



مركز عمليات امنيت  
Security Operation Center



## درباره اسپارا

شرکت راهکار هوشمند امن (اسپارا) برای مقابله با تهدیدات پیچیده و پیشرفته سایبری به همراه جمعی از بهترین متخصصان کشور اقدام به تولید و ارائه محصولات نوین، خدمات متنوع و راهکارهای جامع امنیت سایبری کرده است. از مهم‌ترین محصولات اسپارا می‌توان به XDR، EDR، PAM (Satrap) و EMS اشاره کرد. خدمات و راهکارهای امنیتی اسپارا هم شامل طیف وسیعی از خدمات مانند Threat، Pentest، SOC، Red Team، Hunting Incident Response، مشاوره و آموزش می‌شود.

راهکار هوشمند امن

# آمارهای جهانی

## ۱۶/۱۸ میلیارد دلار

ارزش بازار جهانی SOC تا سال ۲۰۳۰ خواهد بود. ارزش این بازار در حال حاضر ۷/۴۳ میلیارد دلار است. (Polaris market research)

## ۶/۴ هزار میلیارد دلار

پیش بینی افزایش شاخص جهانی هزینه جرائم سایبری بین سالهای ۲۰۲۴ تا ۲۰۲۹ خواهد بود. (Statista)

## ۱۵/۶۳ هزار میلیارد

شاخص جهانی جرائم سایبری در سال ۲۰۲۹ خواهد بود. یازده سال متوالی است که این شاخص رو به افزایش است. (Statista)

## ۷/۵٪

میانگین افزایش سالانه بودجه امنیت فناوری اطلاعات در سال ۲۰۲۴ خواهد بود. (Statista)

# معرفی مرکز عملیات امنیت اسپاراس (SOC)

بدیهی است که با افزایش وابستگی سازمانها به فناوری اطلاعات و گسترده تر شدن آنها، خطرات سایبری هم به مراتب افزایش می یابد. تهدیدات سایبری به سرعت در حال تحول است و محافظت در برابر آنها مستلزم نظارت و واکنش سریع است. پیش بینی ها نشان می دهد که شاخص جهانی هزینه جرایم سایبری بین سال های ۲۰۲۴ تا ۲۰۲۹ در مجموع ۶/۴ هزار میلیارد دلار افزایش می یابد و به ۱۵/۶۳ هزار میلیارد دلار می رسد.

از طرف دیگر این تهدیدها و حملات فقط مختص سازمان های بزرگ و دولتی نیست. خطرات سایبری و هک شدن در کمین هر کسب و کاری است و هرچقدر هم که روش های دفاعی و حفظ امنیت پیشرفته تر شود به همان نسبت هم روش های مهاجمان پیچیده تر می شود. به همین دلیل سازمان ها باید به دنبال شیوه ها و راهکارهای نوین، سریع و به روز برای شناسایی خطرات و تهدیدات در کمترین زمان و واکنش مناسب و به موقع به آنها باشند، مسئولیتی که بر عهده تیم مرکز عملیات امنیت است.

**تیم مرکز عملیات امنیت (SOC) اسپاراس** برای پیشگیری از انواع حملات، تشخیص به موقع و ارائه راهکارهای بهینه، به تکنولوژی های برتر روی آورده تا بتواند حوادث امنیتی را کشف و تحلیل کند. مرکز عملیات امنیت اسپاراس با رصد تجهیزات سازمان، جمعیت لاگ ها و شناسایی فعالانه خطرات امنیتی، از شما در برابر تهدیدات دفاع می کند و با کاهش تاثیرات مخرب آنها به تداوم سرویس دهی کمک می کند.

# سرویس‌های قابل ارائه در SOC اسپارا

# تجهیزاتی که SOC راه‌اندازی می‌کند

**راه‌اندازی و نگهداری مرکز عملیات:** راه‌اندازی، میزان

سازی و نگهداری ابزار موردنیاز برای پایش و تحلیل

رویدادهای امنیتی و تهیه فرایندهای مربوطه

**MDR:** تحلیل و بررسی رخدادهای شناسایی‌شده و ارائه

گزارش‌های جهت تبیین رخدادهای لایه‌های مختلف

سازمان

**پاسخگویی به رخداد:** جمع‌آوری شواهد رخدادهای امنیتی و

بررسی عمیق آن‌ها و همچنین ایجاد مکانیزمی جهت مقابله

با تهدیدات یا اطلاع به بخش‌های مربوطه جهت انجام

اقدامات موردنیاز

**شکار تهدیدات:** جستجوی فعالانه برای تهدیداتی که

تجهیزات امنیتی موجود از شناسایی آن عاجز مانده‌اند

**ارزیابی مراکز عملیات امنیتی:** ارزیابی بلوغ ابعاد مختلف

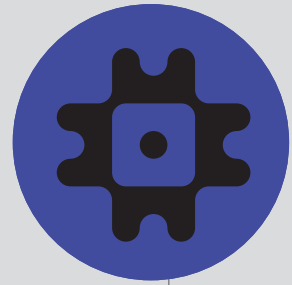
یک SOC و ارائه پیشنهاد جهت بهبود نقاط ضعف احتمالی

