BARDIN GATE

انتقال امن داده میان شبکه‌های ایزوله

ARP

AIR-GAP REGULATED PIPELINE

2U اپلاینس رک‌مونت

بازرسی محتوا و قرنطینه: هیچ فایلی بدون بررسی عبور نمی‌کند

هر فایل پیش از هر حرکتی دو مرحله‌ی جدا را می‌گذراند: اعتبارسنجی قطعی و بازرسی با موتور. هر بررسی فقط «بله» یا «نه» می‌گوید و با نسخه‌ی دقیق ابزارش ثبت می‌شود.

در این کاتالوگ: هفده قاعده‌ی اعتبارسنجی، سه موتور بازرسی، صدور حکم، قرنطینه و شواهدی که می‌ماند

برای: متخصصان امنیت که بررسی محتوا را ارزیابی می‌کنند

https://www.bardin.tech/fa/bardingate-arp/

ARP نام فایل، پسوند، نوع اعلام‌شده، ساختار آرشیو و خروجی موتورها را همه ورودیِ مخرب می‌داند. بررسی فقط روی بایت‌هایی انجام می‌شود که هنگام پذیرش Hash شده‌اند و درون خودِ دستگاه نشسته‌اند، نه روی فایل مبدأ که بیرون از مرز اعتماد است.

دو شبکه‌ی شما از هم جدا می‌مانند و هیچ اتصال فیزیکی میانشان برقرار نمی‌شود؛ اپلاینس رک‌مونت 2U در هر لحظه فقط به یکی از آن‌ها وصل است.

۲	۱۷	۴	۰
مرحله‌ی جدا: اعتبارسنجی، بازرسی	قاعده‌ی اعتبارسنجی قطعی	موتور بازرسی: DLP، ClamAV، YARA، هوش مصنوعی	بایتِ تغییرکرده در فایل تحویلی

دو مرحله، دو ماهیت

اعتبارسنجی قطعی

ورودی یکسان، نتیجه‌ی یکسان. می‌پرسد «فایل همان است که ادعا می‌کند و در حدِ پذیرش این مسیر است؟» نخست اجرا می‌شود تا آرشیو مخرب به هیچ موتوری نرسد.

بازرسی با موتور

وابسته به امضا و قاعده‌ی نصب‌شده: «آیا در فایل چیزی هست که اجازه‌ی عبورش را نداریم؟» هر موتور در هر مسیر الزامی یا اختیاری است و نسخه‌اش با نتیجه ثبت می‌شود.

بله یا نه، و هیچ حالت سوم

بررسی‌ای که اجرا شد پاسخ دارد. بررسی‌ای که اجرا نشد (موتور خراب شد، مهلت گذشت) درباره‌ی فایل چیزی نمی‌گوید؛ این شکست سازوکار است و **هرگز قرنطینه نیست**.

هفده قاعده‌ی اعتبارسنجی

گروه	قاعده‌ها	جلوگیری از
نام	IllegalChars · FilenameLength · MultiExtension · ReservedNames · PathTraversal	نام‌هایی که خراب می‌کنند، گمراه می‌کنند یا از فایل‌سیستم مقصد بیرون می‌زنند؛ از جمله نام دستگاه‌های رزرو و دنباله‌ی پیمایش مسیر.
نوع	ExtensionBlocklist · ExtensionAllowlist · MimeDetect · MimeExtensionMatch	محتوایی که از نوعِ پذیرفته‌شده نیست، یا نوع تشخیص‌داده‌شده‌اش با پسوند نمی‌خواند.
اندازه	MaxFileSize	فایل‌های بزرگ‌تر از ظرفیتی که مسیر و دستگاه برایش تدارک دیده‌اند.
آرشیو	ArchiveEntryCount · ArchiveDepth · ArchiveSymlink · ArchivePathTraversal · ArchivePasswordProtected	بمب آرشیو، فایل‌هایی که از پوشه‌ی استخراج بیرون می‌زنند، پیوندهای رو به بیرون و محتوای رمزگذاری‌شده‌ای که قابل بازرسی نیست.
محتوای فعال	OfficeActiveContent · PdfActiveContent	سندهایی که اسکریپت یا ماکروی نهفته دارند.

«رمزگذاری‌شده» یعنی «قابل بازرسی نیست»، نه «مخرب»

آرشیو رمزدار مخرب قلمداد نمی‌شود؛ محتوایی است که هیچ موتوری درونش را نمی‌بیند. مسیری که چنین آرشیوی را بپذیرد، تصمیمی آگاهانه گرفته است.

چهار موتور بازرسی

DLP

چهار خانواده آشکارساز: الگو، فرهنگ‌واژه، برچسب و آنتروپی. فقط آشکار می‌کند، ماسک یا ویرایش نمی‌کند، و عمداً امتیازدهی یادگیری‌ماشینی ندارد؛ نتیجه باید بازتولیدپذیر و قابل توضیح باشد.

ClamAV

تشخیص بدافزار با امضا؛ مجموعه‌ی امضا بسته‌ی امضاشده‌ی آفلاین است و نسخه‌اش با هر نتیجه ثبت می‌شود.

YARA

قاعده‌های شناسایی تهدید و محتوای ممنوع؛ مجموعه‌ی امضاشده، فعال‌سازی اتمی و بدون اختلاط نسخه.

