المؤتمر الوطني الأول للأمن السيبراني
First National Cyber Security Conference
صنعاء - 7 - 9 يونيو/ حزيران 2021م

وزارة الاتصالات وتقنية المعلومات
Ministry of Telcommunications and Information Technology

ورقة عمل بعنوان :

تحديات الأمن السيبراني على مستوى
- الهاتف النقال
- وشبكات المنظمات

إعداد:
م/ علي حميد الوصابي

رئيس قسم أمن المعلومات – شركة يمن موبايل

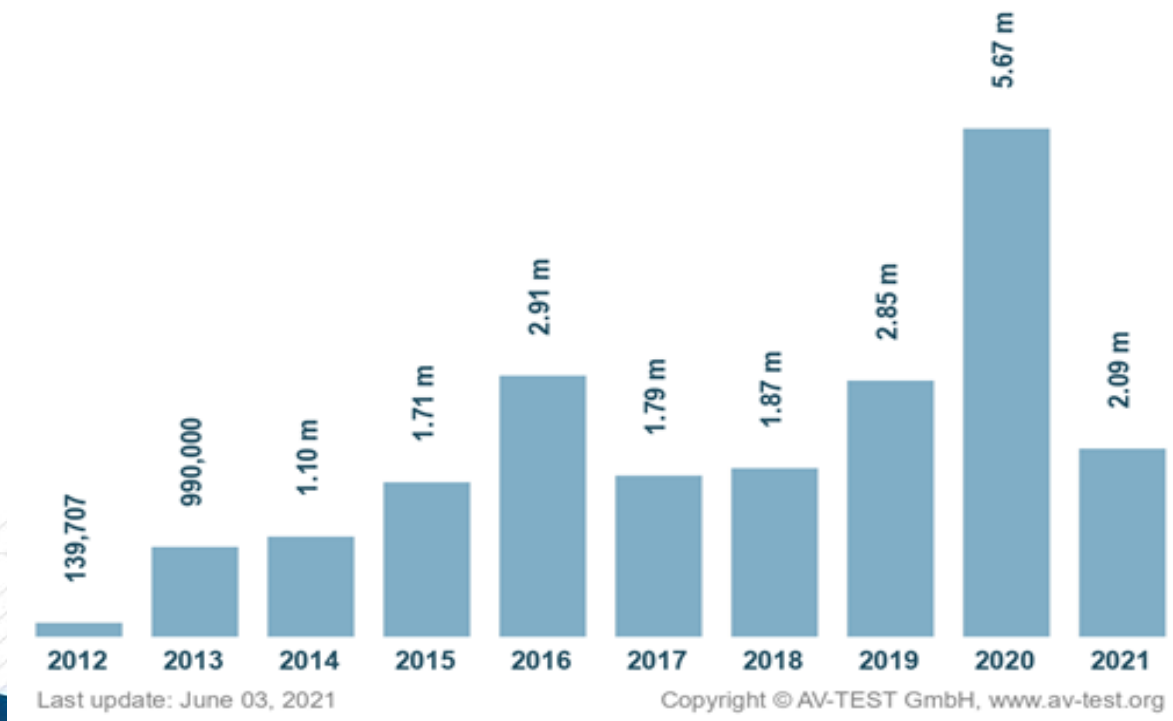
نحو استراتيجية وطنية للأمن السيبراني
Towards a National Cyber Security Strategy

~ *3f#7}1 3 "}107}61$$"£1 487 *9f@1 ĂMalwareÅ ¶f*57}~ *7℗1f§7}

- *9f$*1 1
- 317}65 *9f*#'5}9℗
- 317}65 *9f7@0
- ^7$*1 '95} *9f7*$1
- ^751 1} *9f7*$1
- ^71°7}55]*£11 518°7}¶f*5 7}~ *7℗1f§7}5§0'£1
- ^° f'01}518°7}1 ~ *1151}31"£1 487 ~ }f2@1 f7*$1}99}
- ZeroTrust *9f717" ^719}1 ^7$Za0'}~ *3$#}9711 " f7*$1

مصادر تطوير البرمجيات

الضارة في تصاعد مستمر



POTENTIALLY UNWANTED APPLICATION (PUA)

(التطبيقات غير المرغوبة)

مازالت إمكانيات GOOGLE

محدودة APP STORE & PLAY

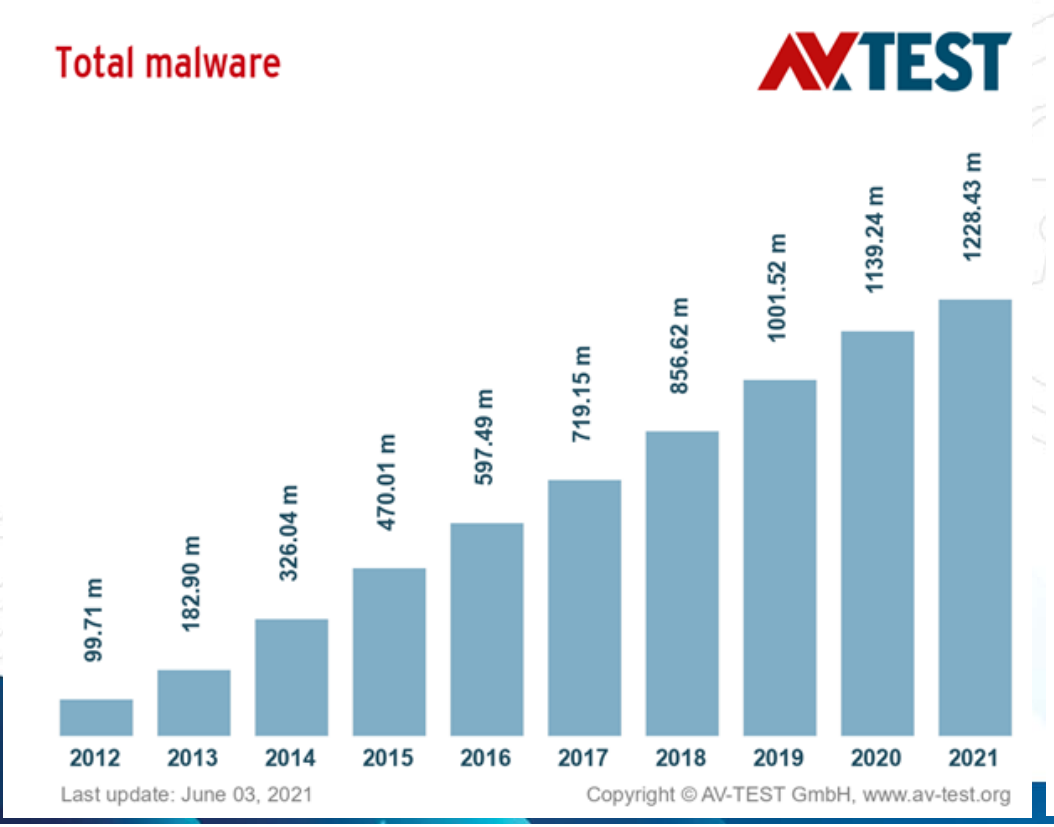
في التعرف على الكثير من انوع

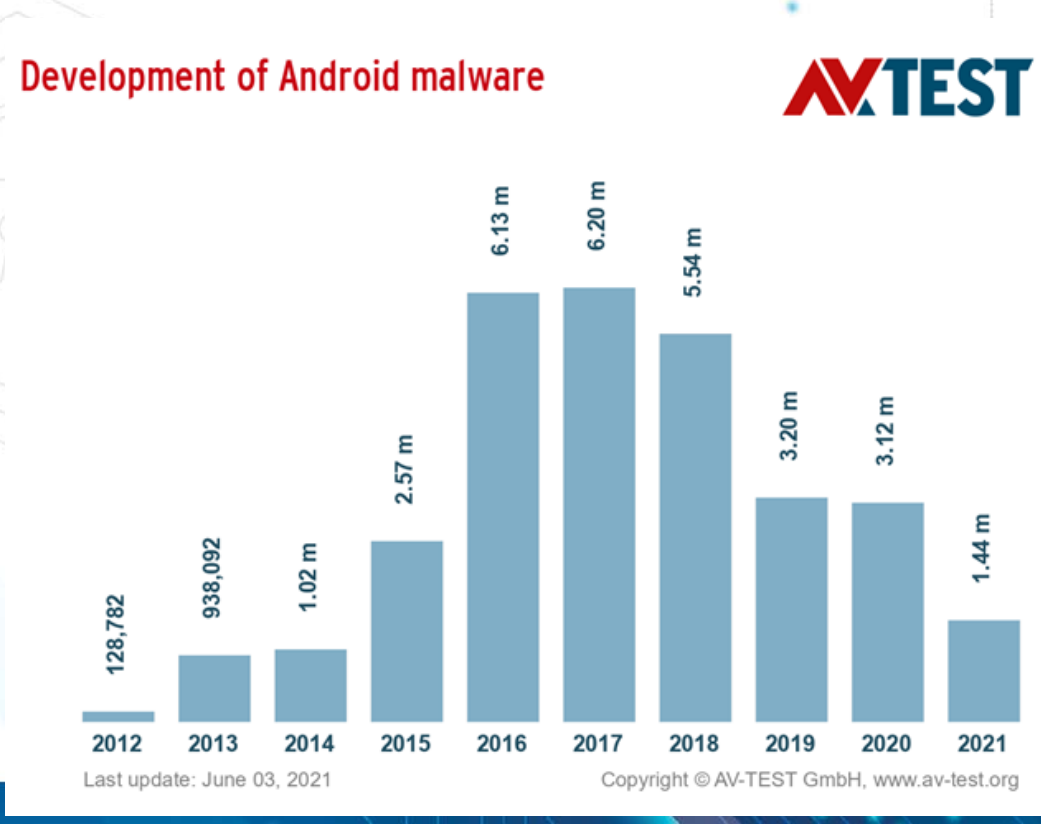
البرمجيات الضارة في التطبيقات والألعاب ،

