شرکت نرم افزاری امن پرداز®
Amnpardaz Software Corporation

گزارش اعتبارسنجی بین‌المللی، جایگاه جهانی و توانمندی‌های Padvish XDR AI

تحلیل نتایج ارزیابی آزمایشگاه AV-Test آلمان، جایگاه در حوزه EDR Telemetry و ارزیابی توانمندی‌های محصول در کشف و پاسخ پیشرفته

Padvish XDR AI نسل جدید **راهکارهای گسترده کشف و پاسخ (XDR)** است که با ترکیب تله‌متری عمیق، تحلیل همبستگی داده‌ها، موتورهای تشخیص چندلایه و هوش مصنوعی اختصاصی، به سازمان‌ها کمک می‌کند تهدیدات پیچیده و چندمرحله‌ای را سریع‌تر و دقیق‌تر شناسایی و مهار کنند.

این سند، به‌صورت فشرده و مستند، سه محور کلیدی را برای تصمیم‌گیران سازمانی ارائه می‌کند:

۱. **اعتبارسنجی مستقل بین‌المللی:** نتایج آزمون AV-TEST و دریافت گواهی A2EDR؛

۲. **جایگاه بین‌المللی در حوزه Telemetry و معماری داده‌محور:** کیفیت مشاهده‌پذیری و داده؛

۳. **توانمندی‌های فنی و عملیاتی:** معماری، موتورهای تشخیص، هوش مصنوعی و تأثیر بر کارایی SOC.

فهرست

خلاصه اجرایی

راهکار Padvish XDR AI پاسخی جامع به چالش‌های ناشی از ابزارهای امنیتی جزیره‌ای و داده‌های پراکنده امنیتی در سازمان‌ها است. این محصول با اتکا بر:

- تله‌متری غنی و چندلایه از نقاط پایانی و سایر لایه‌های شبکه،
- تحلیل رفتاری پیشرفته و همبستگی داده‌ها،
- موتورهای تشخیص چندلایه (Anti-Malware، Memory Scanner، Behavior Protection، Machine Learning، IPS، Sandbox، و سنسورهای شبکه)،
- و قابلیت‌های هوش مصنوعی، به‌ویژه Padvish CyberGPT™،

امکان کشف، تحلیل و پاسخ به تهدیدات پیچیده‌ای را فراهم می‌کند که از دید ابزارهای جزیره‌ای پنهان می‌مانند.

در نوامبر ۲۰۲۵، Padvish XDR AI در آزمایشگاه مستقل AV-TEST تحت ارزیابی پیشرفته Advanced EDR برمبنای حملات پیشرفته (APT) قرار گرفت و پس از ارزیابی با سناریوهای پیچیده جاسوسی سایبری، حملات پیچیده و چند مرحله ای باج‌افزاری هدفمند و شبیه‌سازی حملات پیشرفته پایدار APT موفق به کسب گواهی معتبر AV-TEST Approved Advanced Endpoint Detection and Response (A2EDR) شد. این اعتبارسنجی، درکنار قرارگیری در رتبه‌بندی معتبر جهانی EDR Telemetry نشان می‌دهد که Padvish XDR AI نه‌تنها در سطح موتورهای تشخیص، بلکه در سطح کیفیت داده و مشاهده‌پذیری نیز در کلاس جهانی عمل می‌کند.

این راهکار دید یکپارچه و متمرکز نسبت به تهدیدات سایبری ارائه میکند؛

- از طریق کاهش False Positive ها و تمرکز تحلیلگران بر هشدارهای واقعی، بهره‌وری SOC را بهبود می‌دهد؛
- با بهره‌گیری از Padvish CyberGPT™، تحلیل داده‌های امنیتی را ساده‌تر، سریع‌تر و قابل دسترس‌تر می‌کند؛
- و از نظر کیفیت تله‌متری و مشاهده‌پذیری تهدید در سطحی رقابت‌پذیر با بسیاری از محصولات مطرح جهانی قرار دارد.

Padvish
XDR AI

معرفی سامانه Padvish XDR AI

Padvish XDR AI یک پلتفرم تشخیص و پاسخ توسعه‌یافته مبتنی بر هوش مصنوعی است که مأموریت آن، یکپارچه‌سازی دید امنیتی، شتاب‌دهی به چرخه کشف تا پاسخ، و کاهش پیچیدگی عملیاتی در مرکز عملیات امنیت (SOC) است.

در هسته مرکزی Padvish XDR AI، موتور محافظت پیشرفته آن قرار دارد که با استفاده از بدافزارهای روز صفر (Zero-day) و شبیه‌سازی حملات هدفمند مورد ارزیابی قرار گرفته است. این راهکار با بهره‌گیری از تحلیل رفتاری و مکانیسم‌های شناسایی چندلایه، قادر است تکنیک‌های پیچیده حمله از جمله دسترسی اولیه مبتنی بر فیشینگ، ارتقای سطح دسترسی، جابه‌جایی جانبی، سرقت اعتبارنامه‌ها و فعالیت‌های استخراج داده را شناسایی کند.

ویژگی‌های کلیدی در یک نگاه

۱ مدیریت متمرکز و پاسخ کارآمد در محیط‌های گسترده

امکان استقرار، پیکربندی و واکنش سریع به تهدیدات در زیرساخت‌های توزیع‌شده سازمانی و مدیریت یکپارچه امنیت از یک نقطه واحد.

۲ ردیابی کامل زنجیره حمله و تحلیل رفتار مهاجم

تمامی مراحل حمله، از نفوذ اولیه و ایجاد پایداری (Persistence) تا رمزنگاری باج‌افزاری را ردیابی کرده تا رفتار مهاجم را به دقت ارزیابی کند.

۳ افزایش سرعت و دقت در تشخیص، تحقیق و پاسخ

SOC می‌تواند از مرحله مشاهده اولین نشانه‌ها تا ریشه‌یابی و مهار، با سرعت و اطمینان بیشتر عمل کند.

۴ کاهش False Positive و تمرکز بر هشدارهای مهم

با ترکیب چندین موتور تشخیص و هوش مصنوعی، هشدارهای غیرضروری کاهش یافته و بار تحلیلی تیم کاهش می‌یابد.

۵ استفاده از هوش مصنوعی در تصمیم‌گیری عملیاتی

Padvish CyberGPT™ به‌عنوان دستیار هوشمند امنیت، رخدادها را به زبان طبیعی توضیح، اسکریپت‌ها را تحلیل و پیشنهاداتی برای پاسخ ارائه می‌دهد.

۶ پشتیبانی از زیرساخت‌های مدرن و تحلیل‌های عملیاتی

سازگاری کامل با سیستم‌عامل‌های به‌روز مانند ویندوز ۱۱ و ارائه بینش‌های کاربردی برای اعمال سیاست‌های امنیتی و رفع تهدیدات در لحظه (Real-time).

۷ ارتقای تاب‌آوری در برابر حملات هدفمند

ایجاد یک پلتفرم قدرتمند برای پایش جامع و پاسخ‌دهی که توانمندی سازمان را در مواجهه با تهدیدات سایبری پیچیده به‌طور چشمگیری افزایش می‌دهد.

اعتبارسنجی بین‌المللی Padvish XDR AI در آزمایشگاه AV-TEST آلمان

Padvish XDR AI در نوامبر ۲۰۲۵ تحت یک ارزیابی فنی جامع توسط آزمایشگاه مستقل و بین‌المللی AV-TEST قرار گرفت. این ارزیابی به‌طور مشخص بر قابلیت‌های تشخیص و پاسخ در نقطه پایانی (Endpoint Detection and Response-EDR) تمرکز داشت و با هدف سنجش توانمندی سامانه در شناسایی، تحلیل و مقابله با تهدیدات پیچیده مرتبط با حملات پیشرفته پایدار (APT) انجام شد.

