Defensys

Defensys SENSE

منصة تحليل أمان الأنظمة السيبرانية

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

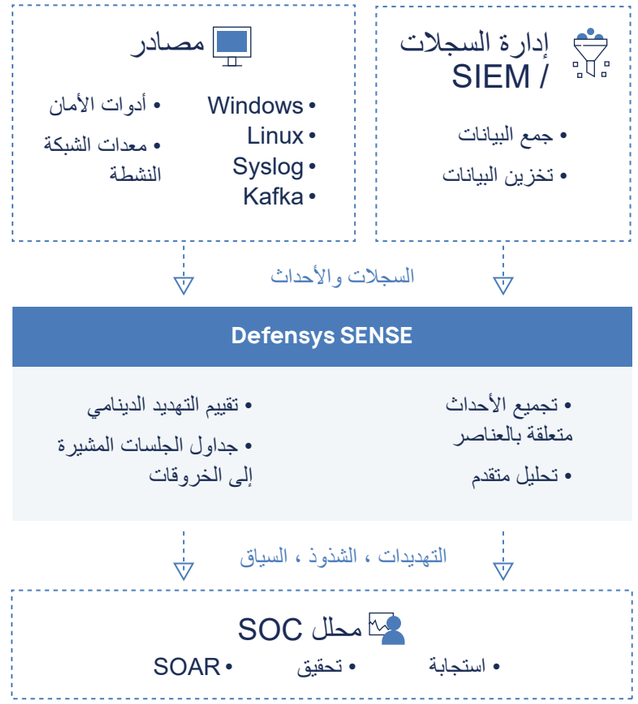
نشرة الأمان السيبراني:
defensys.com/blog/

Defensys

Defensys SENSE هي منصة اكتشاف الاستثناءات في مجال أمان الأنظمة السيبرانية ذات الميزات الكاملة والتي تتمتع بالقدرات التالية:

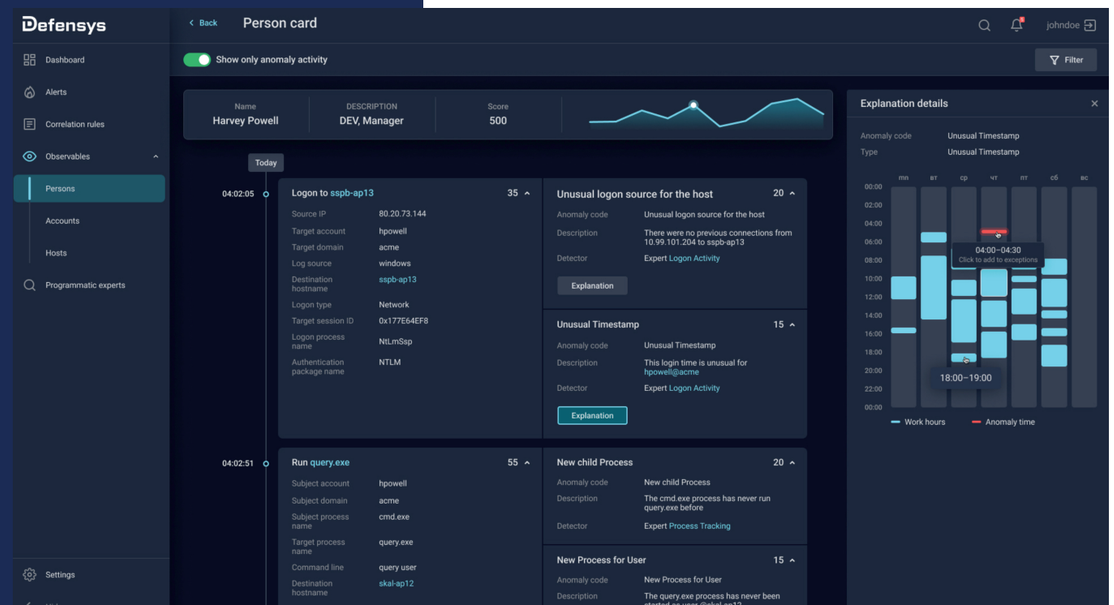
- ✓ اكتشاف التغييرات الغير العادية في حالة النظام.
- ✓ تحديد الأنشطة المشبوهة.
- ✓ تقييم التهديدات والاستثناءات ديناميكياً.

