التطوير المحلي
لمنتجات الأمن السيبراني
في المملكة العربية السعودية

SAMI ADVANCED ELECTRONICS
شركة الإلكترونيات المتقدمة

المحتويات

موجز تنفيذي

يكشف البحث الذي أجراه مركز التنافسية العالمي التابع للمعهد الدولي للتنمية الإدارية عن احتلال المملكة العربية السعودية للمرتبة السابعة في مؤشر الفضاء السيبراني العالمي، وهو إنجاز جدير بالثناء لقطاع الأمن في البلاد. أظهرت حكومة المملكة العربية السعودية مسؤولية كبيرة في تعزيز الجاهزية السيبرانية للمملكة. كان إدخال الاستراتيجية الوطنية لأمن المعلومات في 2011 والهيئة الوطنية للأمن السيبراني في 2013 وبرنامج التحول الوطني في 2016 بمثابة خطوات بارزة لتحسين الوضع الأمني في المملكة. وقد أدى ارتفاع معدل انتهاكات البيانات إلى تطوير هذه السلطات الوطنية التي تبذل جهودًا مكثفة لتعزيز الجاهزية السيبرانية للمملكة.

ويقع قطاع الأمن السيبراني في المملكة العربية السعودية في نطاق خطط التوطين، حيث تتطلع البلاد إلى تطوير منتجات الأمن السيبراني المحلية. وقد برز صمام البيانات باعتباره أكثر التقنيات منفعة في ضمان أمن الاتصالات داخل الفضاء السيبراني. ترتبط شبكات التحكم وشبكات المؤسسات في الفضاء الرقمي ببعضها البعض من خلال تدفق البيانات والمعلومات في اتجاهين. وهو ما يعرض البنية التحتية الحرجة وأنظمة التحكم لعدد من التهديدات السيبرانية. وفي هذا السيناريو، فإن صمام البيانات الذي يمكنه فرض بروتوكول صارم للاتصال أحادي الاتجاه بين الشبكات أمرًا ضروريًا [15]. يمكن تسريع وتيرة التطوير المحلي لصمام البيانات من خلال دمج هذه العملية مع برنامج أرامكو السعودية لتعزيز القيمة المضافة الإجمالية في المملكة (اكتفاء). يركز البرنامج بشكل مثالي على إبراز تطوير المحتوى المحلي في المملكة، وبرزت أرامكو السعودية (إدارة هندسة تقنية المعلومات) وشركة الإلكترونيات المتقدمة كمصنعين محليين رئيسيين في برنامج اكتفاء.

الأمن السيبراني:
شرط أساسي للتحولات الرقمية

تقع رؤية المملكة العربية السعودية 2030 وبرنامج التحول الوطني على رأس التحولات الرقمية داخل المملكة. [1]

إن اختراق الأجهزة وإنترنت الأشياء والتقنيات السحابية وتحولات تقنية المعلومات والاتصالات تتجه بالمملكة نحو النضج الرقمي. [2] في هذا السيناريو من النمو الرقمي السريع، ازدادت الحاجة إلى الجاهزية السيبرانية والأمن السيبراني.

إن نمو تقنية المعلومات والاتصالات نتيجة مباشرة للتحولات الرقمية في جميع أنحاء المملكة العربية السعودية. حققت المملكة نموًا بنسبة 46 % في المؤشر الوطني لتقنية المعلومات والاتصالات سنة 2017. [2] تستدعي تعقيدات تقنية المعلومات والاتصالات الحاجة إلى إطار موازٍ للمرونة السيبرانية وحماية البنية التحتية الرقمية.

الانتهاكات المتعلقة بالبيانات: مأزق للملكة العربية السعودية والشرق الأوسط

الهجمات السيبرانية في المملكة العربية السعودية أعلى بكثير من المتوسط العالمي

التكلفة التنظيمية للانتهاكات المتعلقة ببيانات نشر خسائر الأعمال في المملكة العربية السعودية والإمارات العربية المتحدة:

2.18 مليون دولار [7]

احتمالية انتهاك البيانات في الإمارات العربية المتحدة والمملكة العربية السعودية:

6.23 % [7]

الإنفاق على الاستجابة للانتهاكات المتعلقة ببيانات النشر في الإمارات العربية المتحدة والمملكة العربية السعودية:

