

التقرير السنوي  
**للتحديات  
السيبرانية**

لعام 2022



# المحتويات

مقدمة	01
الهجمات الأكثر شيوعًا في العالم	02
الإحصائيات السعودية	03
معارك sirar	04
الاستنتاجات الرئيسية	05
تعريف مصطلحات sirar	06
المراجع	07

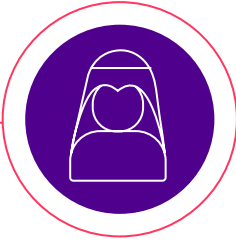
# المقدمة

01



# مقدمة

## المنصة الموثوقة لاقتصاد البيانات



### شركة سعودية

لأننا شركة سعودية 100%، فنحن لا نتأثر بالقيود المفروضة على الشركات الاستشارية الأجنبية.



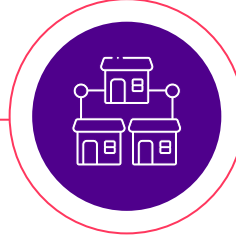
### منظومة شراكات قوية

نظام مبني على بيئة شراكات على أعلى المستويات يمكننا من تقديم الحلول التي تلبي احتياجاتك.



### فريق يمتلك كفاءة عالية

فريقنا بمعدل خبرة 15 عام، في كبرى الجهات العالمية والمحلية.



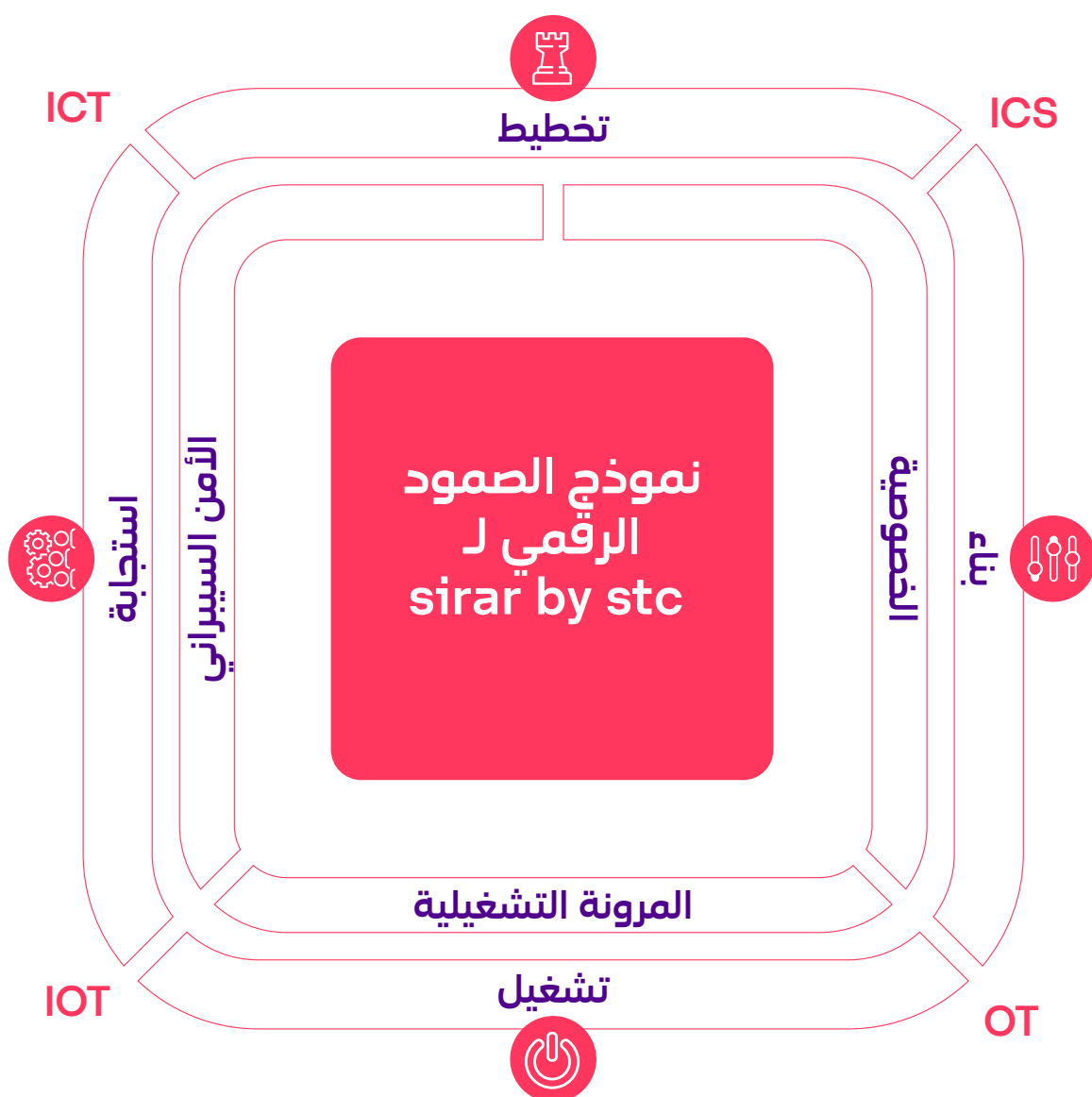
### متجر متكامل

نقدم كل ما تحتاجه الجهة من خدمات الخصوصية والحماية والأمان والصمود و توفر الوقت المبذول للتنسيق بين الموردين.



# حماية مبنية على البيانات الإستباقية

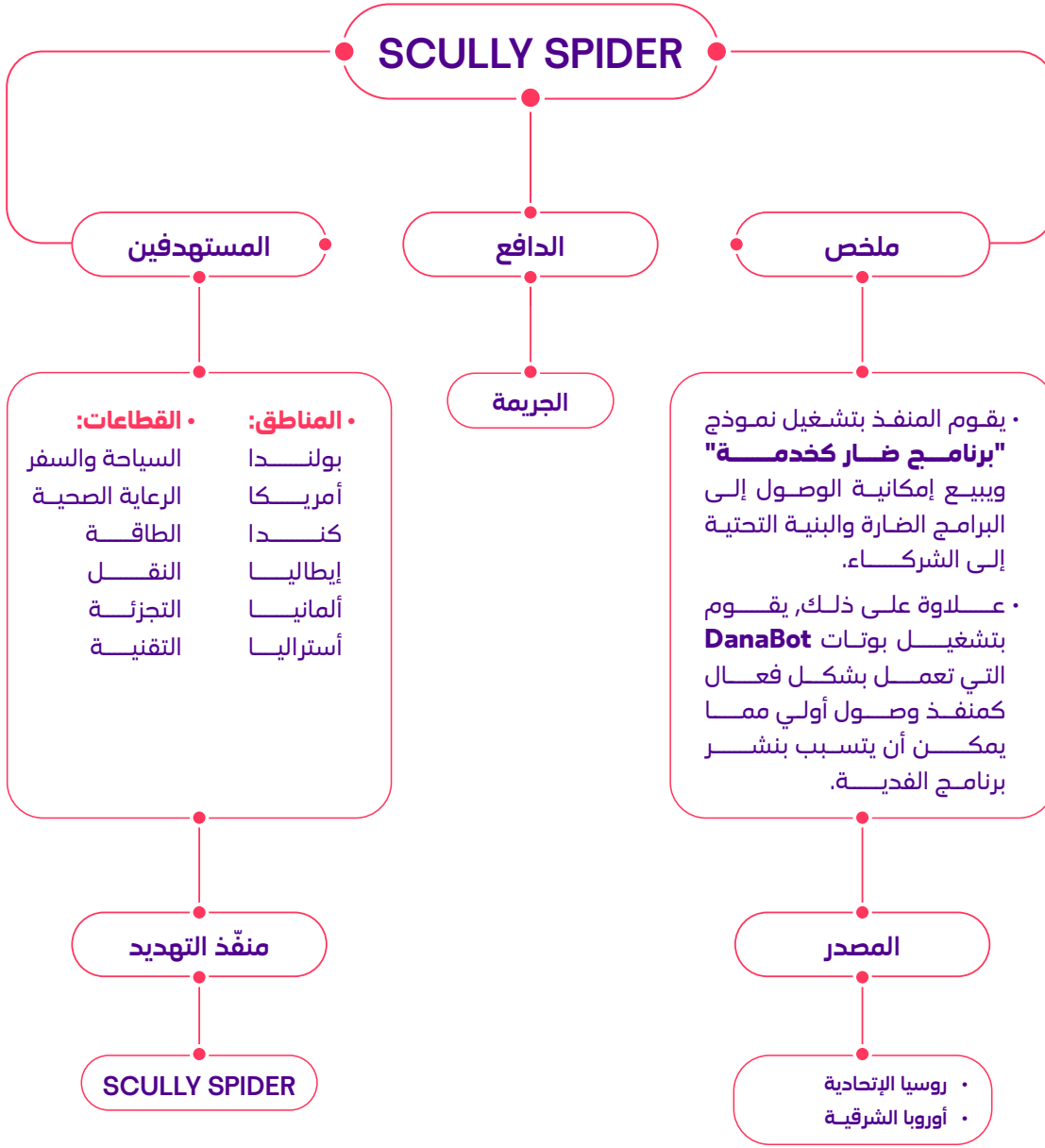
نوفر خدمة المعلومات الإستباقية للتهديدات على أعلى المستويات لما نمتلكه من خبرة واسعة لمشهد التهديدات محلياً وإقليمياً



# الهجمات الأكثر شيوعًا في العالم

02

# أكثر التهديدات المتقدمة والنشطة عالمياً



منفذ التهديد من روسيا وأوروبا



تشير إلى التهديد المتقدم والمستمر

# أكثر التهديدات المتقدمة والنشطة عالمياً

## ToddyCat

### المستهدفين

الحكومة  
القطاع العسكري  
أوروبا  
آسيا

### منفذ الهجوم

ToddyCat

### ملخص

يستهدف **ToddyCat** خوادم التبادل وتبدأ باختراقها من خلال تطبيق سلوك إستغلالي غير معروف على مكونات الخادم.

### المصدر

الصين



الموجة الثالثة

الموجة الثانية

الموجة الأولى

منفذ التهديد من الصين



تشير إلى التهديد المتقدم والمستمر



# ثغرة أمنية في Microsoft Exchange (ProxyNotShell)

## Exchange

تم إستغلال ثغرة أمنية خطيرة (ProxyNotShell) في Microsoft Exchange سمحت بتنفيذ الرمز البرمجي عن بعد. وذلك بحسب الشكاوي التي قدمت من قبل باحثين فيتناميين في جهاز الأمن السيبراني الفيتنامي GTSC وهم أول من كشف الهجمات وأبلغ عنها.

