مرکز کشف و پاسخ به حملات سایبری

(پادویش MDR)

شرکت نرم افزاری امن پرداز

سطح محرمانگی: عادی

نسخه ۱.۷

بهار ۱۴۰۵

فهرست مطالب

فهرست مطالب

فهرست جدول‌ها

فهرست تصاویر

۱. مقدمه

مرکز کشف و پاسخ به حملات سایبری (Padvish MDR) با هدف تشخیص و مقابله با تهدیدات روزافزون و حملات سایبری مانند وقایع هک و نفوذ، آلودگی به تهدیدات پیشرفته پایدار[۱] و حملات هدفمند[۲] در سطح سازمان‌های کشور راه‌اندازی شده است.

با گسترش حملات سایبری و تهدیدات پیشرفته پایدار به کشور، لزوم مقابله با این نوع حملات در سطح بالا احساس می‌شود. طبیعتا مقابله با این حملات که به صورت ترکیبی از فناوری پیشرفته + هدایت انسانی انجام می‌گیرند از طریق ارائه صرف یک محصول یا خدمت قابل انجام نمی‌باشد و نیازمند راهکاریست که در بعد فنی از فناوری‌های پیشرفته و در بعد انسانی از تخصص و تجربه کافی جهت مقابله برخوردار باشد.

هر حمله سایبری دارای مراحلی است که از شناخت و نفوذ اولیه آغاز و تا تثبیت، انتشار و ضربه نهایی تقسیم‌بندی می‌شود. حملات هدفمند ممکن است از چند ساعت تا چندین سال طول بکشند و از این لحاظ پاسخگویی به آنها باید در اسرع وقت و قبل از آنکه نفوذگر بتواند در شبکه به اقدام و ضربه نهایی مدنظر خود برسد انجام بگیرد. مرکز کشف و پاسخ به حملات سایبری، 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.

مرکز کشف و پاسخ به حملات سایبری (Padvish MDR) به صورت یک راهکار امن متمرکز به همین منظور ارائه شده است. در این سند به معرفی این مرکز، نحوه عملکرد و خدمات ارائه شده توسط آن پرداخته می‌شود.

---

[۱] Advanced Persistent Threat - APT

[۲] Targeted Attack

۲. معرفی مرکز کشف و پاسخ به حملات سایبری (Padvish MDR)

