pwc

sirar by stc

CISO500: Empowering Cybersecurity Leaders for KSA Vision 2030

Programme introduction

The CISO500 programme is a prestigious, fully sponsored initiative that reflects PwC and sirar by stc's commitment to building a resilient national cybersecurity leadership.
Purpose-built to advance the goals of Saudi Vision 2030, this five-day program combines strategic foresight, deep technical expertise, and high-impact executive leadership development in cybersecurity. It's a unique opportunity for high-potential cybersecurity leaders to accelerate their professional growth and contribute meaningfully to the Kingdom's digital transformation.

"The CISO500 programme aims to empower 500 CISOs over the next five years with advanced cyber awareness and leadership. It fosters peer-to-peer dialogue, builds technical, business, and soft skills, and creates a strong community of cyber ambassadors.
The programme is designed to help CISOs track their growth and measure their impact on Vision 2030."

Samer Omar
Cybersecurity & Digital Trust Leader,
PwC Middle East

"Through this initiative, we support the Kingdom's leadership in shaping a secure digital future by building and empowering national capabilities. Our collaboration with PwC Middle East reflects our commitment to advancing cybersecurity standards by empowering leaders and sharing knowledge in line with global best practices. "

Yasser Alswailem
CEO, sirar by stc

Why choose CISO500?

Build it. Lead it. Live it.

In today's high-stakes environment, CISOs face complex challenges. This programme helps them better understand these challenges and explore ways to address them through informed leadership and peer collaboration.

Evolving Threats:
AI, quantum computing, IoT, and cloud technologies have expanded the attack surface. 87% of Saudi organisations plan to deploy GenAI tools in the next year – compared to 69% globally.

Talent Gaps:
84% of Saudi CISOs see automation and AI as critical to overcoming resource shortages.

Budget Approvals:
CISOs are under increasing pressure to demonstrate return on security investments, and secure board approvals for cybersecurity investments.

Cross-Functional Collaboration:
70% of global CISOs now prioritise alignment with HR, Finance, C-suite, and ERM functions.

Building Trust and Resilience:
73% of organisations in the Middle East view cybersecurity as a strategic pillar of customer trust, versus 57% globally.

Third-Party Risks:
36% of Middle Eastern organisations express concern over breaches within their vendor ecosystems.

Regulatory Demands:
Navigating local and global cybersecurity regulations is increasingly complex. CISOs must stay ahead of compliance while aligning with national strategies like Vision 2030. 63% of organisations boards in the Middle East are highly effective in executing regulatory responsibilities, significantly higher than the 50% globally.

Source: Statistics from 2025 Global Trust Digital Insights: Middle East findings

Programme at a glance

Duration:

5 Days

Language:

English (with Arabic support where needed)

Format:

