معرفی سامانه کشف و پاسخ به تهدیدات پنهان

(Padvish XDR AI)

شرکت نرم افزاری امن پرداز

سطح محرمانگی: عادی

نسخه ۱.۰

بهار ۱۴۰۴

فهرست مطالب

شکل‌ها

مقدمه

هدف این سند معرفی «**سامانه کشف و پاسخ به تهدیدات پنهان (Padvish XDR AI)**» و ماژول‌ها و امکانات مختلف آن می‌باشد.

۱. جایگاه محصول در اطلس راهکارهای پادویش

پیش از پرداختن به Padvish XDR و ویژگی‌های آن، باید جایگاه این محصول در اطلس راهکارهای پادویش و انتخاب‌های مختلف مشتریان مشخص گردد.

پادویش طیف گسترده‌ای از محصولات و راهکارها را برای پاسخ به نیازمندی سازمان‌های مختلف ارائه می‌دهد که به منظور سهولت در فهم و انتخاب محصول مناسب، در سه بعد امنیت سایبری، امنیت اطلاعات و مدیریت فناوری اطلاعات تقسیم‌بندی می‌شوند. در واقع مشتری می‌تواند از هر یک از این سه بعد، گزینه مدنظر خود را برگزیند و با ترکیب آنها، به راهکار مورد نیاز خود برسد.

۱/۱. بُعد امنیت سایبری

در بعد امنیت سایبری، رده‌های مختلف محصولات شرکت امن‌پرداز مطابق جدول زیر می‌باشد:

جدول1 - راهکارهای پادویش از بعد امنیت سایبری

	EPS[1]	ICD[2]/TN[3]	Vuln Assessment	EDR	MDR[4]	XDR
Padvish Base	✓	×	×	×	×	×
Padvish Corporate	✓	✓	✓	×	×	×
Padvish EDR Base/Select/Expert	✓	✓	✓	✓	×	×
Padvish MDR Optimum	✓	✓	✓	×	✓	×
Padvish MDR Base/Select/Expert	✓	✓	✓	✓	✓	×
Padvish XDR	✓	✓	✓	✓	×	✓
Padvish MXDR	✓	✓	✓	✓	✓	✓

محصولات موجود در جدول فوق به شرح زیر می‌باشند:

- Padvish Base: نسخه امنیت نقطه نهایی (End Point Security – EPS) شامل آنتی‌ویروس، فایروال، ضدباجگیر، IPS و کنترل ابزار
- Padvish Corporate: که علاوه بر تمامی امکانات نسخه Padvish Base، شامل امکانات پویش آسیب‌پذیری، شبکه‌های معتمد، و تشخیص اتصال اینترنت نیز می‌باشد.
- Padvish EDR Base/Select/Expert: که علاوه بر امکانات نسخه Padvish Corporate شامل سامانه EDR پادویش نیز می‌باشد و خود دارای سه زیرگروه EDR Base/Select/Expert می‌باشد.
- Padvish MDR Optimum: نسخه بهینه‌شده Padvish MDR (مرکز کشف و مقابله با حملات سایبری) که فاقد امکانات و کنسول EDR می‌باشد. این مرکز وظیفه اعلام هشدارهای مربوط به کشف نشانه‌های حملات سایبری را برعهده دارد.

[1] End Point Security
[2] Internet Connection Detection: تشخیص اتصال به اینترنت
[3] Trusted Network: شبکه‌های معتمد
[4] خدمات کشف و مقابله با نفوذ مدیریت شده

- Padvish MDR Base/Select/Expert: نسخه کامل Padvish MDR که بر اساس امکانات نسخه EDR متناظر، به سه زیرگروه MDR Base/Select/Expert تقسیم می‌شود و از سازمان در برابر حملات سایبری محافظت می‌کند.
- Padvish XDR Base/Select/Expert: سامانه XDR پادویش که علاوه بر امکانات Padvish EDR شامل امکانات پیشرفته تشخیص و مقابله با تهدیدات پنهان می‌شود.
- Padvish MXDR Base/Select/Expert: راهکار MXDR پادویش که تمامی قابلیت‌های XDR را در کنار خدمات مرکز مقابله با تهدیدات سایبری و خدمات فارنزیک و پاسخ به تهدیدات سایبری در خود جمع کرده است.