**مدیریت آسیب‌پذیری و تنظیمات امنیتی:** شناسایی و

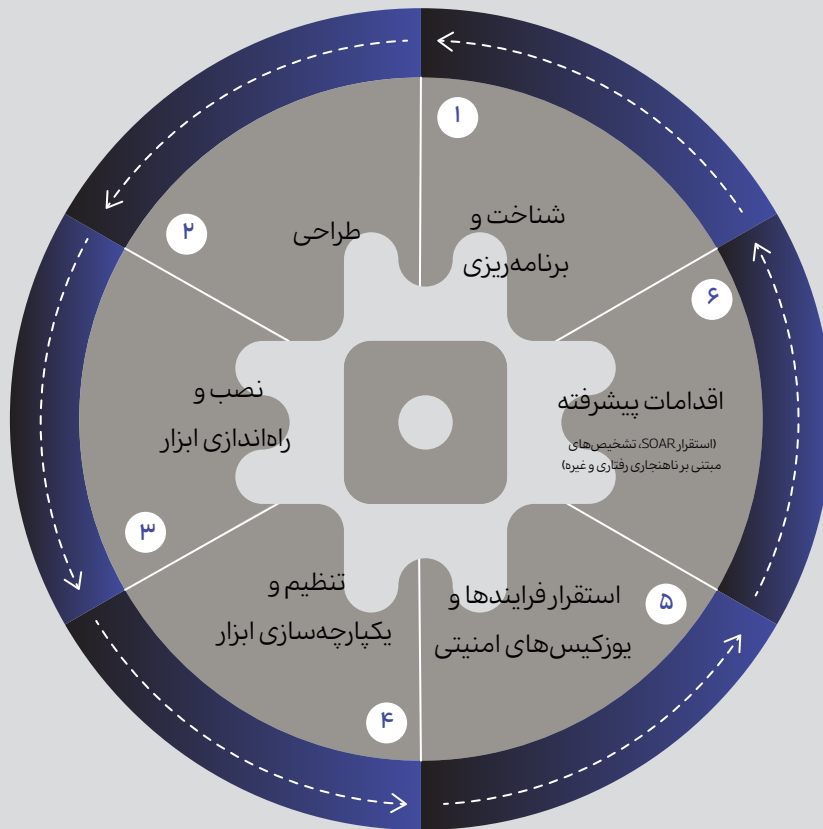
ارزیابی مداوم تنظیمات و آسیب‌پذیری‌های احتمالی روی

دارایی‌های مختلف سازمان

<b>SIEM</b>
<b>TIP (Threat Intelligence Platform)</b>
<b>FIM (File Integrity Monitoring)</b>
<b>IDS</b>
<b>Vulnerability Scanner</b>
<b>FPC (Full Packet Capture)</b>
<b>NTA (Network Traffic Analysis)</b>



# مراحل پیاده‌سازی SOC





# مزایای برون سپاری خدمات امنیتی

باتوجه به تجربیات ارزشمند متخصصان تیم SOC اسپارا، بدون شک یکی از بهترین راهکارها جهت استفاده از این تجربیات و کاهش دغدغه‌های مربوط به تامین نیروی انسانی، برون سپاری کامل سرویس‌های امنیتی به تیم امنیتی اسپارا است. با توسعه خدمات رایانش ابری در دنیا و مزیت‌های این فناوری، الگوی برون سپاری خدمات امنیتی به کسب و کارهای متخصص در این حوزه هم محبوبیت بیشتری پیدا کرده است.

از مهم‌ترین مزایای برون سپاری خدمات امنیتی، تمرکز کسب و کار روی حوزه تخصصی خود و استفاده از تیم‌ها و متخصصان باتجربه بیرونی در حوزه امنیت سایبری است که منجر به کاهش هزینه‌ها و افزایش سطح امنیت خواهد شد.

## SOC اسپارا چه آورده‌ای برای شما دارد؟

- مقیاس پذیری بالا و استفاده از راهکارهای کلان داده (Big Data)
- استفاده از الگوریتم‌های هوش مصنوعی و یادگیری ماشین
- کاهش نرخ مثبت کاذب (FP)
- کاهش عملیات تکراری و بار کاری نیروی انسانی با خودکارسازی بخش‌هایی از فرایند رسیدگی به رخداد
- استفاده بهینه از منابع IT جهت غنی‌سازی رویدادها و کشف حملات
- استفاده از سناریوهای امنیتی متنوع
- پشتیبانی از منابع لاگ مختلف
- امکان ارائه خدمات به شکل متنوع (MSSP، نیروی مقیم و غیره)