1.47 مليونًا [7]

بلغت تكلفة الانتهاكات المتعلقة البيانات في المملكة العربية السعودية والإمارات العربية المتحدة في 2018 نحو

$5.31
ملايين دولارًا أمريكيًا

7.1%
بزيادة بلغت
في تكلفة الانتهاكات المتعلقة البيانات في المملكة العربية السعودية والإمارات العربية المتحدة منذ 2017 [6]

أسباب الانتهاكات المتعلقة بالبيانات

المملكة العربية السعودية والإمارات العربية المتحدة [7]

الخطأ البشري 18%
خلل في النظام 21%
الهجمات الخبيثة أو الإجرامية 61%

على الصعيد العالمي [7]

الخطأ البشري 27%
خلل في النظام 25%
الهجمات الخبيثة أو الإجرامية 48%

صمام البيانات:
دورة حياة النظام البيئي للأمن السيبراني في المملكة العربية السعودية

متوسط عدد السجلات المنتهكة في الإمارات العربية المتحدة والمملكة العربية السعودية (2018):

36,451 [7]

متوسط تكلفة انتهاك البيانات لكل فرد في الإمارات العربية المتحدة والمملكة العربية السعودية:

163 دولار [7]

تكاليف الاكتشاف والتصعيد في الإمارات العربية المتحدة والمملكة العربية السعودية:

1.36 مليون دولار [7]

يُطلب من الشركات والمؤسسات تقسيم شبكاتها من أجل مواجهة الهجمات السيبرانية. أهم نقطتين في تجزئة الشبكة هما جدران الحماية وصمام البيانات. [25] وسائل الوقاية هي أجهزة اتصال ثنائية الاتجاه تظل معرضة للهجمات حتى إذا هُيئت للاتصال أحادي الاتجاه. [13] ومنذ ذلك الحين، ظهر صمام البيانات بالإضافة إلى بروتوكول نقل البيانات أحادي الاتجاه، كمحور للنمو والتطوير في مجال الأمن السيبراني في جميع أنحاء المملكة العربية السعودية.

أهمية صمام البيانات في الأعمال والقطاع العام [14]

تحسين الامتثال: تركز مناطق الشرق الأوسط على فصل شبكات تقنية التشغيل وتقنية المعلومات لتحسين الامتثال.

مراقبة شبكة الحماية: بزيادة استخدام أنظمة المراقبة المادية مثل كاميرات المراقبة في جميع المنظمات السعودية، فثمة حاجة ماسة إلى الفصل بين نقاط جمع البيانات ووحدات المراقبة المركزية.

استمرارية الأعمال: يتطلب الاقتصاد السعودي سريع التحول استمرارية الأعمال في قطاعات متعددة. ومن ثم، فإن صمام البيانات ضروري لمنع الهجمات السيبرانية التي تؤثر على عمليات وسلامة وأداء المنظمات.

