شرکت نرم‌افزاری امن‌پرداز

خدمات مرکز کشف نفوذ و مقابله با تهدیدات پیشرفته

پادویش

عادی

فهرست مطالب

۱. مقدمه ۴

۲. معرفی مرکز کشف و پاسخ به تهدیدات سایبری (Padvish MDR) ۵

۲,۱. هدف ۵

۲,۲. گستره حیطه تحت نظارت ۵

۲,۳. زیرساخت فنی ۵

۲,۳,۱. معماری ابری (MDR Optimum) ۶

۲,۳,۲. معماری اختصاصی (MDR Expert) ۷

۲,۳,۳. مولفه‌های زیرساخت فنی ۷

۲,۴. مشخصات و قابلیت‌های فنی ۸

۲,۵. لایه‌بندی تیم‌های فنی ۱۰

۳. سطوح نظارت و خدمات ۱۲

۳,۱. سطوح هشدارهای امنیتی ۱۲

۳,۲. سطوح نظارتی (عمق سنسورها) ۱۳

۳,۳. سطوح خدمات ۱۴

فهرست جدول‌ها

جدول ۱ – سطوح هشدارهای امنیتی مرکز کشف و پاسخ به تهدیدات سایبری Padvish MDR.....۱۲

جدول ۲ – عمق سنسورها در مرکز کشف و پاسخ به تهدیدات سایبری (Padvish MDR).....۱۳

جدول ۳ – مقایسه سطوح خدمات مرکز کشف و پاسخ به تهدیدات سایبری (Padvish MDR).....۱۴

فهرست تصاویر

تصویر ۱ – معماری مرکز کشف و پاسخ به تهدیدات سایبری (Padvish MDR).....۶

۱. مقدمه

مرکز کشف و پاسخ به تهدیدات 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 تهدیدات 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 تهدیدات 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 تهدیدات 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. گستره حیطه تحت نظارت

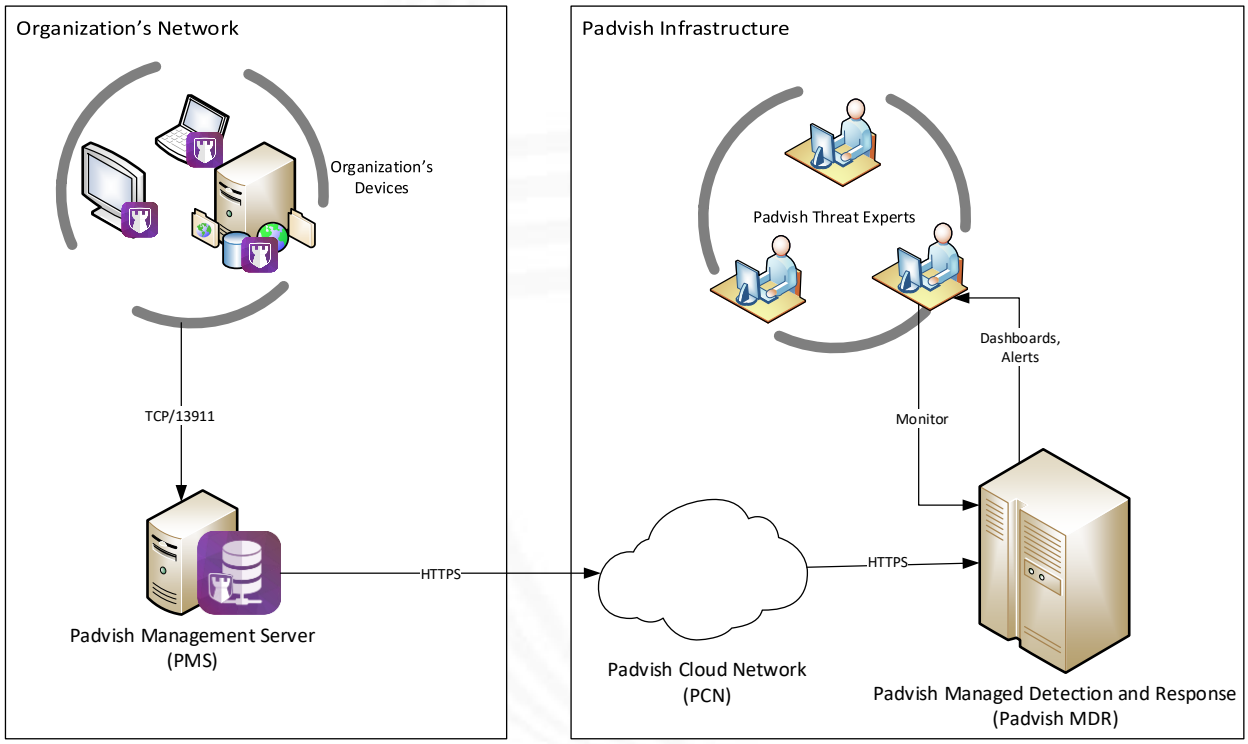
حیطه تحت نظارت این مرکز شامل تمامی کلاینت‌های سازمانی پادویش می‌شود که متصل به کنسول سازمانی پادویش بوده و دسترسی به شبکه ابری پادویش داشته باشند.

