

منتجات وخدمات Darktrace

من خلال تقنية الذكاء الاصطناعي ذاتي التعلم، تتعلم Darktrace "أنماط الحياة" الطبيعية؛ لتوفير الحماية ضد تهديدات الأمن السيبراني غير المعروفة والتي لا يمكن التنبؤ بها. تعتمد أكثر من 5,500 مؤسسة في جميع أنحاء العالم على Darktrace للكشف عن، والتصدي لجميع أنواع تهديدات الأمن السيبراني، منها التي تتضمن أحدث تقنيات الهجمات وهجمات يوم الصفر والتهديدات الداخلية.

تقنية الذكاء الاصطناعي ذاتي التعلم

تمثل تقنية الذكاء الاصطناعي ذاتي التعلم ابتكاراً نوعياً، وخروجاً جوهرياً عن حلول الأمن السيبراني التقليدية، والتي تعتمد في التنبؤ بالتهديدات على بيانات هجمات قديمة مُسجَّلة، كانت قد حصلت في الماضي. بدلاً من اتباع هذا النهج، تدرُس وتتعلم هذه التقنية مؤسستك دراسة شاملة، من الألف إلى الياء، وتبني معلوماتها بناءً على أنماط السلوكيات "الطبيعية" لكل شخص وكل شيء داخل المؤسسة.

وتوفر Darktrace تقنية الذكاء الاصطناعي ذاتي التعلم هذه لبياناتك أينما كانت، بما في ذلك بيانات منصات السحابة، والبرمجيات كخدمة "SaaS"، وبيانات منصات البريد الإلكتروني، إضافة إلى بيانات خدمات إنترنت الأشياء "IoT"، وأجهزة نقاط النهاية والأنظمة السيبرانية الفيزيائية.

على غرار نظام المناعة البشري، فقدره Darktrace على التمييز بين السلوك الحميد والسلوك الخبيث، دون معلومات سابقة عنه، تُمكنها من التعرف على الهجمات السيبرانية التي لولا هذا التدخل كانت لتمر دون أن يلاحظها أحد، ودون ضوابط.

وبفضل التصدي الذاتي "Autonomous Response"، تستغل تقنية الذكاء الاصطناعي من Darktrace معرفتها المفصلة بالمؤسسة بهذا الشكل وتعرض وتصدى للهجمات السريعة الانتشار بدقة متناهية، في حين يعمل محلل الذكاء الاصطناعي السيبراني "Cyber AI Analyst" على أتمتة إجراءات التحقيقات في التهديدات، ويصدر تقاريرًا بشأن النطاق الكامل للأحداث الأمنية.

**ENTERPRISE
IMMUNE SYSTEM**

NOVEL THREAT DETECTION

ANTIGENA

AUTONOMOUS RESPONSE

CYBER AI ANALYST

AUTOMATED INVESTIGATIONS

AUTONOMOUS • CLOUD-NATIVE

DARKTRACE IMMUNE SYSTEM

POWERED BY SELF-LEARNING AI

CLOUD



SAAS



EMAIL



ENDPOINT



NETWORK



OT



هيكل المار ربع تاديدهت ال Darktrace نم يعانطصالا ءاكذلا ةينقت فشتكت :1 ينابل امسرلا اهجلاعت و ةمزالا تاقيقحتل اهل يرجت و ، ةسسؤملل ةلمالكلا ةيمقرلا

منتجات Darktrace

Cyber AI Analyst AI Investigation



- تعزيز قدرات فرق العمل البشرية، وذلك من خلال إجراء تحقيقات آليّة للنطاق الكامل للأحداث الأمنية
- إعداد تقارير تجعل فرق العمل -على الفور- في وضعٍ يُمكنها من اتخاذ الإجراءات
- دمج حدس ومرونة الخبرة البشرية، مع سرعة الذكاء الاصطناعي وقابليته للتوسع
- يمكن أيضًا للتحقيقات أن تنطلق بناء على الطلب، أو استجابة لتحذيرات تقنيات خارجية
- توفير للوقت بما يصل إلى 92% من وقت الفرز وتحديد الأولويات

