پارا
SPARA

EDR

شناسایی و پاسخ به نقاط انتهایی
Endpoint Detection and Response

درباره اسپارا

شـرکت راهـکار هوشـمند امن (اسـپارا) بـرای مقابله بـا تهدیدات پیچیده و پیشـرفته سـایبری به همراه جمعی از بهترین متخصصان کشـور اقدام به تولیـد و ارائه محصـولات نوین، خدمـات متنوع و راهکارهای جامع امنیت سایبری کرده است. از مهم‌ترین محصولات اسـپارا می‌توان به XDR، EDR، PAM و EMS اشاره کرد. خدمات و راهکارهای امنیتی اسـپارا هم شـامل طیف وسیعی از خدمات مانند Threat Hunting، Pentest، SOC، Red Team، Incident Response، مشاوره و آموزش می‌شود.

معرفی سامانه شناسایی و پاسخ به نقاط انتهایی (EDR)

یک شبکه از گروهی از دستگاه‌های کامپیوتری تشکیل شده که داده‌ها را مبادله می‌کنند و به هریک از این دستگاه‌ها نقطه پایانی (Endpoint) گفته می‌شود. به عبارت دیگر، نقطه پایانی هر دستگاهی است که به شبکه کامپیوتری متصل می‌شود. از طرف دیگر شرکت‌ها و کارمندان آن‌ها برای دسترسی روان‌تر به داده‌ها، هر روز بیشتر از گذشته شیوه‌ها را با یکدیگر ترکیب می‌کنند و افزایش روش‌های BYOD (دستگاه خود را بیاورید)، منجر به آسیب‌پذیری چندگانه نقاط انتهایی می‌شود.

ابزارهای امنیتی سنتی برای محافظت از این نقاط انتهایی، به دلیل ضعف‌هایی که دارند نمی‌توانند تهدیدات پیشرفته را شناسایی و متوقف کنند. درواقع آنتی‌ویروس‌ها و دیگر محصولات مشابه (EPP) که از روش‌های تشخیص و جلوگیری مبتنی بر امضا (Signature) استفاده می‌کنند، علی‌رغم الزامی بودنشان برای سازمان‌ها، به‌تنهایی نمی‌توانند در مواجهه با حملات APT، حملات بدون فایل، باج‌افزارهای پیشرفته و حملات فیشینگ کارایی داشته باشند.

محصول **شناسایی و پاسخ به نقاط انتهایی (EDR) اسپارا** با استفاده از روش‌های تحلیل رفتاری و تکنیک‌های تحلیل داده و با هدف افزایش امنیت در سطح نقاط انتهایی، بعد از جمع‌آوری و بررسی عمیق رویدادهای سیستمی، رفتارهای مخرب را تشخیص و گزارش می‌دهد.

آمارهای جهانی

+۳۶
میلیارد دلار

پیش‌بینی ارزش بازار جهانی امنیت نقاط انتهایی تا سال ۲۰۲۸ است. (Statista)

۳۱۷/۵۹
میلیون

تعداد اقدامات باج‌افزاری انجام‌شده در سراسر جهان در سال ۲۰۲۳ بوده است. (Statista)

٪۹۰

از حملات سایبری موفق از نقاط انتهایی آغاز شده‌اند. (IBM)

+۵
میلیون دلار

میانگین هزینه هر حمله باج‌افزاری در سال ۲۰۲۳ بوده است. (Fisher Philips)

