سامانه کشف و پاسخ به تهدیدات پنهان

(پادویش EDR)

شرکت نرم افزاری امن پرداز

سطح محرمانگی: عادی

نسخه ۱.۵

پاییز ۱۴۰۴

فهرست مطالب

شکل‌ها

۱. مقدمه

با پیشرفت تهدیدات سایبری، ابزارهای سنتی جهت جلوگیری از حملات سایبری و تهدیدات جدیدی مانند APT[1]ها دیگر کارایی کافی را ندارند. مقصود از ابزارهای سنتی، طیف محصولاتی مانند آنتی‌ویروس‌ها، فایروال‌ها، سامانه‌های جلوگیری از نفوذ (IDS/IPS)، دیوار آتش وب (WAF) و هر ابزار مشابه دیگری می‌باشد که اگر چه در جای خود مفید هستند، اما برای دفاع در برابر حملات سایبری و هک و نفوذ کافی نمی‌باشند. طبیعتا به ابزارهای جدید برای مقابله با این حملات نیاز است.

برخی نواقص ابزارهای سنتی مذکور، شامل موارد زیر است:

۱. این ابزارها در دسترس مهاجمین نیز قرار دارند، لذا مهاجمین قبل از شروع حمله روش دور زدن یا از کار انداختن سامانه‌های امنیتی مانند WAF و آنتی‌ویروس را پیدا کرده و تست می‌کنند.
۲. نباید فراموش کرد که ابزارهای امنیتی در بهترین حالت یک «ابزار» هستند و نه بیشتر. نمی‌توان انتظار داشت که یک «ابزار» بتواند در برابر حملاتی که توسط یک تیم متخصص انسانی انجام می‌شود به تنهایی مقاومت کند.
۳. حجم رخدادهای در حال وقوع در هر سیستم رایانه‌ای بسیار بالاست. لذا هر ابزار امنیتی یک سطح حساسیت (Threshold) مشخص دارد که در صورتی اعلام هشدار می‌کند که درجه خطر رخدادهای کشف شده توسط سنسورهای آن بیش از سطح حساسیت تنظیم شده باشد. نفوذگران همواره تلاش می‌کنند سطح حساسیت را تشخیص داده و زیر این سطح حساسیت عمل نمایند تا هشداری صادر نشود.
۴. برخی عملیات می‌تواند جنبه دوگانه سالم/نفوذ داشته باشد که برای ابزار به تنهایی قابل کشف نیست. به عنوان مثال، در یک سناریو، ممکن است فردی پس از پنج بار تلاش با پسورد اشتباه، نهایتا روی یک سیستم با اکانت ادمین لاگین کرده و یک نرم‌افزار اسکن شبکه اجرا نماید. این سناریو هر چند مشکوک است، هم می‌تواند نتیجه رفتار یک ادمین باشد و هم عملکرد یک نفوذگر؛ و این موضوع برای ابزاری که در حال پایش سیستم است و کل این رفتار را می‌بیند قابل تشخیص نیست. بلکه نیازمند اطلاعات پیرامونی و خارج از محیط سایبری است.

[1] Advanced Persistent Threat

مقدمه

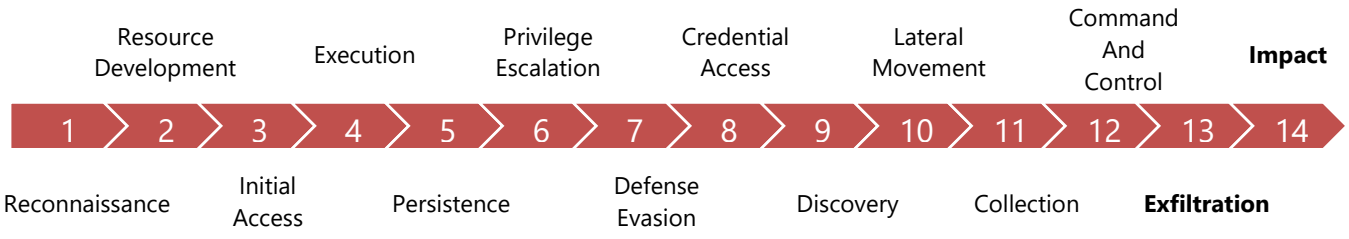
تمامی این موارد نشان می‌دهد که به ابزار(های) جدیدی برای تشخیص و مقابله با حملات سایبری نیاز است. سامانه‌های EDR[2] پاسخی به این نیاز هستند.