۲,۳. زیرساخت فنی

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

۲,۳,۱. معماری ابری (MDR Optimum)

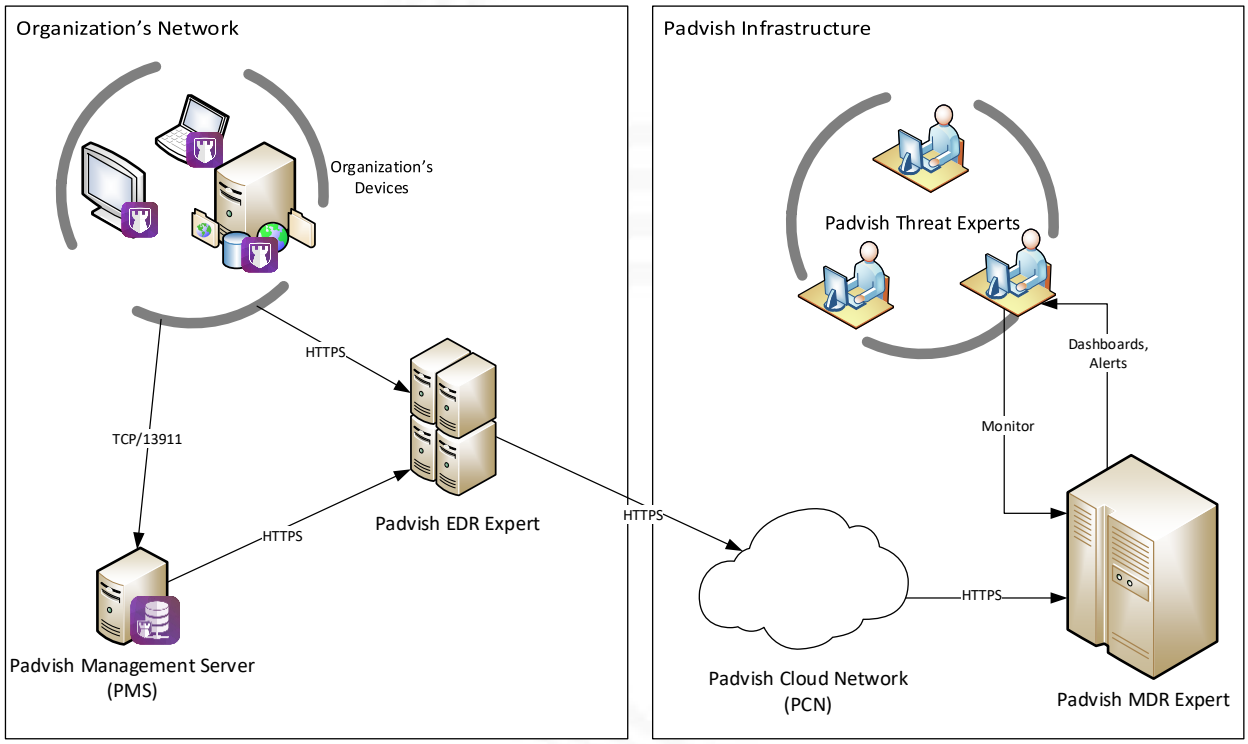
در معماری ابری، تمامی مولفه‌های سرویس مانند ذخیره و پردازش لاگ‌ها توسط سرویس ابری شرکت امن‌پرداز فراهم می‌گردد و در سمت نیازی به راه‌اندازی سرور جداگانه (به غیر از سرور مدیریت مرکزی پادویش Padvish Management Server) نمی‌باشد. این معماری در مورد سطح سرویس رایگان و MDR Optimum کاربرد دارد.



