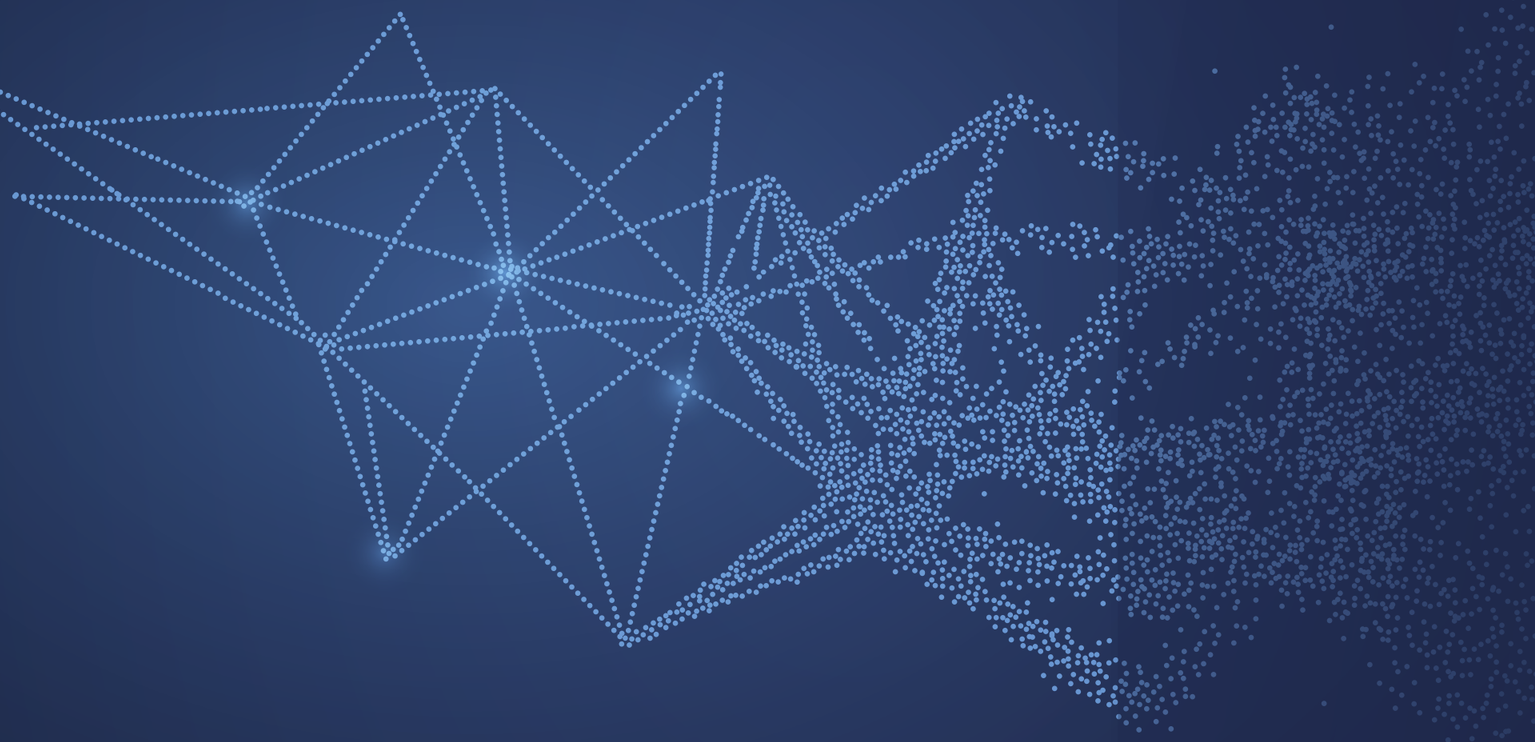
Defensys Threat Intelligence Platform

منصة لاستخبارات التهديد
إدارة البيانات



Defensys

حول Defensys

Defensys 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

نشرة الأمان السيبراني:
defensys.com/blog/

Defensys

The Defensys Threat Intelligence Platform يضمن:

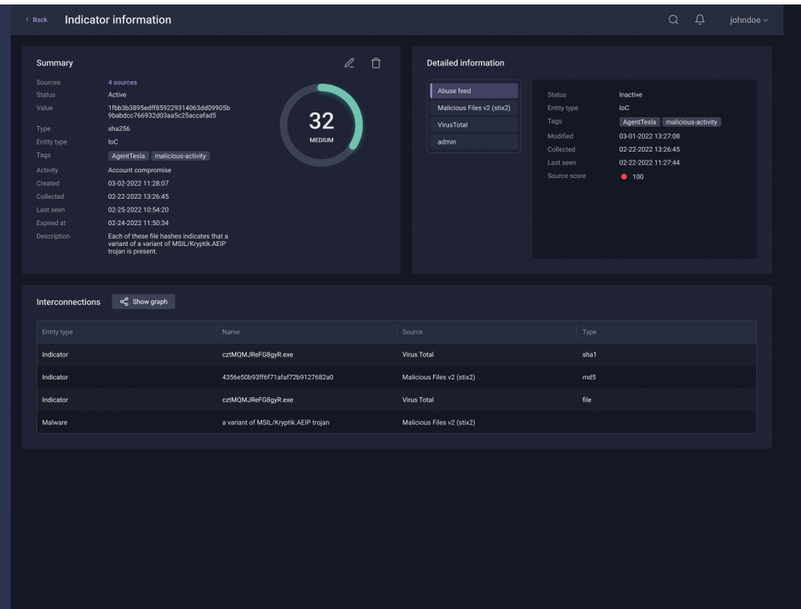
- ✓ جمع ، توحيد وإثراء تلقائي لمؤشرات الاختراق IoCs من مصادر متعددة ، تشمل تلك المصادر مصدر Defensys الخاص ومصادر مفتوحة
- ✓ إرسال البيانات المعالجة مباشرة إلى أدوات الأمان الداخلية
- ✓ البحث عن مؤشرات الاختراق واكتشافها في بنية الشركة الداخلية باستخدام مجسات SIEM.