### الإصدار المتأثر

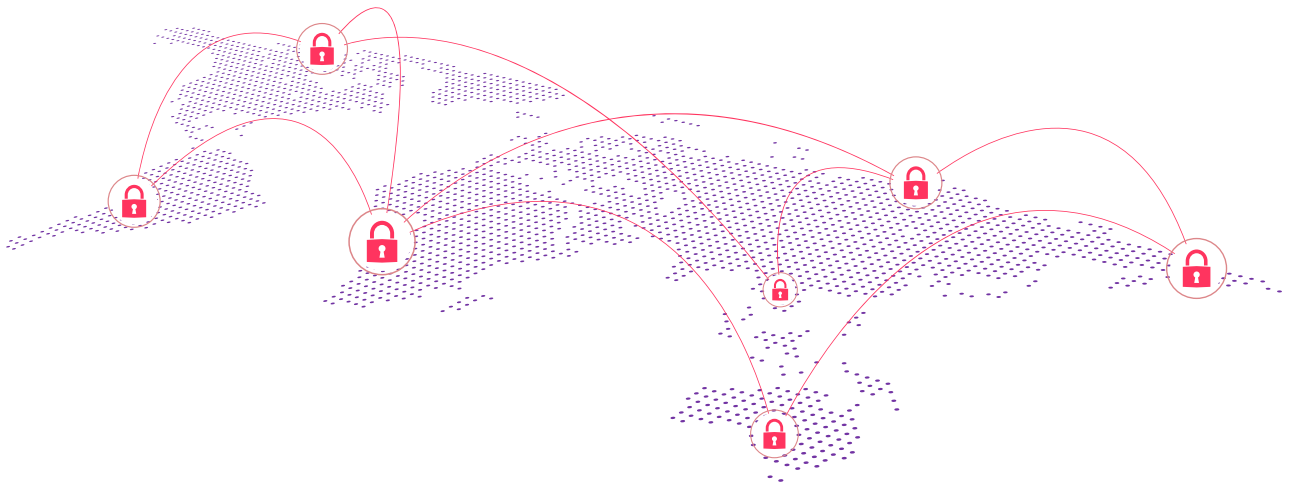
- Microsoft Exchange 2013
- Microsoft Exchange 2016
- Microsoft Exchange 2019

### MITRE ATT&CK TTPs

- جريمة

### المهاجم

**مجموعة تهديد صينية**  
يشتهر بأنها المسؤولة عن الهجمات بناء على كود web shells.



# تحذر Microsoft من هجمات التصيد والاحتيال في المدفوعات

## Microsoft

كشفت Microsoft عن حملة تصيد احتيالي واسعة النطاق تستهدف أكثر من 10000 منظمة وذلك من خلال الإستيلاء على إجراء المصادقة لـ Office 365. حيث يتم إستخدام بيانات مسروقة وملفات ارتباط للوصول الى صناديق بريد المستخدمين المتأثرين لإجراء احتيال في المدفوعات باستخدام تقنية تسمى الاستيلاء على البريد الإلكتروني للضداع.

## التفاصيل التقنية:

**منفذ التهديد:** غير معروف  
**ناقلات التهديد:** موقع تصيد احتيالي  
**التأثير:** بيانات وملفات ارتباط مسروقة, احتيال في المدفوعات  
**الخطورة:** عالية

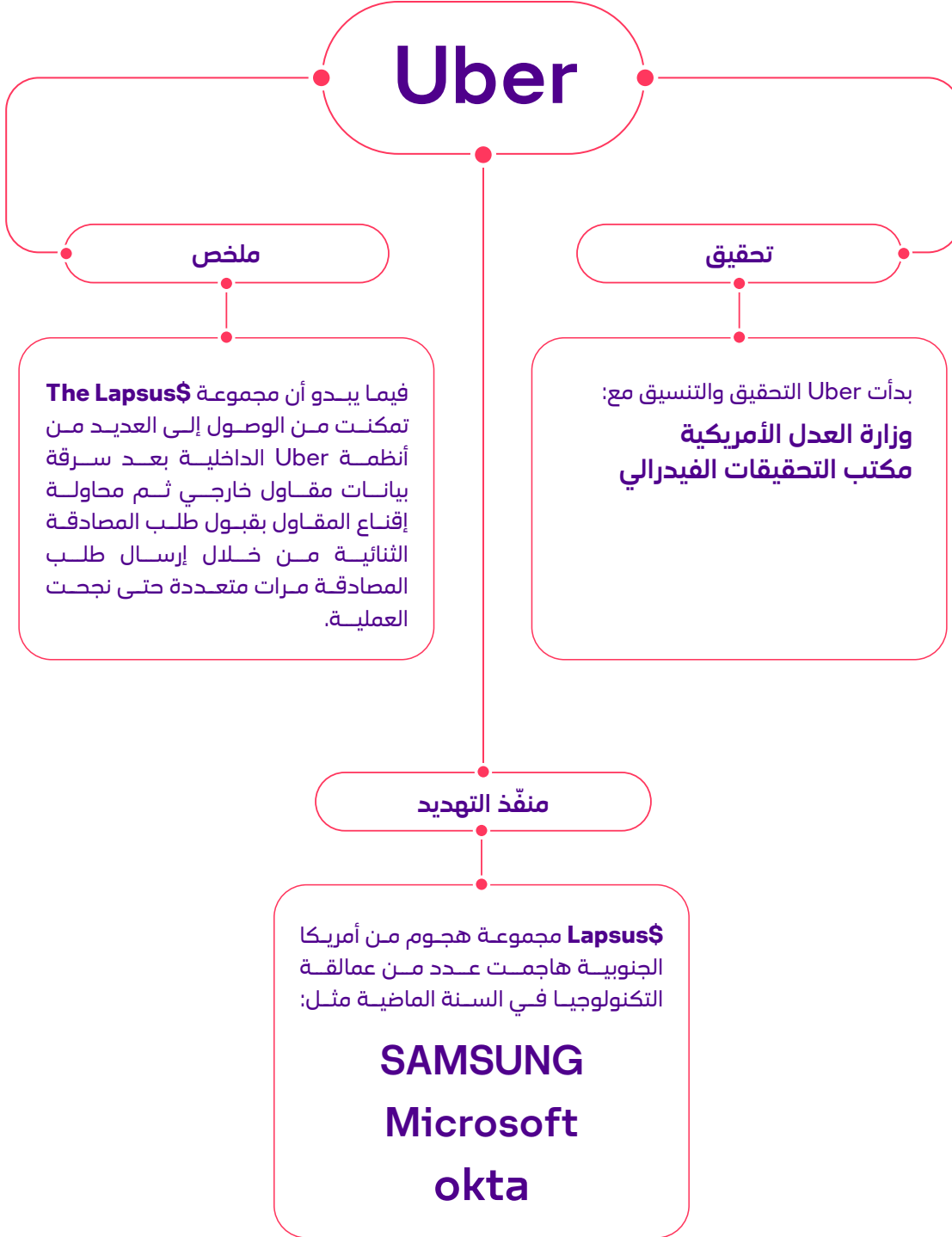


Figure 1: Attacker Action Flow.



Figure 2: Phishing sample.