بر اساس گزارش رسمیAV-TEST، این ارزیابی با استفاده از سناریوهای جامع و چند مرحله ای بر مبنای MITRE ATT&CK انجام شد که سه الگوی تهدید مهم را بازآفرینی می‌کردند:

سناریو حمله پیچیده چندمرحله ای جاسوسی سایبری	سناریو حمله باج افزاری هدفمند	سناریو حمله پیشرفته پایدار
APT18-Style Cyber Espionage	**Bizfum Stealer**	**Helldown Ransomware Emulation**

هر یک از این سناریوها مجموعه‌ای از تاکتیک‌ها و تکنیک‌های مورد استفاده مهاجمان حرفه‌ای را در طول چرخه کامل حمله (از نفوذ اولیه تا اثر نهایی بر سیستم) شبیه‌سازی می کردند.

نتایج نهایی ارزیابی AV-TEST

در جمع‌بندی این ارزیابی، آزمایشگاه AV-TEST اعلام می‌کند:

” Padvish XDR excels at securing the internal network landscape, making it highly effective against advanced persistent threats (APTs) that often bypass initial security measures.The impressive results highlight Padvish XDR’s utility in safeguarding against advanced cyber threats. “

AV TEST
The Independent IT-Security Institute
Magdeburg Germany

«پادویش XDR در ایمن‌سازی فضای شبکه داخلی عملکردی بی نظیر دارد و در برابر تهدیدات پیشرفته پایدار (APT) که غالباً از لایه‌های امنیتی اولیه عبور می‌کنند، بسیار کارآمد است. این نتایجِ چشمگیر، کارایی پادویش XDR را در محافظت در برابر تهدیدات سایبری پیشرفته به خوبی نشان می‌دهد.»

این گزارش همچنین تأکید می‌کند که این راهکار توانسته بردارهای کلیدی حمله را در مراحل مختلف عملیات مهاجم شناسایی کند؛ از اجرای فایل مخرب تا حرکت جانبی پیچیده در شبکه و اقدامات مخرب در سطح سیستم.

این محصول پس از ارزیابی های صورت گرفته، موفق به دریافت گواهی معتبر A2EDR شد:

AV-TEST Approved Advanced Endpoint Detection and Response (A2EDR)

گواهی‌ای که نشان‌دهنده توانمندی عملی راهکار در شناسایی و پاسخ به تهدیدات پیشرفته و حملات پیچیده گروه‌های APT است.

سناریوهای گواهی A2EDR و توانمندی Padvish XDR AI

بـر اسـاس گـزارش رسـمی AV-TEST، ایـن ارزیابـی بـا اسـتفاده از سـناریوهای حملـه شبیه‌سازی‌شـده و چنـد مرحلـه‌ای انجـام شـد کـه سـه الگـوی تهدیـد مهـم را بازآفرینـی می‌کردنـد:

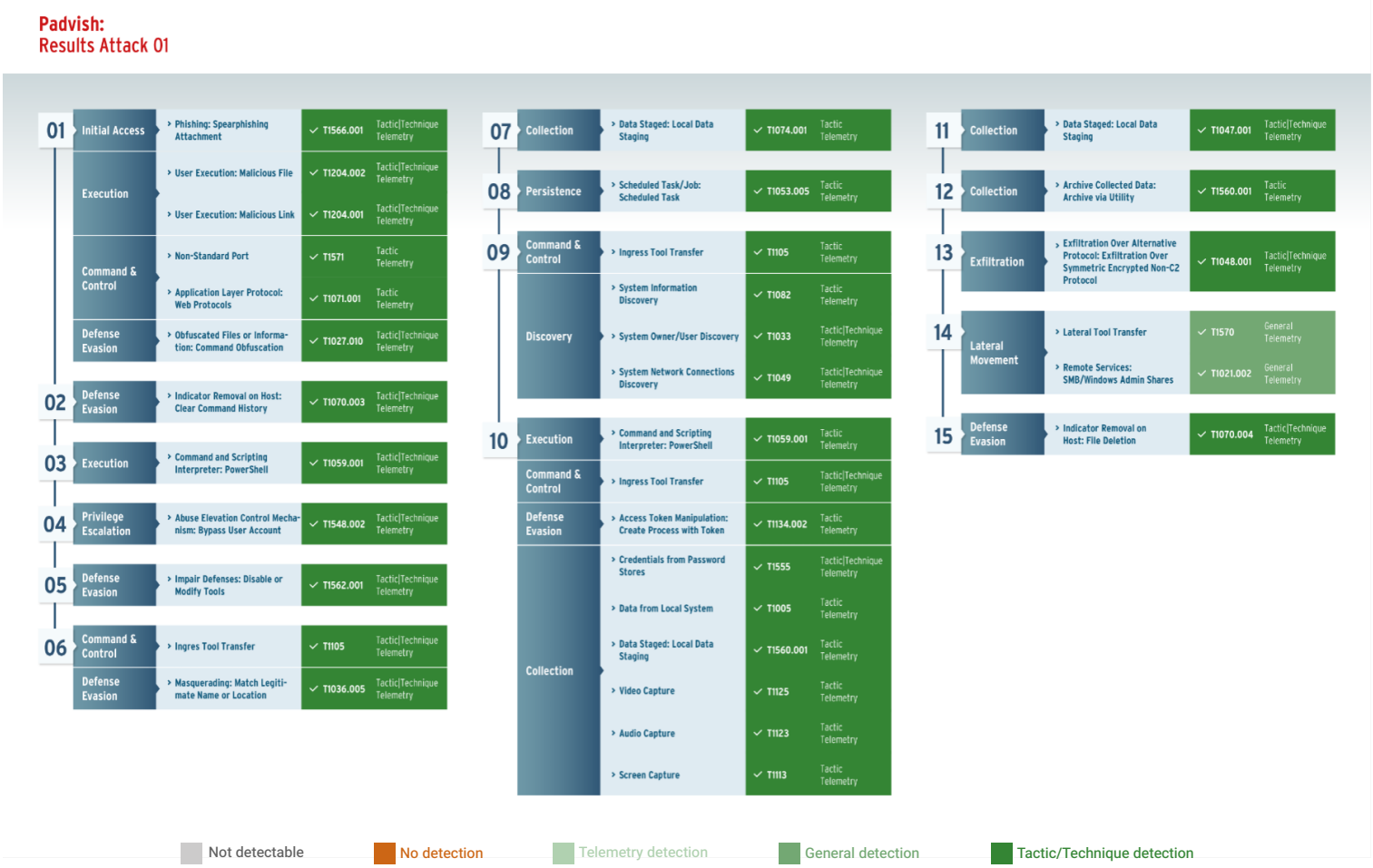
سناریوی اول: شبیه‌سازی حمله جاسوسی سایبری به سبک APT-18

ارزیابی توان دید امنیتی در یک حمله جاسوسی چندمرحله‌ای

در سـناریوی نخسـت، AV-TEST یـک حملـه پیچیـده جاسوسـی سـایبری را شبیه‌سـازی کـرد کـه مبتنـی بـر PowerShell، تکنیک‌هـای دور زدن دفاعـی (Evasion Defense) و حرکـت مرحلـه بـه مرحلـه از پیوسـت فیشـینگ هدفمنـد (Spear-Phishing Attachment) تـا جمع‌آوری و خـروج اطلاعـات (Data Exfiltration) بـود.

نتایـج شبیه‌سـازی تهدیـد در ایـن سـناریو بـر مبنـای مراحـل ماتریـس MITRE ATT&CK در جـدول زیـر ارائـه شـده اسـت. ایـن نتایـج نشـان‌دهنده سـطح بسـیار بالایـی از کشـف تهدیـد در تمامـی مراحـل حملـه اسـت کـه بـا اسـتانداردهای پیشـرفته امنیـت سـایبری در سـطح جهانـی برابـری می‌کنـد.

