آوريكسلابز

جدار حماية النطاقات

تبسيط الأمان القائم على جدار حماية النطاقات

كتيب المنتج

المشهد العام للتهديدات

توفر الإنترنت قيمة هائلة للمؤسسات من خلال ربط أجهزتنا الحاسوبية وهواتفنا وغيرها من الأجهزة، مما يتيح لنا العمل والتعاون والابتكار. ومع ذلك، عندما يتصل المستخدم أو الجهاز بموقع ويب خبيث، يمكن أن تكون النتائج كارثية: كسرقة الملكية الفكرية، وتعريض بيانات العملاء للخطر، وتعطيل الأعمال.

50+
فئة محتوى

99%+
تغطية ويب نشطة

15 جزء من الثانية
تأخير يقل عن

100%
توفر الخدمة بدون انقطاع

بعد اعتماد نظام العمل عن بعد بفعل جائحة كوفيد-19، توسعت سطح الهجوم، وتزايدت تردد الهجمات وتأثيرها بمعدلات مقلقة.

الاعتماد الكبير على الحوسبة السحابية لأغراض شخصية وتجارية زاد أهمية أمان الويب بشكل أكبر.

لننظر إلى بعض الهجمات الشائعة التي تعتمد على نظام أسماء النطاق:

- استخدام نظام أسماء النطاق في هجمات متعددة المراحل المعقدة باستخدام تقنيات مختلفة مثل خوارزميات توليد النطاق
- إخفاء البيانات باستخدام نظام النطاقات
- احتيال بالأخطاء الطباعية
- هجمات رفض الخدمة الموزعة
- هجمات إعادة الربط
- تزييف
- هجمات أخرى متعلقة بالتنصت على مستوى نظام أسماء النطاق

تقريبًا 90٪ من الحوادث الضارة تستخدم نظام أسماء النطاق، وهو النظام العالمي لعناوين المواقع على الإنترنت.

ما الذي يمكن القيام به؟ من خلال تحسين أمان عمليات نظام أسماء النطاق، يمكن منع العديد من الهجمات الإلكترونية حتى قبل أن يقوم المستخدم أو الجهاز بزيارة نطاق خبيث.

جدار حماية النطاقات
أفضل حماية من الهجمات المعتمدة على اسماء النطاقات DNS

2024 WINNER CYBER SECURITY EXCELLENCE AWARDS

قم بمسح رمز الاستجابة السريعة هذا لمعرفة المزيد عن منتجاتنا

حلولنا

يعتمد نظام اوريكسلابز على نهج حديث لمساعدة منظمتك في الدفاع ضد هجمات تعتمد على نظام أسماء النطاق.

فعّال من حيث التكلفة وسهل التشغيل، يراقب كل حركة مرور

نظام أسماء النطاق الصادرة من أجهزة الحاسوب التابعة للمنظمة في مواقعها وأماكن تشغيلها عن بُعد، بما في ذلك الحواسيب والأجهزة اللوحية والأجهزة الذكية والمعدات - مما يضمن عدم إمكانية وصول تلك الأجهزة الطرفية إلى مواقع الويب الخطرة.

يتم تنفيذه من منصة برمجية واحدة دون الحاجة إلى أجهزة جديدة، يستخدم جدار حماية نظام أسماء النطاق تقنيات التعلم الآلي والذكاء الاصطناعي وخوارزميات متقدمة لتقييم وجهة حركة مرور نظام أسماء النطاق الصادرة في الوقت الفعلي أو بالقرب منه.

إذا حاول جهاز الوصول إلى موقع تم تحديده كخبيث أو أي موقع آخر يظهر سمات مشبوهة، يتم حظر الوصول.