مولد المضادات من Darktrace (Antigena): التصدي ذات

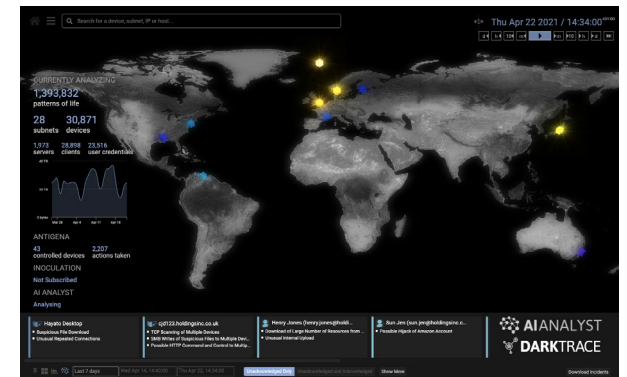
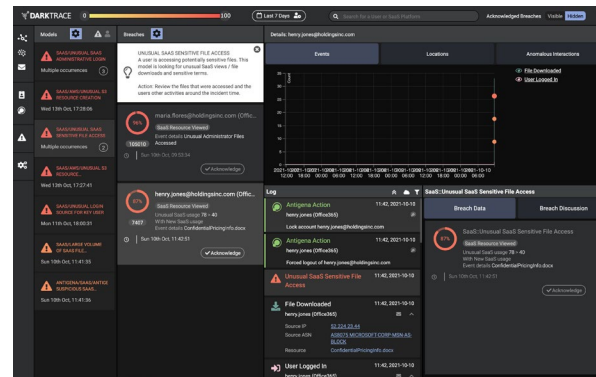
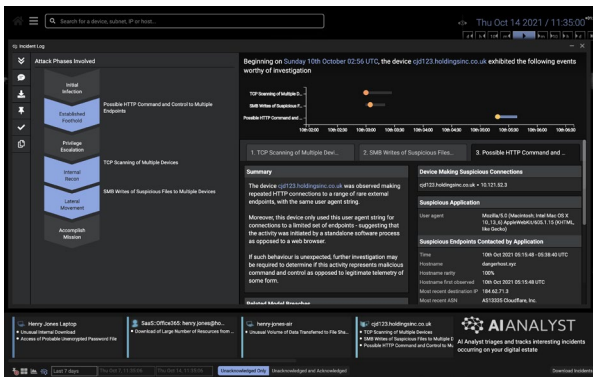


- إتخاذ إجراءات فائقة الدقة للاعتراض والتصدي للهجمات السريعة الانتشار التي لا يمكن التنبؤ بها، خلال ثوانٍ معدودة
- العمل من خلال نهج دائم التطور، والتكيف مع التهديدات كلما أكتشفت
- الحفاظ على سير العمليات الاعتيادية المؤسسة خلال الأحداث من خلال فرض أنماط السلوكيات "الطبيعية"
- المعالجة والتصدي من خلال إجراءات ذاتية التوجيه، أو الدمج مع تقنيات الحماية الموجودة

النظام المناعي للمؤسسة: نظام اكتشاف التهديدات يعتمد على التعلم الذاتي



- تتعلم أنماط السلوكيات الطبيعية بشكل مستمر؛ لتتمكن من اكتشاف التهديدات السببرانية غير المعروفة والتي لا يمكن التنبؤ بها
- حماية للقوى العاملة الديناميكية من أحدث التهديدات وبرامج الفدية والتهديدات الداخلية
- تغطية الحمض النووي "DNA" الرقمي الكامل للمؤسسة عبر السحابة وأجهزة نقاط النهاية وأجهزة إنترنت الأشياء والشبكة
- التداخل مع تحليل الأمن السببراني المعتمد على الذكاء الاصطناعي (Cyber AI Analyst) لإطلاق تحقيقات وإنشاء تقارير ذاتية