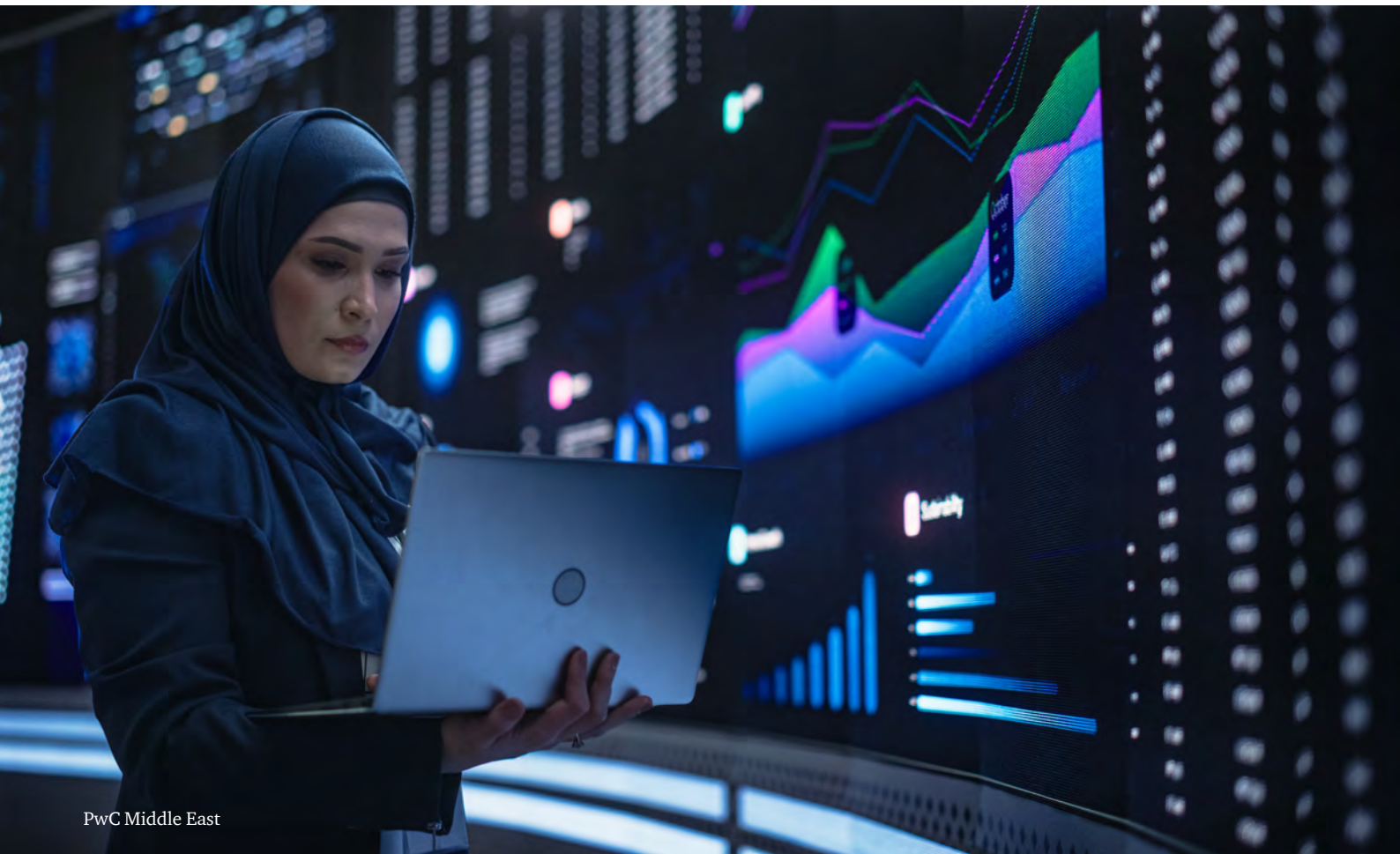
In-person sessions including workshops, peer discussions, and expert panels

Venue:

To be announced

Designed for Saudi's digital transformation journey, the programme equips cybersecurity leaders across key sectors—including finance, energy, healthcare, and smart cities—to anticipate change, adapt strategies, and act decisively.

- Aligns cyber priorities with business goals
- Integrates NCA guidelines, PDPL, and global standards
- Combines technical expertise, executive leadership, and financial strategy
- Custom built for Saudi Arabia's unique regulatory, business and cultural context



What you'll gain?

Strategic insight:

Learn directly from PwC's veteran cybersecurity leaders who have been at the forefront of the Kingdom's transformation initiatives.

Peer networking:

Build meaningful connections and a community across the industry.

Leadership readiness:

Navigate emerging challenges with confidence and clarity.

Real-world application:

Hands-on scenarios and case studies grounded in regional context.

In their own words

CISOs from our first cohort share how CISO500 impacted their leadership journey.

"Attending the programme was truly a standout experience. The experts delivering the sessions brought deep hands-on experience from the region. Insights were sharp, practical and directly aligned with the challenges that cybersecurity leaders face in Saudi Arabia. There was a room full of inspiring, passionate CISOs and future CISOs from across industries, each bringing their own perspective."

"CISO500 is a world-class training programme designed to equip cybersecurity leaders with the skills to tackle current and future challenges through comprehensive, strategic approaches. It also offers valuable opportunities to engage with senior cybersecurity officials across the Kingdom and the region."

