التقرير السنوي

للتهديدات السيبرانية لعام 2023

sirar
by stc

جدول المحتويات

sirar by stc

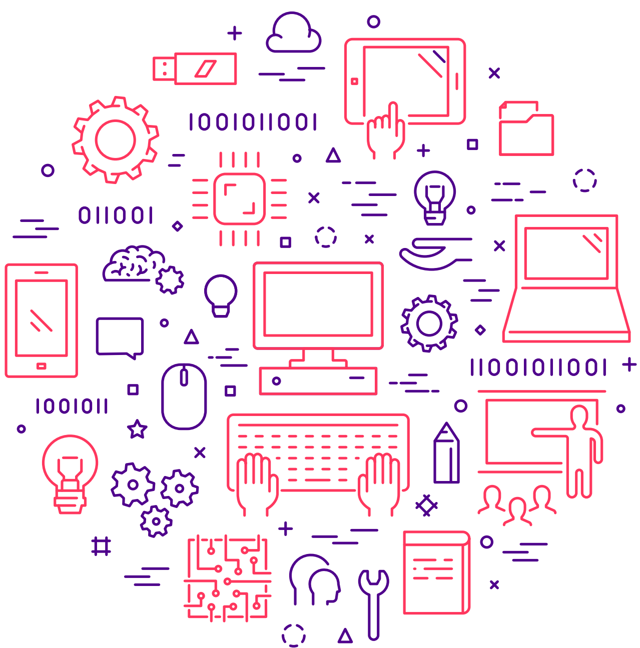
01

المقدمة

المقدمة

ملخص التقرير

يقـدم هـذا التقريـر نظـرة شـاملة علـى التهديـدات والثغـرات الأمنيـة العالميـة والإحصائيـات الإقليميـة والملاحظـة فـي المملكـة العربيـة السـعودية، وذلك لتمكيـن مُتخـذي القرار مـن رفـع مسـتوى الجاهزيـة وتحصيـن دفاعـات البنيـة التحتيـة التقنيـة للمؤسسـة. كمـا يسـتعرض هـذا التقريـر الشـامل مشـهد التهديـدات السـيبرانية بالتفصيـل ومـا وصلـت إليـه مـن تطـورات، كمـا يسـلط الضـوء علـى جهـود sirar الكبيـرة التـي تبذلهـا عنـد خـوض معاركهـا. فمـن خلال منتجاتهـا وخدماتهـا المبتكـرة، توفـر sirar حمايـة شـاملة للعملاء،ممـا يضمـن تأميـن أعمالهـم فـي مواجهـة المخاطـر الناشـئة. علاوة علـى ذلـك، يكشـف التقريـر عـن الـرؤى والأفـكار المقترحـة حـول الحفـاظ علـى أمـن الأعمـال مـن خلال تطبيـق صايـن، وهـو منتـج يحافـظ علـى الأمـن ويعـزز تجـارب العـملاء مـن خلال توفيـر خدمـة التوقيـع الرقمـي. وقـد قمنـا فـي sirar بإعـداد تقريـر التهديـدات السـيبرانية لعـام 2023 بهـدف تزويـد المؤسسـات بالمعرفـة اللازمـة للحمايـة الاسـتباقية مـن التهديـدات السـيبرانية وهـو مصدر قيّم للحفاظ على أمان الأعمال والتنبؤ بالمخاطر المتغيرة ومواجهتها بفعالية.



المقدمة

رؤيتنا ورسالتنا وقيمنا

تتبع الشركة المتقدمة للتقنية والأمن السيبراني (sirar) مجموعة stc، والتي تُعد المزوّد التقني الرائد لتكنولوجيا المعلومات والاتصالات والخدمات الرقمية في المنطقة، حيث تقوم sirar بصفتها المزوّد الرقمي لخدمات الأمن السيبراني المتقدمة بتمكين المؤسسات من التحكم في إمكانياتها الرقمية والإلكترونية.

وبصفتها متخصصة في الأمن السيبراني وتأمين الخصوصيات والتصدي للهجمات السيبرانية، تُقدم sirar مجموعة حلول شاملة تساعد على إدارة المخاطر الرقمية بكفاءة مع الامتثال للقوانين واللوائح ذات الصلة والسير نحو التحول الرقمي بأمان.

الرسالة

نسعى إلى تطوير حلول وقدرات سيبرانية تتوافق مع أعلى المعايير العالمية، مما يمكن عملاءنا في المملكة وخارجها من خوض رحلة تحول رقمي آمنة.

الرؤية

ممكّن الأمن السيبراني الأول للاقتصاد الرقمي

القيم

الحيوية
التفاني
الإقدام

02

الهجمات الأكثر شيوعًا في العالم

الهجمات الأكثر شيوعًا في العالم

ثغرات MOVEit

موجز

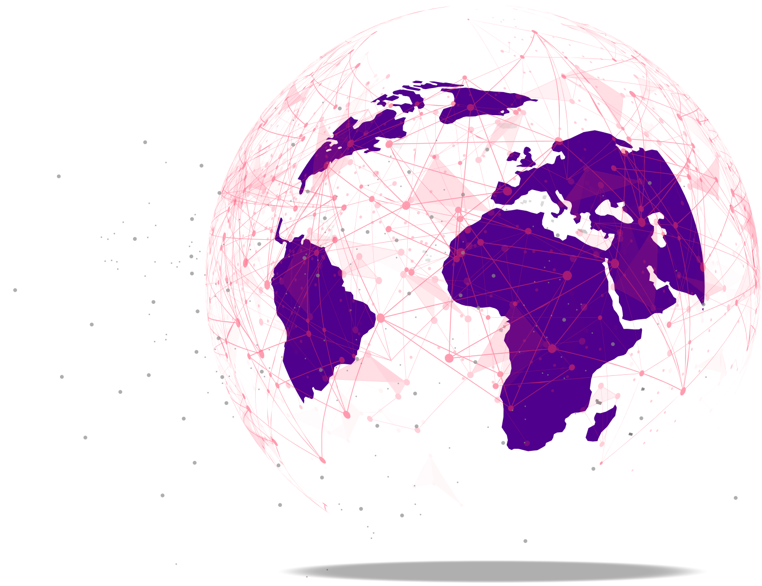
- تم الإعلان عن ثغرات (MOVEit Transfer) في الفترة من مايو إلى يونيو 2023، حيث تم استغلالها على نطاق واسع وأثرت على العديد من القطاعات مثل الطاقة والبنية التحتية الوطنية الحيوية والقطاعات الحكومية.
- تأثرت أكثر من 2300 مؤسسة بشكل عام، استهدف هجوم الفدية المعروف باسم (Cl0p) أكثر من 400 منظمة وأكثر من 60 مليون فرد كضحايا باستخدام ثغرة غير معروفة مسبقاً في (MOVEit)
- ومن ضمن الشركات المتأثرة:
- سي كلينر (Ccleaner) , Siemens) شركة سيمنز للطاقة (Energy، وشنايدر (SchneiderElectric) إليكتريك، (Shell) رويال دتش شل النفطية، ووزارة الطاقة الأمريكية.

التفاصيل

- تم استغلال ثغرة حقن < SQL > حساسة غير المعروفة مسبقاً منذ مارس 2023، حيث تسمح هذه الثغرة للمهاجمين بالوصول المستتر من خلال استغلال (LemurLoot) ثم سرقة البيانات عن طريق استخراجها من خلال (MOVEit Transfer).

البيانات المخترقة

- القطاعات المتأثرة: التعليم (39%)، الصحة (21%)، القطاع المالي (14%)، القطاع العام (3.8%)، القطاع القانوني (0.2%)، قطاعات أخرى (22%). ويعد قطاعا التعليم والصحة هما الأكثر تأثرًا نظرًا لاستعانتهما بخدمات تابعة لأطراف خارجية.
- تم اختراق أنواع متعددة من البيانات أثناء النقل بحسب القطاع: تواريخ الميلاد، عناوين البريد الإلكتروني، المعلومات المالية، المعلومات الشخصية ومعلومات الصحة الشخصية، أرقام الهوية الحكومية وهوية الضمان الاجتماعي.



المصدر:

إحصائيات مستمدة من مصادر المعلومات الاستباقية الإقليمة خلال آخر 6 أشهر عن الهجمات (البرامج الضارة والمنفذين) من قنوات المعلومات الاستباقية من Anomali (البرامج الضارة والمهاجمين) المدعومة من شركاء Anomali وهم Polyswarm وBitdefender.

الهجمات الأكثر شيوعًا في العالم

مجموعة ALPHV لبرامج الفدية

موجز

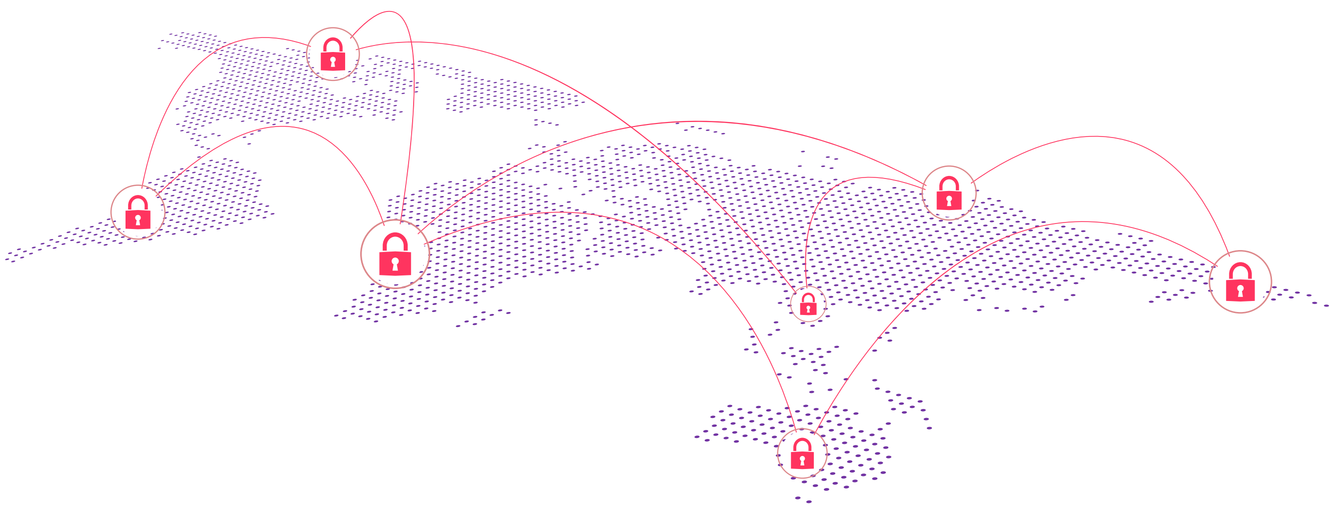
- تتخصص المجموعة في هجمات الهندسة الاجتماعية وهجمات برامج الفدية المدارة.
- برزت مجموعة (ALPHV/BlackCat) لبرامج الفدية بسبب شعبيتها المتزايدة وميلها إلى اختراق الأهداف الثمينة عالية القيمة.

التفاصيل

- استخدام متغيرات متعددة من برامج الفدية ذات تعليمات برمجية مماثلة، بما في ذلك (ALPHV) و (BlackCat) و(Sphynx) و (Noberus).
- تعتمد هذه البرامج على لغة البرمجة (Rust)، ما يجعلها قابلة للتخصيص والتوسع.
- تكتيكات الابتزاز المزدوجة والثلاثية، وفرض فدية لفك تشفير الملفات والتهديد بالكشف عن الملفات أو الانخراط في هجمات حجب الخدمة الموزعة (DDoS) حتى رفع الشكاوى إلى الجهات التنظيمية والرقابية.

المنفذين

- تعمل إما بمفردها أو مع شركائها مثل مجموعة FIN8.



المصدر:

إحصائيات مستمدة من مصادر المعلومات الاستباقية الإقليمية خلال آخر 6 أشهر عن الهجمات (البرامج الضارة والمنفذين) من قنوات المعلومات الاستباقية من Anomali (البرامج الضارة والمهاجمين) المدعومة من شركاء Anomali وهم Polyswarm وBitdefender.

الهجمات الأكثر شيوعًا في العالم

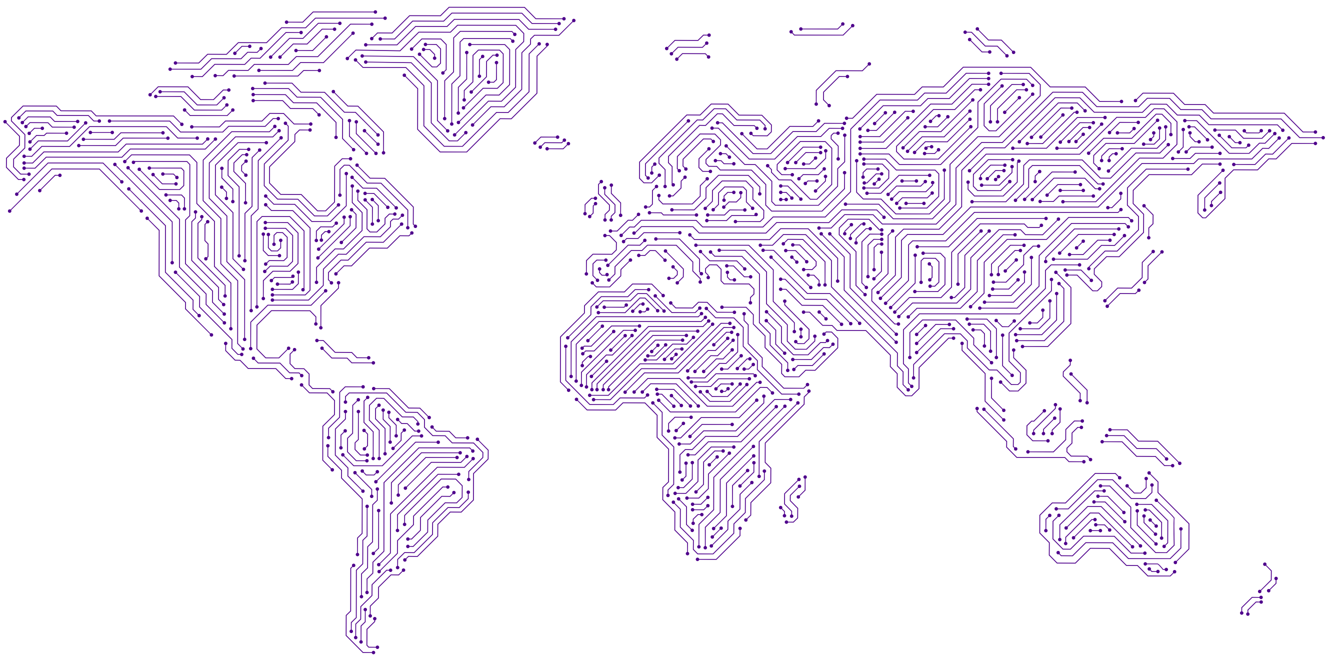
حصان طروادة QakBot

موجز

- (QakBot) المعروف أيضًا باسم (Pinkslipbot) و (Qbot) عبارة عن حصان طروادة (Trojan horse) قديم الأجل وتطور عبر الوقت إلى خدمة توصيل البرمجيات الضارة. وقد أوقفته جهات الأمن الإلكتروني المعنية في أغسطس 2023 إلا أنه بدأ في الظهور مجدداً في ديسمبر 2023 بنسخته غير المرئية (0x500).