سامانه EDR سیستمی است که به‌منظور تامین امنیت و محافظت از نقاط پایانی[3] در یک شبکه کامپیوتری طراحی شده است. این سامانه به‌منظور تشخیص و پاسخ به تهدیدات امنیتی در دستگاه‌های نقطه پایانی نظیر کلاینت‌ها، سرورها، تلفن‌های همراه و دیگر دستگاه‌های مشابه مورد استفاده قرار می‌گیرد.

۱/۱. حملات سایبری و جایگاه EDR در مقابله با آنها

برای مقابله با حمله سایبری باید با روش تفکر یک هکر و مراحل حمله سایبری آشنا شد. مدل MITRE ATT&CK که توسط یکی از موسسات وابسته دانشگاه MIT تدوین شده است، تلاشی برای مدل‌سازی نحوه تفکر هکرها و مراحل حملات سایبری در قالب تاکتیک‌ها و تکنیک‌های مورد استفاده مهاجمین می‌باشد. این مدل در حال حاضر در دنیا مرجع تمامی مقالات و محصولات این حوزه به شمار می‌رود.

در مدل MITRE یک حمله سایبری به ۱۴ مرحله یا تاکتیک تقسیم می‌شود که یک توالی و ترتیب تقریبی دارند. اگر چه یک حمله سایبری خاص، بسته به نیت نفوذگر و شرایط شبکه مورد هدف، ممکن است یک یا چند مولفه مدل مزبور را نداشته باشد، اما به طور کلی این روش جهت مدل کردن همه حملات سایبری مفید می‌باشد.



شکل ۱ - مدل MITRE ATT&CK

در مدل MITRE هر چه در مراحل ابتدایی قرار داشته باشیم تشخیص حملات دشوارتر است و هر چه به سمت مراحل نهایی می‌رویم تشخیص ساده‌تر می‌شود. به نحوی که در مرحله ۱۴ یا Impact، دیگر حمله به نتیجه رسیده و ضربه خود را (مثلا دیفیس سایت یا تخریب اطلاعات) زده است، لذا تشخیص آن بسیار واضح است.

[2] Endpoint Detection and Response
[3] Endpoint

از طرف دیگر هر چه به مراحل نهایی نزدیک‌تر می‌شویم هزینه دفع حمله بیشتر خواهد بود. مثلا اگرچه دفع حمله‌ای که در آن نفوذگر هنوز به مرحله ۵ نرسیده با رفع آسیب‌پذیری مورد استفاده وی و یا نهایتا پاکسازی یک سیستم به سادگی انجام می‌شود، در مرحله ۱۰ یا Lateral Movement، نفوذگر نه تنها به شبکه نفوذ کرده، بلکه اطلاعات اکانت‌ها را نیز به دست آورده و بر روی تعدادی از سیستم‌ها مستقر شده است. لذا یافتن و حذف آثار حمله و تغییر پسوردها و مانند آن یک کار بسیار هزینه‌بر خواهد بود.

سامانه‌های EDR سعی می‌کنند حمله سایبری در هر مرحله‌ای که باشد شناسایی (و سپس دفع) نمایند و هر چه این تشخیص در مراحل ابتدایی باشد بهتر است. در EDR فرض بر این است که با وجود هر ابزار و هر لایه دفاعی در شبکه، باز هم احتمال هک وجود داشته و هدف تشخیص هک‌های در جریان است.

۲. معرفی سامانه EDR

کلمه EDR مخفف Endpoint Detection and Response است که به معنی تشخیص و مقابله (با تهدیدات) بر روی نقاط نهایی می‌باشد. هدف از کلمه نقطه نهایی در این تعریف، سرورها، کلاینت‌ها، دستگاه‌های موبایل، و ... با هر نوع سیستم عاملی می‌باشد. در واقع کلمه نقطه نهایی در مقابل کلمه تجهیزات شبکه قرار دارد، و در EDR با توجه به اهمیت Endpointها که در واقع هدف اصلی حملات سایبری هستند مکانیزم‌های امن‌سازی تعریف می‌شود.

