



ART

AIR-GAP REGULATED TRANSFER



جهاز 2U يُركب في الحامل

فحص المحتوى: من الادعاء إلى الدليل، قبل أي تسليم

يُفترض أن كل ادعاء من الوكيل وكل ملف وكل بيان وصفي معادٍ. والقرار لا يستند إلا إلى البايئات المستلمة، مع أدلة مسماة وإصدارات مسماة.

لمن: متخصصو الأمن

في هذا الكتالوج: الفحوص العشرة بالترتيب، والتحقق، ومكافحة البرمجيات الخبيثة دون اتصال، ولماذا يوقف أي شيء مجهول النقل

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

لا يقبل ART أبدًا أن الملف هو ما يقال إنه هو. فادعاء الوكيل لا يفيد إلا في رفض المحظور الواضح مبكرًا، ولا يحل محل الفحص النهائي أبدًا؛ والجهاز يصدر دائمًا الحكم النهائي على البايئات المخزنة.

الشبكة الآمنة



الشبكة غير الآمنة

تبقى شبكتك منفصلتين ولا تتصلان ببعضهما ماديًا أبدًا؛ وجهاز 2U متصل بإحدهما فقط في أي لحظة.

عشر خطوات، بالترتيب

١

البيانات الوصفية
المعلنة

رفض مبكر رخيص قبل
الاستلام. مؤقت.

٢

الشهادة الخارجية

بيان موقع من نظامك أنت،
قبل الاستلام.

٣

سلامة دائمة

يُعاد حساب SHA-256
على الملف المخزن.

٤

الحقائق المرصودة

الحجم، ونوع MIME،
وبنية الأرشيف والمستند؛
تُستخرج مرة واحدة
وتُشارك.

٥

المعلن مقابل المرصود

عدم التطابق دليل؛
والادعاء لا يتغلب أبدًا على
المرصود.

٦

قواعد التحقق

قواعد دون حالة على
سياق واحد غير قابل
للتغيير.

٧

تحقق منظّم

JSON Schema
XSD 1.0 و 2020-12
و CSV وقيود الحقول.

٨

توقيع bg-sign

توقيع صاحب الملف
المنفصل، يُتحقق منه على
البايئات المستلمة.

٩

الفحص

YARA و ClamAV
ونموذج الذكاء الاصطناعي
في عمليات معزولة.

١٠

تجميع السياسة

سماع، أو رفض، أو حجر،
أو موافقة؛ والسياسة
وحدها تقرر.



لا قاعدة ولا محرك يحكم وحده

القواعد والمحركات لا تفعل إلا جمع الأدلة. السياسة وحدها تقرر، ولا يغيّر حالة النقل إلا العملية الثابتة في الجهاز، فلا يستطيع ماسح أو قارئ ملفات أو واجهة أن يعلن أي شيء سلباً.

✓ التحقق: ما الذي يُفحص فعلاً

المجال	الضوابط
النوع والاسم	الامتداد ونوع MIME دليان مستقلان؛ وعدم التطابق صريح وتتحكم فيه السياسة، وإعادة التسمية لا تغيّر النوع المرصود أبداً.
الأرشفات	عمق التداخل، وعدد المداخل، والحجم بعد الفك، ونسبة الضغط، والمداخل المشفرة، واجتياز المسارات، والروابط، والبنية المشوّهة. وتجاوز أي حد يؤدي إلى الفشل دون أي استخراج غير آمن.
Office و PDF	تُفحص في عملية معزولة: المحتوى النشط، والعلاقات الخارجية، ووحدات الماكرو، والأجزاء المشوّهة، والعجز عن قراءة الملف، ويُسجّل كل منها نتيجةً.
البيانات المنظّمة	JSON Schema 2020-12، وXSD 1.0، ومخطط CSV مغلق، وقيود حتمية بسيطة على الحقول. وهذه تحقق، لا DLP.
الموارد	لكل مرحلة حدود للوقت والذاكرة والمخرجات. ونفاد الموارد أو العجز عن قراءة الملف نتيجة غير حاسمة، ولا يمر الملف.

🔍 مثال: «PDF» ليس PDF

الملف المسمى pdf وبايتاته ليست PDF يُقيّم من المحتوى المرصود ويُسجّل عدم التطابق بين المعلن والمرصود دليلاً؛ ولا يستطيع مرور مبكر من الوكيل أن يجعله صالحاً.

↻ الأدلة غير قابلة للتغيير وإعادة التقييم إضافة

- كل تقييم مربوط بالمحتوى والإعدادات ولقطة السياسة والملف وإصدارات القواعد وإصدار المدخل بالضبط. ونشر إعدادات جديدة لا يعيد كتابة أدلة نقل خاضع للضوابط أبداً.
- إعادة التقييم المشروعة تنشئ جيلاً جديداً يرتبط بالسابق ويُسجّل في التدقيق؛ ويبقى السابق.