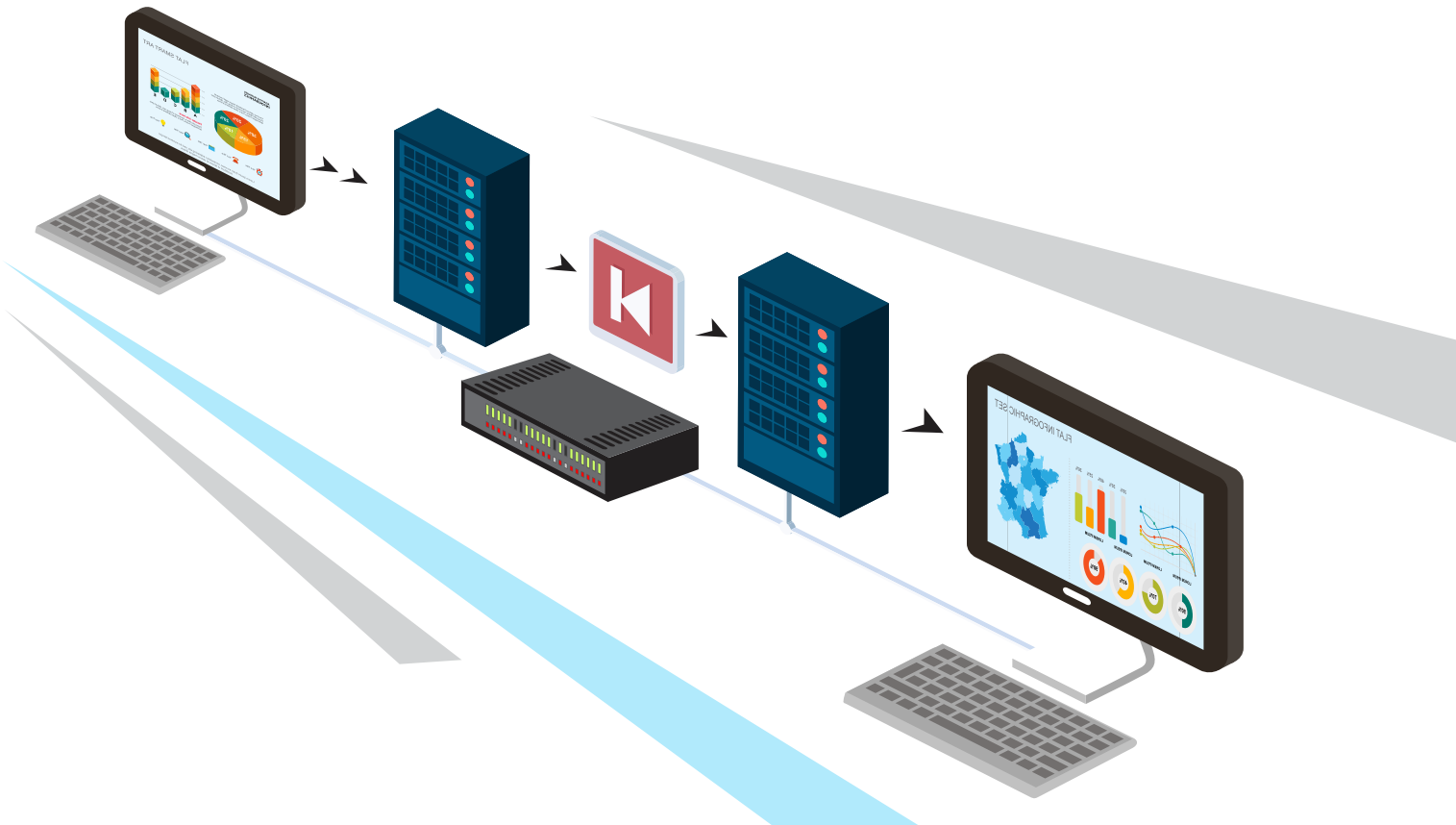
طور صمام بيانات الجيل التالي بشكل مشترك من قبل أرامكو السعودية وشركة الإلكترونيات المتقدمة

الوظيفة: ضمان النقل أحادي الاتجاه للبيانات لتوفير أمان كبير للشبكات التنظيمية.

التطفل والهجمات السيبرانية: في بيئة العمل المعاصرة، أصبحت المنصات الرقمية عرضة للهجمات السيبرانية واقتحام الشبكات المعادية وتدمير البيانات من خلال اختراق الشبكة.

كيف يُساعد صمام البيانات؟ يقوم صمام البيانات بإنشاء بروتوكول نقل بيانات أحادي الاتجاه لجميع الشبكات من خلال الفصل المادي والكهربائي للمضيف والمقصد. وهو ما يمنع البرامج الضارة المعادية من التأثير على شبكاتك أو الوصول إلى أنظمتك أو إجراء تغييرات ضارة.

ما هو المبدأ الأساسي لتقنية صمام البيانات؟ غالبًا ما يُطلب من الشركات والحكومات والمنظمات إرسال معلومات حساسة إلى مصادر خارج شبكتها. وهو ما يجعل الشبكة المضيفة معرضة للهجمات السيبرانية والتهديدات الخبيثة من المصدر الخارجي. ولتفادي ذلك، ينشئ صمام البيانات قناة أحادية الاتجاه يمكنها إرسال البيانات إلى المقصد بدون مسار لتلقي أي شكل من أشكال المعلومات.



