

دورة تدريبية: حوكمة الأمن السيبراني

أساسيات ومفاهيم حوكمة الأمن السيبراني

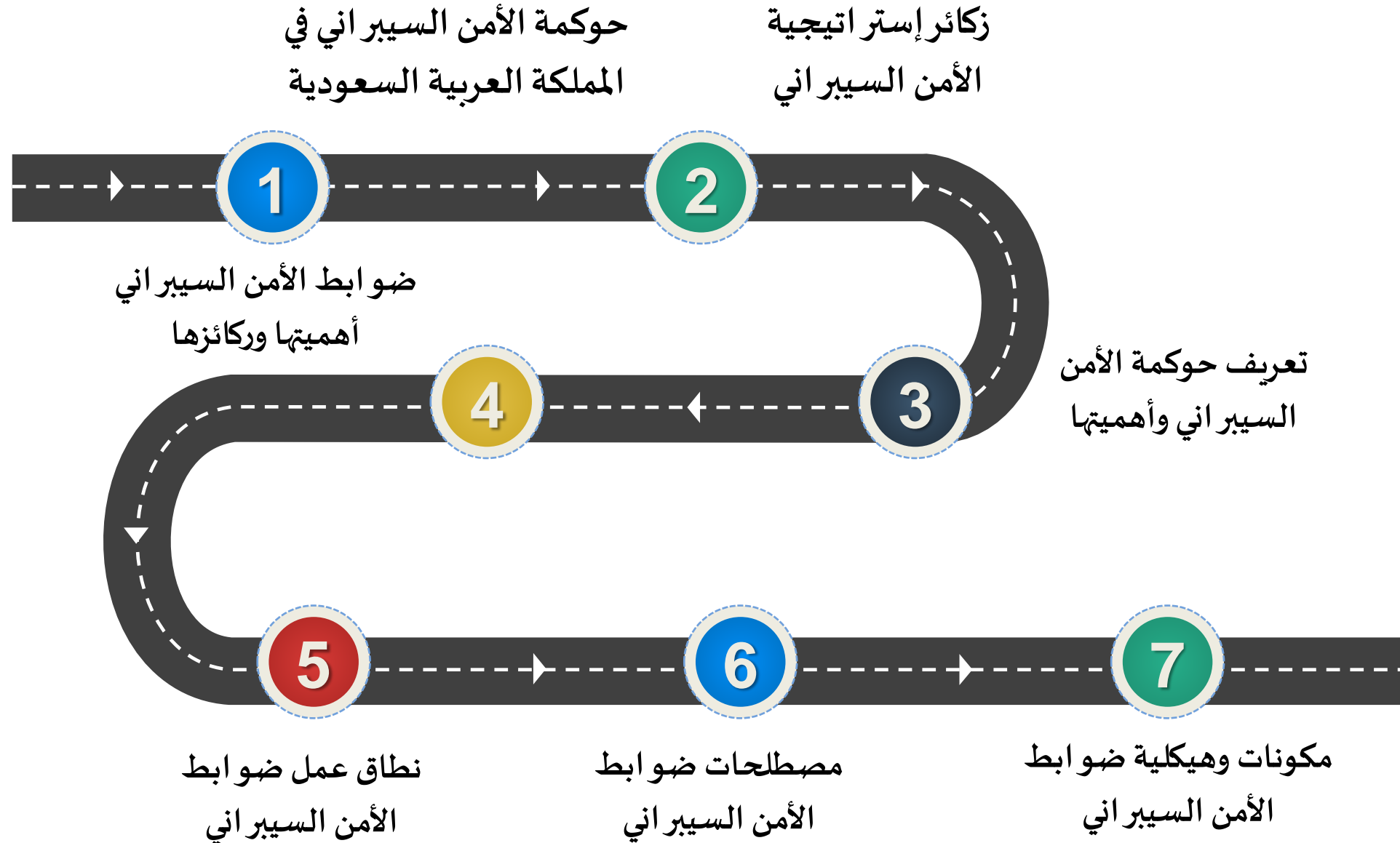
المحاضرة الرابعة

د. غالب الشمري

أستاذ الذكاء الإصطناعي وعلم البيانات المساعد

جامعة الملك سعود

خارطة الطريق





عصف ذهني



ما هو هدف حكومة المملكة
العربية السعودية في ظل التحول
الرقمي المتسارع؟



الأمن السيبراني في المملكة العربية السعودية

مع التسارع الكبير في عمليات التحول الرقمي ارتفعت معدلات الهجمات الإلكترونية ومخاطر اختراق البيانات مما جعل المملكة أكثر حرصًا في توفير بيئة آمنة للبيانات والعمليات الرقمية من خلال نظام أمني متين.