"Attending the CISO500 programme was a great experience that gave me the knowledge and the confidence to move forward in my cybersecurity career.
I feel more prepared to take on advanced roles like CISO."

"I'd like to thank PwC and sirar by stc for delivering such a valuable programme.
The sessions are rich in content and provide cybersecurity leaders with the skills they need to succeed in their roles. I strongly encourage others to apply and take part. We look forward to seeing more CISOs across the Kingdom, advancing the vision of our leadership."

Core modules

Each day focuses on a fundamental domain of CISO leadership:

Day 1: Leading with vision

Redefine the CISO's evolving role	Align cybersecurity with strategic business outcomes	Cultivate self-awareness and executive presence

Day 2: Talent drives culture

Attract, retain, and grow top cybersecurity talent	Embed a security-first mindset across the organisation	Master performance management and governance frameworks

Day 3: Cyber as a business enabler

Integrate cyber strategy with digital transformation	Communicate with clarity and influence at all levels	Build business cases and manage security investments

Day 4: Next-gen tech & ecosystem hygiene

Understand AI, quantum, and next-gen tech implications	Foster innovation through design thinking and creative leadership	Implement third-party risk and vendor oversight frameworks

Day 5: Driving trust & collaboration

Develop trust-centric IAM and data protection practices	Design resilience strategies that scale with the organisation	Forge collaborative alliances across business units

Who should attend?

CISOs, Deputy CISOs, and senior cybersecurity executives

Heads of Cybersecurity and Cyber Risk Leads

Professionals overseeing enterprise-wide cybersecurity programmes

Eligibility

The CISO500 programme is open to:

Saudi nationals passionate about advancing cybersecurity and contributing to Vision 2030

Current CISOs or senior cyber professionals with 8+ years of experience

Leaders managing cybersecurity programmes or reporting directly to a CISO

Please note: This programme is available exclusively to Saudi nationals.

What's included?

Full participation in all programme sessions and workshops

Programme materials and resources

Professional certificate upon completion

Access to post-programme alumni network

How to apply?

Complete the application form

Submit the required support documents

Await your selection status

Cohort schedule

First Cohort:

Completed (20–24 April 2025)

Second Cohort:

22–26 June 2025

Upcoming Cohorts:

Dates to be announced

Note: Dates are subject to change

Contact information

Samer Omar

Cybersecurity & Digital Trust Leader, PwC Middle East
Email: samer.omar@pwc.com
Contact number: +966 53 922 7477

Apply Now

CISO500: تمكين قادة الأمن السيبراني لتحقيق مستهدفات رؤية السعودية 2030

مقدمة البرنامج

إن برنامج CISO500 عبارة عن مبادرة مرموقة ومموّلة بالكامل تعكس التزام شركة بي دبليو سي وشركة سرار التابعة لشركة الاتصالات السعودية بإنشاء قيادة وطنية مرنة للأمن السيبراني. ويجمع هذا البرنامج الذي تمّ تصميمه لتحقيق أهداف رؤية السعودية 2030 ويمتدعلى مدار خمسة أيام ما بين الاستشراف الاستراتيجي، والخبرة التقنية العميقة، وتطوير القيادة التنفيذية ذات الأثر الكبير في مجال الأمن السيبراني. إنها فرصة فريدة بالنسبة إلى قادة الأمن السيبراني ذوي الإمكانات العالية لتسريع وتيرة نموهم المهني والمساهمة بشكل فعّال في تحقيق التحول الرقمي في المملكة .

