دورة تدريبية

حوكمة الأمن السيبراني

د. غالب الشمري

أستاذ الذكاء الإصطناعي وعلم البيانات المساعد

جامعة الملك سعود

حوكمة الأمن السيبراني

الأمن السيبراني

ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية التي تهدف الى الوصول للمعلومات الحساسة أو تغييرها أو إتلافها تسمى بالأمن السيبراني.

أساسيات ومفاهيم الحوكمة

مجموعة السياسات أو القواعد أو الأطر التي تستخدمها الجهة لتحقيق أهداف أعمالها. وهي تحدد مسؤوليات أصحاب المصلحة الرئيسيين، مثل مجلس الإدارة والإدارة العليا.

ضوابط ومعايير الهيئة

أصدرت الهيئة ضوابط وأطر وإرشادات ذات العلاقة بالأمن السيبراني على المستوى الوطني بهدف تعزيز الأمن السيبراني في المملكة حمايةً للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية.

أساسيات GRC

تأهيل ورفع كفاءة العاملين في مجالات الحوكمة وإدارات المخاطر والالتزام والتدقيق والمراجعة الداخلية بكافة أنواعها طبقاً للمعايير العالمية و أفضل الممارسات في حوكمة الجهات،

Teamwork

حوكمة الأمن السيبراني

Ghalib Alshammri, PhD
Artificial Intelligence &
Nano-Network
Communication

https://github.com/galshammri/GRC

About Me

Personal Profile

Ghalib Alshammri, Ph.D.
Assistant Professor at KSU
Teaching Assistant at Stevens Institute of Technology, USA

Work Experience

Assistant Professor in Artificial Intelligence and Nano Communication Networks Consultant @ SEU

Achievements

- 20 Research Publications.
- Talk at Bell Works, NJ USA
- 1 Textbook.
- 1 Provisional Patent.
- Peer-Reviewer in more than 10 IEEE Journals.
- Invited Speaker.
- Grants.

Skills & Languages

Programming
Researcher
Problem-Solving
Leadership
Management skills
Transferable skills

Arabic
English

Education

Ph.D. in Computer Engineering, AI
M. Sc. in Intelligent Systems
B.Ed. in Computer Science

Interesting Area

AI, IoT, Molecular Nano Communication Networks, Unmanned Aerial Vehicles, …, etc.

Contact Info

King Saud University – Community College
Computer Science Department
Building (4), Floor (6), Office (11)

Social Media

LINKEDIN

https://www.linkedin.com/in/ghalib-alshammri-ph-d-3b8aa497/

TWITTER

https://twitter.com/GAlshammri_PhD

EMAILS

galshammri@ksu.edu.sa
galshammri.phd@gmail.com

publons https://publons.com/researcher/2116669/ghalib-alshammri/

ORCID https://orcid.org/0000-0001-9911-2632

WEB OF SCIENCE RESEARCHERID: G-9277-2017

Our Vision

Vision

Our training course seeks to be a world-leading interdisciplinary training course with a focus on innovation in GRC, evidence-driven decision-making development, education and services in the specific broad-based governance areas and domains.

Mission

- To advance the state-of-the-art in GRC;
- To transform all fields, professions, and sectors through the application of GRC;
- To ensure the responsible use of GRC to benefit society.

Goal

- Training and mentoring employees for cyber security governance and GRC program.

محتويات الدورة التدريبية:

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

إستبانة عن حوكمة الأمن السيبراني

- المستوى الوظيفي
- المستوى التعليمي
- التخصص
- أهمية الوعي بالأمن السيبراني
- المستوى المهني

https://forms.gle/LN27P7JcskMtUypB9

قبل الانطلاق

فترة نقـــاش

من وجهة نظرك
ما هي أكثرعناصرومجالات
التقنية أهمية؟
تلعب دوراً مهماً في موازين القوى

الذكاء الإصطناعي وعلم البيانات
والتقنيات الناشئة

أمن المعلومات والأمن
السيبر اني وحوكمتها

إدارة البيانات والمكونات المادية

علم الاتصالات
والشبكات

البيانات والمعلومات
والمكونات المادية

دورة تدريبية: حوكمة الأمن السيبراني

مقدمة عن الأمن السيبراني

المحاضرة الأولى

د. غالب الشمري

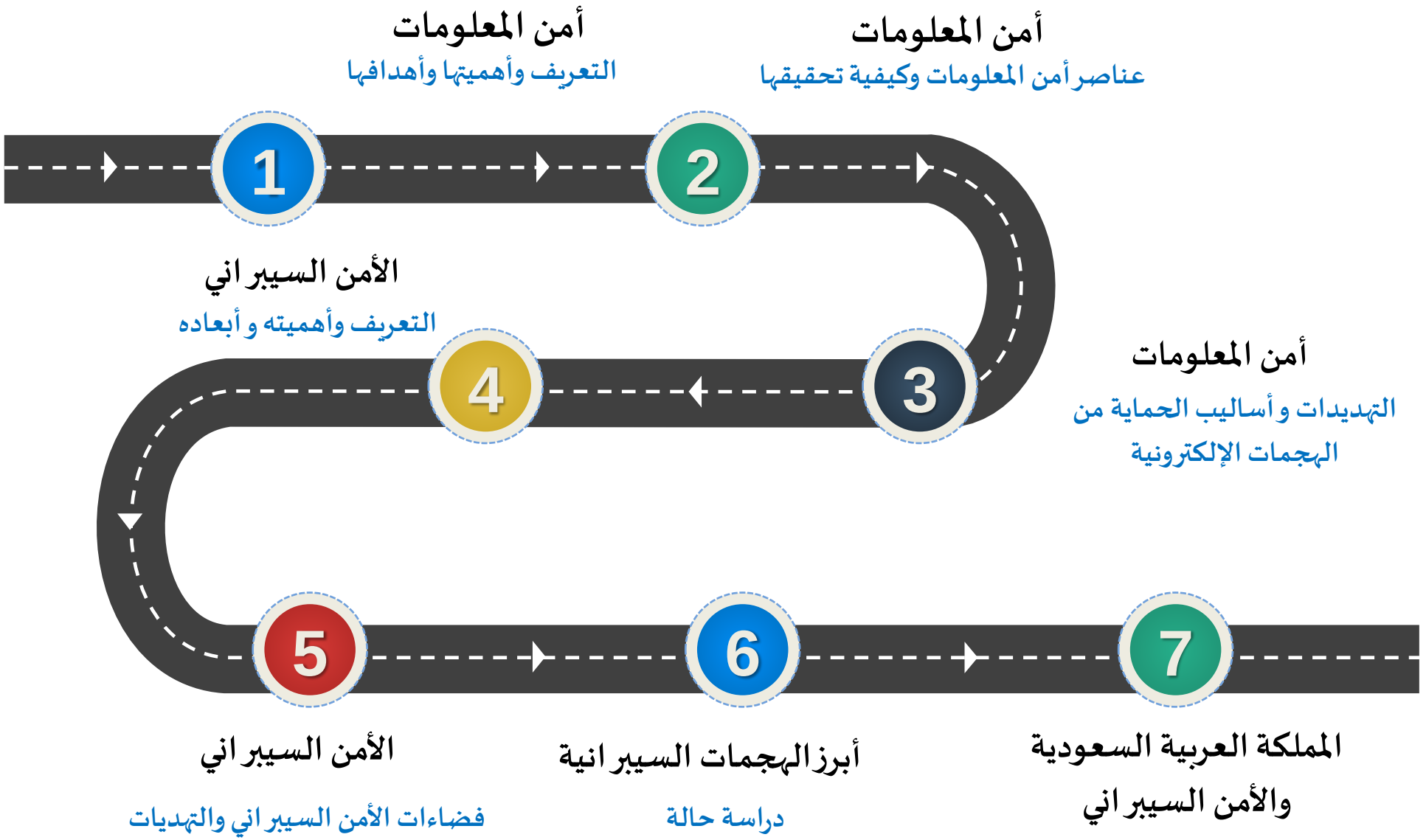
أستاذ الذكاء الإصطناعي وعلم البيانات المساعد

جامعة الملك سعود

محتويات المحاضرة الأولى:

- التعرف على أمن المعلومات وأهميتها وأهدافها
- التعرف على عناصر أمن المعلومات وكيفية تحقيقها
- التعرف على أشهر التهديدات على أنظمة أمن المعلومات
- التعرف على أساليب الحماية من الهجمات الإلكترونية
- التعرف على الأمن السيبراني وأهميته و أبعاده
- التعرف على فضاءات الأمن السيبراني والتهديات
- أبرز الهجمات السيبرانية: دراسة حالة
- المملكة العربية السعودية والأمن السيبراني: دراسة حالة