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

یک سامانه EDR سه کار اصلی انجام می‌دهد: نظارت، تحلیل و پاسخ.

۲٫۱. نظارت (Monitoring)

قسمت نظارت در سامانه EDR نقش بسیار مهمی در امنیت نقاط پایانی دارد. در این بخش، سامانه EDR به نظارت و تشخیص فعالیت‌ها و رفتارهای مشکوک در دستگاه‌های نقطه پایانی می‌پردازد. فرآیند نظارت به‌منظور شناسایی تهدیدهای امنیتی و پیشگیری از وقوع حملات امنیتی صورت می‌گیرد.

معرفی سامانه EDR

سامانه EDR از داشبوردها برای نمایش تمامی رویدادها و نمودارهای مرتبط با فعالیت‌های دستگاه‌ها استفاده می‌کند. این داشبوردها به کارشناسان امنیت امکان مشاهده و پیگیری فعالیت‌های نقطه پایانی را در زمان واقعی می‌دهند.

۲/۲. تحلیل (Analyzing)

قسمت مربوط به تحلیل در سامانه EDR با استفاده از هشدارها (Alerts) به‌منظور تشخیص و اعلام هشدارهای امنیتی برحسب نشانه‌های حمله (IOA[4]) و نشانه‌های آلودگی (IOC[5]) انجام می‌شود. در این بخش، هشدارها نشانگر وقوع رویدادهای مشکوک یا وجود پتانسیل تهدیدات امنیتی در دستگاه‌های نقطه پایانی می‌باشند. سامانه EDR با استفاده از الگوریتم‌ها و الگوهای خاص به تشخیص این هشدارها می‌پردازد.

به علاوه از طریق تکنیک Threat Hunting کارشناسان امنیت می‌توانند به بررسی و شناسایی تهدیدهای ناشناخته و جدید بپردازند. ریشه و مبدا آلودگی را پیدا کنند، و جریان حمله را دنبال کرده و سیستم‌های آلوده شده را پیدا کنند.

۲/۳. پاسخ (Responding)

در سامانه EDR، قسمت مربوط به پاسخ به رخداد، شامل اقداماتی است که به‌منظور مدیریت و کنترل تهدیدات سایبری و رفع اثر آنها انجام می‌شود. در زیر توضیحاتی در مورد پاسخ‌های مختلف به تهدیدات سایبری در این قسمت آمده است:

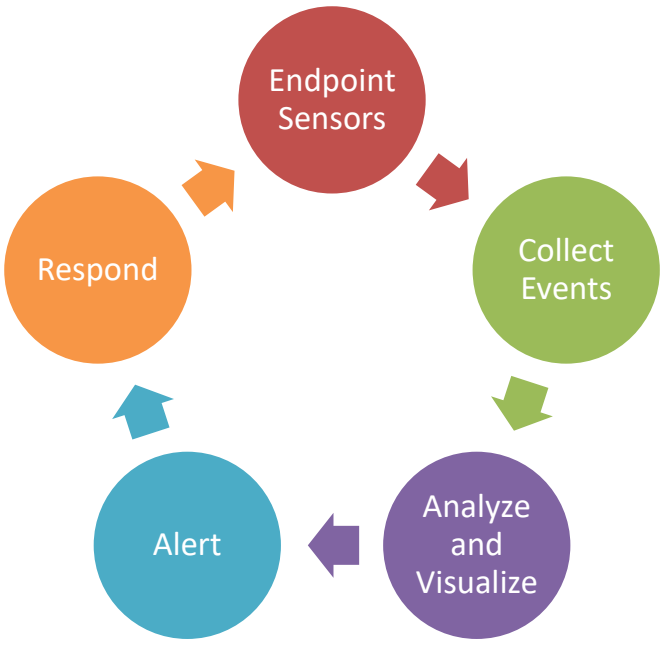
۱. **جداسازی دستگاه (Isolate)**: این عمل به معنای جدا کردن دستگاه مشکوک یا آلوده از شبکه است. سامانه EDR با انجام این دستور، دستگاه را از شبکه جدا کرده و از گسترش تهدید به دیگر دستگاه‌ها، یا ادامه دسترسی نفوذگر به سیستم مذبور جلوگیری کند.
۲. **پایان دادن به فرایند (Kill Process)**: این عمل به معنای خاتمه دادن به یک فرآیند مشکوک یا مخرب می‌باشد. سامانه EDR با اجرای این دستور، فرآیند مشکوک را متوقف و از گسترش آن جلوگیری می‌کند.

