Security Orchestration, Automation and Response (SOAR)

by

Andisheh Pardazan Goya System

(+98)9131046856

نظام

إدارة الحوادث السيبرانية

يحمى

مع التوسع فى استخدام شبكات الكمبيوتر وكذلك نمو استخدام شبكة الإنترنت العالمية فى البلاد، من المهم جدًا الاهتمام بأمن هذه المنصة.

تتيح تقنية SOAR للمؤسسة تلقى الأحداث الأمنية من مصادر مختلفة والتحقيق فى الحدث الأمنى بناءً على سير العمل والإجراءات المحددة.

لماذا SOAR

أسباب الحاجة إلى تقنية SOAR:

1. زيادة رسوم المراجعة الأحداث الأمنية
2. القيام بالمهام المتكررة
3. قوة محلل محدودة
4. إدارة عملية المراجعة الشؤون الأمنية
5. إدارة عملية المراجعة الشؤون الأمنية

ميزة الاستخدام SOAR

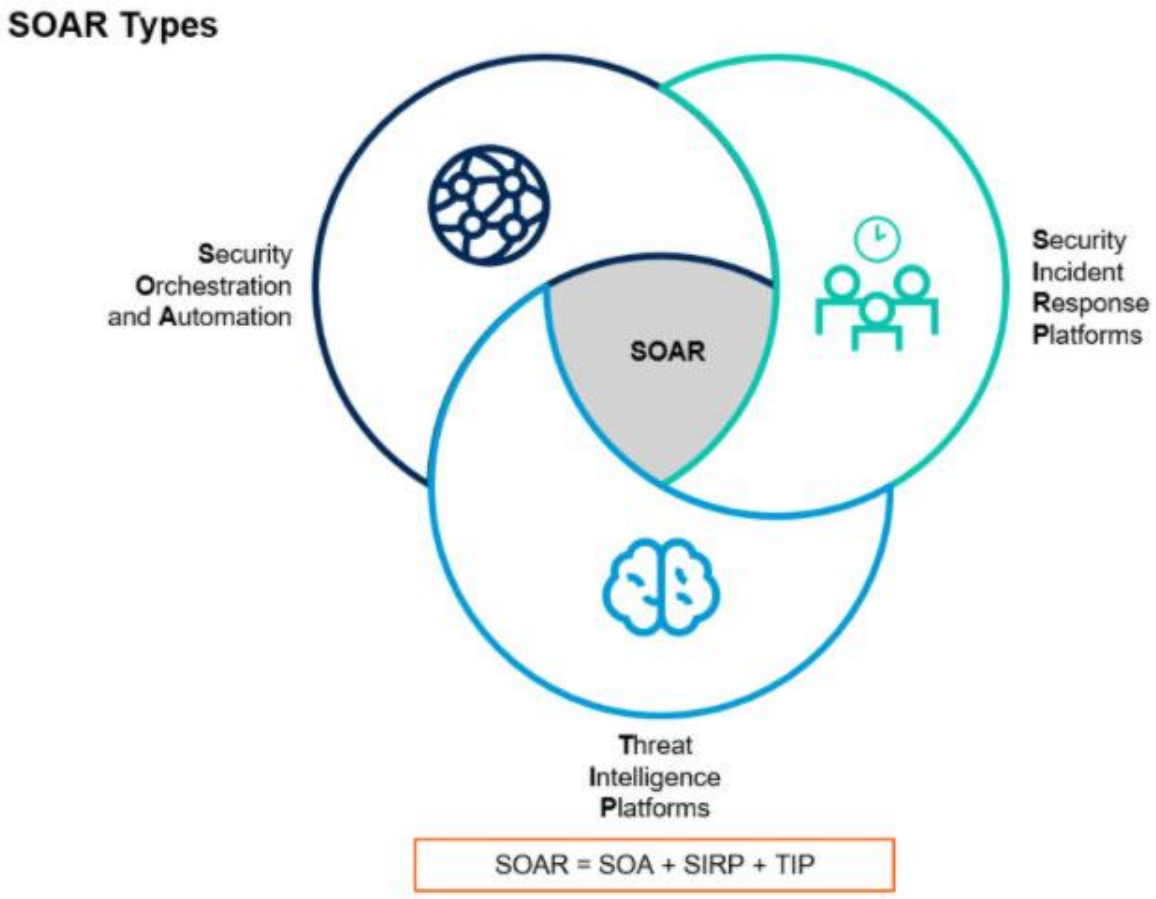
تعزيز وتحسين الاستجابة للحوادث باستخدام معلومات التهديدات	الإزالة النشطة للتحذيرات الأمنية
زيادة الكفاءة باستخدام المقاييس الآلية	تحسين الإدارة مركز العمليات الأمنية أو SOC مع العمليات القياسية