۲/۱. هدف

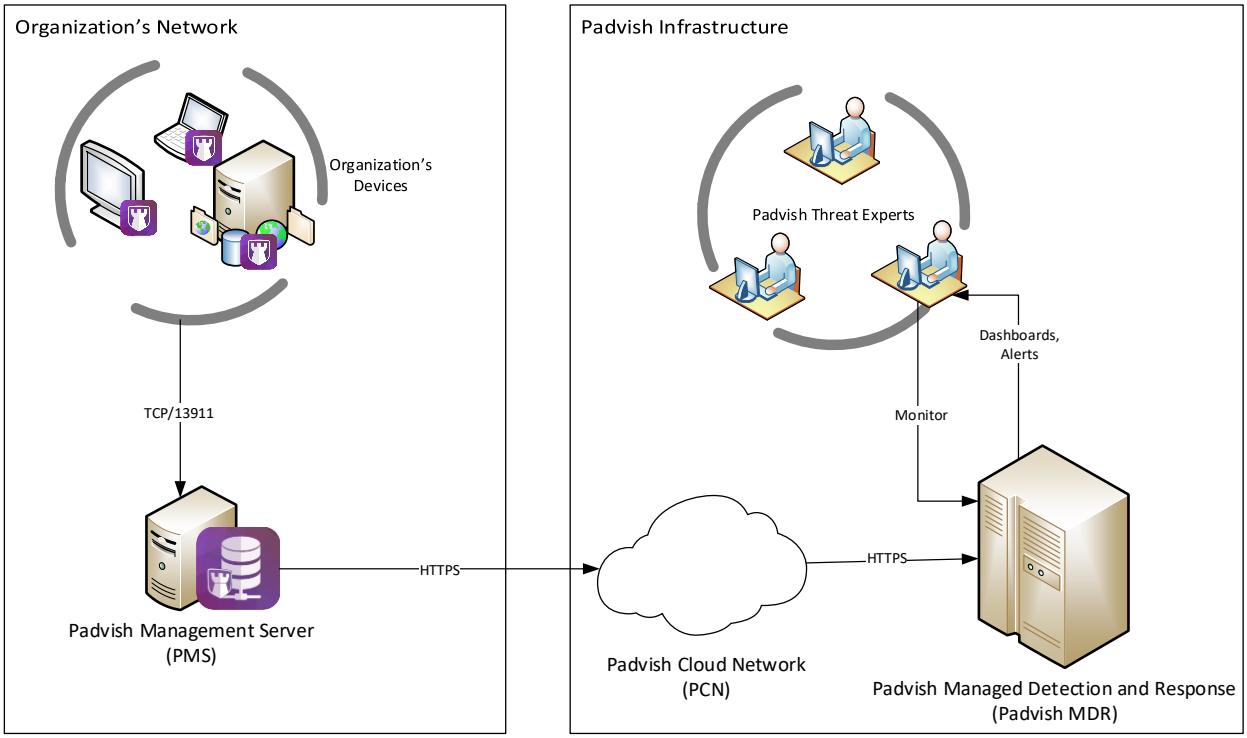
هدف این مرکز تشخیص نفوذ به شبکه سازمان‌ها و کشف تهدیدات پیشرفته در مراحل اولیه و پیش از وقوع یک حمله سایبری و تبعات ناخوشایند آن (مانند نشت یا تخریب اطلاعات) می‌باشد.

۲/۲. زیرساخت فنی

مرکز کشف و پاسخ به حملات سایبری (Padvish MDR) دارای دو معماری متفاوت ابری و اختصاصی می‌باشد.

۲/۲/۱. معماری ابری (MDR Optimum)

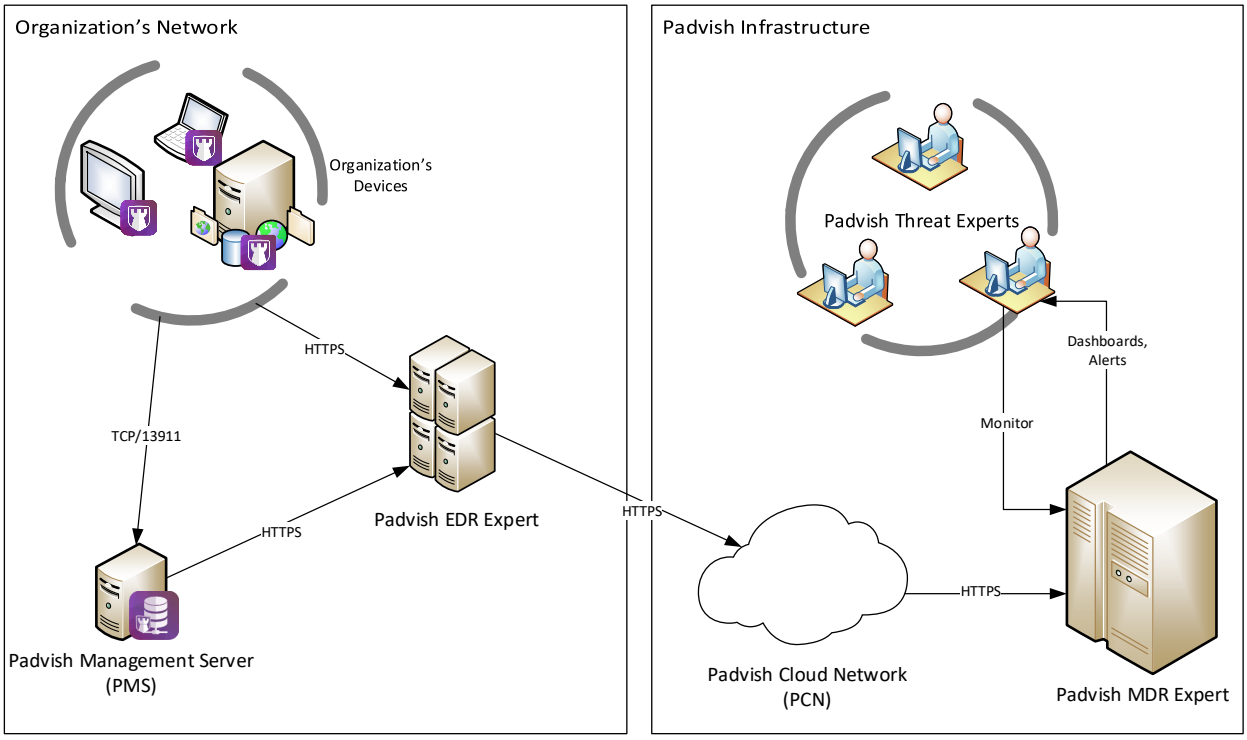
در معماری ابری، تمامی مولفه‌های سرویس مانند ذخیره و پردازش لاگ‌ها توسط سرویس ابری شرکت امن‌پرداز فراهم می‌گردد و در سمت شبکه مشتریان نیازی به راه‌اندازی سرور جداگانه (به غیر از سرور مدیریت مرکزی پادویش Padvish Management Server) نمی‌باشد. این معماری در مورد سطح سرویس رایگان و MDR Optimum کاربرد دارد.