المزايا الرئيسية:

- إدارة بيانات تكنولوجيا المعلومات بسهولة من خلال جمع البيانات بشكل مستمر وتطويرها وتحسينها وتخزينها من مصادر متعددة في قاعدة بيانات واحدة باستمرار.
- أسهل الكشف عن التهديدات الخفية مع الرصد التلقائي شركات النفط IoCs في SIEM مع أجهزة الاستشعار.
- تسريع التحقيقات من خلال الحصول السريع على المعلومات وأتمتة الإجراءات الرئيسية.
- منع التهديدات في الوقت المناسب وتقليل المخاطر مع التحميل التلقائي للبيانات المعالجة مباشرة إلى قوائم الحظر لأدوات الأمان مثل IDS.
- تقليل عدد الإيجابيات الزائفة مع تصنيف مؤشرات التهديد في نموذج تسجيل النقاط IoCs.
- تسريع جمع المؤشرات الخاصة بالتهديدات في البنية التحتية الموزعة جغرافيًا باستخدام مجسات SIEM.

بطاقة الإشارة تحتوي على جميع المعلومات المتاحة:

- ✓ البيانات الخامة من مقدمي معلومات التهديد
- ✓ نتائج التحسين
- ✓ تقارير حول البرمجيات الضارة والثغرات والمؤشرات الأخرى ذات الصلة
- ✓ سجلات اكتشاف الهجمات وتاريخ التحديث



الوظيفة

جمع معلومات الاستخبارات عن التهديدات

تقوم Defensys TIP تلقائيًا بجمع بيانات استخبارات التهديد من مصادر متنوعة. وهي متكاملة بشكل أصلي مع حلول تبادل استخبارات التهديدات التالية:

- IBM X-Force Exchange
- AT&T Open Threat Exchange (OTX)
- Defensys feed
- Group-IB Threat Intelligence
- Kaspersky Threat Intelligence
- RST Threat Feed
- ESET Threat Intelligence
- Shadowserver
- مصادر مفتوحة
- بالإضافة إلى ذلك، يمكن أيضًا ربط مصادر أخرى

معالجة وتحسين البيانات

أثناء عملية المعالجة، يتم توحيد وتجميع مؤشرات التهديد المشهود بها IoCs في نموذج تمثيل واحد، ويتم ربط ودمج المؤشرات المكررة. يمكنك تصنيف كل مؤشر تهديد وتحديد سياسات انتهاء صلاحيته. تقدم Defensys TIP دعمًا لتحسين مؤشرات التهديد بسياق إضافي لاستكمال بيانات مزودي المعلومات. الخدمات المدعومة لتحسين تشمل:

- VirusTotal
- Whois
- Ipgeolocation.io
- MaxMind
- OPSWAT Metadefender
- Hybrid Analysis
- RiskIQ
- ThreatCrowd
- Shodan
- وغيرها

تحليل التفاعلات

يساعد تحليل التفاعلات خبراء الأمان السيبراني في تفسير البيانات بشكل صحيح وبناء صورة شاملة للتهديدات. يقوم نظام Defensys TIP بجمع معلومات حول مؤشرات التهديد المتاحة من مزود البيانات، بالإضافة إلى البيانات ذات الصلة حول:

- التقارير التحليلية
- البرامج الضارة
- الثغرات
- رسم MITRE
- سياق آخر

تحليل مُستنبط لأدوات الأمان

المعالجة الأولية تضمن وجود عدد أقل من الإيجابيات الزائفة، التي غالباً ما تحدث مع البيانات الخام. بعد الانتهاء من المعالجة، يتم إرسال البيانات تلقائيًا إلى أدوات الأمان الداخلية المتاحة:

- Cisco
- McAfee
- Palo Alto Networks
- أدوات أخرى

بالإضافة إلى ذلك، يُمكن تبادل البيانات باستخدام تنسيقات شائعة: STIX 2.1، CSV، JSON.

البحث والاكتشاف في البنية التحتية لتكنولوجيا المعلومات

باستخدام أجهزة الاستشعار، تبحث Defensys TIP بشكل استباقي عن IoCs متعلقة في SIEM. بمجرد اكتشافها، يتم إرسال تنبيهات مؤشرات الاختراق عبر قنوات متعددة.

تأمين تنفيذ سيناريوهات الدفاع

تضمن المنصة إعداد سير العمل لدلائل الاختراق. بعد تكوين سلسلة من القواعد، يمكنك أتمتة معالجة البيانات بالكامل باستخدام السيناريو الأمني من جمعها حتى منعها.

بنية النشرات البسيطة

يساعدك مُنشئ النشرات السهل الاستخدام في إنشاء معلومات حول التهديدات والثغرات وإرسال النشرات إلى المؤسسات المستهدفة، وتصديرها إلى الأنظمة الخارجية باستخدام واجهات البرمجة APIs.