BARDIN GATE

نقل آمن للبيانات بين الشبكات المعزولة

ARP

AIR-GAP REGULATED PIPELINE

جهاز 2U يُركب في الحامل

فحص المحتوى والحجر: لا شيء يعبر دون فحص

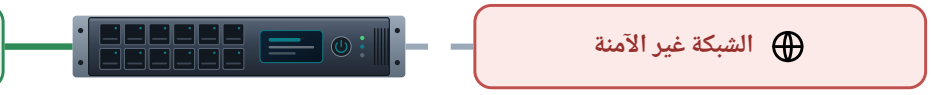
قبل أن يتحرك أي شيء، يمر كل ملف بمرحلتين منفصلتين: تحقق حتمي وفحص بالمحركات. لا يجيب الفحص إلا بنعم أو لا، ويُسجَّل كل جواب مع الإصدار الذي أعطاه.

في هذا الكتالوج: قواعد التحقق السبع عشرة، ومحركات الفحص الثلاثة، وكيف يصدر الحكم، والحجر، والأدلة التي تُحفظ

لمن: متخصصو الأمن الذين يقيّمون طريقة فحص المحتوى

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

يعامل ARP أسماء الملفات وامتداداتها وأنواعها المعلنة وبنى الأرشيفات ومخرجات المحركات على أنها مدخلات معادية. ولا تجري الفحوص إلا على البايتات التي حُسبت بصمتها عند القبول وحُفظت داخل الجهاز، لا على ملف المصدر أبدًا، فهو خارج حدود الثقة.



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

٢	١٧	٤	٠
مرحلتان منفصلتان: التحقق والفحص	قاعدة تحقق حتمية	محركات فحص: DLP وClamAV وYARA والذكاء الاصطناعي	بايت تغيّر في الملف المسلَّم

مرحلتان بطبيعتين مختلفتين

تحقق حتمي

المدخل نفسه، النتيجة نفسها. يسأل: «هل الملف هو ما يدّعيه، ضمن ما يقبله هذا المسار؟». ويجري أولًا، فلا يصل أرشيف معادٍ إلى أي محرك أبدًا.

فحص بالمحركات

يعتمد على التواقيع والقواعد المثبَّتة: «هل في هذا الملف شيء لا نسمح بعبوره؟». كل محرك مطلوب أو اختياري حسب المسار، ويُسجَّل إصداره مع النتيجة.

نعم أو لا، ولا جواب ثالث

الفحص الذي جرى له جواب. أما الفحص الذي لم يجرِ (تعطل المحرك، انتهاء المهلة) فلا يقول شيئًا عن الملف؛ إنه فشل في الآلية و**ليس حجرًا أبدًا**.

سبع عشرة قاعدة تحقق

المجموعة	القواعد	تحمي من
التسمية	IllegalChars · FilenameLength · MultiExtension · ReservedNames · PathTraversal	الأسماء التي تكسر نظام ملفات الوجهة أو تضلّله أو تفلت منه، بما فيها أسماء الأجهزة المحجوزة وتسلسلات اجتياز المسارات.
النوع	ExtensionBlocklist · ExtensionAllowlist · MimeExtensionMatch · MimeDetect	محتوى ليس من نوع مقبول، أو يناقض نوعه المكتشف امتداده.
الحجم	MaxFileSize	ملفات تتجاوز ما جُهّز له المسار والجهاز.
الأرشيف	ArchiveEntryCount · ArchiveDepth · ArchiveSymlink · ArchivePathTraversal · ArchivePasswordProtected	قنابل الأرشيف، والمداخل التي تفلت عند الاستخراج، والروابط إلى الخارج، والمحتويات المشفّرة التي لا يمكن فحصها.
المحتوى النشط	OfficeActiveContent · PdfActiveContent	مستندات تحمل نصوصًا برمجية أو وحدات ماكرو مضمّنة.

«مشفّر» يعني «غير قابل للفحص»، لا «خبيث»

الأرشيف المشفّر لا يُحكم عليه بأنه خبيث؛ إنه محتوى لا يستطيع أي محرك النظر داخله. والمسار الذي يقبله قد اتخذ اختيارًا متعمدًا.

أربعة محركات فحص

DLP

أربع عائلات من الكواشف: الأنماط، والقواميس، والتصنيفات، والعشوائية. يكشف فقط، ولا يُقنِّع ولا يعيد الكتابة، وليس فيه عن قصد تقييم بالتعلم الآلي: يجب أن تكون النتائج قابلة للتكرار والتفسير.

ClamAV

كشف البرمجيات الخبيثة بالتواقيع من مجموعة موقّعة تعمل دون اتصال؛ ويُسجَّل إصدارها مع كل نتيجة.

YARA

قواعد للتهديدات والمحتوى المحظور؛ مجموعات موقّعة، وتفعيل ذري، ولا خلط بين الإصدارات.