تصویر ۱ - زیرساخت معماری ابری مرکز کشف و پاسخ به حملات سایبری (Padvish MDR)

۲/۲/۲. معماری اختصاصی (MDR Base/Select/Expert)

در خصوص سطح سرویس MDR Base تا MDR Expert، با توجه به عمق نفوذ بالاتر سنسورها و حجم بالاتر لاگ‌های جمع‌آوری و پردازش شده، لازم است که نسخه متناظر EDR پادویش در سازمان مستقر گردد و با یک مکانیزم مناسب (مانند VPN، لینک ارتباطی اختصاصی و ...) دسترسی از راه دور به این سرورها جهت ارائه سرویس‌های MDR فراهم گردد.



تصویر ۲ - زیرساخت معماری اختصاصی مرکز کشف و پاسخ به حملات سایبری (Padvish MDR)

۲/۲/۳. مولفه‌های زیرساخت فنی

زیرساخت فوق شامل مولفه‌های زیر می‌باشد:

۱. **تجهیزات سازمان (Organization's Devices)**: شامل همه تجهیزاتی می‌شود که بر روی آنها پادویش نصب بوده و از آنها محافظت می‌کند.

۲. **سرور مدیریتی پادویش (Padvish Management Server – PMS)**: سرور مدیریتی پادویش جزئی از راهکار سازمانی پادویش بوده و به مدیر شبکه امکان می‌دهد که از یک محل مرکزی

سیستم‌های شبکه خود را کشف نموده، پادویش را بر روی آنها نصب کرده و تنظیمات و تسک‌های مورد نظر خود را بر روی آنها اعمال نماید.

۳. **مجموعه سرور EDR پادویش (Padvish EDR Expert)**: این مجموعه سرور وظیفه جمع‌آوری اطلاعات و فایل‌ها از تجهیزات سازمان و نیز سرور مدیریتی پادویش، نگهداری و پردازش این اطلاعات، و نیز ارائه کنسول EDR را در داخل سازمان برعهده دارد. (این مولفه فقط در معماری اختصاصی MDR Base به بالا وجود دارد)