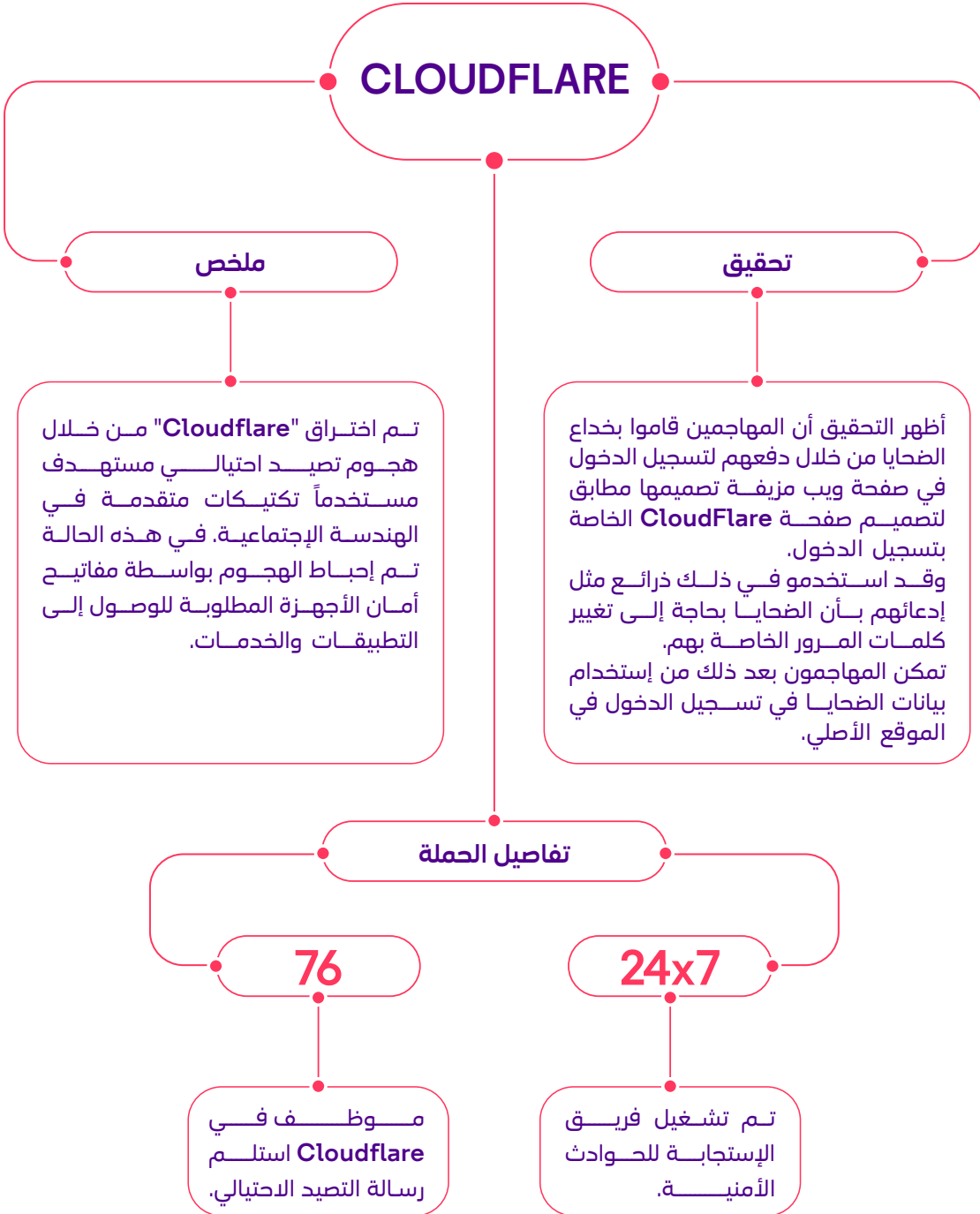
# اختراق الشبكة الداخلية لـ Uber



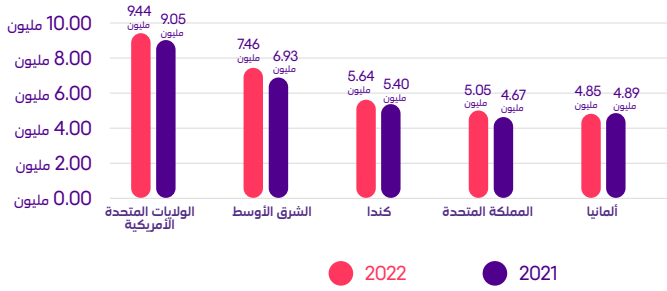
# استهداف شركة Cisco



# حملة تصيد مسجلة على Twilio & Cloudflare



# الاختراق السيبراني للبيانات إحصائيات 2022



متوسط تكلفة اختراق البيانات لأكثر من 5 دول / مناطق

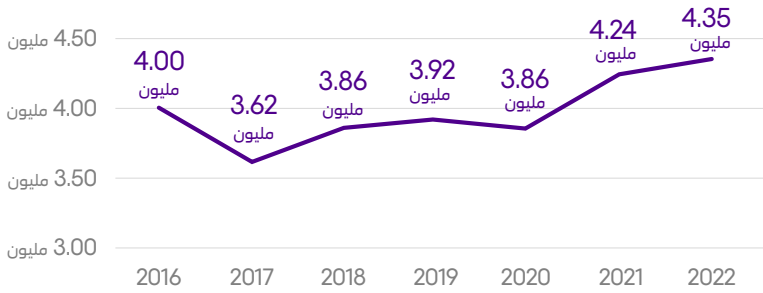
4.24 مليون دولار

هي تكلفة اختراق بيانات السحابة الخاصة في 2022

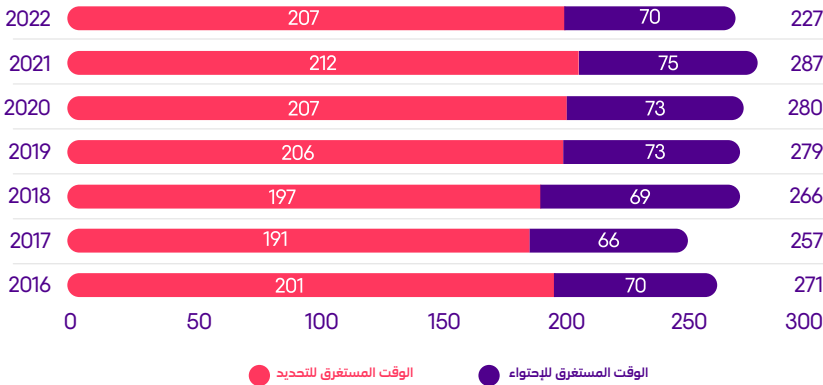
5.02 مليون دولار

هي تكلفة اختراق بيانات السحابة العامة في 2022

تكلفة الاختراقات وأسبابها

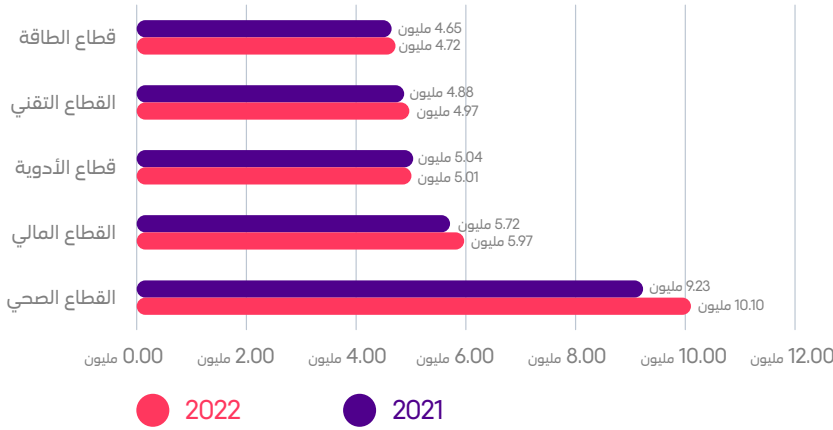


متوسط تكلفة اختراق البيانات

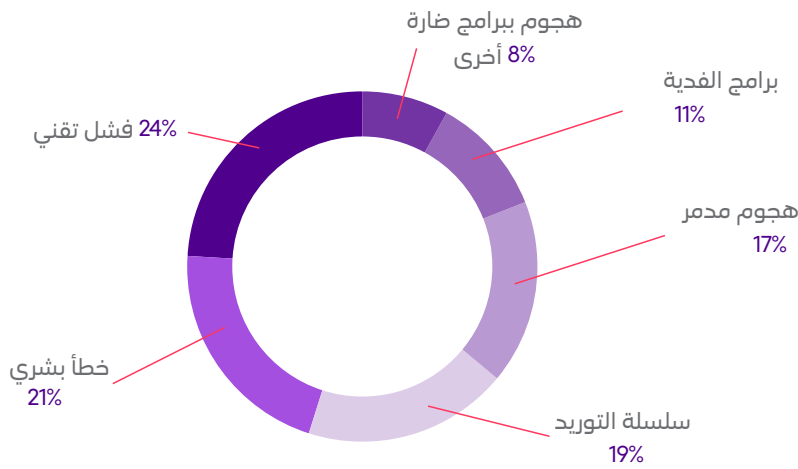


متوسط الوقت المستغرق لتحديد وإحتواء اختراق البيانات

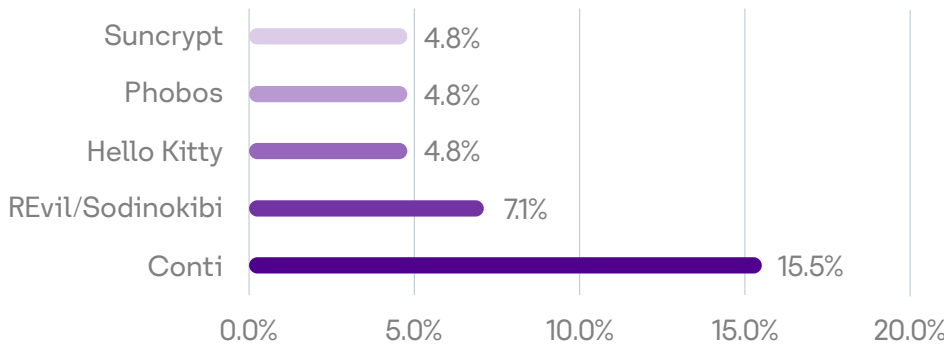
# الاختراق السيبراني للبيانات إحصائيات 2022



متوسط تكلفة  
اختراق البيانات  
لأكبر 5 قطاعات


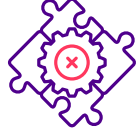





من أنواع  
الاختراقات  
التي تعرضت  
لها المنظمات



أكثر برامج  
الفدية  
نشاطاً

# الهجمات السيبرانية على مختلف القطاعات

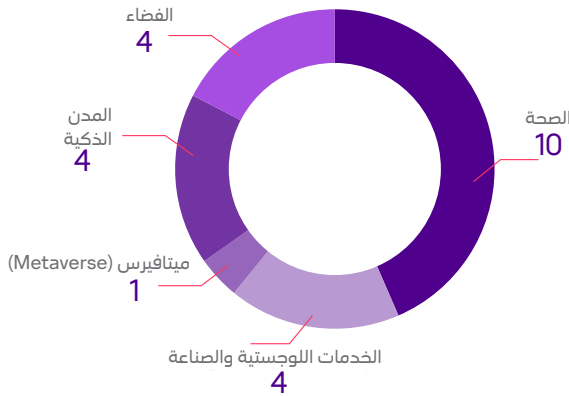
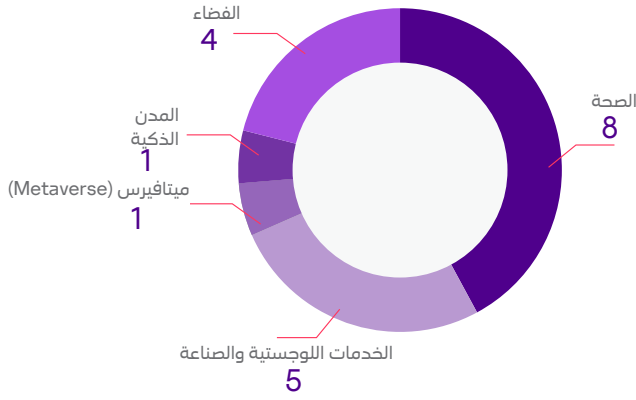
قائمة البرامج الضارة والأدوات	قائمة المنفذين	القطاع
NIGHTROPE BITPAYMER FAKEUPDATES FLASHBANG HANDYAXE SNOWFIRE CASUMARZU CHIPSEAL MIXDOOR SUCCESSFLY	TEMP.Hex UNC2633 UNC2420 UNC2500 UNC3840 APT29 UNC2835 UNC3810	الصحة 
TOUGHQUIZ OLDFLAT ROOMMATE DRABCUBE	UNC1543 UNC2975 UNC2165 FIN11 UNC2824	الخدمات اللوجستية والصناعة 
QUIETEXIT	UNC3524	ميتافيرس (Metaverse) 
CLOP FLOWERPIPE QUICKPEEK SIXFINGERS	FIN11	المدن الذكية 
CLOP INCONTROLLER METEORLIGHT METEOR	GhostSec Gonjeshke Darande UNC4368 Gaza Cybergang	الفضاء 



# الهجمات السيبرانية على مختلف القطاعات

## مؤشر الاختراق حسب القطاع

القطاع	مجموع المؤشرات
الصحة	1,726
الخدمات اللوجستية والصناعة	238
الفضاء	1,899
المدن الذكية	323
ميتافيرس (Metaverse)	7



