



## ART

AIR-GAP REGULATED TRANSFER



2U اپلاینس رک مونت

## تضمین محتوا: از ادعا تا شاهد، پیش از هر تحویل

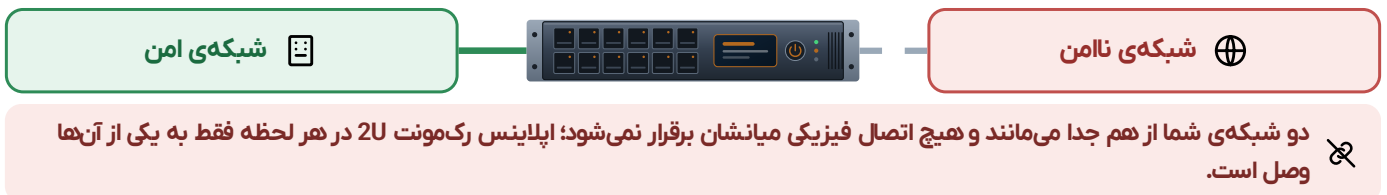
هر ادعای Agent، فایل و فراداده مخرب فرض می‌شود. تصمیم فقط روی بایتهای رسیده، با شاهد مشخص و نسخه‌ی مشخص گرفته می‌شود.

برای: متخصصان امنیت

در این کاتالوگ: ده گام بررسی به ترتیب، اعتبارسنجی، ضدبدافزار بدون اینترنت، و اینکه چرا هر چیز ناشناخته انتقال را متوقف می‌کند

<https://www.bardin.tech/fa/bardingate-art/>

ART هرگز نمی‌پذیرد که «فایل همان است که گفته می‌شود». ادعای Agent فقط برای رد زود هنگام موارد آشکارا ممنوع به کار می‌رود و هیچ‌گاه جای بررسی نهایی را نمی‌گیرد؛ حکم نهایی را همیشه خود دستگاه روی بایتهای ذخیره شده می‌دهد.



## ده گام، به ترتیب

- ادعای اعلام شده**  
رد ارزان موارد ممنوع پیش از دریافت. موقت است.
- گواهی بیرونی**  
گواهی امضاشده‌ی سامانه‌ی خود سازمان، پیش از دریافت.
- یکپارچگی ماندگار**  
SHA-256 روی فایل ذخیره شده دوباره محاسبه می‌شود.
- واقعیت‌های مشاهده شده**  
اندازه، نوع MIME و ساختار آرشو یا سند؛ یکبار استخراج و مشترک.
- ادعا در برابر مشاهده**  
ناهمخوانی خودش شاهد است؛ ادعا هرگز مشاهده را کنار نمی‌زند.
- قاعده‌های اعتبارسنجی**  
قاعده‌های بی‌حالت روی یک بافتار تغییرناپذیر.
- اعتبارسنجی ساخت یافته**  
JSON Schema، XSD 1.0، 2020-12، CSV و قید فیلد.
- امضای bg-sign**  
امضای جداگانه‌ی صاحب فایل، بررسی شده روی بایتهای رسیده.
- بازرسی**  
موتورهای ClamAV و YARA و مدل هوش مصنوعی، هر کدام در محیطی ایزوله.
- جمع بندی سیاست**  
اجازه، رد، قرنطینه یا تأیید؛ فقط سیاست حکم می‌دهد.



## هیچ قاعده یا موتوری خودش حکم نمی‌دهد

قاعده و موتور فقط یافته ثبت می‌کنند. حکم را سیاست می‌دهد و وضعیت انتقال را روند ثابت دستگاه تعیین می‌کند؛ پس هیچ اسکرن، خواننده‌ی فایل یا رابط کاربری نمی‌تواند چیزی را «پاک» اعلام کند.