Padvish:
Results Attack 01



در این سناریو، گزارشAV-TEST تصریح می‌کند:

”Padvish XDR demonstrated outstanding visibility.“
« سامانه Padvish XDR توانایی بینظیری در تشخیص تهدیدات و ایجاد دید امنیتی به نمایش گذاشت.»

”The quality of detection was exceptionally high.“
« دقت و کیفیت تشخیص در سطح بسیار ممتازی قرار داشت. »

این ارزیابی، نه‌تنها بر میزان «پوشش» (گستره شناسایی فعالیت‌های مشکوک توسط Padvish XDR AI در هر گام از حمله) متمرکز بود، بلکه با تحلیل و اندازه‌گیریِ نحوه گزارش‌دهیِ تاکتیک‌ها و تکنیک‌های به‌کاررفته، کیفیت و دقت این شناسایی‌ها را نیز به‌طور عمیق مورد بررسی قرار داد.

در این سناریو، Padvish XDR AI مراحل حیاتی حمله را با موفقیت شناسایی کرد، از جمله:

- اجرای فایل مخرب (Malicious File Execution)
- مبهم‌سازی دستورات (Command Obfuscation)
- ارتقای سطح دسترسی از طریق دور زدن (Privilege Escalation via UAC Bypass)

نکته قابل توجه در این بخش، اشاره مستقیم گزارشAV-TEST به نقش تله‌متری امنیتی (Security Telemetry) است. گزارش بیان می‌کند که حتی در مراحل پایانی حمله-شامل آرشیو و خروج داده‌ها-داده‌های تله‌متری تولید شده توسط سامانه امکان ردیابی کامل زنجیره حمله را فراهم کرده است.

این موضوع نشان‌دهنده یکی از ویژگی‌های کلیدی یک EDR بسیار پیشرفته در سطح بین‌المللی است:

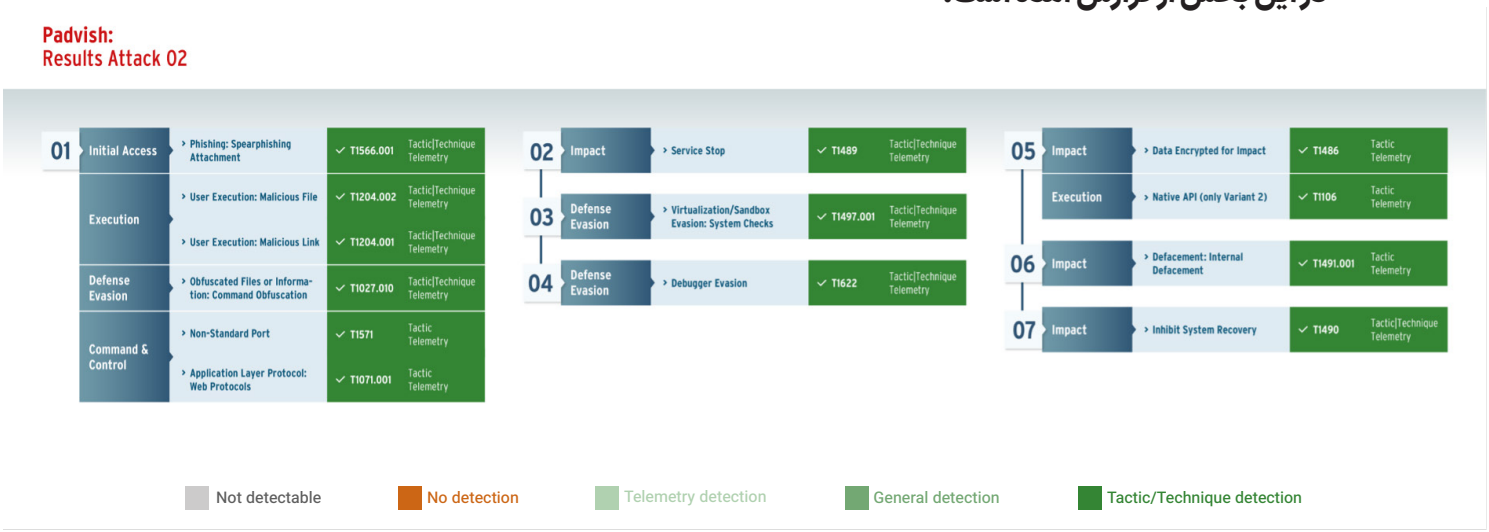
ایجاد دید عملیاتی و تحلیلی نسبت به کل زنجیره حمله، نه صرفا تولید هشدارهای منفرد.

سناریوی دوم: شبیه‌سازی حمله پیچیده Bizfum Stealer

سنجش توان تشخیص در یک حمله باج‌افزاری هدفمند

در این سناریو، توانمندی Padvish XDR AI در مقابله با حملات پیچیده مبتنی بر اختلال در سرویس و رمزنگاری داده‌ها مورد ارزیابی قرار گرفت. این تحلیل، زنجیره کامل حمله از دسترسی اولیه و دور زدن مکانیزم‌های دفاعی تا توقف هدفمند سرویس‌ها، گریز از ساندباکس، رمزنگاری اطلاعات، تخریب چهره سیستم (Defacement) و جلوگیری از بازیابی سیستم را بررسی می‌کند.
نتایج شبیه‌سازی تهدید در این سناریو نیز بر مبنای مراحل ماتریس MITRE ATT&CK در جدول زیر ارائه شده است.

در این بخش از گزارش آمده است:



Padvish XDR demonstrated strong coverage in Scenario 2, effectively monitoring the attack from the initial access to the final encryption and system impact phases.

Padvish XDR در سناریوی دوم، سطح پوشش‌دهی قدرتمندی از خود به نمایش گذاشت و با تسلط کامل، تمامی مراحل حمله را از لحظه رخنه اولیه تا فازهای نهایی رمزنگاری و ضربه عملیاتی به سیستم تحت پایشِ قرار داد.

در این سناریو، سامانه توانست مجموعه‌ای از رفتارهای مخرب را شناسایی کند، از جمله:

اجرای کدهای مخرب	مبهم‌سازی دستورات	ارتباطات شبکه‌ای مشکوک

علاوه بر این، اثرات مخرب حمله نیز به‌درستی تشخیص داده شدند، از جمله:

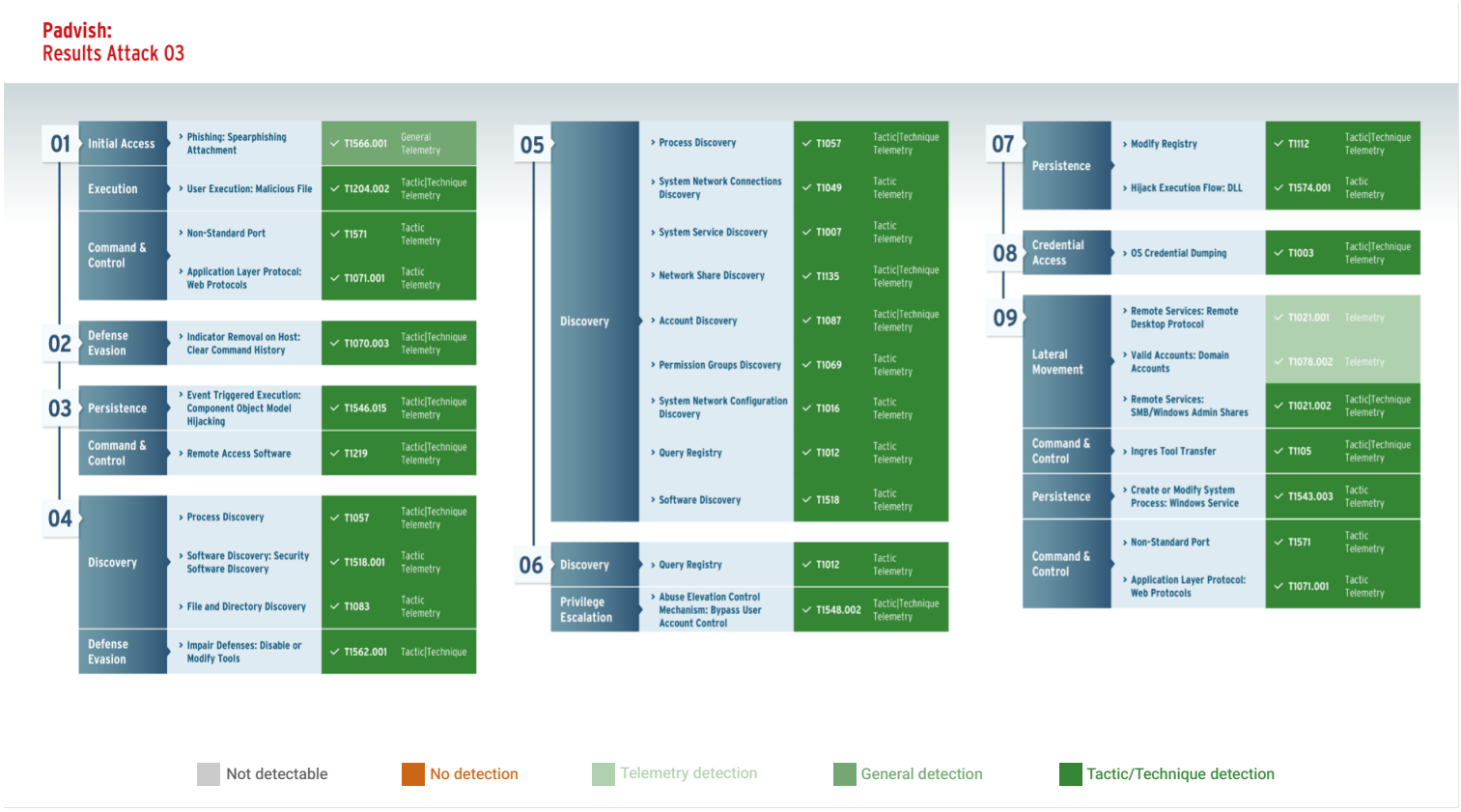
- رمزگذاری داده‌ها (Data Encryption)
- تخریب داخلی سیستم‌ها (Internal Defacement)
- تلاش برای جلوگیری از بازیابی سیستم (Inhibit System Recovery)

گزارش AV-TEST همچنین اشاره می‌کند که پیوست اولیه فیشینگ هدفمند و تکنیک‌های پیچیده فرار از سندباکس باعث ایجاد هشدارهای دقیق در سطح تکنیک حمله (Technique-Level Alerts) شده‌اند.

سناریوی سوم: شبیه‌سازی حملات پنهانکار پیشرفته Helldown Ransomware

ارزیابی تاب‌آوری در برابر حملات پیشرفته و حرکت جانبی در شبکه

در سناریو سوم، تمرکز بر میزان تاب‌آوریِ این راهکار در برابر ماهیتِ ماژولار و انطباق‌پذیرِ یک تهدید پیشرفته پایدار (APT) بود. این تحلیل، چگونگی مقابله Padvish XDR AI با عملیات گسترده شناسایی سیستم ، تکنیک‌های پیچیده گریز و حرکت جانبی که شاخصه حملات هدفمند مدرن هستند را بررسی کرد. نتایج شبیه‌سازی تهدید در این سناریو نیز بر مبنای مراحل ماتریس MITRE ATT&CK در جدول زیر ارائه شده است.



در این سناریو، Padvish XDR AI توانست مراحل کلیدی زیر را شناسایی کند:

۱. پیوست اولیه فیشینگ هدفمند

۲. اجرای فایل مخرب

۳. حرکت جانبی در شبکه از طریق پروتکل Remote Desktop (RDP)

گزارش AV-TEST همچنین تأکید می‌کند که سامانه به‌صورت صریح رفتارهای پیشرفته زیر را شناسایی کرده است:

- استخراج اعتبارنامه‌های سیستم‌عامل (OS Credential Dumping)
- ارتقای سطح دسترسی (Privilege Escalation)
- سوءاستفاده از مکانیزم (COM Hijacking)

علاوه بر این، سامانه فعالیت‌هایی مانند موارد زیر را نیز پایش کرده است:

- شناسایی خودکار سیستم‌ها در شبکه (Automated System Discovery)
- تلاش برای تضعیف یا غیرفعال‌سازی ابزارهای امنیتی (Impairment of Security Tools)

در گزارش AV-TEST، این سطح از مشاهده‌پذیری و تشخیص با عبارت زیر توصیف شده است:

”A high degree of resilience“
«سطح بالایی از تاب‌آوری و مقاومت در برابر حملات پیشرفته.»

” Padvish XDR delivered exceptional, high-fidelity warnings for critical phases of the attack. “

«Padvish XDR در فازهای حیاتیِ حمله، هشدارهایی با دقت خیره‌کننده و استثنایی صادر کرد.»

ارزش عملی اعتبارسنجی A2EDR برای سازمان‌ها

یکی از نکات مهم در روش ارزیابی AV-TEST این است که تحلیل محصول صرفا به تشخیص یک بدافزار یا تولید چند هشدار محدود نشده است.

در این ارزیابی، معیارهای زیر مورد بررسی قرار گرفته‌اند:

پوشش کامل چرخه حمله	کیفیت تشخیص تهدیدات	عمق مشاهده‌پذیری در سطوح
تله‌متری (Telemetry)	تاکتیک (Tactic)	تکنیک (Technique)

به همین دلیل، ارزش واقعی Padvish XDR AI تنها در تشخیص یک تهدید خلاصه نمیشود، بلکه در توانایی سامانه برای بازسازی زنجیره کامل حمله، حفظ زمینه تحلیلی (Context) و فراهم کردن داده‌های قابل استفاده برای عملیات امنیتی نهفته است.

در نتیجه، دریافت گواهی A2EDR نشان می‌دهد که این راهکار در یک ارزیابی مستقل بین‌المللی توانسته در برابر سناریوهایی از جنس:

- جاسوسی سایبری
- باج‌افزار هدفمند
- حملات پیشرفته چندمرحله‌ای

تشخیص مؤثر، دید امنیتی عمیق و قابلیت ردیابی دقیق رفتار مهاجمان را ارائه دهد.

به بیان عملیاتی، نتایج این ارزیابی نشان می‌دهد که Padvish XDR AI می‌تواند از مرحله نفوذ اولیه مهاجم تا اثر نهایی حمله، تصویری قابل اتکا برای تیم‌های امنیتی فراهم کند؛ تصویری که مستقیما در تشخیص تهدید (Threat Detection)، شکار تهدید (Threat Hunting)، پاسخ به رخداد (Incident Response) و کاهش زمان تحلیل و واکنش تیم SOC مؤثر است.

توانایی تشخیص حملات پیشرفته و زنجیره حمله

Padvish XDR AI برای مقابله با تهدیدات مدرن، بر تحلیل زنجیره کامل حمله متمرکز است.

این سامانه قادر است مراحل مختلف یک حمله را مطابق با چرخه‌های متداول (نظیر مدل‌های الهام‌گرفته از MITRE ATT&CK) شناسایی کند، از جمله:

- نفوذ اولیه
- اجرای بدافزار
- ارتقای دسترسی (Privilege Escalation)
- حرکت جانبی (Lateral Movement)
- تخریب یا استخراج داده (Data Exfiltration / Destruction)

سامانه، رفتار مهاجم را در طول این زنجیره تحلیل کرده و با همبستگی رویدادها، روایت واحدی از حادثه برای تحلیلگر ایجاد می‌کند. به‌عنوان نمونه، در گزارش AV-TEST اشاره شده است که:

حتی در مراحل پایانی حمله که شامل آرشیو و خروج داده‌ها بوده است، تله‌متری تولیدشده توسط سامانه، امکان ردیابی زنجیره حمله را فراهم کرده است؛

این سطح از مشاهده‌پذیری، برای تحلیل علت‌ریشه‌ای (Root Cause Analysis) و مستندسازی حادثه حیاتی است.