خارطة الطريق



عصف ذهني

هل تعرضت لعملية إحتيال إلكترونية أو سمعت عن عملية إحتيال إلكترونية؟

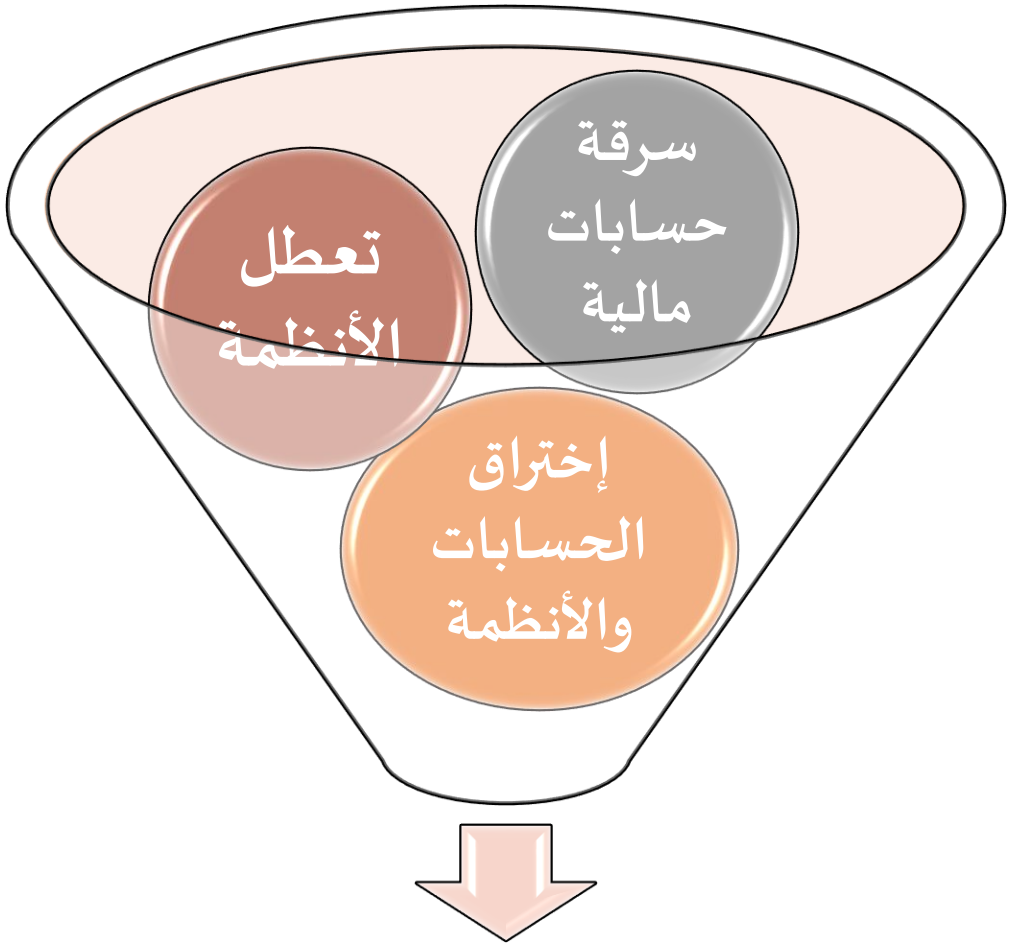
سرقة مبالغ مالية

أضرار مادية (مثل: الأجهزة وغيرها)

سرقة حسابات إجتماعية و إبتزاز

عصف ذهني


10 min


سرقة حسابات مالية
تعطل الأنظمة
إختراق الحسابات والأنظمة
أمن المعلومات

فترة نقـــاش

من وجهة نظرك مما سبق

ما المقصود بمفهوم
علم أمن المعلومات؟

مفهوم أمن المعلومات

أمن المعلومات هو مجموعة من الإجراءات والتدابير الوقائية التي تُستخدم للمحافظة على المعلومات وسريتها والمحافظة عليها من السرقة والإختراق. لذلك المقصود بعلم أمن المعلومات هو العلم الذي يبحث في نظريات وأساليب حماية البيانات والمعلومات ووضع الأدوات والإجراءات اللازمة لضمان حمايتها، يمكن لمفهوم أمن المعلومات أن يشمل المحاور التالية:

- حماية المعلومات من الضرر بمختلف أشكاله
- حماية المعلومات من الوصول الغير مصرح به أو السرقة أو سوء الإستخدام
- حماية قدرة المنشأة على أداء أعمالها بطريقة أمنة
- تمكين أنظمة تقنية المعلومات والبرامج من العمل بشكل آمن ومستمر

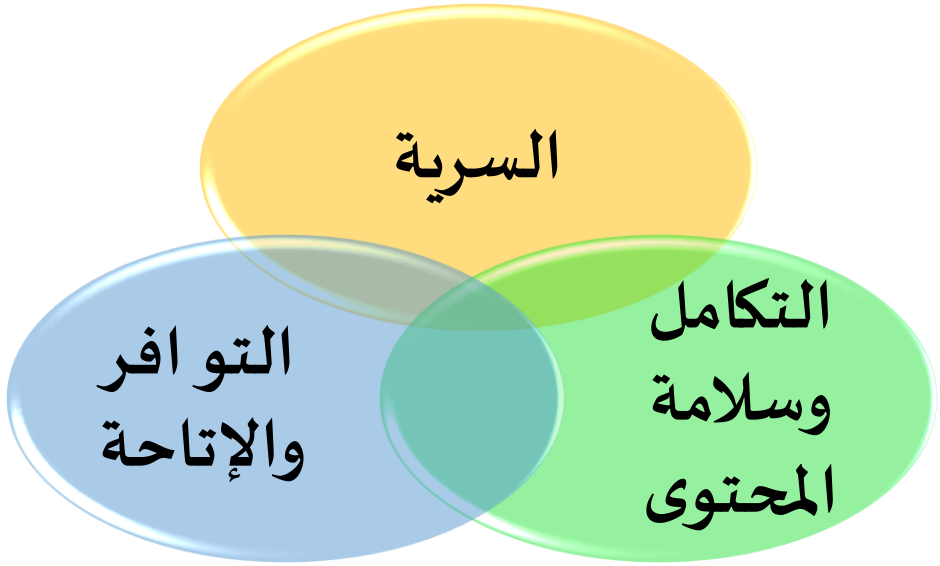
أهداف أمن المعلومات

يسعى أمن المعلومات إلى تحقيق مجموعة من الأهداف، منها:

- تطوير السياسات والإجراءات الأمنية اللازمة
- معالجة الأخطاء أثناء تصميم وبناء وتشغيل الأنظمة
- منع سرقة وإختراق الأنظمة
- الحفاظ على المعلومات من التلف أو أخطاء المستخدم أو البرمجية
- حماية الأصول Information Assets

عناصر أمن المعلومات

تختلف أهمية وأمان المعلومة حسب طبيعتها وأهميتها والبيئة التي تحفظ فيها والوسائل التي تنقل بها. تعرف عناصر أمن المعلومات بأنها مجموعة العناصر الواجب توافرها لحماية المعلومات بحيث يغطي كل عنصر من هذه العناصر جانباً من جوانب الحماية المطلوبة، وللمحافظة على أمن البيانات والمعلومات في الأنظمة يجب أن تتوفر ثلاثة عناصر أساسية:



فترة نقـــاش

من وجهة نظرك

ما هي السرية، التكامل
وسلامة المحتوى، والإتاحة؟

السـرية Confidentiality

الوصول إلى المعلومات للأشخاص المصرح لهم فقط سواءً عند تخزينها أو معالجتها أو نقلها عبر وسائل الإتصال وكذلك تحديد صلاحية التعديل والحذف والإضافة.

التكامل وسلامة المحتوى Integrity

المقصود بها أن تكون المعلومة صحيحة عند إدخالها وكذلك أثناء تنقلها بين الأجهزة في الشبكة والتأكد أنه لم تتعرض إلى أي نوع من التعديل والتحقق منها بإستخدام مجموعة من المنهجيات.