وحدات SOAR

استكمال المعلومات غير الكاملة التى تم جمعها	جمع المعلومات من مصادر مختلفة فى الشبكة
قم بالخطوات مراجعة الحدث باستخدام دليل العملية	الاتصال بمصادر أمنية أخرى للتحقق من الأحداث
	الرد على الأحداث يدويا وتلقائيا

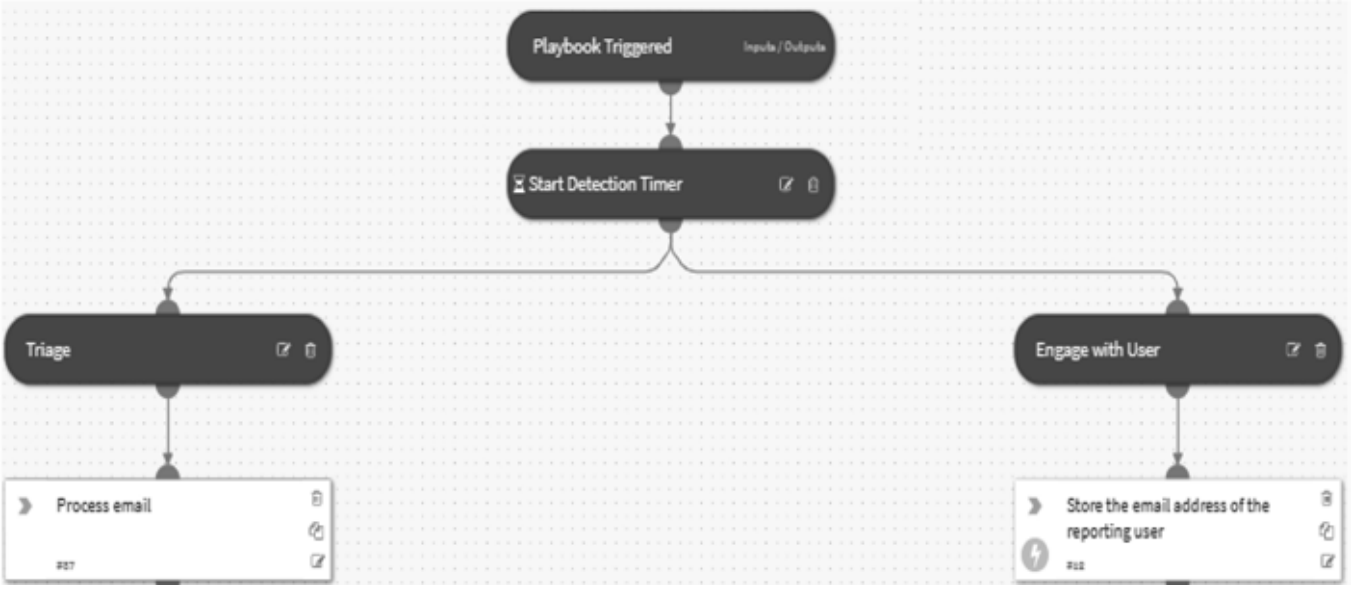
عملية إدارة التشخيص والاستجابة للأحداث

ملخص SOAR


SOAR Types
Security
Orchestration
and Automation
SOAR
Security
Incident
Response
Platforms
Threat
Intelligence
Platforms
SOAR = SOA + SIRP + TIP

