

Defensys SOAR هي منصة حديثة للاستجابة للحوادث مع الميزات الأساسية التالية:

- ✓ جمع بيانات الحوادث من مصادر مختلفة.
- ✓ إثراء بيانات الحوادث بأقصى سياق إضافي.
- ✓ أتمتة معالجة الحوادث الروتينية وسيناريوهات الاستجابة.
- ✓ تنسيق فرق SOC وأعضائها.

تساعد منصة SOAR على تعزيز قدرة الأمان السيبراني لعملك والاستجابة بسرعة لأكثر التهديدات التحولية تعقيدًا.

الميزات الرئيسية

جمع البيانات حول جميع الحوادث في وحدة استجابة واحدة.

تأمين عملية الاستجابة للحوادث بشكل تلقائي عن طريق تشغيل خوارزميات وسيناريوهات مُعدة مسبقًا؛ القدرة على تكيف دليل الاستجابة لتلبية احتياجات شركتك في الوقت الحقيقي؛ معالجة الحوادث بشكل كامل.

إدارة فريق الاستجابة والعمليات، تعيين الأدوار، تنسيق الإجراءات، الإشعار، التصعيد، التخطيط والتحكم في المهام في مساحة عمل واحدة.

جمع المعلومات والسيطرة على الأصول التقنية، إدارة الضعف، رصد البرمجيات؛ اكتشاف البرامج والأجهزة غير المصرح بها والاتصالات الخارجية؛ توحيد حالات أمان البنية التحتية.

وضع العمل المتعدد في تثبيت واحد: نشر عمليات سيناريوهات الاستجابة والموصلات، والحصول على تعليقات؛ تشغيل العديد من سيناريوهات الاستجابة.

الدمج مع SIEM، NGFW، IPS/IDS، أدوات فحص الثغرات، برامج مكافحة الفيروسات، DLP، خدمات TI، ITSM/Service Desk، قواعد البيانات والعديد من المصادر الأخرى عبر الموصلات العالمية.

التفاعل مع أنظمة خارجية أيضًا عبر منسئ الموصلات، والحصول على بيانات حول الحوادث والأصول.