التو افروالإتاحة Availability

تعني بقاء المعلومات متوفرة للمستخدم وإمكانية الوصول إليها في أي وقت وعدم تعطل ذلك نتيجة لخلل في أنظمة إدراة قواعد المعلومات أو وسائل الإتصال

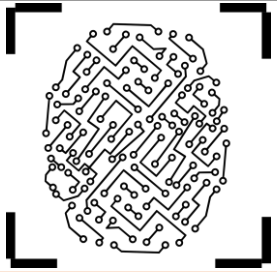
فترة نقـــاش

من وجهة نظرك

ما هي الطرق الممكنة لتحقيق عناصر أمن المعلومات؟

كيفية تحقيق عناصر أمن المعلومات

التشفير Encryption	التصديق الرقمي Digital Authentication
التشفير هو تحويل البيانات الواضحة إلى بيانات غير واضحة بطريقة يستطيع من خلالها كلا الطرفين فك هذه الشفرات. التشفير هو عملية من خلالها يتم تغيير البيانات في شكل غير مفهوم بحيث لا يستطيع إعادتها إلى طبيعتها الإ الأشخاص المصرح لهم بذلك ويتكون من عمليتين التشفير Encryption وفك التشفير Decryption	هو أحد أهم أدوات أمن المعلومات التي تستخدم في التحقق من البيانات وصدورها من جهة موثوقة ويعتمد التصديق الرقمي على نظام تشفير يتكون من عمليتين أساسية هي التوقيع Digital Signature وعملية التحقق من صحة التوقيع Signature Verification. كما أنه يطلق عليه أيضاً التوقيع الإلكتروني



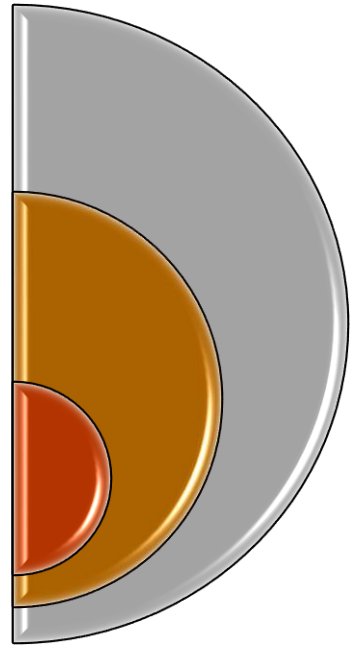
فترة نقـــاش

من وجهة نظرك

ما أنواع التهديدات المكنة
على أنظمة أمن المعلومات؟

تهديدات أنظمة أمن المعلومات

هناك العديد من التهديدات التي تحيط بأنظمة المعلومات، تتعدد وتتنوع بتنوع هياكل الأنظمة المعلوماتية ونقاط الضعف فيها. يمكن تقسيم تهديدات أمن المعلومات إلى ثلاثة فئات رئيسية:



تهديدات بشرية

- إتلاف المعلومات أو تسريبها خارجياً
- الوصول الغير مصرح به للمعلومات

تهديدات فنية

- عيوب في التصميم والتصنيع
- عيوب في التشغيل وتشتت المعلومات

تهديدات طبيعية

- الكوارث الطبيعية مثل الزلازل
- الحرائق

فترة نقـــاش

من وجهة نظرك

لماذا يتم دراسة وتحليل وتحديد تهديدات الأنظمة المعلوماتية بشكل مسبق؟

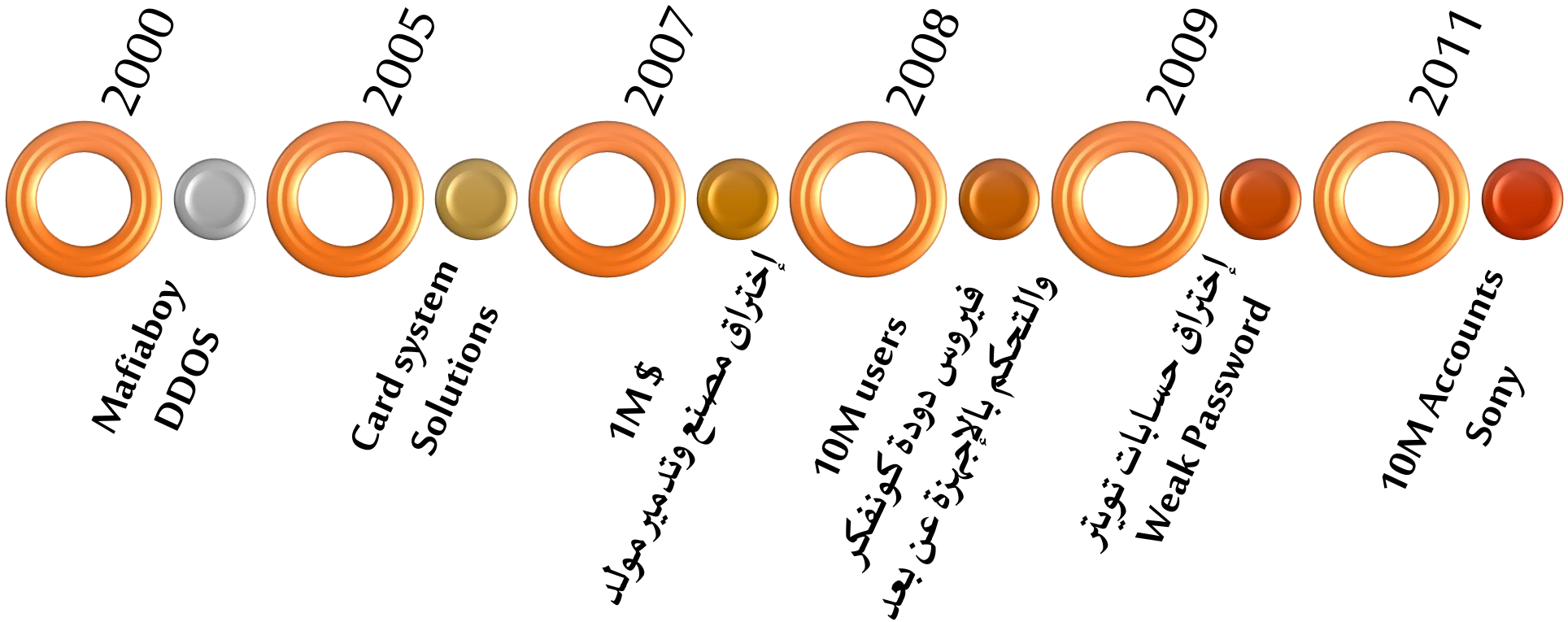
الهجمات الإلكترونية

تُشكل المعلومات في عصرنا الحالي جزء مهم في حياة الفرد والشركات والقطاعات والدول، لكن يحيطها الكثير من المخاطر والأعداء، لذلك يجب حمايتها على الصعيد الشخصي والمؤسسي وتطوير وسائل تقنية حديثة ذكية لمواجهة الهجمات الإلكترونية. يُعد الهدف الرئيسي من الهجمات الإلكترونية هو تعطيل الخدمة أو التجسس بمختلف أنواعه على المستخدمين والمؤسسات أو تدمير الأجهزة والبيانات. لذلك يجب على القطاعات رفع الجاهزية القصوى لكشف الهجمات الإلكترونية قبل وقوعها وتحديد مصدرها وحماية منشأتها بحيث لا تتأثر بعامل المكان والزمان. ومن هذه الهجمات ما يلي:

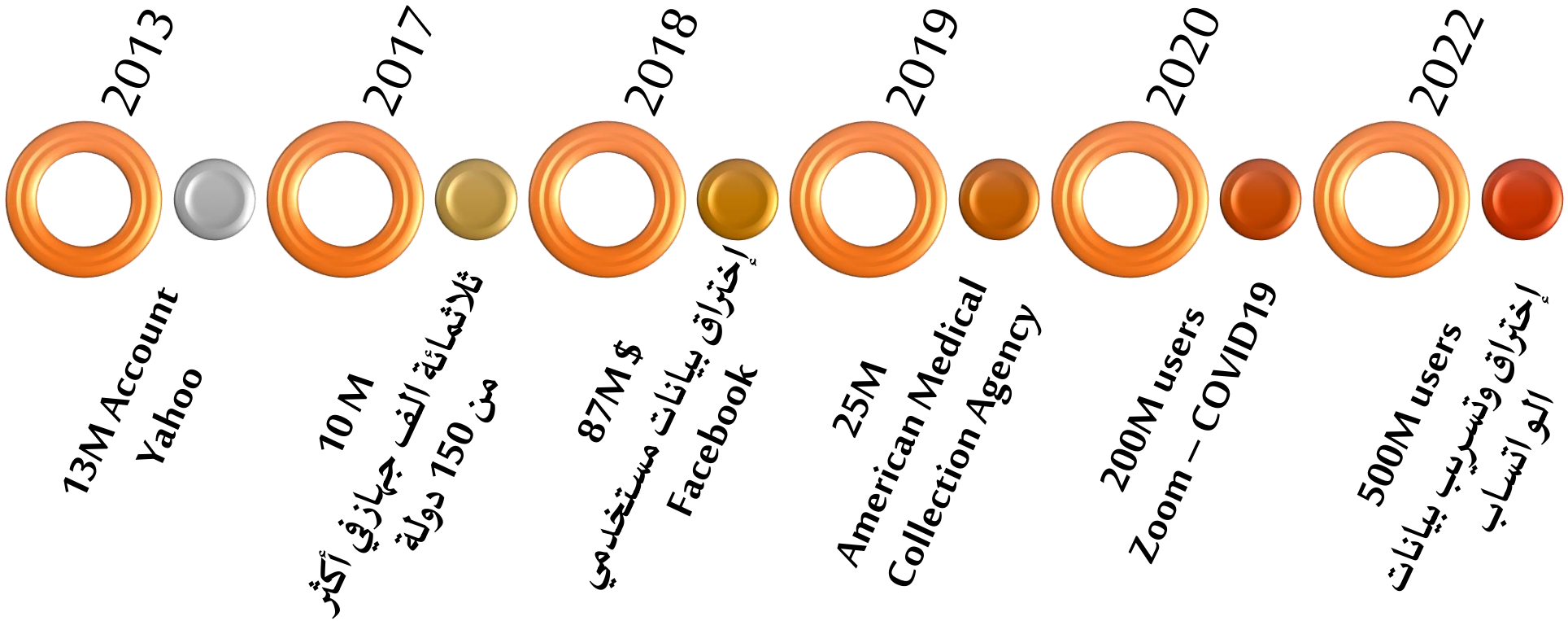
عصف ذهني

أذكر أمثلة على هجمات أمنية تقنية شائعة؟

نظرة تاريخية الهجمات الإلكترونية



نظرة تاريخية الهجمات الإلكترونية



مفهوم الأمن السيبراني Cybersecurity

الأمن السيبراني مشتقة من كلمة (Cyber Security) وكلمة سيبر لاتينية الأصل ومعناها الفضاء المعلوماتي فيصبح المقصود بالأمن السيبراني هو أمن الفضاء المعلوماتي ويعتبر أشمل وأعم من أمن المعلومات. لذا يمكن القول أن الأمن السيبراني هو عبارة عن مجموع الوسائل التقنية والإدارية التي يتم إستخدامها لمنع الإستخدام غير مصرح به وسوء الإستغلال واستعادة المعلومات الإلكترونية ونظم الإتصالات والمعلومات التي تحتويها بهدف ضمان توافر و إستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية ولحماية الموطنين. يشمل الأمن السيبراني أمن المعلومات على أجهزة وشبكات الحاسب الآلي، بما في ذلك العمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو إتالف قد يحدث. لقد أصبح الأمن السيبراني ركيزة أساسية في كل المنظمات والمؤسسات بل وحتى الدول لموجهة الحروب الإلكترونية.

عصف ذهني

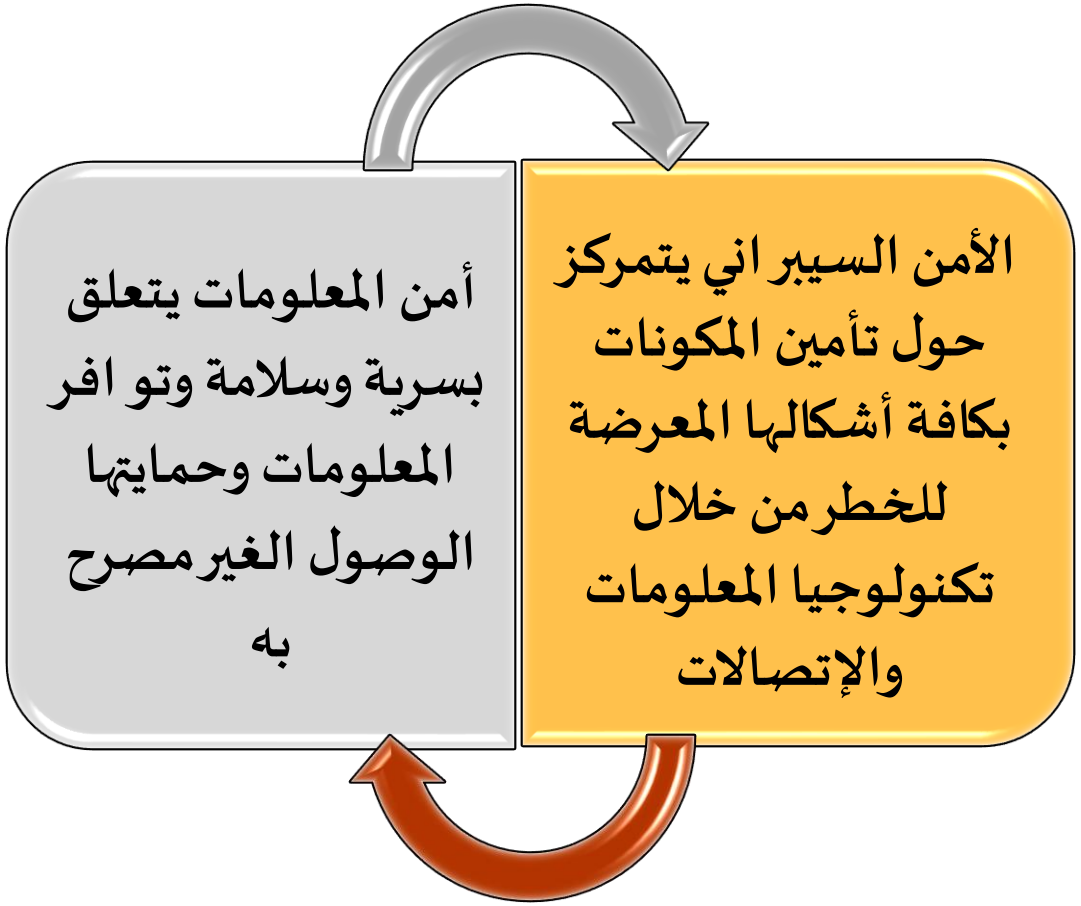
مما سبق
ما هو مفهوم
الأمن السيبراني؟

مفهوم الأمن السيبراني Cybersecurity

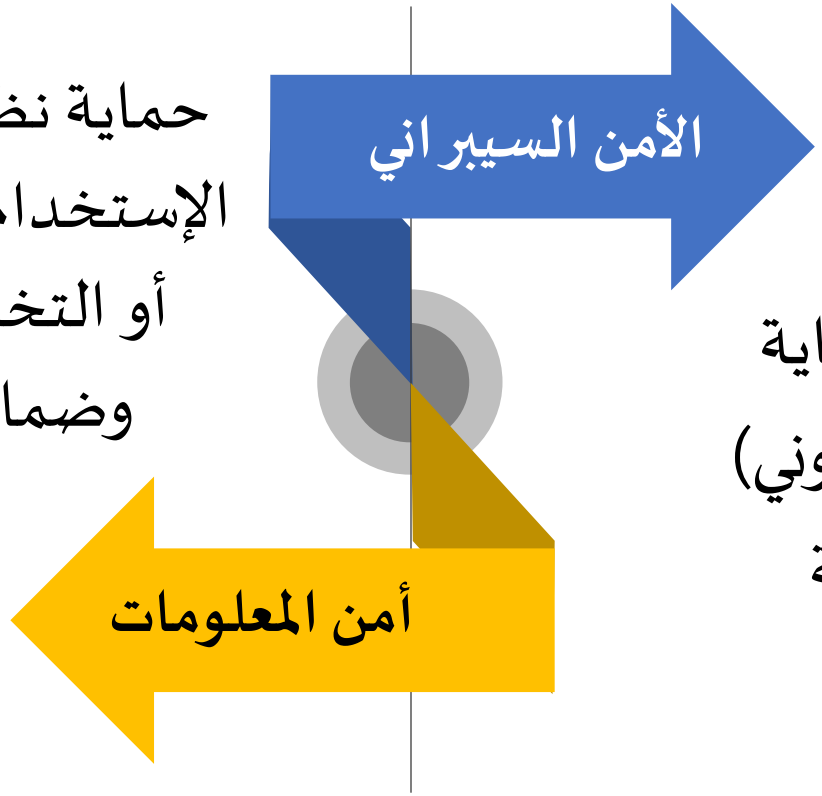
"هو ممارسة الدفاع عن الأجهزة بكافة أشكالها، والأنظمة الإلكترونية، والشبكات، والبيانات وما يتكون منه نظام الاتصالات بشكل كامل من الهجمات الضارة والوصول الغير مصرح به"

الأمن السيبراني وأمن المعلومات

الأمن السيبراني يأخذ بعين الإعتبار أيضاً حماية مواقع تخزين البيانات والتقنيات المستخدمة لتأمينها. بالإضافة إلى حماية تكنولوجيا المعلومات والإتصالات (المكونات المادية والبرمجية) مما يعرف بأمن تكنولوجيا المعلومات والإتصالات.



