دورة تدريبية: حوكمة الأمن السيبراني

الأمن السيبراني في القطاع العسكري

(الجزء الأول)

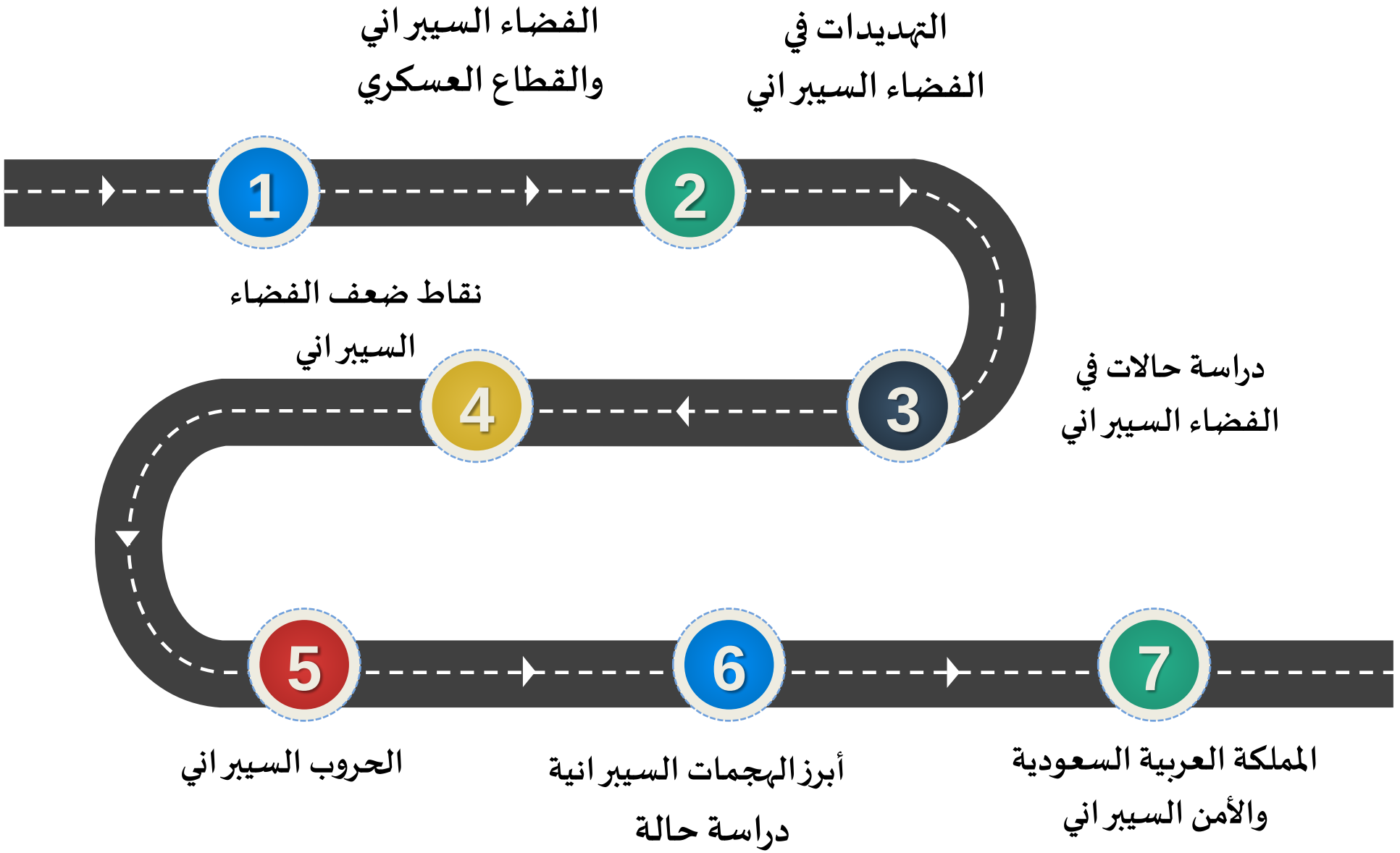
المحاضرة الثانية

د. غالب الشمري

أستاذ الذكاء الإصطناعي وعلم البيانات المساعد

جامعة الملك سعود

خارطة الطريق

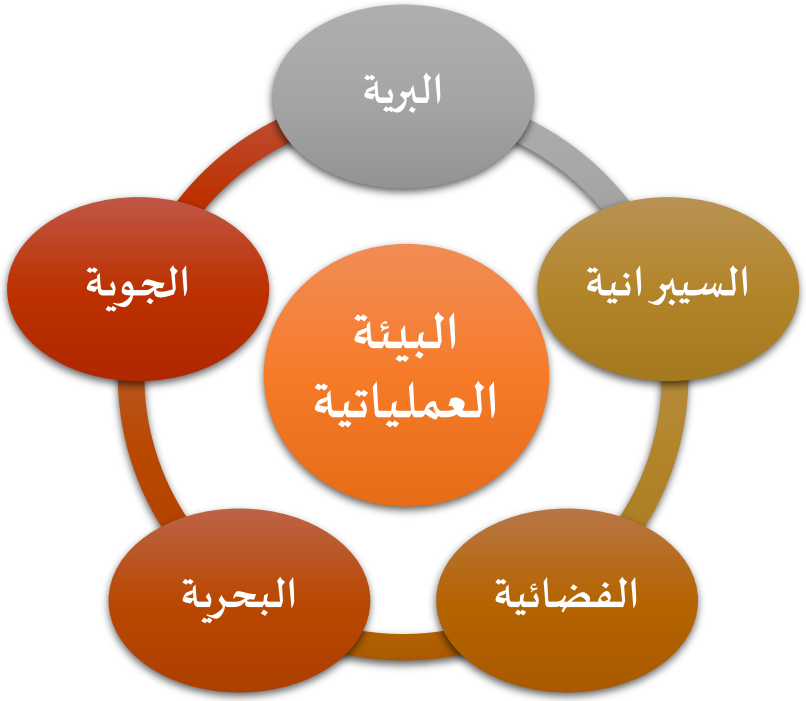


الإطار العملياتي لأنشطة الفضاء السيبراني

عمليات الفضاء السيبراني الدفاعية

الحروب الإلكترونية

عمليات الفضاء السيبراني الهجومية



عصف ذهني

من وجهة نظرك
ما هي الإجراءات العسكرية التي تجري في الفضاء السيبر اني؟ مع أمثلة عليها؟

إجراءات الفضاء السيبراني لتحقيق الأثر في القطاع العسكري

التأثير

01 عمليات الحرمان

إجراءات لإعاقة العدو أو منعه من إستخدام المجال أو الأفراد أو الإمدادات أو المرافق، مثل: تشويش التردد

02 الإضعاف

إجراءات لاستخدام وسائل مؤقتة للتقليل من فاعلية وكفاءة نُظم قيادة وسيطرة الخصم ووسائل جمع معلوماته، مثال: إبطاء سرعة الإنترنت.