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

۲,۳,۲. معماری اختصاصی (MDR Expert)

در خصوص سطح سرویس MDR Expert، با توجه به عمق نفوذ بالاتر سنسورها و حجم بالاتر لاگ‌های جمع‌آوری و پردازش شده، لازم است که نسخه EDR Expert پادویش در سازمان مستقر گردد که نیازمند سرورهای مجزا می‌باشد.



تصویر ۲ – زیرساخت معماری اختصاصی مرکز کشف و پاسخ به تهدیدات سایبری (**Padvish MDR**)

۲,۳,۳. 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 Expert 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 تهدیدات 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.

۲,۴. مشخصات و قابلیت‌های فنی

۱) اتصال و تجمیع رخدادهای کلیه کنسول‌های مدیریتی نسخه‌های سازمانی پادویش در کشور

۲) تگ‌گذاری اطلاعات دریافتی بر حسب سازمان، سرور و موقعیت جغرافیایی

۳) تولید هشدارهای امنیتی هک و نفوذ

٤) داده‌نمایی و مشاهده وضعیت امنیت سایبری سازمان‌ها در یک نگاه

۵) قابلیت عمیق شدن در داده‌ها (Drill Down)

٦) تیم رصد خبره و متخصص با تجربه بررسی حملات سایبری اخیر در کشور

۷) انواع سنسورهای زیر:

a) تشخیص‌های ابزارهای هک و نفوذ

b) تشخیص‌های تهدیدات بدافزاری

c) تشخیص‌های مبتنی بر محافظت رفتاری

d) تشخیص آلودگی سیستم‌ها از طریق ریموت دسکتاپ

e) تشخیص آلودگی از طریق پوشه اشتراکی

f) تشخیص نرم‌افزارهای مشکوک و ناخواسته

g) تشخیص حملات و اکسپلویت‌های شبکه‌ای

h) اطلاعات نرم‌افزارهای نصب شده، نسخ آنها و توزیع نصب

i) عملیات مشکوک مانند تلاش برای حذف ضدبدافزار، ورود پسورد اشتباه و ...

j) سنسورهای ایمنی و تطبیقی (خاموش بودن محافظت، نصب نبودن یا آپدیت نبودن ضدبدافزار، قطعی و عدم اتصال شبکه و ...)

k) و ...

۲,۵. لایه‌بندی تیم‌های فنی

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

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.