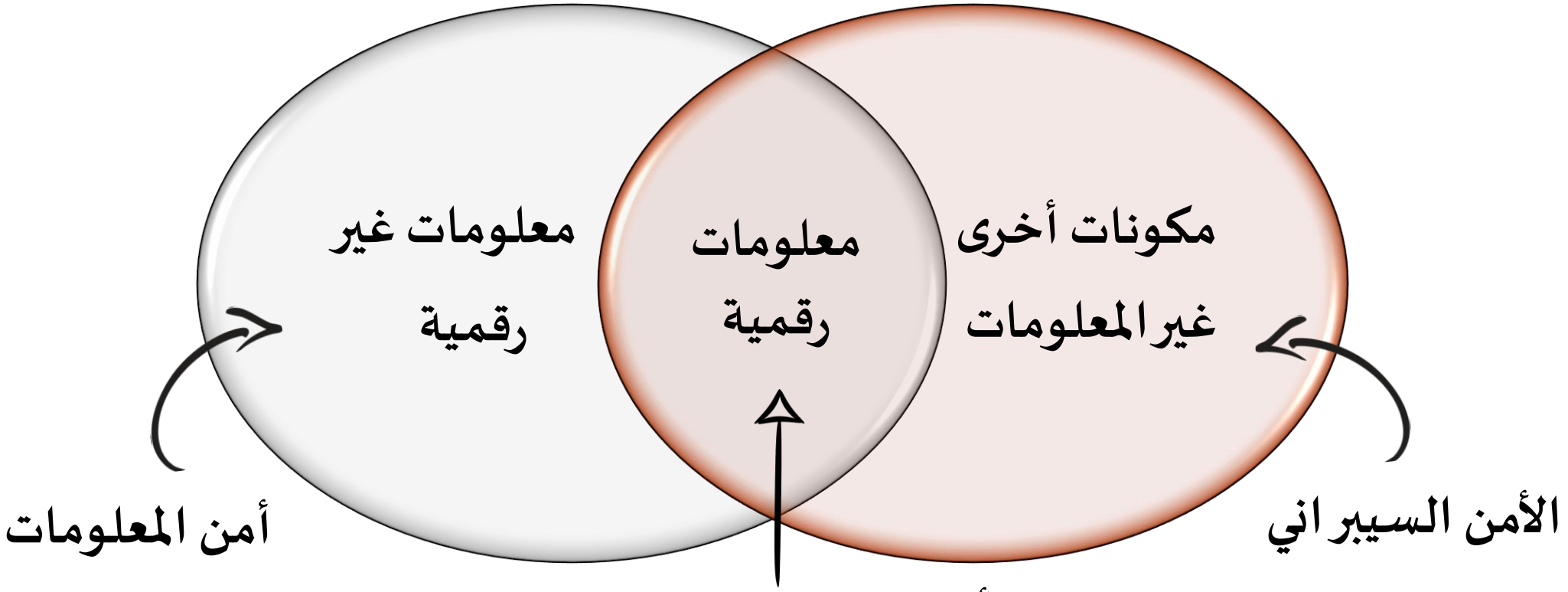
الأمن السيبراني و أمن المعلومات



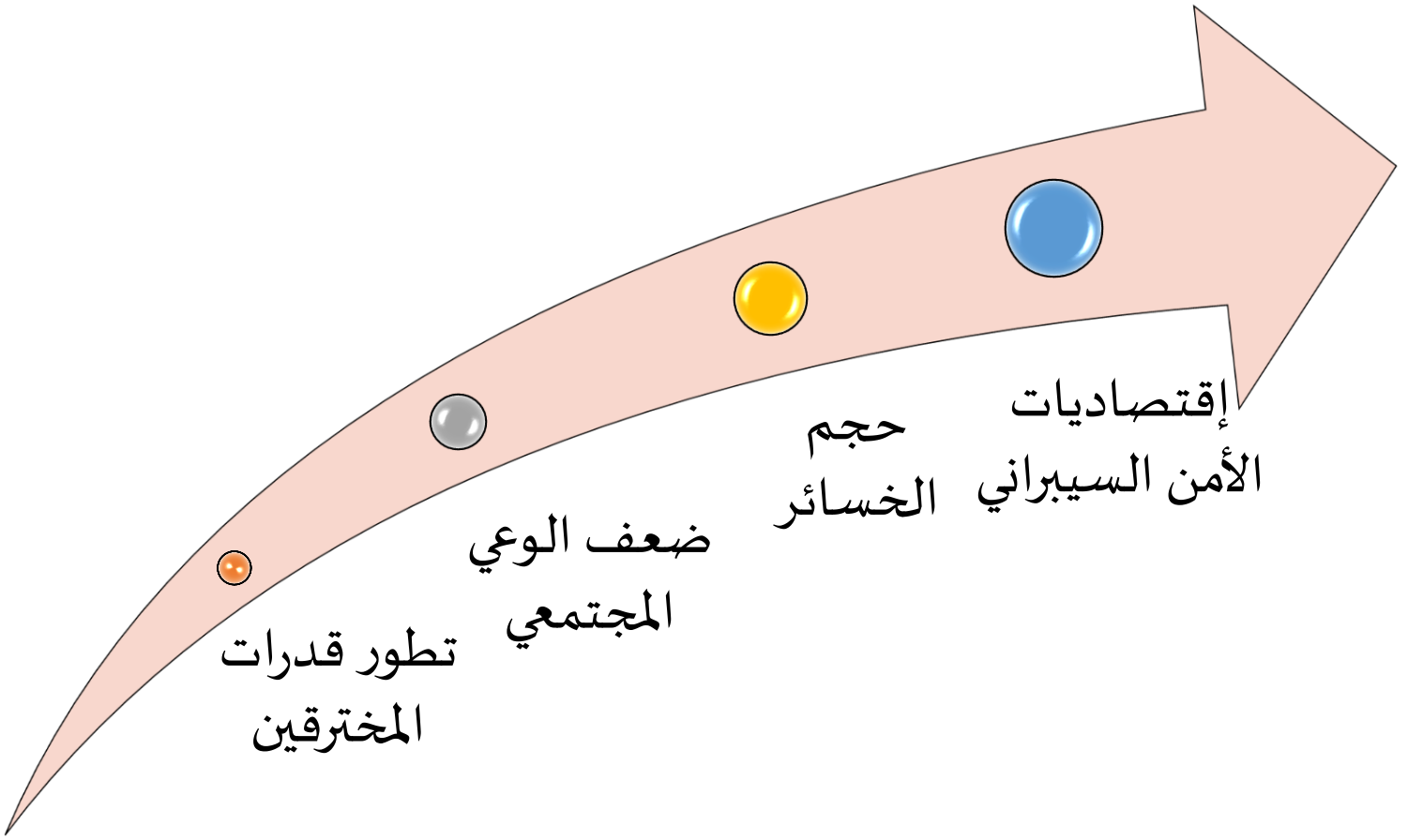
القدرة على الدفاع أو حماية الفضاء السيبراني (الإلكتروني) من الهجمات السيبرانية

حماية نظم المعلومات من الوصول أو الإستخدام الغير مصرح به أو التسريب أو التخريب أو التعديل أو التدمير وضمات توافر السرية والنزاهة والتوافر

الأمن السيبراني وأمن المعلومات



أهمية الأمن السيبراني



Insert Web Page

This app allows you to insert secure web pages starting with https:// into the slide deck. Non-secure web pages are not supported for security reasons.

Please enter the URL below.