ويوميا يتم تحميل تطبيقات ملوثة بالبرمجيات

الضارة

حجم البرمجيات الضارة Malware

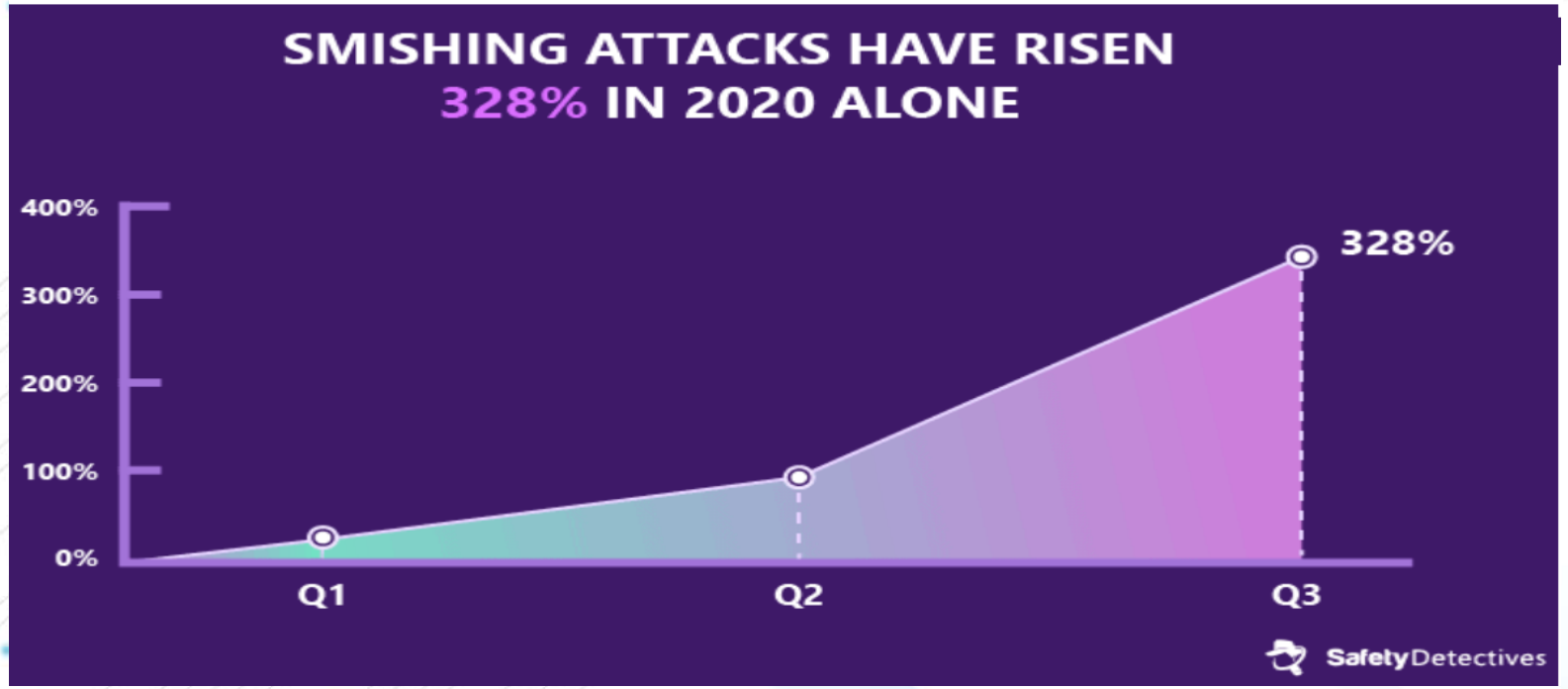




تأثير البرمجيات الضارة يمثل تحدي سيبراني عالمي

- عالميا هناك استغلال لمستخدمي الهواتف النقالة من قبل البرمجيات الضارة ومنها عبر رسائل الـSMS

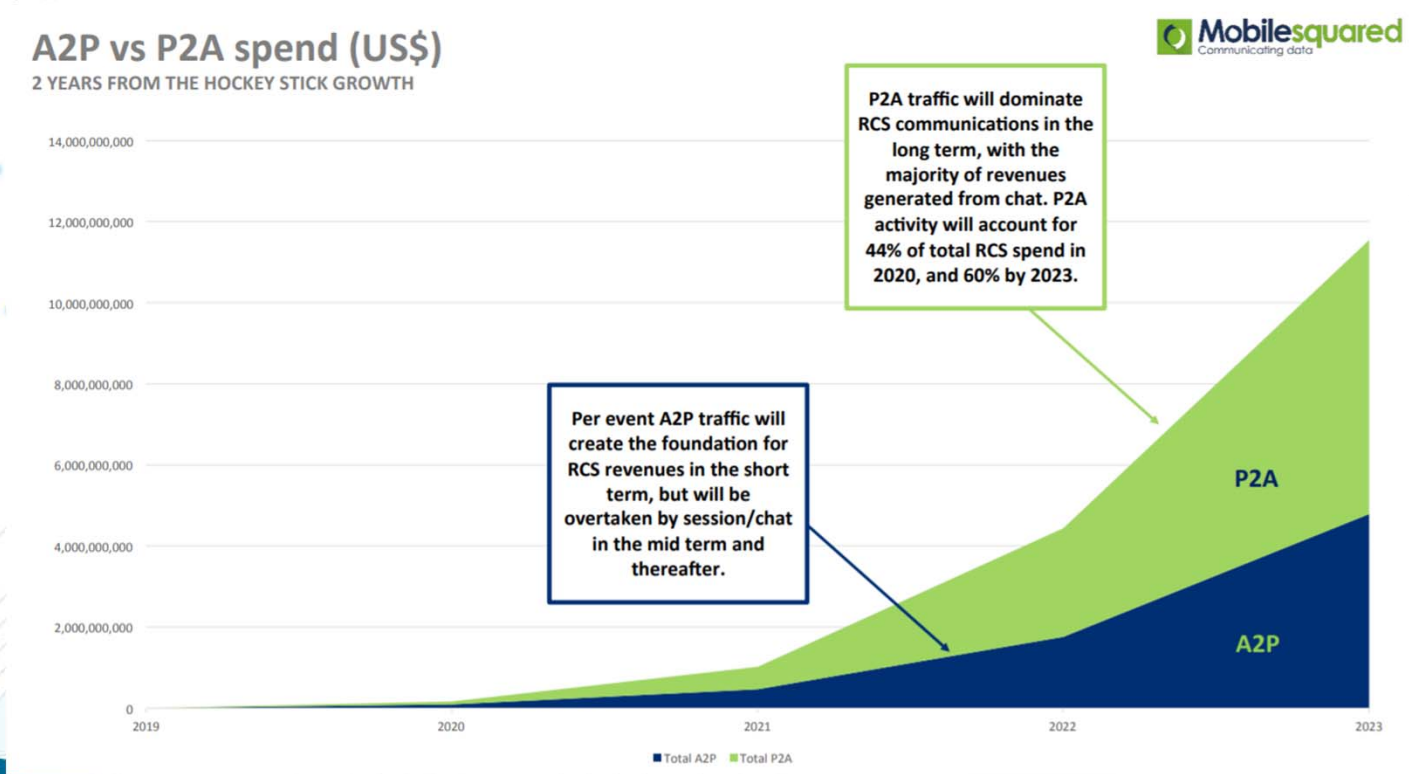
Proofpoint reported that SMS-based scams had risen 328% in the middle of 2020 alone.



تأثير البرمجيات الضارة في اليمن

- تقوم شركات الاتصالات بحجب مئات الآف الرسائل القصيرة التي ترسلها البرمحيات الضارة من بعض الهواتف المصابة ببرمجيات ضارة حتى لاتتضرر أرصدة المشتركين.
- حيث تعمل بعض البرمجيات الضارة في الخفاء وترسل رسائل الى جهات دولية مختلفة (أوتتصل دون علم المستخدم)
- في حال نجحت بعض تلك الرسائل في المرور فأنها لاحقا تستوجب الدفع مقابل هذه الرسائل للمزودين الخارجين (بالعملة الصعبة).

تنتشر حاليا التطبيقات والألعاب التي تطلب ارسال رسالة قصيرة (P2A)عند مستوى معين من اللعبة



تزدهر عالميا أسواق رسائل

PERSON TO APPLICATION (P2A)الـ

بشكل سريع وهذا النوع من الرسائل

سوق كبير قادم ويتطلب وضع سياسات

ووسائل حماية خاصة.

الرسائل القصيرة نوع A2P تتعرض للاحتيال الدولي عبر مسارات رخيصة الـgrey-route وقد لاتصل جميعها

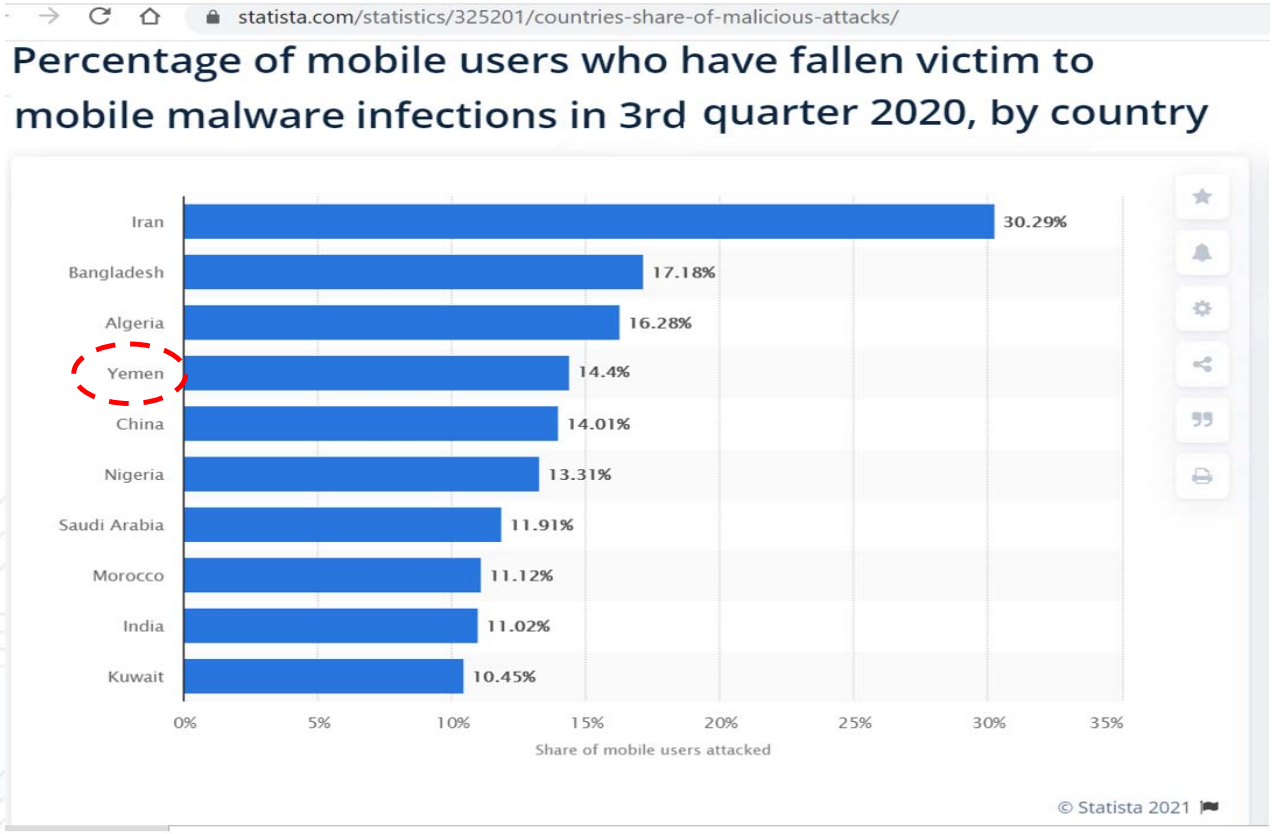
Revenue leakage and fraud prevention are **now the key drivers for mobile operators to capable of blocking grey-route traffic.** Mobilesquared experts forecast that 85% of mobile operators will have invested in SMS firewall solutions by 2022.

Considering the top 3 A2P monetization issues are all fraud related (SIM farms, grey routes, and spam) and cost an estimated $1.5 billion per annum globally,ix

investing in developing a P2A messaging strategy that relies on brand and bot vetting to guarantee a secure and clean communication between the consumer and the brand makes a lot of sense.