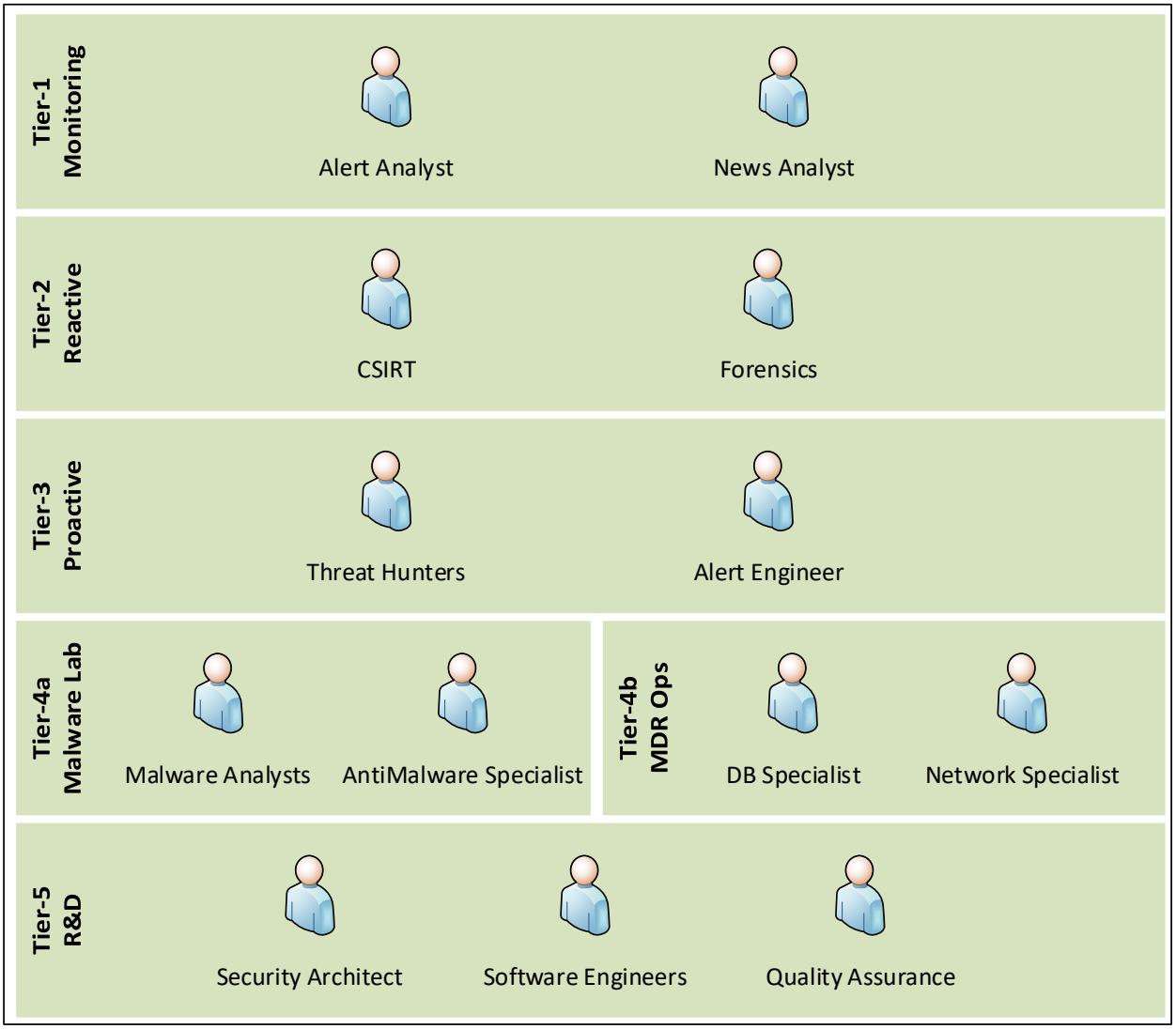
۴. **شبکه ابری پادویش (Padvish Cloud Network)**: بستر شبکه ابری پادویش با متصل نمودن کلاینت‌ها به شبکه اختصاصی اطلاعات تهدیدات پادویش، موجب افزایش قدرت و سرعت تشخیص بدافزارهای جدید می‌گردد.