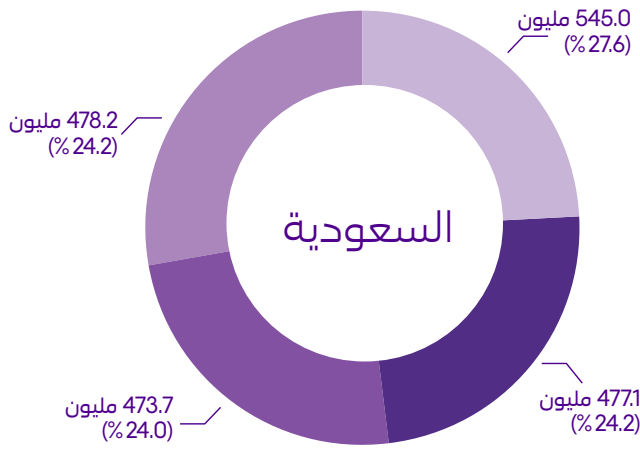
# الإحصائيات الرئيسية

في المملكة العربية السعودية

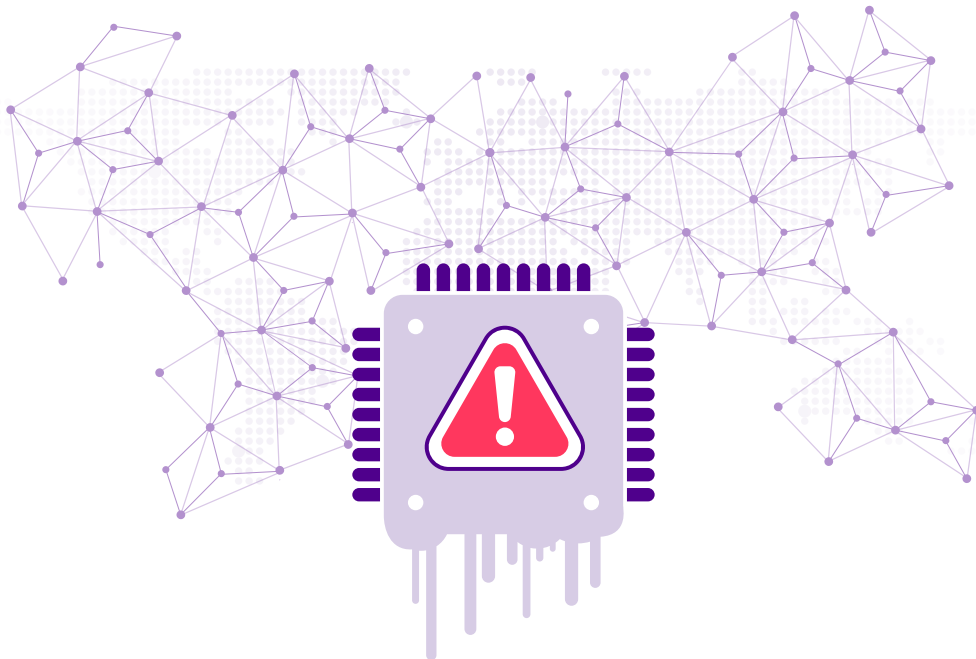
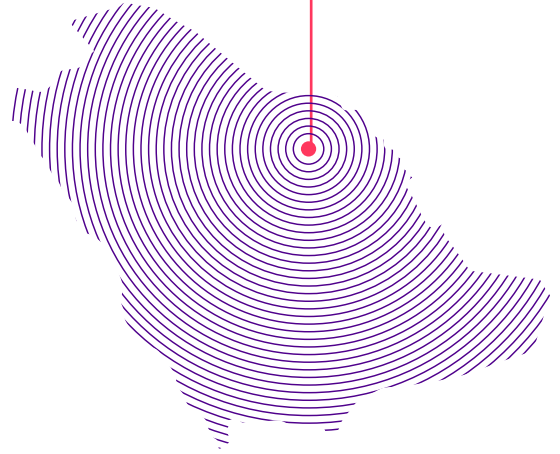
03