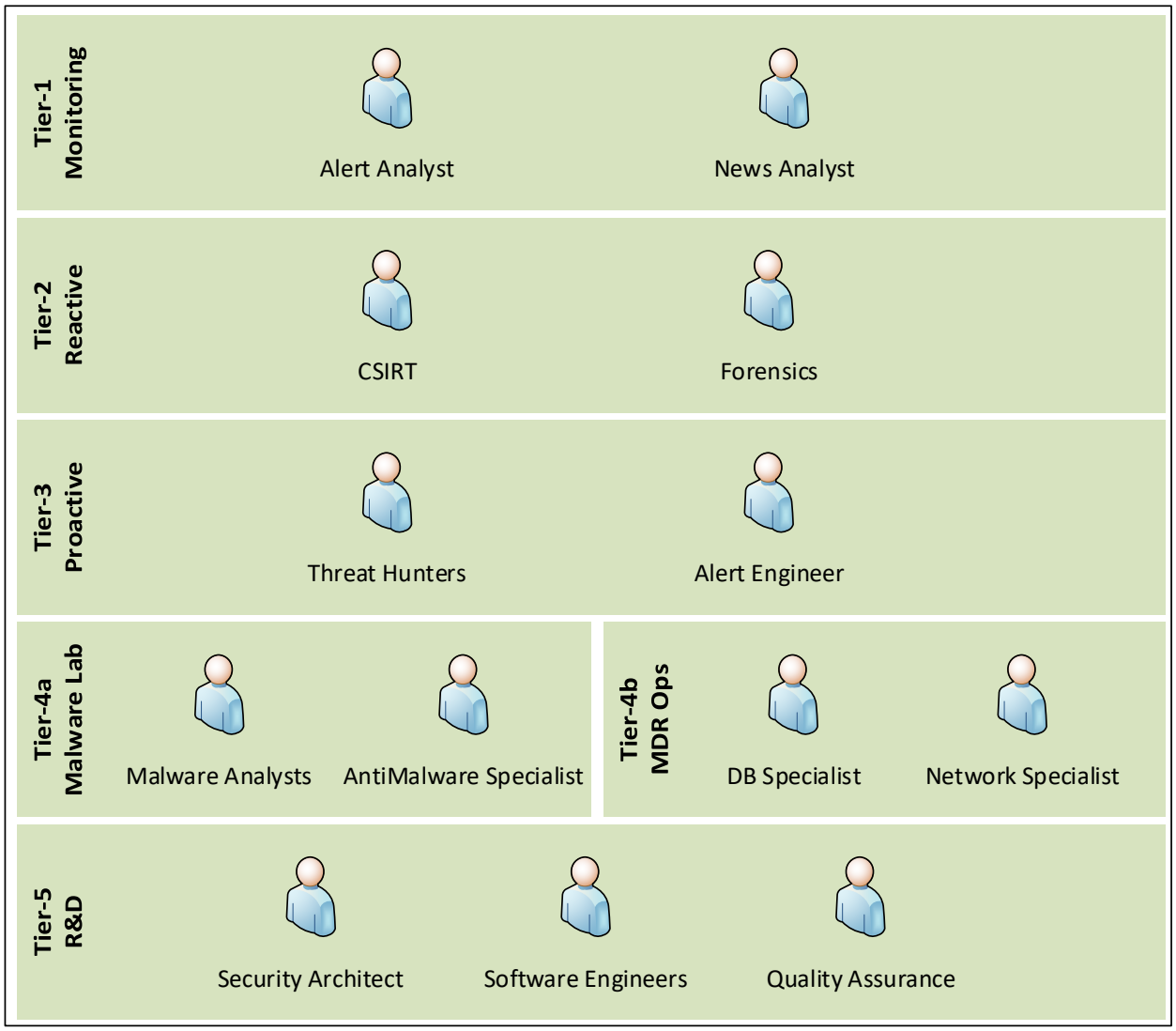
۳. **لایه جستجوی فعال (Pro-active):** این لایه وظیفه جستجوی فعال به دنبال تهدیدات پنهان را برعهده دارد. به علاوه پس از انجام بررسی‌های فعال، این موارد را به صورت هشدارهای امنیتی سیستمی پیاده‌سازی می‌کند تا پس از این توسط لایه یک قابل نظارت باشد.

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.