الفحص

- غالباً ما يصل من خلال التصيد الاحتيالي وسرقة البريد الإلكتروني والهندسة الاجتماعية.
- في عام 2023، استخدم (Qakbot) أساليب مختلفة، بما في ذلك استخدام برنامج (OneNote) أحد تطبيقات (Windows) وهو برنامج غير ضار ومفيد بطبيعته، ولكنه استخدمه بطريقة ضارة، واستخدام ملفات <Windows Installer (MSI)> موقعة رقمياً، وأسلوب التهرب من <Mark of the web (MOTW)> ، وأسلوب <HTML Smuggling> لتهريب الملفات الضارة.
- تم تشغيل <QakBot> بواسطة منفذي التهديد المعروفين باسم <Mallard Spider> ، حيث قاموا أيضاً بعمليات تنفيذ برنامج الفدية <Ransome Knight> من خلال استخدام برنامج التحكم عن بعد <Remcos>.



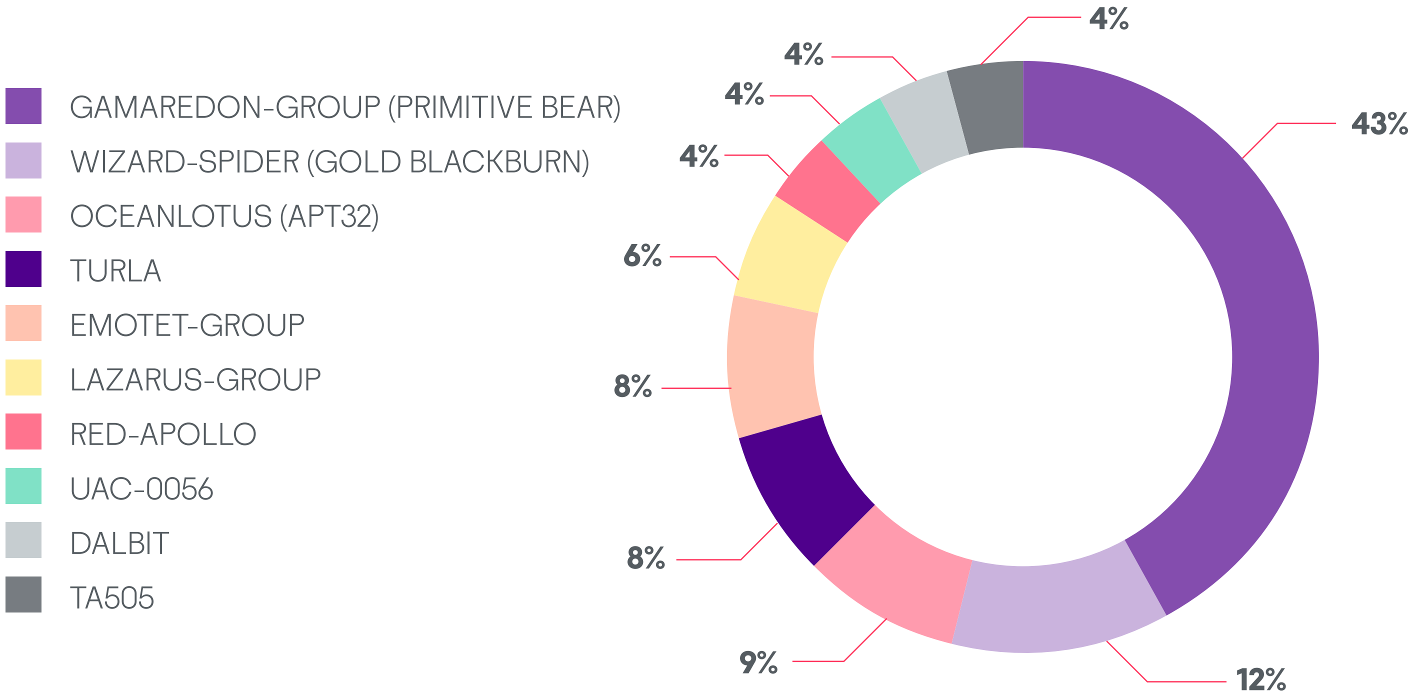
المصدر:
إحصائيات مستمدة من مصادر المعلومات الاستباقية الإقليمة خلال آخر 6 أشهر عن الهجمات (البرامج الضارة والمنفذين) من قنوات المعلومات الاستباقية من Anomali (البرامج الضارة والمهاجمين) المدعومة من شركاء Anomali وهم Polyswarm وBitdefender.

03

الإحصائيات الإقليمية

sirar by stc

أعلى 10 تهديدات سيبرانية
ملاحظة في الشرق الأوسط



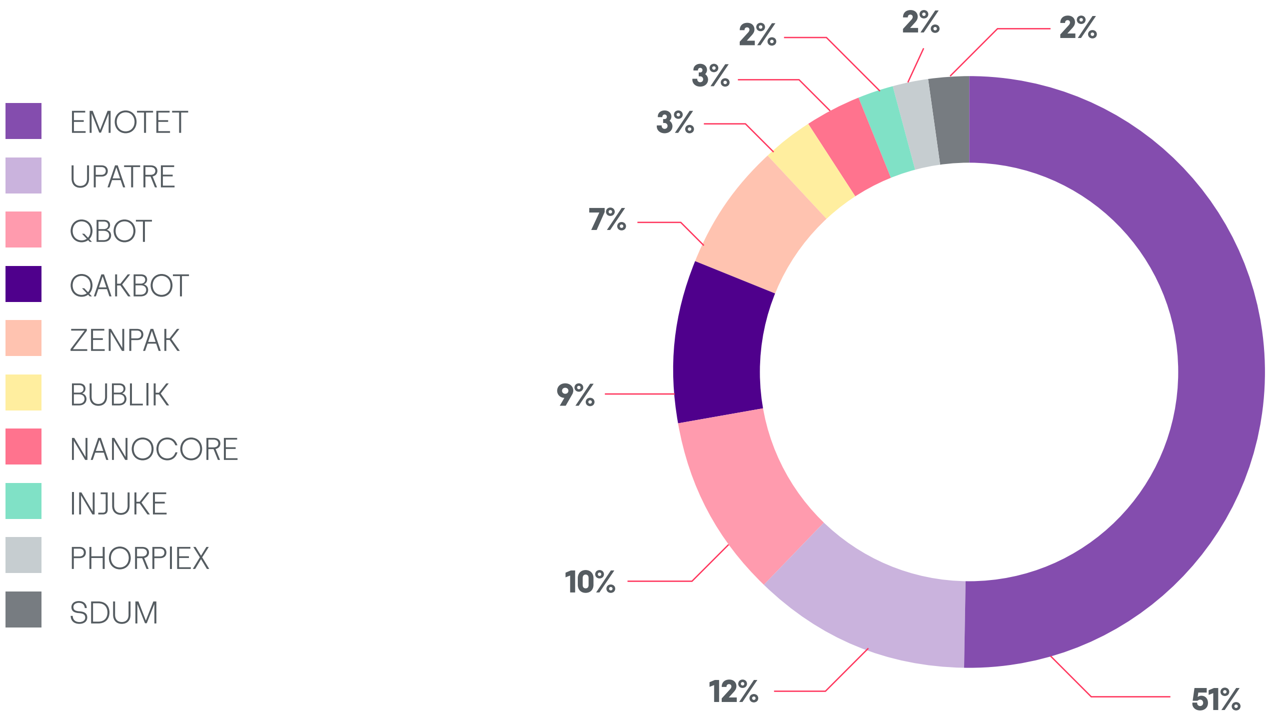
موجز:

يمكن تقسيم المنفذين الرئيسيين الذين يستهدفون منطقة الشرق الأوسط إلى فئتين رئيسيتين: منفذو الجرائم السيبرانية، وهي عبارة عن جهات تهديد ذات دوافع مالية. ومنفذو التجسس السيبراني، وهي جهات تهديد يتم تحفيزها بالمعلومات. وتعد سبع من الجهات العشر مجموعات تجسس سيبراني (Dalbit، وGamaredon Group (Primitive Bear)، وLazarus Group، و Turla، و Red-Apollo، OceanLotus (APT32)، وUAC-0056 (Ember Bear)) بينما تعد الجهات الثلاث المتبقية مجموعات جرائم سيبرانية (Emotet Group وTA505 وWizard Spider). ويشير هذا التقرير إلى أن غالبية أنشطة التهديد التي تستهدف الشرق الأوسط خلال الأشهر الستة الماضية، والمنسوبة إلى هذه الجهات، تم تنفيذها لسرقة معلومات حساسة. وقد تم جمع المعلومات التي تدعم هذه الرؤى من مصادر المعلومات الاستباقية من (Anomali) الخاصة بالمنفذين والبرامج الضارة المرتبطة بملفات تعريف المنفذين في مجال التهديد، والأخبار والاستشارات ومصادر البحث التي يحتفظ بها فريق أبحاث التهديد من (Anomali) على منصة (ThreatStream).

المصدر:

إحصائيات مستمدة من مصادر المعلومات الاستباقية الإقليمية خلال آخر 6 أشهر عن الهجمات (البرامج الضارة والمنفذين) من قنوات المعلومات الاستباقية من Anomali (البرامج الضارة والمهاجمين) المدعومة من شركاء Anomali وهم Polyswarm وBitdefender.

أهم 10 برامج خبيثة
ملاحظة في الشرق الأوسط



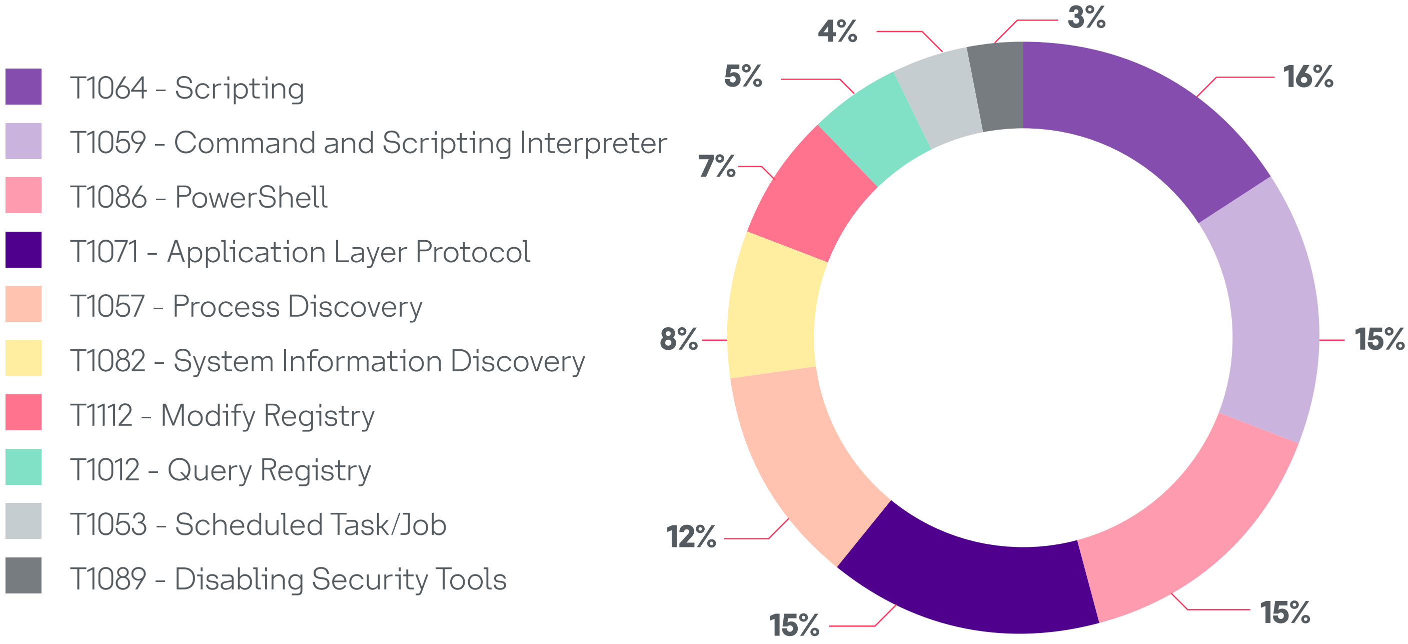
موجز:

كانت أهم ثلاث عائلات للبرمجيات الضارة (Emotet، وQbot، وUpatre)، والتي تمثل 73% من الهجمات التي تستهدف الشرق الأوسط، موجودة منذ ما يقرب من 10 سنوات أو أكثر. كما تُظهر عائلات البرمجيات الضارة هذه استمرارية مطوريها ومشغليها واستمرارهم في أداء الهجمات، بينما تسلط الضوء أيضًا على القيمة التي يراها المهاجمون في البرمجيات الخبيثة القياسية. حيث تُمكّنهم من تجربة طرق متعددة لتحقيق أهدافهم وتنفيذ المهام "أثناء التنقل" بدلاً من الاعتماد دائمًا على تعليمات مبرمجة مسبقًا.

المصدر:

إحصائيات مستمدة من مصادر المعلومات الاستباقية الإقليمية خلال آخر 6 أشهر عن الهجمات (البرامج الضارة والمنفذين) من قنوات المعلومات الاستباقية من Anomali (البرامج الضارة والمهاجمين) المدعومة من شركاء Anomali وهم Polyswarm وBitdefender.