# الأنشطة الضارة في المملكة العربية السعودية

السعودية

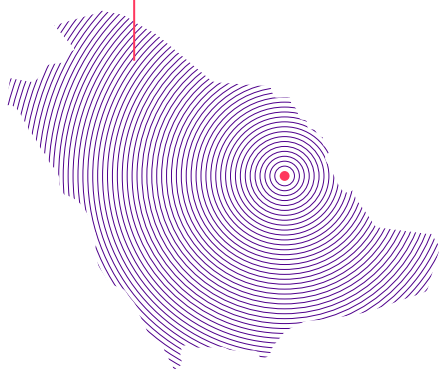


الربع الأول ● الربع الثاني ● الربع الثالث ● الربع الرابع



# محاولات الاستغلال

تقنيات استغلال مكتشفة  
IPS  
1.93 مليار



Log4Shell  
53 مليون



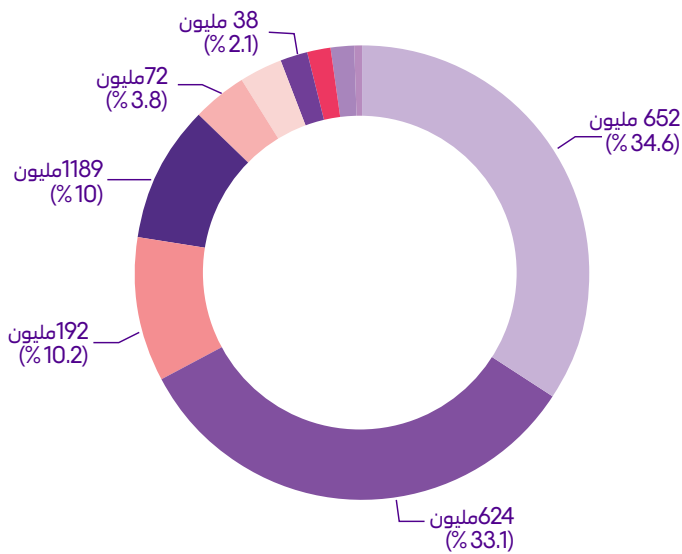
DoublePulsar  
624 مليون



Cross Site Scripting  
3 مليون

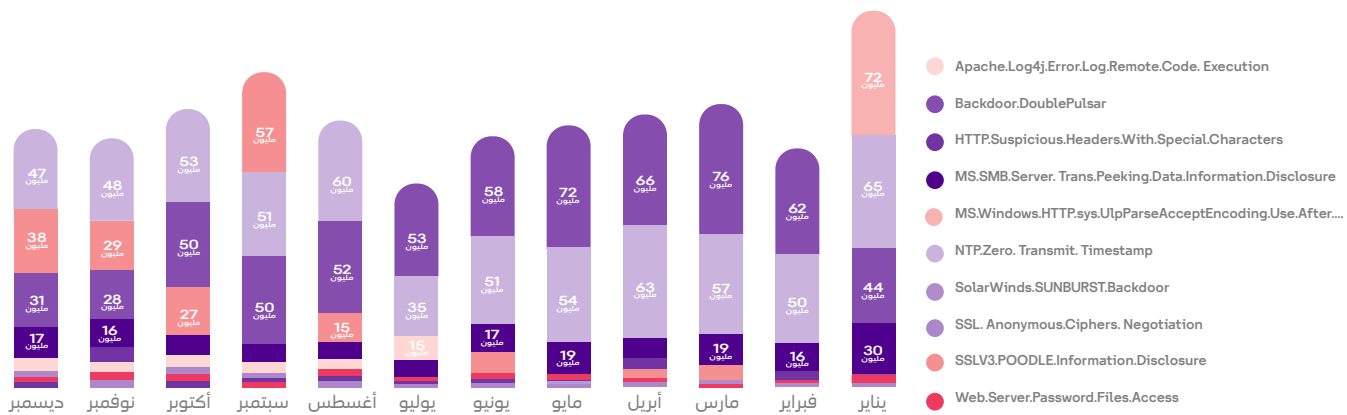


SUNBURTS  
10 مليون



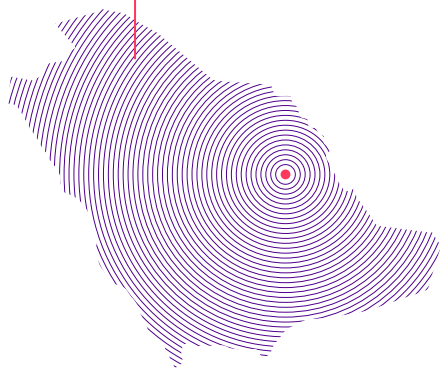
## محاولات الاستغلال موزعة حسب النمط

## تحليل السلوك الأكثر شيوعاً حسب النمط



# إكتشافات البرامج الخبيثة

برامج ضارة موزعة مكتشفة  
AV 10.53 مليون



CryptoMiner  
956 ألف



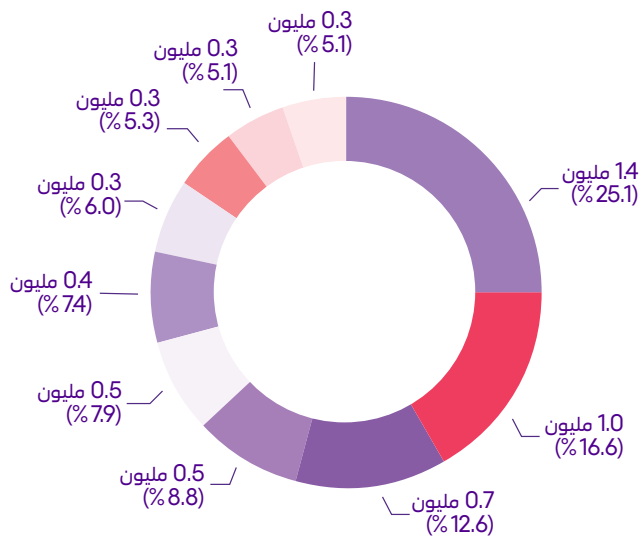
Trojans  
8 مليون



Mal Office Docs  
3 مليون

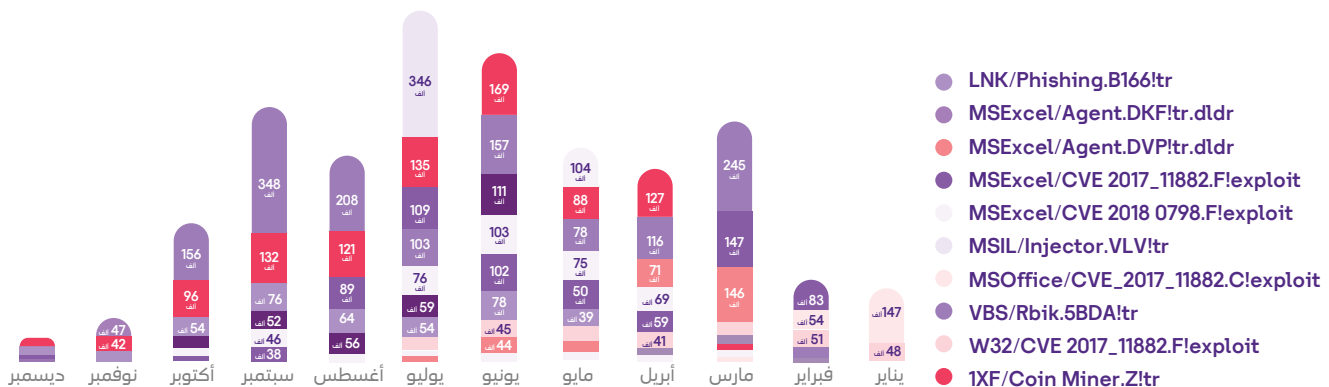


Drive by Download  
1 مليون



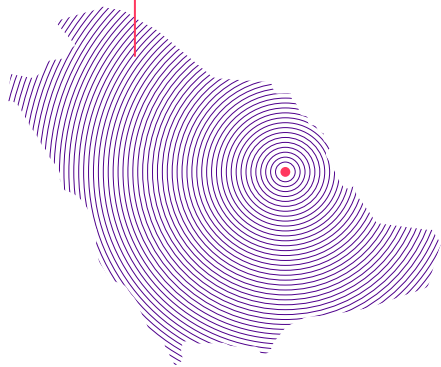
## برامج ضارة موزعة حسب النمط

## تحليل السلوك الأكثر شيوعاً حسب النمط



# نشاط Botnet

C2 أنشطة Botnet مكتشفة  
41.67 مليون



IoT- MIRAI  
1 مليون



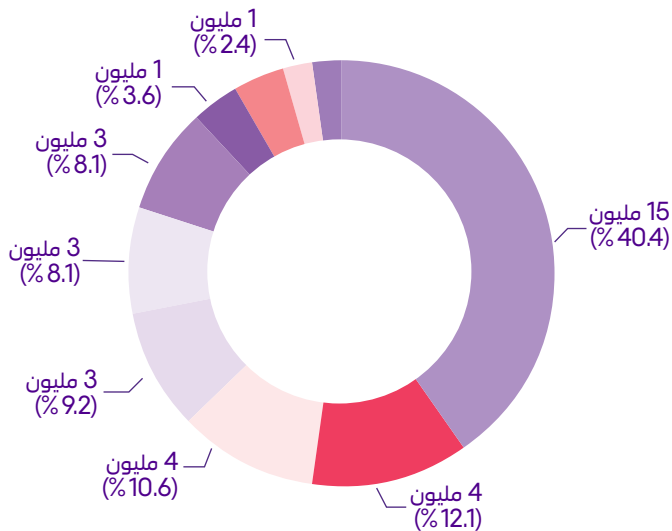
GhOst RAT  
120 ألف



H-Worm  
1 مليون

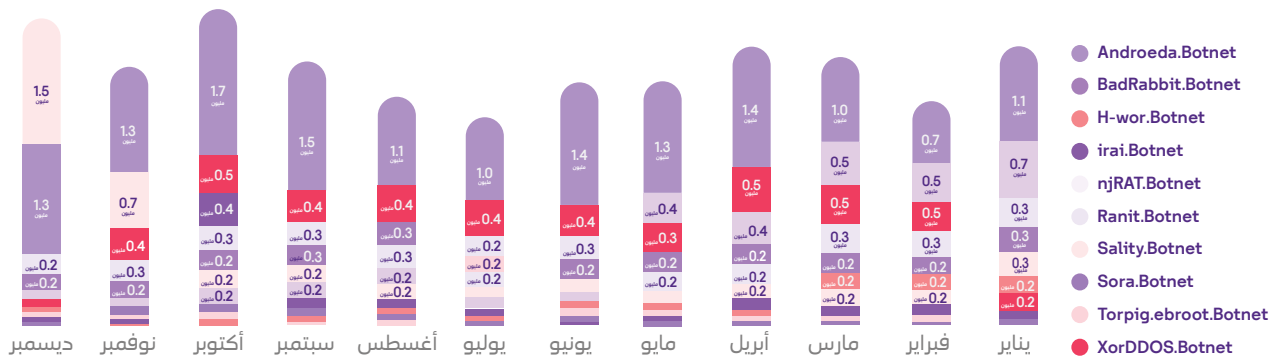


Bad Rabbit  
3 مليون



## Botnet نشاط موزع حسب النمط

## تحليل السلوك الأكثر شيوعاً حسب النمط



# الثغرات الأمنية لأجهزة المستخدم



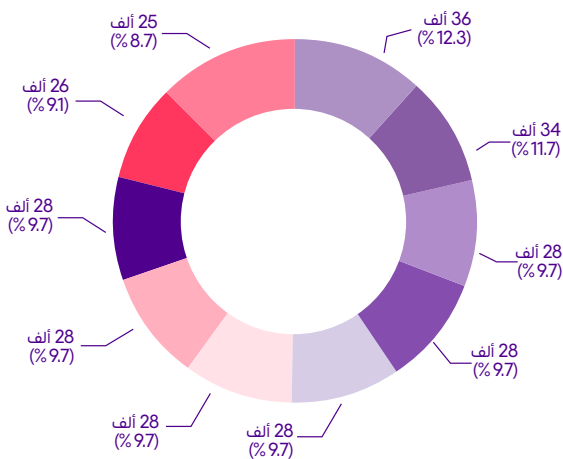
الثغرات الأمنية المكتشفة لأجهزة المستخدمين

1.12 مليون



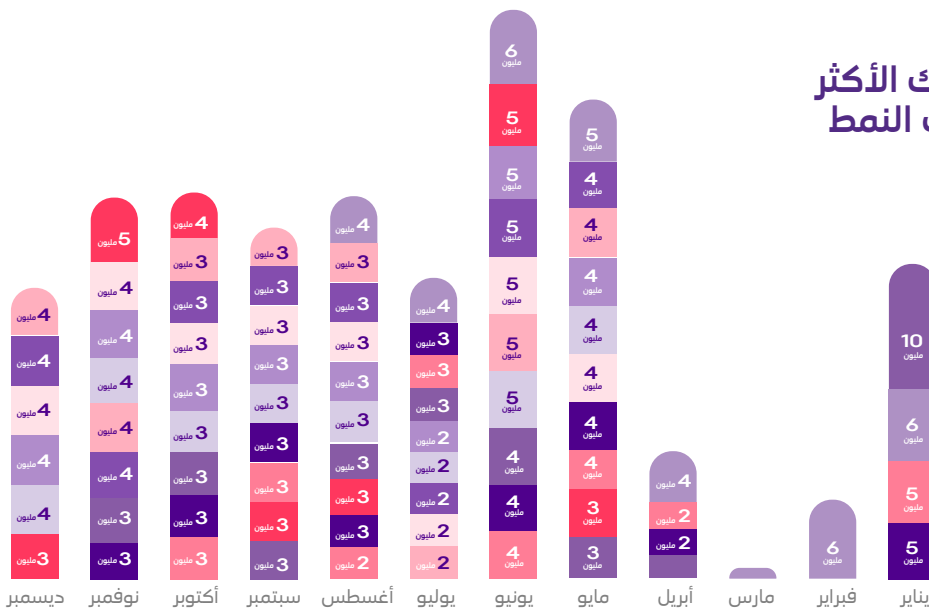
Oracle Vulns  
675 ألف

Log4Net  
34 ألف



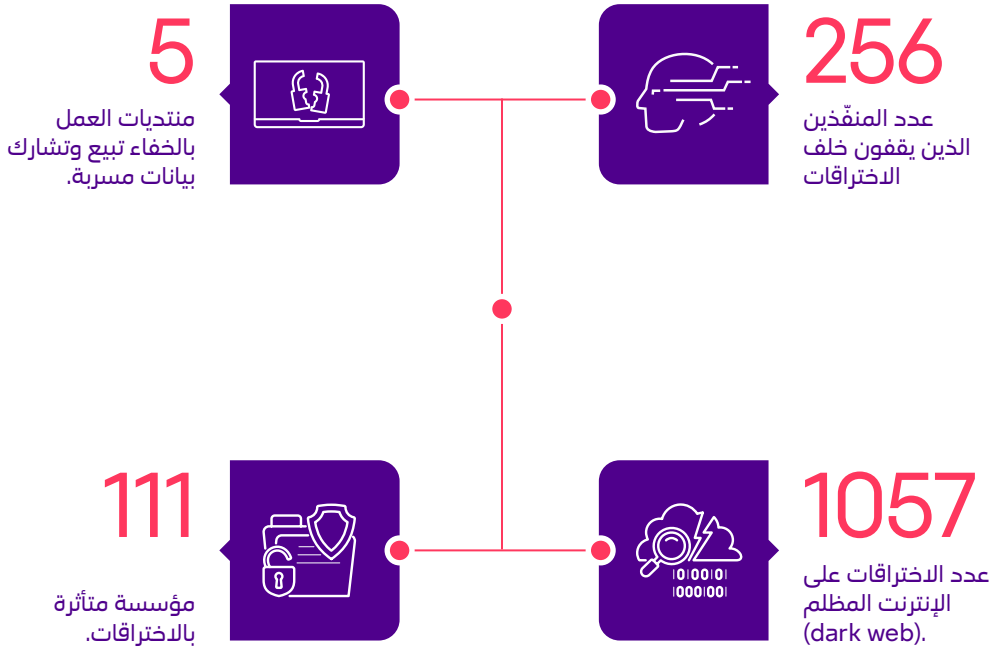
## ثغرات أمنية موزعة حسب النمط

## تحليل السلوك الأكثر شيوعاً حسب النمط



- حجب الخدمة لـ ManageEngine AssetExplorer
- تحديث امني متوفر لـ Adobe Reader APSB17-11
- تحديث امني متوفر لـ Adobe Reader apsb17-24
- ثغرة أمنية لـ lognet CVE-2018-1285
- ثغرة أمنية في Oracle JRE CVE-2022-21426
- ثغرة أمنية في Oracle JRE CVE-2022-21434
- ثغرة أمنية في Oracle JRE CVE-2022-21443
- ثغرة أمنية في Oracle JRE CVE-2022-21476
- ثغرة أمنية في Oracle JRE CVE-2022-21496
- تحذير: لم يعد يدعم بواسطة Adobe Reader X