EDR

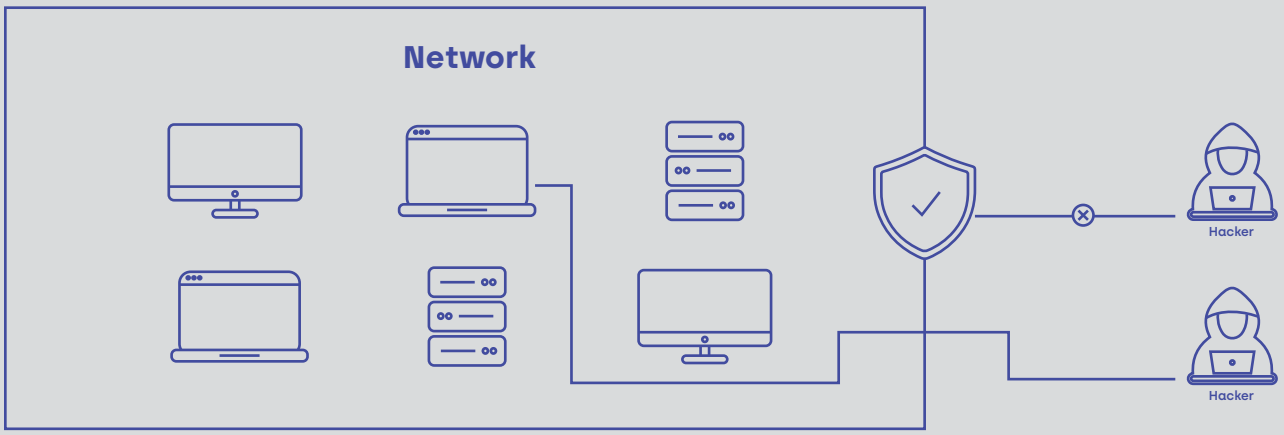
ویژگی‌های محصول EDR اسپارا

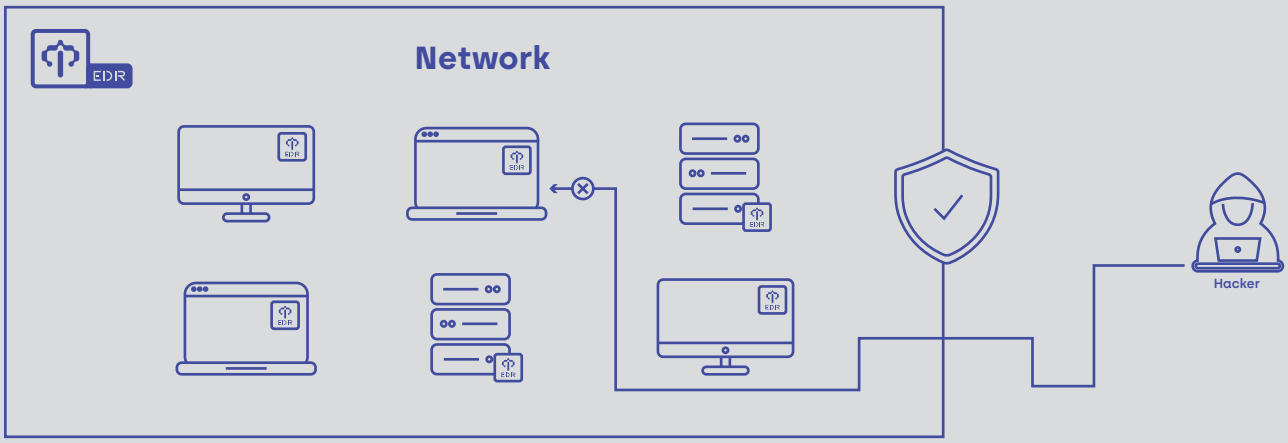
- جمع‌آوری رویدادهای سیستم در سطح کرنل
- امکان پاسخ‌دهی به حملات از طریق ایزوله کردن سیستم یا از بین بردن فرآیندهای مخرب
- امکان اسکن سیستم براساس امضای بدافزارها
- بررسی مطابقت رایانه‌ها بر اساس استاندارد امنیتی مورد استفاده در سازمان
- محافظت در برابر حمله مهاجم به ایجنت EDR
- ایجاد ارتباط امن بین سرور و ایجنت با پروتکل‌های امنیتی به‌روز (TLS1.2)
- پیاده‌سازی الزامات امنیتی EDR افتا
- امکان تشخیص حملات سایبری پیشرفته از طریق تشخیص رفتار (رفتارهای یک مرحله‌ای یا چند مرحله‌ای)
- امکان تشخیص رخدادهای امنیتی براساس تشخیص ناهنجاری با یادگیری ماشین
- استفاده از تکنولوژی‌های به‌روز موتور جستجو برای بررسی رویدادهای کل رایانه‌ها
- استفاده از تکنولوژی داکر برای راه‌اندازی و به‌روزرسانی سریع و راحت

نحوه عملکرد EDR

محصول EDR اسـپارا به‌عنوان یکی از محصولات مهم در صنعت امنیت، با مدل‌سـازی رفتارهای سـطح سیستم در تمامی رایانه‌های شبکه دید جامعی از اتفاقات شبکه به مدیران امنیت می‌دهد و در کاهش زمان کشف، بررسی و پاسخ‌دهی به حملات بسیار تاثیرگذار است.