در خصوص تفاوت انواع محصول Base/Select/Expert در محصولات EDR/XDR/MDR/MXDR، جدول زیر اطلاعات دقیقتری ارائه می‌دهد:

جدول2 – انواع رده‌های محصولات Padvish EDR/XDR/MDR/MXDR

Modules	Padvish EDR AI			Padvish XDR AI		
	Base	Select	Expert	Base	Select	Expert
Anti-Malware	✓	✓	✓	✓	✓	✓
Memory Scanner	✓	✓	✓	✓	✓	✓
Behavior Protection	✓	✓	✓	✓	✓	✓
Machine Learning	✓	✓	✓	✓	✓	✓
IPS	✓	✓	✓	✓	✓	✓
File Library	×	✓	✓	×	✓	✓
Sandbox	×	○	✓	×	○	✓
Multi-AV	×	○	✓	×	○	✓
File Static Analyzers	×	○	✓	×	○	✓
Padvish CyberGPT™	✓	✓	✓	✓	✓	✓
Network Sensor	×	×	×	✓	✓	✓
Appliance Sensor	×	×	×	✓	✓	✓

- ماژول‌هایی که با علامت دایره (○) مشخص شده است به انتخاب مشتری قابل افزودن می‌باشند.
- برای آشنایی با عملکرد هر ماژول به بخش قابلیت‌های تشخیص تهدیدات Padvish XDR AI مراجعه نمایید.

همه راهکارهای فوق می‌توانند با امکاناتی از دو بعد دیگر راهکارهای پادویش (مثلا نسخه DRM و یا SD) ترکیب گردند.

۱/۲. بُعد افزونه امنیت اطلاعات

در بعد امنیت اطلاعات، دو افزونه مهم به راهکارهای فوق اضافه می‌شود:

جدول3 - افزونه‌های راهکارهای پادویش در بعد امنیت اطلاعات

	Digital Rights Management	Software and Device Control
DRM	✓	✗
DLP	✓	✓

محصولات موجود در جدول فوق به شرح زیر می‌باشند:

- DRM: با انتخاب این افزونه، امکانات Digital Rights Management به راهکار انتخابی افزوده می‌شود. این امکان ویژه با بهره‌گیری از الگوریتم‌های پیشرفته و استاندارد رمزنگاری، اسناد مهم سازمان را محافظت کرده و اجازه نشت یا دسترسی غیرمجاز به آنها را نمی‌دهد، بدون اینکه در کار عادی کاربران اختلالی ایجاد نماید.
- DLP: این افزونه علاوه بر امکان DRM شامل امکان Software and Device Control – SDC می‌باشد که تعریف سیاست‌های ریز بر نحوه دسترسی کاربران به فایل‌های درون رسانه‌های قابل حمل را به تفکیک نرم‌افزار، کاربر، ابزار، نوع فایل و زمان امکان‌پذیر می‌کند.

هر یک از این افزونه‌ها می‌توانند به هر یک از محصولات بخش قبل افزوده شوند و به عنوان مثال راهکارهایی مانند Padvish Corporate DRM یا Padvish MXDR DLP را تشکیل دهند.

۱/۳. بُعد افزونه مدیریت فناوری اطلاعات

در بعد مدیریت فناوری اطلاعات، سه افزونه مهم به راهکارهای فوق اضافه می‌شود:

جدول4 – افزونه‌های راهکارهای پادویش در بعد مدیریت فناوری اطلاعات

	Asset Management	Service Desk	Supervisor Console
AM	✓	×	×
SD	✓	✓	×
Padvish Supervisor	×	×	✓

افزونه‌های موجود در جدول فوق به شرح زیر می‌باشند:

- AM: این افزونه شامل امکان Asset Management می‌باشد که جزئی از راهکار میزکار امن‌پرداز (مکاپ) می‌باشد. در واقع با این انتخاب، در ایجنت‌های پادویش، امکانات جمع‌آوری خودکار دارایی‌های سخت‌افزاری و نرم‌افزاری سازمان از طریق کنسول مکاپ فعال می‌گردد.
- SD: این افزونه علاوه بر امکانات نسخه AM شامل امکان Service Desk می‌باشد که بخش دیگری از راهکار میزکار امن‌پرداز (مکاپ) بوده و امکانات میزخدمت، از قبیل ثبت تیکت رخداد، تعریف و آمارگیری از SLA خدمات IT، و... را در بر می‌گیرد.
- Padvish Supervisor: یک افزونه مستقل است که جهت نظارت بر عملکرد مدیریت فاوا قابل استفاده است. این افزونه به صورت یک محصول مستقل نصب شده و تمامی لاگ‌های کنسول مدیریتی پادویش را به صورت بلادرنگ در یک نقطه جمع‌آوری کرده و امکانات نگهداری بلندمدت و گزارشگیری را بدون تاثیر از سمت کنسول مدیریتی و یا احتمال حذف لاگ فراهم می‌کند.

همانطور که گفته شد، این افزونه‌ها نیز می‌توانند به راهکارهای قبلی اضافه شوند و به عنوان مثال محصولاتی از قبیل Padvish Corporate SD یا Padvish MXDR DRM AM را تشکیل دهند.

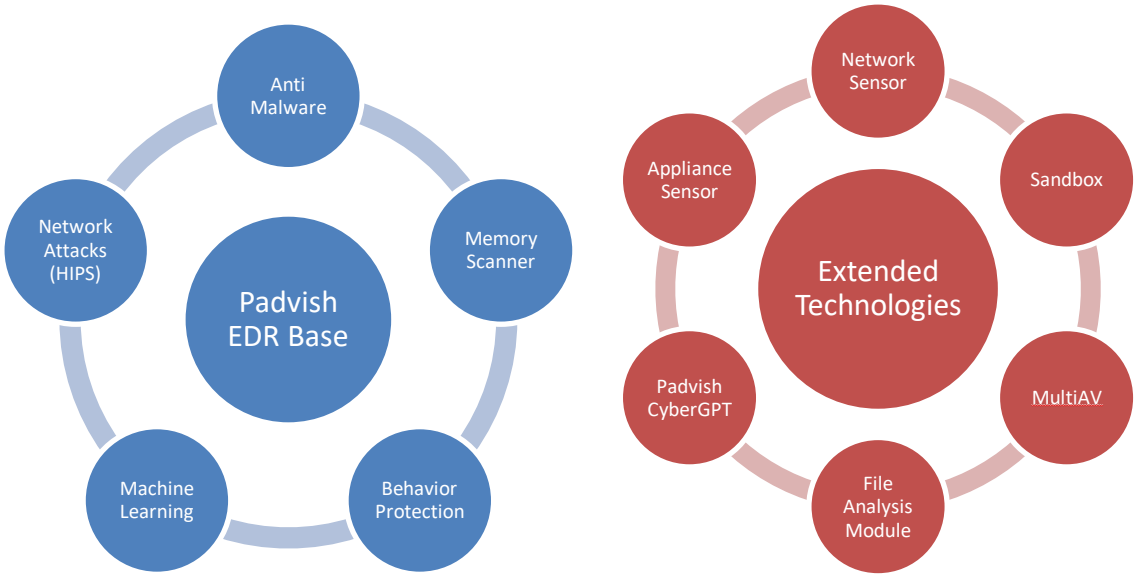
۲. معرفی سامانه Padvish XDR AI

کلمه XDR مخفف Extended Detection and Response است که به معنی تشخیص و مقابله (با تهدیدات) گسترده می‌باشد. هدف از کلمه گسترده در این تعریف، علاوه بر نقاط پایانی مانند سرورها، کلاینت‌ها، دستگاه‌های موبایل، و ... وجود ترافیک شبکه و دستگاه‌های غیر پایانی می‌باشد.