03 التعطيل

مهام تكتيكية يُدمج فيها العمل المباشر والغير مباشر لإرباك الخصم وإضطراب جدوله الزمني، لإتجاذه قرارات سابقه لأوانها، مثل: تعطيل شبكة إتصالات الانترنت

إجراءات الفضاء السيبراني لتحقيق الأثر في القطاع العسكري

التأثير

04 التدمير

مهام تكتيكية تجعل القوة القتالية للخصم غير فعالة مادياً أو لا يمكنها أداء أي وظيفة، مثل: إستخدام الفضاء السيبراني لرفع درجة حرارة آلة محددة

05 التلاعب

السيطرة على معلومات الخصم أو نظم معلوماته أو شبكاته او تغييرها بطريقة تدعم الأهداف المحددة لتضليل صانعي القرار، مثل: تعديل رسالة مرسلة عبر الشبكة

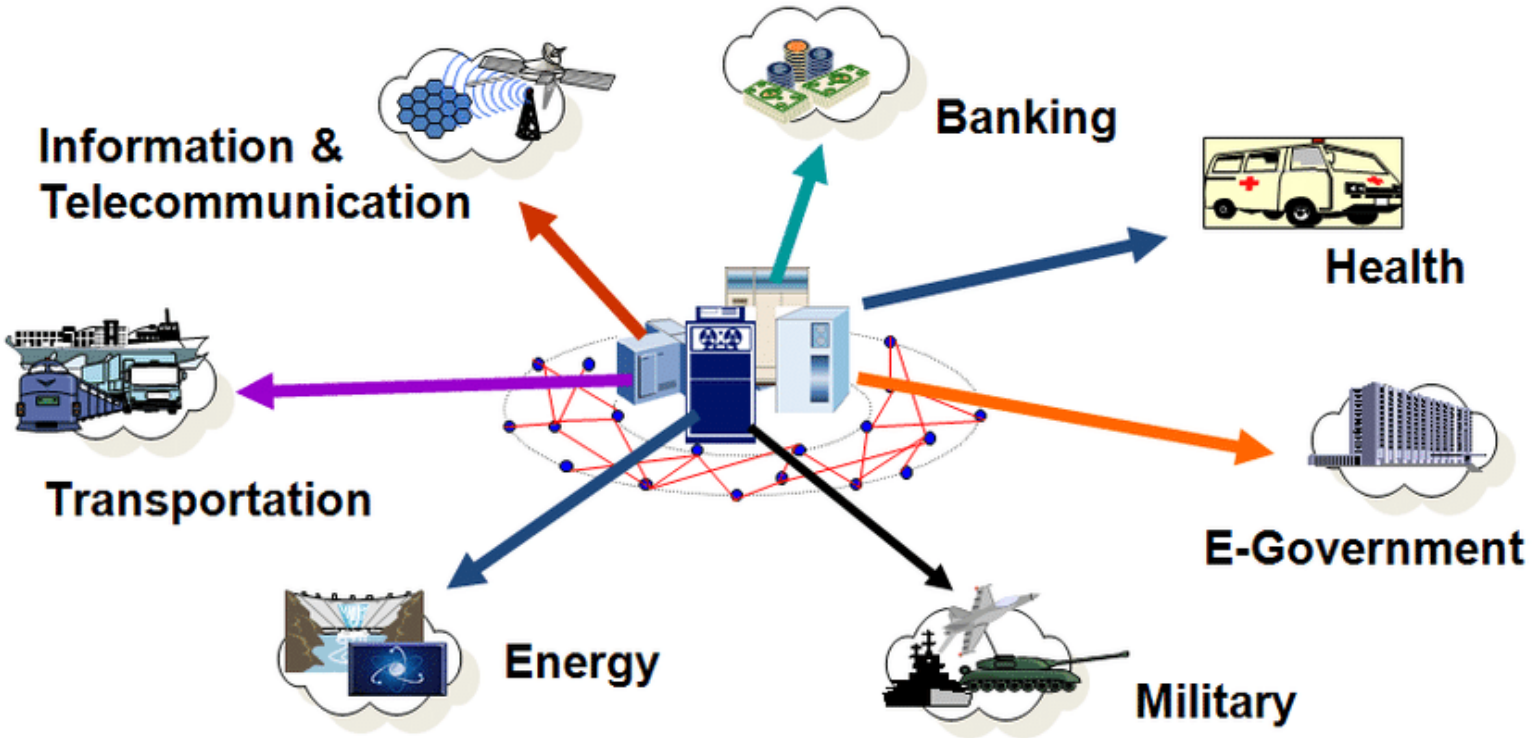
عصف ذهني

ما هو التحدي الحقيقي الذي يمثله الفضاء السيبراني؟

البيئة المعلوماتية للفضاء السيبراني

يتألف الفضاء السيبراني من عدة أبعاد، ما يلي:

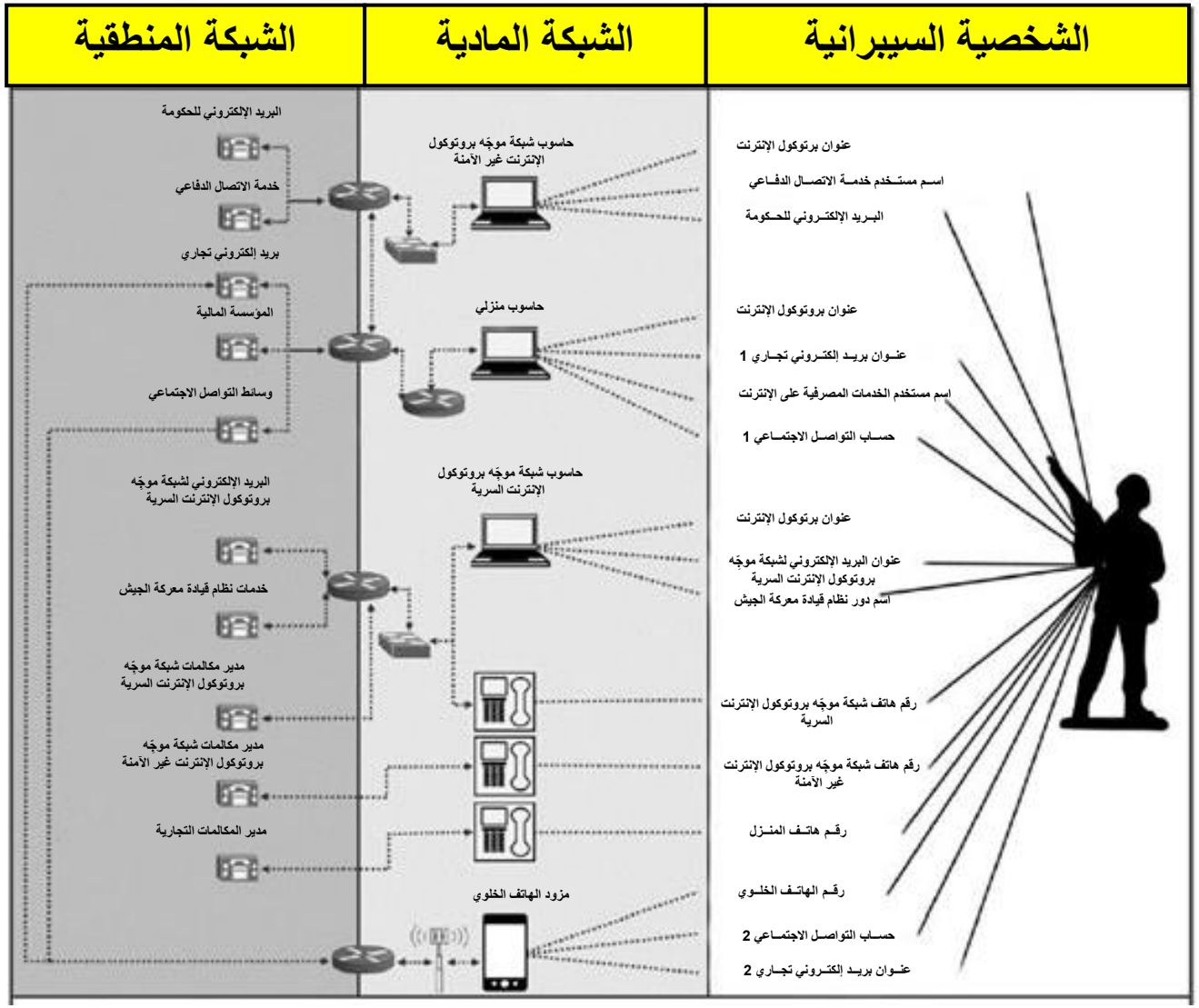
- بُعد مادي
- بُعد معلوماتي
- بُعد إدراكي
- بُعد إجتماعي
  - المستخدم
  - التهديدات