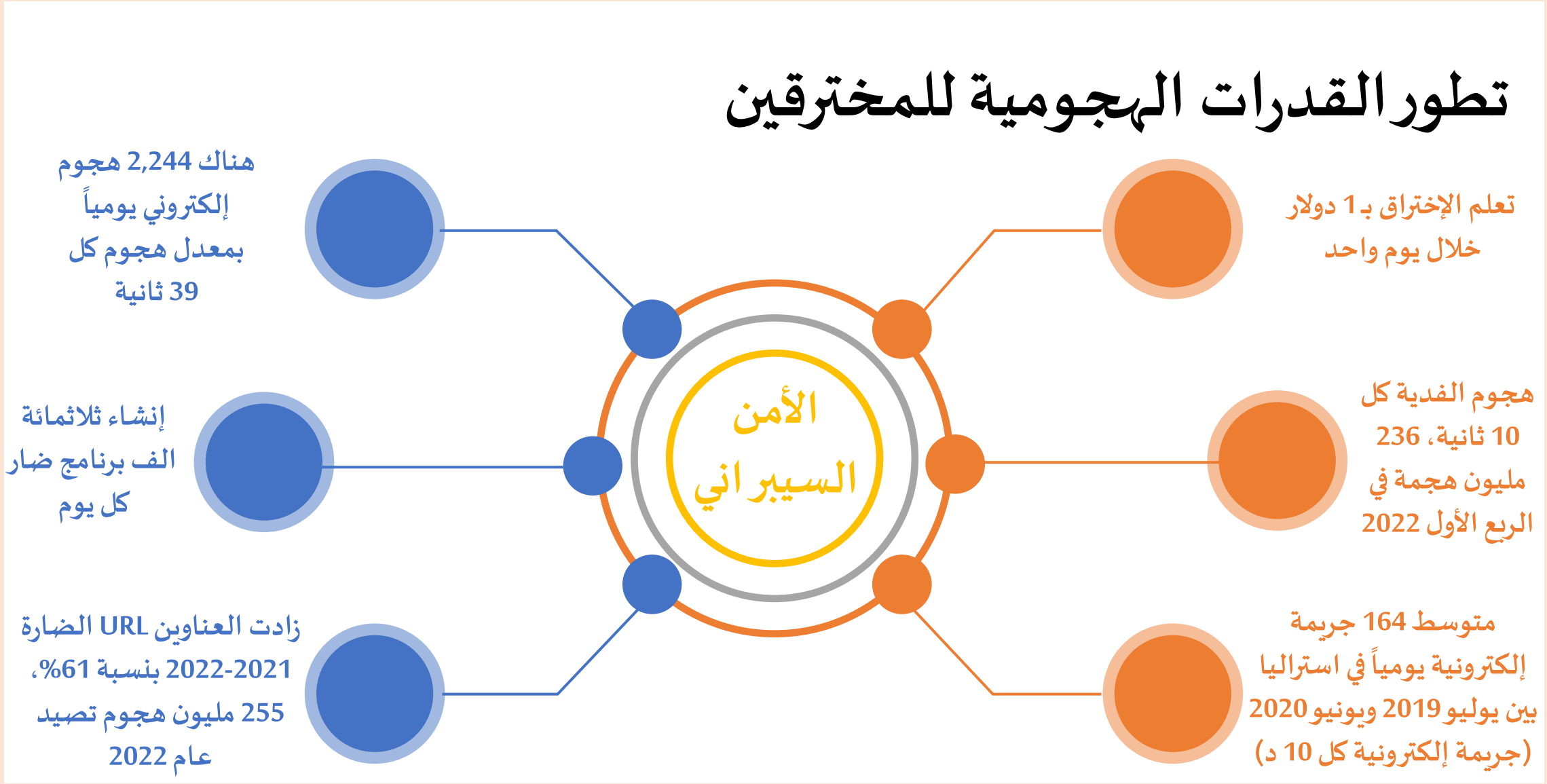
https:// livethreatmap.radware.com/

Note: Many popular websites allow secure access. Please click on the preview button to ensure the web page is accessible.

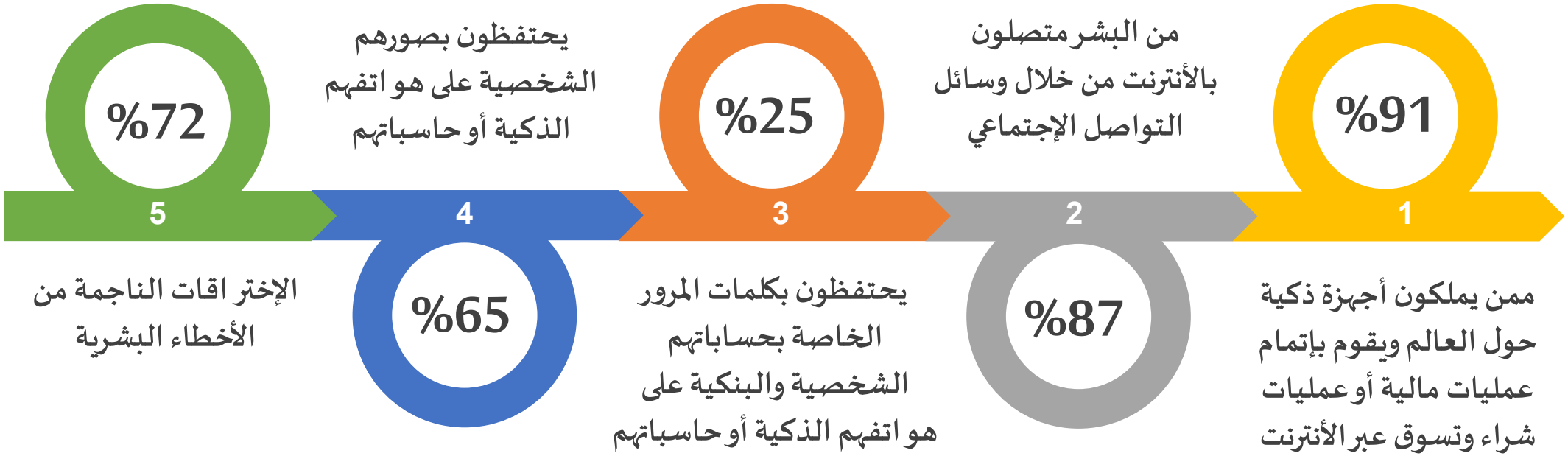
Web Viewer Terms | Privacy & Cookies

Preview

تطور القدرات الهجومية للمخترقين



إحصائيات هامة: الوعي المجتمعي



أهمية الأمن السيبراني: حجم الخسائر

في عام 2021 ، تلقى مكتب التحقيقات الفيدرالي 847,376 شكوى هائلة من جرائم الإنترنت في الولايات المتحدة، بخسائر 6.9 مليار دولار

في يوليو 2022 ، أكد موقع تويتر أن البيانات من 5.4 مليون حساب قد سُرقت

76 مليار دولار من الأنشطة الغير مشروعة التي تعتمد على البيتكوين

العلامات التجارية الأكثر استخدامًا للتصيد الاحتيالي هي لينكد إن (52٪) ، دي إتش إل (14٪)، Google (7%) ومايكروسوفت (6٪) وفيديكس (6٪)

تتجاوز التكلفة العالمية للجرائم الإلكترونية 20 تريليون دولار بحلول 2026، بزيادة 120%

عصف ذهني

مما سبق
وضح أهمية إقتصاديات
الأمن السيبراني؟

أهمية إقتصاديات الأمن السيبراني

- 35 مليون وظيفة شاغرة في مجال الأمن السيبراني في عام 2023م
- بلغت قيمة صناعة الأمن السيبراني أكثر من 156 مليار دولار عام 2022م
- تأثر 51.5% من الشركات بإختراق شبكتها أو بياناتها في عام 2022م
- وفقاً لتقرير 2022م، نقص حاد في الوعي بالأمن السيبراني والتدريب
- في USA، تلقت لجنة التجارة الفيدرالية 5.7 مليون تقرير إحتيال وسرقة هوية

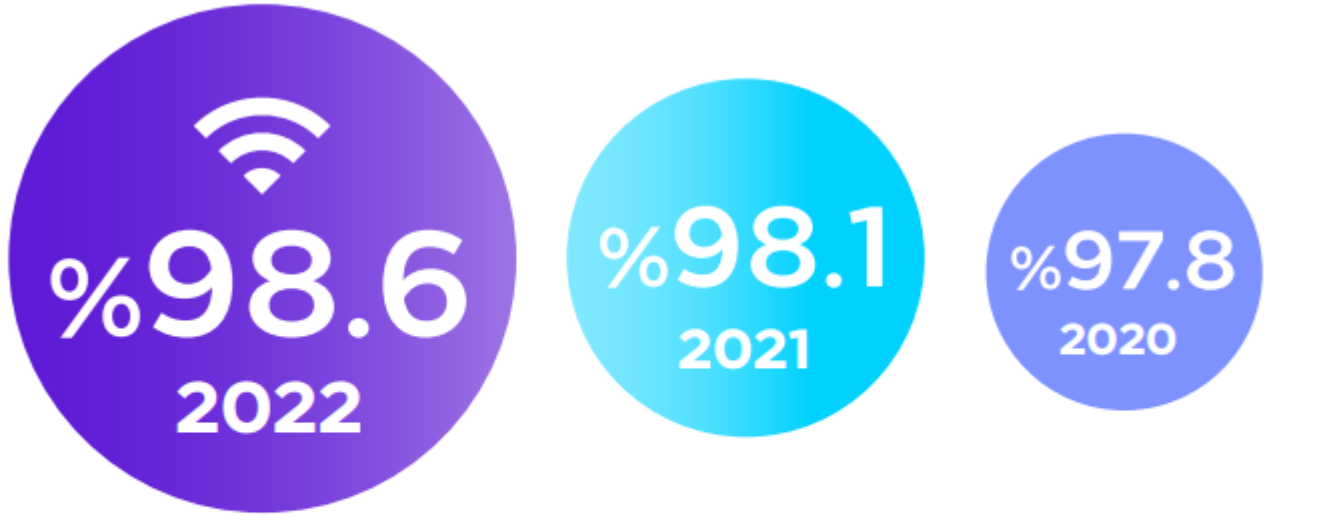
أهمية إقتصاديات الأمن السيبراني

- حجم الإنفاق العالمي على الأمن السيبراني وإدارة المخاطر 150 مليار عام 2021م
- US-SA Business Council يتوقع نمو السوق في المملكة 5.6 مليار دولار عام 2023
- تقرير إريكسون، 29 مليار جهاز متصل بالأنترنت بحلول عام 2022م
- 77% من الشركات ليس لديها خطة للإستجابة لحوادث الأمن السيبراني
- تستغرق معظم الشركات حوالي 6 شهور لكشف خرق للبيانات، حتى الشركات الكبرى