۵. **سامانه مرکزی کشف و مقابله با تهدیدات**: سامانه اصلی مرکز کشف و پاسخ به حملات سایبری (Padvish MDR) که داشبوردها و هشدارهای نظارتی خودکار را فراهم می‌نماید.

۶. **تیم متخصصین خبره تهدیدات سایبری پادویش (Padvish Threat Experts)**: تیمی از متخصصین آموزش‌دیده پادویش که با اتکا به تجربیات اختصاصی پادویش در مقابله با تهدیدات سایبری واقعی در طول سالیان گذشته ایجاد شده است و به صورت شبانه‌روزی (۲۴×۷) وضعیت سایبری شبکه مشتریان را رصد می‌نماید.

۲/۳. لایه‌بندی تیم‌های فنی

تیم‌های فنی مرکز کشف و مقابله با حملات سایبری (Padvish MDR) برحسب نوع عملکرد به پنج لایه تقسیم می‌شوند:



تصویر ۳ - لایه‌بندی تیم‌های مرکز کشف و پاسخ به حملات سایبری (Padvish MDR)

۱. **لایه یک (مانیتورینگ)**: این لایه وظیفه نظارت ۲۴×۷ بر هشدارها و رخدادهای سامانه را برعهده دارد. علاوه بر آن نظارت بر اخبار سایبری و پیگیری هشدارهای تهدیدات شناخته شده ملی و جهانی نیز به عهده این لایه قرار دارد.

۲. **لایه واکنش به رخداد (Re-active)**: این لایه دارای دو نقش پاسخ به حوادث رایانه‌ای (CSIRT یا CERT) و فارنزیک سایبری می‌باشد که در واکنش به هشدارهای اعلام شده از سوی لایه یک وارد عمل می‌شوند.

۳. **لایه جستجوی فعال (Pro-active)**: این لایه وظیفه جستجوی فعال به دنبال تهدیدات پنهان را برعهده دارد. به علاوه پس از انجام بررسی‌های فعال، این موارد را به صورت هشدارهای امنیتی سیستمی پیاده‌سازی می‌کند تا پس از این توسط لایه یک قابل نظارت باشد.

۴. **لایه چهار (پشتیبان عملیات)**: این لایه شامل دو بخش است:

a. **چهار الف – آزمایشگاه بدافزار**: که وظیفه شناخت دقیق بدافزار و افزودن راهکارهای تشخیص و مقابله با آن به صورت فنی و تخصصی را برعهده دارد.

b. **چهار ب – راهبری سامانه**: که سامانه MDR را جهت عملکرد بهینه و بدون خطا مدیریت می‌کنند.

۵. **لایه پنج تحقیق و توسعه (R&D)**: که وظیفه بررسی عملکرد کلی سامانه و تیم‌های مرکز، تحقیق و یافتن راه‌های جدید، و بهبود و توسعه معماری، فرایندها و سامانه‌ها را برعهده دارد.

۳. سطوح نظارت و خدمات

۳/۱. سطوح هشدارهای امنیتی

در مرکز کشف و پاسخ به حملات سایبری (Padvish MDR) هشدارهای امنیتی از نظر درجه خطر و اهمیت به سطوح مختلفی تقسیم‌بندی می‌شوند که با رنگ هشدار مشخص می‌شود:

۱. **هشدار سیاه (بررسی فوری)**: خطر فوری و قطعی هک و نفوذ

۲. **هشدار قرمز (تماس فوری)**: احتمال جدی هک و نفوذ که باید فورا بررسی شود

۳. **هشدار نارنجی (غیرفوری)**: موارد حائز اهمیت بدون فوریت

۴. **هشدار زرد (غیرقطعی):** موارد با احتمال هشدار کاذب که به ادمین ارجاع نمی‌شوند.

هر سطح هشدار با توجه به درجه اهمیت و فوریت خود، از یک SLA جداگانه برخوردار می‌باشد.