نتیجه برای سازمان:

در سناریوهای پیچیده و چندمرحله‌ای، تیم SOC می‌تواند به‌جای تمرکز بر یک هشدار منفرد، کل سناریوی حمله را در یک نمای یکپارچه مشاهده و تصمیم‌گیری کند.

پروژه EDR Telemetry: سنگ‌بنای تشخیص پیشرفته و مزیت رقابتی Padvish XDR AI

موفقیت‌های مستمر Padvish XDR AI در آزمون‌های معتبری همچون AV-TEST آلمان، تنها بخشی از کارنامه عملیاتی این محصول در عرصه‌های بین‌المللی به شمار می‌رود. پیش از این دستاورد، Padvish XDR AI با حضوری مقتدرانه در ارزیابی‌های جهانی، موفق به ورود به رتبه‌بندی معتبر EDR Telemetry Project گردید.

Padvish XDR AI در این رده‌بندی تخصصی، با کسب جایگاه نهم جهان و ایستادن در سطحی بالاتر از بسیاری از برندهای مطرح و پیشگام بین‌المللی، بلوغ فنی خود را در شاخص‌های کلیدیِ پایش و تحلیلِ عمیقِ داده (Telemetry) به اثبات رسانده است. این جایگاه، پادویش XDR را در زمره معدود محصولات شاخص و تراز اول جهان در حوزه کشف و پاسخ پیشرفته به تهدیدات قرار می‌دهد.

نقش تله‌متری در EDR/XDR

در سامانه‌های EDR و XDR، کیفیت تشخیص به کیفیت داده‌هایی بستگی دارد که از سیستم‌ها جمع‌آوری می‌شود. این داده‌ها با عنوان تله‌متری شناخته می‌شوند و شامل مواردی مانند:

- اجرای فرآیندها؛
- ارتباطات شبکه؛
- فعالیت فایل‌ها و تغییرات آن‌ها؛
- اجرای اسکریپت‌ها؛
- تغییرات رجیستری و تنظیمات سیستم؛
- و در معماری XDR، داده‌های لایه‌های فراتر از نقاط پایانی (مانند حسگرهای شبکه).

«تله‌متری در واقع چشم سیستم و ورودی موتور تشخیص است.»

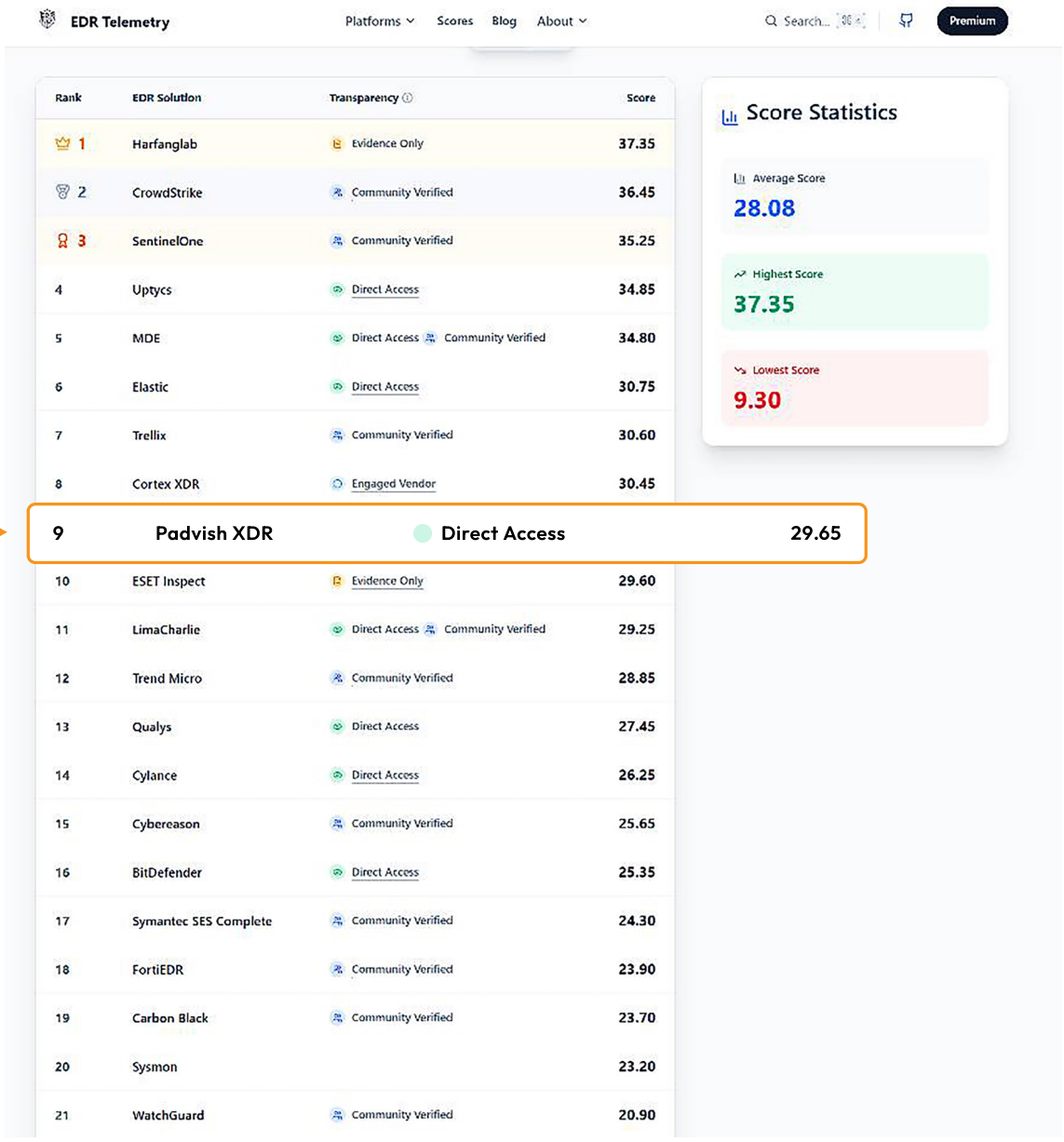
بنابراین: کیفیت تله‌متری، پیش‌نیاز اثربخشی سایر قابلیت‌های EDR/XDR است.

پروژه EDR Telemetry و جایگاه Padvish

پـروژه تخصصـی EDR Telemetry به‌جـای سـنجش صرفـا خروجـی تشـخیص (Detection)، کیفیـت داده ورودی سـامانه‌های EDR را بررسـی می‌کنـد؛ یعنـی اینکـه محصـول تـا چـه حـد:

- رفتارهای سیستم را با جزئیات کافی ثبت می‌کند؛
- در مراحل مختلف یک حمله، داده‌ی قابل تحلیل تولید می‌کند؛
- و امکان بازسازی و تحلیل حادثه را فراهم می‌سازد.

در ایـن ارزیابـی، روش تسـت دسترسـی مسـتقیم (Direct Access) بـرای محصـول پادویـش XDR AI بـه کار رفتـه اسـت. بـه کارگیـری ایـن روش، نشـان‌دهنده بالاتریـن سـطح شـفافیت در تسـت محصـول و ویژگی‌هـای فنـی آن اسـت.