أعلى 10 أساليب MITRE
مستخدمة في الشرق الأوسط



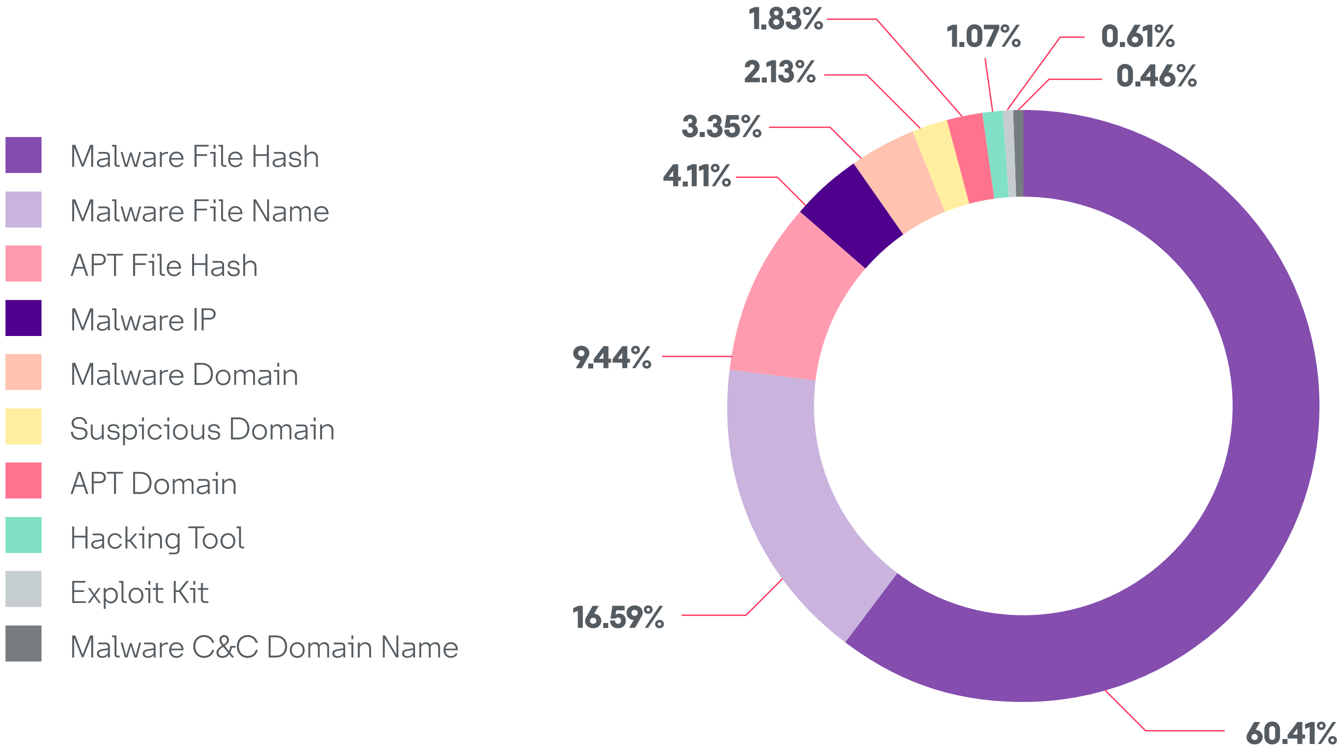
موجز:

تندرج الخطط والأساليب والإجراءات (TTPs) الأكثر استخداماً في الهجمات التي تستهدف الشرق الأوسط من الأكثر استخداماً إلى الأقل استخداماً، من الـ (TTPs) التي تتضمن استخدام البرامج النصية ومفسرات البرامج النصية، إلى الاتصال والاكتشاف، إلى الحفاظ على استمرارية الهجمات. واستخدمت الجهات الفاعلة المهددة والبرمجيات الضارة البرامج النصية (T1064 - Scripting) ومفسرات البرمجة النصية (T1059 - Command and Scripting Interpreter) لتنفيذ أوامر أو إدخال ملفات أو برامج نصية أخرى مثل (T1086 -PowerShell) في محاولات لإساءة استخدام وظائف النظام للقيام بإجراءات عشوائية على الجهاز المستهدف. وللاتصال، استخدم المهاجمون وأدواتهم (T1071 - Application Layer Protocol) التي يمكن استخدامها لإجراءات مختلفة مثل (DNS) والبريد الإلكتروني وتصفح الويب. أمّا في مرحلة الاكتشاف، فيتم استخدام (T1082 - System Information Discovery) واستخدام (T1112 - Modify Registry) استعلام السجل (T1012 - Query Registry) للاستعلام. وفي المرحلة النهائية، استخدمت الجهات الفاعلة والبرامج الضارة (T1053-ScheduledTask/Job) وأدوات التعطيل الأمنية (T1089 – Disabling Security Tool) للحفاظ على الاستمرارية وتجنب الاكتشاف.

المصدر:

إحصائيات مستمدة من مصادر المعلومات الاستباقية الإقليمة خلال آخر 6 أشهر عن الهجمات (البرامج الضارة والمنفذين) من قنوات المعلومات الاستباقية من Anomali (البرامج الضارة والمهاجمين) المدعومة من شركاء Anomali وهم Polyswarm وBitdefender.

أنواع التهديدات
الملاحظة في الشرق الأوسط



موجز:

تواصل منطقة الشرق الأوسط نموها السريع من خلال تحقيق الازدهار الاقتصادي بما يتجاوز مصادر النفط والغاز، حيث أثبتت بلدان كثيرة في المنطقة نفسها كمراكز رائدة للابتكار التقني، مستفيدة من أحدث الابتكارات في المدن الرقمية الجديدة. وإلى جانب ذلك، فقد وسّعت المنطقة نفوذها على المشهد العالمي، سواء اقتصادياً أو فيما يتعلق بالتحديات التي تواجه العالم. ورغم وجود الكثير مما يستحق الاحتفاء والفخر به، إلا أن كل هذا يجذب المزيد من الهجمات الإلكترونية.

ويُظهر الدافع مزيجاً من التجسس الإلكتروني لسرقة البيانات وعناوين بروتوكول الأنترنت (IP Address) الهجمات ذات الدوافع المالية والابتزاز المالي للمؤسسات، وبرامج الفدية، وحجب الخدمة، والاحتيال، والتصيد الاحتيالي. علاوة على ذلك، وكما شهدنا في مناطق أخرى، فإن انقطاع الخدمة والاستفادة من استمرارية انقطاعها يتزايدان كذلك. ويُبرز الرسم البياني المؤشرات الفنية التي تهدد المنطقة حيث تؤكد تحكم وسيطرة البرامج الضارة وما يرتبط بها من القيادة والسيطرة والبنية التحتية لشبكة الروبوتات على أساليب تشغيل الهجمات. ويؤكد كل هذا على الأهمية الحاسمة لفرض الرقابة الأمنية الشاملة والاستجابة المبنية على المعلومات المتعلقة بالتهديدات ذات الصلة، والتي تسمح للمؤسسات بالحد من المناطق المعرضة للهجوم بشكل ديناميكي والتصرف بسرعة ودقة لحماية أعمالها وعملائها وموظفيها مع ظهور تهديدات جديدة وتأثير الهجمات على عملياتها.

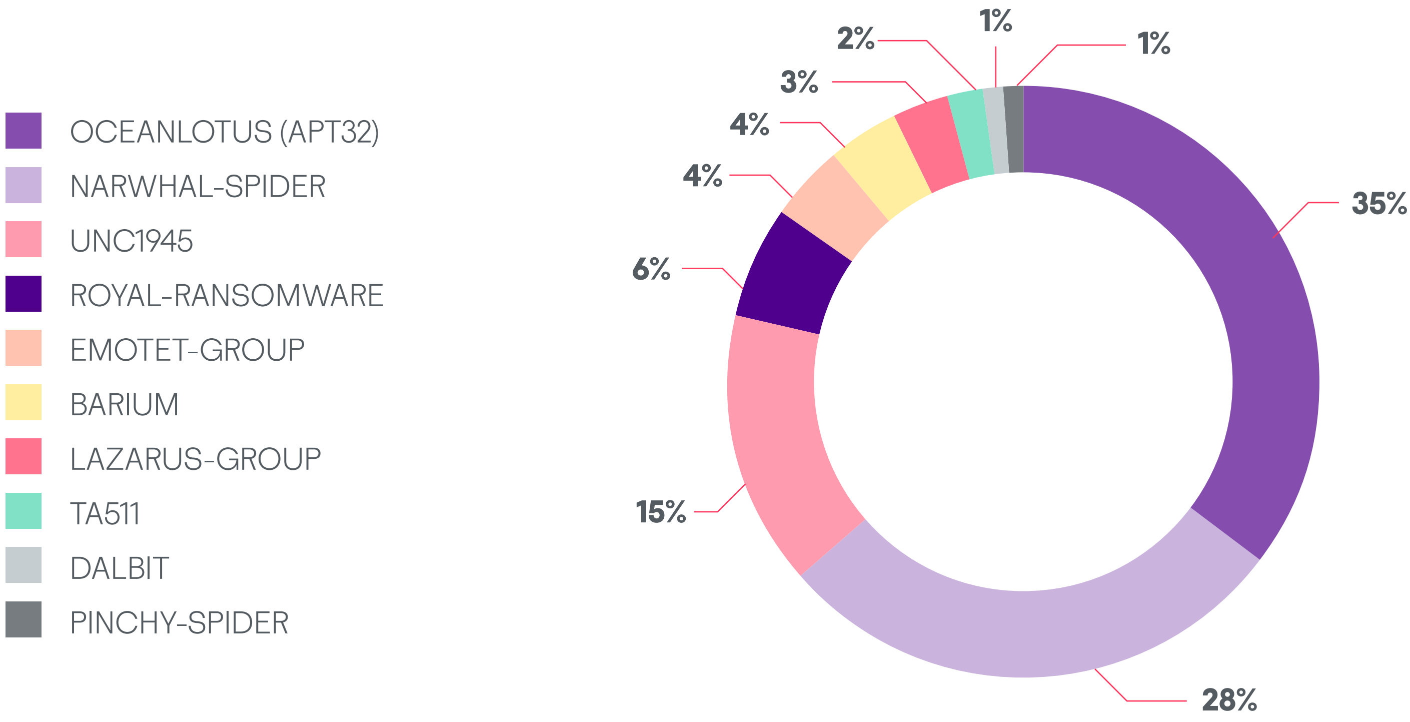
المصدر:

إحصائيات مستمدة من مصادر المعلومات الاستباقية الإقليمية خلال أخر 90 يوم والتي وردت من OSINT وقنوات المعلومات الاستباقية Anomali (البرامج الضارة والمهاجمين) المدعومة من شركاء Anomali وهم Polyswarm وBitdefender.

04

الإحصائيات الرئيسية في المملكة العربية السعودية

أعلى 10 تهديدات سيبرانية
ملاحظة في المملكة العربية السعودية



موجز:

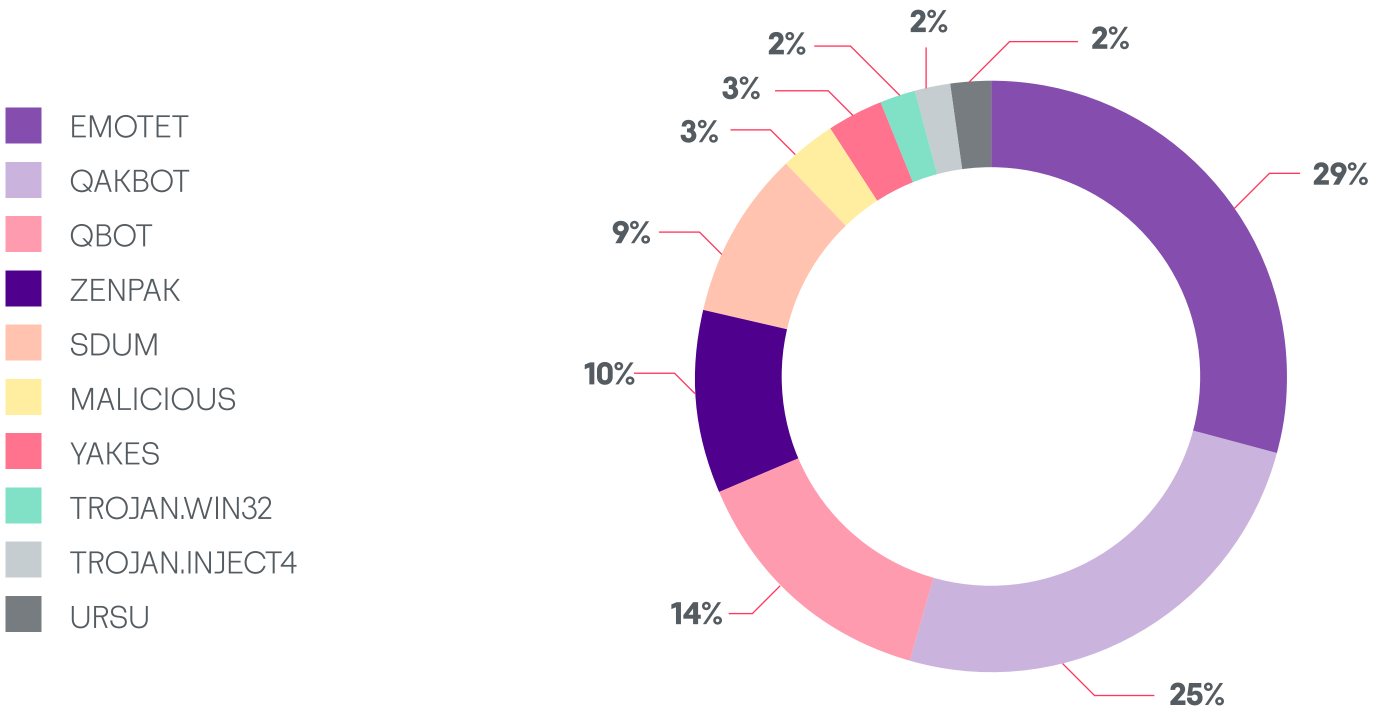
يمكـن تقسـيم المنفذيـن الرئيسـيين الذيـن يسـتهدفون المملكـة إلـى فئتيـن رئيسـيتين وهمـا: منفـذو الجرائـم السـيبرانية، وهـي جهـات تهديـد ذات دوافـع ماليـة، ومنفـذو التجسـس السـيبراني، وهـي جهـات تهديـد مدفوعـة بالمعلومـات. وتعـد سـبعة مـن الجهـات العشـر مجموعـات جرائـم إلكترونيـة (Dalbit، وEmotet ،Mealybug)، TA511، Royal Ransomware، Narwhal-Spider ، وPinchy Spider (Gold Southfield)، وUNC1945)، بينمـا تعـد الجهـات الـثلاث المتبقيـة هـي مجموعـات تجسـس إلكترونـي (Barium و ،(OceanLotus (APT32، وLazarus). ويبيـن هـذا التقريـر أنـه علـى مـدى الأشهر الستة الماضية، كان لدى غالبية المنفذين في مجال التهديد السيبراني التي استهدفت المملكة دوافع مالية.

المصدر:

إحصائيات مستمدة من مصادر المعلومات الاستباقية الإقليمة خلال آخر 6 أشهر عن الهجمات (البرامج الضارة والمنفذين) من قنوات المعلومات الاستباقية من Anomali (البرامج الضارة والمهاجمين) المدعومة من شركاء Anomali وهم Polyswarm وBitdefender.

