شرکت نرم افزاری

امن پرداز

شرکت نرم‌افزاری امن‌پرداز

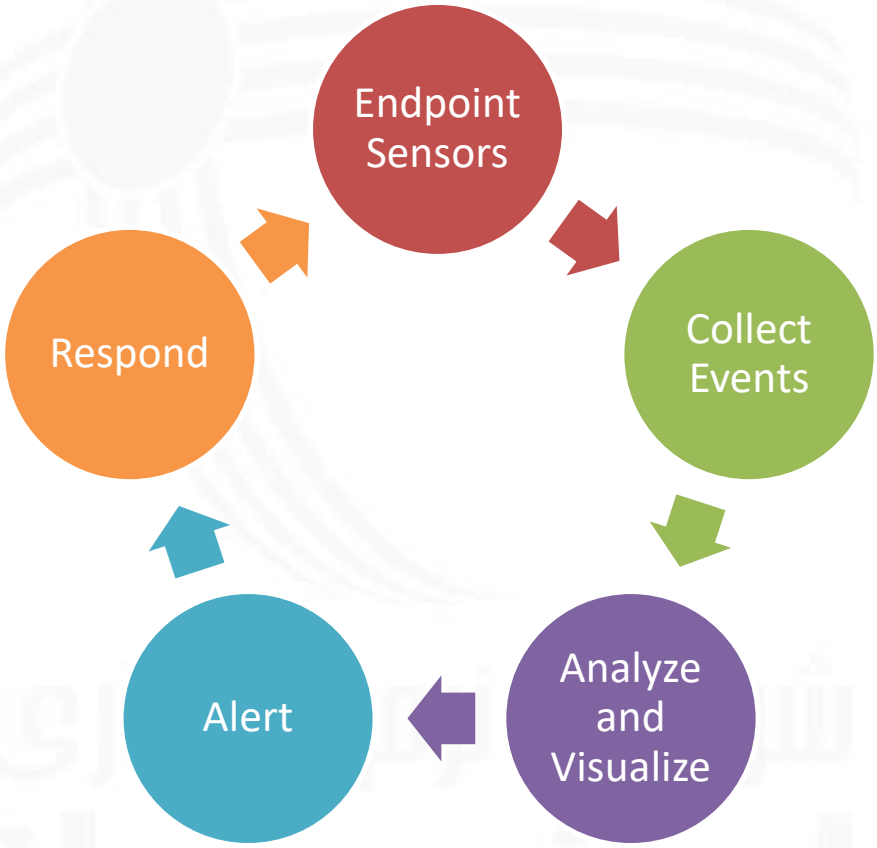
معرفی انواع محصولات Padvish EDR

عادی

فهرست مطالب

۱. پادویش، نسخه کشف و پاسخ به تهدیدات پنهان (Padvish EDR)

سامانه Padvish EDR کل چرخه امنیت را از تشخیص رفتار توسط سنسورهای مستقر در نقطه پایانی، جمع‌آوری اطلاعات، تحلیل و بصری‌سازی، اعلام هشدار، و پاسخ به رویداد را در بر می‌گیرد.



۲. فناوری‌های Padvish EDR

مجموعه فناوری‌های متعددی در Padvish EDR به کار رفته است تا رفتارهای بدافزاری کشف و امکان تشخیص و مقابله با آنها فراهم شود. برخی از این فناوری‌ها در همه یا اغلب سامانه‌های EDR وجود دارند و برخی مانند MultiAV و File Static Analyzers مختص پادویش می‌باشند:

- Behavior Protection
- Anti Malware
- Memory Scanner
- Machine Learning
- Correlation
- Network Attacks Detection (IPS)
- Sandbox
- MultiAV
- File Static Analyzers

۳. انواع لایسنس Padvish EDR

سامانه Padvish EDR در سه نوع لایسنس EDR Base، EDR Select و EDR Expert به فروش می‌رسد:

۱. EDR Base: شامل ماژول‌های اصلی EDR یعنی سنسورها، هشدار، شکار تهدید، پویش و ... می‌باشد.
۲. EDR Select: شامل همه ماژول‌های EDR Base و بخشی از ماژول‌های EDR Expert به انتخاب مشتری می‌باشد.
۳. EDR Expert: نسخه کامل EDR شامل همه ماژول‌های EDR Base به علاوه ماژول‌های آزمایشگاه بدافزار مانند MultiAV، سندباکس و تحلیلگر ایستای فایل می‌باشد.

هر یک از این سه نوع لایسنس بالا، می‌تواند شامل یک افزونه مدیریت دارایی، یا میز خدمت کامل نیز باشد. در افزونه مدیریت دارایی، امکان سنجش و جمع‌آوری اطلاعات کامل دارایی‌های سخت‌افزاری و نرم‌افزاری سازمان، و تشخیص تغییرات آنها مطابق استانداردهای ITIL وجود دارد. افزونه میز خدمت، علاوه بر قابلیت‌های مدیریت دارایی، امکانات کاملی در زمینه تیکتینگ، مدیریت SLA و فرایندهای ITSM سازمان را نیز ارائه می‌دهد.