[4] Indicator Of Attack
[5] Indicator Of Compromise

۳. **راه‌اندازی مجدد (Restart)**: این عمل به معنای راه‌اندازی مجدد سیستم می‌باشد. پس از پاکسازی حمله از روی دیسک، این کار جهت رفع آلودگی‌های انجام شده در حافظه سیستم و برگرداندن سیستم به شرایط پاک انجام می‌شود.
٤. **خاموش کردن (Shutdown)**: این عمل به معنای خاموش کردن سیستم می‌باشد. در صورت تشخیص تهدیدهای فعال در حافظه، این عمل انجام می‌شود تا از گسترش تهدیدها و از دست رفتن داده‌ها جلوگیری شود.

۳. قابلیت‌های تشخیص تهدیدات Padvish EDR

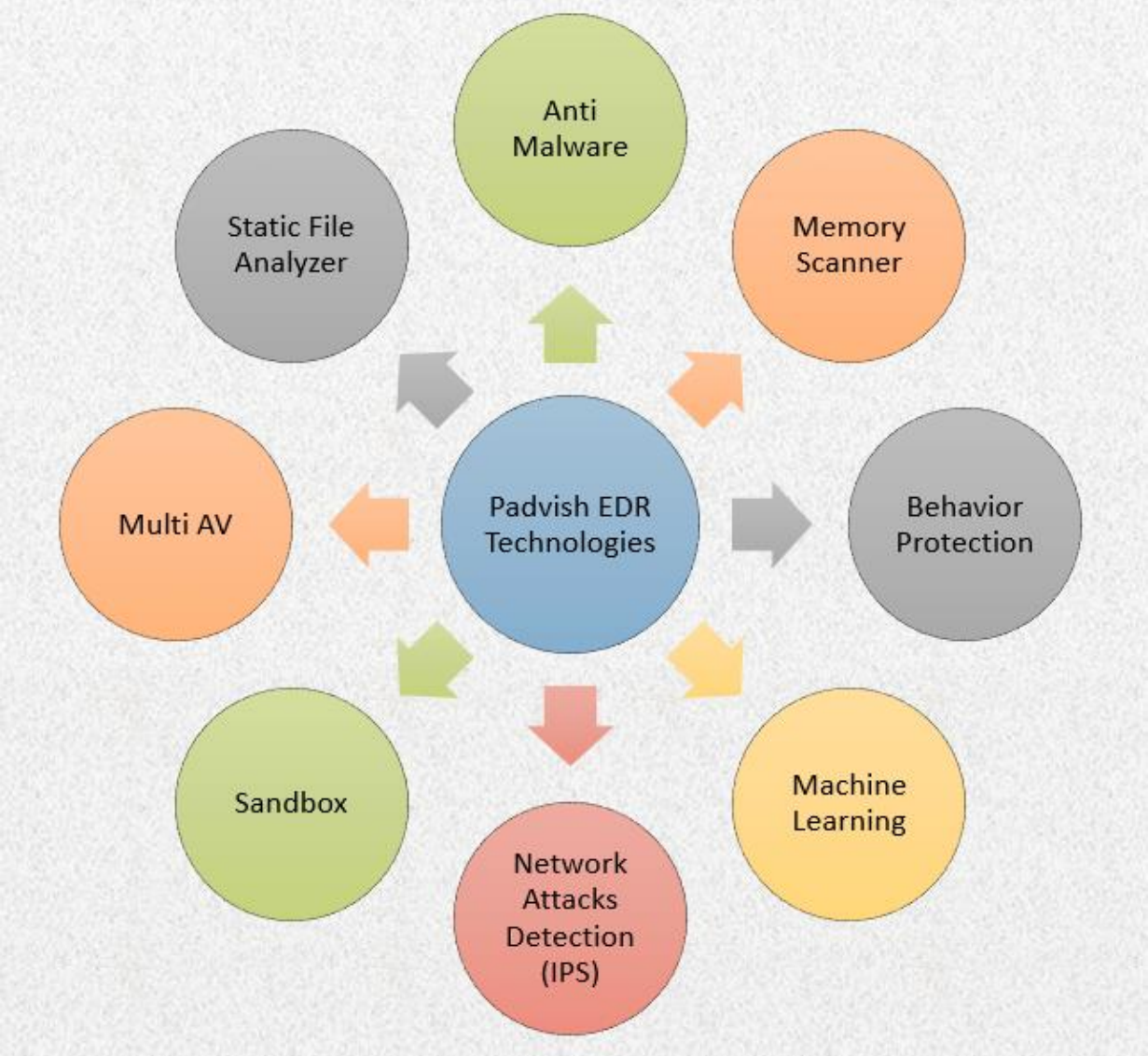
سامانه Padvish EDR کل چرخه امنیت را از تشخیص رفتار توسط سنسورهای مستقر در نقطه پایانی، جمع‌آوری اطلاعات، تحلیل و بصری‌سازی، اعلام هشدار، و پاسخ به رویداد را در بر می‌گیرد.