مميزات صمام بيانات شركة الإلكترونيات المتقدمة

01

بسرعة 1 جيجا بايت

02

يدعم بروتوكولات متعددة - بروتوكول Sysolg وبروتوكول SFTP وبروتوكول FTP وبروتوكول SCP

03

يدعم الواجهة متعددة الوسائط عالية الوضوح (HDMI) ويو إس بي والإيثرنت

04

يُرسل / يعالج بيانات الوقت الحقيقي

05

يدير الأنظمة المالية

06

يحمي المعلومات القيمة من السرقة أو العبث أو التلف

07

يقلل الخطأ البشري

08

يدعن صيغ متعددة - أنظمة سكادا - بي إل سي وأجهزة الاستشعار

الجهات الفاعلة في سوق صمام البيانات في المملكة العربية السعودية

أول - الولايات المتحدة الأمريكية | فوكس آي تي - هولندا
بي أي إي سيستمز - المملكة المتحدة | تريسي - الولايات المتحدة الأمريكية
ديب سورس - المملكة المتحدة

إجمالي حجم السوق (تقريبًا) :

500 مليون ريال سعودي

(يجب التحقق منه)

الحاجة إلى تطوير شبكات أحادية الاتجاه في الفضاء السيبراني

حدود جدران الحماية

تهدف جدران الحماية إلى بناء حواجز بين الشبكة الداخلية وأي مصدر خارجي غير موثوق به. وعلى الرغم من ذلك، يمكن أن تؤدي أخطاء التهيئة في جدران الحماية إلى الوصول غير الآمن إلى الشبكات الداخلية. من الممكن أن يستخدم المهاجمون اتصالات مشفرة لتجاوز جدران الحماية التي قد تضر بدورها سلامة بيانات المصدر. [15] من الناحية الأخرى، يمنع صمام البيانات جميع أشكال التهيئة الضارة والهجمات القائمة على الشبكة الموجهة إلى الشبكة المضيفة.

الحفاظ على سلامة البنية التحتية

لا يمكن إعادة تهيئة صمام البيانات للوصول غير الآمن، وهو ما يقضي على إمكانية الهجمات عبر الإنترنت أو العبث أو تعطل البرامج أو الأخطاء البشرية. [19]

الحاجة إلى نقل موثوق للبيانات

يستخدم صمام البيانات تقنيات النقل المعبأة برؤوس متسلسلة لضمان وسلامة البيانات المطلقة القريبة. [12]

التوطين من خلال البرامج الوطنية

(الاستراتيجية الوطنية لأمن المعلومات والهيئة الوطنية للأمن السيبراني وبرنامج التحول الوطني)

يمكن تحقيق الأهداف التالية من خلال الجمع بين التآزر المشترك بين الاستراتيجية الوطنية لأمن المعلومات والهيئة الوطنية للأمن السيبراني والبرنامج الوطني للتحول [22]:

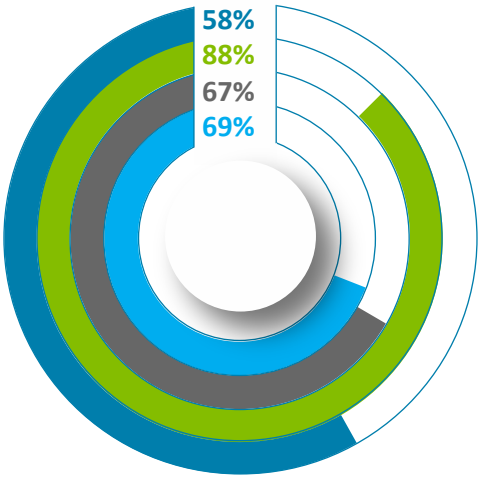
- تعزيز قدرات الباحثين والممارسين ورجال الأعمال السعوديين في مجال أمن المعلومات. [8]
- استخدام قدرات المرآة السعودية لتلبية متطلبات الأمن السيبراني في المملكة العربية السعودية.
- تعيين الشباب الذي يمتلكون مهارات حاسوبية صحيحة. [8]
- تدريب أكثر من 56,000 شاب سعودي على المهارات الأساسية في تقنية المعلومات والاتصالات من خلال برامج تطوير المواهب والشراكة مع شركات تقنية المعلومات العالمية.
- إنشاء الأكاديمية الوطنية للتدريب على المعلومات بالتعاون مع شركة أرامكو السعودية لتطوير وتدريب المواهب السعودية. [9]
- دعم وتمويل الجامعات العامة بشأن الأبحاث في مجال الأمن السيبراني وتقنية المعلومات والاتصالات.