به این ترتیب لیست لایسنس‌های پادویش به شرح زیر است:

لایسنس EDR	Asset Management مدیریت دارایی مکاپ	Service Desk میز خدمت مکاپ
EDR	EDR - AM	EDR - SD
EDR Select	EDR Select - AM	EDR Select - SD
EDR Expert	EDR Expert – AM	EDR Expert – SD

۴. ماژول های Padvish EDR

سامانه Padvish EDR ماژول‌های متعددی دارد که در جدول زیر لیست آنها و اینکه هر ماژول در کدام لایسنس فعال می‌باشد مشخص شده است:

	EDR Base	EDR Select	EDR Expert
Dashboard	✓	✓	✓
EDR Sensors	✓	✓	✓
Alert Engine	✓	✓	✓
Threat Hunting	✓	✓	✓
IOC Scanner	✓	✓	✓
File Library	✘	✓	✓
Multi AV	✘	Selective	✓
Sandbox	✘	Selective	✓
File Static Analyzers (Windows Files)	✘	Selective	✓
File Static Analyzers (Linux Files)	✘	Selective	✓
File Static Analyzers (Android Files)	✘	Selective	✓

با توجه به لایسنس‌های فوق، ماژول‌های انتخابی در Padvish EDR شامل موارد زیر می‌باشند:

۴,۱. ماژول کتابخانه فایل (File Library)

ماژول کتابخانه فایل وظیفه جمع‌آوری فایل‌های اجرایی از تمامی کلاینت‌های EDR را جهت انجام عملیات تحلیلی برعهده دارد. این کتابخانه سرویس پایه‌ای ارائه می‌دهد که بر پایه آن فایل‌ها به صورت خودکار جمع‌آوری، نگهداری و به ماژول‌های تحلیلی مانند MultiAV، سندباکس و تحلیل ایستای فایل ارسال می‌شوند و نتایج تحلیل فایل را نیز در خود نگهداری می‌کند.

۴,۲. ماژول Multi-AV

ماژول Multi AV همانگونه که از اسم آن مشخص است وظیفه پویش فایل‌ها توسط آنتی‌ویروس‌های مختلف و ارائه نتایج آنها را برعهده دارد. یکی از سریعترین راه‌ها برای تشخیص بدافزارهای کم‌تشخیص، استفاده از این تکنیک می‌باشد. به کمک این ماژول قدرت تشخیص آنتی‌ویروس‌ها ترکیب می‌شود، به

این ترتیب که نتایج تشخیص همه آنتی‌ویروس‌ها با همدیگر ترکیب شده و دقت تشخیص حاصل تجمیع آنها خواهد بود.

۴,۳. ماژول سندباکس (Sandbox)

ماژول سندباکس سرویس تحلیل پویای فایل را ارائه می‌دهد. این سرویس یکی از بهترین روش‌های خودکار برای تشخیص بدافزارهای کاملا ناشناخته می‌باشد. در این روش تشخیص، فایل به یک محیط ایزوله (سندباکس) منتقل شده و در آنجا اجرا می‌شود. رفتار دقیق فایل زیر ذره‌بین قرار گرفته و انواع عملیات مشکوک یا غیرمشکوک آن لاگبرداری و گزارش می‌شود. نتیجه نهایی به کاربر کمک می‌کند تا تشخیص دهد که فایل اجرایی مخرب بوده است یا خیر، و اینکه محدوده عملیات آن چه بوده است.

۴,۴. ماژول‌های تحلیل ایستای فایل (File Static Analyzers)

ماژول تحلیل ایستای فایل، وظیفه ارائه یک تحلیل ساختاری (ایستا) از فایل‌های مورد بررسی را برعهده دارد. موتورهای این ماژول به تفکیک نوع فایل و سیستم‌عامل هدف تقسیم‌بندی شده و جداگانه قابل انتخاب می‌باشد. (ویندوزی، لینوکسی، اندرویدی) این ماژول موتورهای تحلیل متفاوت و متنوعی را داراست که اطلاعاتی از قبیل اطلاعات امضای دیجیتال، کتابخانه‌های اجرایی مورد استفاده، رشته‌های مهم، پک و رمزشده بودن/نبودن، نوع ماشین اجرایی و... را از فایل استخراج کرده و اطلاعات آن را جهت تحلیل در اختیار کاربر قرار می‌دهد.

تلفن: ۴۳۹۱۲۰۰۰ فکس: ۴۳۹۱۲۸۰۰
ایمیل: info@amnpardaz.com
وب سایت: www.amnpardaz.com