Defensys Threat Deception Platform

حلاً لاكتشاف التهديدات المجهولة
عبر محاكاة أجزاء البنية التحتية لتقنية المعلومات وتكنولوجيا التشغيل

Defensys

حول Defensys

ديفينسيس هي شركة حائزة على جوائز ومعترف بها على الصعيدين الوطني والدولي في مجال حلول الأمان السيبراني. منذ عام 2011، قمنا بدعم العديد من الوكالات الحكومية وشركات القطاع الخاص لتمكينهم من مواجهة التهديدات السيبرانية الحديثة بثقة وضمان إدارة الأمان القوي في جميع أنحاء العالم. تقنيات ديفينسيس مُدمجة في القطاعات المالية، العامة، النفط والغاز، الطاقة، صناعة المعادن، وغيرها من القطاعات.

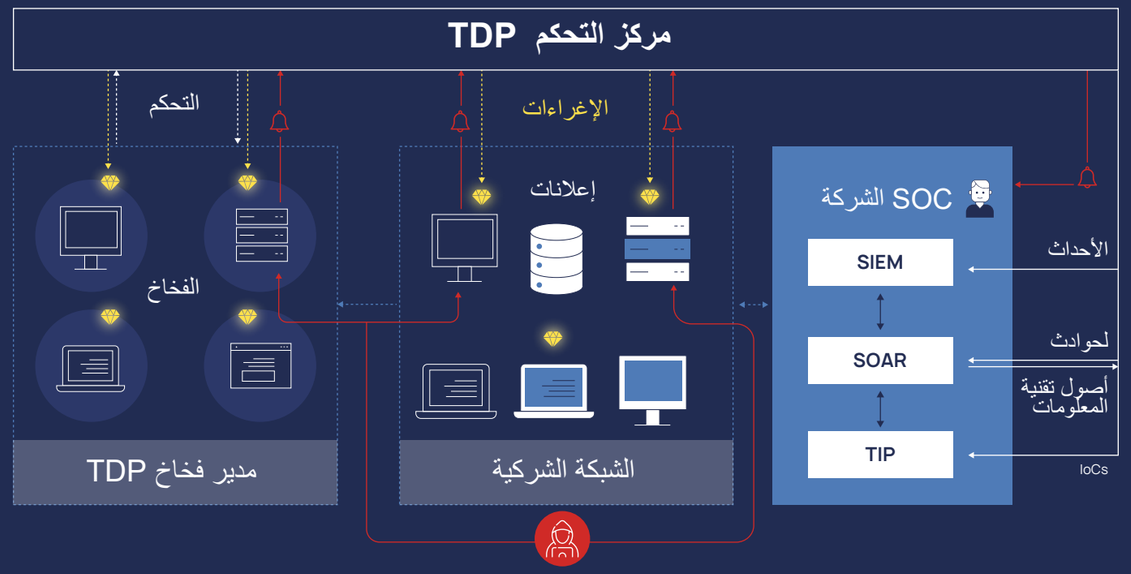
sales@defensys.com

ملخص الأمن السيبراني:
defensys.com/blog/

Defensys Threat Deception Platform هي أداة شاملة متكاملة لمحاكاة البنية التحتية الرقمية مصممة لاكتشاف ومنع الهجمات الإلكترونية بشكل استباقي. باستخدام مجموعة معقدة من الفخاخ، تكتشف منصة Defensys TDP المتسللين، وتوخر تقدمهم داخل الشبكة، وتضمن مكافحة الهجمات الإلكترونية.

مزايا Defensys TDP

- تكتشف هجماتٍ لا تستطيع أدوات أخرى اكتشافها (هجمات مستهدفة، تهديدات يوم صفر، والمزيد)
- تقلل من تقدم المتسللين داخل الشبكة عبر إنشاء طبقة إضافية من العناصر المحاكاة
- تمنع الهجمات في وقتٍ مبكر لتقليل تأثير التهديد
- يُحدّد الثغرات الأمنية لفهم أدوات المتسللين وسلوكهم ضد بنية الشركة



مكونات المنصة:

مدير الفخّ هو خادم إدارة الفخّ

مركز التحكم هو خادم إدارة المنصة

المزايا النظامية

- تكوين مرن للفخاخ والإغراءات لزيادة القدرة على التكيف والاستجابة لتغير ديناميات البنية التحتية الحقيقية للشركة
- أدوات تشبه المتاهة لاستدراج الهجمات عن طريق تقليد نظام حي بجميع الأنشطة المعتادة
- للمستخدمين والخدمات عالية الانتشار والتوسع من خلال نشر تلقائي للفخاخ والإغراءات
- كشف واضح للأنظمة المخترقة واستجابة تلقائية عند النشر مع منتجات Defensys الأخرى

الإدارة المركزية لنظام الفخّ

منصة الدفاع ضد التهديدات Defensys TDP تقدم نظامًا آليًا للأفخاخ يقم بتقميص أصول تكنولوجيا المعلومات الخاصة بشركتك بشكل طبيعي وإدارتها من مركز واحد.

من خلال قوالب نظام الفخّ الجاهزة، يمكنك إعادة إنشاء فروع المؤسسة بسرعة ومحاكاة أنظمة محددة. ومن أجل جعلها أكثر جاذبية وواقعية، تجمع العناصر المحاكاة عناصر مجموعات من الخوادم المتفاعلة أو الخدمات أو التطبيقات التي تعمل معًا لتحاكي بشكل أفضل شبكة الحاسوب.

توليد ونشر الإغراءات تلقائياً

لرفع ملف المهاجم، تقوم منصة Defensys TDP بشكل تلقائي بتعيين فخاخها وإغراءاتها في البنية التحتية الحقيقية. يمكنك توليد الفخاخ والإغراءات تلقائياً وفقًا لمعايير الشركة الخاصة بها.

الكشف عن المتطفلين والبرمجيات الخبيثة

تقوم منصة Defensys TDP بجمع الأحداث عند تسجيل التفاعل مع الإغراءات والفخاخ، ثم تقوم بمعالجتها وإرسال تنبيه بالكشف إلى خبير أمان تكنولوجيا المعلومات. بعد ذلك، يتم إثراء هذه الأحداث بسياق إضافي ويمكن إرسالها تلقائيًا إلى أنظمة خارجية مثل SOAR وSIEM للرد على الهجوم ومنع تقدمه.

معدل منخفض للإيجابيات الزائفة

الفخاخ والإغراءات مصممة بدقة لجذب انتباه المهاجم ولا تُستخدم في سياقات العمل العادية، لذلك فإن أي تفاعل معها من المرجح جدًا أن يكشف عن حادثة.

تحديد الأنظمة المخترقة

باستخدام Defensys TDP مع Defensys SOAR ، يمكنك تقدير نطاق الهجوم بسرعة، وأهدافه، وتحديد أنظمة أخرى تم اختراقها داخل شركتك، وتوتيع الاستجابة، والتخفيف من الهجوم.

جمع سمات المهاجم

أثناء تحليل نشاط المهاجم، يقوم Defensys TDP بجمع السمات والمؤشرات الدالة على الهجوم والتهديدات المعروفة التي يمكن تصديرها على الفور إلى Defensys TDP. التكامل الوثيق بين المنصتين يوفر:

- إثراء البيانات بشكل إضافي
- تكوين رصد تلقائي في أحداث SIEM
- الترابط مع المعلومات المتاحة بشكل إضافي
- التخفيف باستخدام أدوات الأمان

الفخ هو نقطة جذب للمهاجمين. وتتضمن الفخاخ ما يلي:

- الأجهزة الافتراضية لنظام التشغيل Windows/Linux
- المحاكاة التفاعلية:(s)HTTP، SSH، SMB
- المحاكاة الأساسية: Telnet، FTP، HTTP(s)، SSH، POPS، IMAP، SMTP، SOCKS، VNC، RDP PostgreSQL، MySQL
- مكونات التشغيل الزمني (OT)

الإغراء هو معلومات قيمة بالإمكان. وتتضمن الفخاخ ما يلي:

- ملفات التكوين لأدوات الإدارة الشهيرة
- ملفات البيانات (Word / Excel / PDF)
- حسابات المستخدمين
- سجل تصفح الإنترنت
- مفاتيح SSH