تحديات الأمن السيبراني على مستوى - الهاتف النقال - وشبكات المنظمات

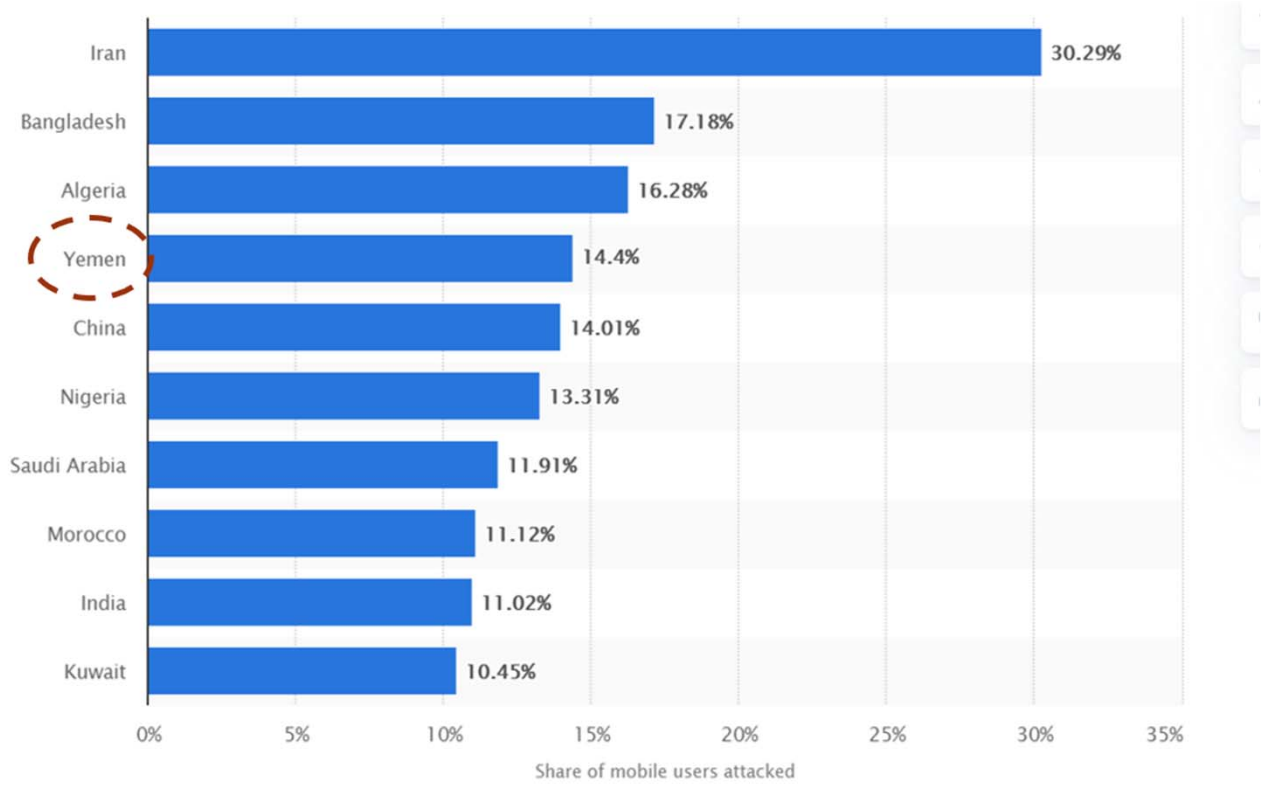
تأثير البرمجيات الضارة في اليمن من بين أكثر 10 دول عالميا من حيث مشاركة البرمجيات الضارة (وتتطلب استراتيجية للحد مخاطرها)



Ten countries with the largest shares of users attacked by mobile malware 1Q2021 Kaspersky

	Country*	%**
1	Iran	25.80
2	China	16.39
3	Saudi Arabia	13.99
4	Algeria	13.22
5	Morocco	10.62
6	Turkey	10.43
7	Yemen	10.05
8	Nigeria	9.82
9	India	8.08
10	Kenya	8.02

Countries most targeted by banking malware attacks in 2020



الحاجة للتوعية بمخاطر الخداع عبر وسائل التواصل كإستغلال عناوين موثوقة لروابط ضارة

وتلك الروابط مثل:

http://d10220.xyz/yemenmobile-bx/?t=1619474386638

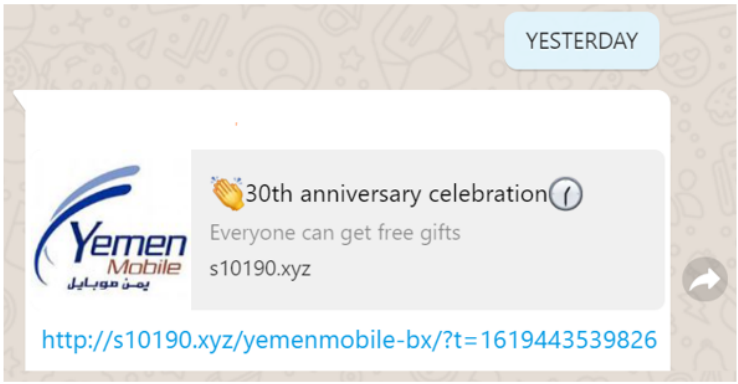
http://s10190.xyz/yemenmobile-bx/?t=1619443539826

http://f10167.xyz/yemenmobile-bx/?t=1619443539826

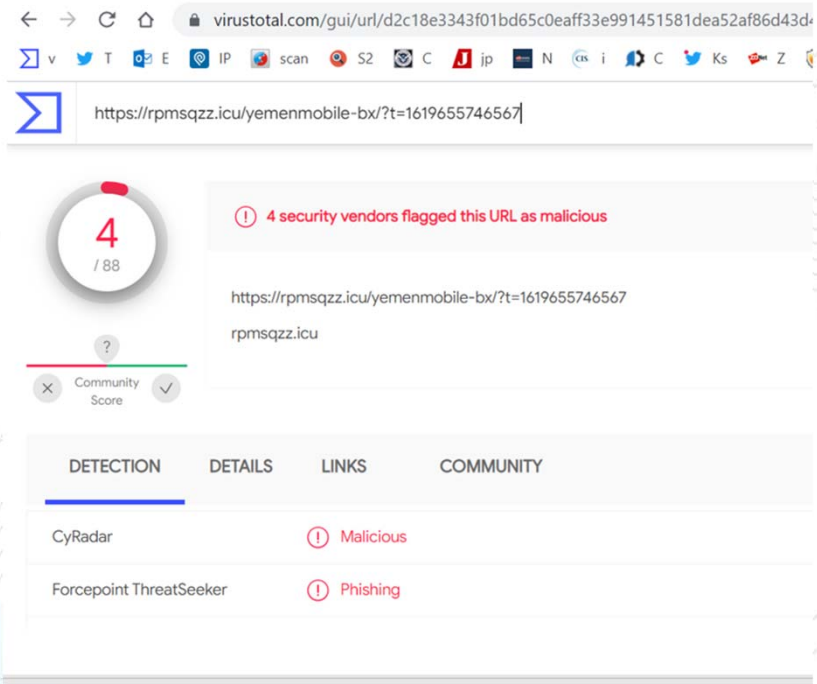
http://cogpd9.store/yemenmobile-bx/?t=1619443539826

http://ddd88.store/yemenmobile-bx/?t=1619443539826

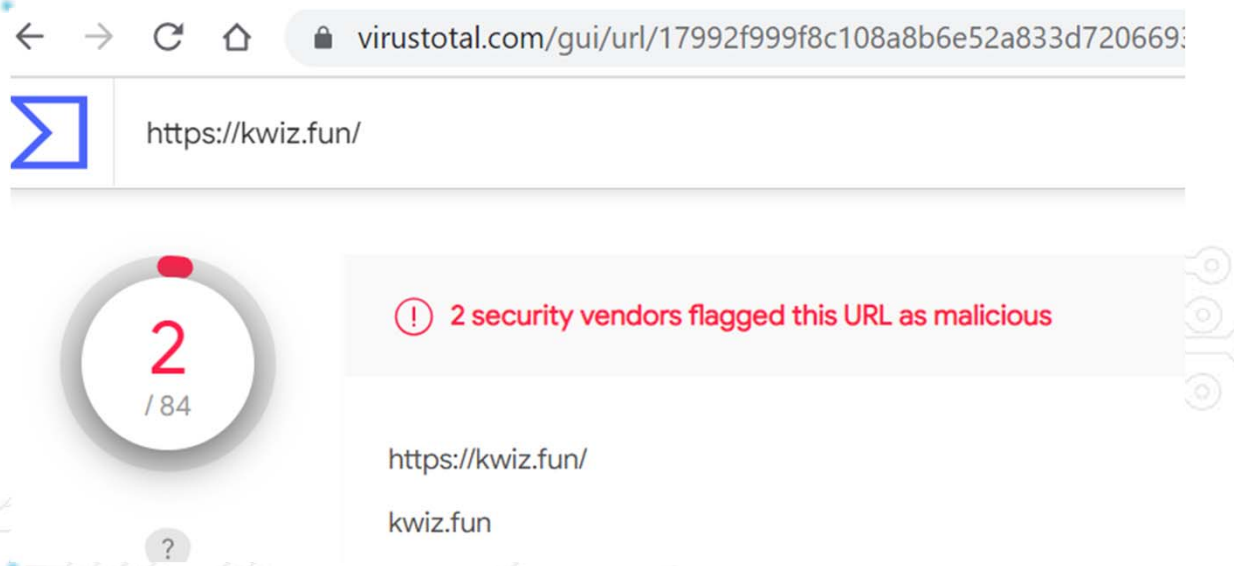
وتظهر في الواتساب بالشكل التالي :

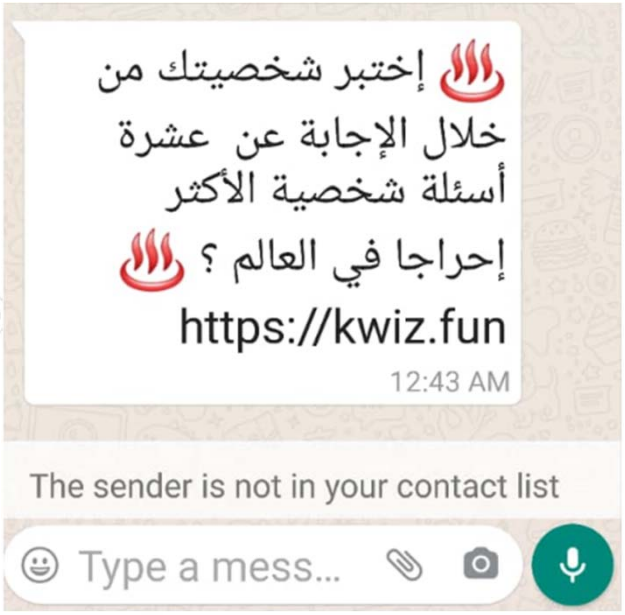


عند فحص أحد تلك الروابط التي تستغل نقص الوعي لدى المواطنين



تتنوع أساليب الاحتيال عبر وسائل التواصل الاجتماعي والتي تتطلب توعية مجتمعية

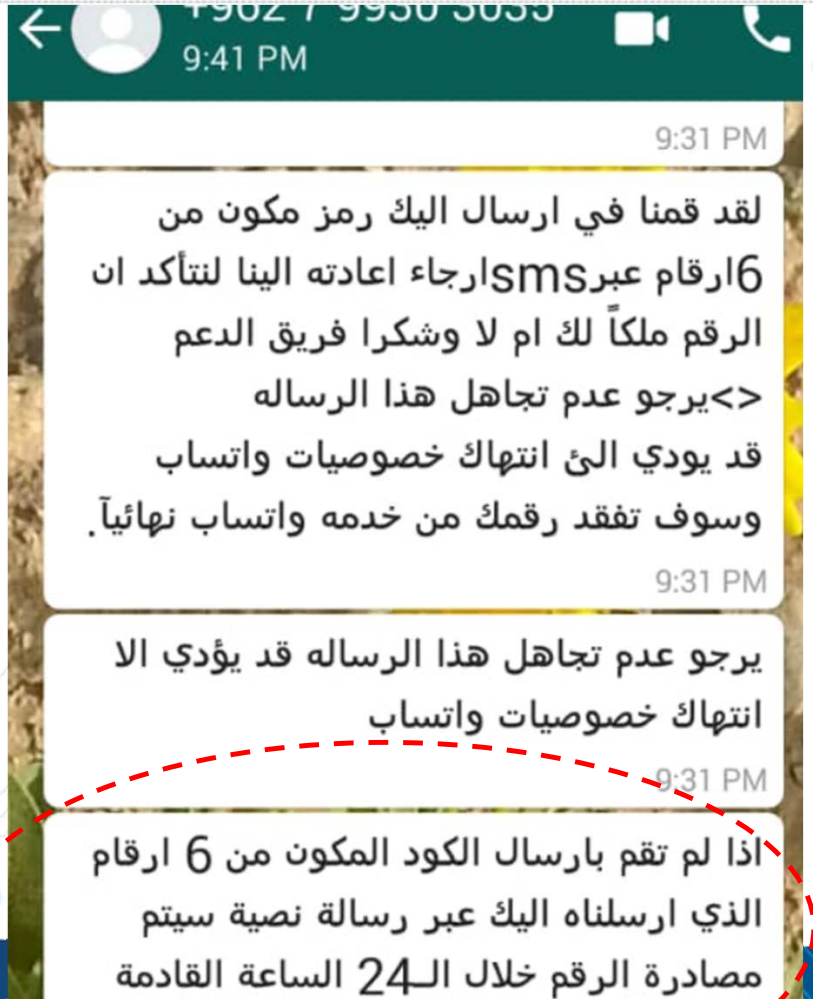




تحديات الأمن السيبراني على مستوى - الهاتف النقال - وشبكات المنظمات

نوع من طرق الاحتيال
(الهندسة الاجتماعية) البسيطة
عبر استغلال خدمة تحويل رقم الضحية
الى رقم المحتال ، لغرض الابتزاز ..