تعمل ميزات التحليل المتقدمة في SENSE على تحسين أداء مركز العمليات الأمنية SOC واكتشاف علامات الهجوم المبكرة بشكل مناسب، و إعطاء الأسبقية لأهم التهديدات في تدفق الأحداث والحوادث.



المزايا الرئيسية

- رصد مستمر، اكتشاف الخروقات وتحذير مبكر من التهديدات.
- اكتشاف التهديدات الداخلية وكذلك الهجمات غير المعروفة مسبقًا.
- تقييم التهديدات والخروقات، مع التركيز على الأهداف عالية الخطورة.
- تقليل عدد الحوادث والإيجابيات الزائفة.
- تبسيط تحليل الحوادث وتتبع الأحداث.



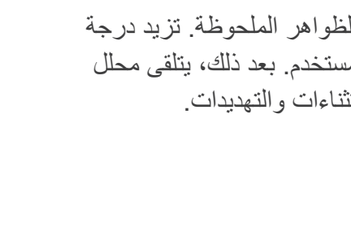
مراقبة حالة الأمان

Defensys SENSE تراقب بشكل مستمر أحداث الأمان من خلال تحليل البيانات من مصادر متنوعة: أنظمة إدارة السجلات، SIEM ، وغيرها. تتم مراقبة البيانات الواردة وتحليلها بالنسبة لعناصر النظام المحددة: المستخدمين، محطات العمل، الملفات، الحسابات، الخدمات، إلخ. من خلال تحليل سلوك هذه العناصر، يقوم Defensys SENSE بإنشاء ملفات تعريف للسلوك الطبيعي أثناء التعلم ويكتشف الأنشطة المشبوهة في حالة وجود أي تناقض مع هذه الملفات.

نظام متعدد المستويات للخبراء البرمجيين

يوفر نظام الخبراء البرمجيين المدمج مراقبة شاملة للتحكم في المهام والأحداث بشكل أفضل. يتم إجراء المراقبة للعمليات :

- ✓ والتطبيقات الجارية،
- ✓ وطلبات تسجيل الدخول،
- ✓ والوصول إلى الملفات عبر العمليات،
- ✓ واتصالات VPN،
- ✓ وأحداث DGA والاتصال بنطاقات تشبهها،
- ✓ والأحداث المتصلة بحركة البريد الإلكتروني،
- ✓ وأحداث تبديل الحسابات،
- ✓ وأحداث إدارة مجموعات الأمان،
- ✓ وأحداث إدارة حسابات المستخدمين،
- ✓ وغيرها.



الترابط التكيفي للأحداث

يقوم Defensys SENSE بتطوير تلقائي لتحليل الاستثناءات المدمج فيها. مع إدخال مصادر البيانات الجديدة وقواعد التحليل المقدمة، يقوم الخبراء البرمجيون بالتكيف تلقائيًا دون الحاجة إلى ضبطها إضافيًا. يتوفر SENSE Defensys على تنسيق بيانات عالمي للتحليل، مما يوفر مرونة في استخدام الأدوات التحليلية.

تقييم التهديد الديناميكي وتقدير الخروقات

نظام SENSE لتقييم الاستثناءات الديناميكي يقوم بحساب تصنيف التهديد للظواهر الملحوظة. تزيد درجة التصنيف في حالة حدوث أي نشاط مشبوه أو تجاوز القيم المحددة من قبل المستخدم. بعد ذلك، يتلقى محلل النظام إشعارًا متناسبًا ليكون قادرًا على اكتشاف والاستجابة على الفور للاستثناءات والتهديدات.

الجدول الزمني للحدث

تُحفظ المعلومات المفصلة حول الأنشطة المشبوهة للمراقبة في شكل جدول زمني. يحتوي كل جدول زمني على تواريخ السلوك الغير العادي الذي تم اكتشافه وسياقته والذي ينشئ السلم الزمني المقابل. تسهل الجداول بشكل كبير تحليل الحوادث واكتشاف مشكلات الأمان.