طبقات الفضاء السيبراني

يُوصف الفضاء السيبراني من خلال ثلاثة طبقات:

- الشبكة المادية
- الشبكة المنطقية
- الشخصية السيبرانية



عصف ذهني

ماذا يستفيد القطاع العسكري من طبقات الفضاء السيبراني؟

خصائص الفضاء السيبراني

الفضاء السيبراني هو **شبكات اتصالات حاسوبية مترابطة (طبقة منطقية)** تجعل المعلومات متاحة عالميًّا من خلال **اتصالات سلكية ولاسلكية** عند معدلات عالية من السرعة **باستخدام الطبقة المادية** التي يصل إليها الأفراد بعد ذلك **باستخدام طبقة الشخصية السيبرانية**. ينتشر الإنترنت في المجتمعات ويتيح الاتصال العالمي وتدفق المعلومات. يتسم الفضاء السيبراني بأنه:

- متصل بالشبكة
- مُمكن إجتماعياً
- تقني
- مترابط ومتداخل
- معرض للخطر

التهديدات السيبرانية

فيروس الفدية Ransomware

هجوم إلكتروني يقوم بتشفير ملفات الجهاز المصاب، كما يُستخدم لإبتزار المستخدم وتحريضه على دفع المال.

عصف ذهني

- ما الذي يعنيه تهديد الهجوم السيبراني مثل برامج الفدية؟
- ضمنياً للقطاع العسكري؟
- من المسؤول عن الحماية من الهجمات السيبرانية؟
- ما الخطوات التي تتخذها شخصياً لحماية المعلومات؟

بيانات سيبرانية: الربع الأول 2020م

أبرز 5 قطاعات تعرضت لتهديدات سيبرانية عالميًا في الربع الأول من العام 2020 [5]

1. القطاع العام - 21,58%
2. قطاع الرعاية الصحية - 13,37%
3. قطاع التعليم - 12,16%
4. القطاع المالي - 11,55%
5. قطاع التصنيع - 7,29%

أبرز 5 تهديدات سيبرانية عالمية في الربع الأول من العام 2020 [5]

1. البرمجيات الخبيثة - 42,09%
2. قرصنة الحسابات - 19,66%
3. الاختراق \ محاولة الاختراق - 11,97%
4. الثغرات الأمنية - 6,20%
5. البريد غير المرغوب به - 4,70%

أبرز 5 تهديدات سيبرانية في المملكة العربية السعودية في الربع الأول من العام 2020 [6]

1. البرمجيات الخبيثة -
2. الدخول، التعديل والاستخدام غير المصرح به -
3. الاختراق/محاولة الاختراق -
4. الاستخدام غير الصحيح -
5. تسرّب البيانات -

الحوادث السيبرانية العالمية

سرقة معلومات من أحد الشركات الائتمانية لأكثر من 140 مليون شخص (2017)

توقفت 60 محطة فرعية في أحد المرافق الكهربائية عن العمل لمدة 90 دقيقة لأحد الدول، مما أدى إلى انقطاع التيار الكهربائي عن 230,000 نسمة (2015)

ستكسنت: تم تدمير أجهزة طرد مركزي نووية بواسطة هجوم إلكتروني (2010)

سرقة معلومات أكثر من 500 مليون عميل لأحد الفنادق العالمية (2018-2014)

سرقة بيانات من شبكات أحد القوات المسلحة باستخدام ذاكرة بيانات فلاش تحوي برمجية خبيثة (2008)

تمت سرقة 81 مليون دولار من خلال التلاعب بأحد أنظمة المعاملات (2016)

قدرات التهديد في الفضاء السيبراني

التهديد	الطرق	المؤشرات	التأثيرات الأولية
هجوم حجب الخدمة	إحداث تزاحم لحركة البيانات على خدمة معينة أو خادم من أجل إستهلاك الموارد المتاحة مما يؤدي إلى حجب الخدمة	الآداء غير الطبيعي للشبكة، وعدم القدرة على تصفح شبكة الإنترنت والوصول إلى المواقع، ورسائل البريد الإلكتروني المزعجة غير المسيطر عليها، وإعادة تشغيل النظام	تدهور قدرات الشبكة وهذه تتراوح من التخطيط العملياتي المحدود إلى الحرمان التام من الاستخدام
إختراق الشبكة	هجمات تصيد إلكتروني أو تشويش للبيانات وإستغلال البيانات الغير مشفرة والصفحات ذات المزايا الأمنية الضعيفة	البريد الإلكتروني الغير مؤلوف، وعناوين البريد الإلكتروني التي تتطلب الرد العاجل، روابط لمواقع غير شرعية، الإنتقال الموجه من موقع إلى مواقع آخر، طلبات الترقية والتحقق من صحة المعلومات	الوصول الغير مسموح للشبكة والغير خاضع للتحكم، القدرة على حجب بعض الخدمات من الشبكة، سرقة البيانات

