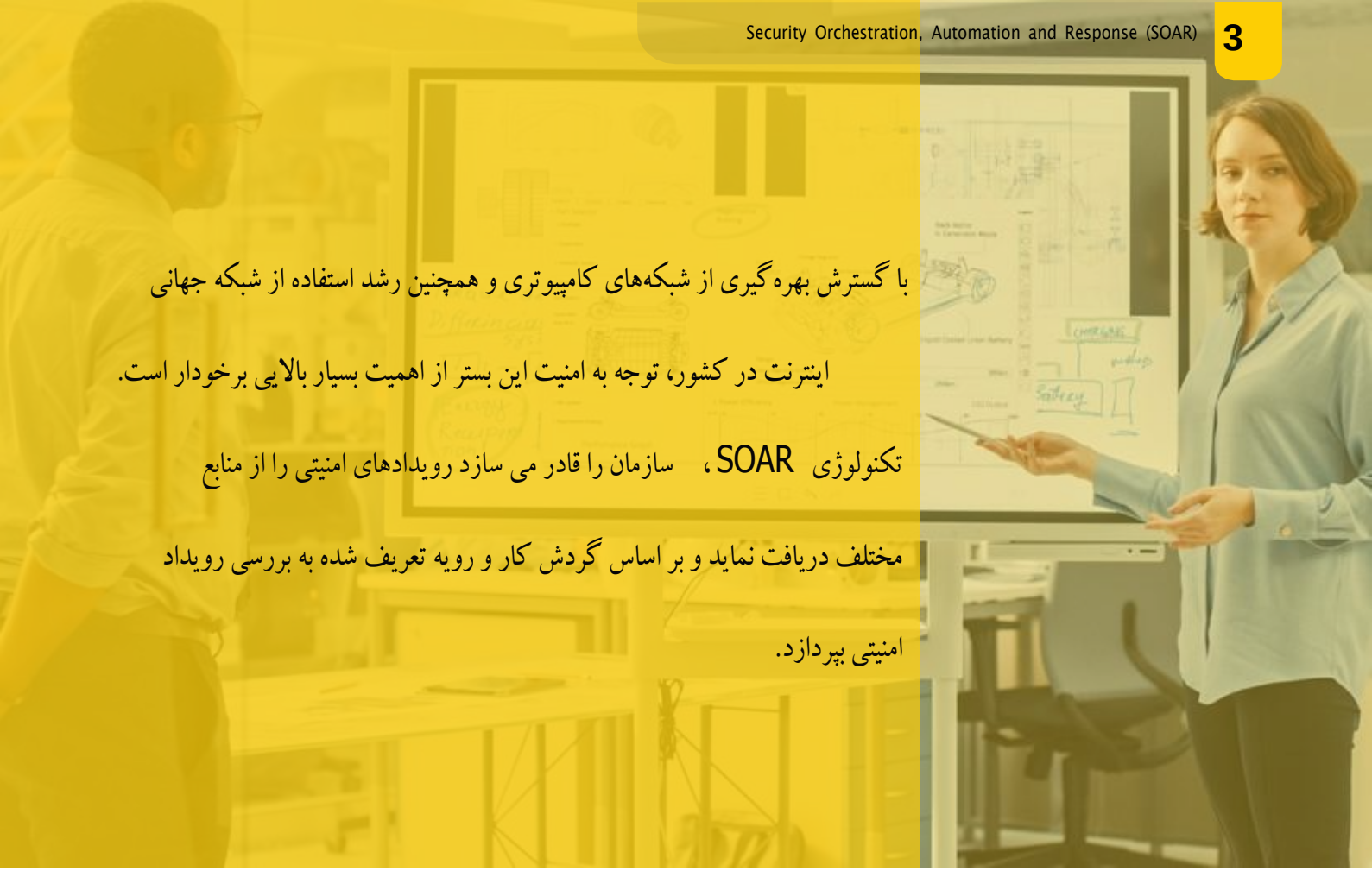
Security Orchestration, Automation and Response (SOAR)

by

Andisheh Pardazan Goya System

(+98)9131046856

سامانه مدیریت رخدادهای سایبری نگهبان



با گسترش بهره‌گیری از شبکه‌های کامپیوتری و همچنین رشد استفاده از شبکه جهانی اینترنت در کشور، توجه به امنیت این بستر از اهمیت بسیار بالایی برخودار است.

تکنولوژی SOAR، سازمان را قادر می سازد رویدادهای امنیتی را از منابع مختلف دریافت نماید و بر اساس گردش کار و رویه تعریف شده به بررسی رویداد امنیتی بپردازد.