نطاق التغطية

السحابة

- حيادية البيانات: تزدهر التقنية في تعقيدات تقنيات السحابة المتنوعة
- التعرف على أخطاء التهيئة والإعداد الخطيرة للسحابة
- اكتشاف هجمات موجهة على أساس الهوية، بما في ذلك مفاتيح الوصول المخترقة
- التصدي للهجمات السحابية من خلال إجراءات ذاتية بسرعة آلية

البرمجيات كخدمة (SaaS)

- تبييد الهجمات التي لا يمكن التنبؤ بها في السحابة وأدوات العمل الجماعي
- قرارات تستند إلى تقنية الذكاء الاصطناعي الذاتي التعلّم، التي "تفهم الإنسان" الموجود خلف حسابات السحابة الديناميكية
- رد فعل يفوق سرعة أي إنسان، حيث إنه ينطلق قبل وقوع أي ضرر
- اتخاذ قرار دقيق، والسماح في الوقت ذاته بسير عمل المؤسسات بشكل طبيعي

البريد الإلكتروني

- قيود معززة بتقنية الذكاء الاصطناعي؛ "تفهم الإنسان" الموجود خلف عنوان البريد الإلكتروني
- تبييد رسائل البريد الإلكتروني الضارة التي لا تستطيع الأدوات الأخرى اكتشافها
- التصدي للتصيد الاحتيالي الموجه وهجمات انتحال الهوية
- إبراز جميع روايات الذكاء الاصطناعي، التي تسرد قصة حملات الهجوم التي تم تبييدها
- النشر عبر السحابة، يُبَيِّن خلال دقائق

نقاط النهاية

- توفير تقنية الذكاء الاصطناعي لنقاط النهاية؛ وحماية الموظفين الذين يعملون عن بُعد، المتصلين بشبكة VPN وغير المتصلين بها
- تعزيز قدرات الاكتشاف الخاصة بكل من Microsoft Defender، وCrowdStrike، وCarbon Black
- تتوافر التصديبات الذاتية من خلال وحدات برمجيات الوكيل الخاصة بـ Darktrace
- التحقيق في أنشطة نقاط النهاية في سياق المؤسسة الرقمية بأكملها

الشبكة

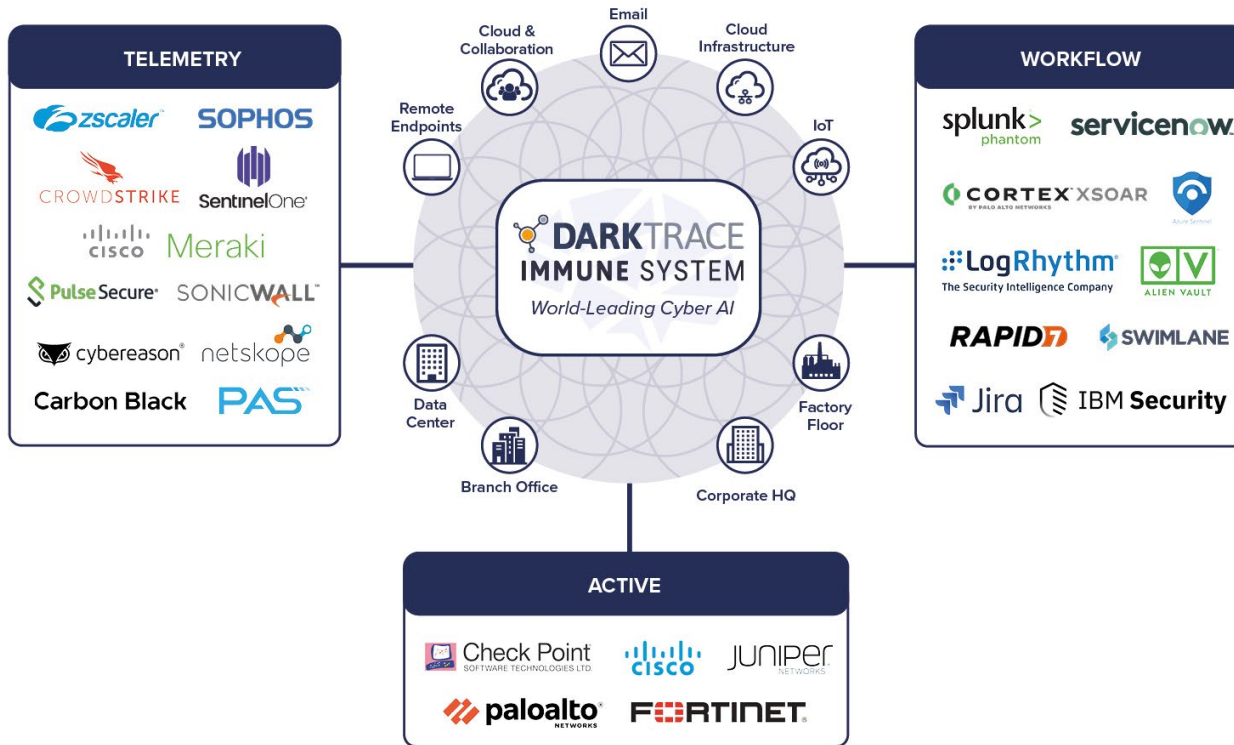
- اكتشاف برامج الفدية في كل مرحلة من مراحل الهجوم ومعالجتها.
- الكشف عن الجهات الداخلية المُخَرَّبَة، والحماية من سرقة البيانات
- الحماية من التهديدات الاحترافية والحديثة
- اتخاذ إجراء لاحتواء الهجمات