عصف ذهني

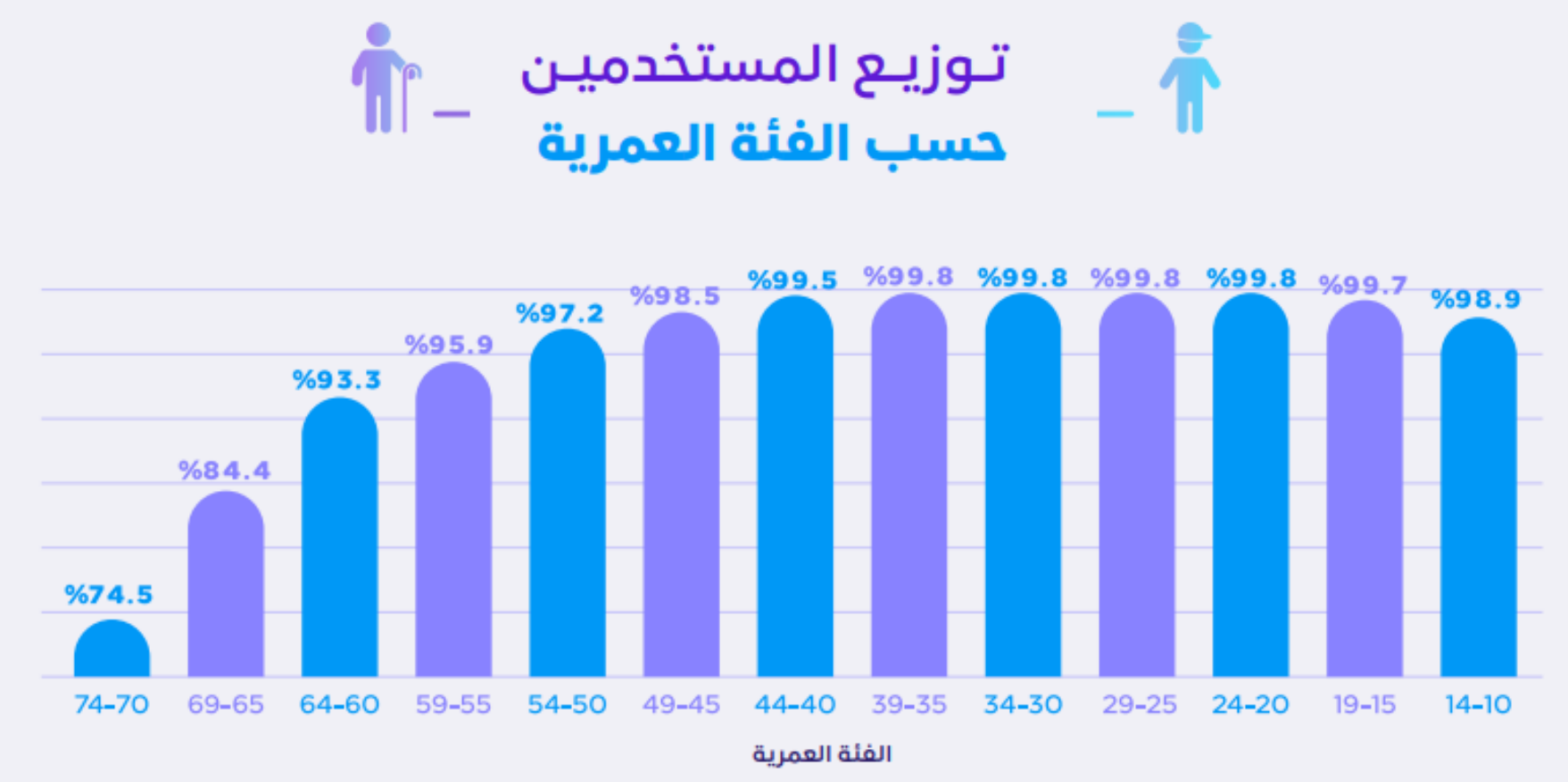
من وجهة نظرك
كيف نقيس حجم فضاء
المكلة العربية السعودية
السيبراني؟