ایـن محصول بـا بهره‌مندی از تکنولوژی‌هـای روز، به‌عنوان یکی از نمونه‌های داخلی موفق به شـمار می‌رود. بسـیاری از مشـتریان دولتی و سازمانی برای تامین امنیت خود به اسپارا اعتماد کرده‌اند و EDR تا کنون در تامین نیازهای این سازمان‌ها در حوزه امنیت نقاط انتهایی موفق عمل کرده است.





منابع موردنیاز

ایجنت محصول EDR اسپارا از سیستم‌های عامل Win7SP1 و بالاتر پشتیبانی می‌کند. اگر مایل به استفاده از نسخه درون سازمانی (On-Permise) محصول هستید، نیاز به یک ماشین با چنین خصوصیاتی دارید:

Minimum System Requirements:
CPU: 8 Core
RAM: 32 GB
Storage: 1 TB SSD (3 Month)

این خصوصیات برای حدود 5K EPS (که برای حدود ۱۰۰۰ کلاینت در نظر گرفته شده) مناسب است.

Recommended System Requirements:
CPU: 16 Core
RAM: 128 GB
Storage: 3TB SSD (3 Month)

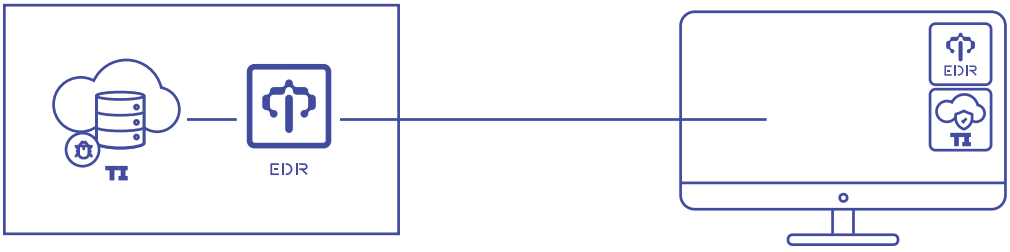
این خصوصیات برای حدود 15K EPS (که برای حدود ۵۰۰۰ کلاینت در نظر گرفته شده) مناسب است.

مراحل اجرا و پیاده‌سازی

راه‌اندازی سرور	نصب ایجنت در نقاط انتهایی
ـ با استفاده از ابزار docker و در محیط container انجام می‌شود. ـ سرویس docker image توسط تیم اسپارا و در داخل ایران راه‌اندازی شده است. ـ به‌روزرسانی سرور در هر زمانی و از طریق دریافت آخرین نسخه docker image امکان‌پذیر است.	ـ تیم اسپارا فایل نصبی با فرمت MSI را در اختیار کارفرما قرار می‌دهد. ـ این فایل با هر ابزار مدیریت دارایی مورد استفاده سازمان، نصب و راه‌اندازی می‌شود. ـ قابلیت استقرار از راه دور توسط ابزارهای استقرار تیم پشتیبانی اسپارا وجود دارد.

سامانه هوش تهدید

سـامانه‌های هوش تهدید که با عنوان «TI» شـناخته می‌شود، زیرسـاخت‌هایی ابری متشکل از داده‌های پیش‌پردازش‌شـده‌ای از حملات اخیر و تهدیدات حال حاضر جهان هستند. این داده‌ها به سامانه‌های EDR کمـک می‌کند تـا از دانش و داده‌های جدیدترین حملات جهان آگاه شـود و روش‌هـای مقابله با آن‌ها را در اختیار داشته باشند. استفاده از سامانه TI در کنار سامانه EDR قابلیت‌های حفاظتی را دو چندان می‌کند.