”

يهدف برنامج CISO500 إلى تمكين 500 من رؤساء الإدارة المعنية بالأمن السيبراني على مدى السنوات الخمس المقبلة من خلال تزويدهم بمهارات متقدّمة على مستوى التوعية والقيادة السيبرانية. وهو يعزز الحوار بين النظراء، ويُنمّي المهارات الفنية والشخصية والمرتبطة بالأعمال كما يُسهم في بناء مجتمع قوي من سفراء الأمن السيبراني. وقد تمّ تصميم البرنامج لمساعدة رؤساء الإدارة المعنية بالأمن السيبراني في متابعة تطور أدائهم وقياس تأثيره على تحقيق مستهدفات رؤية 2030. “

سامر عمر
قائد قسم الأمن السيبراني والثقة الرقمية في بي دبليو سي الشرق الأوسط

”

نقدّم من خلال هذه المبادرة، الدعم لقيادة المملكة في رسم معالم مستقبل رقمي آمن وذلك عبر بناء القدرات الوطنية وتمكينها. كما يعكس تعاوننا مع شركة بي دبليو سي الشرق الأوسط التزامنا بتطوير معايير الأمن السيبراني من خلال دعم القادة ومشاركة المعرفة بما يتماشى مع أفضل الممارسات العالمية . “

ياسر السويلم
الرئيس التنفيذي لشركة سرار التابعة للشركة الاتصالات السعودية

ما هي الدوافع لاختيار برنامج CISO500؟

بناء المستقبل. قيادة التغيير. تنفيذ الرؤية.

يواجه رؤساء الإدارة المعنية بالأمن السيبراني تحديات معقّدة في بيئة اليوم التي تتسم بمخاطر مرتفعة. ويساهم هذا البرنامج في فهم هذه التحديات بشكل أفضل واستكشاف طرق لمعالجتها من خلال القيادة المستنيرة والتعاون مع النظراء.

الموافقة على الميزانية :

يواجه رؤساء الإدارة المعنية بالأمن السيبراني ضغوطاً متزايدة لإثبات تحقيق عائدات على الاستثمارات في مجال الأمن السيبراني، والحصول على موافقات مجالس الإدارة على الاستثمار في هذا المجال.

فجوات المواهب :

يعتقد 84% من رؤساء الإدارة المعنية بالأمن السيبراني في السعودية أن الأتمتة والذكاء الاصطناعي أمران حاسمان للتغلب على تحديات نقص الموارد البشرية والتقنية .

التهديدات المتزايدة والمتطوّرة :

ساهمت تقنيات الذكاء الاصطناعي، والحوسبة الكمية، وإنترنت الأشياء، واعتماد تقنيات الحوسبة السحابية في توسيع نطاق الهجمات السيبرانية

87% من المؤسسات في المملكة العربية السعودية تخطط لاستخدام أدوات الذكاء الاصطناعي التوليدي للأمن السيبراني خلال العام المقبل، مقارنةً بنسبة 69% حول العالم.

التعاون الفعّال مع الإدارات الأخرى:

70% من رؤساء الإدارة المعنية بالأمن السيبراني يفيدون بأن مواءمة الأمن السيبراني مع الإدارات الأخرى مثل الموارد البشرية، والشؤون المالية والقيادات التنفيذية، وفرق إدارة المخاطر المؤسسية أصبحت أولوية حاسمة .

بناء الثقة والمرونة :

73% من المؤسسات في منطقة الشرق الأوسط تعتبر الأمن السيبراني من الأصول الاستراتيجية لتعزيز ثقة العميل، مقارنةً بنسبة 75% حول العالم .

المخاطر المرتبطة بالأطراف الخارجية :

تشعر 36% من المؤسسات في منطقة الشرق الأوسط بالقلق بشأن الاختراقات في منظومة الأطراف الخارجية .

المتطلبات التنظيمية :

يزداد التعامل مع أنظمة الأمن السيبراني المحلية والعالمية صعوبةً أكثر فأكثر. ويتعيّن على رؤساء الإدارة المعنية بالأمن السيبراني مواكبة متطلبات الامتثال والتوافق في الوقت نفسه مع الاستراتيجيات الوطنية مثل رؤية السعودية 2030. وتُظهر الإحصاءات أن 63% من مجالس إدارات المؤسسات في الشرق الأوسط فعّالة للغاية في تنفيذ المسؤوليات التنظيمية، وهي نسبة تفوق بشكل ملحوظ المتوسط العالمي عند 50% .