الجاهزية السيبرانية للمملكة العربية السعودية [23]

في 2071، وبتوجيهات من الملك سلمان، تم اعتبار المركز الوطني للأمن السيبراني في المملكة العربية السعودية مركزًا لتنسيق الأمن السيبراني في المملكة. [3]

المؤشر الوطني للأمن السيبراني هو مؤشر عالمي يقيس مدى استعداد الدول لمنع التهديدات السيبرانية وإدارة الحوادث السيبرانية. كما أن المؤشر الوطني للأمن السيبراني عبارة عن قاعدة بيانات تحتوي على مواد الإثبات المتاحة للعامة وأداة لبناء القدرات الوطنية للأمن السيبراني. [23]

[23]



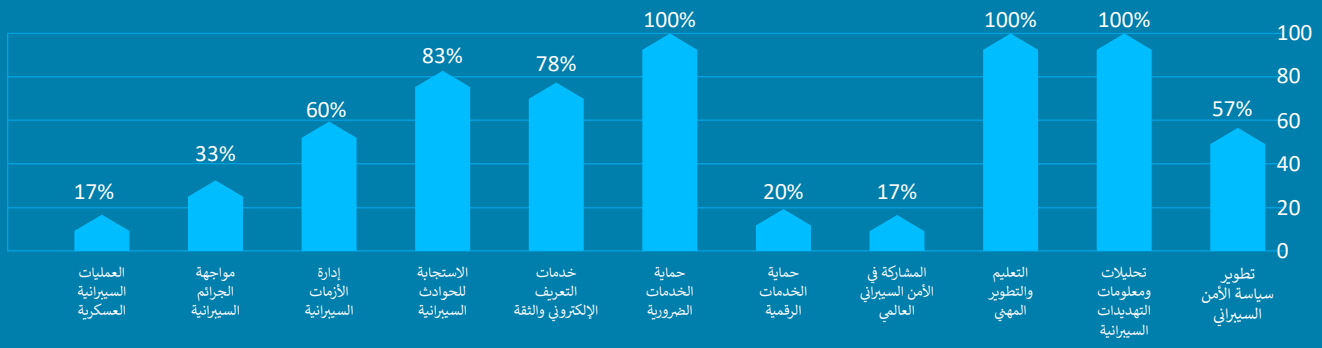
المرتبة 34 في المؤشر الوطني للأمن السيبراني