تكنولوجيا التشغيل

- تتعلم أنماط السلوكيات "الطبيعية" لجميع الأجهزة ووحدات التحكم؛ لتتمكن من اكتشاف المخاطر التشغيلية
- تعزيز التقارب بين تكنولوجيا المعلومات وتكنولوجيا التشغيل
- اكتشاف التهديدات ونقاط الضعف الحديثة، التي قد تؤثر على العمليات
- مستوى متقدم من الرؤية داخل كل طبقة من طبقات نموذج بورديو، بما في ذلك داخل طبقة الشبكة الفرعية المراقبة (DMZ) وحولها
- التعرف السلبي على الأصول

تكامل ودمج النظام المناعي

يفرض نظام Darktrace المناعي (Darktrace Immune System) قيودًا أمنية على بنية شبكية مفتوحة قابلة للتوسع؛ بهدف التمكن من الدمج والتكامل مع النظم الأيكولوجي المتنوع لديك كلما تطور. تستطيع المنصة، من خلال التكامل الذي يتم بنقرة واحدة، استيعاب أشكال جديدة من سُبل قياس تتبع الاستخدام، ومشاركة رؤى ذكاء اصطناعي مُخصصة عبر خطط سير العمل المطبقة، والتفاعل مع مجموعة كبيرة من التقنيات؛ لتوفير معالجة ذاتية تمتد عبر نظم البريد الإلكتروني ونظم الحماية المضمنة ومنصات العمل الجماعي.



خدمات الخبراء Darktrace

مجموعة من تحليلات التهديدات وخدمات الذكاء السيبراني المتاحة للعملاء، والتي يوفرها محللو الأمن السيبراني في Darktrace أو شركاء Darktrace المعتمدين. صُمِّمت خدمات Darktrace لدعم المنظمات من جميع الأحجام وكذلك القطاعات المتنوعة من الصناعات؛ لتتمكن من تقديم خدمة مخصصة ملائمة لكل شركة من الشركات.

أسأل الخبير

- تعقيبات سريعة ونصائح معالجة مُعتمدة على الخبرة من محلي الأمن السيبراني في Darktrace
- أداة دردشة سهلة الاستخدام
- مساعدة على مدار الساعة، طوال أيام الأسبوع

تنبيهات للحماية من التهديدات على مدار الساعة، طوال أيام الأسبوع

- خدمة تنبيهات شاملة للحماية من التهديدات على مدار الساعة
- يتم الاتصال بالعميل على الفور في حال وجود هجوم
- أكثر من 1,000 عميل، من الشركات من الكبيرة والصغيرة
- تُقدم تلك الخدمات من خلال مراكز Darktrace للعمليات الأمنية (SOCs) في كامبريدج، وإنجلترا، وسان فرانسيسكو، وسينغافورة