



## مواجهه با تهدیدات پنهان سایبری

امروزه دنیای امنیت سایبری به سمت تهدیداتی رفته است که پنهان‌تر، مخرب‌تر، پیچیده‌تر و پایدارتر هستند. بسیاری از تهدیدات و حملات سایبری ماه‌ها مخفی می‌مانند و تنها زمانی کشف می‌شوند که کار از کار گذشته است. بنابراین برای تشخیص تهدیدات پنهان و پیچیده، نیاز به ابزارهای جدیدی داریم که آنها را در میان میلیون‌ها رخداد سالم کشف کنند.

## کارایی ابزارهای امنیتی در کنار تیم متخصص

هر تیم امنیتی در تلاش جهت شناسایی و توقف حملات در زمان ابتدایی وقوع آنها می‌باشد. اما همیشه جلوگیری از تهدیدات ممکن است به صورت صددرصد موفقیت آمیز نباشد. لازم به ذکر است که حملات بدون فایل و حملات مبتنی بر مرورگرهای وب، بدون وجود هیچ فایل مخربی شروع به اقدامات خود کرده و حملات پیچیده و چندمرحله‌ای را انجام داده که به راحتی توسط ضدبدافزارها قابل شناسایی و جلوگیری نیستند. امروزه ابزارهای امنیتی رایج کارایی لازم را ندارند چرا که:

- ⑤ مهاجمان هم به این ابزارها دسترسی دارند و قبل از حمله، امکان نفوذ را آزمایش و بررسی می‌کنند.
- ⑤ امروزه تهدیدات توسط افراد خیره برنامه‌ریزی و کنترل می‌گردند.
- ⑤ یک ابزار به تنهایی توانایی مقابله با یک گروه خیره را ندارد.
- ⑤ تنها یک تیم متخصص توان تشخیص و مقابله با چنین حملاتی را دارد.

- ⑤ ضد بدافزارها عموماً بدافزارهای عمومی را شناسایی می‌کنند. همان‌گونه که پلیس با جرائم آشکار برخورد کرده و سازمان‌های امنیتی در برابر عملیات نفوذ جاسوسان فعالیت می‌کنند.
- ⑤ بسیاری از هشدارهای امنیتی توسط ضد بدافزارها نادیده گرفته می‌شوند.

پادویش، نسخه کشف و پاسخ به تهدیدات پنهان (Padvish EDR)، یک راه حل امنیتی یکپارچه برای نقطه انتهایی است که ترکیبی از نظارت مداوم، تحلیل و عکس العمل در لحظه است.

امنیت خوب





### پایش

- رصد رفتارهای مخفی و فعالیت های مشکوک
- نمای کلی از هشدارها با کمک داشبوردها و نمایه های گرافیکی

### تحلیل

- تجزیه و تحلیل هشدارها توسط متخصصین
- تشخیص بهتر با کمک موتور هشدار حملات
- کمک به کارشناس جهت شناسایی تهدیدات ناشناخته توسط شکار تهدیدات

### عکس العمل

- پاسخ مناسب به رویدادهای امنیتی در زمان واقعی



Padvish EDR

پادویش، نسخه کشف و پاسخ به تهدیدات پنهان

جهت کسب اطلاعات بیشتر اسکن نمایید.

+۹۸ ۲۱ ۴۳۹۱۲۰۰۰

www.padvish.com