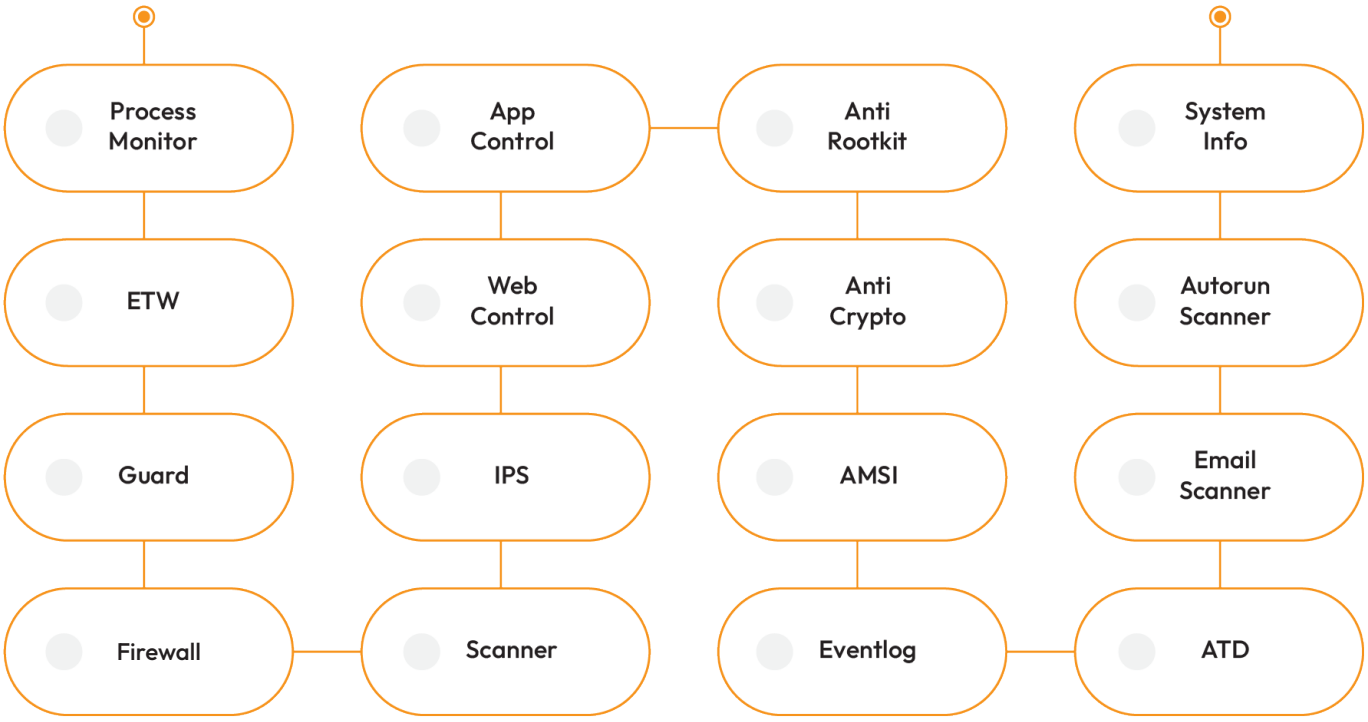
در این حوزه، قرارگیری پادویش بالاتر از بسیاری از رقبای جهانی نشان میدهد:

این محصول از نظر عمق مشاهده‌پذیری و کیفیت داده‌های امنیتی در سطحی رقابت‌پذیر با بسیاری از محصولات مطرح جهانی قرار دارد، و مزیت پادویش تنها در تولید هشدار نیست؛ بلکه در تولید داده امنیتی غنی و قابل تحلیل است که پایه واقعی تشخیص پیشرفته را تشکیل می‌دهد.

به بیان دیگر:

- سازمانی که Padvish XDR AI را مستقر می‌کند، صرفا یک «سیستم هشدار» دریافت نمی‌کند؛
- بلکه یک زیرساخت داده امنیتی به‌دست می‌آورد که می‌تواند پایه‌ی Threat Hunting، تحلیل رفتاری و گزارش‌دهی تحلیلی باشد.

موتورهای تله متری Padvish XDR AI



معماری فنی سامانه Padvish XDR AI

معماری Padvish XDR AI بر سه لایه‌ی اصلی استوار است:

۱ - لایه جمع‌آوری داده (Data Collection Layer)

- عامل‌های نصب‌شده بر روی نقاط پایانی (Endpoint Agents)
- سنسورهای شبکه و سایر نقاط جمع‌آوری
- جمع‌آوری تله‌متری غنی و استاندارد از محیط سازمان

۲ - لایه تحلیل (Analytics & Correlation Layer)

- تجمیع و نرمال‌سازی داده‌ها
- تحلیل رفتاری و آماری
- همبستگی رویدادها برای کشف سناریوهای حمله
- اجرای موتورهای تشخیص چندلایه و مدل‌های یادگیری ماشین

۳ - لایه مدیریت و ارائه (Management & Presentation Layer)

- داشبوردهای مدیریتی برای SOC و مدیران ارشد
- ابزارهای جست‌وجو، گزارش‌دهی و Visualization
- امکانات پاسخ به حادثه

این معماری سه‌لایه‌ای، هم با نیازهای عملیاتی SOC و هم با الزامات حاکمیتی و گزارش‌دهی سازگار است؛ به‌گونه‌ای که هم تحلیلگر فنی و هم مدیر غیر فنی بتوانند وضعیت امنیتی را در سطح مورد نیاز خود مشاهده کنند.

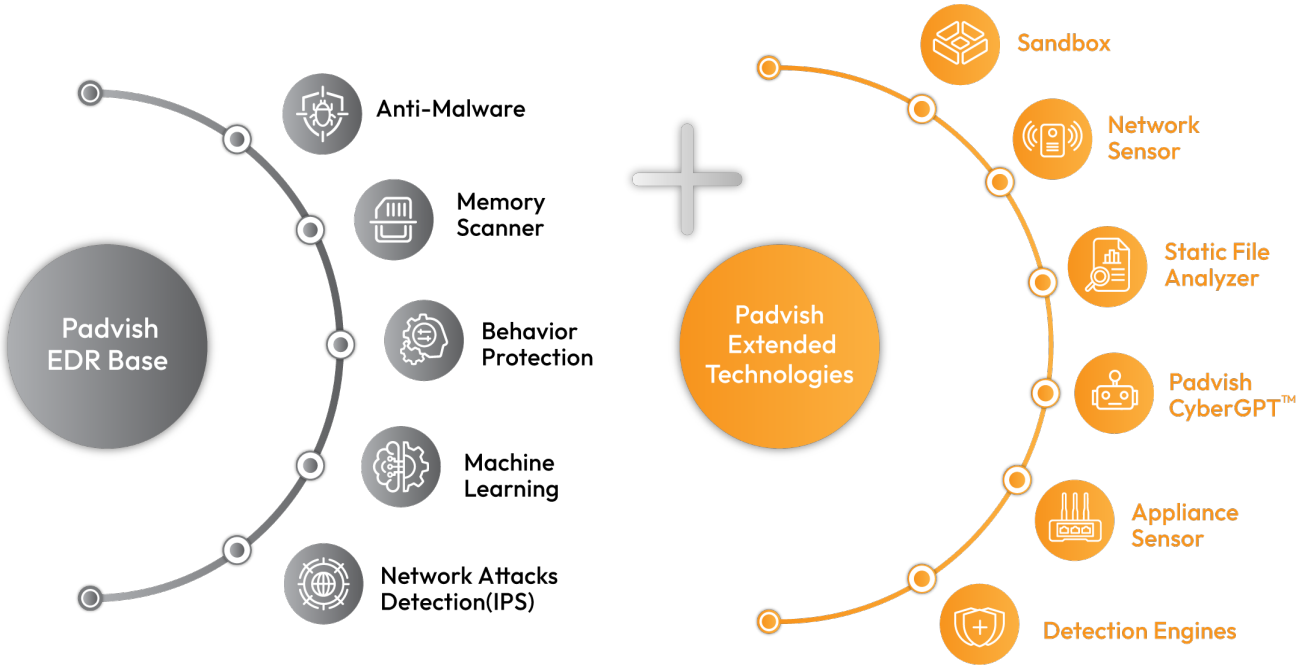
معماری استقرار (Architecture Deployment)

محصول Padvish XDR AI دارای معماری ارتباطی انعطاف‌پذیری است که در کامل‌ترین حالت، استقرار آن می‌تواند شامل لایه‌های زیر باشد:

- لایه جمع‌آوری در نقاط پایانی و شبکه؛
- هسته XDR Core Services در مرکز داده یا محیط ابری سازمان؛
- اتصال امن به ماژول‌های هوش مصنوعی مانند Padvish CyberGPT™؛
- و یک لایه ارائه برای SOC، تیم پاسخ‌گویی به حادثه و مدیران ارشد؛

این معماری امکان مقیاس‌پذیری، جداسازی منطقی و انطباق با الزامات مختلف (On prem / Hybrid) را فراهم می‌کند.