"بناء فضاء سيبراني سعودي آمن وموثوق
يمكن النمو والازدهار"

عصف ذهني

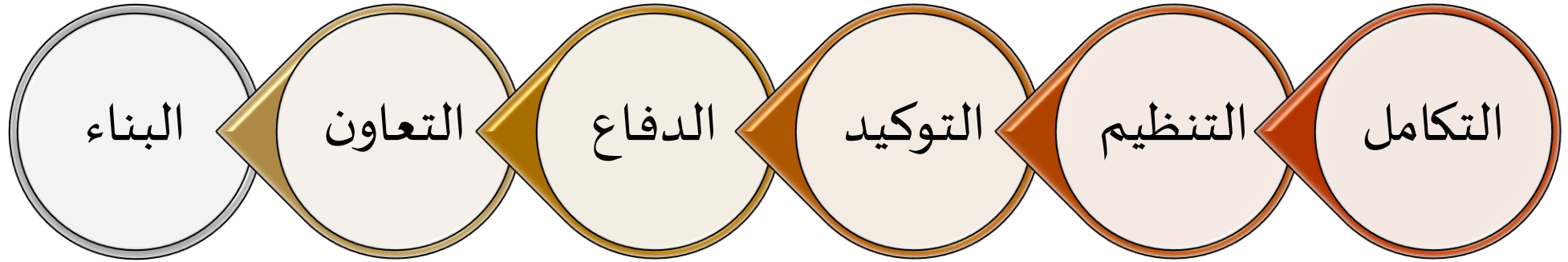


كيف يتم تحقيق هدف
"فضاء سيبراني سعودي آمن وموثوق"؟



الأمن السيبراني في المملكة العربية السعودية

من خلال **بناء إستراتيجية وطنية للأمن السيبراني** تعكس الطموح الإستراتيجي للمملكة العربية السعودية بأسلوب متوازن بين الأمان والثقة والنمو. تشمل هذه الإستراتيجية ستة محاور أساسية:



عصف ذهني



من وجهة نظرك
ما هي الأهداف المرجوة من بناء
إستراتيجية وطنية للأمن
السيبراني؟



الأمن السيبراني في المملكة العربية السعودية

تهدف الإستراتيجية الوطنية إلى:

حوكمة متكاملة للأمن السيبراني على المستوى الوطني

إدارة فعالة للمخاطر السيبراني على المستوى الوطني

حماية الفضاء السيبراني

تعزيز القدرات الوطنية في الدفاع ضد التهديدات السيبرانية

تعزيز الشراكات والتعاون في الأمن السيبراني

بناء القدرات البشرية الوطنية وتطوير صناعة الأمن السيبراني في المملكة

عصف ذهني

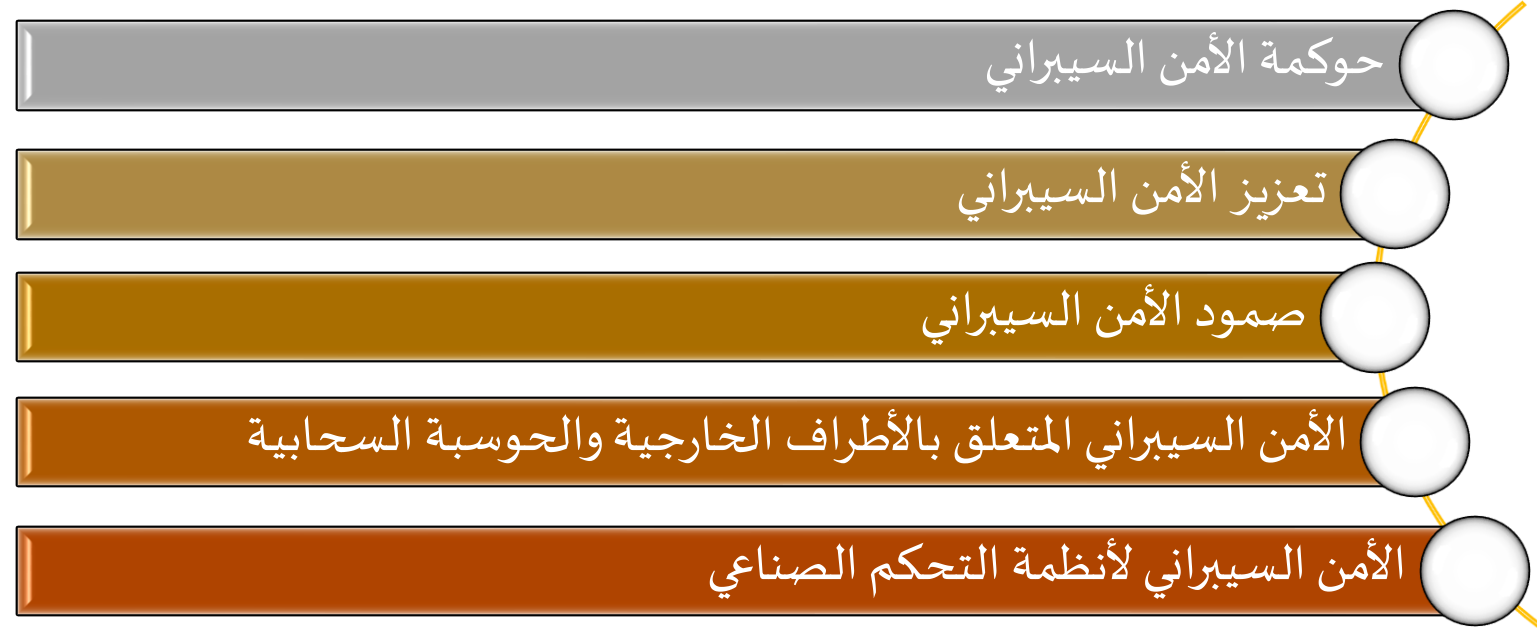


من وجهة نظرك
كيف يتم التحقق من الإلتزام
بالإستراتيجية؟ مع ذكر مكونات
التي تساعد بالإلتزام؟