# مشتریان اسپارا



بانک پارسیا گاد



MIDHCO



شرکت کسپوتین  
انرژی پارسیا



بیمه پارسیا گاد



شرکت پرداخت الکترونیک  
پارسیا گاد



فناپ تلکام  
FANAP TELECOM



فناپ تک  
FANAP TECH



فناپ  
زیرساخت



شرکت نرم‌افزاری دانش آبرین ششم



بانک اطلاع‌رسانی پشتیبانی پاد



پارسیا  
PARSA.CO



بانک تجارت



ZAFTA



پست بانک ایران



بانک آینده  
AYANDEH BANK



شرکت فناوری اطلاعات ناورو



HATEL  
شاتل



هواداول



ایرانسل  
MTN



تنتاسا



Zitel



WALLEX



کنزبان



پادرق  
سازمان مدیریت ایران ۱۳۵



شرکت سیم‌دگذاری سروکس  
ایران به‌لار و تسویه وجوه (سخت‌نا)



ساییا



سارپو  
SARPO



سازمان فناوری اطلاعات ایران



آلفا  
ALPHA



فرزان فن اندیش فردا  
FARZANFANANDISH



addrun  
توسعه راهکارهای هوشمند آدران



MES BROKER



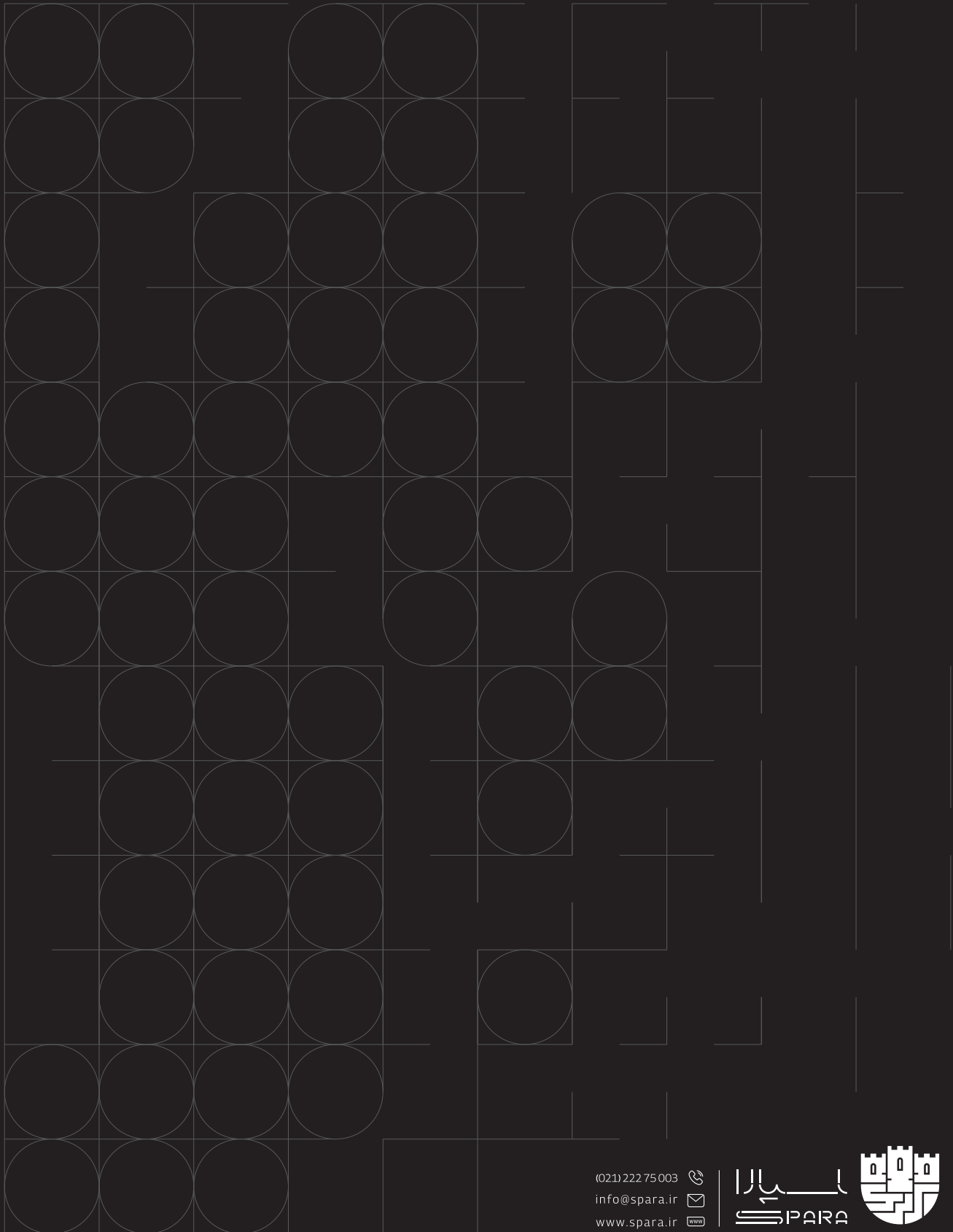
مستشاران بورس بومی



ریاست جمهوری  
معاونت علمی و فناوری



آتیه داده پرداز



(021) 222 75 003  
info@spara.ir  
www.spara.ir



سپارا  
S PARA