چرا SOAR

دلایل نیاز به تکنولوژی SOAR عبارتند از:

1. **افزایش هزینه های بررسی رویدادهای امنیتی**
2. **انجام کارهای تکراری**
3. **نیروی انالیزور محدود**
4. **مدیریت روند بررسی امور امنیتی**
5. **کاهش وابستگی به نیروی انسانی**

مزیت استفاده از SOAR

تقویت و بهبود پاسخ به
رویدادها با هوش تهدید

رفع فعال
هشدارهای امنیتی

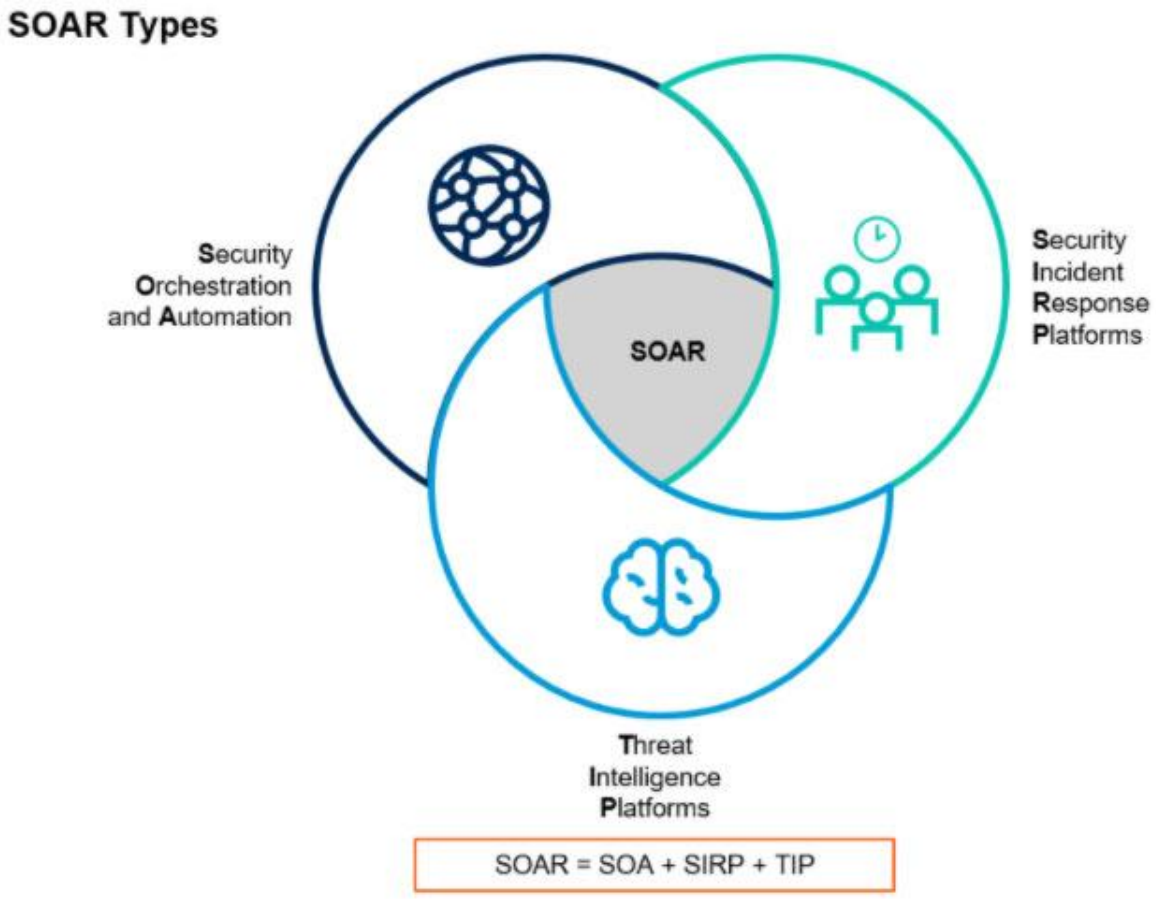
افزایش کارآیی
با معیارهای
خودکارسازی شده