الضوابط والسياسات الأساسية للأمن السيبراني

من أجل تقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية للجهات على مستوى داخلي أو خارجي، عملت الهيئة على 114 ضابط أساسي للأمن السيبراني مقسم على خمسة مكونات رئيسية:



عصف ذهني



من وجهة نظرك
ما المقصود بحوكمة الأمن
السيبراني؟

حوكمة الأمن السيبراني

تُعرف حوكمة الأمن السيبراني Cybersecurity Governance بأنها النظام المكون من العمليات والإجراءات التي تُساعد المنظمات على تنظيم العمل في الفضاء السيبراني وإكتشاف الهجمات السيبرانية، وتحديد كيفية الإستجابة لها، ومنع حدوثها.

- حوكمة الأمن السيبراني جزء من النظام المسؤول عن مخاطر أمن المعلومات.
- حوكمة الأمن السيبراني تركز على التخطيط الإستراتيجي، بينما تركز الإدارة على الإشراف والتنفيذ

أهمية حوكمة الأمن السيبراني

ستهدف رؤية المملكة العربية السعودية 2030 التطوير الشامل للوطن وأمنه واقتصاده ورفاهية مواطنيه وعيشتهم الكريم، ولقد كان من الطبيعي أن يكون أحد مستهدفاتها التحول نحو العالم الرقمي وتنمية البنية التحتية الرقمية؛ بما يعبر عن مواكبة التقدم العالمي المتسارع في الخدمات الرقمية وفي الشبكات العالمية المتجددة، وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ويتمشى مع تنامي قدرات المعالجة الحاسوبية وقدرات التخزين الهائلة للبيانات وتراسلها، وبما يهيئ للتعامل مع معطيات الذكاء الاصطناعي وتحولات الثورة الصناعية الرابعة.

- تأسيس الهيئة الوطنية للأمن السيبراني بالأمر الملكي رقم 6801 وتاريخ 11 / 2 / 1439هـ
- أكد الأمر الملكي رقم 57231 وتاريخ 10 / 11 / 1439هـ بأن "على جميع الجهات الحكومية رفع مستوى أمنها السيبراني لحماية شبكاتها وأنظمتها وبياناتها الإلكترونية، والإلتزام بما تصدره الهيئة الوطنية للأمن السيبراني من سياسات وأطر ومعايير وضوابط وإرشادات"



عصف ذهني



من وجهة نظرك
لكي يتم تحقيق المستهدفات من
إستراتيجية أمن المعلومات، لابد من
ركائز تقوم عليها، ناقشها؟



ركائز إستراتيجية الأمن السيبراني



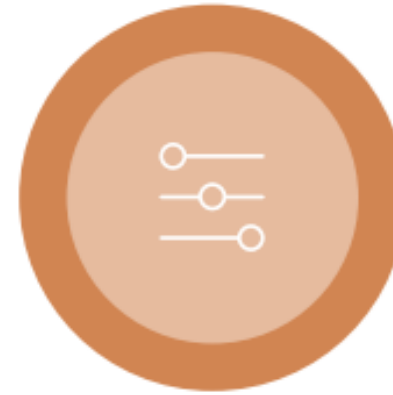
قدرات الأمن السيبراني

تطوير المعارف والمهارات
والقدرات ذات الصلة لتأمين
البيئة السيبرانية.



مرونة الأمن السيبراني

التأكد من القدرة على الاستجابة
للتحديات السيبرانية
والتعافي منها.



حوكمة الأمن السيبراني

تعزيز الرقابة القيادية عن طريق
وضع إطار عمل مخصص
لحوكمة الأمن السيبراني.

ركائز إستراتيجية الأمن السيبراني



الابتكار في الأمن السيبراني

ترسيخ الابتكار المستدام
باعتباره أحد إمكانات الأمن
السيبراني.



نضج الأمن السيبراني

تعزيز الوعي بالأمن السيبراني
وأطر الإدارة الملائمة للتهديدات
السيبرانية.



شراكات الأمن السيبراني

ضمان التعاون من خلال شراكات
متعددة الأطراف لتحسين
الفضاء السيبراني.



عصف ذهني



من وجهة نظرك
ما المقصود بمرونة الأمن السيبراني؟



الركيزة الأولى: حوكمة الأمن السيبراني

تُعنى هذه الركيزة بوضع إطار حوكمة للأمن السيبراني لكافة القطاعات، بحيث لن يعمل هذا الإطار على ترسيخ قيادة مخصصة وهيكل تنظيمي مناسب فحسب، بل أيضاً ترسيخ إجراءات شاملة لتحقيق الأهداف الإستراتيجية وإستدامتها. **تهدف** هذه الركيزة لإنشاء إطار قوي لحوكمة الأمن السيبراني يضم مجموعة من أوجه المساءلة والمسؤوليات.