الهندسة الاجتماعية في إنتحال الهوية عبر وسائل التواصل الاجتماعي



الهندسة الاجتماعية وإستغلال الأحداث والظواهر البارزة للخداع والاستغلال

تطورعمليات الإحتيال والإبتزازعبرالبريد الإلكتروني وارتفعت بنسبة 250% منذ 2018

واصبحت الرسائل الاحتيالية تخاطب كل بلد بلغتهم وتترجم آليا

تأثير فيروسات الفدية Ransomware في اليمن

Middle East

In 2019, the countries with the greatest share of users that encountered ransomware on any device in the Middle East were as follows:

Country	%*
Pakistan	19.03%
Palestine	6.74%
Yemen	6.55%
Egypt	6.41%
Iraq	6.28%

*Share of users attacked with ransomware out of all users encountering malware in the country

ارتفعت إحصائيات فيروسات الفدية عالميا بمقدار 350% منذ 2018م

اليمن في المرتبة (2) عالميا في 2020م من حيث مشاركة الهواتف لفيروسات الفدية

In 2020, the five countries with the greatest share of users encountering ransomware remained the same with a few small adjustments.

Country	%*
Pakistan	14.88%
Yemen	7.49%
Egypt	6.45%
Palestine	5.48%
Iraq	5.37%

**Share of users attacked with ransomware out of all users encountering malware in the country*

Pakistan still had the greatest share of users, but the overall percentage declined to 14.88%. The percent of users encountering ransomware in Yemen actually increased to 7.49%, while the percentage of users in Palestine and Iraq lowered, and the share of affected Egyptians remained pretty much the same.

أهم مخاطر الأمن السيبرانى على مستوى مستخدمى الهاتف النقال :

1. الاستغلال الإقتصادي (عبر البرمجيات الضارة SMS , CALL، وعبر عروض مزيفة او مخادعة)
2. استغلال أجهزة المستخدمين في تنفيذ عمليات هجمات سيبرانية
3. استغلال اجهزة المشتركين في عمليات تعدين العملات المشفرة
4. استغلال أجهزة المستخدم لنشر البرمجيات الضارة في المجتمع
5. مخاطر تسريب وسرقة المعلومات من المشتركين (وسائل التواصل، **جهاز mobile ، و ..الخ)**
6. سرقة الحسابات وانتحال الهوية
7. خداع المستخدمين وجرهم الى روابط الغرض منها تربح أفراد و جهات خارجية
8. الاستغلال الاقتصادي للافراد وما قد ينتج عنه من تسديد مبالغ لجهات اوشركات خارجية.

أبرز الثغرات :

1. نقص الوعي بأمن المعلومات ومخاطر الفضاء السيبراني
2. صعوبة وتكلفة الحصول على برمجيات الحماية المرخصة
3. صعوبة وتكلفة شراء البرمجيات المرخصة (انظمة،برامج مكتبية،برامج مساعدة ،التطبيقات الألعاب..)
4. عدم توفر التحذيرات والتنبيهات حول الثغرات المتلاحقة في مختلف انوع البرمجيات
5. صعوبة وتكلفة تحديث الثغرات المعلنة في الأنظمة والبرمجيات والتطبيقات
6. الإضطرار لتشارك البرمجيات المسروقة(المكركة) والتي تزيد من انتشار البرمجيات الضارة
7. صعوبة تنزيل التحديثات يساهم في الاضطرار لحلول بديلة ذات مخاطر

(كعدم إمكانية استكمال التحديثات المجانية الطارئة، العزوف عن تفعيل التحديث التلقائي، نسخ البرمجيات المكركة)

أهم الحلول المقترحة:

1. وجود جهة مختصة بوضع برامج التوعية المجتمعية حول أمن المعلومات ومخاطر الأمن السيبراني
2. تمويل برامج للتوعية عبر موقع رسمي وعبر وسائل التوعية المختلفة الملائمة وتوجيه التوعية بشكل مركز الى المدارس حيث المراهقين والى ارباب الاسرة ومخاطبة كل شريحة مجتمعية بطريقة مناسبة والتركيز على إيضاح مخاطر الأمن السيبراني وذكر بعض الحوادث الأمنية التي ترسخ الوعي.
3. العمل على دراسة المخاطر والثغرات وتوفير الحلول الممكنة التي تساهم في الحماية من تسريب او سرقة المعلومات من المواطنين وبمشاركة الجهات المختصة وشركات الاتصالات ومشاركة مجتمعية للحد من مخاطر الأمن السيبراني في المجتمع.
4. البحث في رفد البنية التحتية باي تقنيات أو تجهيزات حماية تساهم في الحماية والحد من مخاطر الأمن السيبراني

على مستوى المنظماتorganization

أهم المخاطر والثغرات والحلول المقترحة

أهم مخاطر الأمن السيبرانى على مستوى المنظمات:

1- مخاطر فيروسات الفدية على المنظمات وتزداد هذه المخاطر مع زيادة التطور في وسائل وطرق نشر فيروسات الفدية ، وأن اليمن مايزال ضمن الـ10 دول الأولى عالميا فيما يخص انتشار فيروسات الفدية بين الأفراد بحسب التقارير العالمية وهناك مخاطر كبيرة من تسلل فيروسات الفدية الى شبكات المنظمات.

أهم مخاطر الأمن السيبرانى على مستوى المنظمات:

2- مخاطر البقاء على الأساليب القديمة في الحماية والتي تتضمن:

A. غلق شبكة المنظمة الداخلية عن الفضاء السيبراني وعدم متابعة وتحديث الثغرات التي تصدر بشكل شبه يومي مما يجعل الأنظمة والبرمجيات المعزولة داخل شبكة المنظمة مخزن هائل للثغرات التي تتراكم فيها (لتصبح قنبلة موقوته).

B. التقليل من أهمية التهديدات التي قد تأتي من داخل المنظمة وعدم مواكبة المخاطر المستحدثة التي اصبحت تهدد شبكة المنظمة.

C. البقاء على التصميم القديم للشبكات الداخلية المبني على اعتماد الثقة بعد الوصول الى الشبكة الدخلية مما يسمح بالوصول والتخاطب مع كل او أغلب انظمة المنظمة وجعلها متاحة للتسريب والاختراق الكلي لشبكة المنظمة.

أهم مخاطر الأمن السيبرانى على مستوى المنظمات:

3 – نقص الكوادر المؤهلة وعدم توفر مصادر جاهزة نتيجة عدم وجود أقسام مختصة في مجال أمن المعلومات والأمن السيبراني في الجامعات والمعاهد التعليمية.

4-مخاطر ضعف التوعية بمخاطر هجمات الأمن السيبراني والبرمجيات الضارة والأدوات والوسائل المطلوبة في مجال أمن المعلومات لحماية وتأمين المنظمات بشكل معياري.

5- أهم مخاطر عدم تطبيق سياسات أمن المعلومات بحسب المعايير:

A. عدم احتساب مخاطر أجهزة الموبايل ودورها في تسريب وسرقة البيانات ومخاطر البرمجيات الضارة عبر الموبايل خصوصا أن البريد الإلكتروني اصبح مفتوح عبر جهاز الموبايل Bring your own device (BYOD)

B. عدم احتساب مخاطر البرمجيات الضارة عبر شبكة (الواي فاي) في المنازل (نتيجة عبث الاطفال في الفضاء السيبراني) وإمكانيات تسلل البرمجيات الضارة الى/ وعبر لابتوبات كوادر المنظمة.

C. عدم احتساب مخاطر انتقال البرمجيات الضارة عبر شبكات الواي فاي (في العمل) داخل المنظمة.

D. عدم احتساب مخاطر انتقال البرمجيات الضارة عبر وسائط التخزين المتنقلة (الفلاشات والهاردات ..)

E. مخاطر عدم وجود متابعة يومية للثغرات المتجددة وعدم تحديث الثغرات في الأنظمة والبرمجيات في خوادم المنظمة ولابتوبات الموظفين وأجهزة الموبايل .

5- مخاطر عدم تطبيق سياسات أمن المعلومات بحسب المعايير:

F. عدم احتساب مخاطر أهمية ودور التوعية الأمنية لكوادر المنظمة حول أمن المعلومات

G. عدم احتساب أهمية وضع سياسات تنظم استخدام اللابتوب والموبايل وشبكات (الواي فاي) ووسائط التخزين المتنقلة.

H. عدم وجود سياسات صارمة لإدارة وضبط الهوية للمستخدمين وإدارة الصلاحيات

I. عدم وجود سياسة وخطة لإدارة حوادث أمن المعلومات وعدم القدرة والجاهزية في الاستجابة لها

J. عدم وجود سياسة وضوابط لإدارة الأصول المعلوماتية

K. عدم وجود سياسات وخطط لإدارة الطوارىء واستمرارية الأعمال

L. عدم وجود سياسات تنظم إدارة التغيير

أبرز الثغرات على مستوى المنظمات:

1. متطلبات التخلص من اي برمجيات غير مرخصة (مكركه) سواء في الأجهزة المكتبية او لابتوبات الموظفين وأحيانا في الخوادم.
2. متطلبات اعتماد توفير منظومات متخصصة في حماية ومنع تسريب او سرقة البيانات في الكثير من المنظمات.
3. متطلبات تأمين شبكات المنظمات يزيد من التكلفة التشغيلية اليدوية (غير الدقيقة) ويتطلب منها استحداث منظومات آلية متطورة للمساعدة في الكشف عن التهديدات والثغرات واتمتة التحديثات.
4. متطلبات ترقية واستبدال أي تجهيزات قديمة في الشبكات (التي تصبح ثغرة بحد ذاتها) وتتطلب مواكبتها بجيل حديث يتضمن وسائل حماية حديثة.

أبرز الثغرات على مستوى المنظمات:

5. متطلبات التكامل والدقة في عمل تجهيزات وانظمة حماية الشبكات يفرض تقليل الاعتماد على تعدد الموردين للحد من الوقوع في ثغرات تعدد الموردين.
6. متطلبات التوعية لجميع موظفي وكوادر المنظات حول اساليب مواجهة الهندسة الاجتماعية وأساسيات ومبادىء أمن المعلومات ومخاطر الفضاء السيبراني
7. متطلبات التأهيل للمختصين في المنظمات وتوفير بنى تحتية ومدربين في إختصاصات أمن المعلومات والأمن السيبراني ، ودعم وتمويل استحداث أقسام مختصة في الجامعات والمعاهد اليمنية.