قابلیت های فنی راهکار Padvish XDR AI

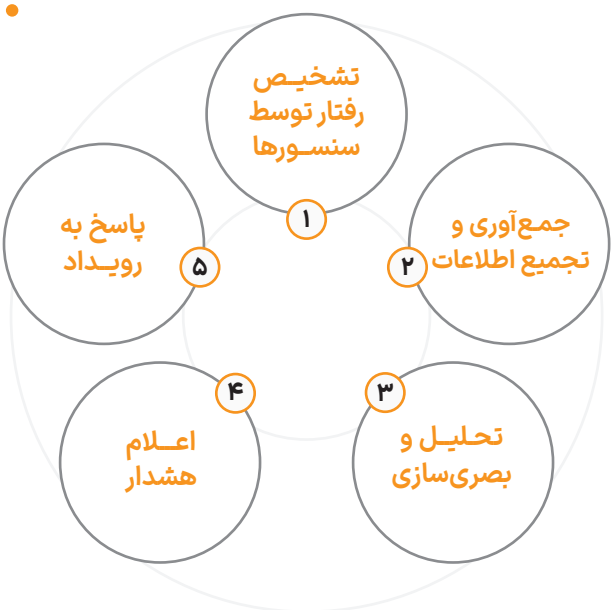


- **Anti-Malware:** برای شناسایی نشانه‌های آلودگی (IoC) مانند هش فایل‌های آلوده، دنباله‌ای از کدهای مخرب و پاسخ سریع به آن‌ها.
- **Memory Scan:** برای تشخیص و پایش حملات سایبری بر اساس تحلیل حافظه سیستم‌ها و پردازه‌های در حال اجرا.
- **Behavior Protection:** تحلیل و مانیتور رفتارهای پردازه‌های سیستم با استفاده از مجموعه سنسورها و تشخیص حملات سایبری با شناسایی الگوها و تغییرات غیرعادی.
- **Machine Learning:** به کارگیری الگوریتم‌های یادگیری ماشین به منظور شناسایی کدهای مشکوک، تهدیدات امنیتی و الگوهای غیرعادی و ناشناخته.
- **IPS:** تشخیص و محافظت از شبکه‌ها و سیستم‌ها در برابر حملات و اکسپلویت‌های شبکه‌ای از قبیل Log4j, ZeroLogon و حملات مشابه.
- **Sandbox:** تست و ارزیابی فایل‌های مشکوک در یک محیط ایزوله به منظور تعیین رفتار آن‌ها.

- **Network Sensor:** پـردازش و گـزارش تهدیـدات و حمـلات بـا بررسـی پکت‌هـای خـام ترافیـک کل شـبکه و شناسـایی حملاتـی کـه از طریـق نقـاط پایانـی فاقـد محافظـت یـا نقـاط خـارج از حیطـه مـورد مراقبـت شـبکه انجـام می‌شـوند.
- **Static File Analyzer:** تجزیـه و تحلیـل فایل‌هـا بـه منظـور شناسـایی تهدیدهـای امنیتـی و نشـانه‌های آلودگـی یـا پنهـان‌کاری و مشـخص کـردن ویژگی‌هـای ایسـتای آن‌هـا.
- **Padvish CyberGPT™:** تجزیـه و تحلیـل اطلاعـات بـا اسـتفاده از هـوش مصنوعی، ارائه خلاصـه‌ای از موضوعات و مـوارد مشـکوک و اقدامـات لازم و نیـز تحلیـل اسـکریپت‌های پیچیـده و تولیـد کوئری‌هـای شـکار تهدیـدات سایبری.
- **Appliance Sensor:** دریافـت لاگ از تجهیـزات شـبکه‌ای و زیرسـاختی، ماننـد زیرسـاخت مجازی‌سـازی، زیرسـاخت ذخیره‌سـازی، سـوییچ‌ها و روترهـا و اعـلام هشـدار در صـورت بـروز مـوارد مشـکوک و خطرنـاک.
- **Detection Engines:** ترکیـب چندیـن موتـور مختلـف تشـخیصی ماننـد آنتـی ویروس‌هـا بـرای افزایـش دقـت در تشـخیص و ردیابـی تهدیـدات امنیتـی.

چرخه عملیات امنیت

Padvish XDR AI کل چرخه امنیت را پوشش می‌دهد:



- سنسورهای نقطه پایانی و شبکه، رفتارها و رویدادها را ثبت می‌کنند.
- ماژول پاسخ‌دهی Padvish XDR با تحلیل هوشمند از طریق ایزوله‌سازی شبکه، توقف فرآیندهای مخرب و بازنشانی استراتژیک سیستم، زنجیره حمله را به‌سرعت قطع می‌کند. این راهکار با حذف کامل آثار آلودگی از حافظه و دیسک، مانع از گسترش افقی تهدیدات و نشت داده‌ها در زیرساخت می‌شود. این رویکرد عملیاتی، تاب‌آوری شبکه را در برابر پیچیده‌ترین حملات سایبری تضمین می‌نماید.
- داده‌ها در لایه تحلیل جمع‌آوری و نرمال‌سازی می‌شوند.
- سنسورهای نقطه پایانی و شبکه، رفتارها و رویدادها را ثبت می‌کنند.
- موتورهای تحلیل و همبستگی، الگوهای مشکوک را شناسایی و در قالب نمودارها، گراف‌ها و تایم‌لاین‌ها نمایش می‌دهند.

با این چرخه، سازمان از یک وضعیت واکنشی و موردی به سمت یک وضعیت پیشگیرانه و داده‌محور حرکت می‌کند.

هوش مصنوعی و Padvish CyberGPT™

نقش هوش مصنوعی در Padvish XDR AI

هوش مصنوعی در Padvish XDR AI، صرفاً یک ویژگی جانبی نیست، بلکه بخشی از هسته تصمیم‌گیری و تحلیل است. از جمله کاربردهای هوش مصنوعی در این سامانه:

- تحلیل رفتارها و رویدادها با استفاده از مدل‌های یادگیری ماشین؛
- کاهش مثبت کاذب از طریق مدل‌سازی رفتار عادی و غیرعادی؛
- اولویت‌بندی هشدارها و ریسک‌محور کردن تصمیم‌گیری؛
- پشتیبانی از تحلیلگر در فهم سریع‌تر حجم بالای داده‌ها.

Padvish CyberGPT™: دستیار هوشمند تحلیل امنیت

Padvish CyberGPT™ اولین مدل زبانی بزرگ (LLM) است که در این اکوسیستم، به‌صورت اختصاصی برای حوزه امنیت سایبری به‌کار گرفته شده است. CyberGPT:

- نه‌تنها یک ابزار پردازش متن، بلکه یک دستیار هوشمند امنیتی است که توانایی درک، تحلیل و پاسخ به چالش‌های پیچیده سایبری را دارد؛
- بستری امن برای سازمان‌ها فراهم می‌کند تا از هوش مصنوعی در تصمیم‌گیری سریع‌تر، تحلیل تهدیدات و پاسخ به حوادث بهره ببرند.

