

مواجهه با تهدیدات پنهان سایبری

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

امنیت
حس خوب



Padvish EDR

پادویش، نسخه کشف و پاسخ به تهدیدات پنهان

کارایی ابزارهای امنیتی در کنار تیم متخصص

هر تیم امنیتی در تلاش جهت شناسایی و توقف حملات در زمان ابتدایی وقوع آنها می باشد. 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:

🕒 مهاجمان هم به این ابزارها دسترسی دارند و قبل از حمله، امکان نفوذ را آزمایش و بررسی می کنند.

🕒 امروزه تهدیدات توسط افراد خبره برنامه ریزی و کنترل می گردند.

🕒 یک ابزار به تنهایی توانایی مقابله با یک گروه خبره را ندارد.

🕒 تنها یک تیم متخصص توان تشخیص و مقابله با چنین حملاتی را دارد.

🕒 ضد بدافزارها عموماً بدافزارهای عمومی را شناسایی می کنند. همان گونه که پلیس با جرائم آشکار برخورد کرده و سازمان های امنیتی در برابر عملیات نفوذ جاسوسان فعالیت می کنند.

🕒 بسیاری از هشدارهای امنیتی توسط ضد بدافزارها نادیده گرفته می شوند.

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.

چرخه عملکرد Padvish EDR



وظایف Padvish EDR

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

جهت کسب اطلاعات بیشتر اسکن نمایید.

+۹۸ ۲۱ ۴۳۹۱۲۰۰۰

www.padvish.com