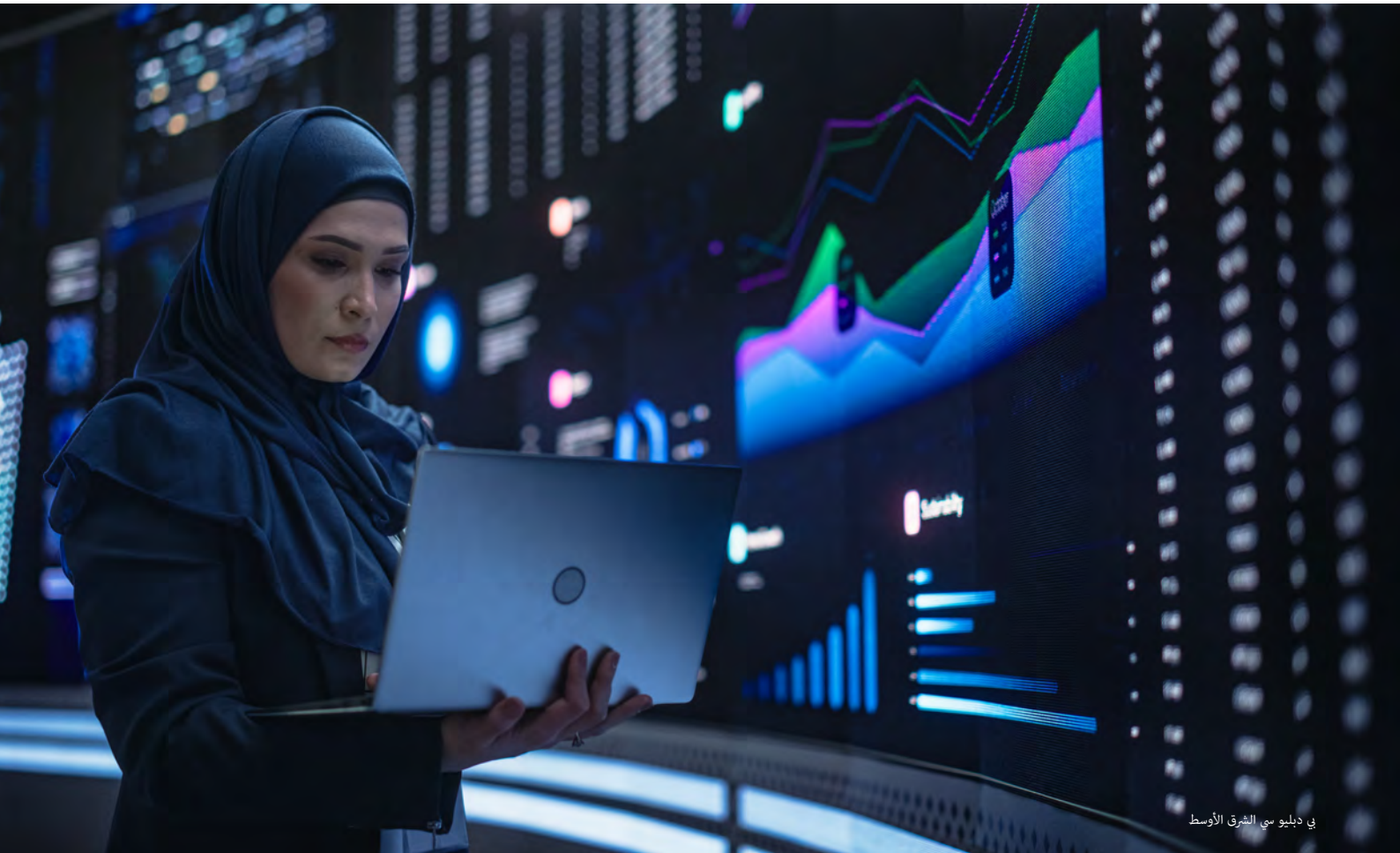
المصدر: إحصاءات من تقرير المعطيات حول الثقة في المجال الرقمي 2025: نتائج منطقة الشرق الأوسط