أهم 10 برامج خبيثة

ملاحظة في المملكة العربية السعودية



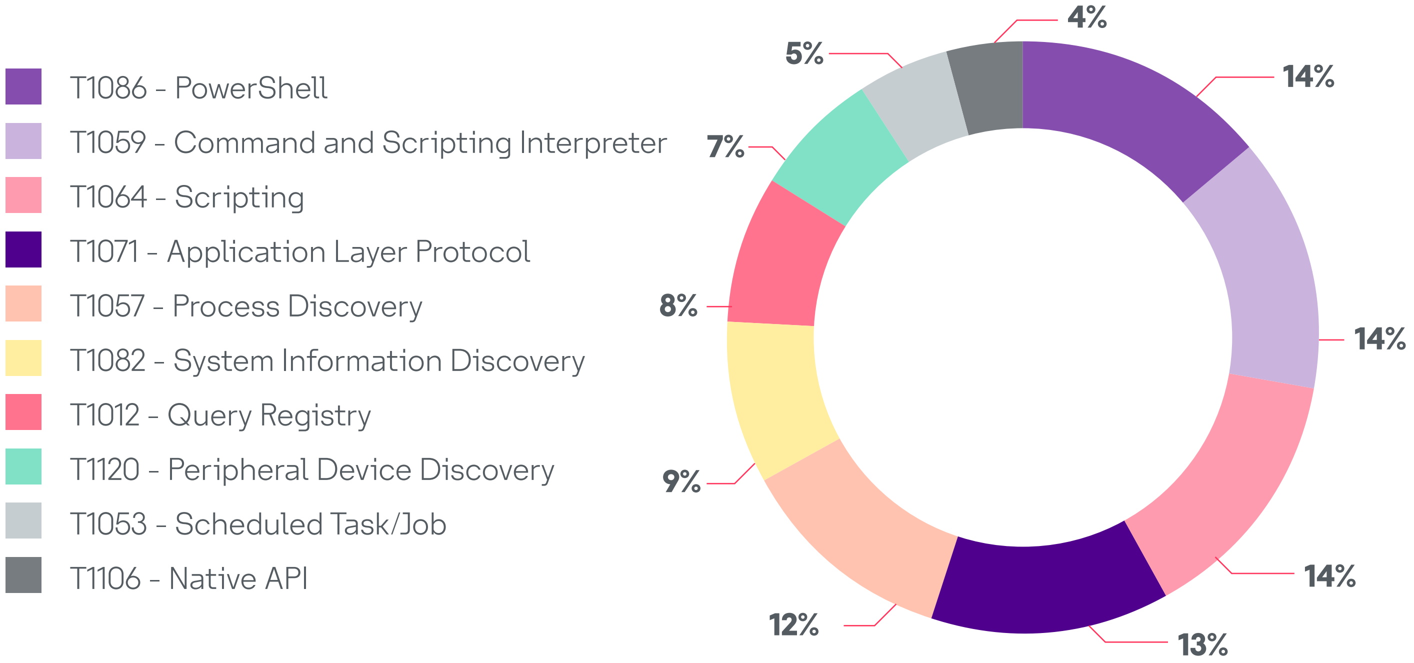
موجز:

تمثل المجموعات التالية (Emotet و Upatre و Qakbot) أكبر أربع مجموعات برمجيات ضارة استُخدِمت في 68% من الهجمات التي استهدفت المملكة العربية السعودية. ويبين هذا التقرير أن نفس الاتجاهات الخاصة بالبرمجيات الضارة التي تستهدف منطقة الشرق الأوسط يمكن تطبيقها أيضًا على البرمجيات الضارة التي تستهدف المملكة العربية السعودية فقط. وتعد عائلات البرمجيات الضارة هذه بمثابة منتج وغالبًا ما يتم توزيعها على نطاق واسع وبشكل عشوائي. وتتيح الوظيفة القياسية للبرمجيات الضارة لها العمل كعدة برامج ضارة في برنامج واحد، لا سيما مع القدرة على العمل كأداة تنزيل لملفات ضارة أخرى مع امتلاكها أيضًا القدرة على سرقة المعلومات و/ أو قدرات الفيروسات المتنقلة ذاتها.

المصدر:

إحصائيات مستمدة من مصادر المعلومات الاستباقية الإقليمة خلال آخر 6 أشهر عن الهجمات (البرامج الضارة والمنفذين) من قنوات المعلومات الاستباقية من Anomali (البرامج الضارة والمهاجمين) المدعومة من شركاء Anomali وهم Polyswarm وBitdefender.

أعلى 10 تقنيات MITRE
مستخدمة في المملكة العربية السعودية



موجز:

تندرج الخطط والأساليب والإجراءات (TTPs) الأكثر استخداماً في الهجمات التي تستهدف المملكة العربية السعودية، من الأكثر إلى الأقل، من الـ TTPs التي تتضمن استخدام البرامج النصية ومفسرات البرامج النصية، والاتصال والاكتشاف، والحفاظ على استمرارية الهجمات. وقد استخدمت الجهات المنفذة والبرمجيات الضارة البرامج النصية (T1086 – PowerShell) وتفاعلت مع مفسرات الأوامر والنصوص البرمجية (T1059 - Command and Scripting Interpreter) في محاولاتهم لتنفيذ البرامج النصية (T1064 - Scripting)، وبشكل أقل تكراراً مع واجهة برمجة التطبيقات الأصلية (T1106 - Native API) لتشغيل الأوامر وفتح التطبيقات أو الملفات. وللاتصال، استخدم المهاجمون وأدواتهم بروتوكولات طبقات التطبيقات (T1071 - Application Layer Protocol) التي يمكن استخدامها لإجراءات مختلفة مثل DNS والبريد الإلكتروني وتصفح الويب. وقد تم اتخاذ إجراءات الاكتشاف لتحديد العمليات (T1057 - Process Discovery)، ومعلومات النظام (T1082 - System Information Discovery)، وسجلات الاستعلام (T1012 - Query Registry)، واكتشاف الأجهزة الطرفية (T1120 - Peripheral Device Discovery). وفي مرحلة الحفاظ على استمرارية الهجمات، اعتمد المنفذين والبرامج الضارة بشكل كبير على المهام/ الوظائف المجدولة (T1106 - Native API).

المصدر:

إحصائيات مستمدة من مصادر المعلومات الاستباقية الإقليمة خلال آخر 6 أشهر عن الهجمات (البرامج الضارة والمنفذين) من قنوات المعلومات الاستباقية من Anomali (البرامج الضارة والمهاجمين) المدعومة من شركاء Anomali وهم Polyswarm وBitdefender.

05

معارك sirar

sirar
by stc

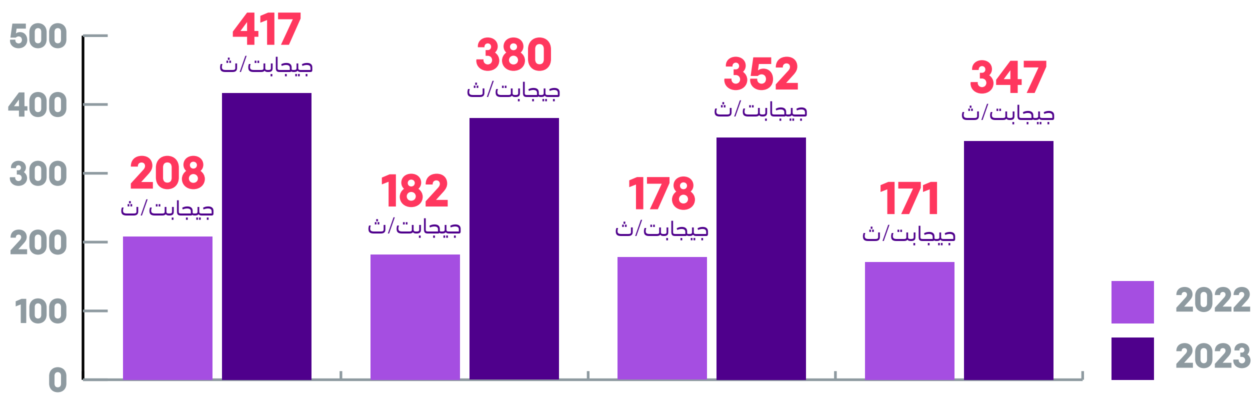
معارك sirar

الحماية من هجمات حجب الخدمة الموزعة

sirar
by stc

أكبر هجمات حجب الخدمة الموزعة

في المملكة العربية السعودية خلال عام 2023 بالمقارنة مع عام 2022



زاد متوسط حجم الهجمات بمعدل **121%**

أكبر **4** هجمات من حيث الحجم

حجم أكبر **هجمات حجب الخدمة الموزعة** التي تم التصدى لها عام **2022-2023**

مجموع ساعات توقف الخدمة التي تم منعها

2023
6,639 ساعة

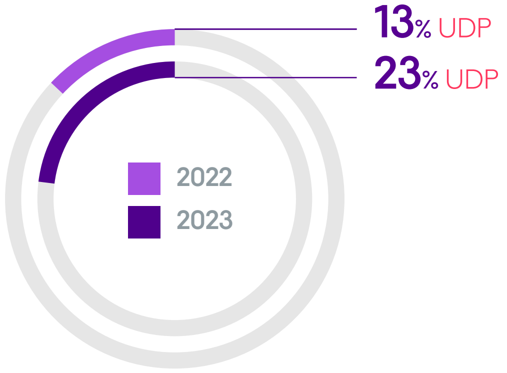
2022
5,560 ساعة

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

4 تيرابايت/ث

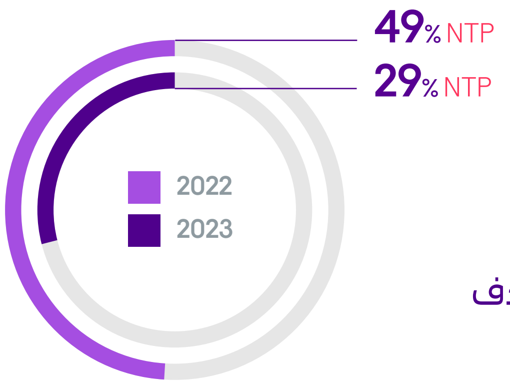
مراكز التقنية المحلية التابعة لـ sirar (وهي الأكبر في المنطقة) قادرة على التصدي لهجمات حجب الخدمة الموزعة على الصعيد المحلي والدولي حتى **4 تيرابايت** في الثانية (محليًا في المملكة)

تفاصيل هجمات
حجب الخدمة الموزعة



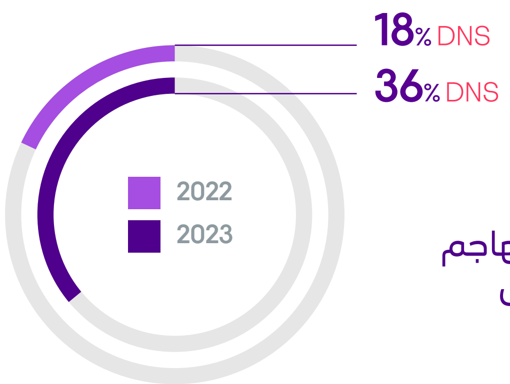
تدفق UDP

تبدأ هجمات حجب الخدمة الموزعة عندما يرسل المهاجم عددًا كبيرًا من حزم برتوكول بيانات المستخدم (UDP) إلى منافذ عشوائية أو إلى مضيف بعيد.



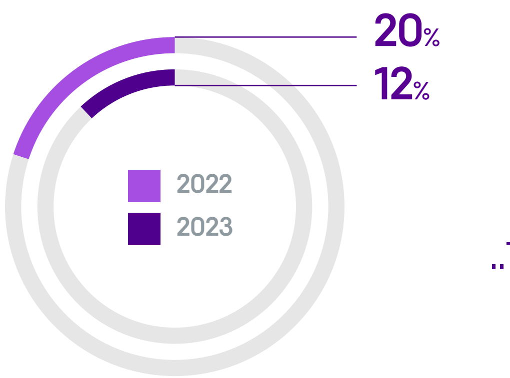
تضخيم NTP

تقوم هذه النوعية من هجمات حجب الخدمة الموزعة باستغلال خوادم بروتوكول وقت الشبكة (NTP) لإغراق الهدف بحركة بيانات NTP.



تضخيم DNS

يحدث الهجوم من خلال تضخيم (DNS) عندما يستهدف المهاجم خوادم DNS التكرارية المفتوحة وذلك لغرض استهلاك عرض النطاق الترددي بشكل مفرط.

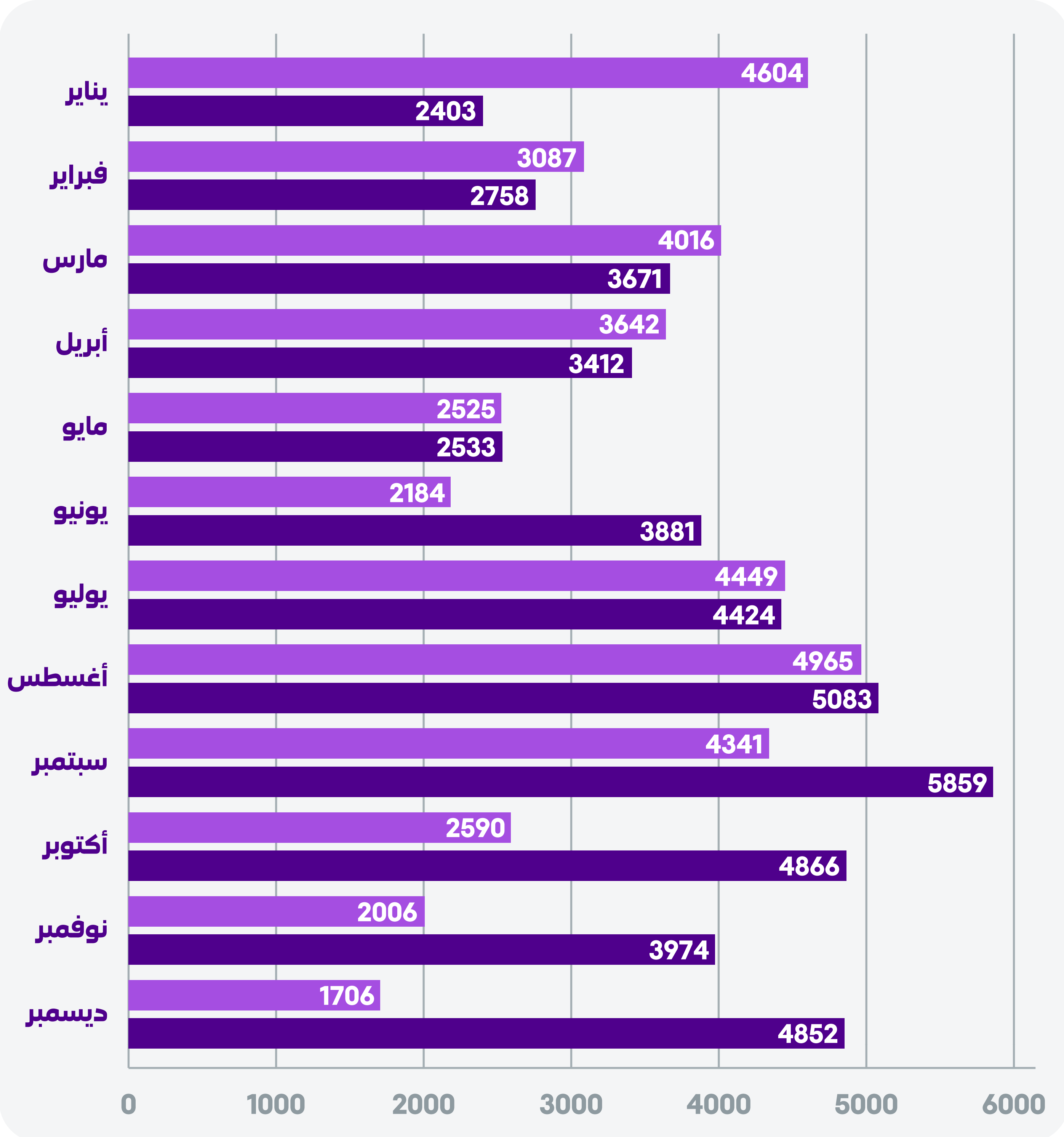


هجمات أخرى

هناك وسائل أخرى مثل TCP SYN, CLDAP, Memcache.. وغير ذلك.

أكبرهجمات حجب الخدمة الموزعة

عدد هجمات حجب الخدمة الموزعة في الشهر



2022 ■ 2023 ■

زاد عدد الهجمات بمعدل **19%**
مقارنة بالعام الماضي.

معارك sirar

إدارة الثغرات الأمنية وكشفها والاستجابة لها

sirar by stc

إدارة الثغرات الأمنية وكشفها والاستجابة لها (VMDR)

توفر خدمة إدارة الثغرات الأمنية وكشفها والاستجابة لها التي تقدمها ***sirar by stc*** التقييمات المستمرة لثغرات الأمن السيبراني للبنية الأساسية لديك وحالة الامتثال للضوابط.

احصل على رؤية شاملة عبر جميع أصول تقنية المعلومات، واعمل على أتمتة طريقة تحديد أولويات التهديدات، والتصحيح، وغير ذلك من الاستجابات الأخرى، لتستبق التهديدات المتطورة بما يعزز وضع الأمن السيبراني لديك، والعمل على حماية الأصول الهامة من خلال الاستفادة من هذه الخدمات الاستباقية.