XDR توسط سازمان ها به عنوان یک جزء اساسی از سیاست‌ها و ابزارهای امنیتی به‌کار گرفته می‌شود. وظیفه اصلی XDR شامل نظارت بر فعالیت‌ها و رفتارهای مشکوک در دستگاه‌ها، تجزیه و تحلیل تهدیدات امنیتی و اعمال اقدامات اصلاحی در صورت شناسایی تهدیدها می‌باشد.

۲/۱. قابلیت‌های تشخیص تهدیدات Padvish XDR AI

سامانه Padvish XDR AI کل چرخه امنیت را از تشخیص رفتار توسط سنسورهای مستقر در نقطه پایانی، جمع‌آوری اطلاعات، تحلیل و بصری‌سازی، اعلام هشدار، و پاسخ به رویداد را در بر می‌گیرد. این محصول شامل فناوری‌های تشخیص مختلفی می‌باشد که در ادامه به بررسی آن‌ها می‌پردازیم.



شکل ۱- بررسی تکنولوژی Padvish XDR AI

۱. Anti-Malware: این فناوری برای تشخیص IOCها مورد استفاده قرار می‌گیرد. در بحث امنیت سایبری، اصطلاح IOC مخفف Indicator of Compromise یا «نشانه آلودگی» است و به آثار و نشانه‌هایی اطلاق می‌شود که از یک فعالیت مخرب یا نفوذ در سیستم یا شبکه باقی می‌مانند. IOCها به تیم‌های امنیتی کمک می‌کنند تا عملیات مخرب شناخته شده را به سرعت تشخیص داده و به‌طور موثر پاسخ دهند. مثال‌هایی از این دست شامل هش فایل‌های آلوده، دنباله‌ای از کدهای مخرب، و ... می‌باشد.

۲. Memory Scan: مموری اسکن یکی از فناوری هایی است که در سامانه Padvish XDR AI برای تشخیص و مانیتورینگ تهاجم‌های سایبری استفاده می‌شود. این ویژگی به تحلیل، حافظه (مموری) سیستم‌ها و پردازه‌های در حال اجرا می‌پردازد. نفوذها و حملات سایبری ممکن است به‌نحوی

انجام شوند که فقط در حافظه سیستم اجرا شوند. به عنوان مثال، برخی از بدافزارها و تروجان‌ها ممکن است مستقیما در حافظه رمزگشایی شده و فرآیندهای مخربی را اجرا کنند.

۳. Behavior Protection: اساس عملکرد هر سامانه XDR بخش محافظت رفتاری است. این فناوری در سامانه Padvish XDR AI با مجموعه سنسورهای خود به تحلیل و مانیتور کردن رفتارهای پردازه‌های سیستم می‌پردازد و در واقع با شناسایی الگوها و تغییرات غیرعادی، حملات سایبری را تشخیص می‌دهد.

٤. Machine Learning: در این فناوری از الگوریتم‌های یادگیری ماشین برای تشخیص تهدیدهای امنیتی و تشخیص الگوهای غیرعادی استفاده می‌شود. سامانه Padvish XDR AI با استفاده از الگوریتم‌های یادگیری ماشین می‌تواند نقشه ذهنی از ویژگی‌های نرم‌افزارها بسازد و کدهای مشکوک را شناسایی کند.

۵. IPS: این فناوری وظیفه تشخیص و محافظت از شبکه‌ها و سیستم‌ها در برابر حملات و اکسپلویت‌های شبکه‌ای از قبیل Log4j, ZeroLogon و حملات مشابه را دارد.

٦. Sandbox: این فناوری به اجرای فایل‌ها و برنامه‌ها در یک محیط مجازی و ایزوله اشاره دارد که با استفاده از این شیوه، به شناسایی و تجزیه و تحلیل تهدیدهای امنیتی کمک می‌کند. سامانه Padvish XDR AI از سندباکس به‌منظور تست و ارزیابی فایل های مشکوک استفاده می‌کند. این ماژول در نسخه Base وجود نداشته و در Expert و Select فعال می‌باشد.

۷. Multi AV: این فناوری با استفاده از چندین موتور آنتی‌ویروس به تشخیص و ردیابی تهدیدات امنیتی در سامانه Padvish XDR AI می‌پردازد. این ماژول در نسخه Base وجود نداشته و در Expert و Select فعال می‌باشد.