قدرات التهديد في الفضاء السيبراني

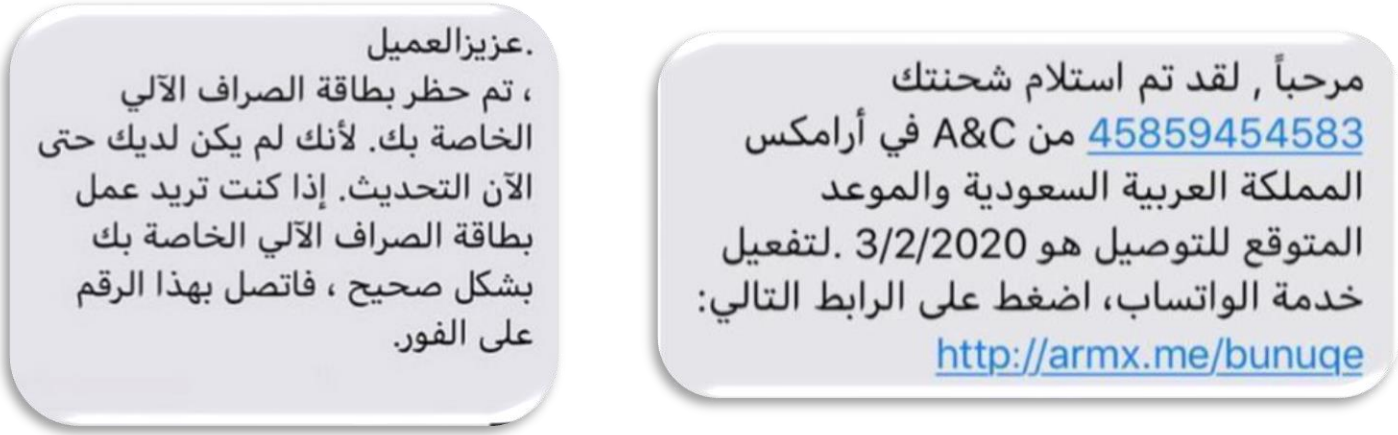
التهديد	الطرق	المؤشرات	التأثيرات الأولية
البرمجيات الضارة	التصيد، الإحتيال الإلكتروني الموجه، تزوير المواقع، خدمات المصادر المفنوحة، أجهزة التخزين التي يجري نقلها بين أجهزة الضحايا	النوافذ المنبثقة، تقارير الأخطاء، وسائط التخزين القابلة للإزالة، مرفقات البريد الإلكتروني، التطبيقات الغير معروفة المصدر، التنزيلات التلقائية، الشبكة المتدهورة أو العامة	تسمح برامج التجسس والبرمجيات الضارة على الأنظمة المتأثرة بالاستطلاع الالكتروني، والاستغلال، وإضعاف آداء النظام
تعطل نظم المعلومات أو حجب الطيف الكهرومغناطيسي	منع هوائيات القوات الصديقة من تلقي البيانات المرسلة عبر الطيف الكهرومغناطيسي عن طريق استخدام أجهزة ليزر عالية الطاقة وأجهزة الميكروويف عالية الطاقة، وأنظمة الاتصالات المُعدلة أو المُعاد تصميمها سواء العسكرية منها أو المتوفرة تجاريًّا	قد لا تكون الأعراض واضحة إذا كان الهجوم غير نشط؛ فقد تظهر على شكل تداخل في الإرسال أو عطل في البرامج أو الأجهزة، أو عدم القدرة على نقل البيانات	تدهور الخدمة أو حجبها بالكامل وعدم القدرة على التحكم في الطيف الكهرومغناطيسي مما يمنع وصول الخدمة ويُضعف التخطيط العملياتي

قدرات التهديد في الفضاء السيبراني

التهديد	الطرق	النتائج
التخريب	البرمجيات الخبيثة الإختراق إغراق الخادم بالطلبات	تعطل الخدمة تخريب الأجهزة تدمير البنية التحتية
سرقة البيانات وإستغلال الحسابات الشخصية	الإختراق الهندسة الاجتماعية التصيد الإلكتروني	الحصول على بيانات هامة، سرقة الأموال والحسابات، سرقة الهوية بهدف التحايل وإتمام عمليات باسم الضحية، سرقة العناوين والبريد الإلكتروني بهدف إستهداف الضحايا
التجسس	البرمجيات الخبيثة الإختراق	السيطرة الكاملة على الأجهزة، الإطلاع على البيانات الحساسة للضحايا والتجسس عليهم

التهديدات السيبرانية: الهندسة الإجتماعية

الهندسة الاجتماعية هي فن التلاعب بالمستخدمين وخداعهم بهدف الحصول على بيانات خاصة وحساسة لكشف معلوماتهم أو حساباتهم السرية دون علمهم وذلك بإستهداف نقاط الضعف، بناءً على إحصائيات سيسكو عام 2021م أثبتت أن 90% من جرائم إختراق المعلومات كانت ناتجة عن هجمات التصيد التي تتم عن طريق الهندسة الاجتماعية.