تفاوت EDR با محصولات EPP

محصولات EPP مانند آنتی‌ویروس در مقایسه با سامانه‌های EDR اهداف مشابه دارند اما نیازهای متفاوتی را پوشـش می‌دهند. محصولات EPP با تشخیص فایل‌ها و عملکردهای مخرب از طریق رویکردهای مبتنی بر امضا، نسبت به جلوگیری از رفتارهای مخرب اقدام و با جلوگیری از اجرای فایل‌های مخرب، امنیت سیستم را حفظ می‌کنند. به عبارت دیگر آنتی‌ویروس می‌تواند جلوی بدافزار را بگیرد اما مشخص نمی‌کند که این بدافزار به چه طریق وارد شبکه شده و گسترش پیدا کرده است.

در مقابل سامانه‌های EDR با رویکرد تحلیل رفتار با فرض وجود مهاجم در شبکه اقدام به شکار تهدیدات سایبری می‌کند. رویکرد سامانه‌های EDR مکمل رویکرد محصولات EPP است. درواقع EPPها اولین خط دفاعی سازمان در مقابل حملات هستند و EDR دومین لایه محافظتی سازمان به‌شمار می‌رود. حملاتی که توسط EPPها قابل کشف نیستند با رویکرد تحلیل رفتاری EDR کشف می‌شوند یا به تحلیل‌گر امنیتی قابلیت‌هایی برای شکار این تهدیدات ارائه می‌دهند. یک استراتژی امنیت دفاعی موثر در یک سازمان، از رویکرد جلوگیری (EPP) و رویکرد کشف و شکار (EDR) به‌طور همزمان استفاده می‌کند.

در جدول زیر برخی تفاوت‌های دو محصول EDR و EPP عنوان شده است:

EDR	EPP
تمرکز روی شناسایی تهدید است	تمرکز روی جلوگیری از تهدید است
شناسایی تهدید فعال	شناسایی تهدید منفعل
جمع‌آوری داده‌های رویداد از نقاط انتهایی	دید محدود نسبت به فعالیت نقاط انتهایی
امکان پاسخ‌دهی و مهار سریع حملات	ارائه سطح اولیه‌ای از جلوگیری از تهدید
فراهم کردن داده‌ها و زمینه برای حملاتی که چندین نقطه انتهایی را در بر می‌گیرد	تمرکز بر محافظت از هر نقطه انتهایی به‌صورت ایزوله
استفاده از رویکرد تحلیل رفتار	استفاده از رویکردهای مبتنی بر امضا

تفاوت EDR با SIEM

علی‌رغم شباهت‌های بسیار زیاد این دو محصول از بعضی ابعاد، در محل استفاده و کارکرد دو تفاوت اصلی دارند:

تفاوت در کشف حملات

- سامانه‌های EDR دقت کشف حملات را بالا می‌برد
- سامانه‌های EDR باعث کاهش میزان False positive هشدارها و هزینه عملیات می‌شود
- EDR قابلیت‌های بالاتری نسبت به SIEM در زمینه تحلیل و واکاوی داده‌های نقاط انتهایی دارد
- EDR ابزار دفاع قدرتمندتری نسبت به SIEM در مقابل حملات سطح نقاط انتهایی است

تفاوت در قابلیت‌های پاسخ‌دهی به حملات

EDR	SIEM
با قابلیت‌های مختلف محدودسازی، از گسترش حمله جلوگیری می‌کند	ذاتا قابلیت پاسخ‌دهی به حملات را ندارند و متکی به محصولات دیگری مانند SOAR هستند
محدوده تحت شعاع حمله را کاهش می‌دهد	—
با در اختیار داشتن ابزارهای بررسی عمیق به تحلیل‌گر امنیتی در شناسایی نقطه شروع و ریشه حمله کمک می‌کند	—
در نهایت استراتژی بهینه این است که شناسایی تهدیدات سمت نقاط انتهایی به EDR سپرده شود و لاگ‌های سامانه‌های EDR برای جمع‌بندی به SIEM ارسال شود.	