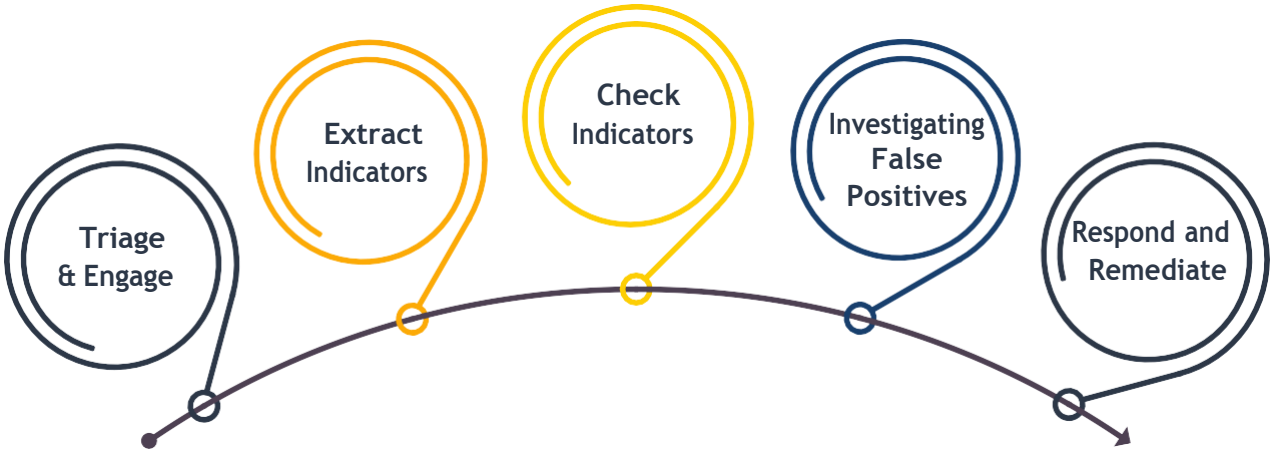
جزء من مميزات المكونات الرئيسية للنظام

- ✓ واجهه المستخدم
- ✓ تعريف دليل العملية
- ✓ التقارير ولوحات المعلومات
- ✓ جمع البيانات
- ✓ القدرة على الاتصال بأنظمة تحديد الهوية الأخرى
- ✓ إمكانية تأكيد المستخدم للتعرف على الهجمات
- ✓ القدرة على تحديد المؤشرات للكشف عن الهجمات
- ✓ ...

