباقية والتحليل \>

01

التنبؤ الاستباقي
للتهديدات

02

تسريع التحقيقات
الجنائية الرقمية

03

مواجهة التزييف
العميق والمحافظة
على نزاهة الأدلة

04

حوكمة
الاستخدام وبناء
الثقة العامة

< الأركان الاستراتيجية لتعزيز القدرات الوطنية لمكافحة الترويج الرقمي للمخدرات

رصد استباقي للمحتوى

عبر أنظمة ذكاء اصطناعي متقدمة لتحليل الأنماط وتتبع الرسائل المشفّرة والمؤشرات الرقمية عالية الخطورة

التعاون مع مزودي الخدمات

لتوفير حلول لمواجهة التحديات المرتبطة بالترويج الرقمي للمخدرات

توظيف أدوات الذكاء الاصطناعي

داخل منصات التواصل لرصد الحسابات المشبوهة، تحليل الأنماط غير الطبيعية، واكتشاف المحتوى المرتبط بالترويج الرقمي للمخدرات بشكل استباقي

رفع مستوى الوعي المجتمعي

عبر برامج موجهة للأسر والشباب حول طرق اكتشاف الحسابات المضلّلة وأساليب الحماية الرقمية

ثورة التكنولوجيا القادمة... فرص جديدة وتحديات غير مسبوقة

الحوسبة السحابية
Cloud & Fog Computing

الأنظمة فائقة الترابط

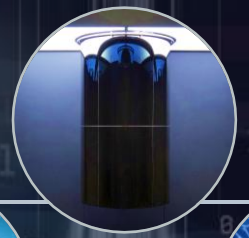
الواقع الافتراضي والمعزز
(الميتافيرس)

Web 3.0

الهندسة الحيوية المتقدمة

البنى التحتية الذكية

الحوسبة الكمية



التوائم الرقمية

الحروب السيبرانية

الذكاء الاصطناعي العام
Artificial General Intelligence

الفضاء والعوالم الجديدة

< نموذج دولة الإمارات السيبراني />

الاستراتيجية الوطنية للأمن السيبراني 2025 - 2031

الشراكة

الحوكمة

الحماية

الابتكار

البناء

< البناء \>

التقنيات

مركز عمليات الأمن السيبراني الوطني (NSOC)

القدرات والكوادر البشرية

القناص السيبراني

GLOBAL CYBERDRILL

الحوكمة

السياسات الوطنية

مجلس الوزراء برئاسة محمد بن راشد يعتمد حزمة سياسات وبرامج وطنية للأمن السيبراني في الدولة