مزایای رقابتی EDR اسپارا

افزایش سرعت
بررسی تهدیدات

ارائه دید جامع از
تمام فعالیت‌های
سیستم‌های
انتهایی

دقت بالای ارسال
هشدار و میزان
False Positive
پایین

راه‌اندازی سرویس
بدون نیاز به
Reboot و
Down-Time

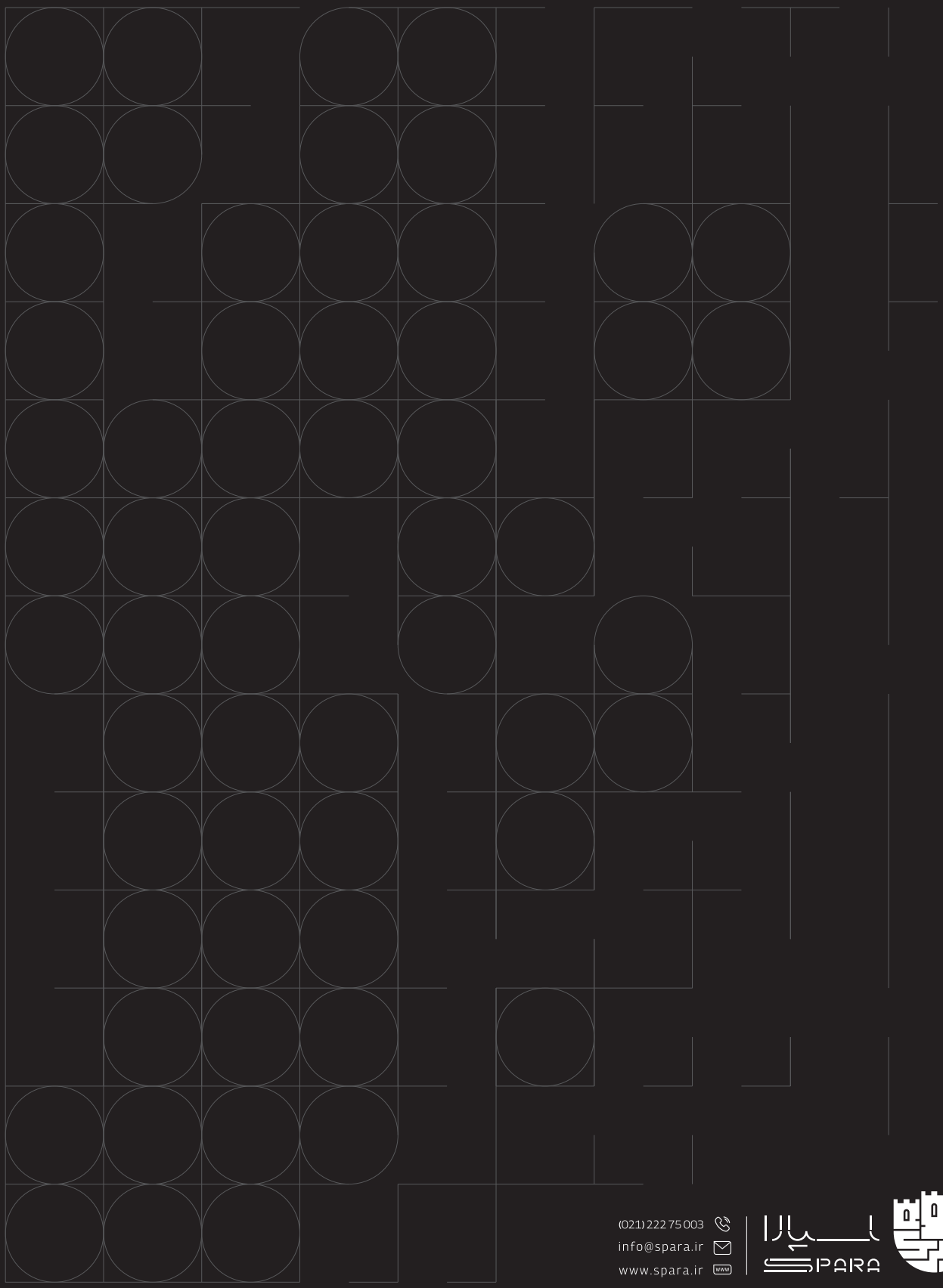
استفاده از پایگاه
داده‌ای از حملات و
داده‌های پردازش
شده

افزایش سرعت
پاسخ‌دهی به
حملات

بهبود شکار
تهدیدات با ارائه
داده‌های زمینه‌ای
از حملات

دانش فنی تیم در
پیاده‌سازی
آزمون‌های نفوذ و
شبیه‌سازی
حملات

مشتریان EDR اسپارا



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

اسپارا
SPARA