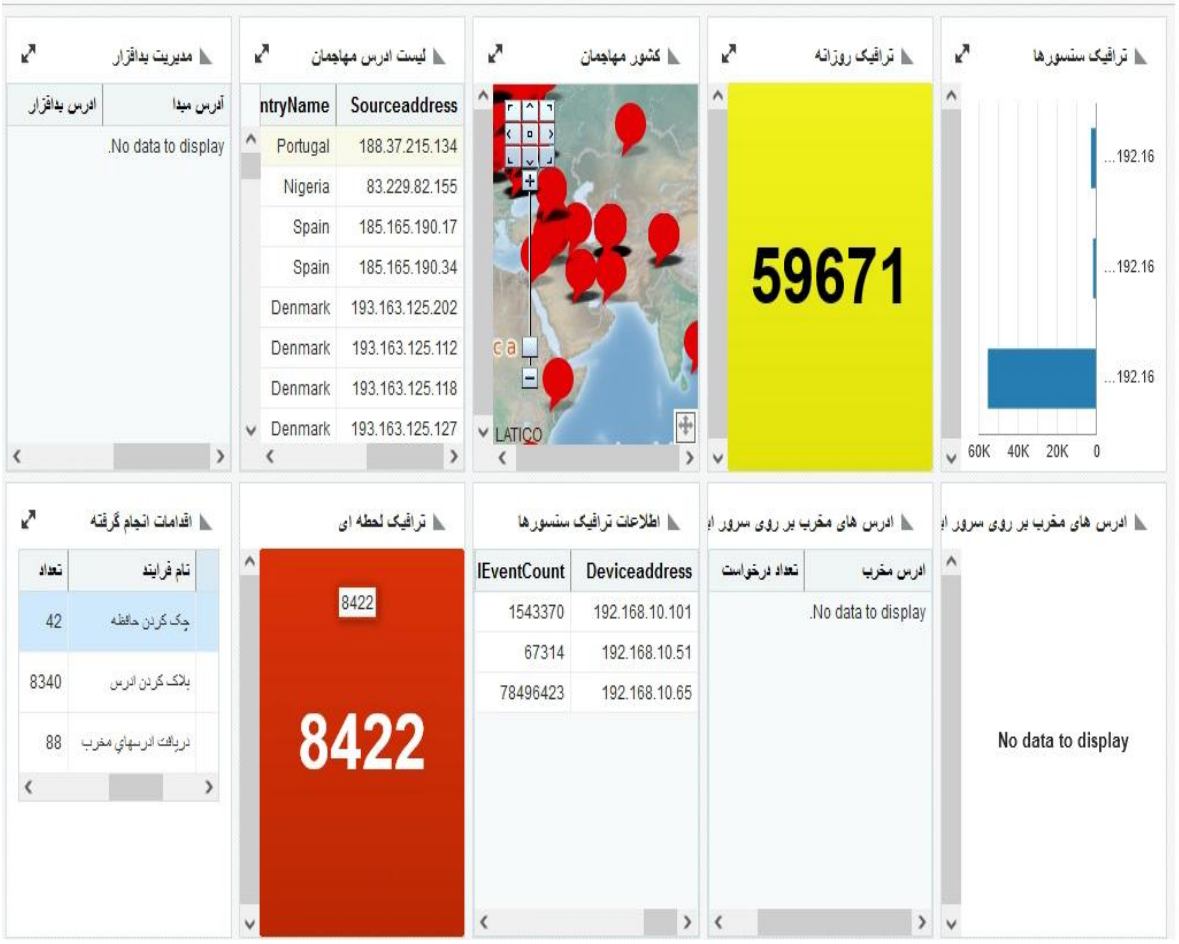


المرافق الاخرى

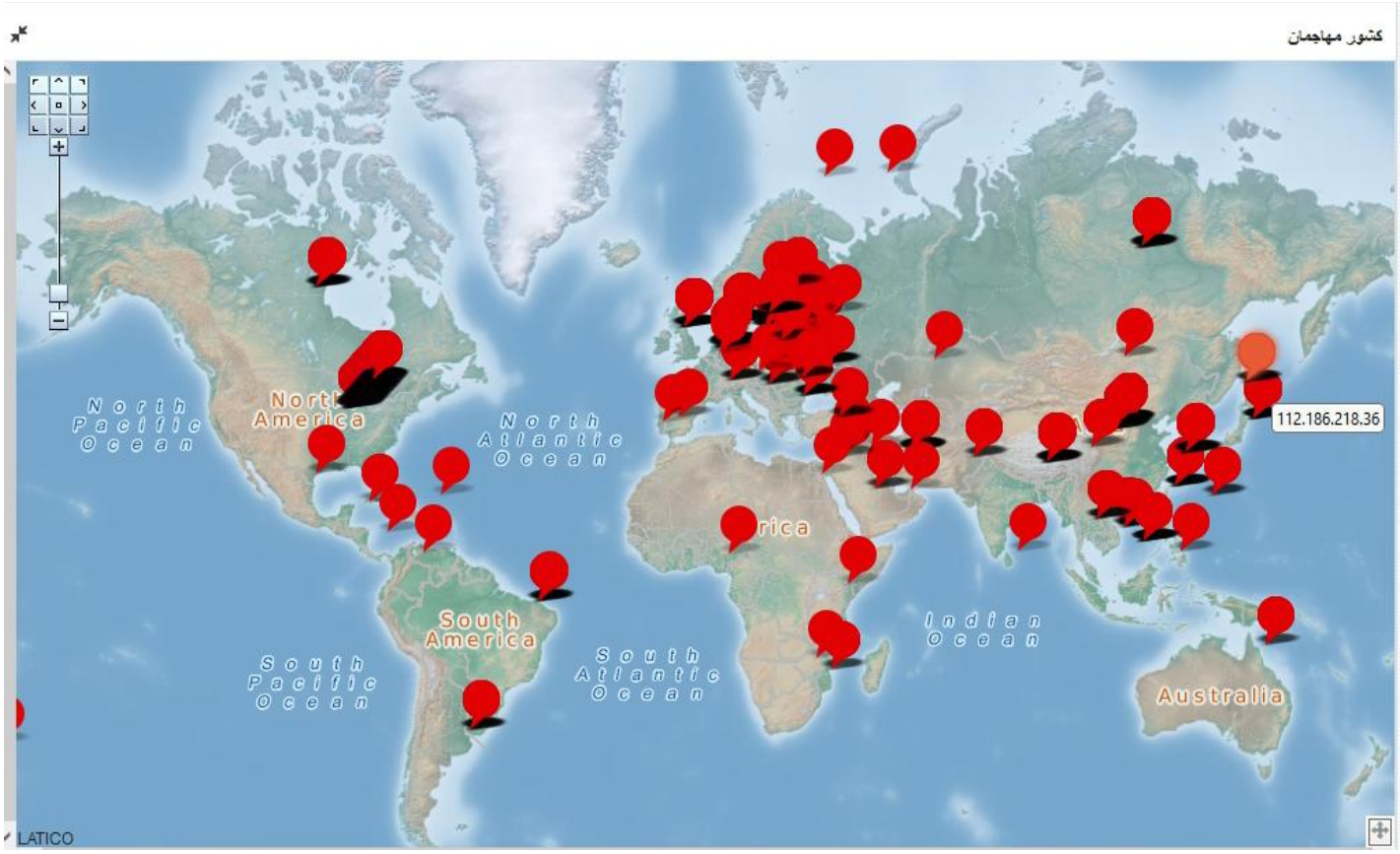
- ✓ لا يوجد حد لعدد السياسات والقدرة على تعيين وإضافة سيناريوهات الأمان من قبل المستخدم
- ✓ قاعدة بيانات معرفية كاملة ومتقدمة
- ✓ القدرة على تحديد عدد غير محدود من المستخدمين ومجموعات المستخدمين وإدارة المستخدمين المتقدمة
- ✓ القدرة على إرسال البريد الإلكترونى والرسائل النصية القصيرة عند إنشاء التنبيهات ونظام التذاكر
- ✓ القدرة على التفاعل مع مراكز العمليات الأمنية الأخرى
- ✓ إمكانية معالجة نتائج استكشاف الثغرات الأمنية فى محرك معالجة الارتباط
- ✓ القدرة على مراقبة حركة مرور الشبكة الواردة والصادرة بشكل كامل حسب المكونات
- ✓ قابلية التحديث



نموذج لنموذج تقرير الإدارة



نموذج لنموذج تقرير الإدارة



قارن المنتجات المماثلة

Guard	QRadar	Arcsight	Splunk	SOLAR WINDS	شاخص ها
OK	OK	OK	OK	OK	USE CASE
MOSTLY	400+	400+	MOSTLY	-	Data source
1000000	1000000	100000	PETABYTE DAILY	25M PER DAY	MAX EPS
MACHINE LEARNING	MACHINE LEARNING AND UEBA AND FORENSICS	MACHINE LEARNING	MACHINE LEARNING AND UEBA	ABNORMAL BEHAVIOR	INTELLIGENCE
SOFTWARE OR CLOUD	APPLIANCE OR SOFTWARE OR CLOUD	APPLIANCE OR SOFTWARE OR CLOUD	SOFTWARE OR CLOUD	VIRTUAL APPLIANCE	DELIVERY
SC,UF,Syslog,CUSTOM	Wincollect,Syslog	SC,Syslog	UF	SEM	Support Agent
BASE ON MAX DAILY DATA OR EPS	PER MONTH	BASE ON MAX DAILY DATA OR EPS	BASE ON MAX DAILY DATA GB/DAY	PER NODES	PRICING

شكراً