الركيزة الثانية: مرونة الأمن السيبراني

تُعنى هذه الركيزة بضمان تهيئة بيئة قوية لكافة القطاعات وقادرة على مواجهة التهديدات السيبرانية والتكيف مع الظروف المتغيرة، بما يشمل القدرة على تحمل جميع أنواع الهجمات، والتعافي السريع من الآثار السلبية، والحد من أضرار الهجمات على المنشآت الصحية والأفراد والمجتمع. **تهدف** هذه الركيزة إنشاء إطار إستجابة سيبرانية مع إدارة التهديدات ومخاطر وحوادث الأمن السيبراني، تقليل المشاكل ونقاط الضعف المحددة في النظم والتطبيقات والبنية التحتية وذلك بإتباع نهج قائم على إدارة المخاطر، ووضع الخطط الإستمرارية للأمن السيبراني على مستوى القطاعات.

عصف ذهني



من وجهة نظرك
ناقش بعض المبادرات التي تنبثق من
الركيزة الأولى والثانية وفقاً لقطاعك؟



مبادرات حوكمة ومرونة الأمن السيبراني

- إنشاء هياكل داخلية مناسبة لضمان كفاءة وتنفيذ المسؤوليات [1.1]
- وضع إجراءات رصد وإبلاغ تتميز بالكفاءة والفاعلية وكذلك مؤشرات أداء رئيسية للمتطلبات الحالية والمستقبلية [1.1]
- تشكيل فريق إستجابة متقدم لإدارة الحوادث يمتلك مجموعة من المهارات للتعامل مع حوادث وهجمات الأمن السيبراني [2.1]
- التعاون مع الهيئات والجهات المعنية لإعداد لوائح وإجراءات تعزز الأمن السيبراني [2.2]
- وضع سياسات إستمرارية للقطاعات والتحقق منها من خلال التشغيل التلقائي للتجهيزات الإحتياطية والتدريب على تلك الخطط بشكل متكرر [2.3]

الركيزة الثالثة: قدرات الأمن السيبراني

تُعنى هذه الركيزة بتطوير المعارف والمهارات والقدرات ذات الصلة بتعزيز القدرة على مواجهة مخاطر وتهديدات الأمن السيبراني، بما يشمل تطوير الوظائف والقدرات لتيسير الابتكار التقني في جميع القطاعات. **تهدف** لتهيئة بيئة تقنية تدعم المنصات التقنية الأمنة والتحول الرقمي للأمن للمنشآت، وكذلك رفع الوعي بأمن المعلومات والأمن السيبراني من خلال إرساء فهم الآثار المترتبة على الأفراد والإجراءات والتقنيات.

الركيزة الرابعة: شراكات الأمن السيبراني

تُعنى هذه الركيزة بضمان التعاون من خلال شراكات متعددة الأطراف لتعزيز الأمن السيبراني في المنظمات؛ وذلك بهدف الحماية من التهديدات السيبرانية، وزيادة تبادل المعلومات المتعلقة بمسارات التهديد، واتخاذ إجراءات ضد أطراف التهديد السيبراني المختلفة. **تهدف** لإقامة إتحادات محلية ودولية لتحسين التعاون بين مجتمع الأمن السيبراني، وكذلك تعزيز منصات ومنتديات التهديد السيبراني لمشاركة معلومات التهديدات السيبرانية.

عصف ذهني



من وجهة نظرك
ناقش بعض المبادرات التي تنبثق من
الركيزة الثالثة والرابعة وفقاً لقطاعك؟



مبادرات قدرات وشراكات الأمن السيبراني

- تعزيز تقنية الآتمتة لتقليل إهدار الوقت والتأخير في الإجراءات والتفاعلات الأمنية بهدف تحسين التعرف على التهديدات السيبرانية والإستجابة لها [3.1]
- إعداد وتنظيم برامج تثقيفية وتوعوية بالأمن السيبراني تستهدف جميع القادة والموظفين لضمان الوعي [3.2]
- التعاون مع الموردين والشركاء والجهات المعنية لتعزيز مبادئ التصميم الأمن في تطوير المنتجات [4.1]
- إعداد دليل معرفي أساسي لتقنية المعلومات بمكونات الفضاء السيبراني للمنظمة بهدف تجميع نقاط الضعف المحددة والتصحيحات والمشاكل الشائعة وكيفية حلها [4.2]



عصف ذهني



من وجهة نظرك
ما المقصود بالإبتكار في الأمن السيبراني؟



الركيزة الخامسة: نضج الأمن السيبراني

تُعنى هذه الركيزة بتحسين نضج الممارسات والإجراءات المتعلقة بالأمن السيبراني؛ حيث إنه من الضروري وضع إجراءات لتقييم فاعلية الضوابط والأطر الأمنية بشكل مستمر. ومع تطور مشهد التهديدات السيبرانية، ينبغي التكليف بوضع إطار أمني سيبراني ناضج ومتطور لتعزيز القدرات. **تهدف** لتعزيز إطار الأمن السيبراني وذلك بوضع التشريعات اللازمة وإستحداث مقاييس الإلتزام بها وتحديد متطلبات المجال من أفراد وإجراءات وتقنيات، وكذلك تعزيز حماية المعلومات من الوصول الغير مصرح به من خلال إستحداث آلية الأمن اللازمة للبنية التحتية الرقمية.