المرتبة 13 في المؤشر العالمي للأمن السيبراني

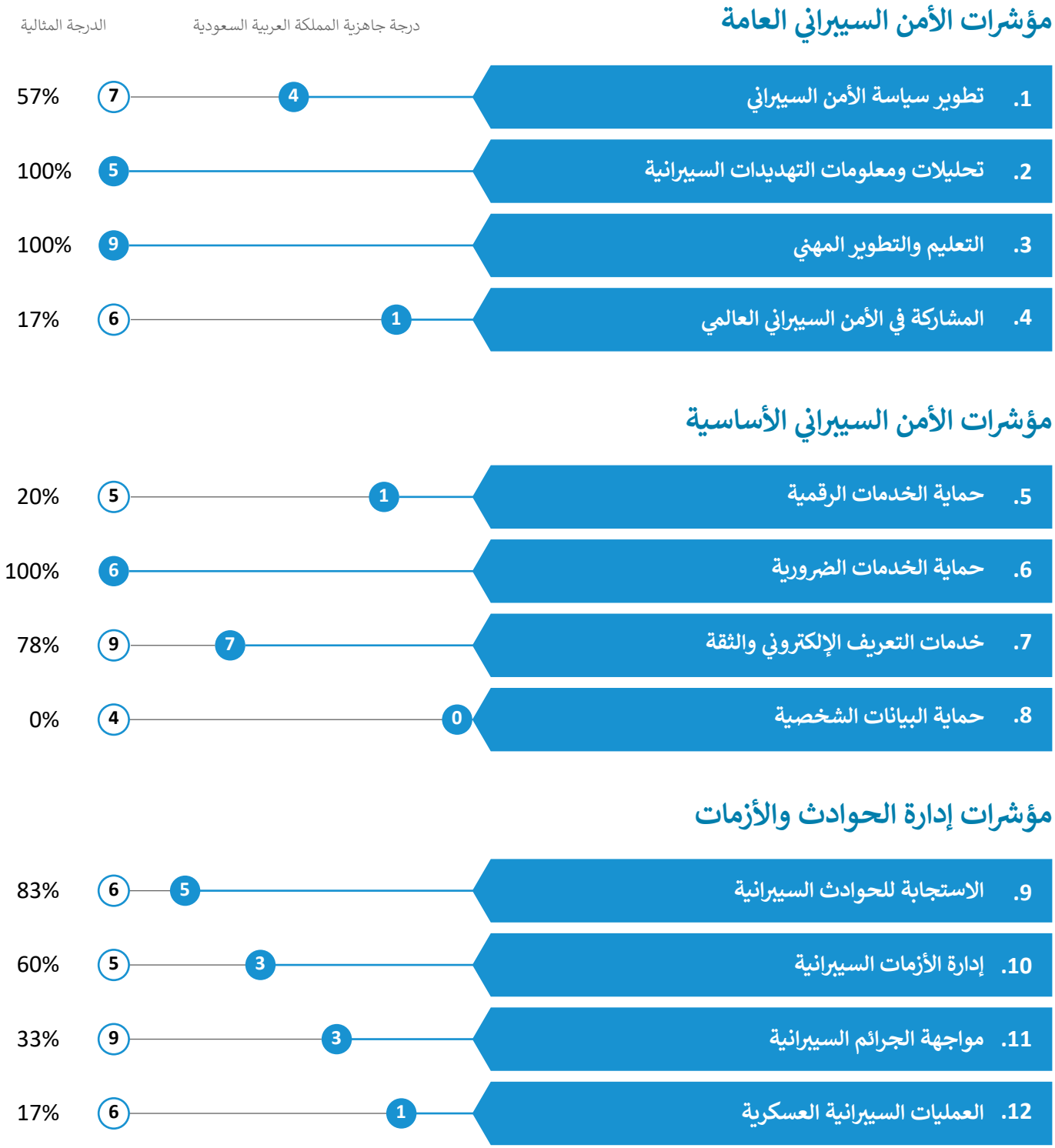
المرتبة 54 في مؤشر تطوير تقنية المعلومات والاتصالات

المرتبة 33 في مؤشر جاهزية الشبكة

نسبة الوفاء بالمؤشر الوطني للأمن السيبراني [23]



الجاهزية السيبرانية للمملكة العربية السعودية [23]



الأهمية الصناعية لتقنية صمام البيانات

قطاع النفط والغاز:

يتمتع قطاع النفط والغاز في المملكة العربية السعودية بأهمية كبيرة للعالم، وهذا القطاع معرض للهجمات السيبرانية بشكل كبير. من الممكن أن تسبب انتهاكات البيانات في صناعة النفط والغاز في جميع أنحاء المملكة العربية السعودية ردة فعل اقتصادية واجتماعية شديدة. ومن ثم، فإن استخدام تقنية صمام البيانات في صناعة النفط والغاز في المملكة متقلب في الآونة الأخيرة. [16]

قطاع الطاقة:

كما تنشر المملكة العربية السعودية تقنية صمام البيانات في مواقع توليد الطاقة ومرافق تحلية المياه وعمليات البتروكيماويات. [17]

أنظمة الأتمتة الصناعية والتحكم:

بنمو قطاع تقنية المعلومات والاتصالات والقطاعات الرقمية، استوعبت المملكة العربية السعودية الأتمتة في القطاع الصناعي. يمكن تحقيق وظائف أنظمة الأتمتة الصناعية والتحكم الرئيسية مثل مراقبة حالة النظام وتكرار البيانات ومراقبة النسخ الاحتياطي عن بعد وإدارة التصحيح عن طريق تقنية صمام البيانات. [18]

القطاع العسكري والفضاء الجوي:

يحتفظ القطاع العسكري والفضاء الجوي بقاعدة بيانات لقوائم الجرد بغية تتبع العجز في المخزون. وعند انخفاض المخزون، تُرسل معلومات من قاعدة البيانات إلى البائعين. يساعد صمام البيانات في ضمان حماية شبكات مشاركة المعلومات من التهديدات الخارجية. [24]