## ✓ اعتبارسنجی؛ آنچه واقعاً بررسی می‌شود

| حوزه              | کنترل‌ها                                                                                                                                               |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| نوع و نام         | پسوند و MIME دو شاهد مستقل‌اند و ناهمخوانی‌شان صریح و تحت سیاست است؛ تغییر نام فایل، نوع مشاهده‌شده را عوض نمی‌کند.                                    |
| آرشیو             | عمق تو در تو، شمار عضوها، حجم بازشده، نسبت فشرده‌سازی، عضو رم‌دار، پیمایش مسیر، پیوند نمادین و ساختار خراب. تخطی از حد، بدون استخراج ناایمن رد می‌شود. |
| Office و PDF      | در محیطی ایزوله بررسی می‌شود: محتوای فعال، ارتباط بیرونی، ماکرو، بخش خراب و شکست در خواندن فایل، هر کدام یافته‌ای جدا ثبت می‌شود.                      |
| داده‌ی ساخت‌یافته | JSON Schema 2020-12، XSD 1.0، طرح بسته‌ی CSV و قیده‌ای ساده و قطعی فیلد. اینها اعتبارسنجی‌اند، نه DLP.                                                 |
| ظرفیت             | هر مرحله حد زمان، حافظه و خروجی دارد. تمام‌شدن منبع یا شکست در خواندن فایل «نامعلوم» است و فایل عبور نمی‌کند.                                          |

## 🔍 نمونه: فایل «PDF» که PDF نیست

فایلی که پسوندش pdf است ولی بایتهایش PDF نیست، بر پایه‌ی بایتهای مشاهده‌شده ارزیابی می‌شود و ناهمخوانی ادعا/مشاهده را به‌عنوان شاهد ثبت می‌کند؛ موفقیت پیشاپیش Agent نمی‌تواند این را معتبر کند.

## 🔄 شاهد تغییرناپذیر است و بازارزیابی، افزودنی

- هر ارزیابی به محتوای دقیق، پیکربندی، تصویر سیاست، پروفایل، نسخه‌ی قاعده‌ها و نسخه‌ی ورودی بسته است. انتشار پیکربندی تازه، شاهد انتقال ضابطه‌مند را بازنویسی نمی‌کند.
- بازارزیابی مجاز، نسل تازه‌ای می‌سازد که به نسل قبل پیوند دارد و ممیزی می‌شود؛ نسل قبل می‌ماند.

## ClamAV و YARA، آفلاین



### پردازش ایزوله

clamd بدون دسترسی root و فقط روی سوکت محلی (بدون TCP)؛ YARA با تعداد محدودی پردازش همزمان، هر بار یک فایل.



### یک صف ماندگار

پذیرش، پایداری، بازیابی پس از ریاستارت و فشار معکوس در یک صف مشترک است؛ صف مخفی در موتورها نیست.



### مجموعه‌ی امضاشده

امضا و قاعده‌ها بسته‌ی امضاشده، نسخه‌دار و تغییرناپذیرند، اتمی فعال می‌شوند و نسخه‌شان با هر نتیجه ثبت می‌شود.

## امضای bg-sign

صاحب فایل می‌تواند امضای جداگانه‌ی خود را در یک ویژگی فایل سیستم بگذارد. Agent آن را فقط حمل می‌کند و ادعایش مخرب فرض می‌شود؛ دستگاه کلید عمومی، اختیار امضاکننده و خود امضا را روی SHA-256 فایل رسیده بررسی می‌کند. کلید خصوصی امضا هیچ‌گاه به دستگاه نمی‌رسد.

اگر سیاست امضای معتبر بخواهد، امضای ناموجود، نامعتبر، ناپشتیبانی‌شده، نامطمئن یا نامعلوم هر کدام وضعیت جداگانه دارد و انتقال پیش نمی‌رود.

## گواهی بیرونی سازمان

سازمان می‌تواند بخواهد سامانه‌ای از خودش پیش از حمل فایل نظر بدهد. این گواهی‌دهنده بیرون از دستگاه است و Agent فقط پیک است؛ دستگاه تصدیق می‌کند. نتیجه پیش از دریافت محتوا اثر می‌کند و هیچ‌گاه بررسی‌های خود ART را سست نمی‌کند: گواهی «پذیرش» هم فایل را معتبر نمی‌کند.