ClamAV وYARA، دون اتصال



عمليات معزولة

clamd دون root على مقبس محلي (دون TCP)؛ YARA بعدد محدود من العمليات المتوازية، ملفًا واحدًا في كل مرة.



طابور دائم واحد

القبول والحفظ والاسترداد بعد إعادة التشغيل والضغط العكسي في طابور مشترك واحد؛ ولا طوابير مخفية داخل المحركات.



مجموعات موقعة

التوقييع والقواعد موقعة، وذات إصدارات، وغير قابلة للتغيير، وتُفَعَّل تفعيلاً ذرياً، وتُسَجَّل مع كل نتيجة.

توقيعات bg-sign

يستطيع صاحب الملف أن يضع توقيعاً منفصلاً في سمة من سمات نظام الملفات. ينقله Agent فقط ويُعامل ادعاؤه على أنه عدائي؛ ويتحقق الجهاز من المفتاح العام وصلاحيّة الموقع والتوقيع على SHA-256 للملف المستلم. ولا يصل مفتاح التوقيع الخاص إلى الجهاز أبداً. حين تشترط السياسة توقيعاً صالحاً، يكون لكل توقيع مفقود أو غير صالح أو غير مدعوم أو غير موثوق أو غير محسوم حالته الخاصة، ولا يمضي النقل.

شهادة نظام المؤسسة

تستطيع المؤسسة أن تشترط أن يُبدي نظام من أنظمتها رأيه قبل نقل الملف. هذا الشاهد خارج الجهاز، وAgent مجرد ناقل؛ والجهاز هو من يتحقق. تسري النتيجة قبل استلام المحتوى ولا تُضعف أبداً فحوص ART نفسها: حتى القبول لا يجعل الملف صالحاً.

- يُقَارَن الملخص المشهود له مرتين بملخص الملف، والثانية قبل الإيصال الدائم. ولا يمكن لقبول ملف أن يُدخل ملفاً آخر.
- غياب الشهادة غير بطلانها؛ والشهادة الباطلة ترفض في كل الأوضاع.

النتيجة الحتمية (ClamAV FOUND، أو YARA MATCH، أو رفض تحقق) لا يُعاد تجربتها أبداً على محرك أو قاعدة أضعف؛ أما تعطل المحرك أو انتهاء المهلة أو الرد المشوّه فنتيجة غير حاسمة، ولا يتقدم النقل.

✦ لا شيء يحتاج إلى ضبط يوماً بعد يوم

تختار السياسة الفحوص التي تجري، والفحوص تجري وحدها. وتُحدَّث التوقييع والقواعد بحزمة بيانات موقعة تعمل دون اتصال، دون أي تغيير في البرمجيات.

أي شيء مجهول يوقف النقل

الموقف	السلوك
المحرك غير متاح، أو تعطل، أو انتهت مهلته، أو ردًا مشوّهاً	غير حاسم؛ ولا يتقدم النقل
مجموعة التواقيع أو القواعد غير متوافقة مع المحرك	الجهاز غير جاهز؛ والقبول ينتظر
دليل مطلوب مفقود أو إصداره مجهول	رفض، لا مرور صامت أبدًا
تجاوز حد للأرشيف أو للموارد	رفض دون أي استخراج غير آمن
نتيجة خبيثة حتمية	حجر؛ ولا إعادة محاولة بأداة أضعف

الأصل يبقى بعيدًا عن المتناول

- مخرجات المحرك الخام، والأسرار، وتفاصيل القواعد الداخلية، ومحتوى الملف لا تظهر أبدًا في التدقيق أو في الأخطاء التي يراها المستخدم.
- يتلقى المرسل النتيجة ورمزًا مرجعيًا؛ ويبحث دور مخوّل عن الأدلة بذلك الرمز في لوحة التحكم، فلا يعلم الجواب المهاجم ما الذي يمر.
- المعاينة الآمنة تعرض فقط صفحات PNG تُنتجها عملية معزولة؛ ولا يتلقى المتصفح الملف الأصلي أبدًا.

ما الذي يُختبر

- ترتيب المراحل، وتفرد النتيجة، ومعنى ثابت أيًا كان ترتيب القواعد وتوازيها.
- إعادة التشغيل أثناء الفحص تبقي مهمة دائمة واحدة ولا تنشئ نتيجة مكررة؛ ولا تُخلط مجموعة تواقيع بإصدار آخر أبدًا في المحاولة الواحدة.

ما لم يثبت نفسه لا يعبر؛ وما عبر يحمل دليله.

كتالوجات أخرى لهذا المنتج

كتالوج ٤

الأمن والتشفير

كتالوج ٢

تجربة المستخدم

كتالوج ١

نظرة عامة على المنتج



للاستشارة وطلب عرض توضيحي ومعلومات الاتصال:

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

قد تتغير المواصفات دون إشعار مسبق.