الركيزة السادسة: الابتكار في الأمن السيبراني

تُعنى هذه الركيزة بتقديم الابتكار المستدام باعتباره أحد ممكنات الأمن السيبراني، من خلال تبني الإتجاهات السائدة للتقنيات المستخدمة في مختلف القطاعات لتقديم أفضل الممارسات المستقبلية ضمن بيئة تشهد أقل قدر ممكن من التهديدات السيبرانية. ولا يشمل ذلك مجال التقنية فحسب، بل يشمل أيضاً جانبي الأفراد والإجراءات. **تهدف** لتنظيم وتمكين منظومة الابتكار من أجل تحقيق التحول الأمن سيبرانياً، وكذلك تشجيع الابتكار الأمن وتعزيز نضج الأمن السيبراني في ذات الوقت.



عصف ذهني



من وجهة نظرك
ناقش بعض المبادرات التي تنبثق من الركيزة
الخامسة والسادسة وفقاً لقطاعك؟



مبادرات نضح الأمن السيبراني والإبتكار

- تطوير منصة لتدقيق ومراقبة المنشآت بهدف تقييم حالة تطبيق معايير وسياسات المنظمة للأمن السيبراني ومدى الإلتزام بها [5.1]
- إنشاء عمليات توثيق / إعتقاد للنظم التي تعالج بيانات المنشآت وتتعامل مع الأجهزة المتصلة بالشبكة [5.2]
- وضع اللوائح والمعايير والسياسات لدعم تبني الإبتكار الآمن [6.1]
- تحديد وتبني التقنيات المستجدة في مختلف القطاعات والدول النظرية عالمياً لتحسين الوضع الأمني للمنظمات [6.2]



فترة نقاش




من وجهة نظرك
كيف يتم تحديد مدى حساسية
المعلومات ومقدر مشاركتها مع
الأطراف المختلفة؟

بروتوكول الإشارة الضوئية (TLP)

تم إنشاء نظام بروتوكول الإشارة الضوئية لمشاركة أكبر قدر من المعلومات الحساسة ويستخدم على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

 **أحمر – شخصي وسري للمستلم فقط**

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد سواء من داخل او خارج المنشأة خارج النطاق المحدد للاستلام.

 **برتقالي – مشاركة محدودة**


المستلم بالإشارة البرتقالية يمكنه مشاركة المعلومات في نفس المنشأة مع الأشخاص المعنيين فقط، ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

بروتوكول الإشارة الضوئية (TLP)

تم إنشاء نظام بروتوكول الإشارة الضوئية لمشاركة أكبر قدر من المعلومات الحساسة ويستخدم على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

 أخضر – مشاركة في نفس المجتمع

حيث يمكنك مشاركتها مع آخرين من منشأتك أو منشأة أخرى على علاقة معكم أو بنفس القطاع، ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

 أبيض – غير محدود



فترة نقاش



من وجهة نظرك
ما هي أهداف ضوابط الأمن
السيبراني ومكوناتها؟

أهداف وركائز ضوابط الأمن السيبراني

تهدف هذه الضوابط إلى توفير الحد الأدنى من المتطلبات الأساسية للأمن السيبراني المبنية على أفضل الممارسات والمعايير العالمية لتقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية للمنظمات من التهديدات (Threats) الداخلية والخارجية. والتي تتطلب حماية الأصول المعلوماتية والتقنية للمنظمة، التركيز على الأهداف الأساسية للحماية، وهي:

■ سرية المعلومات Confidentiality

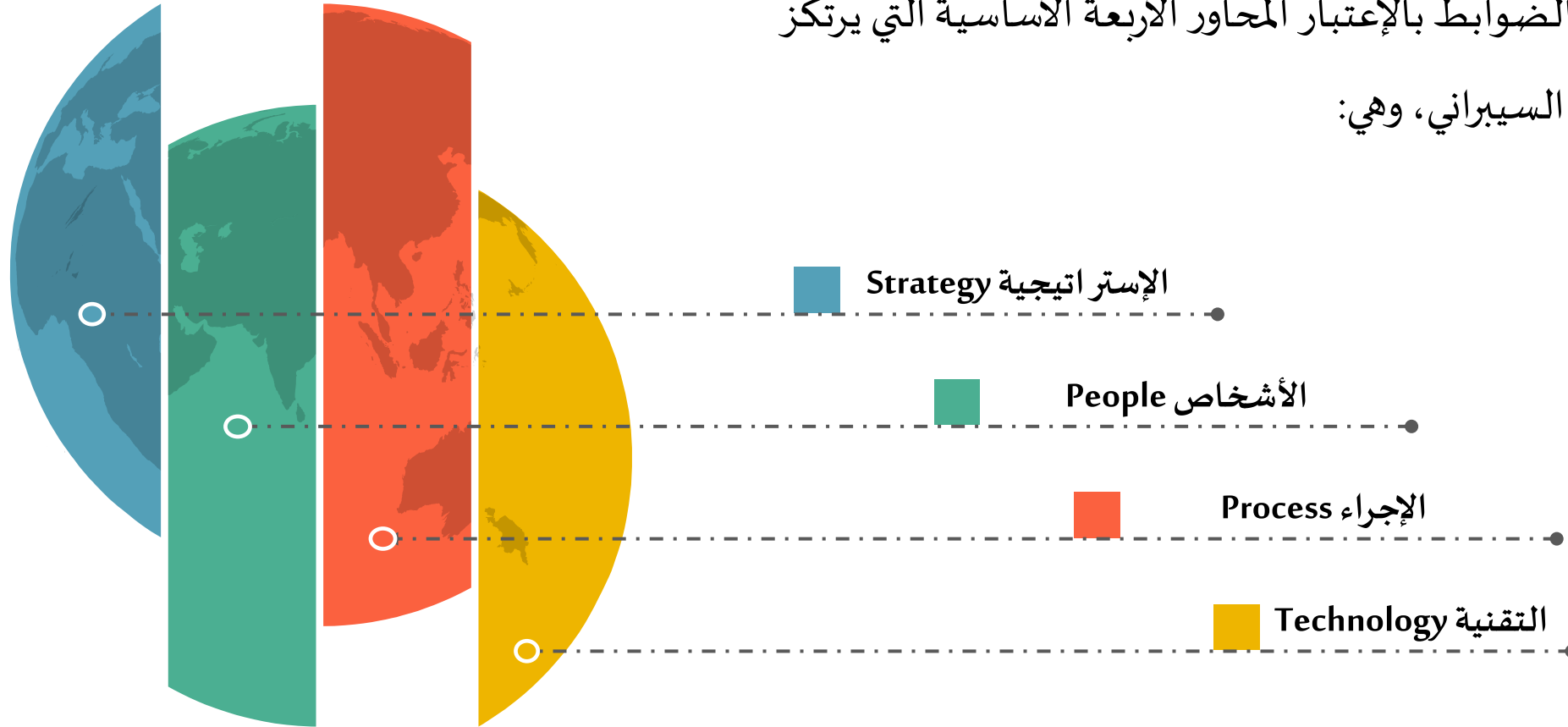
■ سلامة المعلومات Integrity

■ توافر المعلومة Availability

أهداف وركائز ضوابط الأمن السيبراني

تأخذ هذه الضوابط بالإعتبار المحاور الأربعة الأساسية التي يركز

عليها الأمن السيبراني، وهي:





فترة نقاش



من وجهة نظرك
ما هو نطاق العمل لهذه الضوابط؟
ومدى إمكانية تطبيقها؟

نطاق عمل ضوابط الأمن السيبراني وقابلية التطبيق

مُلزمة جميع الجهات الحكومية في المملكة العربية السعودية بتطبيق ضوابط الأمن السيبراني (وتشمل الوزارات والهيئات والمؤسسات وغيرها) والجهات التابعة لها، وجهات القطاع الخاص التي تمتلك بنى تحتية وطنية حساسة Critical National Infrastructures CNIs أو تقوم بتشغيلها أو إستضافتها. كما أن هذه الضوابط يمكن تطبيقها للحصول على أفضل الممارسات في الأمن السيبراني وتطويره داخل القطاع الخاص. تهدف سياسة الأمن السيبراني إلى:

- حوكمة الأمن السيبراني وإدارة المخاطر
- تقييم وتنفيذ ومراقبة ضوابط الأمن السيبراني بشكل دوري
- ضمان تحديد وتوثيق وإعتماد الإجراءات الضرورية المتعلقة بالأمن السيبراني
- ضمن إستعداد المنظمة للإستجابة لمخاطر الأمن السيبراني

نطاق عمل ضوابط الأمن السيبراني وقابلية التطبيق

مُلزمة جميع الجهات الحكومية في المملكة العربية السعودية بتطبيق ضوابط الأمن السيبراني (وتشمل الوزارات والهيئات والمؤسسات وغيرها) والجهات التابعة لها، وجهات القطاع الخاص التي تمتلك بنى تحتية وطنية حساسة Critical National Infrastructures CNIs أو تقوم بتشغيلها أو إستضافتها. كما أن هذه الضوابط يمكن تطبيقها للحصول على أفضل الممارسات في الأمن السيبراني وتطويره داخل القطاع الخاص. تهدف سياسة الأمن السيبراني إلى:

- حماية أصول معلومات المنظمة من التهديدات الداخلية والخارجية
- ضمان إستمرارية تحسين مستوى الأمن السيبراني في المنظمة
- ضمان سرية وصحة توافر المعلومات عند الحاجة إليها

نطاق عمل ضوابط الأمن السيبراني وقابلية التطبيق

كما أن هذه الضوابط ملائمة لإحتياجات الأمن السيبراني لجميع الجهات والقطاعات والمنظمات في المملكة العربية السعودية بتنوع طبيعتها وأعمالها وإستخدامها للتقنية، على سبيل المثال لتفاوت قابلية التطبيق لدى الجهات:

■ ضوابط الأمن السيبراني للحوسبة السحابية:

تكون قابلية للتطبيق للجهات التي تستخدم خدمات الحوسبة السحابية

■ ضوابط الأمن السيبراني لأنظمة التحكم الصناعي:

قابلة للتطبيق في الجهات التي تستخدم أنظمة تحكم صناعي أو تخطط لإستخدامها

بالإضافة إلى أنه تم تقسيم الضوابط إلى 11 مكون أساسي، كما يلي:

[حوكمة الأمن السيبراني – أمن الموارد البشرية – إدارة الأصول المعلوماتية – إدارة الهوية والوصول – الأمن المادي – إدارة البنية التحتية والعمليات الأمنية – أمن التطبيقات – التشفير – إدارة حوادث الأمن السيبراني وعمليات المراقبة – إدارة إستمرارية الأعمال – أمن الأطراف الخارجية والحوسبة السحابية]