شکل ۲ – چرخه امنیت در سامانه Padvish EDR

قابلیت‌های تشخیص تهدیدات Padvish

Padvish EDR، شامل فناوری‌های تشخیص مختلفی می‌باشد که در ادامه به بررسی آن‌ها می‌پردازیم.



شکل ۳- بررسی تکنولوژی Padvish EDR

قابلیت‌های تشخیص تهدیدات Padvish

۱. Anti-Malware: این ماژول 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 ماژول هایی است که در سامانه Padvish EDR 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 EDR بخش محافظت رفتاری است. این ماژول در سامانه Padvish EDR 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 ماژول از الگوریتم‌های یادگیری ماشین برای تشخیص تهدیدهای امنیتی و تشخیص الگوهای غیرعادی استفاده می‌شود. سامانه Padvish EDR با استفاده از الگوریتم‌های یادگیری ماشین می‌تواند نقشه ذهنی از ویژگی‌های نرم‌افزارها بسازد و کدهای مشکوک را شناسایی کند.

۵. IPS: این ماژول 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 ماژول 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 EDR از سندباکس به‌منظور تست و ارزیابی فایل های مشکوک استفاده می‌کند. لازم به ذکر است این ماژول در نسخه Expert و Select فعال می‌باشد.

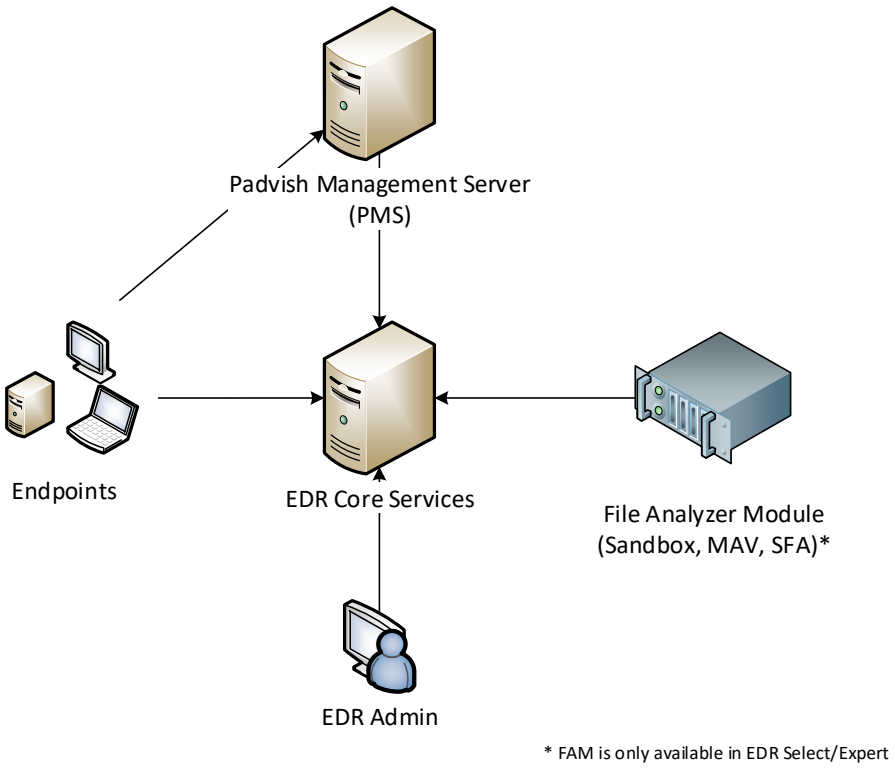
بسترهای نرم‌افزاری Padvish EDR

۷. Multi AV: این ماژول با استفاده از چندین موتور آنتی‌ویروس به تشخیص و ردیابی تهدیدات امنیتی در سامانه Padvish EDR می‌پردازد. این ماژول نیز در نسخه Expert و Select فعال می‌باشد.

۸. Static File Analyzer: این ماژول 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 نیز در نسخه Expert و Select فعال می‌باشد.

۴. بسترهای نرم‌افزاری Padvish EDR

محصول Padvish EDR مولفه‌های متعددی دارد که معماری استقرار آنها را در شکل زیر مشاهده می‌کنید:



شکل ۴- معماری Padvish EDR

۴٫۱. ماژول اصلی EDR Core Services

سرویس‌های اصلی EDR پادویش در این ماشین مجازی قرار می‌گیرند که شامل دریافت داده از سیستم کاربران، ارائه کنسول مدیریتی EDR به مدیر شبکه، و پایگاه‌های داده‌ای و سرویس‌های اختصاصی EDR 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 به این سرویس متصل می‌شوند و اطلاعات رویدادها را ارسال می‌کنند.