	2022	2023
ثغرة أمنية تم إغلاقها	402 ألف	604 ألف
ثغرة أمنية تم كشفها	785 ألف	701 ألف

نحمي عملاءنا من خلال الفحص المستمر واكتشاف ثغرات أمنية بناءً على قاعدة بيانات الثغرات الأمنية لدى sirar وفقًا للمكتشف منها حديثًا لدى الجمهور.

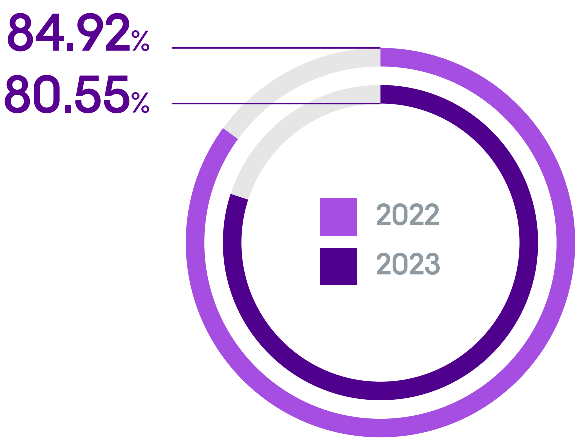
معارك sirar

حماية البريد الإلكتروني

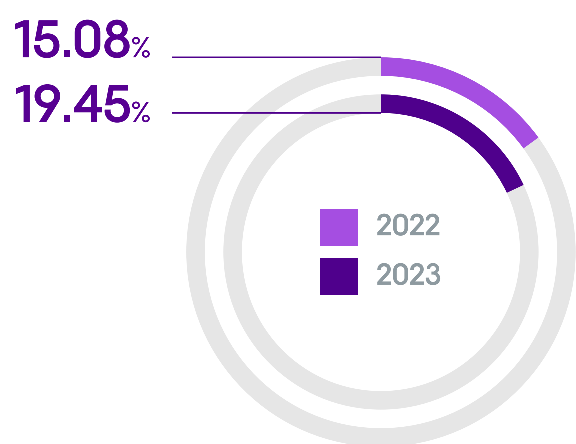
sirar by stc

حماية البريد الإلكتروني

تساعد خدمة حماية البريد الإلكتروني السحابية التي تقدمها ***sirar by stc*** في توفير حماية قوية ضد مجموعة كبيرة من تهديدات البريد الإلكتروني. فبفضل آليات الدفاع المتقدمة، تعمل هذه الخدمة على منع واكتشاف البريد العشوائي والتصيد الاحتيالي والبرامج الضارة وأحدث التهديدات وهجمات انتحال الشخصية وحوادث اختراق البريد الإلكتروني للشركات (BEC). وتغطي هذه الخدمة المعترف بها عالميًا دورة حياة البريد الإلكتروني بأكملها دون الحاجة إلى تثبيت أجهزة أو برامج في الموقع، ما يقلل من التعقيد والاحتياجات من الموارد.



نسبة رسائل البريد الإلكتروني النظيفة



نسبة رسائل البريد الإلكتروني الضارة

معارك sirar

الإنترنت الآمن

الإنترنت الآمن

خدمة الإنترنت الآمن من ***sirar by stc*** هي حل شامل عالي الأمان لحماية المؤسسات من مجموعة واسعة من التهديدات المنتشرة عبر الإنترنت. وتعمل هذه الخدمة على تبسيط إجراءات الأمان وخفض التكاليف وتحسين تجارب تصفح الويب من خلال بنية تحتية يتم توزيعها محليًا عبر الحوسبة السحابية. وبفضل الحماية التي يمكن توسيع نطاقها لجميع المستخدمين، تلغي هذه الخدمة الحاجة إلى إنشاء بنية تحتية واسعة النطاق للشبكة، ما يؤدي إلى خفض التكاليف وتبسيط عمليات الصيانة.

	2022	2023
إجمالي عدد التهديدات التي حجبتها sirar	2.4 مليون	7.3 مليون

أكثر من **200%** زيادة في عدد التهديدات المحجوبة.

التهديدات المتقدمة المحجوبة من خلال المعاملات التي جرت في 2023:

مواقع برامج الإعلانات المتسللة/ برامج التجسس	44%
التصيد الاحتيالي	28%
المحتوى الضار	24%
أخرى	4%

معارك sirar

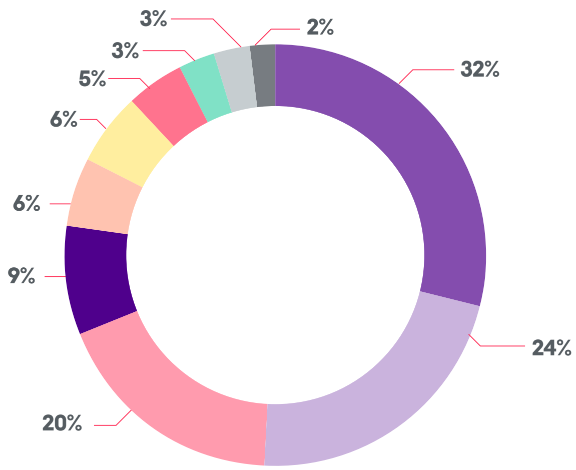
خدمة مركز عمليات الأمن السيبراني

sirar by stc

خدمة مركز عمليات الأمن السيبراني (SOCaaS)

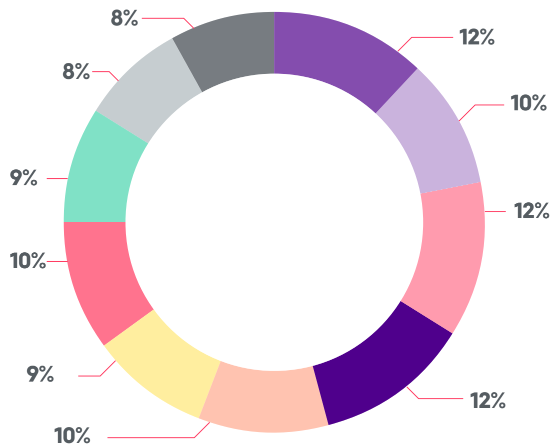
يقدم مركز عمليات الأمن السيبراني التابع لـ ***sirar by stc*** خدمة مراقبة واستجابة متميزة على مدار الساعة وطوال أيام الأسبوع. وتجمع حلولنا الشاملة بين الخبراء من ذوي المهارات العالية والتقنيات المتقدمة والامتثال للمعايير التنظيمية والرقابية. ويقع مقرنا في المملكة العربية السعودية، ونساعد المؤسسات على تحديد التهديدات السيبرانية والتصدي لها بشكل استباقي.

أكثر 10 هجمات شيوعًا:



- Brute Force
- Malicious/Suspicious connection
- Suspicious/Malicious file
- Unauthorized access
- Account Access Manipulation
- Web application attack
- Suspicious/Malicious process
- System Network Discovery
- Network Scanning
- Phishing Email

أكثر القطاعات المستهدفة:



- الحكومة والجيش
- الخدمات المالية
- الاتصالات
- التصنيع
- التعليم
- تكنولوجيا المعلومات
- النقل
- العقارات
- الطاقة
- الضيافة

معارك sirar

الاستجابة للحوادث

sirar
by stc

الاستجابة للحوادث

يقدم هذا القسم نظرة ثاقبة على حالات الاستجابة للحوادث (Incident Response) التي تعاملت معها sirar خلال عام 2023.

الوقت المستغرق للكشف عن التهديدات السيبرانية (Dwell Time)

يتم تعريف الوقت المستغرق للكشف عن التهديدات السيبرانية على أنه المدة التي يظل فيها التهديد السيبراني غير مكتشف داخل النظام، ويتم قياس الفترة اعتبارًا من الاختراق الأولي وحتى اكتشافه.

	عدد الأيام
متوسط الوقت المستغرق للكشف عن التهديدات السيبرانية	13

وسائل الهجوم الأولية

وسائل الهجوم الأولية تمثل الطريقة المحددة التي يستطيع من خلالها المخترق الدخول للشبكة.

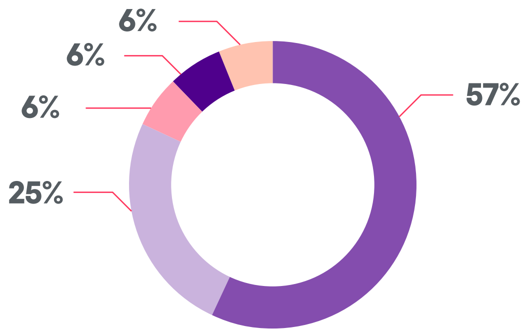
مصدر الاكتشاف

هو مقياس لاستعراض كيفية اكتشاف الهجوم، إما بالاكتشاف الذاتي، أو تنبيه من جهة خارجية أو من خلال رسالة بريد إلكتروني/ ملاحظة من المخترق.

الاستجابة للحوادث

فئات الهجمات

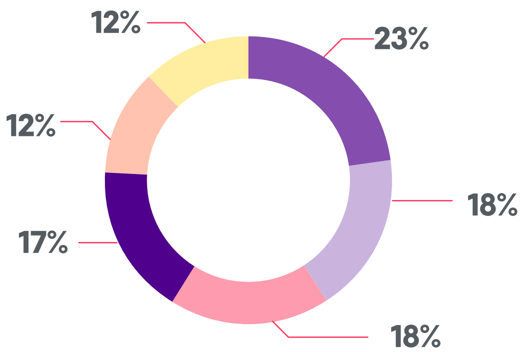
تشير فئات الهجمات إلى تصنيف التهديد السيبراني بناءً على أساليبه وتقنياته وأهدافه.



- هجمات تطبيقات الويب
- البرمجيات الخبيثة
- الوصول والدخول غير المصرح به
- الابتزاز السيبراني
- التصيد الاحتيالي

دوافع المهاجم

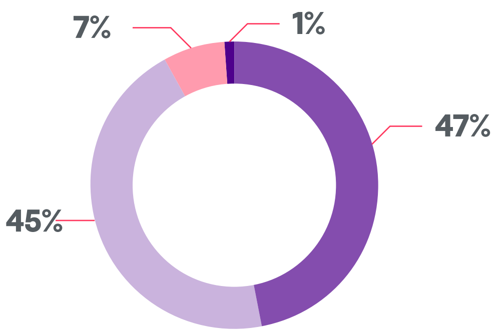
يشير دافع المهاجم إلى الأسباب أو الأهداف الكامنة التي تدفع فردًا أو مجموعة إلى المشاركة في الهجمات السيبرانية.



- اكتساب المعرفة
- الربح المالي
- اكتساب الوصول
- سرقة البيانات
- التخريب وتعطيل الخدمات
- السعي للشهرة واكتساب التقدير والاعتراف

مؤشرات الاختراق (IOCs) حسب الفئة

هي أدلة رقمية تستخدم للكشف عن وجود نشاط ضار أو اختراق داخل النظام أو الشبكة.



- دوال الاختزال للملفات (File Hash)
- عنوان بروتوكوب الإنترنت (IP Address)
- اسم النطاق (Domain Name)
- معرف البريد الإلكتروني

الاستجابة للحوادث

استغلال الثغرات الأمنية الشائعة

يتضمن استغلال الثغرات الأمنية الاستفادة من نقاط الضعف أو العيوب في أمان النظام للوصول غير المصرح به أو التلاعب بالنظام أو اختراقه، وغالبًا ما يستغل المهاجمون السيبرانيون الثغرات الأمنية لأهداف ضارة.

أوراكل لتخطيط موارد المؤسسات (ERP من Oracle)

CVE-2022-21587 درجة الأهمية 9.8

ثغرة أمنية في تنفيذ التعليمات البرمجية عن بُعد:

ثغرة أمنية في منتج Oracle Web Applications Desktop Integrator الخاص بـ Oracle E-Business Suite، ويمكن أن يؤدي استغلالها إلى تنفيذ تعليمات برمجية عن بعد غير مصادق عليها.

Apache Log4j2

CVE-2021-44228 درجة الأهمية 10.0

ثغرة أمنية في تنفيذ التعليمات البرمجية عن بُعد:

تم التعرف على ثغرة أمنية خطيرة في الإصدار 2.0.0 والإصدارات الأقدم من Apache Log4j. ويمكن للمهاجم تشغيل تعليمات برمجية عشوائية عن بعد عن طريق استهداف المكون الإضافي للبحث JNDI في خادم LDAP.

خادم Microsoft Exchange Server

تسمى مجموعة من الثغرات الأمنية المعروفة باسم ProxyShell والتي تستهدف خادم Microsoft Exchange Server للمهاجم بالإفلات من المصادقة وتشغيل التعليمات البرمجية باعتباره مستخدمًا ذو صلاحيات مرتفعة. ويمكن دمج الثغرات الأمنية الثلاث التالية واستخدامها في تنفيذ سلسلة هجوم فردية لـ ProxyShell:

CVE-2021-34473 درجة الأهمية 9.8

ثغرة أمنية في تنفيذ التعليمات البرمجية عن بُعد:

ثغرة أمنية في تنفيذ التعليمات البرمجية عن بُعد: يمكن أن تؤدي ثغرة المصادقة المسبقة في Microsoft Exchange -عند استغلالها- إلى قيام المهاجم بتجاوز التحكم في الوصول.

CVE-2021- 34523 درجة الأهمية 9.8

ثغرة تصعيد الصلاحيات:

يمكن للمهاجم استغلال ثغرة حديثة لتصعيد صلاحياته والوصول غير المصرح به إلى خادم Exchange.

CVE-2021-31207 درجة الأهمية 7.2

ثغرة تجاوز ميزة الأمان:

ثغرة ما بعد المصادقة في Microsoft Exchange والتي تستخدم الكتابة العشوائية للملفات التي يمكن أن تؤدي إلى تنفيذ التعليمات البرمجية عن بُعد (RCE).

Microsoft SharePoint

CVE-2019-0604 درجة الأهمية 9.8

ثغرة أمنية في تنفيذ التعليمات البرمجية عن بُعد:

ثغرة أمنية في تنفيذ التعليمات البرمجية عن بُعد: أدى عدم كفاية التحقق من صحة المدخلات أثناء فحص علامات المصدر لحزمة التطبيق إلى وجود ثغرة أمنية في Microsoft SharePoint. ويمكن للمهاجم الناجح في استغلال الثغرة الأمنية أن يصبح قادرًا على تنفيذ تعليمات برمجية عشوائية.

NetScaler ADC and NetScaler Gateway

CVE-2023-3519 درجة الأهمية 9.8

ثغرة أمنية في تنفيذ التعليمات البرمجية عن بُعد:

ثغرة أمنية تتعلق بإدخال التعليمات البرمجية بما يؤثر في NetScaler ADC وNetScaler Gateway، والتي يمكن للمهاجمين استغلالها عن طريق رفع ملفات واجهات أوامر الويب والبرامج النصية الضارة، ما يمكنهم من البحث في الشبكات واستخراج البيانات الخاصة.

تعتمد درجة الأهمية على الإصدار X.3 من نظام تسجيل الثغرات الامنية الشائعة (CVSS) والمقاس باستخدام قاعدة بيانات الثغرات الأمنية الوطنية (NVD) التابعة للمعهد الوطني للمعايير والتقنية (NIST).