الفضاءات السيبرانية في المملكة العربية السعودية



تقرير هيئة الاتصالات والفضاء والتقنية عام 2023

الفضاءات السيبرانية في المملكة العربية السعودية



تقرير هيئة الاتصالات والفضاء والتقنية عام 2023

الفضاءات السيبرانية في المملكة العربية السعودية

استخدام الإنترنت

مكان استخدام الإنترنت

المنزل
%83

أثناء التنقل
%73.8

العمل
%39.9

%49.4

من مستخدمي الإنترنت في المملكة يقضون 7 ساعات فأكثر يوميًا في استخدام الإنترنت

تقرير هيئة الاتصالات والفضاء والتقنية عام 2023

الفضاءات السيبرانية في المملكة العربية السعودية

استخدام الإنترنت حسب نوع الجهاز

الهاتف المتنقل
%97.9

أجهزة الكمبيوتر
%59.2

الجهاز اللوحي
%36.7

أخرى
الساعات الذكية، منصات الألعاب الإلكترونية، قارئ الكتب الإلكترونية
%26.8

%37

الحصول على معلومات من المؤسسات الحكومية

%34.6

إرسال البريد الإلكتروني واستقباله

تقرير هيئة الاتصالات والفضاء والتقنية عام 2023

الفضاءات السيبرانية في المملكة العربية السعودية

البنية التحتية للإنترنت

180.2 Mbps

متوسط سرعات التحميل للإنترنت المتنقل في المملكة

ضمن أعلى 10 دول في سرعات الإنترنت المتنقل

استخدام الخدمات الإلكترونية الحكومية

نسبة استخدام الخدمات الإلكترونية الحكومية

تقرير هيئة الاتصالات والفضاء والتقنية عام 2023

الفضاءات السيبرانية في المملكة العربية السعودية

حجم حركة بيانات الإنترنت في المملكة

35,088,769
تيرا بايت

معدل استهلاك بيانات الإنترنت المتنقل للفرد

37
جيجا بايت
شهريا

نسبة حجم حركة البيانات المحلية

%57

نسبة حجم حركة البيانات الدولية

%43

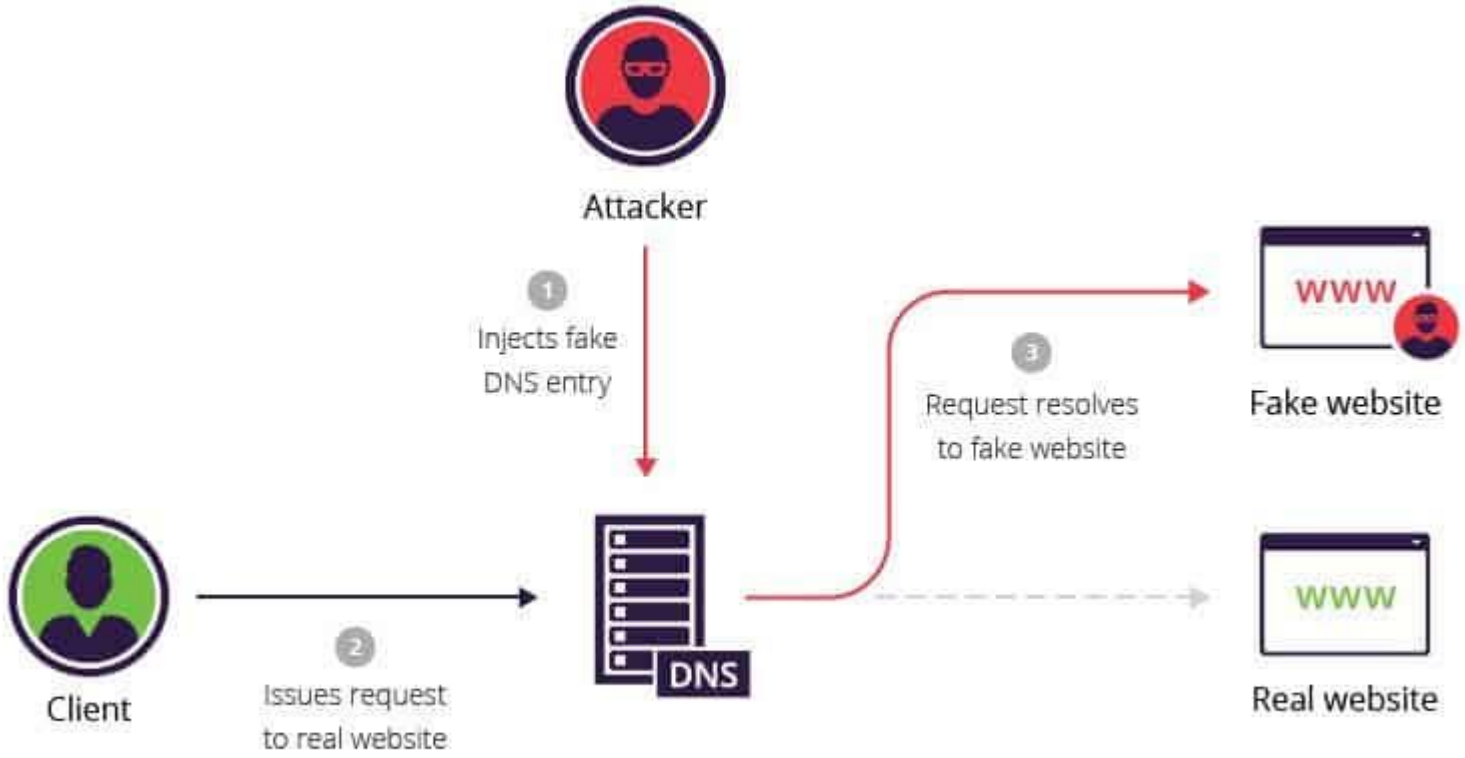
تقرير هيئة الاتصالات والفضاء والتقنية عام 2023

فترة نقـــاش

من وجهة نظرك

ما هو الإمتداد الآمن لأسماء النطاقات DNSsec ؟

الإمتداد الآمن لأسماء النطاقات DNSsec



الفضاءات السيبرانية في المملكة العربية السعودية

الفضاءات السيبرانية في المملكة العربية السعودية

انتشار إنترنت الأشياء IoT

عدد اشتراكات شرائح إنترنت الأشياء

+11 مليون

عدد أبراج الاتصالات التي تدعم تقنية NB-IOT

+20,000

نسبة التغطية السكانية لتقنية NB-IoT في المناطق الحضرية

+%98

تقرير هيئة الاتصالات والفضاء والتقنية عام 2023

فترة نقـــاش

من وجهة نظرك

ما هي مكونات الفضاء السيبراني في المملكة العربية السعودية ؟

مكونات الفضاء السيبراني في المملكة العربية السعودية

فترة نقـــاش

من وجهة نظرك

ما هي ركائز الأمن السيبراني الوطني التي تعتمد عليه المملكة العربية السعودية؟

ركائز الأمن السيبراني الوطني

ردع الجريمة السيبرانية

التعاون الوطني بين الحكومة ومجتمع صناعة الاتصالات والمعلومات

خلق قدرات وطنية لإدارة الحوادث السيبرانية

تحفيز ثقافة وطنية للأمن السيبراني

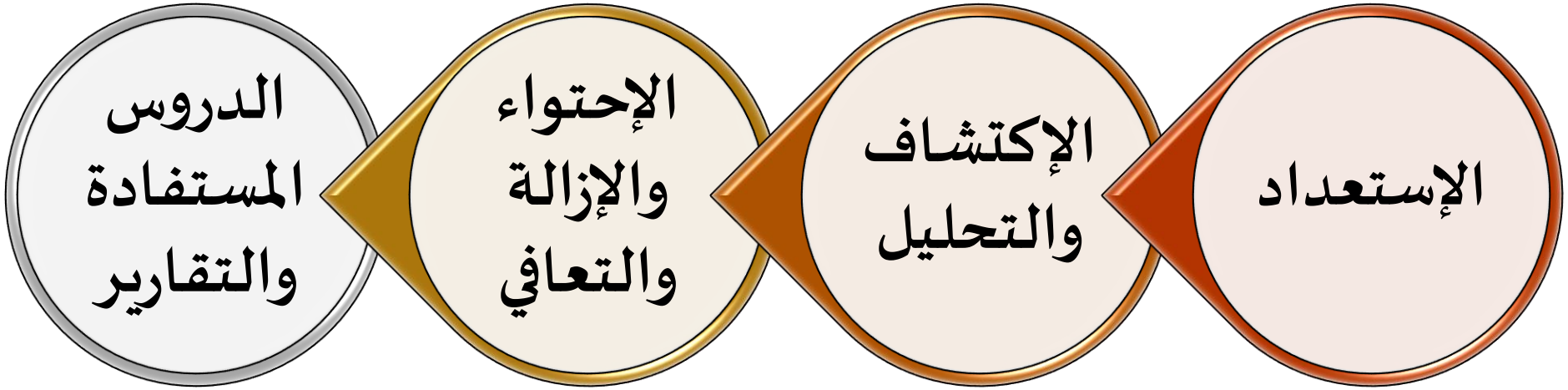
تطوير إستراتيجية وطنية للأمن السيبراني وحماية البنية التحتية

فترة نقـــاش

من وجهة نظرك

كيف يتم التحضر والمواجهة للهجمات السيبرانية؟

منهجية الإستجابة للحوادث السيبرانية NIST Standard



فترة نقـــاش

من وجهة نظرك

كيف يتم الإستعداد
للحوادث السيبرانية؟

منهجية الإستجابة: الإستعداد

لابد من التحقق من توفر ما يلي:

- تدريب وتجهيز فريق العمل للإستجابة السريعة للحوادث السيبرانية
- حصر الأصول التقنية في البنية التحتية للأنظمة والشبكات والتطبيقات وبالأخص الحساسة منها
- التأكد من إستيفاء الشروط الخاصة بضوابط الأمن السيبراني
- تجهيز برمجيات خاصة بالإستجابة للحوادث السيبرانية
- التأكد من وجود نسخ إحتياطية لجميع البيانات على خوادم مستقلة
- بناء خطة للإستجابة لحوادث الأمن السيبراني عند وقوعها
- وغيرها .....

فترة نقـــاش

من وجهة نظرك

كيف يتم إكتشاف الحوادث السيبرانية؟

منهجية الإستجابة: الإكتشاف والتحليل

يتم الإكتشاف والتحليل حسب المراحل التالية:

- مراقبة الأنظمة والفضاء السيبراني
- رصد وإكتشاف الوصول الغير مصرح به والعمليات الضارة على الفضاء السيبراني
- تحليل العمليات المشبوهه وتحديد مصدرها والغرض الرئيسي منها
- كتابة التقرير الأولى عن الحادثة السيبرانية

فترة نقـــاش

من وجهة نظرك

كيف يتم إحتواء الحوادث السيبرانية والتعافي منها؟

منهجية الإستجابة: الإحتواء والإزالة والتعافي

يتم مرحلة الإحتواء والإزالة والتعافي من خلال الخطوات التالية:

- حصر الأصول التقنية المصابة وتحديدها
- أخذ نسخة رقمية للأجهزة المصابة والبدء بتحليلها
- تحليل البرمجيات والملفات الضارة
- حصر مؤشرات الإختراق
- حجب مؤشرات الإختراق من الشبكة
- التأكد من خلو الشبكة من مؤشرات الإختراق
- عزل الأنظمة المصابة وإعادة تهيئتها
- تفعيل خطة التعافي

منهجية الإستجابة: الدروس المستفادة والتقارير

تتحقق هذه المرحلة بعمل ما يلي:

- عمل تقرير شامل عن الحادثة
- مراقبة جميع الأنشطة المشبوهة التي تم اكتشافها من الحادثة من خلال مركز السجلات المركزية
- حصر الدروس المستفادة من الحادثة لتجنب تكررها لاحقاً

فترة نقاش

هناك العديد من أبعاد الأمن السيبراني، أذكر مثال لكل بُعد؟

- البُعد العسكري
- البُعد الإجتماعي
- البُعد السياسي
- البُعد الإقتصادي
- البُعد القانوني

عصف ذهني + نقاش

من وجهة نظرك

ما هي التهديدات السيبرانية المحتملة في قطاعك العسكري؟

شكراً لإستماعكم وتفاعلكم

- فترة الأسئلة -