۲. **رابط کاربری EDR:** سرویس وب و رابط کاربری مدیریتی EDR 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 EDR جهت دریافت اطلاعات و ارسال تحلیل‌ها مورد استفاده قرار می‌گیرند. اتصال به این سرویس‌ها باید به ماژول تحلیل فایل محدود گردد.

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. کتابخانه فایل‌ها که جهت ماژول تحلیل فایل استفاده شده و به صورت فایل‌سیستمی ذخیره می‌شود.

۴٫۲. ماژول تحلیل فایل File Analysis Module

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 EDR در ارتباط می‌باشند.

بسترهای نرم‌افزاری Padvish EDR

۴/۲/۱. Multi AV

در Padvish EDR 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.

۴/۲/۲. Static File Analyzer

هنگامی که یک فایل در Padvish EDR 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.

۴/۲/۳. Sandbox

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.

۴/۳. 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 EDR در ارتباط است و وضعیت کلاینت‌ها را به آن اعلام می‌کند.

۴/۴. 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 EDR پادویش ارسال می‌کنند.

۴٫۵. دستیار هوش‌مصنوعی 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.

۵. راه‌اندازی

۵٫۱. نیازمندی‌های فنی

چک لیست زیر نشان می‌دهد که پیش از نصب، چه نیازمندی‌های فنی برای سامانه کشف و مقابله با تهدیدات پنهان (Padvish EDR)، باید فراهم گردند:

رج	نیازمندی	EDR Base/Select	EDR Expert
۱.	استقرار آخرین نسخه ایجنت و کنسول پادویش	✓	✓
۲.	استقرار سرور مرکزی Padvish EDR	✓	✓
۳.	استقرار ماژول‌های مرتبط Padvish EDR (سندباکس، تحلیل ایستا، MultiAV)	❋	✓

جدول ۳ – نیازمندی‌های فنی بهره‌برداری از خدمات مرکز کشف و پاسخ به حملات سایبری (Padvish MDR)

❋ بسته به ماژول‌های انتخابی در EDR Select متفاوت می‌باشد. در بخش‌های بعدی نیازمندی‌های سخت‌افزاری به تفکیک هر ماژول آورده شده است.