جدول ۱ – سطوح هشدارهای امنیتی مرکز کشف و پاسخ به حملات سایبری Padvish MDR

سطح هشدار	زرد (غیرقطعی)	نارنجی (غیرفوری)	قرمز (تماس فوری)	سیاه (بررسی فوری)
شرح	**احتمال هشدار کاذب** هشدار توسط تیم انسانی مرکز MDR سطح‌بندی می‌شود	**بررسی فوریت ندارد** آلودگی بدافزاری غیر هک، یا بقایای یک هک قدیمی	**نیازمند کسب اطلاع فوری** رفتار مشکوک مشاهده شده است که احتمال دارد توسط ادمین انجام شده باشد	**خطر فوری هک** خطر هک جدی و نزدیک به قطعی است و باید فورا بررسی شود
اعلام هشدار از طریق تماس	✗	✔	✔	✔
زمان تماس	–	ساعات کاری (۷ صبح تا ۷ شب)	۲۴×۷	۲۴×۷
الزام بررسی	–	با نظر ادمین	در صورت عدم اطلاع ادمین	الزامی
مهلت آغاز بررسی	–	۱ هفته	۱ روز	۱ ساعت
اعلام کتبی هشدار	–	✗	✔	✔

۳/۲. سطوح نظارتی (عمق سنسورها)

بسته به سطح خدمات انتخاب شده (Optimum تا Expert) عمق سنسورهای نظارتی مرکز کشف و پاسخ به حملات سایبری (Padvish MDR) نیز متفاوت است.

جدول ۲ - عمق سنسورها در مرکز کشف و پاسخ به حملات سایبری (Padvish MDR)

رج	سنسورها	MDR Optimum	MDR Base/Select	MDR Expert
۱.	تشخیص ابزارهای هک و نفوذ	✓	✓	✓
۲.	تشخیص تهدیدات بدافزاری	✓	✓	✓
۳.	تشخیص‌های مبتنی بر محافظت رفتاری	✓	✓	✓
۴.	تشخیص آلودگی سیستم‌ها از طریق ریموت دسکتاپ	✓	✓	✓
۵.	تشخیص آلودگی از طریق پوشه اشتراکی	✓	✓	✓
۶.	تشخیص نرم‌افزارهای مشکوک و ناخواسته	✓	✓	✓
۷.	تشخیص حملات و اکسپلویت‌های شبکه‌ای	✓	✓	✓
۸.	اطلاعات نرم‌افزارهای نصب شده	✓	✓	✓
۹.	عملیات مشکوک مانند تلاش برای حذف ضدبدافزار، ورود پسورد اشتباه و ...	✓	✓	✓
۱۰.	پایش هفتگی سنسورهای ایمنی و تطبیقی (خاموش بودن محافظت، آپدیت نبودن ضدبدافزار، قطعی و عدم اتصال شبکه و ...)	–	✓	✓
۱۱.	لاگبرداری نرم‌افزارهای خوداجرا و تغییرات آنها (درایورها، سرویس‌ها، تسک‌ها، اسکریپت‌های روشن/خاموش شدن و ...)	–	✓	✓
۱۲.	لاگبرداری تمامی اتصالات شبکه‌ای (جهت فارنزیک)	–	✓	✓
۱۳.	لاگبرداری تمامی پردازه‌های اجرایی و ماژول‌های آنها (جهت فارنزیک)	–	✓	✓
۱۴.	لاگبرداری تغییرات نرم‌افزاری و سخت‌افزاری	–	✓	✓
۱۵.	پویش فایل‌های اجرایی با MultiAV	–	*	✓
۱۶.	امکان ارسال فایل‌های اجرایی به سندباکس	–	*	✓

رج	سنسورها	MDR Optimum	MDR Base/Select	MDR Expert
۱۷.	پویش فایل‌های اجرایی با موتورهای تحلیل ساختاری (ایستا)	–	*	✓

* این موارد بسته به انتخاب ماژول مربوطه در MDR Select ارائه می‌شوند.