بهبود مدیریت
مرکز عملیات امنیت یا SOC
با فرآیندهای استاندارد

ماژول های SOAR

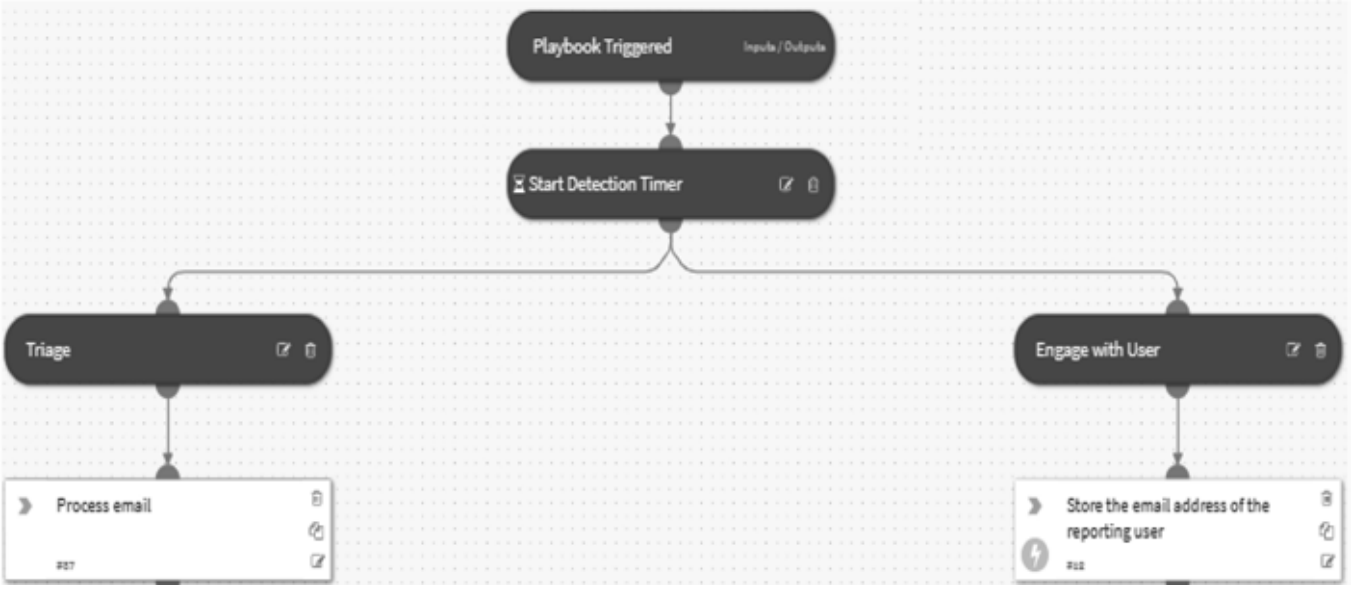
تکمیل اطلاعات ناقص جمع اوری شده	جمع اوری اطلاعات از منابع مختلف در شبکه
انجام مراحل بررسی رویداد با استفاده از کتابچه فرایند	اتصال به سایر منابع امنیتی برای بررسی رویدادها
	پاسخ به رویدادها به صورت دستی و اتوماتیک

نمای کلی SOAR



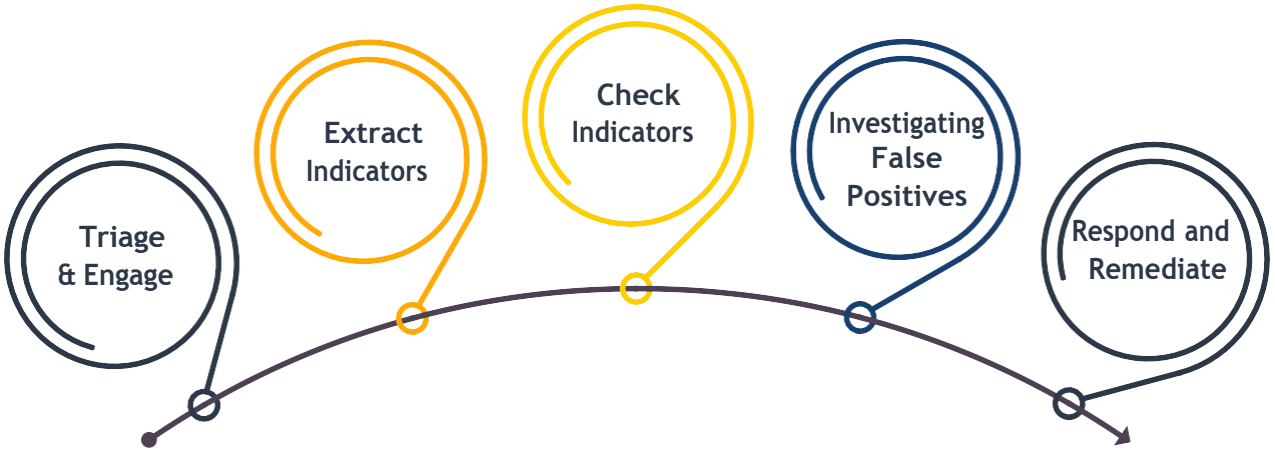
بخشی از ویژگی‌های اجزای اصلی سامانه

- ✓ رابط کاربری
- ✓ تعریف کتابچه فرایند
- ✓ گزارش‌دهی و داشبورد
- ✓ جمع‌آوری داده‌ها
- ✓ امکان اتصال به سامانه های شناسایی دیگر
- ✓ امکان تایید کاربر جهت شناسایی حملات
- ✓ امکان تعریف شاخص برای تشخیص حملات
- ✓ ...