نظرة عامة عن البرنامج

المدّة :	اللغة :	الصيغة :	المكان :
5 أيام	الإنجليزية (مع توفير شرح باللغة العربية عند الحاجة)	جلسات حضورية تشمل ورش العمل والمناقشات مع النظراء، ولجان الخبراء	ستتمّ مشاركة الموقع في حينه

يهدف هذا البرنامج، الذي تمّ تصميمه لتحقيق رحلة التحوّل الرقمي في المملكة، إلى تزويد القادة في مجال الأمن السيبراني بالمهارات اللازمة عبر قطاعات رئيسية – بما فيها الشؤون المالية، والطاقة، والرعاية الصحية، والمدن الذكية – لاستباق التغييرات، وتكييف الاستراتيجيات، واتخاذ قرارات حاسمة

- مواءمة الأولويات السيبرانية مع أهداف الأعمال
- دمج توجيهات الهيئة الوطنية للأمن السيبراني، ونظام حماية البيانات الشخصية، والمعايير العالمية
- الجمع بين الخبرة التقنية والقيادة التنفيذية والاستراتيجية المالية
- تصميم برنامج يتناسب مع السياق الفريد الذي يميّز المملكة على صعيد الأنظمة والأعمال والثقافة



ما هي منافع البرنامج؟

الرؤى الاستراتيجية :

التعلّم مباشرة من القادة المتمرسين في مجال الأمن السيبراني في بي دبليو سي الذين تولوا قيادة مبادرات التحوّل في المملكة

بناء شبكة علاقات مع النظراء :

بناء علاقات مجدية ومجتمع فعّال عبر القطاع

جاهزية القيادة :

التعامل مع التحديات الناشئة بثقة ووضوح

التطبيق في العالم الحقيقي :

سيناريوهات عملية ودراسات حالة قائمة على السياق الإقليمي

في ما يلي اقتباسات من خبراء في المجال

في رحلتهم القيادية CISO500 يشارك رؤساء الإدارة المعنية بالأمن السيبراني في المجموعة الأولى كيف أثّر برنامج .

”

كانت المشاركة في البرنامج تجربة مميّزة بالفعل. فقد نقل الخبراء الذين قدّموا الدورات رؤى عملية عميقة نابعة من تجربتهم في المنطقة. وتميّزت هذه الرؤى بالوضوح وبالطابع العملي، كما عكست فهماً دقيقاً للتحديات التي يواجهها قادة الأمن السيبراني في المملكة. وجمعت القاعة التي استضافت البرنامج نخبة من الخبراء الملهمين والشغوفين من مختلف القطاعات، حيث عرض كل منهم وجهة نظره الخاصة . “

”

يُعتبر برنامج CISO500 عبارة عن برنامج تدريب من الطراز العالمي يهدف إلى تزويد قادة الأمن السيبراني بالمهارات اللازمة لمواجهة التحديات الحالية والمستقبلية من خلال اعتماد مقاربات استراتيجية شاملة. كما يقدّم فرصاً قيّمة للتواصل مع كبار المسؤولين في مجال الأمن السيبراني في المملكة والمنطقة . “

”

كانت المشاركة في برنامج CISO500 تجربة رائعة زوّدتني بالمعرفة والثقة للمضي قدماً في مسيرتي في مجال الأمن السيبراني. وأشعر اليوم بأنني أكثر استعداداً لتولي أدوار قيادية متقدّمة مثل رئيس الإدارة المعنية بالأمن السيبراني.“

”

أود أن أشكر شركة بي دبليو سي وشركة سرار التابعة لشركة الاتصالات السعودية على تقديم برنامج قيّم بهذا القدر. فقد تميّزت الدورات بمحتواها الغني وتركيزها على المهارات التي تمكّن قادة الأمن السيبراني من أداء أدوارهم بكفاءة ونجاح. لذا أنصح الجميع بتقديم طلبات للانضمام إلى البرنامج والمشاركة فيه ونحن نتطلع إلى رؤية المزيد من رؤساء الإدارة المعنية بالأمن السيبراني في . مختلف أنحاء المملكة، بما يسهم في دعم رؤية قيادتنا . “

المحاور الأساسية

يركّز كل يوم على مجال أساسي من قيادة رؤساء الإدارة المعنية بالأمن السيبراني :