التهديدات السيبرانية: الهندسة الإجتماعية

الإحتيال بهدف الحصول
على المال

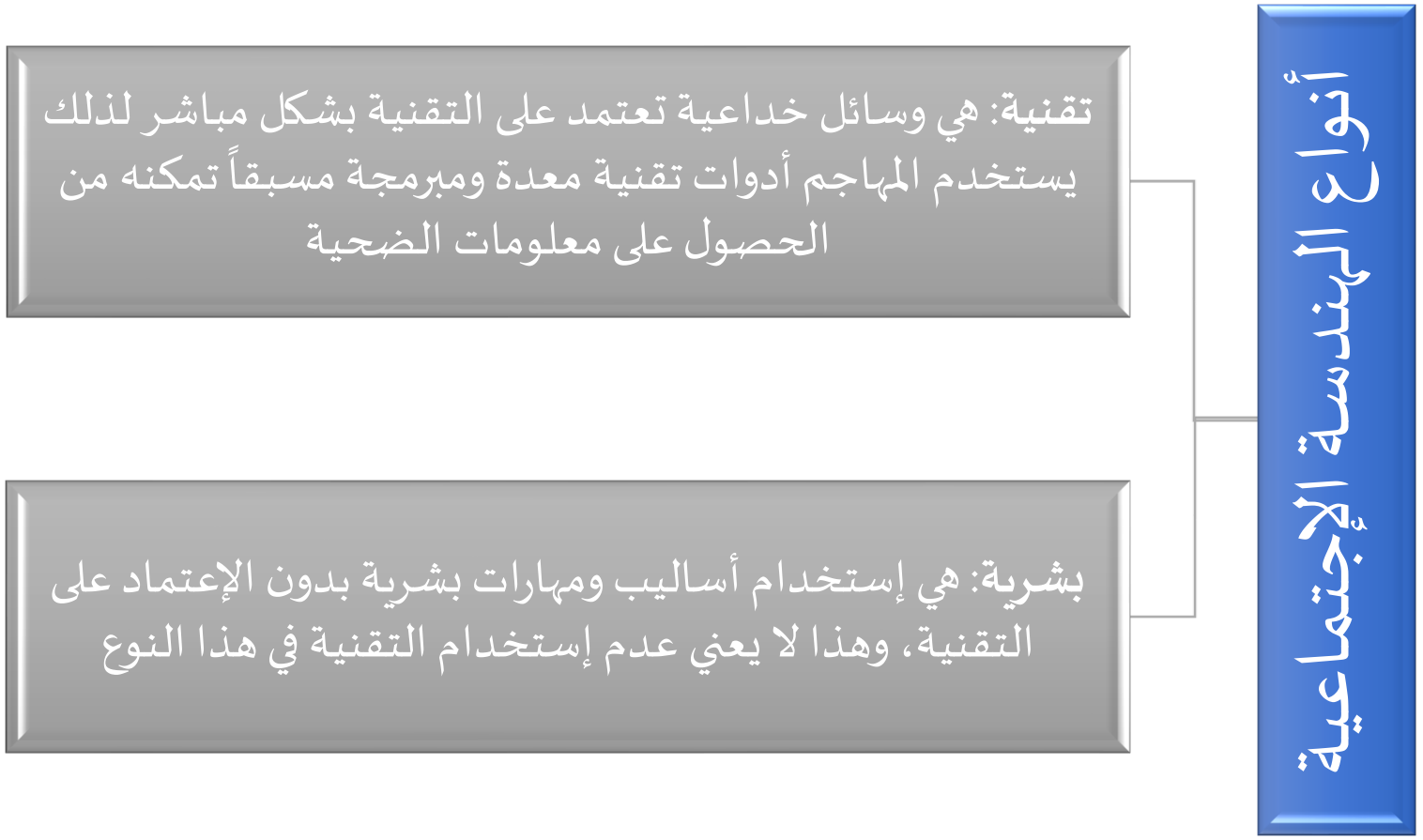
دفع المستخدم لزيارة
مواقع خبيثة

الحصول على كلمة المرور

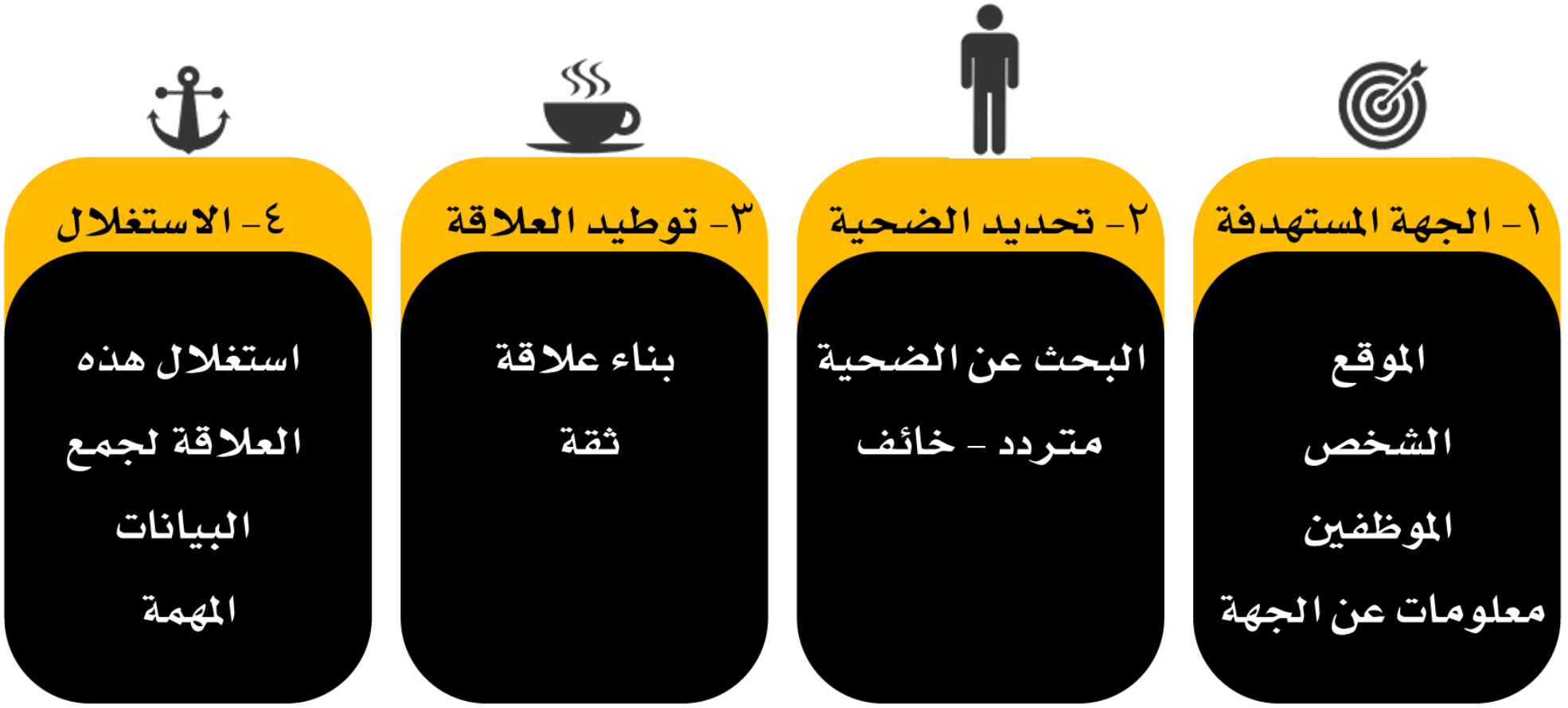
التظليل

إصابة جهاز الضحية

التهديدات السيبرانية: الهندسة الإجتماعية



التهديدات السيبرانية: مراحل الهندسة الإجتماعية



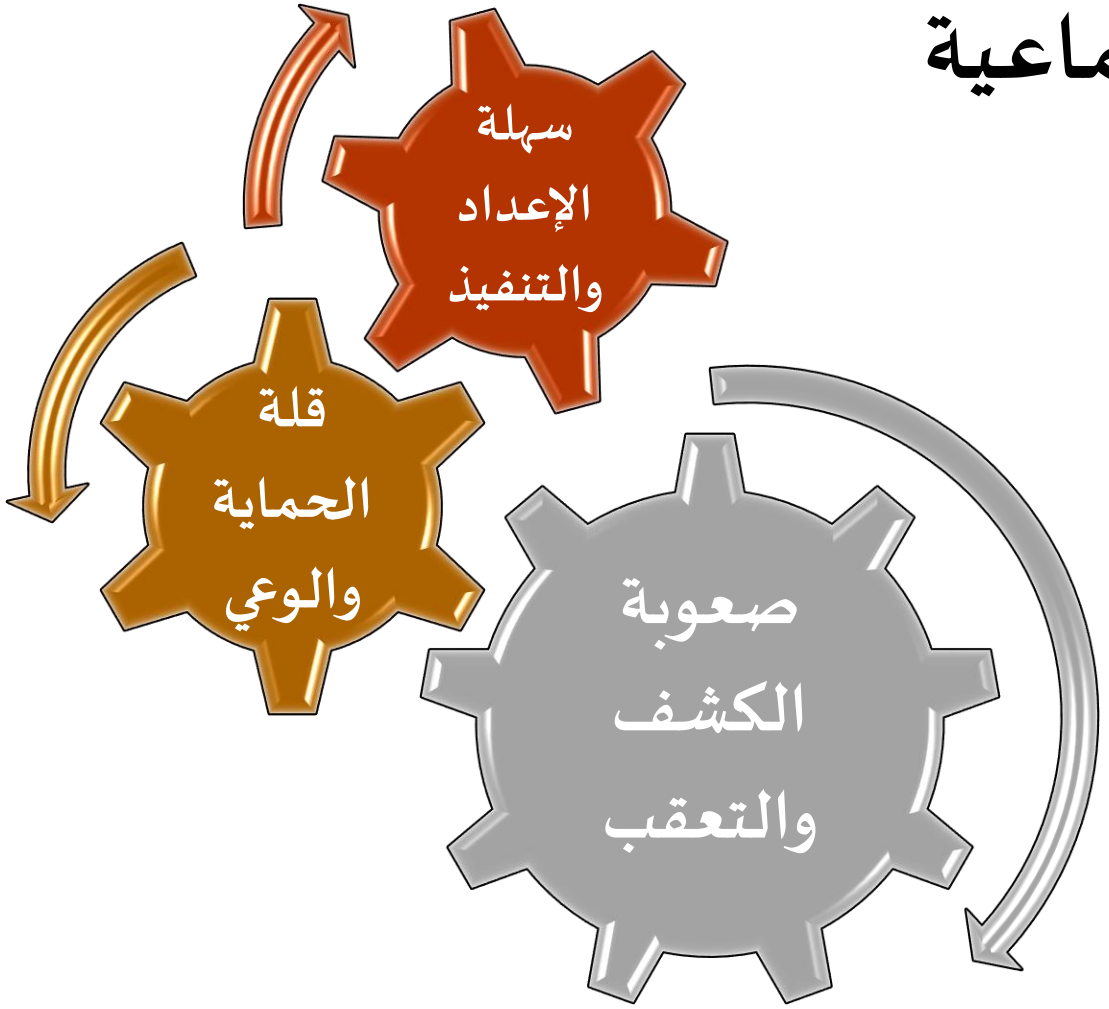
عصف ذهني

مما سبق
أذكر بعض الأساليب المتبعة
في الهندسة الاجتماعية؟

عصف ذهني

من وجهة نظرك
لماذا تنجح الهندسة
الاجتماعية؟

لماذا تنجح الهندسة الإجتماعية



التهديدات السيبرانية: التصيد الإلكتروني

التصيد الإلكتروني Phishing هو نوع من أنواع الجرائم الإلكترونية الأكثر إنتشاراً، كما يُعد أحد أساليب الإحتيال عبر الأنترنت وذلك لمحاولة الحصول على معلومات حساسة (شخصية أو مالية) عن طريق البريد الإلكتروني أو المواقع الإلكترونية وذلك من خلال التنكر ككيان جدير بالثقة.

التهديدات السيبرانية: التصيد الإلكتروني

يعتبر التصيد الإلكتروني من أهم عوامل التهديد لأكثر من 30% من المنشآت الصغيرة والمتوسطة.

يمكن استخدام التصيد الإلكتروني ضد موظفي المنشأة للوصول إلى أنظمة غير مصرح بها.

واحدة من كل 118 رسالة بريد إلكتروني في المملكة العربية السعودية هي رسالة تصيد إلكتروني.

عصف ذهني

من وجهة نظرك

كيف تحمي نفسك من التصيد الإلكتروني؟

التهديدات السيبرانية: التصيد الإلكتروني

لحمايتك من التصيّد الإلكتروني

حدّث جميع التطبيقات، وثبّت أدوات الحماية الموثوقة.

لا تفتح الرسائل أو الروابط أو الملفات المشبوهة ومجهولة المصدر.

تحقّق من الجهة قبل التصريح بأي معلومات شخصية.

احذر من زيارة المواقع المشبوهة وغير الموثوقة.

خصائص التهديد السيبراني

01 مدى الوصول

للتهديدات السيبرانية انتشاروتأثيرواسعي النطاق في جميع أنحاء العالم

02 تعددية الإستخدامات

التأثيرمتعدد الإستخدام القدرة على عكس نفسه، على سبيل المثال: قد يحقق الهجوم السيبراني غرضه، ثم يتم وقفه للسماح للطرف الآخربالجلوس إلى طاولة المفاوضات

03 التأثيرغيرالمتماثل

قد يكون للهجمات الفردية أوالتي تقف خلفها منظمات والتي تنفّذ باستخدام موارد كبيرة أوصغيرة تأثيراستراتيجيّ محدود أو كبيرمع التهديدات السيبرانية

خصائص التهديد السيبراني

04

حجب الهوية / الغزو / الإنكار