# هجمات سببرانية تستهدف السعودية من الإنترنت المظلم (dark web)





# معارك sirar

04



# مشارك sirar

هجمات حجب الخدمة الموزعة

هجمات حجب  
الخدمة الموزعة

# أكبر هجمات حجب الخدمة الموزعة في السعودية في عام 2022

حجم أكبر هجمات حجب الخدمة الموزعة عام 2022

• 208 جيجابت/ث •

أكبر 4 هجمات حسب الحجم

182 جيجابت/ث

178 جيجابت/ث

171 جيجابت/ث

مجموع ساعات توقف الخدمة التي تم منعها

• 5,560 ساعة تصدي للهجمات •

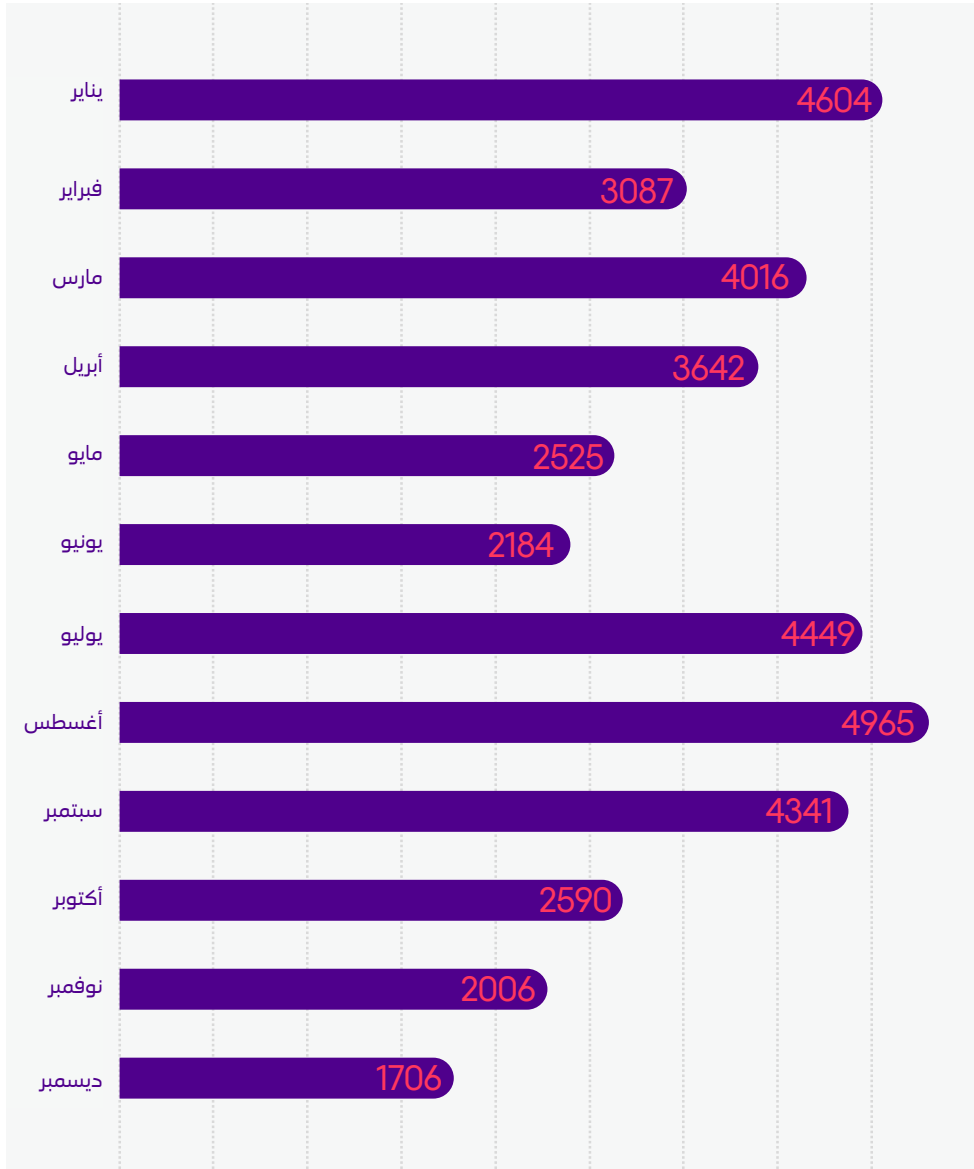
الفترة الزمنية التي من الممكن أن يسبب فيها هجوم حجب الخدمة الموزعة تعطيل الخدمات / الشبكة / التطبيقات اذا لم يتم التصدي للهجوم.

• 4 تيرابايت/ث •

وحدة التنقية المحلية التابعة لـ sirar (وهي الأكبر في المنطقة) قادرة على التصدي للهجمات حتى 8 تيرابايت في الثانية على مستوى السحابة.



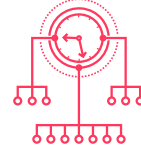
# أكبر هجمات حجب الخدمة الموزعة في عام 2022:



عدد هجمات حجب الخدمة  
الموزعة في عام 2022

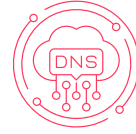
# أنواع هجمات حجب الخدمة الموزعة

49% NTP  
تضخيم



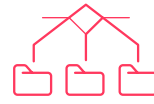
تقوم هذه النوعية من هجمات حجب الخدمة الموزعة باستغلال خوادم NTP المتاحة عبر شبكة الانترنت لتغرق الهدف بفيض من بيانات UDP

18% DNS  
تضخيم



تقوم هذه النوعية من هجمات حجب الخدمة الموزعة باستغلال خوادم DNS المتاحة عبر شبكة الانترنت ليقوم باستغلال كامل للنطاق الترددي للهدف

20%  
أخرى



أبعاد أخرى مثل TCP SYN, CLDAP, Memcache..إلى أخرى

13%  
UDP



يمكن تشكيل هجمات حجب الخدمة الموزعة عندما يقوم المهاجمون بإرسال عدد كبير من حزم UDP إلى منافذ عشوائية موجودة لدى الخادم.

# معارك sirar

VMDR

إدارة الثغرات الأمنية

# إدارة الثغرات الأمنية



في 2022

402 ألف

ثغرة أمنية تم إغلاقها

وهذا يمثل إرتفاع بنسبة **172%** عن ما تم إغلاقه من الثغرات الأمنية في العام السابق.

785 ألف

ثغرة تم كشفها

وهذا يمثل إرتفاع بنسبة **192%** عن ما تم كشفه من الثغرات الأمنية في العام السابق.

إن خدمة إدارة الثغرات الأمنية وكشفها والاستجابة لها التي تقدمها **sirar by stc** تساعد منشآتكم في تقييم مستمر لثغرات الأمن السيبراني وحالة الإمتثال للضوابط.

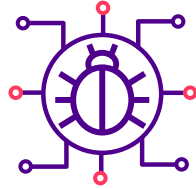
# معارك sirar

حماية البريد الإلكتروني





# حماية البريد الإلكتروني



في 2022

84.92%

نسبة رسائل البريد الموثوقة

15.08%

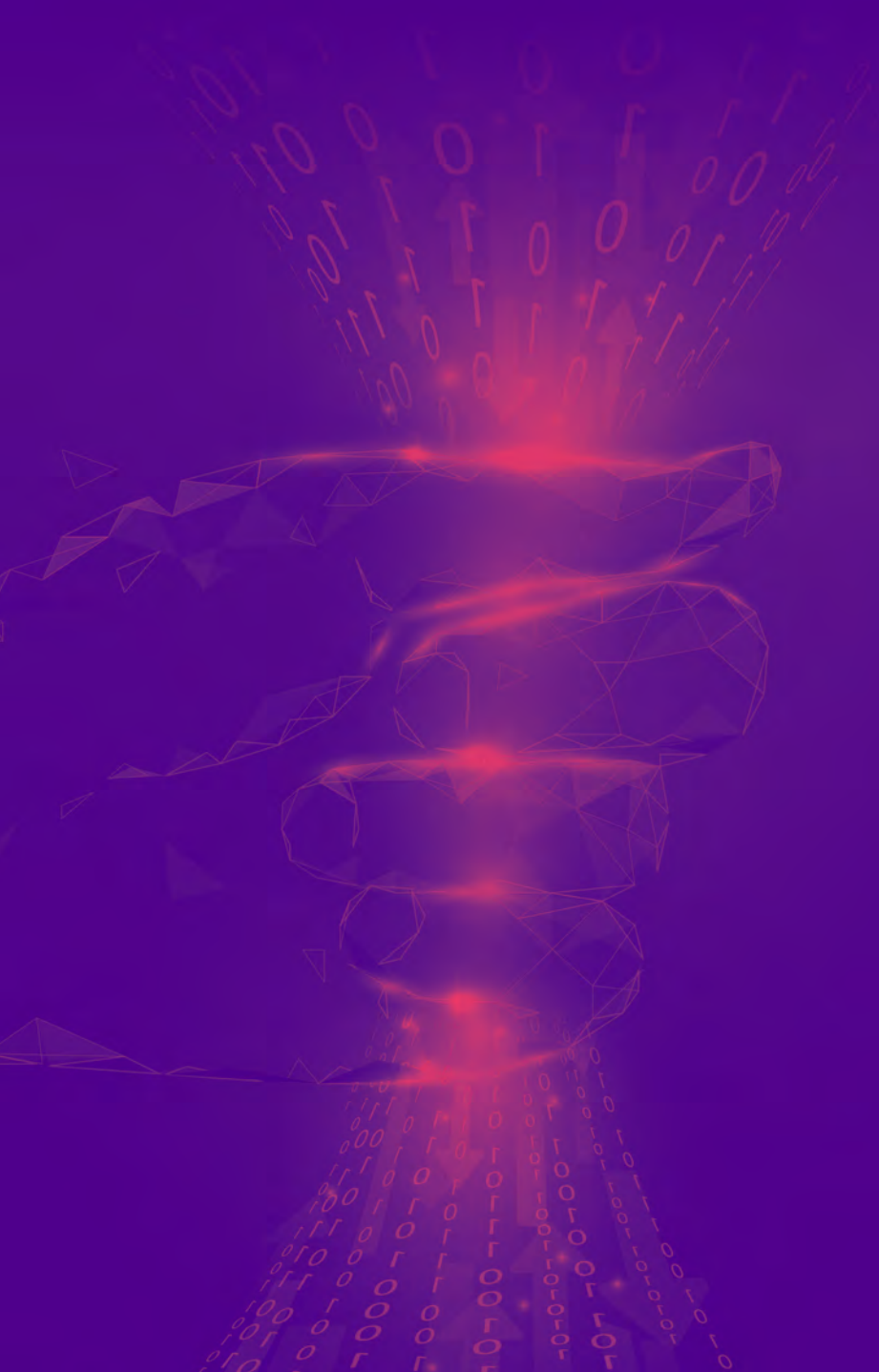
نسبة رسائل البريد المحظورة

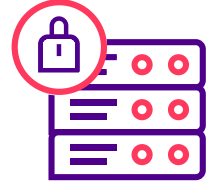
تساعد خدمة حماية البريد الإلكتروني في توفير حماية متقدمة متعددة الطبقات ضد مجموعة كبيرة من التهديدات التي يحملها البريد الإلكتروني. كما تساعد في منع أحدث التهديدات التي يحملها البريد الإلكتروني وإكتشافها والإستجابة لها، بما في ذلك البريد الإلكتروني العشوائي والتصيد الاحتيالي والبرامج الضارة والتهديدات غير المباشرة وهجمات كشف/اختراق البريد الإلكتروني للأعمال.