تمثل السياسات أطرًا أمنية لحماية المعلومات وتعزيز الثقة في الأنظمة الرقمية

اعتماد 5 سياسات وطنية

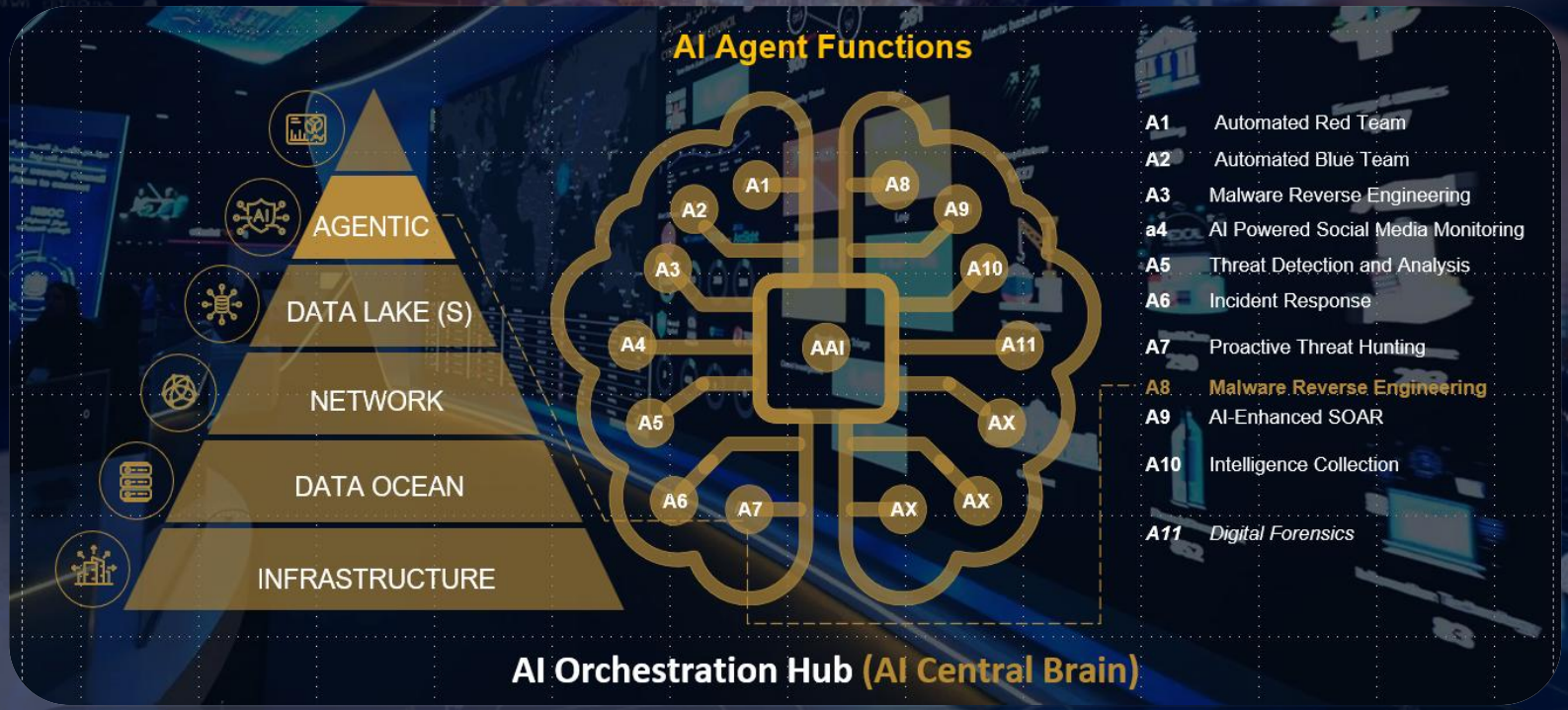
1. السياسة الوطنية لأمن الذكاء الاصطناعي.
2. السياسة الوطنية للتشفير.
3. السياسة الوطنية لأمن تبادل البيانات.
4. السياسة الوطنية للعمل الآمن عن بُعد.
5. السياسة الوطنية للكشف عن الثغرات الأمنية السيبرانية.

تحديث 8 سياسات وطنية

- السياسة الوطنية لأمن إنترنت الأشياء.
- إطار تبادل المعلومات في الأمن السيبراني.
- السياسة الوطنية للأمن السحابي.
- القدرات الأساسية لمركز العمليات الأمنية.
- الإطار الوطني لحوكمة الأمن السيبراني.
- سياسة حماية البنية التحتية للمعلومات الحيوية.
- البرامج الوطني لاعتمادات الأمن السيبراني.
- إطار الاستجابة للحوادث السيبرانية.