برنامج أرامكو السعودية لتعزيز القيمة المضافة الإجمالية في المملكة (اكتفاء)

يهدف برنامج أرامكو السعودية اكتفاء إلى إحداث قيمة محلية وقيادة النمو الاقتصادي وتشجيع الاختلاف بغية دعم النحو السريع لاقتصاد المملكة. [10] وفي هذا السياق، فإن التطوير المحلي لبيانات صمام البيانات في شركة الإلكترونيات المتقدمة ذو اتصال وثيق بالبرنامج.

تتعاون أرامكو السعودية مع الموردين المحليين لوضع خطط مدتها 5 سنوات من شأنها أن تقود الازدهار والقدرات المحلية والاكتفاء الذاتي الاستراتيجي والقيمة المحلية للمملكة.

توطين اكتفاء وأهداف خلق الوظائف [10]

70%
محتوى محلي

500,000
وظيفة

30%
خبراء

تحت رعاية أرامكو السعودية، أجرت شركة الإلكترونيات المتقدمة أبحاث وتطويرات رائدة في مجال الأمن الإلكتروني لتطوير "صمام البيانات"، وهو أحد منتجاتها الرئيسية.

تُحدث أرامكو السعودية قيمة للاقتصاد السعودي من خلال دعم مبادرات التوطين، وقد بذلت الشركة جهودًا رئيسية في تقوية تقنية صمامات البيانات الخاصة بشركة الإلكترونيات المتقدمة.

الخاتمة

شهد الوضع الأمني السيبراني في المملكة العربية السعودية تحسينات رئيسية على مدار العقد الماضي. كما تحسن مؤشر الاستثمار في المملكة في مجال الأمن السيبراني، مما أدى إلى نمو الأعمال وإحداث القيمة والتصنيع المحلي داخل المملكة. يساهم برنامج اكتفاء بهمة في تعزيز إنتاج المحتوى المحلي في الصناعات الرئيسية بما في ذلك الأمن والحوسبة والتقنيات.

تتجنب المملكة العربية السعودية الهجمات السيبرانية تحت الأهداف الثلاثي (السرية والنزاهة والتوافر). ظهر صمام البيانات كبديل رئيسي لتقنيات نقل البيانات الأخرى بسبب بروتوكول الاتصال السابق أحادي الاتجاه. بالإضافة إلى ذلك، أدت قدرة صمام البيانات أحادي الاتجاه إلى حماية الأسرار والأصول بالإضافة إلى شعبية هذه التقنية.

تتماشى أرامكو السعودية وشركة الإلكترونيات المتقدمة، في تقنية صمام البيانات الداخلي، مع أهداف تطوير المحتوى المحلي في إطار برنامج اكتفاء. سيتوقف نمو اقتصاد المملكة العربية السعودية بشكل كبير على مساعي التوطين في مجال التقنيات السيبرانية.