# معارك sirar

حماية الإنترنت





# حماية الإنترنت

في 2022

مجموع

• العمليات الالكترونية •

التي أجريت في sirar

251.7 مليون

مجموع

• التهديدات •

التي تم إيقافها في sirar

2.398 مليون

مجموع

• حجم البيانات •

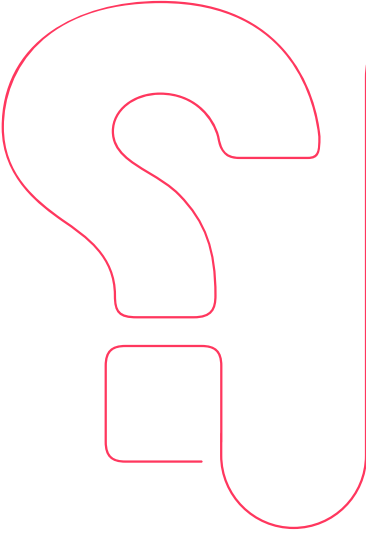
الحجم:

266.6 جيجا بايت

# مشارك sirar

الحج واليوم الوطني

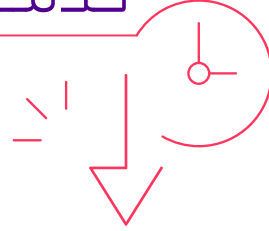
# مساهماتنا للحفاظ على أمن وطننا



## ماذا حدث خلال الحج؟

### 1 مساهمة sirar

خدمات المراقبة من sirar



**600** مليون  
عدد البيانات الواردة الضارة  
التي تم التصدي لها



**39** عدد البرمجيات  
الخبثة المحظورة



# مساهماتنا للحفاظ على أمن وطننا

## 2 مساهمة sirar

هجمات حجب  
الخدمة خلال موسم الحج

( 29 يونيو - 11 يوليو )



هجمات  
حجب  
الخدمة  
الموزعة

مجموع الهجمات: **1266**

حجم أكبر هجمات  
**DDoS**  
المخفضة

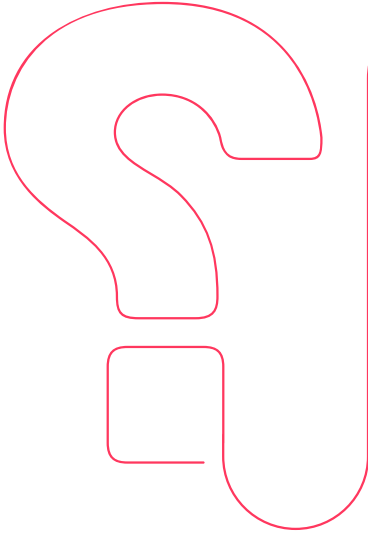
**66**  
جيجا بايت

مجموع

ساعات توقف الخدمة التي تم منعها

**167:12:38**  
ساعة

# مساهماتنا للحفاظ على أمن وطننا

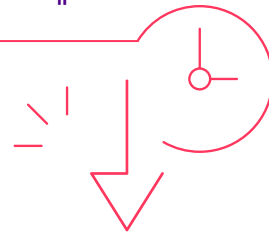


## ماذا حدث خلال اليوم الوطني؟

### مساهمة sirar

تمكنت sirar خلال اليوم الوطني من حماية المملكة من هجمات متعددة

معظم الكيانات المستهدفة كانت من الجهات الحكومية والبنية التحتية الحساسة



رابط تصيد احتيالي تم رصده

74



نطاق تصيد احتيالي تم رصده

111



تهديدات متقدمة ومستمرة

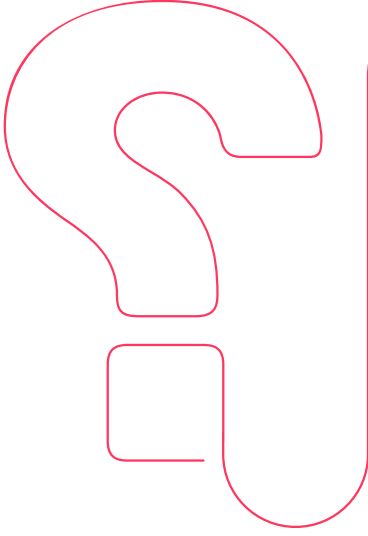
10



برمجيات خبيثة

9

# مساهماتنا للحفاظ على أمن وطننا

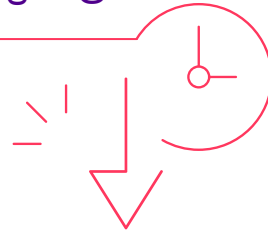


## ماذا حدث خلال قمة جدة؟

### مساهمة sirar

دافعت sirar عن قمة جدة للأمن والتنمية  
من الهجمات السيبرانية

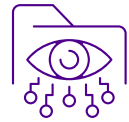
**33+**  
عدد الهجمات التي تم إيقافها



**5.5** جيجا بايت  
حجم أكبر هجوم



**8+ ساعات**  
عدد ساعات التوقف التي تم منعها





# الاستنتاجات الرئيسية

04

# الاستنتاجات الرئيسية

تعد الحماية الإستباقية والنسخ الإحتياطي للبيانات وضوابط الأمان الأخرى ضرورةً لمنع فيروسات الفدية



تعد حماية كود البرنامج أساسية لمنع هجمات سلاسل التوريد



تطبيق سياسات حوكمة أمن سيبراني فعالة



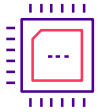
يعد وعي المستخدم مهماً لمنع التأثير بالتصيد الاحتيالي



القيام ببناء التدابير المضادة لكشف تسريب البيانات باستخدام خدمة حماية الإنترنت



اعتماد الذكاء الاصطناعي/ تعلم الآلة لوقف الهجمات المعقدة



الأمن السيبراني أولاً هي ثقافة يجب غرسها لمنع الاختراقات



حافظ على توافرية خدماتك الالكترونية مع خدمة منع حجب الخدمة الموزعة



# تعريف مصطلحات

sirar

05



# تعريف مصطلحات sirar

## الأمن السيبراني (Cybersecurity)

الأمن السيبراني هو إجراء يقلل من خلاله الأشخاص والمنظمات من خطر تعرضهم للهجمات الإلكترونية، الهدف الرئيسي من الأمن السيبراني هو منع سرقة أو تخريب الأجهزة الإلكترونية التي نستخدمها جميعاً (والتي تتضمن أجهزة الحاسب المكتبي والمحمولة والأجهزة اللوحية والهواتف الذكية) بالإضافة إلى الخدمات التي نستخدمها في كل من العمل والمنزل.

## مركز عمليات الأمن السيبراني كخدمة (SOCaaS)

مركز عمليات الأمن السيبراني يقدم على مدار الساعة مراقبة شاملة للتهديدات السيبرانية المتقدمة على شبكة العميل والبيئة السحابية وخدمة البرمجيات والتطبيقات ونقاط النهاية لأجهزة المستخدمين وعلى سجلات الأحداث المدعومة باستقصاء التهديدات، يحتوى مركز عمليات الأمن السيبراني على مطلين خبراء يقومون بتنفيذ كشف التهديدات على السجلات مما يحسن من قدرات الكشف عن الحالات الغريبة التي لا يمكن كشفها بشكل تلقائي بالإضافة إلى الكشف القائم على إستقصاء التهديدات، مركز عمليات الأمن السيبراني يتبع التكتيكات والتقنيات القائمة على أطر الأمن السيبراني الرائدة.

## هجوم برامج الفدية (Ransomware Attack)

هو نوع من البرامج الضارة التي يستخدمها المهاجمين عبر الأنترنت بشكل نشط لتخريب المنظمة المستهدفة من خلال تشفير الملفات الهامة للمنظمة وجعلها غير مقروءة ويتم طلب فدية مقابل إلغاء التشفير.

## هجمات حجب الخدمة الموزعة (Distributed Denial of Service)

هجوم حجب الخدمة الموزعة هو محاولة خبيثة لتعطيل حركة البيانات الإعتيادية على الخادم المستهدف أو الخدمة أو الشبكة من خلال إغراق الهدف أو ما يحيط به من البيئة التحتية بفيض من البيانات.

## نموذج التهديدات السيبرانية (MITRE ATT&CK)

وهو عبارة عن إطار ومجموعة من مصفوفات البيانات وأدوات التقييم تم تطويرها بواسطة مؤسسة MITRE لمساعدة المنظمات في فهم استعدادها الأمني وكشف الثغرات في نظامها الدفاعي.

## البرامج الضارة (Malware)

البرامج الضارة هي برامج اختراق مصممة لتخريب وتدمير أجهزة الكمبيوتر وأنظمتها، أمثلة عن البرامج الضارة الشائعة تتضمن الفيروسات وفيروسات تورجان و worms و وبرامج التجسس؛ برامج أدوير و برامج الفدية.

## هجمات التصيد الاحتيالي (Phishing Attacks)

هجمات التصيد الاحتيالي هي عملية تنفيذ اتصالات احتيالية تبدو في الظاهر انها واردة من مصدر موثوق، يتم تنفيذه عادة عبر البريد الإلكتروني بهدف سرقة البيانات الحساسة مثل بطاقة الائتمان أو معلومات تسجيل الدخول أو تثبيت برامج ضارة على جهاز الضحية، يعتبر التصيد الاحتيالي نوعاً شائعاً من الهجمات السيبرانية التي تستغل أضعف طرفة في الأمن السيبراني وهو العنصر البشري.

## بنية الأمن السيبراني (Cybersecurity Architecture)

بنية الأمن السيبراني هي أساس دفاع المؤسسة ضد التهديدات السيبرانية ، وتضمن أن جميع مكونات البنية التحتية لتقنية المعلومات محمية.

# تعريف مصطلحات sirar

## نموذج أمان الثقة الصفرية (Zero Trust Security)

أمان الثقة الصفرية هو إطار عمل لحماية البنية التحتية والبيانات بما يضمن تحقيق خطط التحول الرقمي الحديثة، كما يقوم بشكل منفرد بتحديد التحديات التي تواجه تطور الأعمال في الآونة الأخيرة كحماية اتصال الموظفين أثناء قيامهم بعملهم عن بعد وحماية البيانات السحابية المختلطة والحماية من برامج الفدية. بينما قام العديد من الموردين بإنشاء تعريفاتهم الخاصة للثقة المعدومة هناك عدد من المعايير التي تم وضعها من المنظمات المعترف بها والتي يمكن أن تساعدك في مواءمة الثقة المعدومة مع منظمتك.

## الإنترنت المظلم (Dark web)

الإنترنت المظلم هو مجموعة من مواقع الإنترنت المخفية التي لا يمكن الوصول إليها إلا من خلال مستعرض إنترنت متخصص. يتم استخدامه لإبقاء نشاط الإنترنت مخفي وخاص، الذي يمكن أن يساعد في استخدام كل من التطبيقات القانونية وغير القانونية. بينما يستخدمه البعض للتهرب من الرقابة الحكومية فمن المعروف أيضاً أنه يستخدم في أنشطة غير قانونية لا حصر لها على سبيل المثال: بيع بيانات الضحية أو معلومات بطاقة الائتمان أو حتى تقديم خدمات الهجمات السيبرانية مقابل رسوم.