۳٫۳. سطوح خدمات

خدمات Padvish MDR شامل دو سطح زیر می‌گردد که توسط بهره‌بردار در زمان خرید قابل انتخاب می‌باشد و با لایسنس از یکدیگر تفکیک می‌شوند:

- **سطح بهینه**: در این سند مقصود از «سطح بهینه» مجوز Padvish MDR Optimum می‌باشد و شامل خدمات پایه‌ای Padvish MDR به صورت ابری است. در این سطح، احتیاجی به نصب *مولفه‌های Padvish EDR* در شبکه نبوده و از همان *سرور مدیریت مرکزی پادویش* جهت جمع‌آوری و ارسال اطلاعات به *سامانه مرکزی Padvish MDR* استفاده می‌شود. این سطح عمق سنسور کمتری داشته و فاقد کنسول وب در اختیار *بهره‌بردار* است.
- **سطح پیشرفته**: در این سند مقصود از «سطح پیشرفته» مجوز Padvish MDR Base/Select/Expert می‌باشد و شامل خدمات پیشرفته Padvish MDR است که بر روی محصول Padvish EDR بنا می‌شود و لذا دارای کنسول و رابط کاملی در سمت بهره‌بردار و عمق سنسور کاملی نیز دارد.

جدول ۳ – مقایسه سطوح خدمات مرکز کشف و پاسخ به حملات سایبری (Padvish MDR)

رج	قابلیت	سطح بهینه	سطح پیشرفته
۱.	نظارت ۷ در ۲۴	✓	✓
۲.	تیم متخصص با تجربه بررسی حملات سایبری اخیر کشور	✓	✓
۳.	عمق سنسورهای پیشرفته	متوسط	عمیق
۴.	اعلام هشدارهای امنیتی	✓	✓
۵.	اعلام هشدار از طریق پیامک/تماس	✓	✓
۶.	اعلام هشدارهای مهم به صورت کتبی	✓	✓
۷.	شکار تهدیدات فعال	✓	✓

رج	قابلیت	سطح بهینه	سطح پیشرفته
۸.	سطح سرویس تضمین شده	✓	✓
۹.	نگهداری هشدارها تا یکسال	✓	✓
۱۰.	گزارش دوره‌ای وضعیت شبکه	✓	✓
۱۱.	عملیات فارنزیک تا سقف ساعت مشخص	✓	✓
۱۲.	ارزیابی وضعیت امنیتی شبکه	–	✓
۱۳.	اعلام نقاط ضعف و قابل بهبود شبکه	–	✓
۱۴.	نگهداری لاگ‌های خام به مدت تعیین شده توسط سیاست سازمان	–	✓
۱۵.	دسترسی به سامانه وب Padvish EDR	–	✓

۴. راه‌اندازی

۴/۱. نیازمندی‌های فنی

چک لیست زیر نشان می‌دهد که پیش از راه‌اندازی، چه نیازمندی‌های فنی برای استفاده از خدمات مرکز کشف و پاسخ به حملات سایبری (Padvish MDR)، باید فراهم گردند:

جدول ۴ – نیازمندی‌های فنی بهره‌برداری از خدمات مرکز کشف و پاسخ به حملات سایبری (Padvish MDR)

رج	نیازمندی	MDR Optimum	MDR Base/Select	MDR Expert
۱.	استقرار آخرین نسخه ایجنت و کنسول پادویش	✓	✓	✓
۲.	اتصال به سامانه مرکزی کشف و مقابله با تهدیدات (از طریق اینترنت، VPN، یا لینک اختصاصی)	✓	✓	✓
۳.	مشخص نمودن رابط از سمت کارفرما جهت هماهنگی‌های لازم در زمان کشف حادثه سایبری	✓	✓	✓
۴.	استقرار سرور مرکزی Padvish EDR	–	✓	✓
۵.	استقرار ماژول‌های مرتبط Padvish EDR (سندباکس، تحلیل ایستا، MultiAV)	–	❋	✓
۶.	امکان دسترسی راه دور به سامانه Padvish EDR	–	✓	✓