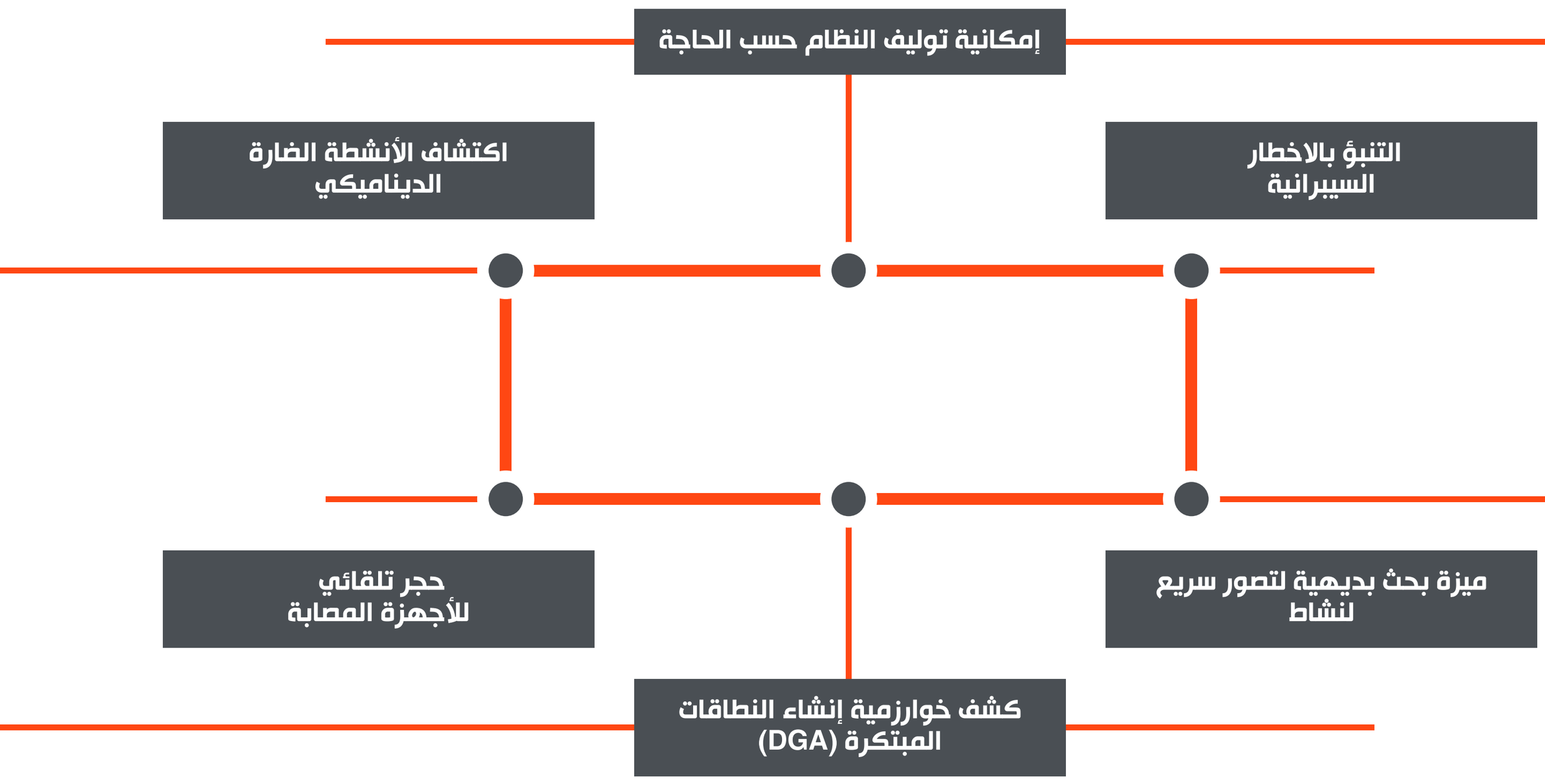
نتيجة لذلك، يتم منع موقع الويب الذي تم الإبلاغ عنه من تنفيذ أو تثبيت هجمات التصيد الاحتيالي، وبرامج الفدية، وبرامج التجسس، وبرامج التعدين الضارة للتشفير، واستغلال مجموعات الأدوات، أو الاتصال بخوادم القيادة والتحكم.

يراقب الحل أيضًا باستمرار جميع الأجهزة بحثًا عن حل وسط محتمل، ويحتوي على تلك الأجهزة ويعزلها الإنترنت وبقية الأجهزة.

بالإضافة للقدرة على عرض كل طلبات النطاقات في الوقت القريب من الوقت الفعلي وتجميعها في مكان واحد.

كما يمكن من عرض واجهات التحكم وتقارير مفصلة تمكن خبراء الأمن السيبراني من استنباط و تتبع كل طلبات أسماء النطاقات.

ميزات فريدة



الفوائد الرئيسية

التوفر العالي وزمن وصول منخفض

شبكة نظام أسماء النطاقات موزعة عالميًا، مما يضمن وقت تشغيل بنسبة 100٪. زمن وصول منخفض (أقل من 15 مللي ثانية)، مما يضمن أداء دقة نظام أسماء النطاقات الأمثل.

الكشف الدقيق عن البرامج الضارة وتصنيف المحتوى

الأفضل في فئته، مما يضمن الحد الأدنى من النفقات التشغيلية للتعامل مع النتائج الإيجابية الكاذبة. (< 0.5٪ معدل إيجابي كاذب)

حماية نظام أسماء النطاقات فعالة خارج شبكة المؤسسة

توفير الحماية على خدمة التجوال لآجهزة (ويندوز، ماك او اس اكس، اي او اس واندرويد) حتى عندما يكونون خارج شبكة الشركة. عزل العملاء المتجولين المصابين لمنع انتشار العدوى.

سهولة التركيب

خلال 10 دقائق فقط يمكن للنظام قيد التشغيل.