تزيد الهجمات مجهولة المصدر والهجمات غير المُسندة من حالة عدم اليقين، وربما تقلل الخطر السياسي وفرصة الانتقام. فإذا أنكر عدو معيّن هجومًا معيّنًا إنكارًا معقولًا، فمن الصعب أن إسناد الهجوم إلى بلدٍ معين أو جماعة إرهابية أو مخترق بعينه

05

التوقيت

وفقاً لإعتبارات الطرف الآخر يتم تحديد وقت التحضير للمهمة، كما أنه قد تكون التأثيرات فورية، محفزة أو متأخرة، بالإضافة إلى ان وتيرة العمليات تحتمل أن تكون عالية جداً أو تغيرها ثابت وفقاً للمعطيات

أنواع تهديدات الوصول

01 الوصول المادي

هو الوصول المباشر إلى أجهزة أو شبكة معينة، مثل: جهاز تخزين محمول USB بشكل مباشر على الأجهزة الحاسوبية

02 الوصول عن قرب

هو الوصول إلى أجهزة أو شبكة معينة عن طريق المنصات أو الأفراد أو المعدات التي تعمل داخل شبكة المنظمة، مثل: الوصول إلى جهاز متصل بشبكة المنظمة عن طريق WiFi

03 الوصول عن بعد

هو القدرة على الوصول إلى أجهزة أو شبكة معينة من مو اقع خارجية (مادية أو إفتراضية) يمكن إعتبارها خارج نطاق تلك الشبكة او المنظمة

فترة نقاش

ناقش أمثلة هجمات سيبر انية لها تأثير عسكري و إقتصادي؟

الهجوم السيبر اني: دراسة حالة

صراع روسيا – جورجيا عام 2008م

- هاجم مخترقون ناشطون من روسيا 38 موقعاً إلكترونياً عند إندلاع الحملة الروسية
- إستبدال محتوى موقع حكومي جورجي وإعادة توجيه الاتصالات
- تزامنت الهجمات السيبر انية مع هجوم بري روسي
- إرباك جميع المر افق الحكومية الجورجية

- تصدت جورجيا لذلك بإستخدام مو اقع غربية لإستضافة مو اقعها

الهجوم السيبراني: دراسة حالة

هجوم البرمجيات الضارة ضد أرامكو

- فيروس شمعون: أرامكو السعودية - تضرر أكثر من 35 الف جهاز
- سرقة صلاحيات الأجهزة والمنظمات
- تدمير البيانات في محرك الأقراص أو تشفيرها

أرامكو السعودية
Saudi Aramco

https://www.youtube.com/watch?v=q6289XVvRyc

فترة نقاش

هل قيادة طيران الأمن مستعدة للدفاع عن الهجمات السيبرانية بعد فيروس شمعون؟ من وجهة نظرك

عصف ذهني

ما هي نقاط ضعف الفضاء السيبراني؟

هل يمكن للتقدم التقني إحداث نقاط ضعف للفضاء السيبراني؟

ماذا يترتب على هذا ضمنياً للقادة العسكريين؟

نقاط ضعف الفضاء السيبراني

هي مواطن الضعف في نظام معين أو في تصميمه التي من خلالها تسمح بتنفيذ الأوامر والوصول إلى بيانات غير مصرح بها و / أو إجراء هجمات لحجب الخدمة، ومن الأمثلة عليها:

- العنصر البشري (المستخدم): مثل توافر البيانات الشخصية في منصات التواصل الاجتماعي (الهندسة الاجتماعية)
- أجهزة النظام وبرمجياته: مثل الوصول للبيانات الحساسة بالإعتماد على قواعد بيانات غير محمية
- أنظمة الاتصالات: مثل ضعف التحقق من الهوية وإدارة جلسة الإتصال
- السياسات والإجراءات المستخدمة في الأنظمة: مثل سوء تهيئة الإعدادات الأمنية بإستخدام برامج غير محدثة

عصف ذهني

كيف يمكن للقطاع العسكري الحد من نقاط الضعف في الفضاء السيبراني (سوء تهيئة الإعدادات الأمنية) من وجهة نظرك

نقاط ضعف: سوء تهيئة الإعدادات الأمنية

سوء تهيئة الإعدادات الأمنية هو أكثر نقطة ضعف شيوعًا وخطورة، من الأمثلة النموذجية على عيوب سوء تهيئة الإعدادات الأمنية ما يلي:

- إستخدام البرمجيات الغير محدثة والقديمة
- التطبيقات والمنتجات التي تعمل في وضع التصحيح
- إضافة وتشغيل الخدمات الغير ضرورية على الأنظمة
- السماح بالوصول إلى مصادر الخوادم Servers والخدمات التي يمكن أن تؤدي إلى الكشف عن المعلومات الحساسة أو التي تسمح للمهاجم بالإختراق
- عدم تغيير إعدادات المصنع (مثل كلمة المرور الإفتراضية)، وعدم تغيير كلمات المرور بشكل منتظم
- إستخدام الحسابات الإفتراضية

عصف ذهني

كيف يمكن للقطاع العسكري التقليل من قابلية التعرض للتهديدات الداخلية؟

التدابير الوقائية للفضاء السيبراني

- تطوير السياسات والإجراءات الأمنية بشكل مستمر
- توفير برامج تعليمية وتدريبية مخصصة لمجال الأمن السيبراني
- تزويد المستخدمين بإرشادات إستخدام الشبكة
- التدقيق والإمتثال وإدارة مخاطر الفضاء السيبراني
- تطوير وإتاحة الإجراءات التقنية

عصف ذهني

هل الهجمات السيبرانية تُعد أعمال حرب سيبرانية؟

هل الحرب السيبرانية حرباً حقيقة؟

هل مواقع التواصل الاجتماعي التي تؤثر في المعايير الاجتماعية أو تدمرها تُعد أسلحة سيبرانية؟

الحروب السيبرانية

يعرفها القانون الدولي بأنها "جميع العمليات السيبرانية سواء كانت دفاعية أو هجومية، والتي يعتقد بأنها تسبب إصابات أو وفيات بشرية، أو تلف وضرر للمكونات المادية أو الأنظمة أو التجسس والوصول الغير مصرح به للبيانات الحساسة"

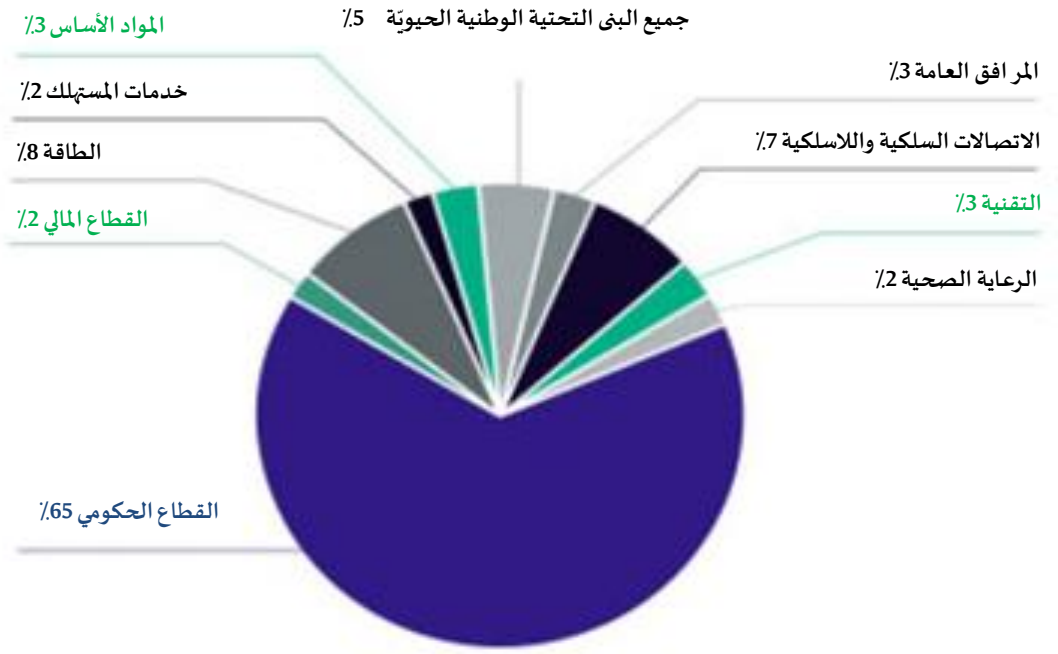
لذلك الذي يبرر الحرب القانونية هو تقييم أثر الهجمات السيبرانية في العالم المادي:

- التدمير والضرر والوفيات البشرية
- قابلية قياس أثر الهجمات السيبرانية
- البُعد السياسي من الهجمات السيبرانية

الحرب السيبر انية: المملكة العربية السعودية

"تلعب المملكة دوراً حاسمًا في الحفاظ على الأمن والاستقرار في المنطقة بسبب أهميتها الاقتصادية، والسياسية، والثقافية، وكذلك بسبب موقعها الاستراتيجي"

القطاعات المستهدفة



- **كيف يمكنك إستخدام هذه المعلومات شخصياً في الوحدة التي تنتمي لها في قيادة طيران الأمن؟**
- **ما هي التغييرات التي تحتاجها قيادة طيران الأمن للتحصير للحرب السيبر انية؟**

الحرب السيبرانية: التكامل

"لن تنتظر حتى تصبح المعركة في السعودية"

ولي العهد

العمل الموحد: في الفضاء السيبراني نقاط الضعف المكشوفة والعلاقات المتبادلة المعقدة بين الشبكات الوطنية والعالمية تتطلب وجود عمل منسق بين الكيانات الحكومية الأخرى على كافة المستويات

التعاون بين الوكالات: يجب أن يعمل القطاع العسكري مع شركائه في الجهات الحكومية والقطاع الخاص والدول المتحالفة والمشاركة من أجل ردع وصد أي هجوم سيبراني له أثار على المصالح الوطنية