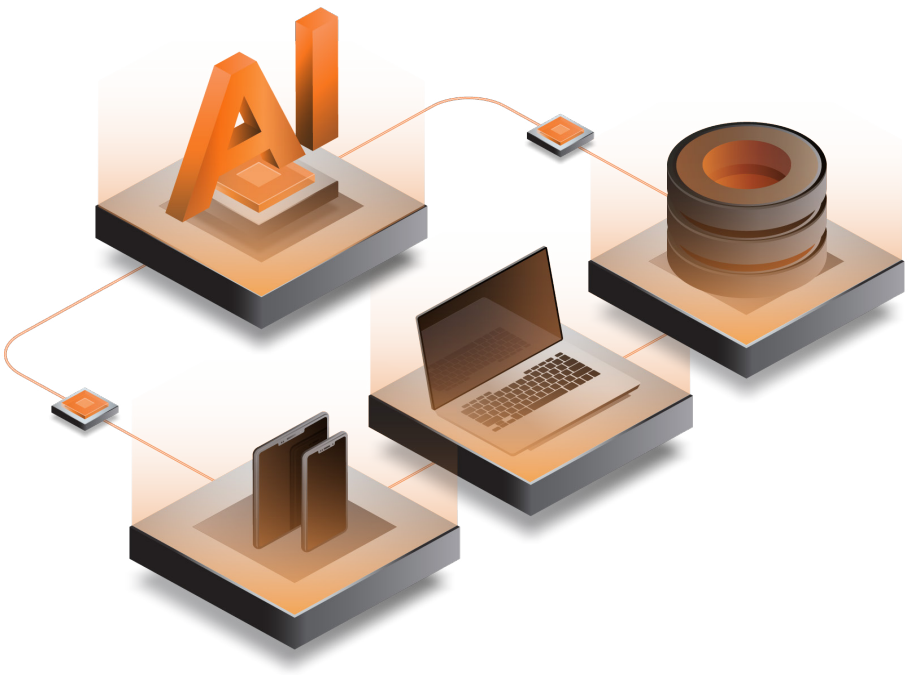
Padvish CyberGPT™ می‌تواند:

- رویدادها و لاگ‌های سامانه XDR را به زبان طبیعی تفسیر کند؛
- مفاهیم فنی و ساختار داده‌های امنیتی را برای تحلیلگر توضیح دهد؛
- تحلیل رخداد را تسریع و از وقوع حوادث ثانویه پیشگیری کند؛
- اقدامات پیشنهادی برای پاسخ به حوادث سایبری ارائه دهد؛
- فعالیت‌های مشکوک را خلاصه، اسکریپت‌های پیچیده را تحلیل و کوئری‌های Threat Hunting تولید کند.

به بیان دیگر:

Padvish CyberGPT™ فراتر از یک فناوری ساده، نقطه‌ی شروعی برای سازمان‌ها جهت پذیرش نسل بعدی سیستم‌های امنیتی است.

این دستیار هوشمند، فاصله‌ای را که معمولاً بین تیم‌های غیر متخصص، مدیران و داده‌های پیچیده امنیتی وجود دارد کاهش می‌دهد و سطح بلوغ عملیات امنیت را یک پله بالاتر می‌برد.



تأثیر Padvish XDR AI بر کارایی SOC و ارزش تجاری

از دید یک سازمان، ارزش Padvish XDR AI صرفاً در «فناوری» نیست، بلکه در تأثیر آن بر کارایی عملیاتی و مدیریت ریسک است. مهم‌ترین نتایج:

کاهش مثبت کاذب و تمرکز بر هشدارهای واقعی

تحلیلگران SOC به‌جای صرف وقت روی هشدارهای کم‌اهمیت، بر رخدادهای با ریسک بالا و واقعی تمرکز می‌کنند.

بهبود کارایی SOC

با دید یکپارچه، گردش‌کار استاندارد و تحلیل خودکار، ظرفیت مؤثر SOC بدون افزایش خطی در تعداد نیروی انسانی، افزایش می‌یابد.

افزایش سرعت و دقت در Detection، Investigation و Response

همبستگی داده‌ها، استفاده از هوش مصنوعی و راهنمایی CyberGPT باعث می‌شود زمان میان تشخیص تا مهار به‌طور محسوسی کاهش یابد.

امکان مستندسازی و گزارش‌دهی بهتر

تله‌متری غنی و دید کامل زنجیره حمله، مستندسازی حوادث و ارائه گزارش به مدیریت ارشد یا نهادهای ناظر را تسهیل می‌کند.

پشتیبانی از استراتژی امنیت داده‌محور

Padvish XDR AI برای سازمان‌هایی که می‌خواهند امنیت را به‌عنوان یک جریان داده و تحلیل مداوم ببینند، زیرساخت لازم را فراهم می‌کند.

خدمات پشتیبانی تخصصی

پادویش برای مشتریان سازمانی خود یک ساختار پشتیبانی فنی چندلایه و تخصصی فراهم کرده است تا سازمان‌ها بتوانند در کوتاه‌ترین زمان ممکن مشکلات عملیاتی، رخدادهای امنیتی و پرسش‌های فنی خود را پیگیری و حل کنند. این ساختار به گونه‌ای طراحی شده است که از پاسخ‌گویی سریع تا تحلیل فنی عمیق تهدیدات را پوشش دهد.

کانال‌های رسمی پشتیبانی

سامانه تیکتینگ پشتیبانی

ثبت، پیگیری و مدیریت درخواست‌های فنی از طریق سامانه اختصاصی:

support.amnpardaz.com

ایمیل پشتیبانی فنی

برای ارسال درخواست‌های پشتیبانی و پرسش‌های تخصصی:

support@amnpardaz.com

ساختار خدمات پشتیبانی پادویش شامل مجموعه‌ای از خدمات عملیاتی و تخصصی است، از جمله:

- پشتیبانی تلفنی ۲۴ ساعته برای مشتریان سازمانی
- پشتیبانی ایمیلی و پاسخ‌گویی فنی تخصصی
- اتصال و بررسی از راه دور برای عیب‌یابی سریع‌تر
- اعزام کارشناس فنی در موارد خاص یا پروژه‌های سازمانی

این خدمات به‌گونه‌ای طراحی شده‌اند که سازمان‌ها بتوانند پایداری عملیاتی سامانه امنیتی خود را حفظ کرده و در صورت بروز رخداد امنیتی، در سریع‌ترین زمان ممکن به راهکار مناسب دست یابند.

شماره تماس پشتیبانی: ۰۲۱-۴۳۹۱۲۰۰۰

جمع‌بندی

Padvish XDR AI با ترکیب:

- اعتبارسنجی مستقل AV-TEST و دریافت گواهی A2EDR؛
- تله‌متری عمیق و رقابت‌پذیر در سطح جهانی در حوزه EDR Telemetry؛
- معماری سه‌لایه و موتورهای تشخیص چندگانه؛
- دستیار هوشمند Padvish CyberGPT™؛
- و تمرکز بر افزایش کارایی SOC و کاهش پیچیدگی عملیاتی؛

یک راهکار Enterprise-grade برای سازمان‌هایی است که به‌دنبال افزایش مشاهده‌پذیری، کاهش ریسک و ارتقای بلوغ امنیتی خود هستند.

به زبان ساده‌ی مدیریتی:

با استقرار Padvish XDR AI، سازمان شما یک لایه دید و دفاع یکپارچه به دست می‌آورد؛

داده‌های امنیتی از حالت جزیره‌ای خارج و به یک تصویر منسجم و قابل‌اقدام تبدیل می‌شوند؛

و با بهره‌گیری از هوش مصنوعی، هیچ تهدید مهمی بدون ثبت، تحلیل و امکان پاسخ مناسب، از دید سامانه خارج نمی‌ماند.