نموذج الذكاء الاصطناعي

يعمل على الجهاز نفسه دون اتصال، ويفحص ما مرّ من القواعد الثابتة. يستطيع أن يوقف ملفًا، ولا يستطيع أبدًا أن يمرّره؛ ويُسجَّل إصداره مع كل نتيجة.

الحكم: من الأدلة إلى النتيجة

ما وُجد	النتيجة
نتيجة بدرجة CRITICAL أو HIGH أو MEDIUM	حُكم ضده: حجر
يحكم نموذج الذكاء الاصطناعي بأن الملف خبيث أو في غير موضعه	حُكم ضده: حجر
نتائج LOW أو INFO فقط	مرور
لا نتائج، واكتمل كل محرك مطلوب	مرور
محرك مطلوب لم يكتمل، أو لم يكن متاحًا، أو استنفد محاولاته	فشل بسبب عطل في الآلية، ولا يُحجر أبدًا

الحجر نهائي

الملف المحجور لا يُسلَّم أبدًا. وهي تُفرض في عدة مواضع مستقلة حتى لا يفتحه خطأ واحد: دورة حياة النقل لا مخرج فيها من الحجر، وواجهة REST لا نقطة فيها للإفراج، وقائمة الصلاحيات لا صلاحية فيها للإفراج، وصفحة الحجر في لوحة التحكم لا زر فيها للإفراج.

ما يستطيع المُشغِّل فعله وما لا يستطيع

الإجراء	متاح
رؤية كل عنصر محتجز مع المسار والسبب والأدلة كاملة	نعم
تصدير تقرير بالبيانات الوصفية والأدلة	نعم؛ دون المحتوى أبدًا
التخلص المبكر من المحتوى المحتجز	نعم، مع تسجيل السبب في التدقيق
قراءة المحتوى المحتجز أو تنزيله	لا؛ لا يوجد طريق لذلك
الإفراج، أو نقض الحكم، أو إعادة المعالجة	لا

مهمة المُشغِّل أن يفهم ويرفع الأمر، لا أن ينقض الحكم. يُعالج الملف المحجور خطأً بالحديث مع مالك النظام المنتِج، وإن كانت السياسة خاطئة فبتغيير مسجَّل في التدقيق للسياسة؛ ثم يعيد المصدر الإرسال.

> **لا شيء يحتاج إلى ضبط يومًا بعد يوم**
>
> تختار ملف المسار مرة واحدة وتجري الفحوص وحدها. وتُحدَّث التواقيع والقواعد بحزمة بيانات موقّعة تعمل دون اتصال، دون أي تغيير في البرمجيات.

⚠ أربع نهايات استثنائية، لكل منها صاحب

النهاية	المعنى	مشكلة من
QUARANTINED	حكم فحص المحتوى ضد الملف.	المحتوى: أرسل النظام المنتِج شيئًا لا يقبله هذا المسار.
REJECTED	رفضه موافِق، أو لم يقرر أحد في الوقت المحدد.	الإجراءات: رفض شخص أو لم تتصرف المؤسسة.
FAILED	فشلت آلية واستُنفدت محاولاتها.	الجهاز أو البيئة: المضيفون أو المحركات أو السعة.
سُلّم، ولم يُسوَّ	وصل الملف لكن التصرف في المصدر فشل.	نظام المصدر.

لأن هذه الأربع لا تُجمع أبدًا تحت «أخطاء»، يرى المُشغِّل الإشارة: ارتفاع FAILED يعني أصلح الجهاز، وارتفاع QUARANTINED يعني تحدّث مع المنتِج، وارتفاع REJECTED بسبب انتهاء المهلة يعني أن أحدًا لا يتابع طابور الموافقات.

أدلة تدوم

كل تشغيل يترك سجلًا واحدًا غير قابل للتغيير

- ما الذي جرى وبأي إصدار
- مقابل أي إصدار من مجموعة المحتوى
- الحكم ورمز السبب والنتائج المحدودة
- بما فيها التشغيلات التي لم تكتمل

ما لا يُحفظ أبدًا

- المحتوى المطابق خارج سياق محدود ومُقنَّع
- نص التوقيع أو القاعدة
- مخرجات المحرك الخام وتتبعات الأخطاء
- المسارات المطلقة على المضيف

الملف الذي يفشل لا يعبر أبدًا، والملف الذي لم يُفحص لا يُعلن سليمًا أبدًا.

كتالوجات أخرى لهذا المنتج

كتالوج ١
نظرة عامة على المنتج

كتالوج ٢
المسارات والسياسة

كتالوج ٤
الأمن والتشغيل

للاستشارة وطلب عرض توضيحي ومعلومات الاتصال:
https://www.bardin.tech/ar/bardingate-arp/

قد تتغير المواصفات دون إشعار مسبق.