در صورت تمایل کارفرما، امکان استفاده از راهکار MDR نیز وجود دارد. برای اطلاعات بیشتر در این خصوص به سند خدمات مرکز کشف و پاسخ به حملات سایبری (Padvish MDR) مراجعه فرمایید.

۵/۲. نیازمندی‌های ارتباطی

Source	Destination	Port
Padvish Agent	EDR Core Service	**5440**
Padvish Agent	Padvish Management Server	**13911**
Padvish Management Server	EDR Core Service	**5440**
User	EDR Core Service	**80, 443**
File Analyzer Module	EDR Core Service	**SMB**
File Analyzer Module	EDR Core Service	**58XX (5800-5899)**
EDR Core Service	File Analyzer Module	**5443**
EDR Core Service	cloudcybergpt.padvish.com	**443**

۵/۳. نیازمندی سخت‌افزاری کلاینت

روی کلاینت‌ها نیازمندی سخت‌افزاری اضافه بر آنچه جهت نصب آنتی‌ویروس پادویش لازم است وجود ندارد. ماژول EDR به عنوان بخشی از آنتی‌ویروس پادویش عمل کرده و بار اضافه‌ای روی سیستم ایجاد نمی‌کند.

ارتقا کلاینت‌ها به Padvish EDR نیز به سادگی و با انتخاب کلاینت‌های مورد نظر در کنسول مدیریتی پادویش و اختصاص لایسنس انجام می‌گیرد و به هیچ عمل اضافه‌ای از قبیل نصب ماژول یا ... نیاز ندارد.

۵/۴. نیازمندی‌های سمت سرور

این نیازمندی‌ها با توجه به ماژول‌های انتخاب شده در EDR Select یا EDR Expert مشخص می‌شوند. در زیر لیست نیازمندی هر ماژول را می‌بینید، با این توضیح که در صورت انتخاب هر ماژول، نیازمندی‌ها باید با سایر نیازمندی‌ها جمع گردد.

۵/۴/۱. سامانه مرکزی EDR Base

این بسته پایه EDR بوده و فاقد ماژول‌های انتخابی می‌باشد. در صورت انتخاب ماژول‌های دیگر، میزان نیازمندی آنها نیز باید دیده شود.

راه‌اندازی

Clients	Estimated EPS	CPU(Core)	RAM (GB)	SSD(GB)	HDD(GB)	Network (Mbps)
1,000	300	4	19	10	650	2.4
2,000	600	4	20	20	1,200	4.8
5,000	1,500	5	22	50	3,000	12
10,000	3,000	6	26	100	6,000	24
20,000	6,000	8	34	200	12,000	48
50,000	15,000	14	58	500	30,000	120

۱. در شبکه‌های با تعداد کلاینت و EPS بالا لازم است از NVMe به جای SSD استفاده شود.

۲. مقادیر فوق برای حداقل سطح پایین نیازمندی شبکه تخمین زده شده است و بسته به EPS ممکن است نیاز به ارتقا و تطبیق وجود داشته باشد، **لذا توصیه می‌شود حداقل EPS چهار برابر عدد فوق در نظر گرفته شود.**

۳. مقادیر فوق برای نگهداری ۳۰ روز داده سنسورها تخمین زده شده است و نگهداری برای مدت بیشتر مستلزم افزایش ظرفیت هارد HDD است.

۵/۴/۲. ماژول File Library

Clients	FPD	RAM (GB)	CPU (Core)	HDD (GB)	Network (Mbps)
1,000	1,000	2	2	10	0.026
2,000	2,000	2	2	20	0.053
5,000	5,000	2	2	50	0.132
10,000	10,000	2	2	100	0.265
20,000	20,000	2	2	200	0.530
50,000	50,000	2	2	500	1.325

۱. مقادیر مشخصات فوق باید با مقادیر EDR Base و سایر ماژول‌های مورد استفاده جمع گردد.