۸. Static File Analyzer: این فناوری به تجزیه و تحلیل فایل‌ها به‌منظور شناسایی تهدیدهای امنیتی و نشانه‌های آلودگی یا پنهان‌کاری در آن‌ها و مشخص کردن ویژگی‌های ایستای آنها می‌پردازد. این ماژول در نسخه Base وجود نداشته و در Expert و Select فعال می‌باشد.

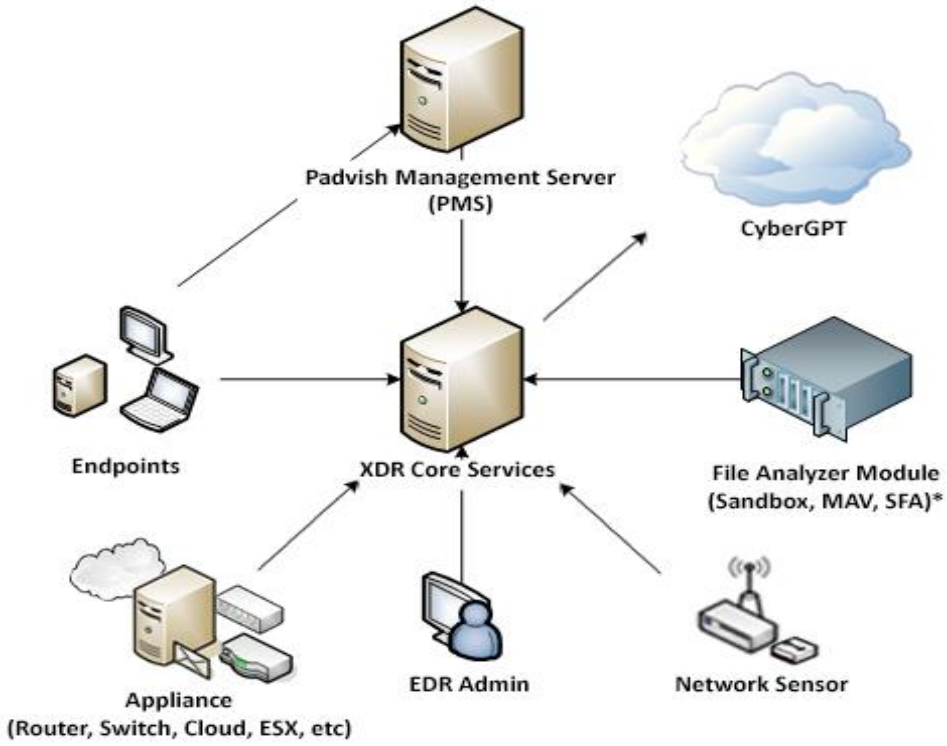
۹. Network Sensor: این فناوری با بررسی پکت‌های خام ترافیک کل شبکه، تهدیدات و حملات شبکه‌ای را پردازش و گزارش می‌کند. با استفاده از این ویژگی حملاتی که از طریق نقاط پایانی فاقد محافظت و یا نقاط خارج از حیطه مورد مراقبت شبکه انجام می‌شوند شناسایی می‌شوند.

۱۰. Appliance Sensor: این فناوری با دریافت لاگ از تجهیزات شبکه‌ای و زیرساختی، مانند زیرساخت مجازی‌سازی، زیرساخت ذخیره‌سازی، سوییچ‌ها و روترها و ... در صورت بروز موارد مشکوک و خطرناک مانند حملات در حال انجام به مدیر شبکه هشدار می‌دهد.