فترة نقاش



من وجهة نظرك
كيف يتم التحقق من إلتزام الجهات
بضوابط الأمن السيبراني؟

إنشاء أداة تقييم وقياس مدى
إلتزام الجهات بتطبيق الضوابط
الأساسية للأمن السيبراني

مصطلحات ضوابط الأمن السيبراني

المصطلح	التعريف
الحماية من التهديدات المتقدمة المستمرة Advanced Persistent Threat (APT) Protection	الحماية من التهديدات المتقدمة التي تستخدم أساليب خفية تهدف إلى الدخول غير المشروع على الأنظمة والشبكات التقنية ومحاولة البقاء فيها لأطول فترة ممكنة عن طريق تفادي أنظمة الكشف والحماية. وهذه الأساليب تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware) لتحقيق هدفها.
الأصل Asset	أي شيء ملموس أو غير ملموس له قيمة بالنسبة للجهة. هناك أنواع كثيرة من الأصول؛ بعض هذه الأصول تتضمن أشياء واضحة، مثل: الأشخاص، والآلات، والمرافق، وبراءات الاختراع، والبرمجيات والخدمات. ويمكن أن يشمل المصطلح أيضاً أشياء أقل وضوحاً، مثل: المعلومات والخصائص (مثل: سمعة الجهة وصورتها العامة، أو المهارة والمعرفة).
هجوم Attack	أي نوع من الأنشطة الخبيثة التي تحاول الوصول بشكل غير مشروع أو جمع موارد النظم المعلوماتية أو المعلومات نفسها أو تعطيلها أو منعها أو تحطيمها أو تدميرها.



عصف ذهني



من وجهة نظرك
ما الفرق بين التدقيق والتحقق في
ضوابط الأمن السيبراني؟



مصطلحات ضوابط الأمن السيبراني

المراجعة المستقلة ودراسة السجلات والأنشطة لتقييم مدى فعالية ضوابط الأمن السيبراني ولضمان الالتزام بالسياسات، والإجراءات التشغيلية، والمعايير والمتطلبات التشريعية والتنظيمية ذات العلاقة.	تدقيق Audit
التأكد من هوية المستخدم أو العملية أو الجهاز، وغالباً ما يكون هذا الأمر شرطاً أساسياً للسماح بالوصول إلى الموارد في النظام.	التحقق Authentication
خاصية تحديد والتأكد من حقوق/تراخيص المستخدم للوصول إلى الموارد والأصول المعلوماتية والتقنية للجهة والسماح له وفقاً لما حدد مسبقاً في حقوق/تراخيص المستخدم.	صلاحية المستخدم Authorization
ضمان الوصول إلى المعلومات والبيانات والأنظمة والتطبيقات واستخدامها في الوقت المناسب.	توافر Availability
الملفات والأجهزة والبيانات والإجراءات المتاحة للاستخدام في حالة الأعطال أو الفقدان، أو إذا حذف الأصل منها أو توقف عن الخدمة.	النسخ الاحتياطية Backup

مصطلحات ضوابط الأمن السيبراني

الفضاء السيبراني Cyberspace	الشبكة المترابطة من البنية التحتية لتقنية المعلومات، والتي تشمل الإنترنت وشبكات الاتصالات وأنظمة الحاسب الآلي والأجهزة المتصلة بالإنترنت، إلى جانب المعالجات وأجهزة التحكم المرتبطة بها. كما يمكن أن يشير المصطلح إلى عالم أو نطاق افتراضي كظاهرة مجربة أو مفهوم مجرد.
تصنيف البيانات والمعلومات Data and Information Classification	تعيين مستوى الحساسية للبيانات والمعلومات التي ينتج عنها ضوابط أمنية لكل مستوى من مستويات التصنيف، يتم تعيين مستويات حساسية البيانات والمعلومات وفقاً لفئات محددة مسبقاً حيث يتم إنشاء البيانات والمعلومات أو تعديلها أو تحسينها أو تخزينها أو نقلها. مستوى التصنيف هو مؤشر على قيمة أو أهمية البيانات والمعلومات للجهة.
أرشفة البيانات Data Archiving	عملية نقل البيانات التي لم تعد مستخدمة بشكل فعال في جهاز تخزين منفصل للحفاظ طويل الأجل. تتكون بيانات الأرشيف من بيانات قديمة لا تزال مهمة للجهة وقد تكون مطلوبة للرجوع إليها في المستقبل، وبيانات يجب الاحتفاظ بها للالتزام بالتشريعات والتنظيمات ذات العلاقة.
الدفاع الأمني متعدد المراحل Defense-in-Depth	هو مفهوم لتوكيد المعلومات (Information Assurance) حيث يتم وضع مستويات متعددة من الضوابط الأمنية (كدفاع) في نظام تقنية المعلومات (IT) أو تقنية التشغيل (OT).