الحلول المقترحة على مستوى المنظمات:

1. أن تعتمد المنظمات هيكل إداري خاص بأمن المعلومات يطابق المعايير.
2. اعتماد السياسات المحلية (وزارة الاتصالات) والمعايير في مجال أمن المعلومات (ISO27K) .
3. التوعية لجميع الموظفين والمستخدمين حول أمن المعلومات ومخاطر الأمن السيبراني.
4. التأهيل وعمل الدورات التخصصية والدورية للمختصين في مجالات الشبكات وأمن المعلومات
5. التركيز على متابعة الثغرات المعلنة بشكل يومي وتنفيذ عمليات التحديث للثغرات
6. فرض ودعم تطبيق سياسات أمن المعلومات بحسب المعايير ومتطلبات الحماية الدولية
7. فرض الرقابة على تطبيق السياسات والامتثال لمعايير حماية وسلامة المنظمات.

تحديث البنى التحتية للمنظمات والانتقال بتصاميم الشبكات التقليدية

إلى التصاميم المبنية على معايير أكثر حماية لمواكبة تهديدات الأمن السيبراني

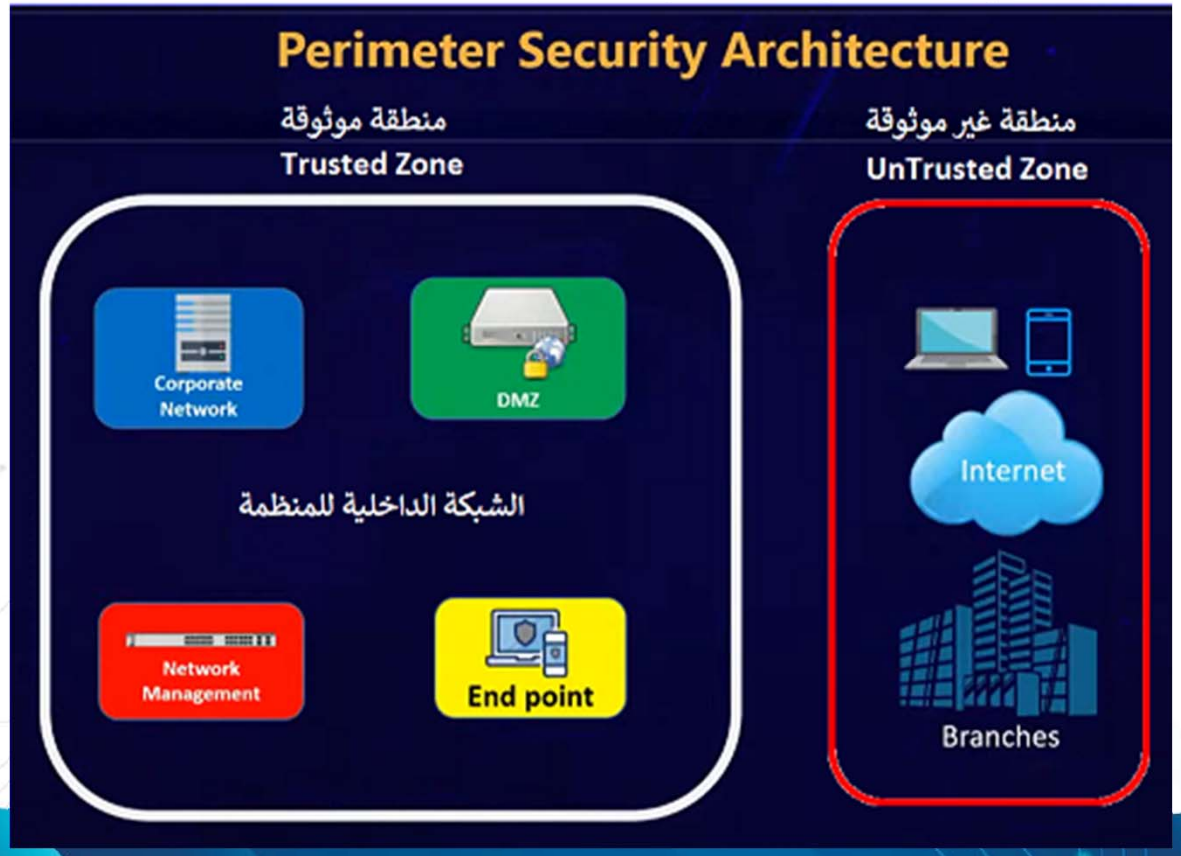
مخاطر تصاميم الشبكات التقليدية

- وحلول التقنيات الحديثة لحماية شبكات المنظمات
- Zero Trust

تحديات الأمن السيبراني على مستوى - الهاتف النقال - وشبكات المنظمات

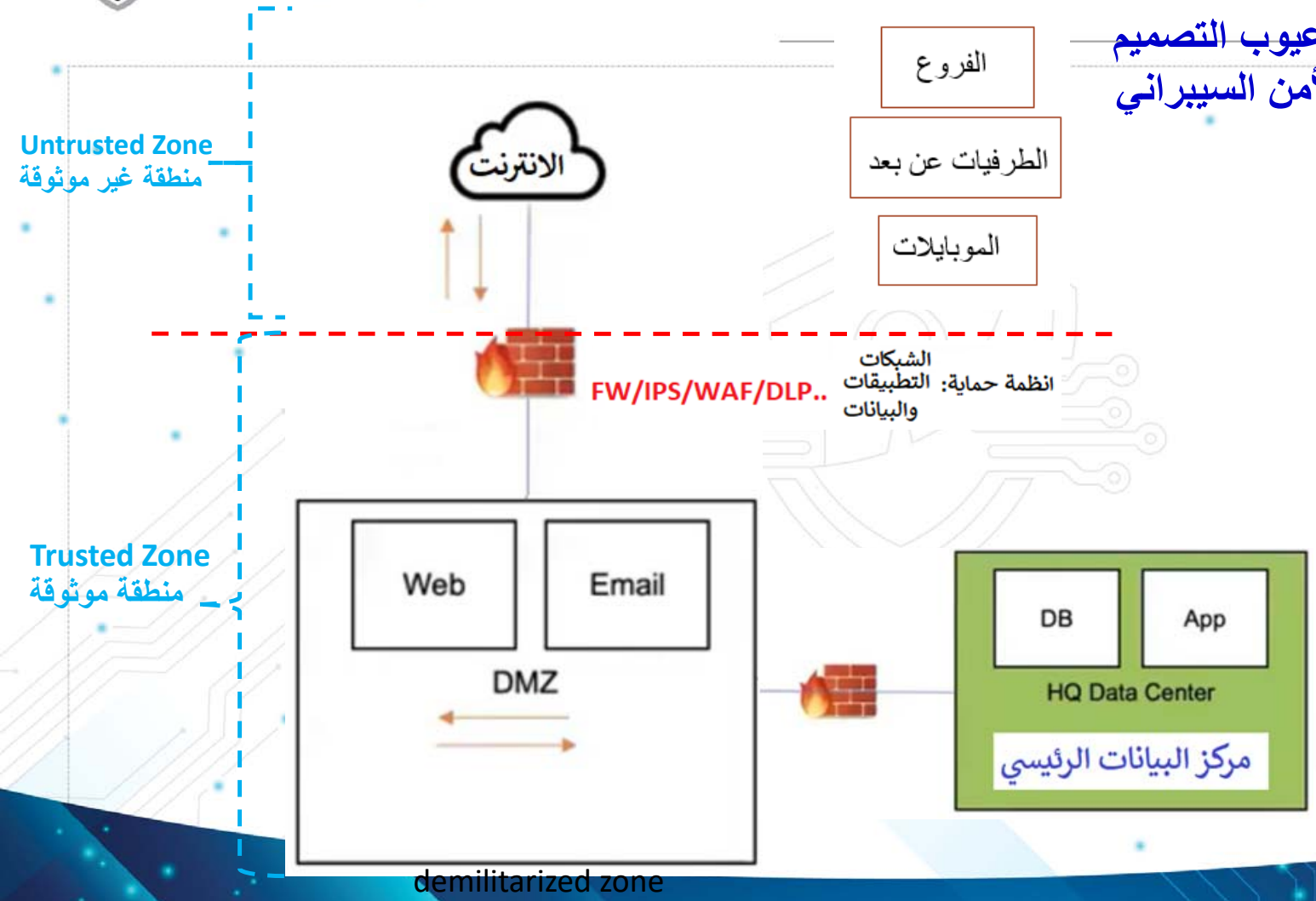
وضع الشبكات التقليدية وعيوب التصميم بعد تطور هجمات الأمن السيبراني

التي كانت تعتمد على الحد الفاصل (Perimeter) بين الشبكة الداخلية والشبكات الخارجية