۱۱. Padvish CyberGPT™: این فناوری از هوش مصنوعی به عنوان دستیار تحلیلگر امنیت در سیستم استفاده می‌کند. به این ترتیب که الگوریتم‌های AI از یک طرف با خواندن اطلاعات جزئیات لاگ‌ها، هشدارها و تشخیص‌ها، یک تصمیم کلی شامل خلاصه موضوع و موارد مشکوک، بررسی احتمالی صحت و شدت خطر، و اقداماتی که باید در قبال آن انجام شود را ارائه می‌کند. علاوه بر این امکان تحلیل اسکریپت‌های پیچیده و نیز تولید خودکار کوئری‌های پیشرفته جهت شکار تهدیدات سایبری بر اساس خواسته کاربر نیز وجود دارد. مجموعه این قابلیت‌ها، سرعت شکار تهدیدات را افزایش می‌دهد و حتی رفتارهای غیرمعمول را نیز شناسایی می‌کند.

۳. معماری استقرار Padvish XDR AI

محصول Padvish XDR AI دارای معماری ارتباطی می‌باشد که در کامل‌ترین حالت خود با معماری زیر مستقر می‌شود:



شکل ۲- معماری Padvish XDR AI

در تصویر فوق، ماژول File Analyzer Module (FAM) که شامل Sandbox، Multi-AV و Static File Analyzer می‌شود در نسخه Base وجود نداشته و مخصوص نسخه‌های Select و Expert هستند.

در ادامه هر یک از مولفه‌ها شرح داده شده است:

۳٫۱. ماژول اصلی XDR Core Services

سرویس‌های اصلی XDR پادویش در این ماشین مجازی قرار می‌گیرند که شامل دریافت داده از سیستم کاربران، ارائه کنسول مدیریتی XDR به مدیر شبکه، و پایگاه‌های داده‌ای و سرویس‌های اختصاصی XDR پادویش می‌شود.

این ماژول سه نوع سرویس ارائه می‌دهد:

۱. **سرویس جمع‌آوری اطلاعات:** وظیفه جمع‌آوری اطلاعات از شبکه بر عهده این سرویس است. عامل پادویش از روی نقاط انتهایی شبکه و سرور مدیریتی پادویش و تجهیزات شبکه به این سرویس متصل می‌شوند و اطلاعات رویدادها را ارسال می‌کنند.
۲. **رابط کاربری** XDR: سرویس وب و رابط کاربری مدیریتی XDR از این طریق ارائه می‌شود که توصیه می‌شود دسترسی به آن به ایستگاه‌های کاری کارشناسان امنیت شبکه محدود گردد.
۳. **سرویس‌های پس‌زمینه‌ای:** سرویس‌هایی هستند که توسط ماژول تحلیل فایل XDR جهت دریافت اطلاعات و ارسال تحلیل‌ها مورد استفاده قرار می‌گیرند. اتصال به این سرویس‌ها باید به ماژول تحلیل فایل محدود گردد. این سرویس در نسخه Base وجود نداشته و اختصاصی نسخه Select و Expert می‌باشد.

ذخیره اطلاعات در ماژول اصلی انجام می‌گیرد که به سه فرمت انجام می‌شود:

۱. اطلاعات ساختارمند و تراکنشی که در قالب پایگاه داده SQL Server میکروسافت انجام می‌شود.
۲. موتور جستجوی سریع که در قالب NoSQL بر روی سرویس Elastic Search انجام می‌شود.
۳. (در نسخه Select و Expert) کتابخانه فایل‌ها که جهت ماژول تحلیل فایل استفاده شده و به صورت فایل‌سیستمی ذخیره می‌شود.

۳٫۲. ماژول تحلیل فایل File Analysis Module

در نسخه‌های Select و Expert، ماژول FAM وظیفه تحلیل فایل‌ها را برعهده دارد. این ماژول روی سخت‌افزاری فیزیکی (Bare Metal) نصب شده و سرویس‌های سندباکس، MultiAV و تحلیل ایستای فایل روی آن قرار می‌گیرند. جهت دریافت اطلاعات و اجرای عملیات به صورت مستقیم با سرویس‌های پس‌زمینه ماژول اصلی XDR در ارتباط می‌باشند.

۳٫۲٫۱. Multi AV

در Padvish XDR AI هنگامی که یک فایل بارگذاری می‌شود، و یا زمانی که ایجنت به صورت خودکار متوجه تغییر یک فایل اجرایی بشود، فایل توسط چندین آنتی ویروس آنالیز شده و نتیجه در اختیار کاربر قرار داده می‌شود.