يرجى الرجوع إلى صفحة المراجع للاطلاع على المصادر.

الاستجابة للحوادث

الربط مع إطار (MITRE ATT&CK)

ربط الخطط والأساليب والإجراءات (TTPs) التي يتبعها المهاجمون مع إطار (MITRE) بواسطة خارطة توزيع لاستعراض الخطط والأساليب الأكثر استخدامًا.

نسبة خطط وأساليب (MITRE ATT&CK) الأكثر استخدامًا

1-3% (green) · 4-6% (yellow) · >7% (red)

Reconnaissance

Technique
Active Scanning
Gather Victim Network Information

Resource Development

Technique
Stage Capabilities

Initial Access

Technique
Exploit Public-Facing Application
External Remote Services
Valid Accounts
Phishing

Execution

Technique
Command and Scripting Interpreter
System Services

Persistence

Technique
Boot or Logon Autostart Execution
Create Account
External Remote Services
Server Software Component (WebShell)
Valid Accounts
Create or Modify System Process

Privilege Escalation

Technique
Abuse Elevation Control Mechanism
Valid Accounts

Defense Evasion

Technique
Subvert Trust Controls
Impair Defenses

Credential Access

Technique
OS Credential Dumping
Brute Force
Unsecured Credentials
Adversary-in-the-Middle

Discovery

Technique
Account Discovery
File and Directory Discovery
Network Service Discovery
Network Share Discovery
Remote System Discovery
Software Discovery
System Information Discovery
System Network Configuration Discovery

Lateral movement

Technique
Remote Services

Collection

Technique
Data from Local System
Data from Network Shared Drive

Command and Control

Technique
Ingress Tool Transfer
Application Layer Protocol

Exfiltration

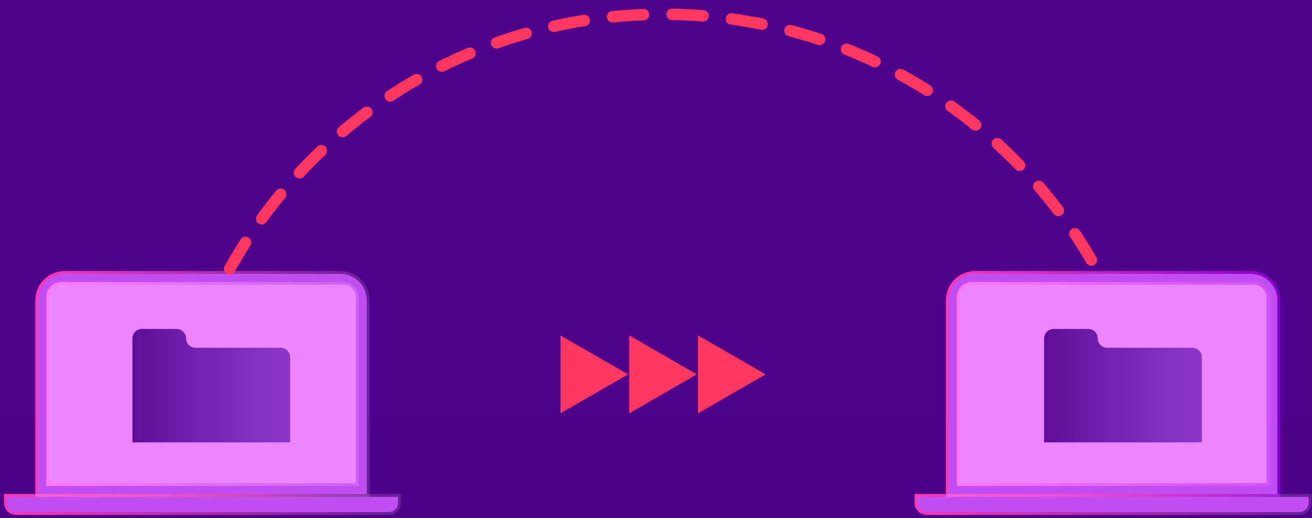
Technique
Automated Exfiltration
Exfiltration Over C2 Channel

Impact

Technique
Data Encrypted for Impact
Inhibit System Recovery
Defacement

06

توصيات عامة



sirar by stc

توصيات عامة

الثغرات الشائعة في الأمن السيبراني، إلى جانب التوصيات المقترحة لتعزيز الوضع الأمني للمؤسسات.

الوصول إلى الحسابات وإدارتها

1- التحكم في الوصول:

- تطبيق التحقق من الهوية متعدد العناصر (MFA) -إذا كانت مدعومة- على جميع تطبيقات المؤسسة أو التطبيقات الخارجية المعرضة لخطر الاختراق.
- تأمين الوصول الخارجي عن بُعد إلى موارد المؤسسة باستخدام الشبكة الافتراضية الخاصة (VPN).
- منع الأجهزة غير المُدارة وغير المتوافقة من الوصول إلى النظام الداخلي والاتصال به.

2- إدارة حسابات الشركات والوعي بها:

- وضع سياسات وإجراءات إدارة الحساب وتوثيقها وفرضها.
- إجراء جرد لجميع الحسابات ذات الصلاحيات الهامة والحساسة وإجراء مراجعة دورية وتحديث للحسابات المميزة لمنع الوصول غير المصرح به.
- تطبيق مبدأ الصلاحيات الأدنى للحسابات ذات الصلاحيات الهامة والحساسة وتنفيذ ضوابط الوصول المستندة إلى الأدوار (RBAC) لضمان وصول الموظفين فقط إلى الموارد اللازمة لأداء أدوارهم.
- توفير برامج تدريب وتوعية للموظفين بشكل منتظم لتثقيف الموظفين حول أهمية كلمات المرور القوية.

3- خاصية المصادقة متعددة العوامل:

- فرض تطبيق التحقق من الهوية متعدد العناصر (MFA) – إذا كانت مدعومة – لجميع المستخدمين والخدمات.
- دمج المصادقة متعددة العوامل مع أنظمة إدارة الهوية، حيثما ينطبق ذلك، للتحكم والمراقبة المركزية.
- إجراء تدقيق أمني منتظم لتحديد ومعالجة الثغرات الأمنية المحتملة في تنفيذ MFA.

4- إدارة كلمات المرور:

- وضع سياسة وإجراءات إدارة كلمات المرور وتوثيقها وتطبيقها.
- اعتماد استخدام حلول إدارة كلمات المرور، والتي من شأنها تحسين أمان كلمات المرور بشكل عام من خلال إنشاء كلمات مرور عشوائية وقوية.
- تثقيف الموظفين حول المخاطر المرتبطة بكلمات المرور الافتراضية وأهمية تغييرها.

أمان البنة التحتية

1. أدوات الإدارة عن بُعد:

- تحديد وتوثيق وتنفيذ سياسات التحكم في الوصول للتأكد من أن الموظفين المصرح لهم فقط هم من يمكنهم استخدام أدوات الإدارة عن بُعد.
- مراجعة أذونات الوصول وتحديثها بانتظام بناءً على الأدوار والمسؤوليات.
- تزويد الموظفين بالتدريب على الاستخدام المناسب لأدوات الإدارة عن بُعد، والتأكد من اطلاعهم على المخاطر الأمنية المحتملة، والتأكيد على أهمية الإبلاغ الفوري عن أي أنشطة مشبوهة.

توصيات عامة

2. استضافة البريد الإلكتروني خارجيًا:

- وضع وتوثيق وتنفيذ سياسات وإجراءات أمن البريد الإلكتروني الشاملة التي تشمل عناصر التحكم في الوصول وإدارة المستخدم وكلمة المرور والتشفير والنسخ الاحتياطي والاسترداد والإعدادات الآمنة.
- الالتزام باللوائح ذات الصلة المتعلقة بالبنية الأساسية للبريد الإلكتروني الخارجي.

3. أمن أجهزة المستخدمين:

- تطبيق حلول حماية أجهزة المستخدمين على جميع الخوادم وأجهزة المستخدمين.
- تطوير وتوثيق وتنفيذ عملية إدارة تصحيح منتظمة لمعالجة الثغرات الأمنية في أجهزة المستخدمين على الفور.
- تطوير وتوثيق وتنفيذ آليات التسجيل المناسبة من خلال الاستفادة من حل إدارة السجلات المركزي.

4. أمن شبكة الإنترنت:

- تنفيذ وتطبيق أدوات أمن الشبكة للحصول على رؤية شاملة للشبكة.
- تنفيذ تجزئة الشبكة، باستخدام الفصل المادي أو الفصل المنطقي أو كليهما من خلال استخدام جدران الحماية وقوائم التحكم في الوصول (ACLs) والشبكات المحلية الافتراضية (VLANs).
- تنفيذ إجراءات أمن الشبكة مثل جدران الحماية وأنظمة كشف/ منع التسلل (IDS/IPS) وحلول التحكم في الوصول إلى الشبكة (NAC) لتعزيز أمن الشبكة عن طريق التحكم في الأجهزة التي يمكنها الوصول إلى الشبكة وضمان التزامها بالمعايير الأمنية المطلوبة.

5. الإعدادات الآمنة:

- تطبيق الحد الأدنى من معايير الأمن الأساسية (MBSS) مع تطبيق أفضل الممارسات على كل الأصول لتعزيز الوضع الأمني العام.
- إنشاء عملية منهجية للمراجعة والتحديث الدوري للتكوينات الافتراضية للبرامج والأجهزة وأجهزة الشبكة ثم توثيقها وتطبيقها.
- الالتزام بالإرشادات الأمنية المقدمة من موردي الأجهزة والبرامج والامتثال لتوصياتهم المتعلقة بالتكوينات الآمنة وذلك لتقليل المخاطر المحتملة.

6. ضوابط الدفاع الأمني:

- تنفيذ ضوابط دفاعية قوية ومتنوعة لمراقبة أقسام الشبكة وجميع أجهزة المستخدمين على حدٍ سواء.
- إنشاء وتطبيق منهجية لاعتماد قدرات الاكتشاف والاستجابة ومراجعتها وتنقيحها بانتظام.
- صياغة سياسة وإجراءات وإرشادات واضحة لإدارة السجلات الأمنية بهدف الاكتشاف السريع والاستجابة للتهديدات الناشئة.

7. حماية خدمات الويب:

- تنفيذ إستراتيجية أمنية دفاعية متعمقة متعددة الطبقات، بما في ذلك جدار حماية تطبيقات الويب (WAF) أو تثبيت جدار حماية تطبيقات الويب على المستضيف إذا لم يكن (WAF) قابلاً للتطبيق.
- الالتزام بسياسة وعملية وإجراءات محددة جيدًا لإدارة الثغرات الأمنية لاكتشاف الثغرات الأمنية في الخدمات المنشورة.
- تنفيذ ضوابط أمنية للدفاع العميق (Defense-in-Depth).

توصيات عامة

حوكمة الأمن والعمليات

1. إدارة الأصول:

- وضع سياسات وإجراءات إدارة الأصول وتوثيقها وتنفيذها.
- إجراء جرد دقيق وحديث لجميع الأصول التي يجب أن تشمل جميع أجهزة المستخدمين (المادية والافتراضية)، وتطبيقات الأجهزة، وأجهزة الشبكة، وما إلى ذلك.
- استخدام أدوات اكتشاف الأصول للكشف والتنبيه تلقائيًا عن محاولات الأجهزة غير المصرح بها الوصول إلى الشبكة.

2. إجراء النسخ الاحتياطي:

- صياغة سياسات وإجراءات شاملة للنسخ الاحتياطي للبيانات تحتوي على جميع المعلومات الأساسية ثم توثيقها وتطبيقها.
- الاحتفاظ بنسخ احتياطية خارج المنشأة أو في موقع جغرافي بعيد لتقليل المخاطر المرتبطة بالكوارث الطبيعية.
- التأكد من امتثال ممارسات إدارة النسخ الاحتياطي للوائح المعمول بها في المجال وقوانين حماية البيانات التي تخضع لها المؤسسة.

3. إدارة التغيير:

- صياغة سياسات وإجراءات إدارة التغيير وتوثيقها وتطبيقها، على أن تحتوي على الخطوات اللازمة لاقتراح التغييرات ومراجعتها واختبارها واعتمادها وتطبيقها.
- إجراء تقييم مخاطر لكل تغيير مقترح لتقييم آثاره المحتمله على النظام والأمن والعمليات التجارية بشكلٍ عام.
- دمج عمليات إدارة التغيير مع عمليات إدارة الحوادث لضمان الاستجابة المنسقة في حالة حدوث مشكلات غير متوقعة نتيجة للتغيير.

4. خطة الاستجابة للحوادث (IRP):

- وضع خطة وإجراءات أمنية محددة تحديداً واضحاً للاستجابة للحوادث ومجموعة من الإجراءات التي يجب أن يتبعها فريق الاستجابة للحوادث.
- إجراء جلسات تدريبية منتظمة وتدريبات محاكاة للتأكد من أن فريق الاستجابة للحوادث على دراية بأدوارهم والإجراءات الموضحة في خطة الاستجابة للحوادث.
- مراجعة وتحديث خطة الاستجابة للحوادث بانتظام بناءً على التغييرات في بيئة تكنولوجيا المعلومات والتهديدات الناشئة والدروس المستفادة من الحوادث السابقة.

5. إدارة ورصد التسجيل:

- صياغة سياسات وإجراءات شاملة لإدارة السجلات وتوثيقها وفرضها.
- مراجعة وتعزيز قدرات الرقابة الحالية على أساس منتظم.
- نشر آليات المراقبة والكشف في الوقت الحقيقي لتحديد التهديدات المحتملة ومعالجتها على الفور (SIEM).

6. إدارة التصحيح:

- صياغة سياسات وإجراءات محددة لإدارة التصحيح وتوثيقها ثم تطبيق تلك السياسات والإجراءات.
- أدوات تصحيح مؤتمتة لتبسيط عملية استخدام أدوات تصحيح البرامج والثغرات الأمنية وتسريعها.
- إنشاء بيئة تجريبية بغرض تقييم أدوات تصحيح البرامج والثغرات الأمنية قبل استخدامها في الإنتاج.

توصيات عامة

7. **التوعية بالتصيد الاحتيالي عبر البريد الإلكتروني:**
- رفع وعي الموظفين من خلال توفير الدورات التدريبية والبرامج التوعوية المنتظمة لهم والقيام بحملات محاكاة التصيد الاحتيالي.
- إنشاء آلية سهلة الاستخدام للإبلاغ عن الرسائل الإلكترونية المريبة وتشجيع الموظفين على الإبلاغ عن هذه الرسائل.
- تقييم فاعلية مبادرات التوعية من التصيد الاحتيالي بانتظام من خلال استطلاعات الرأي أو الاختبارات أو الملاحظات والاستفادة من الآراء المتحصل عليها لتحسين البرامج التدريبية وتطويرها.

8. **التقييم الأمني:**
- صياغة سياسات وإجراءات التقييم الأمني وتوثيقها ثم تنفيذها.
- إجراء تقييمات أمن سيبراني دورية، بما في ذلك تقييم الثغرات الأمنية واختبار الاختراقات وعمليات التدقيق الأمني لتحديد الثغرات الأمنية في النظام ومن ثم معالجتها.
- مراجعة سياسات التقييم المطبقة بانتظام للتأكد من توافقها مع أفضل الممارسات الحالية في المجال والمتطلبات التنظيمية والتهديدات الناشئة.