اليوم 1: القيادة القائمة على الرؤية

إعادة تحديد الدور المتغيّر لرؤساء الإدارة المعنية بالأمن السيبراني	مواءمة الأمن السيبراني مع نتائج الأعمال الاستراتيجية	تحسين الوعي الذاتي والحضور التنفيذي

اليوم 2: الموهبة كمحرّك رئيسي لترسيخ الثقافة بالأمن السيبراني

استقطاب واستبقاء وتنمية أفضل المواهب في مجال الأمن السيبراني	ترسيخ ثقافة الأمن السيبراني أولاً عبر مستويات المؤسسة كافة	إتقان أطر الحوكمة وإدارة الأداء

اليوم 3: الأمن السيبراني كممكّن رئيسي لأعمال المؤسسة

دمج الاستراتيجية السيبرانية مع التحوّل الرقمي	التواصل بفعالية ووضوح عند مختلف المستويات	إعداد دراسات الجدوى وإدارة الاستثمار في مجال الأمن السيبراني

اليوم 4: تقنيات الجيل القادم وصحة المنظومة السيبرانية

فهم تداعيات تقنيات الذكاء الاصطناعي، والحوسبة الكمية، والجيل القادم	تعزيز الابتكار من خلال التفكير التصميمي والقيادة الإبداعية	تطبيق الأطر الخاصة بمخاطر الأطراف الخارجية والرقابة على الموردين

اليوم 5: تعزيز الثقة والتعاون

تطوير ممارسات قائمة على الثقة في مجال التحقق من الهوية وإدارتها وحماية البيانات	تصميم استراتيجيات المرونة التي يمكن توسيع نطاقها لتتكيف مع المؤسسة	إقامة تحالفات تعاونية عبر وحدات الأعمال

من يجب أن يشارك في البرنامج؟

رؤساء الإدارة المعنية بالأمن السيبراني، ونواب رؤساء الإدارة المعنية بالأمن السيبراني، وكبار المسؤولين التنفيذيين في مجال الأمن السيبراني

رؤساء قيادات الأمن السيبراني والمخاطر السيبرانية

القادة الذين يشرفون على برامج الأمن السيبراني على مستوى المؤسسة ككل

الأهلية

يمكن للفئات التالية الالتحاق ببرنامج CISO500 :

المواطنون السعوديون الذين يودّون تطوير خبراتهم في مجال الأمن السيبراني والمساهمة في تحقيق مستهدفات رؤية السعودية 2030

رؤساء الإدارة المعنية بالأمن السيبراني، أو القادة في مجال الأمن السيبراني الذين يمتلكون ما لا يقل عن 8 سنوات من الخبرة في المجال

الأفراد في المناصب القيادية الذين يديرون برامج الأمن السيبراني أو يرفعون تقاريرهم مباشرة إلى رئيس الإدارة المعنية بالأمن السيبراني

ملاحظة: هذا البرنامج متاح حصرياً للمواطنين السعوديين

ما الذي يشمله البرنامج؟

المشاركة الكاملة في جميع دورات وورش عمل البرنامج

مواد وموارد البرنامج

شهادة مهنية عند استكمال البرنامج

الوصول إلى شبكة الخريجين في مرحلة ما بعد البرنامج

كيفية التقدّم للمشاركة في البرنامج؟

قم بتعبئة نموذج الطلب

قدم المستندات الداعمة المطلوبة

انتظر إشعار اختيارك

جدول المجموعات

المجموعة الأولى :	المجموعة الثانية:	المجموعات المرتقبة :
مكتملة (20-24 أبريل 2025)	يونيو 2025 22-26	سيتمّ الإعلان عن التواريخ في حينه

ملاحظة: التواريخ قابلة للتغيير

معلومات التواصل

سامر عمر

قائد قسم الأمن السيبراني والثقة الرقمية في بي دبليو سي الشرق الأوسط

البريد الإلكتروني: samer.omar@pwc.com

رقم الاتصال: 7477 922 53 966 +

قدّم الآن