- هاش گواهی‌شده دو بار با هاش فایل مقایسه می‌شود؛ بار دوم پیش از ثبت رسید ماندگار. گواهی یک فایل نمی‌تواند فایل دیگری را وارد کند.
- نبودن گواهی و نامعتبربودن آن دو چیز متفاوتند؛ گواهی نامعتبر در هر حالتی رد می‌کند.

یافته‌ی قطعی (FOUND در ClamAV، MATCH در YARA، رد اعتبارسنجی) دوباره امتحان نمی‌شود تا موتور یا قاعده‌ی ضعیف‌تری آن را عوض کند؛ خرابی، مهلت یا پاسخ مخدوش موتور، «نامعلوم» است و انتقال جلو نمی‌رود.

### ❖ چیزی برای تنظیم دائمی نیست

سیاست مشخص می‌کند کدام بررسی‌ها اجرا شوند و بررسی‌ها خودکارند. امضاها و قاعده‌ها با یک بسته‌ی داده‌ی امضاشده و آفلاین به‌روز می‌شوند، بی‌آنکه نرم‌افزار عوض شود.



## هر چیز نامعلوم، انتقال را متوقف می‌کند

| وضعیت                                                     | رفتار                                       |
|-----------------------------------------------------------|---------------------------------------------|
| موتور در دسترس نیست، خراب شد، مهلت گذشت یا پاسخ مخدوش داد | نامعلوم؛ انتقال پیش نمی‌رود                 |
| مجموعه‌ای امضا یا قاعده با موتور ناسازگار است             | دستگاه «آماده» نمی‌شود؛ پذیرش متوقف می‌ماند |
| شاهد لازم موجود نیست یا نسخه‌اش ناشناخته است              | رد؛ هرگز عبور بی‌صدا                        |
| حد آرشو یا منبع رد شد                                     | رد بدون استخراج نایمن                       |
| یافته‌ی قطعی بدخواهانه                                    | قرنطینه؛ بدون تلاش مجدد با ابزار ضعیف‌تر    |

## جدا از فایل اصلی، همیشه

- خروجی خام موتور، رمز، متن قاعده‌های بدون محدودیت و محتوای فایل در ممیزی یا پیام خطای کاربر نمی‌آید.
- فرستنده فقط نتیجه و شناسه‌ی پیگیری می‌گیرد؛ نقش مجاز با همان شناسه، شواهد را در کنسول می‌بیند. بدین ترتیب پاسخ، راهنمای مهاجم نمی‌شود.
- پیش‌نمایش ایمن فقط صفحه‌های PNG ساخته‌شده در محیطی ایزوله را نشان می‌دهد؛ فایل اصلی هیچ‌گاه به مرورگر نمی‌رسد.

## آنچه آزمایش می‌شود

- ردیف‌شدن مراحل، یکتایی نتیجه و ثبات معنای حکم با هر ترتیب و هم‌زمانی قاعده‌ها.
- رایستارت وسط بازرسی یک کار ماندگار نگه می‌دارد و حکم تکراری نمی‌سازد؛ مجموعه‌ای امضا هرگز در یک تلاش با نسخه‌ی دیگر مخلوط نمی‌شود.

## چیزی که نتوانست درستی‌اش را ثابت کند، عبور نمی‌کند؛ و آنچه عبور کرد، اثبات دارد.

کاتالوگ‌های دیگر این محصول

کاتالوگ ۴

امنیت و بهره‌برداری

کاتالوگ ۲

تجربه‌ی کاربر

کاتالوگ ۱

معرفی محصول



برای مشاوره، درخواست نمایش و اطلاعات تماس:

<https://www.bardin.tech/fa/bardingate-art/>

مشخصات ممکن است بدون اطلاع قبلی تغییر کند.