إدارة التهديدات

1. **البحث الاستباقي المستمر عن التهديدات الأمنية:**
- إنشاء وتنفيذ برنامج محدد بدقة وشامل للبحث الاستباقي عن التهديدات الأمنية.
- الاستفادة من المعلومات المرصودة من خلال البرامج الراصدة للتهديدات للبقاء على اطلاع بأحدث الخطط والأساليب والإجراءات التي يستخدمها المنفذون.
- مراجعة نتائج أنشطة البحث الاستباقي عن التهديدات الأمنية بانتظام وتقييم فعالية الإجراءات التي يتم تنفيذها وإجراء التعديلات وفقًا لذلك.

2. **برنامج معلومات التهديدات:**
- تطوير برامج معلومات راصدة للتهديدات وذلك لتحديد أي ثغرات أمنية أو تهديدات بشكل استباقي قبل حدوث الهجوم.
- دمج المعلومات المرصودة عن التهديدات مع أدوات الأمان، مثل إدارة المعلومات والأحداث الأمنية (SIEM) ونظام كشف الاختراق (IDS) ومنعه (IPS) بغرض أتمتة عملية اكتشاف التهديدات والاستجابة لها.
- ربط البيانات المتحصل عليها من مصادر المعلومات الاستباقية بسجلات الأمن الداخلي ومعلومات الحوادث لتحديد الأنماط والمؤشرات المحتملة للاختراق.

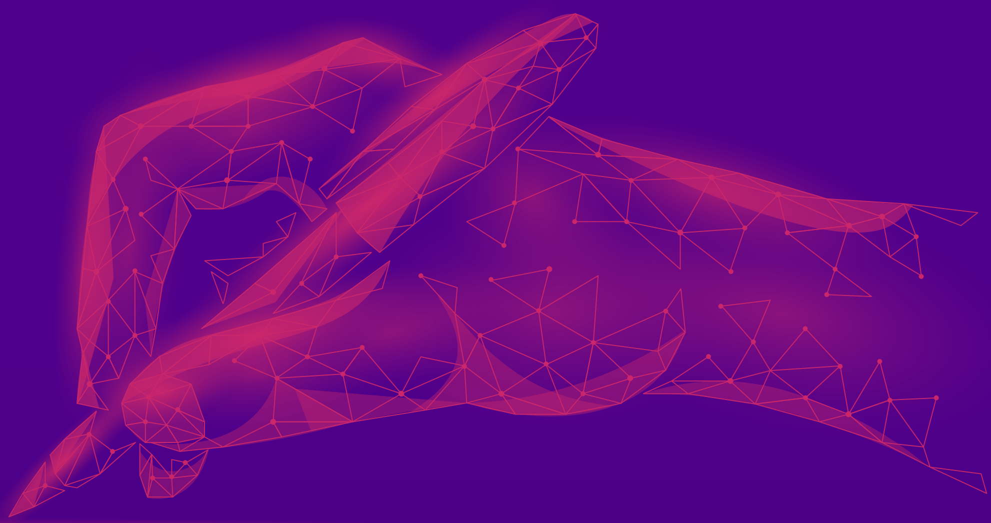
تخطيط القوى العاملة

1. **تثقيف موظفي الأمن السيبراني:**
- تشكيل فريق فني للأمن السيبراني مؤهل لاكتشاف التهديدات والاستجابة لها بكفاءة في الوقت المناسب.
- الاستفادة من الأدوات الأمنية المؤتمتة في إنجاز المهام الاعتيادية بما يتيح للموظفين الحاليين الفرصة للتركيز على مهام الأمن السيبراني الإستراتيجية الأكثر تعقيدًا.
- تقديم تدريبات وشهادات لموظفي الأمن السيبراني الحاليين بشكل مستمر بما يضمن مواكبة مهاراتهم مع متطلبات الأمن السيبراني.

07

رقمنة التوقيعات

مع "صاين"



sirar
by stc

رقمنة التوقيعات

مع "صاين"

نظرة عامة

خدمة التوقيع الرقمي "صاين" هي المزود المعتمد لتقنيات PKI وخدمات DTS، وهي خدمة مرخصة ومعتمدة من هيئة الحكومة الرقمية. وتضمن خدمة **صاين** المعززة تأمين تدفق المستندات من خلال التوقيعات الرقمية المشفرة، ما يضمن النزاهة والإقرار بأصالتها وصحتها واعتمادها. وتكتسب المؤسسات ميزة تنافسية من خلال تبني الرقمنة بثقة مع الحفاظ على الأمان وتحسين تجارب العملاء.

ميزات المنتج

- مسار عمل غير ورقي **وفعّال من حيث التكلفة** وغني ويسهل مشاركته والاطلاع عليه وتوقيعه
- يمكنك التوقيع من **أي جهاز** وفي **أي وقت** ومن **أي مكان**
- تسجيل **موثوق، وتوقيع مجموعة من المستندات مرة واحدة،** والدعم الفني **على مدار الساعة**

القيمة التجارية

- موثوق به من: جانب **WebTrust، Adobe، Microsoft، Google** وغيرها.
- يضمن النزاهة والإقرار **بأصالة** المستندات وصحتها ويحول دون التنصل منها.
- **مرخص** ومعتمد من هيئة الحكومة الرقمية.

حالات استخدام خدمة "صاين"

كيف استفادا قطاعي التجزئة والخدمات المصرفية من خدمة التوقيع الرقمي "صاين"؟

أثبتت خدمة التوقيع الرقمي **"صاين"** المبتكرة كونها حلاً جوهريًا في قطاعي التجزئة والخدمات المصرفية، حيث عززت بشكل كبير التجربة الشاملة للعملاء والموردين والموظفين على حد سواء. وبفضل سجلها الحافل الذي يضم أكثر من **142,000** معاملة، مع حفظ أكثر من مليون مستند ورقي، لم تُحدث صاين تحسينًا على المستوى التشغيلي فحسب، بل حققت أيضًا تقليصًا كبيرًا في الوقت ومدخرات كبيرة في التكلفة بلغت نسبتها **300%**، بما يعادل **2.1 مليون** ريال سعودي. ومن خلال الاستفادة من تقنية صاين المتطورة، شهدت المؤسسات المصرفية ومؤسسات التجزئة تحسنًاملحوظًا في التطبيقات عبر الإنترنت، وتبسيط إدارة العقود، وتحسين الخدمات المالية مثل بطاقات الائتمان والقروض. وقد أدى هذا الحل المبتكر بلا شك إلى رفع معايير خدمة العملاء والتميز التشغيلي في قطاعي البنوك والتجزئة.

حالات استخدام خدمة "صاين"

كيف ساعدت خدمة التوقيع الرقمي "صاين" قطاعي المشتريات والموارد البشرية؟

برزت خدمة التوقيع الرقمي **"صاين"** باعتبارها حلًا مبتكرًا يعزز بشكل فعّال من إدارة الموردين ويعزز رضا الموظفين في قطاعي الموارد البشرية والمشتريات. في إطار هذين القطاعين، حققت خدمة صاين إنجازات ملحوظة، حيث عملت على تسهيل أكثر من **64،000** معاملة وتوفير ما يقرب من **640،000** ورقة. وقد انعكس هذا في توفير كبير في الوقت والتكلفة بنسبة بلغت **300%**، أي ما يعادل **مليون ريال سعودي**. ومن خلال دمج خدمة **"صاين"** في عملياتها، شهدت الشركات تحسنًا كبيرًا في طلبات الشراء من الموردين، وإدارة العقود، بالإضافة إلى تبسيط عروض وعقود العمل. وساهمت تقنية صاين في رسم صورة لتعزيز الكفاءة، وتحسين العلاقات مع الموردين، وزيادة رضا الموظفين في قطاعي الموارد البشرية والمشتريات.

08

قاموس مصطلحات sirar

sirar
by stc

قاموس مصطلحات sirar

قوائم التحكم في الوصول (Access Control Lists "ACLs"):
القواعد التي تسمح بالوصول إلى جهاز الكمبيوتر أو ترفضه.

اكتساب الوصول (Access Gaining):
دافع المهاجم المتمثل في الوصول للنظام المستهدف.

رسالة بريد إلكتروني/ ملاحظة من المهاجم (Attacker Email/Note):
رسالة يرسلها المهاجم وعادة ما تكون في شكل رسالة بريد إلكتروني أو ملاحظة لإخطار المؤسسة بحدوث اختراق ناجح للشبكة، وغالبًا ما تكون مصحوبة بتهديدات أو طلبات أو محاولات ابتزاز.

دوافع المهاجم (Attacker Motivation):
الأسباب أو الأهداف الكامنة التي تدفع فردًا أو مجموعة إلى تنفيذ الهجمات السيبرانية والاشتراك فيها.

النقاط المعرضة للاختراق (Attack Surface):
عدد جميع النقاط المحتملة، أو وسائل الهجوم، والتي يمكن من خلالها للمستخدم غير المخوّل الوصول إلى النظام واستخراج البيانات.

وسائل الهجوم (Attack Vector):
طريقة وصول المهاجمين إلى الشبكة أو النظام.

الثغرات الأمنية والتعرضات الشائعة (Common Vulnerabilities and Exposures "CVE"):
قائمة بالعيوب الأمنية للكمبيوتر المفصَح عنها علنًا.

الابتزاز السيبراني (Cyber Extortion):
قيام المهاجم بتهديد الأفراد أو الشركات أو المؤسسات أو ابتزازهم للحصول على أموال أو أصول قيّمة أخرى.

الأمن السيبراني (Cybersecurity):
فن حماية الشبكات والأجهزة والبيانات من الوصول غير المصرح به أو الاستخدام لأغراض إجرامية وممارسات ضمان سرية المعلومات وسلامتها وتوافرها.

سرقة البيانات (Data Theft):
عندما يهدف المهاجم إلى سرقة المعلومات الرقمية المخزنة على أجهزة الكمبيوتر أو الخوادم أو الأجهزة الإلكترونية للحصول على معلومات سرية أو اختراق الخصوصية.

هجمات حجب الخدمة الموزعة (DDoS):
هجوم حجب الخدمة الموزعة هو محاولة خبيثة لتعطيل حركة البيانات الاعتيادية على الخادم وتعطيل قدرة الخادم أو الشبكة على العمل أو إخراج الموقع أو التطبيق المستهدف عن الخدمة من خلال إغراق الهدف أو ما يحيط به من البنية التحتية بفيض من حركة البيانات على الإنترنت.

خوادم نظام أسماء النطاق (DNS Servers):
خادم نظام اسم النطاق هو خادم حاسوب يحتوي على قاعدة بيانات لعناوين (IP) العامة للوصول إليها وأسماء المضيفين المرتبطة بها.

قاموس مصطلحات sirar

الوقت المستغرق للكشف عن التهديدات السيبرانية (Dwell time):

يتم تعريفه على أنه المدة التي يظل فيها التهديد السيبراني غير مكتشف داخل النظام، ويتم قياس الفترة اعتبارًا من الاختراق الأولي وحتى اكتشافه.

أجهزة المستخدمين (Endpoint):

هـي الأجهزة التي تتصل بنظام الشـبكة مثل الأجهزة المحمولـة وأجهزة الكمبيوتر والأجهـزة الافتراضية والأجهزة المدمجة والخوادم.

البرامج الانتهازية (Exploits):

هي جزء من برنامج أو بيانات تنتهز عيبًا في نظام التشغيل أو التطبيق للسماح لمُنفذين غير مصرح لهم بالوصول لتلك الأنظمة أو التطبيقات. ويمكن استخدام البرامج الانتهازية هذه لتثبيت المزيد من البرامج الضارة أو لسرقة البيانات.

الكسب المالي (Financial Gain):

عندما يكون دافع المهاجم هو تحقيق مكاسب مالية، فإنه يسعى إلى سرقة معلومات حساسة، مثل بيانات بطاقة الائتمان أو المعلومات الشخصية أو بيانات اعتماد تسجيل الدخول، والتي يمكنه بيعها في السوق السوداء، أو استخدامها في أنشطة احتيالية، أو طلب دفع فدية.

جدران الحماية (Firewalls):

جهاز أمان الشـبكة الذي يراقب ويصفي حركة مرور الشـبكة الواردة والصادرة بناءً على سياسـات الأمان الموضوعة مسـبقًا للمؤسسة.

خطة الاستجابة للحوادث (Incident Response Plan "IRP"):

هي عملية توثيق لمجموعة محددة مسـبقًا من التعليمات أو الإجراءات الهادفة إلى اكتشـاف عواقب الهجمات السـيبرانية الضارة على أنظمة معلومات المؤسسة والتصدي لها والحد منها.

مؤشرات الاختراق (Indicators of Compromise "IoC"):

الأدلة والقرائن التي تفيد بوقوع اختراق للبيانات.

أنظمة اكتشاف الاختراق (Intrusion Detection Systems "IDS"):

أداة تأمين الشبكة التي تراقب حركة مرور الشبكة بحثًا عن أي نشاط مشبوه والتنبيه عند اكتشاف مثل هذا النشاط.

أنظمة منع الاختراق (Intrusion Prevention Systems "IPS"):

أداة تأمين الشبكة التي تراقب الشبكة بشكل مستمر بحثًا عن أي نشاط ضار وتتخذ الإجراءات اللازمة لمنعه.

اكتساب المعرفة (Knowledge Gaining):

دافع المهاجم المتمثل في جمع بيانات عن النظام المستهدف وبنيته التحتية.

البرامج الضارة (Malware):

البرامـج الضارة هـي برامج اختراق مصممة لتخريب وتدمير أجهـزة الكمبيوتر وأنظمتها. ويعتبر مصطلـح "Malware" اختصارًا لمصطلـح "malicious software". وتشـمل الأمثلـة الشـائعة للبرامج الضارة فيروسـات الكمبيوتر والفيروسـات المتنقلة (worms) وأحصنة طروادة وبرامج الإعلانات المتسللة (adware) وبرامج التجسس و برامج الفدية.

قاموس مصطلحات sirar

الحد الأدنى لمعايير الأمن (Minimum Baseline Security Standard "MBSS")
مجموعة من الإرشادات والمتطلبات لضمان أمن نظم المعلومات والبيانات.

إطار 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.

خاصية المصادقة متعددة العوامل (Multi-Factor Authentication "MFA"):
طريقة المصادقة الإلكترونية التي لا يتم منح المستخدم إمكانية الوصول إلى موقع ويب أو تطبيق من خلالها إلا بعد تقديم دليلين أو أكثر بنجاح إلى آلية المصادقة.

مبدأ الحاجة إلى المعرفة (Need-To-Know Principle):
يجب إلا يتمتع المستخدم بإمكانية الوصول إلى المعلومات التي تتطلبها وظيفته.

التحكم في إمكانية الوصول إلى الشبكة (Network Access Control "NAC"):
حل أمني يفرض السياسة على الأجهزة التي تصل إلى الشبكات لزيادة رؤية الشبكة وتقليل المخاطر.

بروتوكول وقت الشبكة (Network Time Protocol "NTP"):
هو بروتوكول يساعد على مزامنة أوقات ساعة أجهزة الكمبيوتر في الشبكة.

هجمات التصيد الاحتيالي (Phishing Attacks):
هجمات التصيد الاحتيالي هي عملية تنفيذ اتصالات احتيالية تبدو في الظاهر أنها واردة من مصدر موثوق. يتم تنفيذها 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 نوعًا شائعًا من الهجمات السيبرانية التي تستغل أضعف حلقة في الأمن السيبراني وهو العنصر البشري.

