



چرخه ی حیات حمله سایبری



مواجهه با تهدیدات و حملات سایبری

با گسترش حملات سایبری و تهدیدات پیشرفته پایدار به کشور، لزوم مقابله با این نوع حملات در سطح بالا بیش از پیش احساس می شود. طبیعتاً مقابله با این حملات که به صورت ترکیبی از فناوری پیشرفته و هدایت انسانی انجام می گیرند، از طریق به کارگیری یک محصول یا خدمت به تنهایی قابل انجام نمی باشد و نیازمند راهکاری است که علاوه بر به کارگیری فناوری های پیشرفته، از نیروی انسانی متخصص و باتجربه جهت مقابله با این نوع تهدیدات برخوردار باشد.

اهداف Padvish MDR

- شناسایی و مقابله با حملات هدفمند
- تشخیص و جلوگیری از نفوذ به شبکه سازمانها
- جلوگیری از نشت یا تخریب اطلاعات سازمان
- کشف تهدیدات پیشرفته پایدار در مراحل اولیه و پیش از وقوع حمله روزافزون
- تشخیص و مقابله با تهدیدات روزافزون

پادویش، نسخه کشف و پاسخ به حملات سایبری (Padvish MDR) به صورت یک راهکار امن متمرکز است، که بر پایه اطلاعات دقیق و عمیق جمع آوری شده توسط محصولات پادویش از سیستم های شبکه، و با تگ گذاری، جمعیت، تولید هشدار و داده نمایی آنها مطابق تجربیات و دانش کسب شده از حملات قبلی سایبری، نفوذ را کشف نموده و از ادامه فعالیت نفوذگر در شبکه جلوگیری می کند.



مولفه های زیرساخت Padvish MDR

- 1 تجهیزات سازمان
(Organization's Devices)
- 2 سرور مدیریتی پادویش
(Padvish Management Server - PMS)
- 3 شبکه ابری پادویش
(Padvish Cloud Network)
- 4 سامانه مرکزی کشف و مقابله با حملات
(Padvish MDR)
- 5 تیم متخصصین خبره حملات سایبری پادویش
(Padvish Threat Experts)

سنسورهای تشخیص انواع حملات

- تغییرات نرم افزاری
- تشخیص ابزارهای هک و نفوذ
- حملات بدون فایل
- حملات مبتنی بر RDP
- تشخیص برنامه های ناخواسته و Risktools
- تشخیص های حملات شبکه (IPS)
- تشخیص رفتارهای مشکوک (رمز عبور نادرست، دور زدن ضد بدافزار و ...)

حس خوب امنیت



Padvish MDR

پادویش، نسخه کشف و پاسخ به حملات سایبری

جهت کسب اطلاعات بیشتر اسکن نمایید.

+۹۸ ۲۱ ۴۳۹۱۲۰۰۰

www.padvish.com