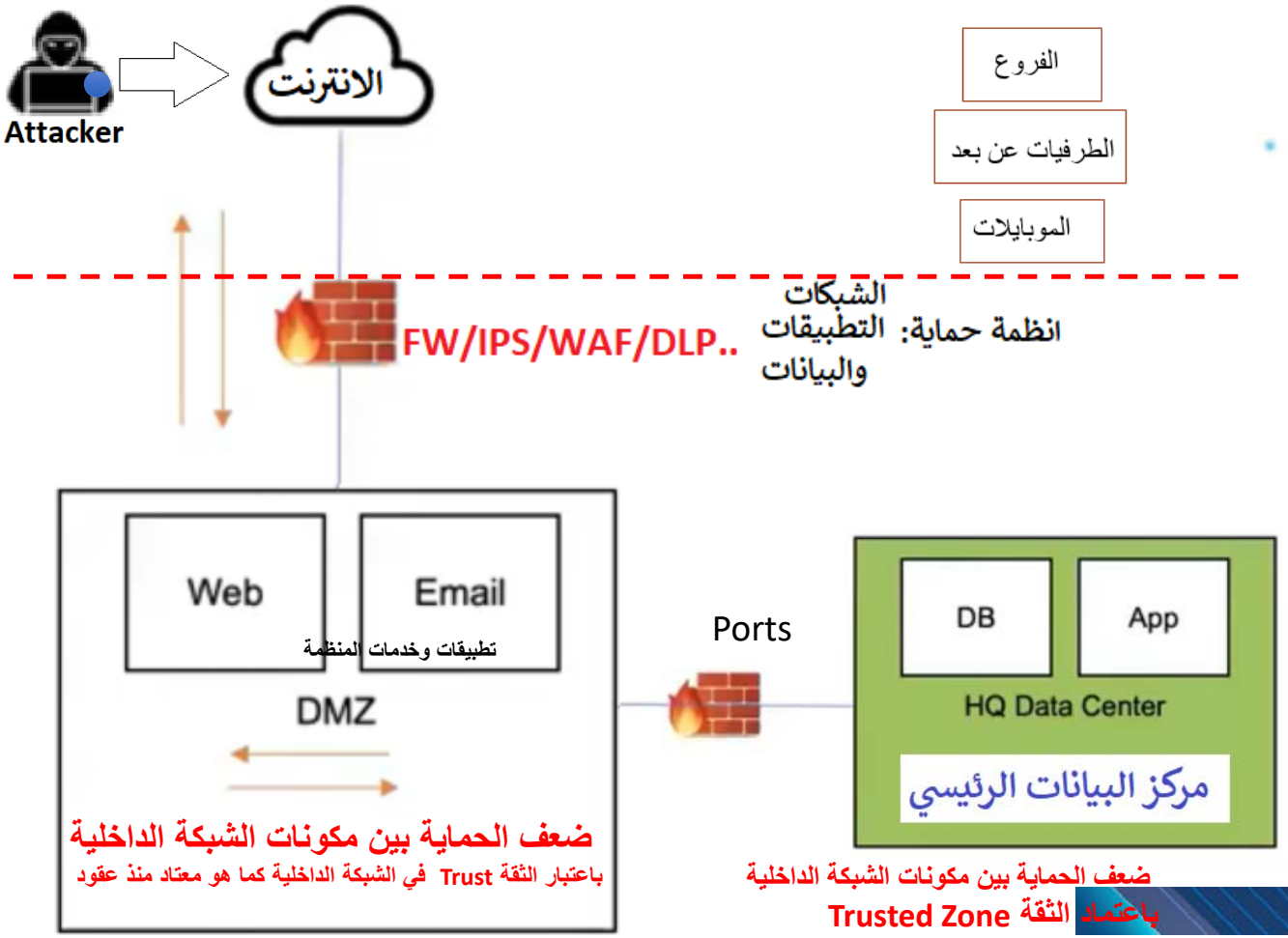


تحديات الأمن السيبراني على مستوى - الهاتف النقال - وشبكات المنظمات

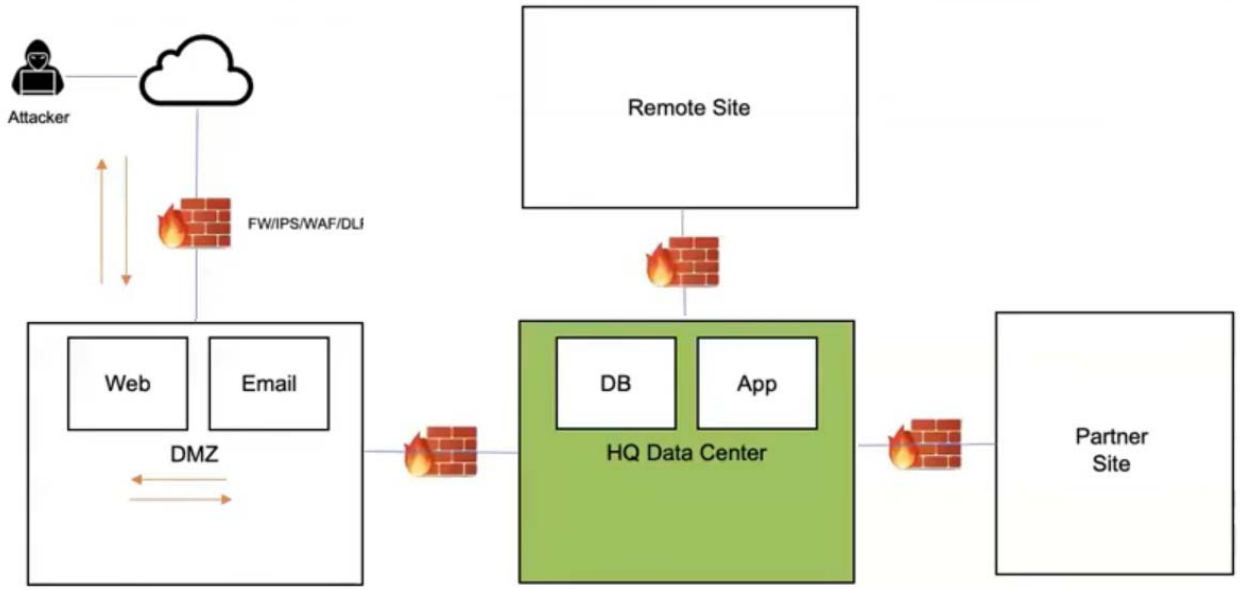
وضع الشبكات التقليدية وعيوب التصميم بعد تصاعد حدة هجمات الأمن السيبراني



تصميم الشبكات التقليدية ومخاطر ومتطلبات الأمن السيبراني



Traditional Network Security



What is bad about Traditional Network Security Approach?

- **The big problem : Internal Access is trusted by default**
- **Lateral movement is possible**
- **Insider threat not considered**

What is Zero Trust ?

What is the approach?

Zero Trust is a strategic or concept that helps prevent successful data breaches by eliminating the concept of trust from an organization's network architecture.

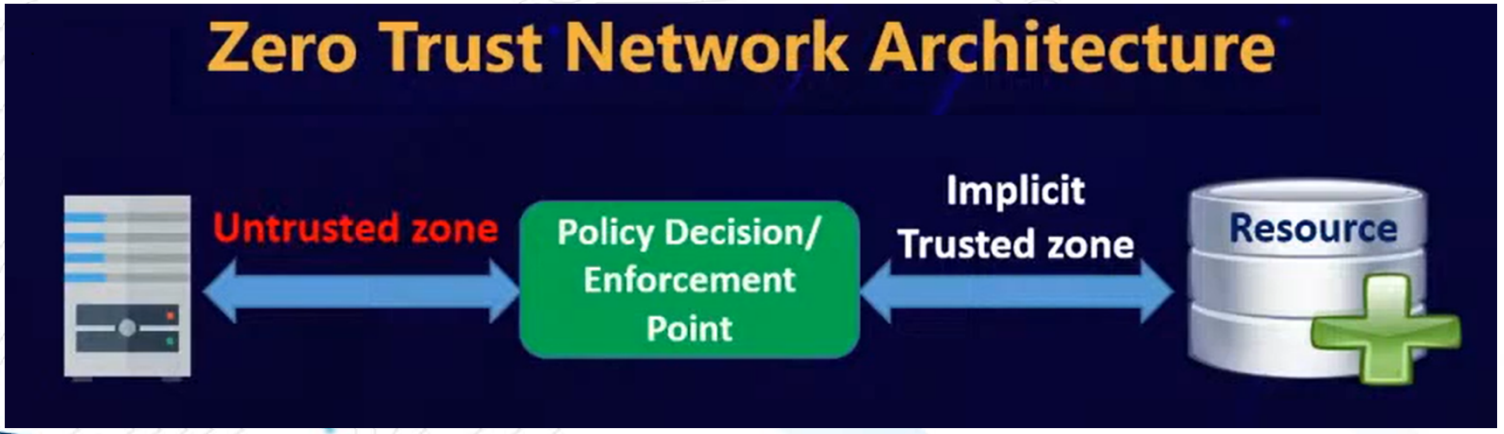
It is a concept , NOT a Technology or device

The concept is:

Do not trust anything, verify everything

مفهوم تصميم الـZero Trust في حماية الشبكات

- كل مكون في الشبكة هو عبارة عن Resource
- يجب حماية كل المكونات(Resources) بحسب مبدأ الـZero Trust.
- كل من يحاول الوصول إلى أي Resource يعتبر Untrusted



What the core of Zero Trust Architecture(ZTA)?

ZTA core components typically include:

Control Plane:

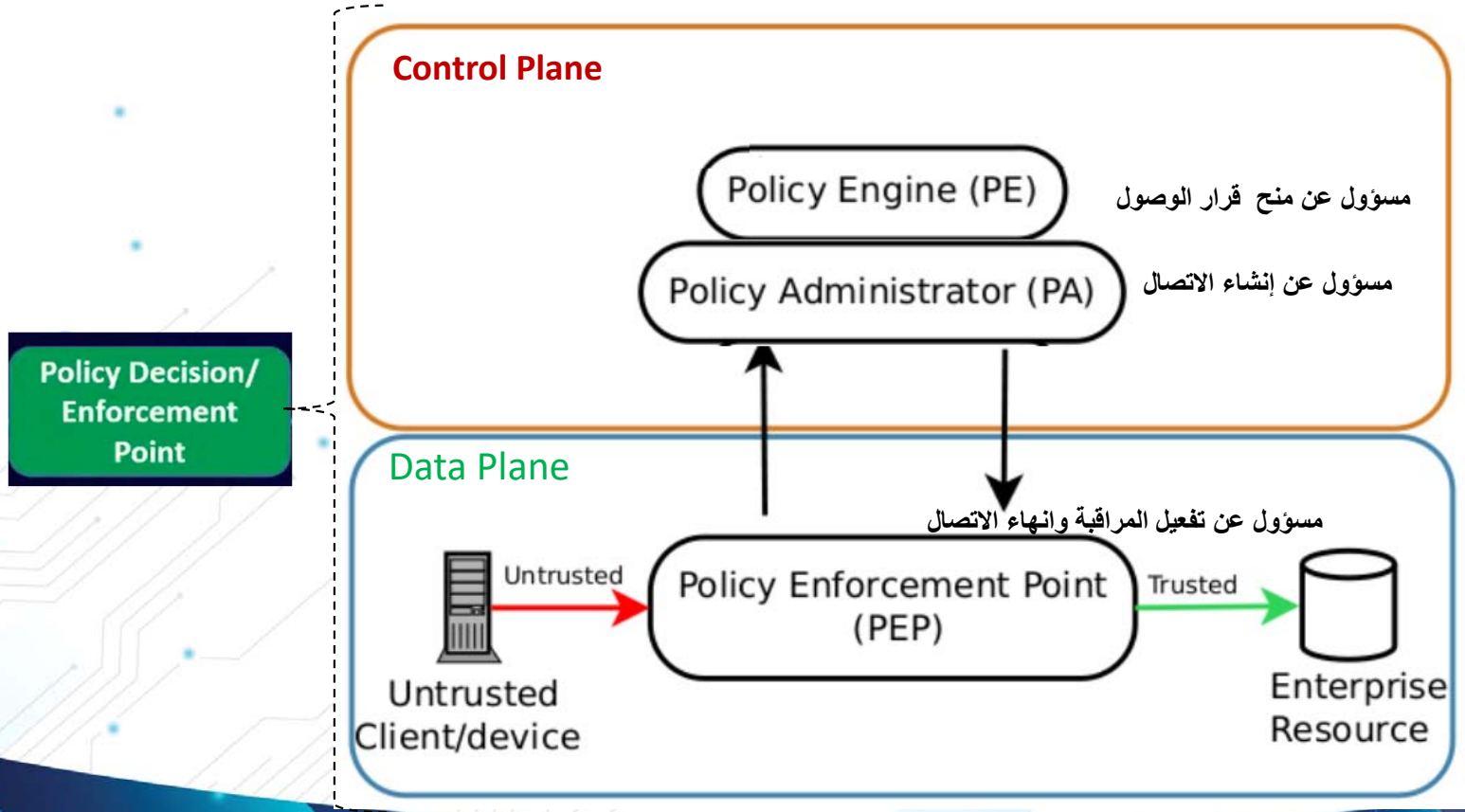
A **policy engine (PE)** مسؤول عن منح قرار الوصول

A **policy administrator (PA)** مسؤول عن إنشاء الاتصال

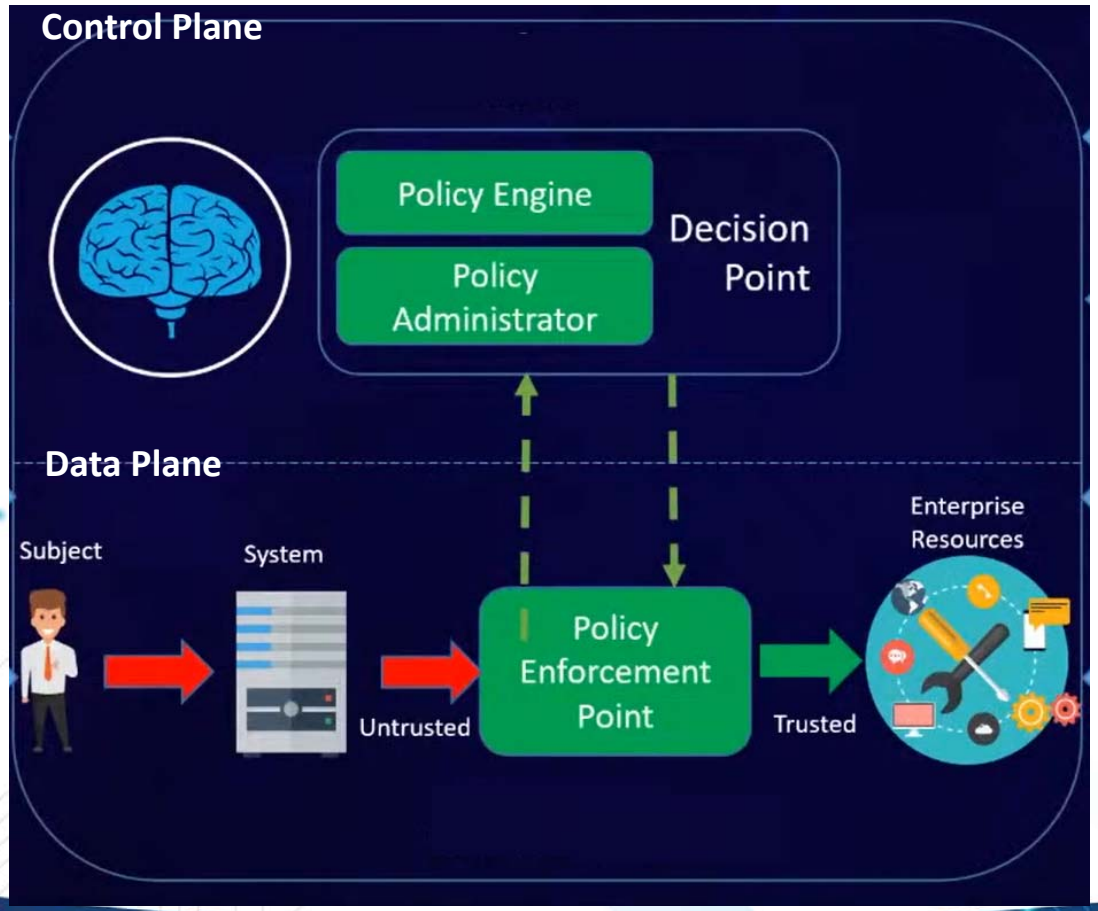
Data Plane:

A **policy enforcement point (PEP)** مسؤول عن تفعيل المراقبة وانهاء الاتصال

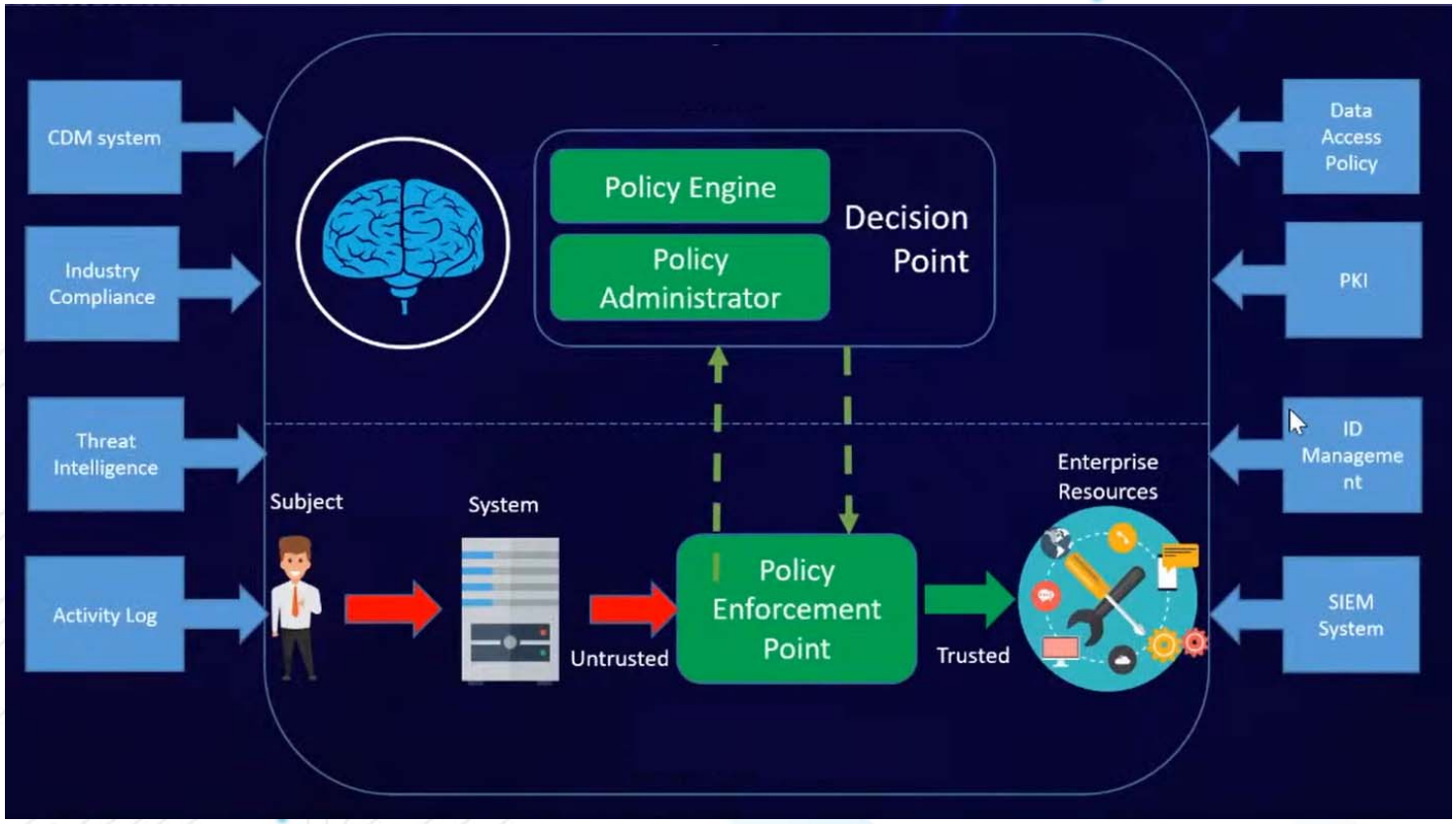
Zero Trust Logical view



Zero Trust logical Architecture



Zero Trust Logical Architecture



Zero Trust Concept

- تمر جميع الإتصالات عبر segregation gateway كبوابة للتحقق وفحص طلب الاتصال وإتخاذ القرار برفض أو قبول طلب الاتصال

- في حال قبل الاتصال يتم توجيهه بصلاحيات حسب مبدأ الـLeast privilege الى Resource محدد.

- تستمر عملية المراقبة والتوثيق للاتصال والـsession وأي تغيير قد يؤدي لقطع الاتصال بالشبكة بحسب متطلبات الحماية القصوى وعدم الثقة Zero Trust.

توجد أنواع من نماذج التطبيق تعتمد على بنية شبكة المنظمة

يمكن أيضا تطبيق أكثر من نموذج بحسب طبيعة أنشطة المنظمة.

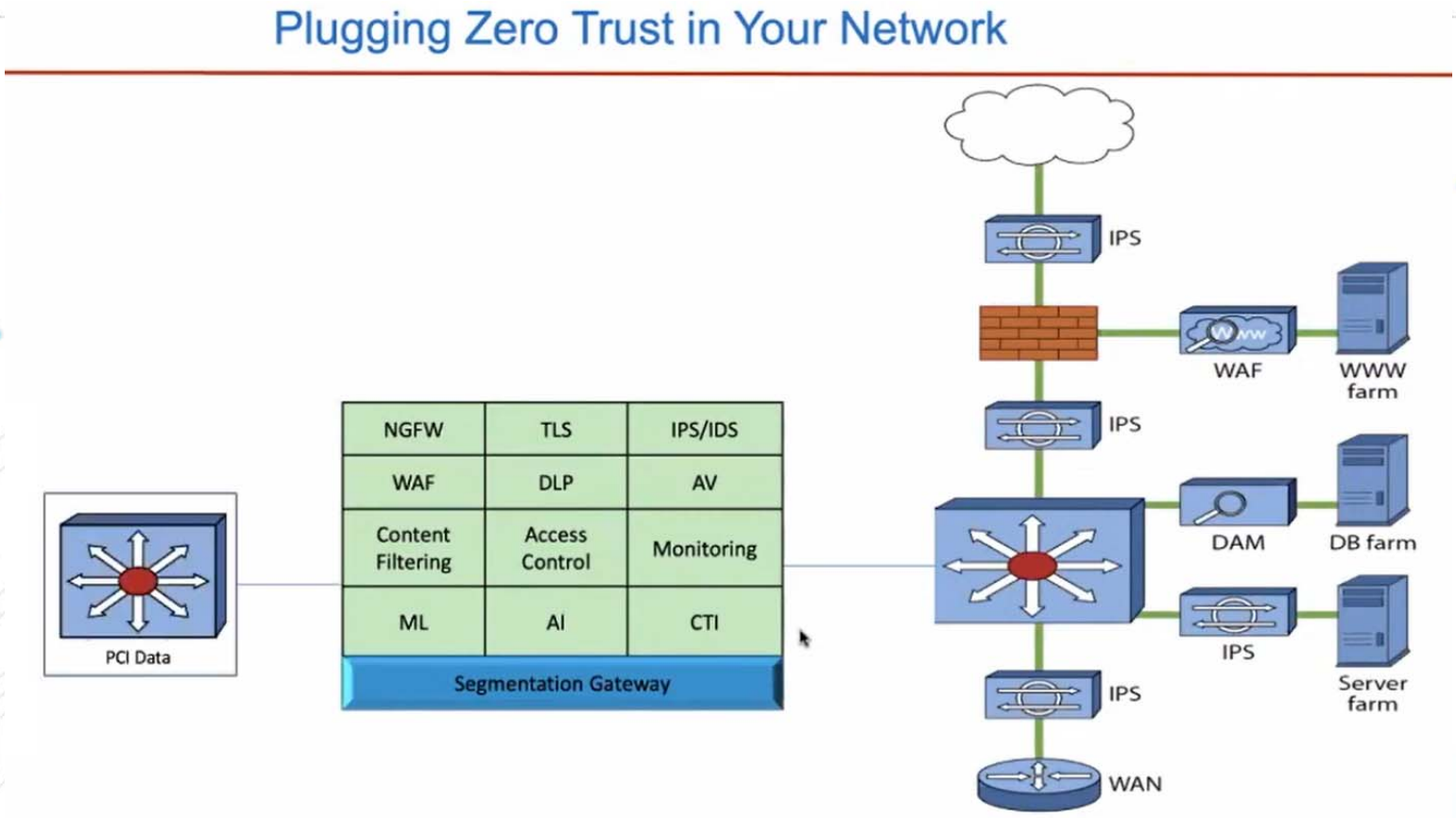
Variations of Zero Trust Architecture Approaches

- ZTA Using Enhanced Identity Governance
- ZTA Using Micro-Segmentation
- ZTA Using Network Infrastructure and Software Defined Perimeters

Variations of Zero Trust Architecture Approaches depending on how an enterprise network is set up, multiple ZTA deployment models may be in use for different business processes in one enterprise.