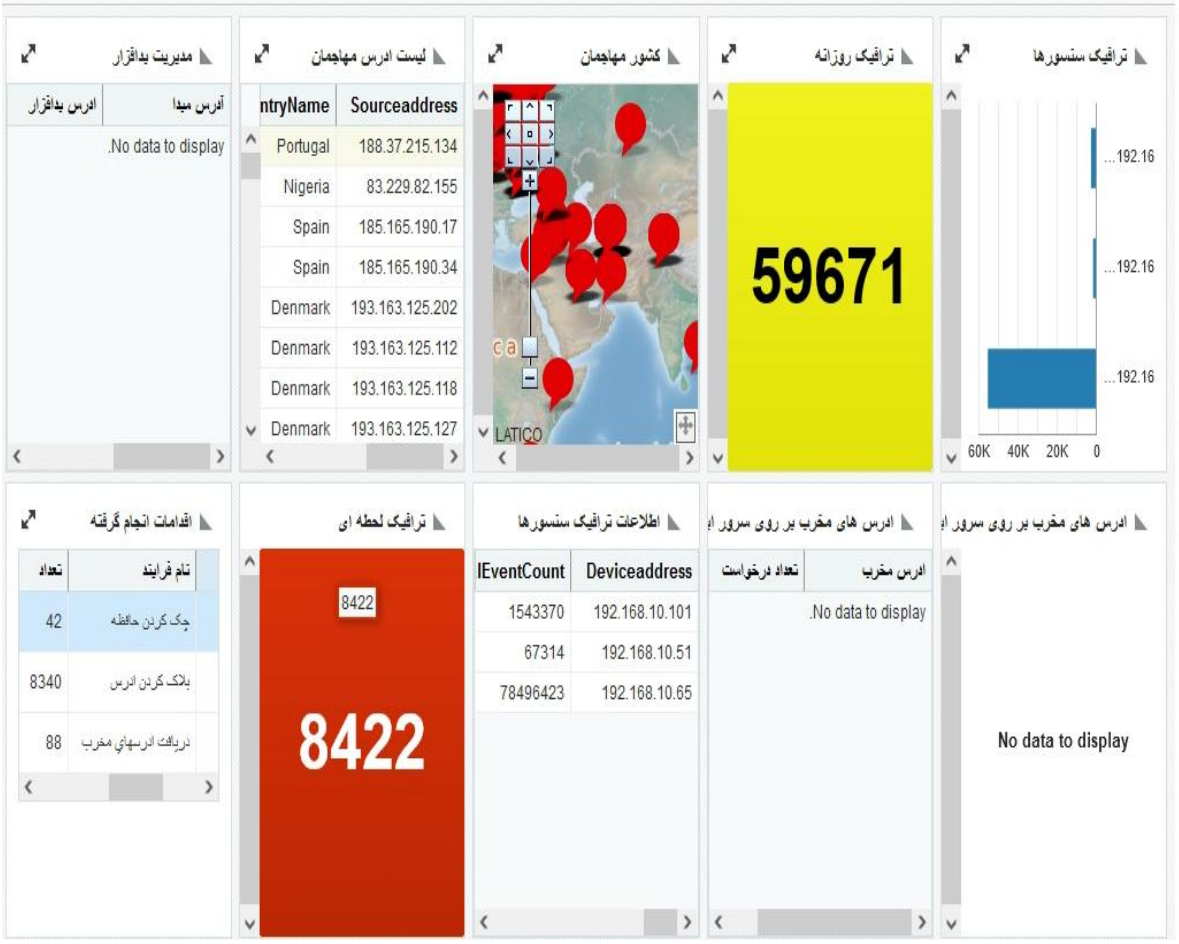


سایر امکانات

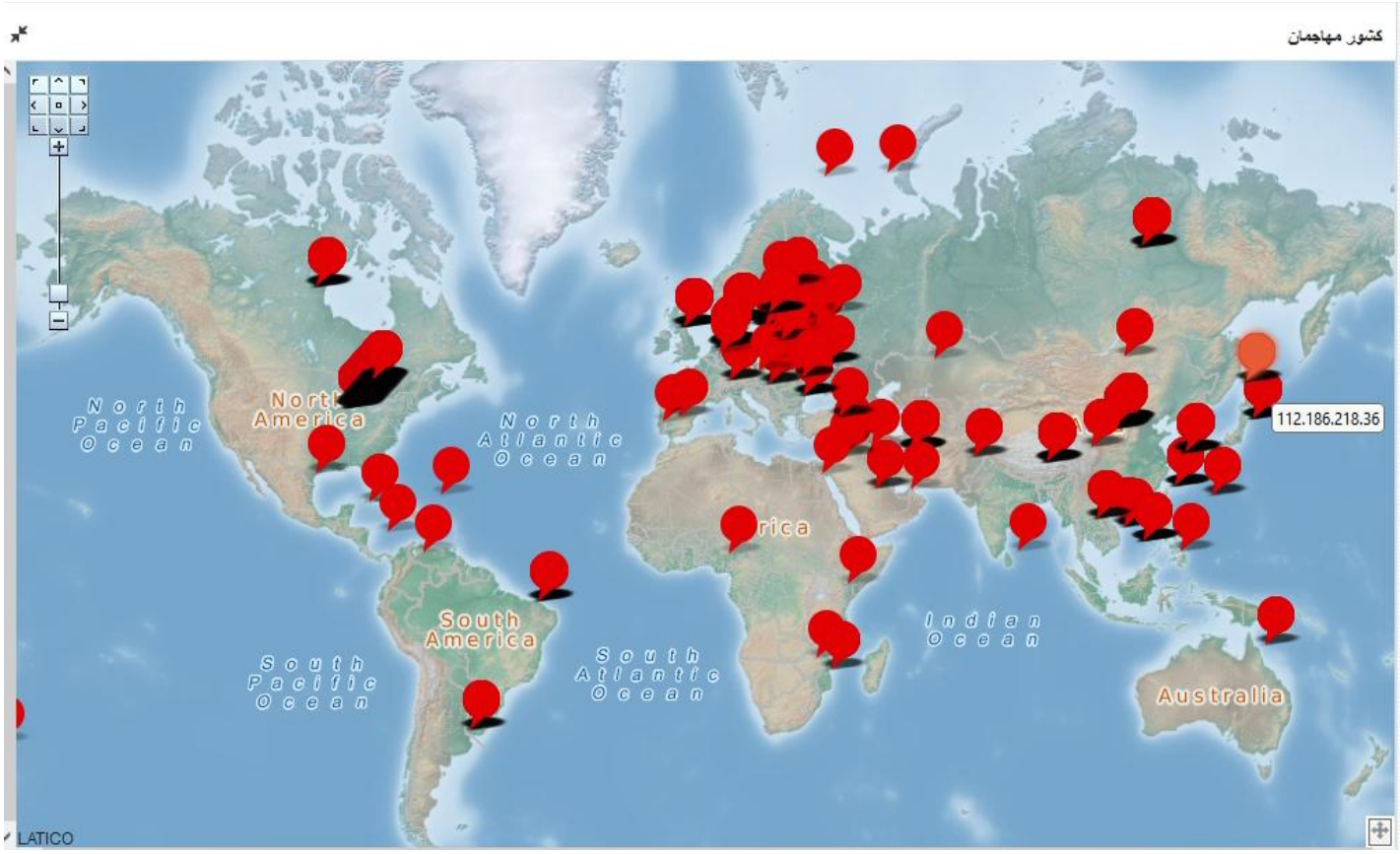
- ✓ **عدم محدودیت در تعداد** Policy**ها و قابلیت تنظیم و اضافه کردن سناریوهای امنیتی توسط کاربر**
- ✓ **پایگاه دانش (** Knowledge Database **) کامل و پیشرفته**
- ✓ **امکان تعریف کاربران و گروه‌های کاربری به تعداد نامحدود و مدیریت پیشرفته کاربران**
- ✓ **امکان ارسال ایمیل و پیامک به هنگام تولید هشدار و سیستم** Ticketing
- ✓ **قابلیت تعامل با دیگر مراکز عملیات امنیت**
- ✓ **امکان پردازش نتایج کاوش آسیب‌پذیری‌ها در موتور پردازش همبستگی**
- ✓ **قابلیت مانیتورینگ کامل ترافیک ورودی و خروجی شبکه به تفکیک اجزاء**
- ✓ **قابلیت به‌روزرسانی**



نمونه فرم گزارش مدیریتی



نمونه فرم گزارش مدیریتی



مقایسه محصولات مشابه

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	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

با تشکر