تصویر ۳ – لایه‌بندی تیم‌های مرکز کشف و پاسخ به تهدیدات سایبری (**Padvish MDR**)

۳. سطوح نظارت و خدمات

۳,۱. سطوح هشدارهای امنیتی

در مرکز کشف و پاسخ به تهدیدات 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

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 تهدیدات سایبری Padvish MDR

سطح هشدار	زرد (غیرقطعی)	نارنجی (غیرفوری)	قرمز (تماس فوری)	سیاه (بررسی فوری)
شرح	**احتمال هشدار کاذب** هشدار باید توسط تیم انسانی سطح‌بندی شود	**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 (رایگان، Optimum یا Expert) عمق سنسورهای نظارتی مرکز کشف و پاسخ به تهدیدات سایبری (Padvish MDR) نیز متفاوت است.

جدول ۲ – عمق سنسورها در مرکز کشف و پاسخ به تهدیدات سایبری (Padvish MDR)

رج	سنسورها	سطح رایگان	MDR Optimum	MDR Expert
۱.	تشخیص‌های ابزارهای هک و نفوذ	✓	✓	✓
۲.	تشخیص‌های 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.	سنسورهای ایمنی و تطبیقی (خاموش بودن محافظت، آپدیت نبودن ضدبدافزار، قطعی و عدم اتصال شبکه و ...)	–	✓	✓

رج	سنسورها	سطح رایگان	MDR Optimum	MDR Expert
۱۱.	لاگبرداری نرم‌افزارهای خوداجرا و تغییرات آنها (درایورها، سرویس‌ها، تسک‌ها، اسکریپت‌های روشن/خاموش شدن و ...)	–	–	✓
۱۲.	لاگبرداری تمامی اتصالات شبکه‌ای (فارنزیک)	–	–	✓
۱۳.	لاگبرداری تمامی پردازه‌های اجرایی و ماژول‌های آنها (فارنزیک)	–	–	✓
۱۴.	لاگبرداری تغییرات نرم‌افزار و سخت‌افزاری	–	–	✓
۱۵.	پویش فایل‌های اجرایی با MultiAV	–	–	✓

۳,۳. سطوح خدمات

جدول زیر مقایسه‌ای از سطح خدمات انتخاب شده (رایگان، Optimum یا Expert) را ارائه می‌دهد:

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

رج	قابلیت	سطح رایگان*	MDR Optimum	MDR Expert
۱۶.	نظارت ۷ در ۲۴	✓	✓	✓
۱۷.	تیم متخصص با تجربه بررسی حملات سایبری اخیر کشور	✓	✓	✓
۱۸.	عمق سنسورهای پیشرفته	کم	متوسط	عمیق
۱۹.	اعلام هشدارهای امنیتی	✓	✓	✓
۲۰.	اعلام هشدار از طریق پیامک/تماس	✓	✓	✓
۲۱.	اعلام هشدارهای مهم به صورت کتبی	✓	✓	✓
۲۲.	شکار تهدیدات فعال	–	✓	✓
۲۳.	سطح سرویس تضمین شده	–	✓	✓
۲۴.	نگهداری هشدارها تا یکسال	–	✓	✓
۲۵.	گزارش ماهانه وضعیت شبکه	–	✓	✓

ردیف	قابلیت	سطح رایگان*	MDR Optimum	MDR Expert
۲۶.	فارنزیک تا سقف ۲۰ ساعت	–	✓	✓
۲۷.	فارنزیک تا سقف ۵۰ ساعت	–	–	✓
۲۸.	ارزیابی وضعیت امنیتی شبکه	–	–	✓
۲۹.	اعلام نقاط ضعف و قابل بهبود شبکه	–	–	✓
۳۰.	نگهداری لاگ‌های خام به مدت تعیین شده توسط سیاست سازمان	–	–	✓
۳۱.	دسترسی به سامانه وب Padvish MDR	–	–	✓

* در سطح رایگان طبیعتا تعهدی در ارائه خدمات و سطح آن وجود ندارد و صرفا در حد معقول تلاش می‌شود موارد مهم اعلام گردد.

تلفن: ۴۳۹۱۲۰۰۰ فکس: ۴۳۹۱۲۸۰۰
ایمیل: info@amnpardaz.com
وب سایت: www.amnpardaz.com