مبدأ الحد الأدنى للصلاحيات (Principle of Least Privilege "PoLP") :
يجب ألا يحظى المستخدم أو الجهة بإمكانية الوصول إلى البيانات والموارد والتطبيقات المحددة اللازمة لإكمال المهمة المطلوبة.

هجوم برامج الفدية (Ransomware Attack):
هو نوع من البرامج الضارة التي يستخدمها المهاجمين عبر الإنترنت بشكل نشط لتخريب المنظمة المستهدفة من خلال تشفير الملفات الهامة للمنظمة وجعلها غير مقروءة ويتم طلب فدية مقابل إلغاء التشفير.

التخريب وتعطيل الخدمات (Sabotage and Disruption):
عندما يهدف المهاجمون إلى تعطيل البنية التحتية أو الخدمات أو العمليات الحيوية لأسباب سياسية أو أيديولوجية.

الاكتشاف الذاتي (Self-Detection):
الاكتشاف بمعرفة المؤسسة.

طرف ثالث (Third Party):
هو جهة خارجية أو فرد لا يرتبط مباشرة بالمؤسسة.

مُنفّذ التهديد (Threat Actor):
هو شخص أو مجموعة من الأشخاص يشاركون في إجراء يهدف إلى إلحاق الضرر بالعالم السيبراني بما يشمل أجهزة الكمبيوتر أو الأجهزة أو الأنظمة أو الشبكات.

البحث عن الإثارة (Thrill-Seeking):

عندمـا يكون المهاجم مدفوعًا بحلم الشـهرة والتحدي والإثارة المتمثلة في اختراق الأنظمة أو الشـبكات أو مواقع الإنترنت وربمـا للحصول علـى التقدير في مجتمع المخترقين. وبعبـارات أخرى، يمكن القول أن بعض المخترقين يريدون اكتسـاب حق التفاخر فيما بينهم.

برنامج حصان طروادة (Trojan):

هـو برنامـج ضـار في الظاهر يبدو أنه برنامج مشـروع متخفي فـي صورة برامج نظام تشـغيل أصلية أو ملفـات غير ضارة مثل التنـزيلات المجانيـة. ويتم تثبيت أحصنة طروادة من خلال تقنيات الهندسـة الاجتماعية مثل مواقـع الإنترنت الخاصة بالتصيد الاحتيالي أو كطُعم.

الوصول غير المصرح به (Unauthorized Access):

يحـدث الوصـول غير المصرح به عندما يتم الدخول إلى النظام من قبل شـخص غير مصرح له بالاتصال بالنظام أو اسـتخدامه بطريقة غير مقصودة من جانب مالك النظام.

المسح غير المصرح به (Unauthorized Scanning):

يتضمن المسح غير المصرح به فحص أنظمة الكمبيوتر أو تحليلها دون الحصول على إذن مناسب، وعادةً ما يكون ذلك بقصد الضرر لتحديد نقاط الضعف والثغرات الأمنية ونقاط الدخول المحتملة لتحقيق الوصول غير المصرح به.

بروتوكول مخطط بيانات المستخدم (User Datagram Protocol "UDP"):

هو بروتوكول في طبقة النقل، وهو جزء من مجموعة بروتوكولات الإنترنت التي 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 وقادرة على تحمل فقدان البيانات عبر الشبكة. كما يتيح بروتوكول UDP عملية معالجة الاتصال.

الشبكات المحلية الافتراضية (Virtual LANs "VLAN"):

اتصال افتراضي يربط عدة أجهزة وعُقد من شبكات محلية مختلفة في شبكة منطقية واحدة.

الشبكة الافتراضية الخاصة (Virtual Private Network "VPN"):

آلية لإنشـاء اتصال آمن بين جهاز الكمبيوتر وشـبكة أجهزة الكمبيوتر، أو بين شـبكتين، باستخدام وسيلة اتصال غير آمنة مثل شبكة الإنترنت العامة.

جدار حماية تطبيقات الويب (Web Application Firewall "WAF"):

جدار الحماية الذي يحمي تطبيقات الويب عن طريق تصفية ومراقبة حركة مرور الـHTTP بين تطبيق الويب والإنترنت.

هجمات تطبيقات الويب (Web Attack):

تسـتهدف الثغـرات الأمنيـة في مواقع الإنترنت للوصول بشـكل غير مصرح بـه، أو للحصول على معلومات سـرية، أو لتقديم محتوى ضار، أو لتغيير محتوى مواقع الإنترنت.

تشويه موقع الويب (Web Defacement):

هو الهجوم على مواقع الويب بهدف تغيير مظهر أو شكل الموقع أو الصفحة المستهدفة.

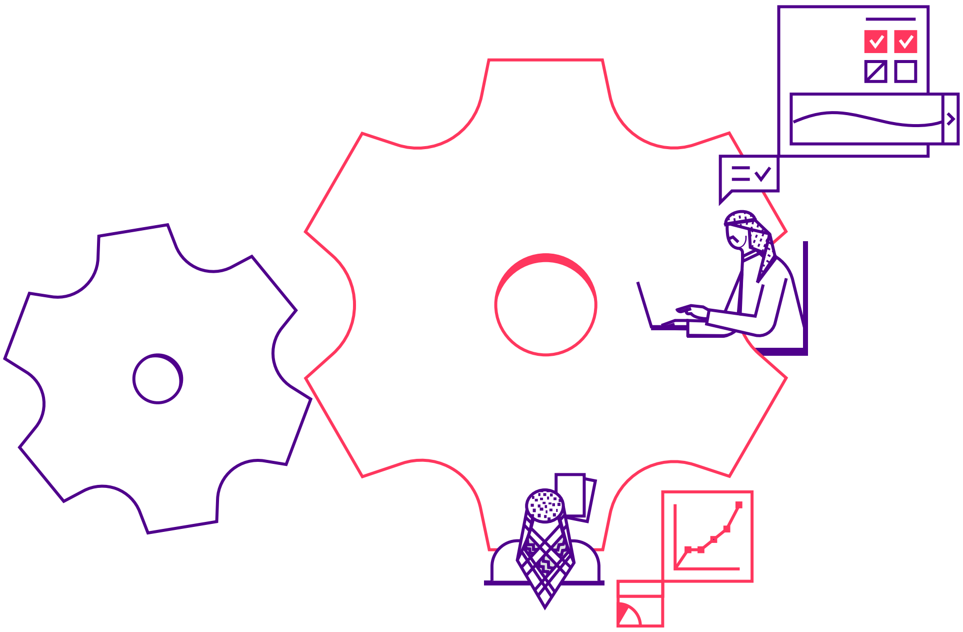
قاموس مصطلحات sirar

واجهات أوامر الويب (WebShell):

برنامج نصي للويب يتم وضعه على خادم ويب يمكن الوصول إليه بشــكل مفتوح للســماح للمهاجم باســتخدام خادم الويب كبوابة إلى الشبكة.

الإدراج على القائمة البيضاء (Whitelisting):

عدم السماح بالوصول إلى نظام أو شبكة أو خدمة معينة إلا للمدرجين على القوائم المعتمدة والمحددة بشكل صريح (مثل البرامج أو المستخدمين أو الجهات، أو غير ذلك) مع حظر جميع الآخرين.



09

المراجع

المراجع

Cisco. (2022, December 21). What is phishing? Cisco.
https://www.cisco.com/c/en/us/products/security/email-security/what-isphishing.Html

Ransomware spotlight: Clop. Security News.
https://www.trendmicro.com/vinfo/us/security/news/ransomwarespotlight/ransomware-spotlight-clop

What is a distributed denial-of-service (ddos) attack? - cloudflare.
https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/Network time protocol (NTP). GeeksforGeeks.
https://www.geeksforgeeks.org/network-time-protocol-ntp/

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

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

What is malware? - definition and examples. Cisco. (2023, November 16).
https://www.cisco.com/site/us/en/learn/topics/security/what-is-malware.html#:~:text=Malware%2C%20short%20for%20malicious%20software,spyware%2C%20adware%2C%20and%20ransomware.

10 most common types of cyber attacks today - crowdstrike. crowdstrike.com. (2023, November 9).
https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/

Yasar, K. (2023, July 18). What is cyber extortion?: Definition from TechTarget. Security.
https://www.techtarget.com/searchsecurity/definition/cyberextortion#:~:text=Cyber%20extortion%20is%20a%20broader,money%20or%20other%20valuable%20assets.

Unauthorized access. Information Security. (2017, December 20).
https://security.tennessee.edu/unauthorized-access/#:~:text=Unauthorized%20Access%20is%20when%20a,for%20this%20is%20%E2%80%9Chacking%E2%80%9D.

Web attacks. CIS. (2021, June 15).
https://www.cisecurity.org/insights/spotlight/ei-isac-cybersecurity-spotlight-web-attack

Business advisories. Advisories || Business.
https://www.csa.gov.gh/website_defacement.php#:~:text=Website%20defacement%20is%20an%20attack,is%20a%20form%20of%20vandalism.

Server software component: Web shell. Server Software Component: Web Shell, Sub-technique T1505.003 - Enterprise | MITRE ATT&CK®.
https://attack.mitre.org/techniques/T1505/003/#:~:text=A%20web%20shell%20is%20a%20web%20script%20placed%20on%20an,the%20broader%20server%20operating%20system.

Kaspersky. (2023, April 19). What is data theft and how to prevent it. me.
https://me-en.kaspersky.com/resource-center/threats/data-theft

Threat actors explained: Motivations and capabilities. SOPHOS. (2024, January 12).
https://www.sophos.com/en-us/cybersecurity-explained/threat-actors#:~:text=Some%20common%20motivations%20for%20threat,or%20use%20for%20fraudulent%20activities.

What is a Network Access Control List (ACL)?. Fortinet.
https://www.fortinet.com/resources/cyberglossary/network-access-control-list#:~:text=An%20access%20control%20list%20(ACL)%20is%20made%20up%20of%20rules,are%20allowed%20in%20the%20doors.

What is an attack surface? definition and how to reduce it. Fortinet.
https://www.fortinet.com/resources/cyberglossary/attack-surface#:~:text=The%20attack%20surface%20is%20the,easier%20it%20is%20to%20protect.

What is an attack vector? | cloudflare.
https://www.cloudflare.com/learning/security/glossary/attack-vector/

المراجع

Arntz, P. (2023, September 18). The mystery of the cves that are not vulnerabilities. Malwarebytes.
https://www.malwarebytes.com/blog/news/2023/09/the-mystery-of-the-cves-that-are-not-vulnerabilities#:~:text=The%20Common%20Vulnerabilities%20and%20Exposures,%2C%20databases%2C%20and%20services).

Dwell time. Plurilock. (2023, September 14).
https://plurilock.com/deep-dive/dwell-time/#:~:text=In%20the%20ever%2Devolving%20landscape,within%20a%20network%20or%20system.

What is an endpoint?: Microsoft security. What Is an Endpoint? | Microsoft Security.
://www.microsoft.com/en/security/business/security-101/what-is-an-endpoint#:~:text=Endpoints%20are%20physical%20devices%20that,%2C%20embedded%20devices%2C%20and%20servers.

Bferrite. (2023, September 7). What is a Firewall? the different types of firewalls. Check Point Software.
://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/#:~:text=A%20Firewall%20is%20a%20network,network%20and%20the%20public%20Internet.

Incident response plan - glossary: CSRC. CSRC Content Editor.
https://csrc.nist.gov/glossary/term/incident_response_plan#:~:text=Definitions%3A,organization's%20information%20systems(s).

What are indicators of compromise (IOC): Proofpoint us. Proofpoint. (2023, November 13).
://www.proofpoint.com/us/threat-reference/indicators-compromise

Lutkevich, B. (2021, October 7). What is an intrusion detection system (IDS)? definition searchsecurity. Security.
://www.techtarget.com/searchsecurity/definition/intrusion-detection-system#:~:text=An%20intrusion%20detection%20system%20(IDS)%20is%20a%20system%20that%20monitors,when%20such%20activity%20is%20discovered.

What is intrusion prevention system? | vmware glossary.
https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html

Minimum baseline security standard development. IT SECURITY C&T. (2023, April 4).
https://itsecurityct.com/services-solutions/consulting-services/technical-security-consultation/infrastructure-security/minimum-baseline-security-standard-development/#:~:text=The%20Minimum%20Baseline%20Security%20Standard,systems%20to%20protect%20sensitive%20information.

Mitre ATT&CK®. MITRE ATT&CK®.
https://attack.mitre.org/

Multi-factor authentication policy. Fordham University.
https://www.fordham.edu/information-technology/it-security--assurance/it-policies-procedures-and-guidelines/multi-factor-authentication-policy/#:~:text=Multi%2DFactor%20Authentication%20is%20an,knowledge%2C%20possession%2C%20and%20inherence.

Security: The need-to-know principle. TECHCOMMUNITY.MICROSOFT.COM. (2021, May 28).
https://techcommunity.microsoft.com/t5/azure-sql-blog/security-the-need-to-know-principle/ba-p/2112393#:~:text=This%20principle%20states%20that%20a,a%20Need%2Dto%2Dknow.

Cisco. (2023a, July 24). What is Network Access Control (NAC)?. Cisco.
https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html

What is the principle of least privilege?. Palo Alto Networks.
https://www.paloaltonetworks.com/cyberpedia/what-is-the-principle-of-least-privilege#:~:text=The%20principle%20of%20least%20privilege%20(PoLP)%20is%20an%20information%20security,to%20complete%20a%20required%20task.

What is VLAN (virtual lan)? - it glossary. SolarWinds.
https://www.solarwinds.com/resources/it-glossary/vlan

What is a WAF? | web application firewall explained | Cloudflare.
https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

NVD.
https://nvd.nist.gov/vuln/detail/CVE-2022-21587

المراجع

NVD.
https://nvd.nist.gov/vuln/detail/CVE-2021-44228

Mandiant. ProxyShell exploiting Microsoft Exchange Servers.
https://www.mandiant.com/resources/blog/pst-want-shell-proxyshell-exploiting-microsoft-exchange-servers

CVE-2019-0604: Critical microsoft sharepoint remote code execution flaw actively exploited. Tenable®. (2019, December 12).
https://www.tenable.com/blog/cve-2019-0604-critical-microsoft-sharepoint-remote-code-execution-flaw-actively-exploited

Sangolekar, V., Kumar, A., Gupta, N., & Sandila, V. (2024, January 5). Security advisory: Remote code execution vulnerability (CVE-2023-3519). CVE-2023-3519 | ThreatLabz.
https://www.zscaler.com/blogs/security-research/security-advisory-remote-code-execution-vulnerability-cve-2023-3519

ProxyShell vulnerabilities in Microsoft Exchange: What to do. Sophos News.(2022, September 30).
https://news.sophos.com/en-us/2021/08/23/proxyshell-vulnerabilities-in-microsoft-exchange-what-to-do/

What is cybersecurity?: CISA. Cybersecurity and Infrastructure Security Agency CISA. (2024, January 29).
https://www.cisa.gov/news-events/news/what-cybersecurity

What you need to know about network DNS servers. Lifewire. Fisher, T. (2023, October 17).
https://www.lifewire.com/what-is-a-dns-server-2625854

تواصل معنا

للمزيـد مـن المعلومـات تواصلوا معنا على القنوات التالية:

www.sirar.com.sa

info@sirar.com.sa

@sirar_bystc

sirarbystc

شكرًا

لكم

sirar by stc