الريادة في دولة الإمارات العربية المتحدة

الكيان الوحيد المملوك لدولة الإمارات العربية المتحدة والذي يقدم حلولاً إلكترونية تركز على نظام أسماء النطاقات، وهو اعتبار بالغ الأهمية، نظرًا لرؤية الحل في جميع طلبات نظام أسماء النطاقات الخاصة بالعملاء.

التخصيص

مرنة بما يكفي لتمكين تخصيصات المنتجات المختلفة لتلبية المتطلبات والطلبات التنظيمية أو التشغيلية الفريدة.

قابل للتطوير

تم تصميم منتجنا لينمو بسلاسة جنبًا إلى جنب مع مؤسستك واحتياجاتها، حيث تم تصميمه ليتناسب مع حجمه.

سهولة التكامل مع المعلومات الأمنية وإدارة الأحداث

اربط بيانات طلب نظام أسماء النطاقات مع الأحداث المهمة الأخرى في المؤسسة للكشف عن رؤى قيمة.

خدمة مؤسستكم

يضمن زمن الوصول المنخفض والتوافر العالي أن جدار حماية نظام أسماء النطاقات ليس له أي تأثير على أداء الشبكة وعمليات المؤسسة.

وتؤكد عمليات التحقق المستقلة التي تجريها جهات خارجية أن وقت الاستجابة أقل من 15 مللي ثانية، وهو أقل بكثير من المعايير العالمية.

يسمح محرك اكتشاف نظام أسماء النطاقات الخبيث عالي الدقة لموظفي الأمن الرئيسيين بالتركيز على المبادرات المهمة وعدم قضاء وقت ثمين في التعامل مع النتائج الإيجابية الكاذبة.

يساعد جدار الحماية لنظام أسماء النطاقات مؤسستك على تقليل مخاطر تعطل الأعمال والإضرار بالسمعة الناجم عن الخروقات الأمنية أو سرقة بيانات العملاء.

تضمن وحدات الحل الموزعة عالميًا توفرًا عاليًا مع ضمان الأداء الأمثل في أي مكان عبر العالم.

مع وجود دعم فني على مدار 24 ساعة طوال أيام الأسبوع ، يضمن جدار حماية نظام أسماء النطاقات أن تتمكن مؤسستك من التركيز على عملياتك الأساسية.

> "تقوم وكالات الأمن السيبراني في الولايات المتحدة والمملكة المتحدة وأماكن أخرى، التي تتمتع بإمكانية الوصول إلى الحلول الأكثر تقدمًا، بفرض إجراءات حماية تركز على نظام أسماء النطاقات لحكوماتها وأمنها القومي والبنية التحتية الحيوية."

أوريكسلابز

من نحن

تأسست شركة اوريكسلابز في أبو ظبي عام 2020 مع شغفها بالهندسة التي تركز على الأمن السيبراني.

انضم فريق عمل متنوع بفخر ينتمون إلى 22 دولة مختلفة بخلفيات تتراوح من الدفاع الوطني إلى أفضل مؤسسات هندسة البرمجيات ذات الشهرة العالمية معًا لتطوير أفضل الحلول الأمنية في فئتها.

نحن نستفيد من البحث والابتكار لتقديم الحلول في أربع مجالات رئيسية:

- تقييم الأمن السيبراني
- المراقبة
- الوقاية
- التحسين

عند دمج حلول اوريكسلابز فانها توفر نظم رقابة لحظية مما يزيد من الوعي السيبراني ويقلل من احتمالية التعرض للهجمات السيبراني.

مهمتنا

تتمثل مهمتنا في تزويد فرق الأمن السيبراني بحلول استخباراتية وتقنية من الدرجة الأولى تعمل على تقييم البيئات ومراقبتها وتحسينها باستمرار للتخفيف من الهجمات المستمرة أو المستقبلية.

لماذا نحن

باعتبارنا شركة منافسة ومبتكرة تركز على الأمن السيبراني، فإننا نفخر بقدرتنا على صياغة حلول مصممة خصيصًا لتلبية المتطلبات الأمنية للمستخدم او المنشاة.

وبفضل خبرتنا في مجالات التعلم العميق، وأبحاث الثغرات الأمنية والبيانات الضخمة، والشراكات مع خبراء متخصصين ذوي شهرة عالمية، يمكنك الاطمئنان إلى أن حلولنا مبنية وتعمل على معلومات دقيقة وفي الوقت المناسب.

شركة الأمن السيبراني الأكثر ابتكارا في الشرق الأوسط

2024 WINNER CYBER SECURITY EXCELLENCE AWARDS

أفضل مزود لحلول الأمن السيبراني

ORYXLABS

الطابق الحادي والعشرون، المقر
الرئيسي للدار، شاطئ الراحة،
ص.ب. صندوق البريد: 33289
أبو ظبي، الإمارات العربية المتحدة

oryxlabs.ae