## بروتوكول وقت الشبكة (NTP) (Network Time Protocol)

هو بروتوكول يساعد أجهزة الكمبيوتر لتكون متزامنة في الشبكة. هذا البروتوكول هو بروتوكول تطبيق مسؤول عن مزامنة الأجهزة المضيفة على شبكة TCP / IP. تم تطوير NTP بواسطة David Mills في عام 1981 في جامعة ديلاوير. هذا البروتوكول مطلوب في آلية الاتصال بحيث ينشئ اتصال سلس بين أجهزة الحاسب.

## بروتوكول مخطط بيانات المستخدم (User Datagram Protocol)

هو بروتوكول في طبقة النقل، وهو جزء من مجموعة بروتوكولات الإنترنت، يشار إليها بمجموعة UDP / IP. على عكس TCP، فهو بروتوكول غير موثوق به وغير متصل. لذلك لا يوجد حاجة لإنشاء اتصال قبل نقل البيانات. يساعد بروتوكول UDP على إنشاء اتصالات ذات زمن انتقال منخفض ويتناسب مع الإنقطاعات عبر الشبكة. يتيح بروتوكول UDP عملية معالجة الاتصال.

## خوادم نظام أسماء النطاق (Domain Name system servers)

خادم نظام اسم المجال (DNS): عندما يكتب المستخدمون أسماء المجال في شريط URL في متصفحهم، تكون خوادم DNS مسؤولة عن ترجمة أسماء المجالات هذه إلى عناوين IP رقمية مما يقودهم إلى موقع الإنترنت الصحيح.

## إدارة الثغرات الامنية واكتشافها والاستجابة لها

### (Vulnerability Management, Detection & Response (VMDR))

تحديد الثغرات السيبرانية بشكل استباقي. يتغير الأمن السيبراني باستمرار وتظهر تهديدات جديدة بشكل يومي. تمنح خدمات الكشف عن إدارة الثغرات الأمنية والاستجابة لها مؤسستك تقييمًا مستمرًا ودائمًا للثغرات الأمنية السيبرانية للبنية التحتية ومستوى الامتثال. رؤية شاملة عبر أصول تقنية المعلومات بالكامل أينما كانت مع تحديد أولويات التهديدات المضمنة تلقائيًا والتصحيح، وقدرات الاستجابة الأخرى.

# تعريف مصطلحات sirar

## التنقية (Scrubbing)

التنقية هو أسلوب شائع لتخفيف هجوم حجب الخدمة الموزعة، تتم إعادة توجيه حركة البيانات لنطاق محدد من عناوين IP حيث يتم تنقية أو تنظيف أي حركة مرور ضارة ثم إعادة توجيه حركة البيانات النظيفة إلى التسليم، مما يسمح ببقاءك متصلاً دون فقدان الخدمة.

## هجوم القوة العمياء (Brute force attack)

هجوم القوة الغاشمة هو طريقة تستخدم التجربة والخطأ لاخترق كلمات المرور وبيانات تسجيل الدخول ومفاتيح التشفير، إنه تكتيك بسيط وفعال للحصول على وصول غير مصرح به إلى الحسابات الفردية وأنظمة وشبكات المنظمات يحاول المهاجم استخدام أسماء مستخدمين وكلمات مرور متعددة وغالبًا ما يستخدم جهاز حاسب لاختبار عدد كبير من المجموعات حتى يجدوا المعلومات الصحيحة لتسجيل الدخول.

## ثغرة (Log4Shell)

Apache Log4j 2 وهي مكتبة Java مشهورة لتسجيل رسائل الخطأ في التطبيقات وتحتوي على ثغرة في البرامج تسمى Log4Shell، إذا كان الجهاز يستخدم إصدار محدد من Log4j 2 فإن الثغرة الأمنية التي تم تحديدها على أنها CVE-2021-44228 تسمح للمهاجم بالتحكم بالجهاز عن طريق الإنترنت.

## ثغرة (Doublepulsar)

DOUBLEPULSAR عبارة عن محطة تحميل للبرامج الضارة الإضافية التي تهدف إلى توفير قناة سرية يتم بواسطتها تحميل برامج ضارة أو ملفات تنفيذية أخرى، تستخدم جميع عمليات استغلال SMB و RDP في إطار استغلال FuzzBunch تستخدم DoublePulsar حمولة أساسية.

## برنامج (Cryptominer) الضار

البرنامج الضار Cryptominer أو "cryptojacking" وهو برنامج هجوم ضار يشترك في اختياف موارد الهدف من أجل تعدين العملات المشفرة مثل البيتكوين، تستخدم هذه البرامج الضارة المعالج وأحيانًا وحدة معالجة الرسومات لإجراء عمليات حسابية معقدة ينتج عنها سلاسل أجدية رقمية طويلة تسمى Hashes.

## برنامج حضان طروادة الضار (Torjan)

وهو برنامج ضار في الظاهر يبدو أنه برنامج مشروع متخفي في صورة برامج نظام تشغيل أصلية أو ملفات غير ضارة مثل التنزيلات المجانية، يتم تثبيت أصدنة طروادة من خلال تقنيات الهندسة الاجتماعية مثل مواقع الإنترنت الخاصة بالتصيد الاحتيالي أو كطعم.

## برنامج (Bad Rabbit)

هي سلاطة من برامج الفدية ظهرت لأول مرة في عام 2017 وهي نوع شبيه ب Petya، وكأي من برنامج فدية آخر فإنه عند الإصابة ب Bad Rabbit يتم إغلاق أجهزة الحاسب للضحايا أو للخدام أو للملفات ويتم منعهم من استعادة الوصول إلى أن يتم دفع فدية بعملة البيتكوين عادة.

# مراجع

06



# مراجع\*

"California, Security Operations Center as a service (SOCaaS). CDT Services.  
From <https://cdt.ca.gov/services/security-operations-center-as-a-service-socaaS/> "

"Threatlabz Ransomware Review: The advent of double extortion.  
From <https://info.zscaler.com/resources-white-papers-threatlabz-ransomware-review>"

"What is a distributed denial-of-service (ddos) attack? - cloudflare.  
From <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/> "

"Cisco. (2022, June 6). What is malware? - definition and examples. Cisco.  
From <https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html> "

"Cisco. (2022, December 21). What is phishing? Cisco.  
From <https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html> "

"Chkadmin. (2022, May 11). What is a cyber security architecture? Check Point Software.  
From <https://www.checkpoint.com/cyber-hub/cyber-security/what-is-a-cyber-security-architecture/>"

"What is Zero trust security? principles of the zero trust model (2022, November10).  
From <https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/>"

"Kaspersky. (2022, October 21). What is the deep and dark web?.  
From <https://www.kaspersky.com/resource-center/threats/deep-web> "

"Network time protocol (NTP). GeeksforGeeks.  
From <https://www.geeksforgeeks.org/network-time-protocol-ntp/> "

"User datagram protocol (UDP). GeeksforGeeks. (2022, November 1).  
From <https://www.geeksforgeeks.org/user-datagram-protocol-udp/> "

"What is a DNS server? | cloudflare.  
From <https://www.cloudflare.com/learning/dns/what-is-a-dns-server/>"

" (2022, September 13). What is Log4j? A cybersecurity expert explains the latest internet vulnerability, how bad it is and what's at stake. The Conversation.  
From <https://theconversation.com/what-is-log4j-a-cybersecurity-expert-explains-the-latest-internet-vulnerability-how-bad-it-is-and-whats-at-stake-173896> "



## \* مراجع

"What is a brute force attack?: Definition, Types & How It Works. Fortinet.  
From <https://www.fortinet.com/resources/cyberglossary/brute-force-attack>"

"Bhat, S. (2022, March 16). Doublepulsar – a very sophisticated payload for windows.  
SecPod Blog.  
From <https://www.secpod.com/blog/doublepulsar-a-very-sophisticated-payload-for-windows/> "

"Cryptomining malware - definition, examples, & detection - extrahop. ExtraHop.  
From <https://www.extrahop.com/resources/attacks/cryptomining/>"

"What is malware? detection & removal methods: CrowdStrike.  
From <https://www.crowdstrike.com/cybersecurity-101/malware/> "

"What is bad rabbit ransomware?: Proofpoint us. Proofpoint. (2022, November30).  
From <https://www.proofpoint.com/us/threat-reference/>"

Paganini, P. (2022, May 3). UNC3524 APT uses IP cameras to deploy backdoors and Target Exchange. Security Affairs.  
Retrieved from <https://securityaffairs.com/130838/apt/unc3524-apt-ip-cameras.html>

Mandiant.UNC3524: Eye spy on your email. Mandiant.  
Retrieved from <https://www.mandiant.com/resources/blog/unc3524-eye-spy-email>

Ransomware spotlight: Clop. Security News.  
Retrieved from <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-clop>

Hacktivist attacks show ease of hacking industrial control systems. SecurityWeek.  
Retrieved from <https://www.securityweek.com/hacktivist-attacks-show-ease-hacking-industrial-control-sys>

Microsoft 365 Defender Research Team, M. T. I. C. (M. S. T. I. C. (2022, July 12). From cookie theft to BEC: Attackers use AITM phishing sites as entry point to further financial fraud. Microsoft Security Blog.  
Retrieved from <https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/>

## \* مراجع

Westfall, S. (2022, November 3). Threat brief: CVE-2022-41040 and CVE-2022-41082: Microsoft Exchange Server (ProxyNotShell). Unit 42. Retrieved from <https://unit42.paloaltonetworks.com/proxynotshell-cve-2022-41040-cve-2022-41082/>

Conger, K., & Roose, K. (2022, September 16). Uber investigating breach of its computer systems. The New York Times. Retrieved from <https://www.nytimes.com/2022/09/15/technology/uber-hacking-breach.html>

Biasini, N. (2022, November 2). Cisco Talos shares insights related to recent cyber-attack on Cisco. Cisco Talos Blog. Retrieved from <https://blog.talosintelligence.com/recent-cyber-attack/>

Prince, M. (2023, January 13). The mechanics of a sophisticated phishing scam and how we stopped it. The Cloudflare Blog. Retrieved from <https://blog.cloudflare.com/2022-07-sms-phishing-attacks/>

IBM - United States. Retrieved from <https://www.ibm.com/downloads/cas/3R8N1DZJ>

Westfall, S. (2022, November 3). Threat brief: CVE-2022-41040 and CVE-2022-41082: Microsoft Exchange Server (ProxyNotShell). Unit 42. Retrieved from <https://unit42.paloaltonetworks.com/proxynotshell-cve-2022-41040-cve-2022-41082/>

 **sirar**  
by **stc**

الأمن السيبراني

كما يجب أن يكون