رج	نیازمندی	MDR Optimum	MDR Base/Select	MDR Expert
۷.	حجم تقریبی پهنای باند موردنیاز با مرکز MDR (به ازای هر ۱۰۰۰ کلاینت)**	80kbps	100kbps	100kbps

* بسته به ماژول‌های انتخابی در MDR Select متفاوت می‌باشد.

** مقادیر ذکر شده تقریبی بوده و بسته به وضعیت آلودگی و حجم رویداد در شبکه متفاوت است.

۴/۲. گام‌های بهره‌برداری

در جدول زیر گام‌های بهره‌برداری از خدمات مرکز کشف و پاسخ به حملات سایبری (Padvish MDR) به تفصیل تشریح شده‌اند.

جدول ۵ - گام‌های بهره‌برداری از خدمات مرکز کشف و پاسخ به حملات سایبری (Padvish MDR)

رج	عملیات پیاده سازی	مجری	توضیحات
۱.	بروز رسانی نسخه کنسول‌های مدیریتی پادویش	پیمانکار	برای جلوگیری از هرگونه اختلال احتمالی عملیات بصورت پلکانی توسط پشتیبان مقیم اجرا می شود
۲.	بروز رسانی نسخه کلاینت‌های آنتی ویروس پادویش	پیمانکار	برای جلوگیری از هرگونه اختلال احتمالی عملیات بصورت پلکانی توسط پشتیبان مقیم اجرا می شود
۳.	دسترسی سرور های مدیریت متمرکز پادویش به سامانه MDR	کارفرما	تمامی سرورهای مدیریتی پادویش باید به آدرس cloudpms.padvish.com روی پورت TCP/443 به صورت Outgoing دسترسی داشته باشند. (این دسترسی می‌تواند بر بستری غیر از اینترنت نیز فراهم شود)
٤.	تطبیق لیست سرورها و تایید برقراری اتصال با سامانه MDR	پیمانکار	توسط پشتیبان مقیم هماهنگ با تیم‌های مستقر در شرکت امن‌پرداز
۵.	معرفی نماینده‌ای از طرف پیمانکار	پیمانکار	جهت ارتباط مستقیم با نماینده کارفرما و مسئول تهیه گزارش رخدادها
٦.	معرفی نمایندگان کارفرما	کارفرما	لازم است نماینده/نمایندگان معرفی شده به صورت ۲۴×۷ در دسترس بوده و با تمامی راهبران اصلی شبکه‌های زیرمجموعه کارفرما در ارتباط باشد.

			همچنین در زمان حادثه، اختیارات لازم را جهت هماهنگی و برقراری دسترسی‌های مورد نیاز تیم‌های پاسخ به رخداد سایبری پیمانکار به زیرمجموعه‌های کارفرما داشته باشد.
۷.	تهیه فهرست شماره تلفن‌های همراه کارشناسان شبکه زیرمجموعه‌های کارفرما	کارفرما	با توجه به حساسیت این سامانه و لزوم عملکرد ۲۴×۷ آن، فهرست گردآوری شده و در اختیار نمایندگان کارفرما و پیمانکار قرار گیرد. طبیعتا این لیست باید در طول دوره بهره‌برداری از سامانه به روز گردد
۸.	برقراری ارتباط امن VPN	پیمانکار /کارفرما	به جهت پایش سیستم‌ها این امکان می‌تواند دائمی نبوده و در ساعات مشخص فعال گردد.
۹.	معرفی ایمیل‌های مسئولان مرتبط	کارفرما	به جهت ارسال گزارش‌های سامانه و درخواست‌های مربوطه
۱۰.	آغاز بهره‌برداری از خدمات سامانه MDR	پیمانکار	