THREATS

CYBERE71



الحماية

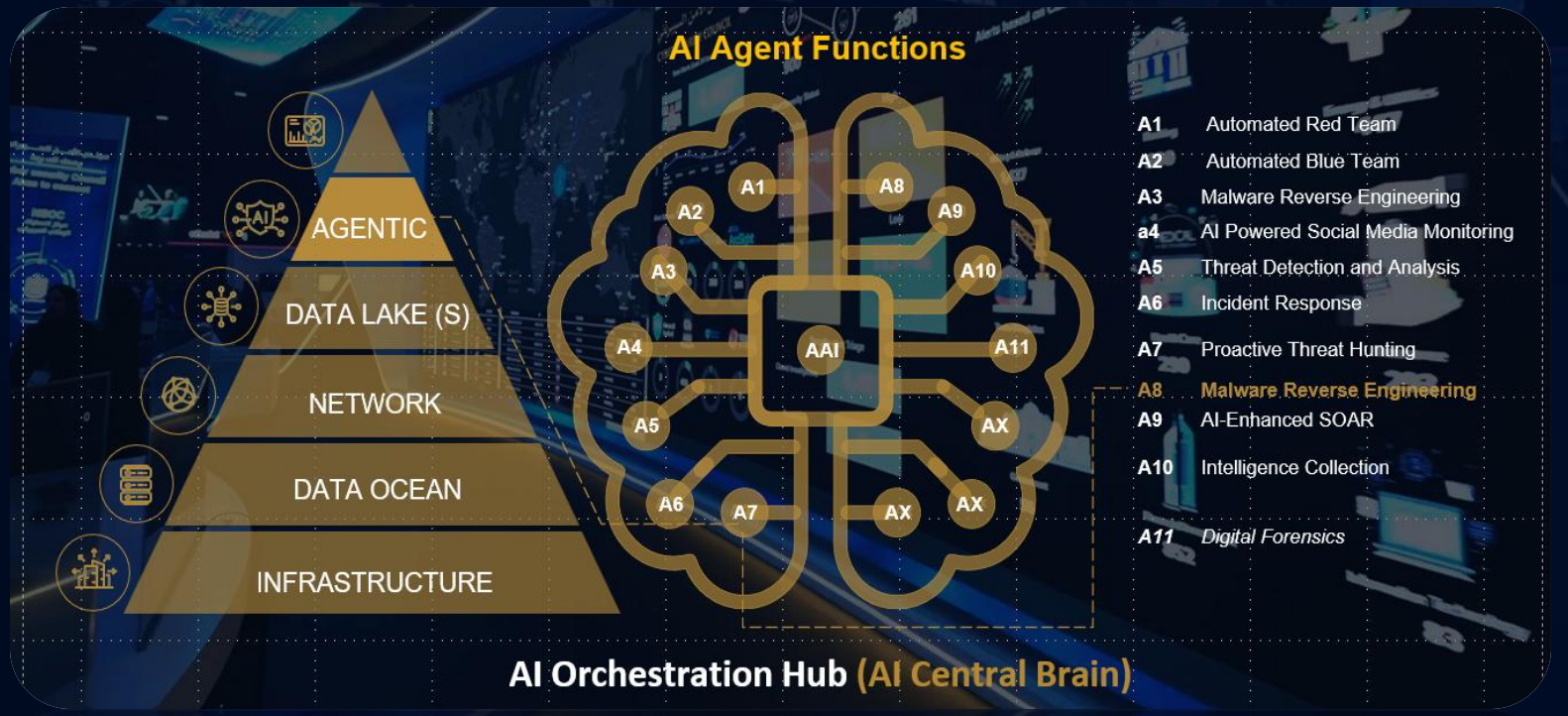
حلول ردع هجمات الحرمان من الخدمة الموزعة (DDOS Mitigation Solution)

المراقبة الذكية

حماية متعددة الطبقات

مركز عمليات الأمن السيبراني الوطني (NSOC)

E -THREATS



الحوكمة

1

- برنامج الاعتماد الخاص بالأمن السيبراني
- القدرات الأساسية لمركز العمليات الأمنية السيبراني
- إطار عمل مشاركة المعلومات
- الخطة الوطنية للاستجابة للحوادث
- سياسة أمن إنترنت الأشياء
- سياسة أمن السحابة
- سياسة حماية البنية التحتية للمعلومات الحيوية
- إطار حوكمة الأمن السيبراني الوطني

2

- سياسة الأمن السيبراني المتعلقة بالأطراف الخارجية
- سياسة أمن الذكاء الاصطناعي
- سياسة أمن البلوك تشين
- سياسة أمن تبادل البيانات
- سياسة التشفير
- سياسة العمل عن بعد

3

- Cyber Threat Exposure Management
- Zero Trust
- Cyber Materiality
- Virtual Reality Device Security
- Software Pipeline Security
- Digital Identity
- Cyber Extortion
- Cyber Crisis Management
- Quantum Computing Cyber Security

< الشراكة \>

لدينا شركاء/داعمون

4P : Public, Private, People, Partnership

الشراكات بين القطاع العام، والقطاع الخاص، والمجتمع

القطاع العام (Public): تعاون الجهات والحكومات لدفع عجلة التحول الرقمي الآمن

القطاع الخاص (Private): شركاء يُمكِّنون الابتكار والوصول إلى تقنيات وحلول حديثة

المجتمعات (Public): تمكين الأفراد والمبدعين والخبراء في الدولة في منظومة الأمن السيبراني

الشراكات (Partnership): جهة موحدة للأمن السيبراني المستدام

GITEX GLOBAL

GLOBAL CYBERDRILL

THE WHITE HOUSE WASHINGTON

CRI INTERNATIONAL COUNTER RANSOMWARE INITIATIVE

CSCGOVAE

www.csc.gov.ae