۲. حجم تغییرات فایل‌های اجرایی (FPD: File Per Day) به صورت میانگین بلندمدت در شرایط معمول محاسبه گردیده است. لذا اعداد فوق باید به صورت حداقلی در نظر گرفته شوند.

۳. میزان حجم هارد مورد اختصاص برای آرشیو فایل‌ها می‌باشد و در صورتی که نیازی به آرشیو بلند مدت نباشد فایل‌های جدید جایگزین قبلی‌ها می‌شوند.

۵/۴/۳. ماژول Multi-AV

Clients	FPD	RAM (GB)	CPU (Core)	HDD (GB)	Network (Mbps)
10,000	14,400	2	2	25	–
20,000	28,800	4	4	50	–
50,000	72,000	10	10	125	–

۱. این مقادیر به ازای هر آنتی‌ویروس باید تکرار شود. اگر از هر ۶ آنتی‌ویروس استفاده می‌شود باید ضربدر ۶ گردد.

۲. مقادیر مشخصات فوق باید با مقادیر EDR Base و سایر ماژول‌های مورد استفاده جمع گردد.

۳. حجم تغییرات فایل‌های اجرایی (FPD: File Per Day) به صورت میانگین بلندمدت در شرایط معمول محاسبه گردیده است. لذا اعداد فوق باید به صورت حداقلی در نظر گرفته شوند.

٤. این ماژول باید با ماژول File Library استفاده گردد و هر FPD برای آن ماژول در نظر گرفته می‌شود در این خصوص نیز اعمال گردد.

۵/۴/۴. ماژول File Static Analyzers

Clients	FPD	RAM (GB)	CPU (Core)	HDD(GB)	Network (Mbps)
10,000	144,000	2	1	25	–
20,000	288,000	4	2	50	–
50,000	720,000	10	5	125	–

۱. مقادیر مشخصات فوق باید با مقادیر EDR Base و سایر ماژول‌های مورد استفاده جمع گردد.

۲. حجم تغییرات فایل‌های اجرایی (FPD: File Per Day) به صورت میانگین بلندمدت در شرایط معمول محاسبه گردیده است. لذا اعداد فوق باید به صورت حداقلی در نظر گرفته شوند.

۳. این ماژول باید با ماژول File Library استفاده گردد و هر FPD برای آن ماژول در نظر گرفته می‌شود در این خصوص نیز اعمال گردد.

۵/۴/۵. ماژول SandBox

Clients	FPD	RAM (GB)	CPU (Core)	HDD(GB)
1,000	1,000	6	4	45
2,000	2,000	8	6	70
5,000	5,000	14	12	145
10,000	10,000	24	22	270
20,000	20,000	44	42	520
50,000	50,000	104	102	1,270

۱. مشخصات فوق در قالب مشخصات ماشین فیزیکی (هاست) مورد نیاز می‌باشد. **حداقل نیازمندی سخت‌افزاری سرور HP G9 DL380 (نسل ۹) می‌باشد.**

۲. مقادیر مشخصات فوق باید با مقادیر EDR Base و سایر ماژول‌های مورد استفاده جمع گردد.

۳. این ماژول باید با ماژول File Library استفاده گردد.

٤. اعداد جدول یک برآورد منطقی و معمول می‌باشد. ارسال فایل به سندباکس بر اساس نظر ادمین صورت می‌گیرد و لذا در صورت نیاز می‌توانید ماشین قوی‌تر یا ضعیف‌تر از سطر مربوط به خود را انتخاب نمایید.

۶. جمع‌بندی

در این سند محصول Padvish EDR، ویژگی‌ها، معماری، و نیازمندی‌های آن معرفی گردید. از آنجاکه استفاده از محصولات EDR 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 MDR) امکانی را فراهم می‌کند که سازمان با حداقل هزینه خود را در برابر حملات سایبری مقاوم نماید.

جمع‌بندی

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 MDR) 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 «راهکار کشف و پاسخ به حملات سایبری (پادویش MDR)» را مطالعه بفرمایید.

شرکت نرم افزاری امن پرداز®
Amnpardaz Software Corporation®
www.amnpardaz.com