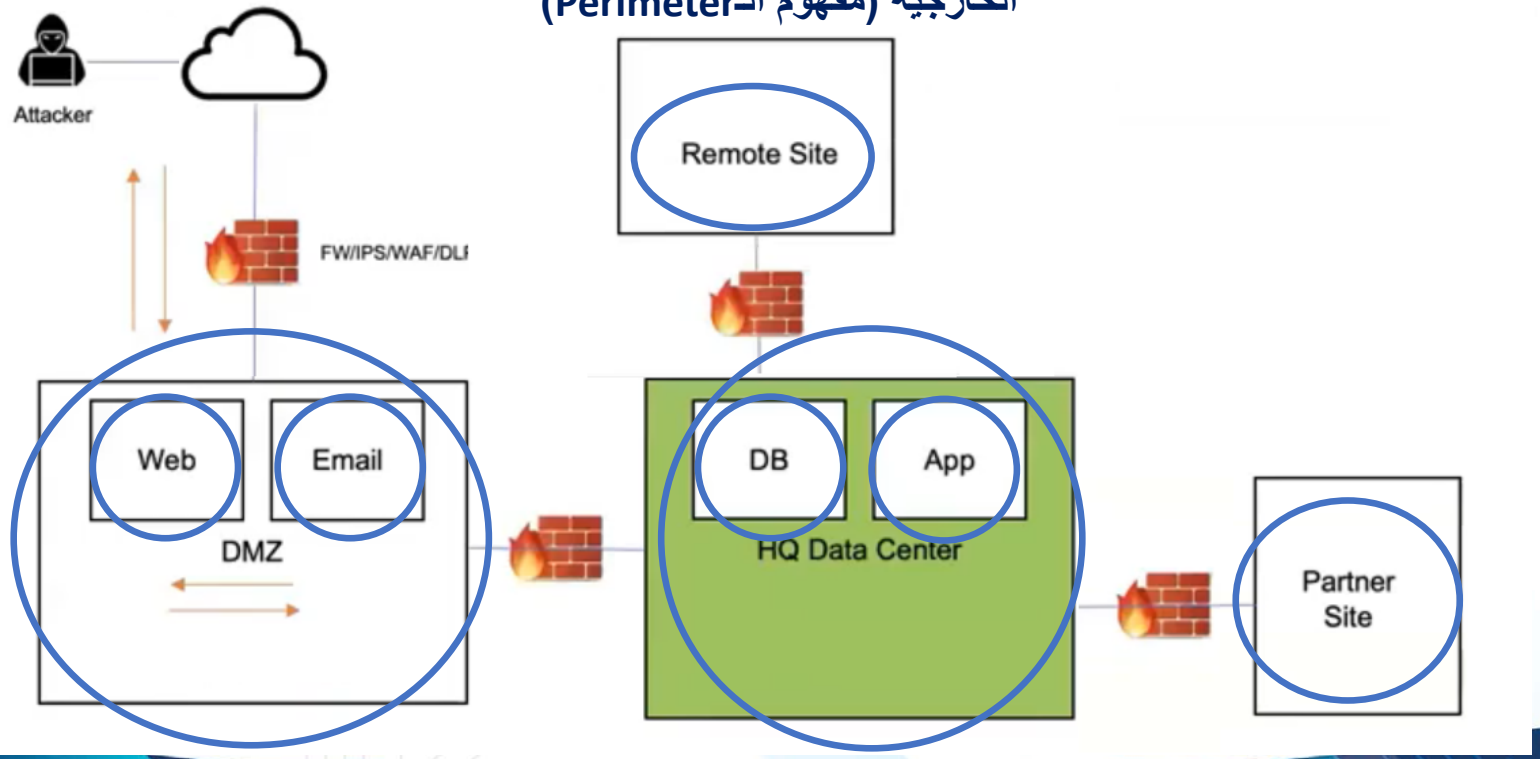
تحديات الأمن السيبراني على مستوى - الهاتف النقال - وشبكات المنظمات

NGFW	TLS	IPS/IDS
WAF	DLP	AV
Content Filtering	Access Control	Monitoring
ML	AI	CTI
Segmentation Gateway		

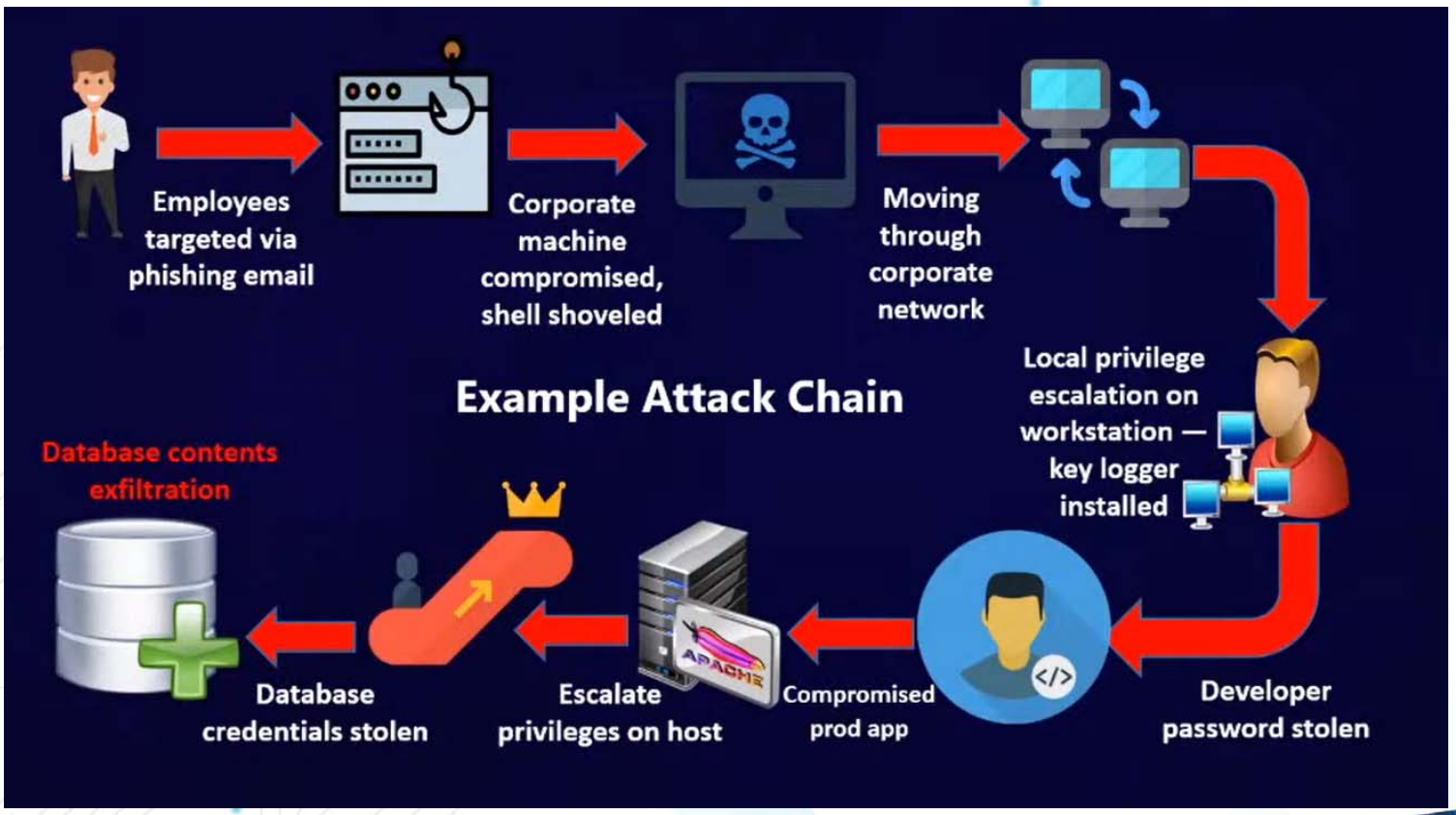

Plugging Zero Trust in Your Network
PCI Data
NGFW
TLS
IPS/IDS
WAF
DLP
AV
Content Filtering
Access Control
Monitoring
ML
AI
CTI
Segmentation Gateway
IPS
WAF
WWW farm
IPS
DAM
DB farm
IPS
Server farm
IPS
WAN

Zero Trust Security

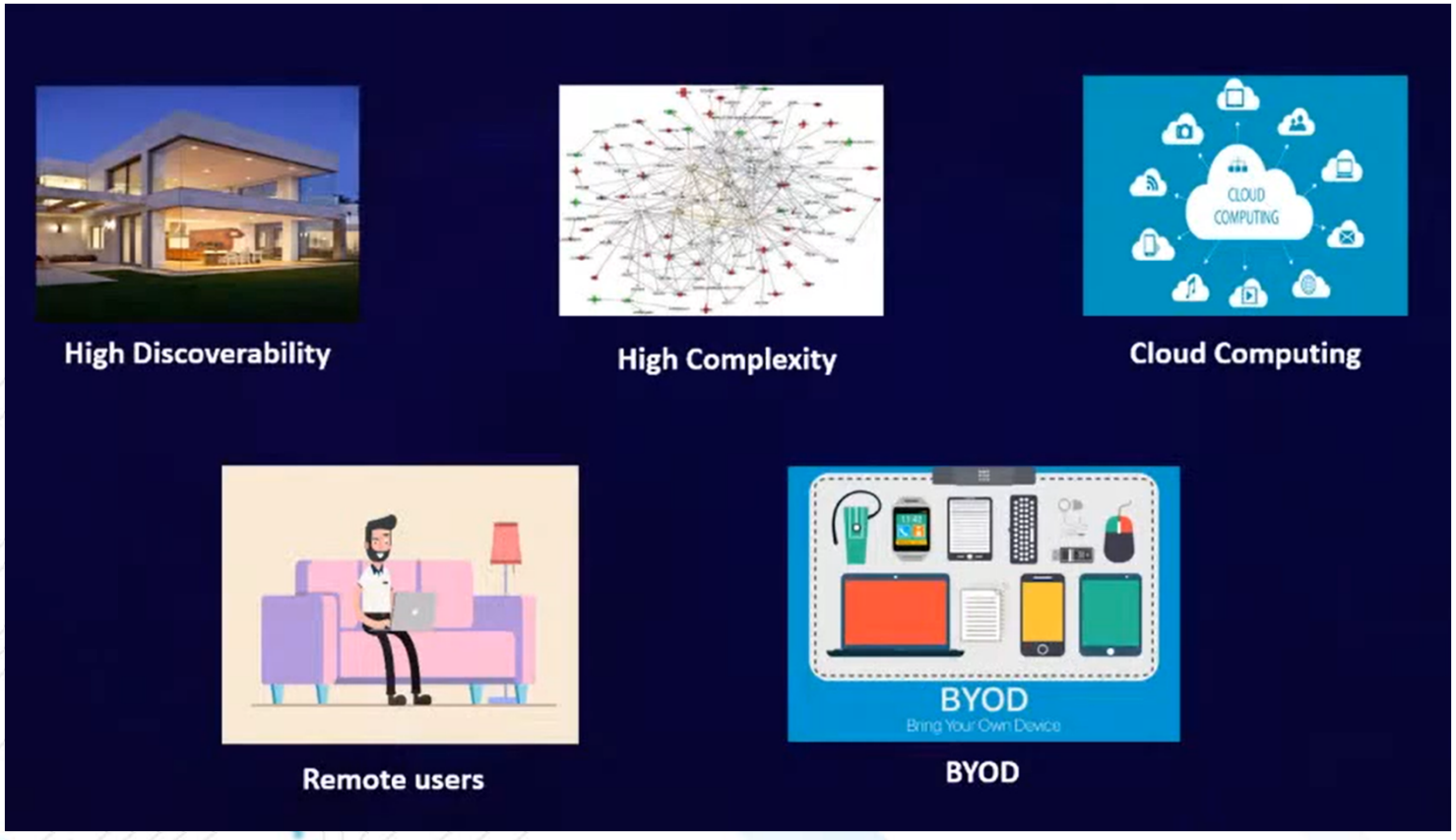
تكون النتيجة حماية كل المكونات داخل إطار الشبكة الداخلية بمنطق الـUntrust بنفس حماية حدود الشبكة الخارجية (مفهوم الـPerimeter)



أهمية التحول نحو الـ Zero Trust



تحديات التحول نحو الـZero Trust



سؤال : هل يمكن تطبيق هذ المبدأ Zero Trust في جوانب أخرى؟

بعض أهم المصادر:

Zero Trust Architecture: NIST Publishes SP 800-207
https://csrc.nist.gov/publications/detail/sp/800-207/final

EWG6464$1^ivs$Xvywx$Q ship$sj$G}fiwigyvmx}$1Elq ih$Efhipleq m
lxxtw>33{{{2}syxyfi2gsq3{exglCzA=HRQ=U;Jn:s*efcglerripAEvefWigyvmx}Gsrjivirgi

Zero Trust : A Technical Implementation Guide - AbdulrahmanAl-Nimari
https://www.youtube.com/watch?v=ckn7tdj8TxA&ab_channel=AbdulrahmanAl-Nimari
lxxtw>33{{{2}syxyfi2gsq3{exglCzA<ZYEq SFjtNM*xA66;9w