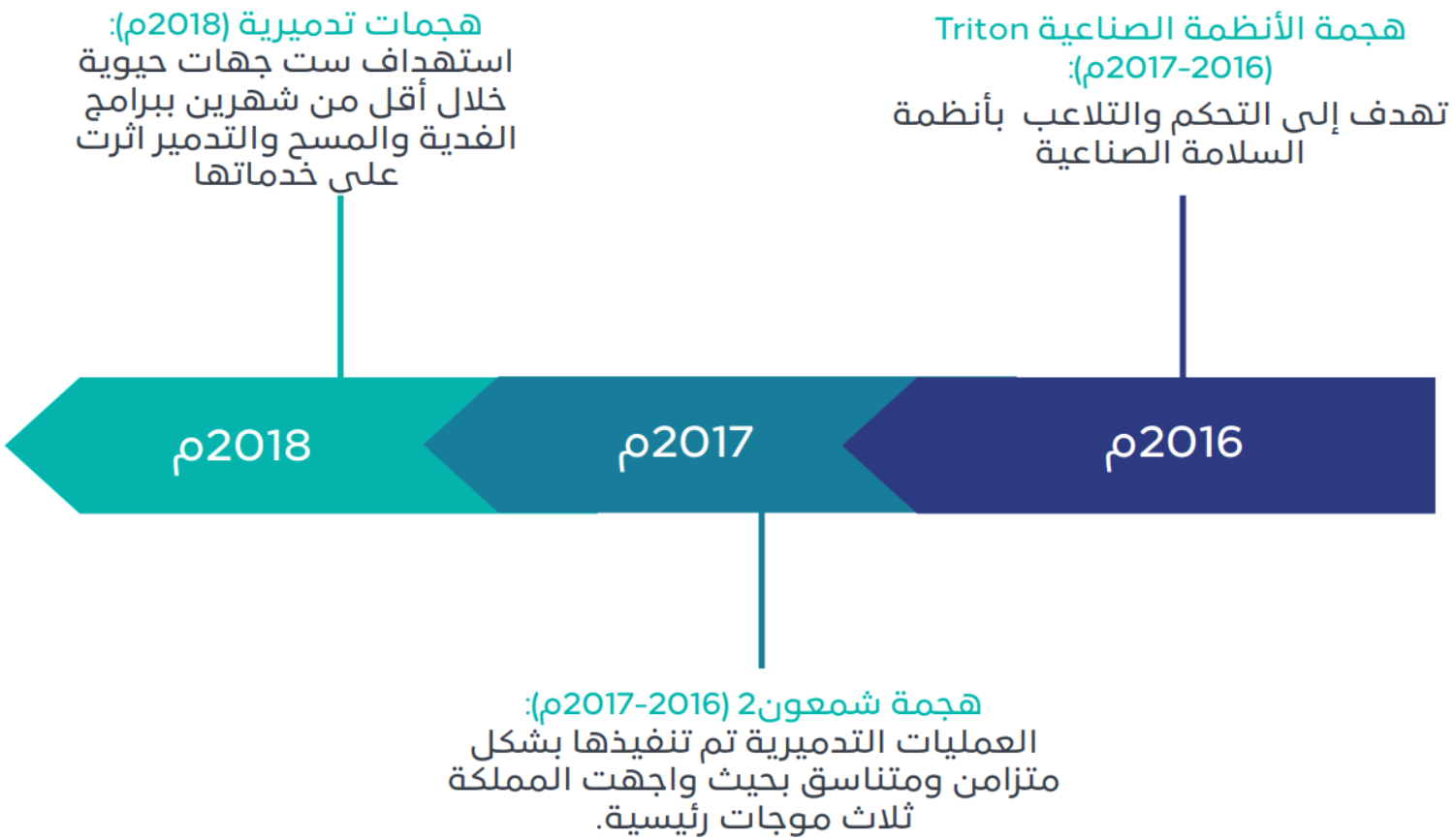
إجراءات الفضاء السيبراني لتحقيق الأثر في القطاع العسكري

- التعرف على أساسيات ومفاهيم الحوكمة وإدارة المخاطر والإمتثال في الأمن السيبراني
- التعرف على مكونات الحوكمة وإدارة المخاطر والإمتثال
- التعرف على إستراتيجية إدارة المخاطر الأمنية
- التعرف على طرق تعزيز الأداء المنضبط
- التعرف على كيفية إستعراض ضوابط ومعايير الهيئة الوطنية للأمن السيبراني

عصف ذهني

إستعرض مجموعة من الأمثلة على هجمات سيبرانية على المملكة العربية السعودية؟

المملكة العربية السعودية والأمن السيبراني



المملكة العربية السعودية والأمن السيبراني: قمة العشرين

إن مجموعة العشرين عبارة عن منتدى دولي يجمع أكبر اقتصادات العالم، وتمثل الدول الأعضاء في المجموعة أكثر من 80% من الناتج المحلي الإجمالي العالمي و75% من حجم التجارة العالمية و60% من التعداد السكاني العالمي. وبالنظر إلى مستوى الأطراف المشاركة ودرجة أهميتها، فضلاً عن الطبيعة الرقمية للتواصل، تبرز الأهمية الكبيرة لتعزيز الأمن السيبراني خلال رئاسة مجموعة العشرين.

حصلت المملكة العربية السعودية على المرتبة **الأولى** بين الدول العربية في مؤشر الأمن السيبراني العالمي (GCI) لعام 2020م والمرتبة **الثانية** عالمياً بين 194 دولة.

المملكة العربية السعودية والأمن السيبراني : قمة العشرين

المملكة العربية السعودية والأمن السيبراني: قمة العشرين

المملكة العربية السعودية والأمن السيبراني: قمة العشرين

المملكة العربية السعودية والأمن السيبراني: قمة العشرين

المملكة العربية السعودية والأمن السيبراني: قمة العشرين

مكونات برنامج صمود الأمن السيبراني قمة العشرين

المملكة العربية السعودية والأمن السيبراني: المبادئ الثلاثة

1

أولاً، **الشمولية**، وينطوي ذلك على تحديد الجهات المعنية الرئيسية المشاركة في استقبال المشاركين واستضافتهم ونقلهم وحمايتهم. ويشمل ذلك إنشاء إدارة للأمن السيبراني داخل الأمانة السعودية لمجموعة العشرين.

2

ثانيًا، **الصمود**، وتم الاسترشاد فيه بتحليل مدى تعقيد المجال السيبراني وتحديات الأمن السيبراني لتأمين رئاسة مجموعة العشرين. وقد أتاح هذا التحليل إعداد نموذج يعتمد على سبل الحماية التي تتسم بالصمود والموثوقية والقدرة على التحذير من التهديدات السيبرانية والاستجابة لها، مع العمل في الوقت نفسه على اكتشاف الثغرات السيبرانية ومعالجتها في مرحلة مبكرة. كذلك، أطلقت حملات لتوعية جميع الجهات المعنية بهدف تعزيز ثقافة الأمن السيبراني طوال سنة رئاسة مجموعة العشرين وخلال قمة القادة.

المملكة العربية السعودية والأمن السيبراني: المبادئ الثلاثة

3

ثالثًا، **التعاون**، وقد تضمّن ذلك الربط بين منظومة معقدة تتكون من الجهات العامة والخاصة على الصعيدين الوطني والدولي. وقد أثمرت الشراكات الناتجة عن تعزيز الثقة بين جميع الجهات وتمكين النموذج من تحقيق مستويات عالية من المشاركة. كما كان التكامل بين الهيئة وذراعها التقني، الشركة السعودية لتقنية المعلومات (سايت)، من أهم العوامل التي ساهمت في نجاح النموذج.

شكراً لإستماعكم وتفاعلكم

- فترة الأسئلة -