المراجع

1. “Transforming the Economy of Saudi Arabia by Going Digital.” Cequens.Com, 2019, www.cequens.com/story-hub/transforming-the-economy-of-saudi-arabia-by-going-digital.
2. Deloitte. National Transformation in the Middle East A Digital Journey.
3. Hathaway, Melissa, et al. KINGDOM OF SAUDI ARABIA CYBER READINESS AT A GLANCE. 2017.
4. Cyber Readiness Index. “Cyber Readiness Index.” Potomac Institute, Potomac Institute, www.potomacinstitute.org/academic-centers/cyber-readiness-index.
5. Ministry of Communications and Information Technology. “National Cyber Security Strategy of Saudi Arabia.” Europa.Eu, 2013,www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategy-of-saudi-arabia/.
6. Bridge, Sam. “Revealed: The Cost of Saudi, UAE Data Breaches.” ArabianBusiness.Com, 2017, www.arabianbusiness.com/technology/401429-wkd-revealed-the-cost-of-saudi-uae-data-breaches.
7. IBM. 2018 Cost of Data Breach Study Global Overview. 2018.
8. The BusinessYear. “ICT Infrastructure Targeted in 1,000 Cyberattacks in 2016.” The Business Year, 14 Aug. 2017, www.thebusinessyear.com/saudi-arabia-2017/eng-abdullah-al-swaha-minister-communications-information-technology/vip-interview.
9. MCIT Saudi. Developing National Information Security Strategy for the Kingdom of Saudi Arabia.
10. ITU. “Developing National Information Security Strategy for the Kingdom of Saudi Arabia.” MCIT, 2013.
11. IKTVA. In-Kingdom Total Value Add (Iktva) Program 5-Year IKTVA Plan Format Guide.
12. Bell, Jennifer. “KSA Must Become More Resilient against Cyberattacks.” Arab News, Arabnews, 22 July 2018, www.arabnews.com/node/1343151/saudi-arabia.
13. “How Data Diode Cybersecurity Is Being Used to Protect Critical Infrastructure in the Middle East: Owl Cyber Defense.” Owlcyberdefense.Com, 2018, www.owlcyberdefense.com/blog/2018/10/11/data-diode-cybersecurity-protect-critical-infrastructure-middle-east.
14. PLC, NCC Group. “Private Sector Cyber Resilience and the Role of Data Diodes.” Nccgroup.Trust, 2019, www.nccgroup.trust/uk/our-research/private-sector-cyber-resilience-and-the-role-of-data-diodes/.
15. Okhravi, Hamed, and Fredrick Sheldon. Data Diodes in Support of Trustworthy Cyber Infrastructure.
16. Owl Cyber defense. Global Oil & Gas Company Enables Secure, One-Way Production Data Transfer to HQ Company Overview. Owl Cyber Defense.Owlcyberdefense.Com, 2018, https://owlcyberdefense.com/wp-content/uploads/2019/05/owlcyberdefense-use-case_global-oil-gas.pdf
17. Owl Cyber Defense. “How Data Diode Cybersecurity Is Being Used to Protect Critical Infrastructure in the Middle East: Owl Cyber Defense.” Owlcyberdefense.Com, 2018, owlcyberdefense.com/how-data-diode-cybersecurity-is-being-used-to-protect-critical-infrastructure-in-the-middle-east/.
18. SANS. “SANS Institute: Reading Room - Firewalls & Perimeter Protection.” Sans.Org, 2018, www.sans.org/reading-room/whitepapers/firewalls/paper/36057.
19. “Electrical Monitor:: Data Diode Technology Can Help Solve Complex Smart Grid Cyber Security Issues.” Electricalmonitor.Com, 2012, www.electricalmonitor.com/ArticleDetails.aspx?aid=1206&sid=11.
20. “A Strategy for Smart Meters and Smart Grids in the Kingdom of Saudi Arabia.” Ecra.Gov.Sa, 2019, www.ecra.gov.sa/en-us/ECRAStudies/Pages/study2.aspx.
21. Owl Cyber Defense. “Data Diodes: Firewalls.” Owlcyberdefense.Com, 2019, owlcyberdefense.com/wp-content/uploads/2019/05/19-OWL-DataDiodes-Firewalls.pdf.
22. NTP. “National Transformation Program | Saudi Vision 2030.” Vision2030.Gov.Sa, Vision2030.gov.sa, 2019, vision2030.gov.sa/en/programs/NTP202.0.
23. National Cyber Security Index. “NCSI:: Saudi Arabia.” Ncsi.Ega.Ee, 2019, ncsi.ega.ee/country/sa/.
24. Owl Cyber Defense. PROTECTING USAF ICS USAF MAINTENANCE FACILITY SECURES AND AUTOMATES PARTS MANAGEMENT COMMUNICATIONS COMPANY OVERVIEW. Owl Cyber Defense, 2018. https://owlcyberdefense.com/wp-content/uploads/2019/05/owlcyberdefense-use-case_protecting-air-force-ics.pdf
25. Lerner, A. (2019). Network Segmentation. [online] Andrew Lerner. Available at: https://blogs.gartner.com/andrew-lerner/2017/11/09/network-segmentation/

SAMI
ADVANCED
ELECTRONICS
شركة الإلكترونيات المتقدمة

شركة الإلكترونيات المتقدمة

مطار الملك خالد. المنطقة الصناعية
P.O.Box 90916,
الرياض 11623, المملكة العربية السعودية

info@aecl.com +966112201350

/AECSaudiArabia