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 می‌شود.
طبیعتا مقابله با این حملات که به صورت ترکیبی از فناوری پیشرفته و هدایت انسانی انجام می‌گیرند، از طریق به‌کارگیری یک محصول یا خدمت به تنهایی قابل انجام نمی‌باشد و نیازمند راهکاری است که علاوه بر به‌کارگیری فناوری‌های پیشرفته، از نیروی انسانی متخصص و باتجربه جهت مقابله با این نوع تهدیدات برخوردار باشد.

چرخه‌ی حیات حمله سایبری

1. شناخت
2. نفوذ اولیه
3. تثبیت
4. انتشار
5. ضربه نهایی

پادویش، نسخه کشف و پاسخ به حملات سایبری (Padvish MDR) به صورت یک راهکار امن متمرکز است، که بر پایه اطلاعات دقیق و عمیق جمع‌آوری شده توسط محصولات پادویش از سیستم‌های شبکه، و با تگ‌گذاری، تجمیع، تولید هشدار و داده‌نمایی آنها مطابق تجربیات و دانش کسب شده از حملات قبلی سایبری، نفوذ را کشف نموده و از ادامه فعالیت نفوذگر در شبکه جلوگیری می‌کند.

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
- تشخیص و مقابله با تهدیدات روزافزون

شرکت نرم افزاری امن پرداز
Amnpardaz Software Corporation

Padvish MDR

پادویش، نسخه کشف و پاسخ به حملات سایبری

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 ...)

مولفه‌های 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)

حس خوب امنیت

جهت کسب اطلاعات بیشتر اسکن نمایید.

+۹۸ ۲۱ ۴۳۹۱۲۰۰۰

www.padvish.com