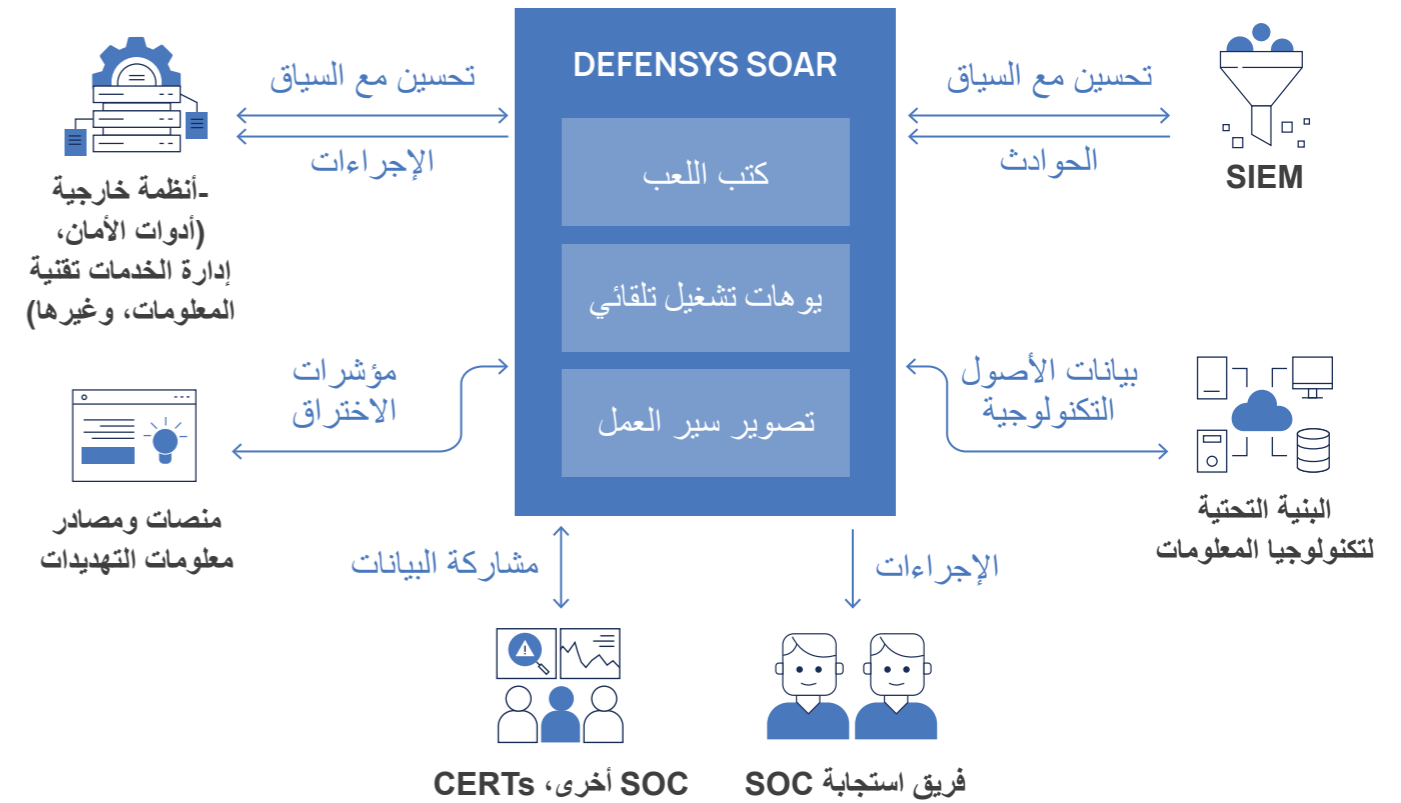
تنظيم الأنظمة المتصلة، وتنسيق تفاعلها ضمن دليل الاستجابة، وإدارة تشغيل الدلائل ومعالجة الحوادث.

تصور المعلومات على مستويات تمثيل مختلفة، ومجموعة محددة مسبقًا من مقاييس الاستجابة، ومنسئ الرسوم البيانية والتوجيه، ومجموعة من التقارير المثبتة مسبقًا ومنسئ التقارير، إنشاء وتوزيع التقارير تلقائيًا وبشكل مجدول، تصديرها إلى تنسيقات مختلفة.

مزايا النظام

- ترتيب الحوادث حسب مستوى الأهمية
- سيناريوهات الاستجابة الديناميكية ومحرر الرسوميات سهل الاستخدام
- وضع التعدد
- التكيف المرن مع البنية التحتية لتقنية المعلومات الحالية والعمليات
- آليات الاندماج الفريدة
- سيناريوهات الأتمتة جاهزة للاستخدام

-ديفنسيس SOAR تعمل كواجهة عمل واحدة لمحلي أمن مركز عمليات الأمان SOC



CISO الفوائد

- رصد البنية التحتية لتقنية المعلومات ومستوى أمانها
- أتمتة عمليات إدارة الحوادث والثغرات
- التخفيف من المخاطر
- بيانات شاملة عن التعرض للمخاطر وتقارير ومقاييس لاتخاذ القرارات

SOC فوائد التحليل

- تقليل بشكل كبير الوقت المستغرق في الاستجابة لحوادث الأمان السيبراني الروتينية
- العمل في واجهة واحدة مع تتبع حالة الأمان السيبراني للبنية التحتية
- زيادة الكفاءة ومرونة فريق SOC
- أتمتة مهام معالجة الحوادث الروتينية
- بناء تفاعل فعال بين أقسام الأمان السيبراني وتقنية المعلومات

Defensys SOAR

لأتمتة الأمن السيبراني، لرصد
الحوادث والاستجابة

Defensys

حول Defensys

ديفينسيس هي شركة حائزة على جوائز ومعترف بها على الصعيدين الوطني والدولي في مجال حلول الأمن 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