Static File Analyzer .۳/۲/۲

هنگامی که یک فایل در Padvish XDR AI بارگذاری می‌شود، توسط موتورهای تحلیل ایستا مورد بررسی قرار می‌گیرد. این موتورها قادرند فایل‌های اجرایی ویندوز، فایل‌های اندرویدی، فایل‌های اجرایی لینوکس، داکیومنت‌های آفیس و ... را تحلیل و آنالیز کنند و نتیجه را در اختیار کاربر قرار دهند.

Sandbox .۳/۲/۳

یک محیط مجازی یا ایزوله می‌باشد که به‌منظور آزمایش و تجزیه و تحلیل فایل‌ها یا برنامه‌های مخرب به‌کار می‌رود. سندباکس‌ها به‌عنوان یکی از ابزارهای امنیتی استفاده می‌شوند و اجازه می‌دهند نمونه‌های مشکوک در یک محیط ایزوله و جداگانه بدون اینکه به سیستم‌های اصلی دسترسی داشته باشند، اجرا شوند و رفتارهای مشکوک آنها ثبت گردد.

۳/۳. سرور مدیریتی پادویش Padvish Management Server

سرور مدیریتی آنتی‌ویروس است که در اختیار مدیر شبکه قرار داشته و از آن طریق کلیه کلاینت‌های پادویش مدیریت می‌شوند. سرور مدیریتی آنتی‌ویروس پادویش از طریق پورت جمع‌آوری اطلاعات با ماژول اصلی XDR در ارتباط است و وضعیت کلاینت‌ها را به آن اعلام می‌کند.

۳/۴. نقاط انتهایی Endpoints

نقاط انتهایی یا اصطلاحا کلاینت‌ها، شامل همه سرورها، دستگاه‌ها و نقاط انتهایی است که در شبکه سازمان وجود دارند و عامل پادویش روی آنها نصب شده است. این کلاینت‌ها از یک طرف به سرور مدیریتی پادویش متصل هستند و از طرف دیگر اطلاعات درلحظه خود را از طریق پورت جمع‌آوری اطلاعات به ماژول اصلی XDR پادویش ارسال می‌کنند.

۳/۵. ماژول Appliance

این ماژول شامل تجهیزات شبکه و دستگاه‌های غیر پایانی شامل تمام انواع روترها و سوییچ‌ها و فایروال ها و سرورهای ESX و ... می‌باشند. این دستگاه‌ها لاگ را از طریق پروتکل Syslog به این ماژول ارسال می‌کنند.

۳/۶. ماژول سنسور ترافیک Network Sensor

این ماژول ترافیک کل شبکه را از طریق پورت SPAN یا مکانیزم مشابه دریافت کرده و با اعمال مکانیزم‌های IDS بر روی آن، ترافیک‌های مشکوک و خطرناک را شناسایی می‌کند.

۴. جمع‌بندی

در این سند محصول Padvish XDR AI، ویژگی‌ها، معماری، و نیازمندی‌های آن معرفی گردید. از آنجاکه استفاده از محصولات XDR نیازمند تخصص و مهارت بالایی می‌باشد، در بسیاری از سازمان‌ها نیاز به خدمات راهبری این سامانه نیز احساس می‌شود. مرکز کشف و پاسخ به حملات سایبری (Padvish MXDR) امکانی را فراهم می‌کند که سازمان با حداقل هزینه خود را در برابر حملات سایبری مقاوم نماید.

حتی در سازمان‌هایی که تیم مرکز عملیات امنیت (SOC) متبحری دارند، استفاده از خدمات و تجربیات اختصاصی مرکز کشف و پاسخ به حملات سایبری (Padvish MXDR) در مقابله با حملات واقعی، می‌تواند به تشخیص حملات سایبری مخفیانه گروه‌های پیشرفته سایبری کمک کند.

- جهت اطلاعات بیشتر در این خصوص دعوت می‌کنیم سند «معرفی راهکار کشف و پاسخ به حملات سایبری (Padvish MXDR)» را مطالعه بفرمایید.