مدل هوش مصنوعی

روی خود دستگاه و بی‌اتصال، آنچه را قاعده‌های ثابت رد نکرده‌اند بررسی می‌کند. می‌تواند فایلی را نگه دارد، اما هرگز نمی‌تواند فایلی را عبور دهد؛ نسخه‌اش با هر نتیجه ثبت می‌شود.

حکم: از شواهد تا نتیجه

آنچه یافت شد	نتیجه
یافته‌ی با شدت CRITICAL، HIGH یا MEDIUM	علیه محتوا حکم داده شد: قرنطینه
مدل هوش مصنوعی فایل را مخرب یا نابه‌جا تشخیص دهد	علیه محتوا حکم داده شد: قرنطینه
فقط یافته‌ی LOW یا INFO	عبور
بدون یافته، همه‌ی موتورهای الزامی کامل شدند	عبور
موتور الزامی کامل نشد، در دسترس نبود یا تلاش‌هایش تمام شد	ناموفق (شکست سازوکار)، نه قرنطینه

قرنطینه پایانی است

فایل قرنطینه‌شده هرگز تحویل نمی‌شود. در چند جای مستقل اعمال می‌شود تا یک اشتباه آن را باز نکند: خود روند دستگاه هیچ راهی از قرنطینه به بیرون ندارد، رابط REST راهی برای آزادسازی ندارد، فهرست مجوزها مجوز آزادسازی ندارد و صفحه‌ی قرنطینه‌ی کنسول دکمه‌ی آزادسازی ندارد.

اپراتور چه می‌تواند و چه نمی‌تواند

کار	امکان
دیدن همه‌ی موردهای مهارشده با مسیر، دلیل و شواهد کامل	بله
خروجی گزارش فراداده و شواهد	بله؛ هرگز محتوا
حذف زودهنگام محتوای مهارشده	بله، با ثبت دلیل در ممیزی
خواندن یا دانلود محتوای مهارشده	نه؛ هیچ مسیری وجود ندارد
آزادسازی، رد حکم یا بازپردازش	نه

اپراتور برای فهمیدن و اطلاع‌رسانی است، نه برای نقض حکم. فایلی که به اشتباه قرنطینه شده، با گفت‌وگو با مالک سیستم تولیدکننده و در صورت اشتباه‌بودن سیاست، با تغییر ممیزی‌شده‌ی سیاست حل می‌شود؛ سپس مبدأ دوباره می‌فرستد.

چیزی برای تنظیم دائمی نیست

پروفایل را یک‌بار برای مسیر برمی‌گزینید و بررسی‌ها خودکار اجرا می‌شوند. امضاها و قاعده‌ها با یک بسته‌ی داده‌ی امضاشده و آفلاین به‌روز می‌شوند، بی‌آنکه نرم‌افزار عوض شود.

⚠ چهار پایان غیرعادی، چهار مسئول

پایان	معنا	پاسخ‌گو
QUARANTINED	بازرسی محتوا علیه فایل حکم داد.	محتوا: سیستم تولیدکننده چیزی فرستاده که این مسیر نمی‌پذیرد.
REJECTED	تأییدکننده رد کرد یا تا مهلت کسی تصمیم نگرفت.	فرایند: یک نفر نپذیرفت یا سازمان اقدام نکرد.
FAILED	یک سازوکار شکست خورد و تلاش‌ها تمام شد.	دستگاه یا محیط: میزبان، موتور یا ظرفیت.
تحویل شد، تسویه نشد	فایل رسید ولی حذف یا بایگانی اصل در مبدأ ناموفق بود.	سیستم مبدأ.

چون این چهار را با هم «خطا» نشمرده‌ایم، اپراتور سیگنال را می‌بیند: افزایش FAILED یعنی دستگاه را درست کنید، افزایش QUARANTINED یعنی با تولیدکننده صحبت کنید، و افزایش REJECTED به‌علت انقضا یعنی کسی صف تأیید را نگاه نمی‌کند.

☰ شواهد؛ آنچه می‌ماند

هر اجرا یک رکورد ثابت می‌سازد

- چه چیزی اجرا شد و با چه نسخه‌ای
- روی کدام نسخه‌ی مجموعه‌ی امضا
- حکم، کد دلیل و یافته‌های محدود
- حتی اجراهایی که کامل نشدند

آنچه هرگز نگه داشته نمی‌شود

- متنِ تطبیق‌خورده بیش از یک زمینه‌ی محدودِ ماسک‌شده
- متن امضا یا قاعده
- خروجی خام موتور و ردّ پشته
- مسیر مطلق میزبان

فایلی که رد شد هرگز عبور نمی‌کند و فایلی که بررسی نشد هرگز «پاک» گزارش نمی‌شود.

کاتالوگ‌های دیگر این محصول

کاتالوگ ۱	کاتالوگ ۲	کاتالوگ ۴
معرفی محصول	مسیر و سیاست	امنیت و بهره‌برداری

برای مشاوره، درخواست نمایش و اطلاعات تماس:
https://www.bardin.tech/fa/bardingate-arp/

مشخصات ممکن است بدون اطلاع قبلی تغییر کند.