مصطلحات ضوابط الأمن السيبراني

الإفصاح عن أو الحصول على معلومات لأشخاص غير مصرح تسريبها أو الحصول عليها، أو انتهاك السياسة الأمنية السيبرانية للجهة بالإفصاح عن أو تغيير أو تخريب أو فقد شيء سواء بقصد أو بغير بقصد.	انتهاك أمني Compromise
ويقصد بالانتهاك الأمني الإفصاح عن أو الحصول على بيانات حساسة أو تسريبها أو تغييرها أو تبديلها أو استخدامها بدون تصريح (بما في ذلك مفاتيح تشفير النصوص وغيرها من المعايير الأمنية السيبرانية الحرجة).	
الاحتفاظ بقيود مصرح بها على الوصول إلى المعلومات والإفصاح عنها بما في ذلك وسائل حماية معلومات الخصوصية والملكية الشخصية.	السرية Confidentiality
الأنشطة والبرامج والخطط المصممة لإرجاع وظائف وخدمات الأعمال الحيوية للجهة إلى حالة مقبولة، بعد التعرض إلى هجمات سيبرانية أو تعطل لهذه الخدمات والوظائف.	التعافي من الكوارث Disaster Recovery
نظام تقني يستخدم قاعدة بيانات يتم توزيعها عبر الشبكة و/أو الإنترنت تسمح بتحويل أسماء النطاقات إلى عناوين الشبكة (IP Addresses)، والعكس، لتحديد عناوين الخدمات مثل خوادم المواقع الإلكترونية والبريد الإلكتروني.	نظام أسماء النطاقات Domain Name System



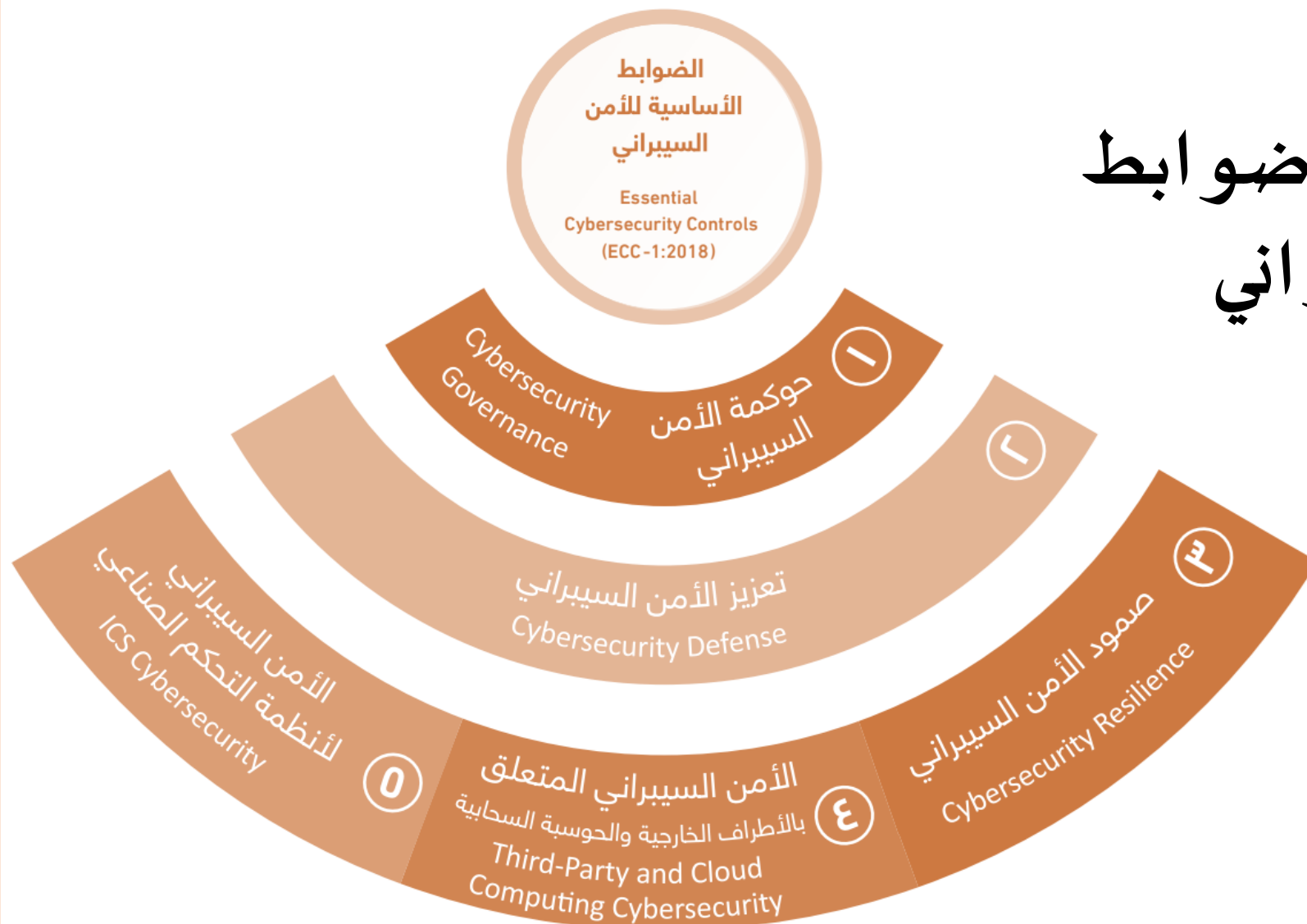
عصف ذهني



مما سبق نستنتج
مكونات وهيكلية ضوابط الأمن
السيراني؟



مكونات وهيكلية ضوابط الأمن السيبراني





شكراً لإستماعكم وتفاعلكم

- فترة الأسئلة -