BARDIN GATE

انتقال امن داده میان شبکه‌های ایزوله

ARP

AIR-GAP REGULATED PIPELINE

2U اپلاینس رک‌مونت

امنیت و بهره‌برداری: دستگاهی که خودش را می‌پاید

امنیت از ساختار دستگاه می‌آید و بهره‌برداری عمداً بی‌دردسر است: راه‌اندازی هدایت‌شده، به‌روزرسانی امضاشده با بازگشت خودکار، و دستگاهی که خودش را درست می‌کند.

در این کاتالوگ: راه‌اندازی اولیه، به‌روزرسانی و بازگشت، خودترمیمی، جایگزینی و بازیابی، و نصب دستگاه

برای: متخصصان امنیت و تیم بهره‌برداری

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

امنیت ARP یک ویژگی روی محصول نیست؛ ساختار دستگاه است. اگر هر لایه خطا کند، دستگاه «می‌بندد» و ادامه‌ی غلط نمی‌دهد.

شبکه‌ی ناامن — شبکه‌ی امن

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.

جداسازی فیزیکی

یک کلید فیزیکی داخل دستگاه در هر لحظه فقط یکی از دو شبکه را وصل می‌کند و پیش از وصل‌کردن دیگری، اولی را کاملاً قطع می‌کند. در هر راه‌اندازی هم همه‌چیز نخست قطع است، و قطع‌بودن با بازخورد خودِ کلید اثبات می‌شود، نه با اینکه «فرمان اجرا شد».

راه‌اندازی مطمئن

UEFI Secure Boot، بوت اندازه‌گیری‌شده در تراشه‌ی TPM 2.0 و سیستم فقط‌خواندنی که بلوک‌به‌بلوک با dm-verity راستی‌آزمایی می‌شود. زنجیره‌ی بوت یک‌بار ساخته می‌شود و روی همه‌ی دستگاه‌ها یکسان است.

داده‌ی ذخیره‌شده

داده از نخستین بوت با LUKS2 و AES-256-XTS رمز می‌شود. کلید فقط برای راه‌اندازیِ امضاشده‌ی سازنده آزاد می‌شود و رمز بازیابی فقط یک بار به راه‌انداز نشان داده می‌شود.

بازرسی در فضای ایزوله

تجزیه‌گرها و موتورهای بازرسی در کانتینر بدون ریشه، با AppArmor، seccomp، بدون شبکه، ریشه‌ی فقط‌خواندنی و سقف منابع اجرا می‌شوند. هر خرابی به «بستن» ختم می‌شود.

هوشمندی روی دستگاه

فایل از روی بایت‌های واقعی‌اش سنجیده می‌شود. مدل هوش مصنوعی آفلاین فایل را نگه می‌دارد ولی هرگز رد نمی‌کند، و جریان غیرعادی هشدار می‌دهد.

هویت و دسترسی

- **دستگاه تنها مرجع است.** مرورگر، فایل‌های واردشده و هر چیز دیگر فقط «ادعا» می‌آورند و هیچ‌کدام نمی‌توانند اختیار بدهند.
- **پیش‌فرض، رد است.** نقش‌ها با دامنه‌ی مشخص تعریف می‌شوند و هر مجوزِ ننوشته، یک امتناع است.
- **رمز عبور، و دوباره رمز.** کارهای پرخطر (نقش‌ها، سیاست امنیتی، مجوز و به‌روزرسانی، اصلاح زمان، بازیابی، وارد کردن پیکربندی) رمز را دوباره می‌خواهند.
- **هیچ در پشتی وجود ندارد.** رمز مدیر سازنده، حساب پنهان، بازنشانی با ایمیل یا دور زدن بی‌ثبت نیست. بازیابی آخرین مدیر یک رویه‌ی فیزیکی در محل دستگاه است.
- **SSH فقط یک حساب پشتیبانی محدود.** فقط گزارش، لاگ و وضعیت را می‌دهد و ریشه SSH ندارد؛ پوسته‌ی عادی یا ورود مستقیم به پایگاه‌داده نیست.

ممیزی و SIEM

ویژگی	مقدار
افزودنی و مقاوم در برابر دستکاری	هر رویداد به Hash قبلی زنجیر می‌شود؛ هر بخش با ۱۰٬۰۰۰ رویداد یا یک ساعت بسته و نقطه‌ی بازرسی‌اش امضا می‌شود.
چه ثبت می‌شود	هر تلاش و نتیجه‌ی امنیتی، مدیریتی و حیاتیِ کسب‌وکار، با شناسه‌ی هم‌بسته؛ از جمله کارهای پرخطرِ ردشده.
زمان معتبر	آفلاین؛ ساعت امنیتی را خود دستگاه نگه می‌دارد و ناهنجاری ساعت نمی‌تواند مجوز یا مهلت نگهداری را دراز کند.
SIEM	خروجی یک‌طرفه و تایپ‌شده به SIEM شما؛ پیش‌فرض TCP روی TLS، mTLS اختیاری، قالب RFC 5424 JSON یا CEF؛ نشانی‌ها به‌صورت شبه‌نام. متن ساده یا UDP نیازمند هشدار تأییدشده و ثبت در ممیزی است.
آنچه هرگز صادر نمی‌شود	بایت‌های فایل، رمز، توکن و کلید خصوصی.

کار روزمره: دیدن، تأیید کردن، و بس

اپراتور داشبورد را می‌بیند و تأییدکننده مورد را تأیید می‌کند. نه SSH لازم است، نه اسکریپت، نه زمان‌بندی؛ دستگاه تا جایی که بتواند خودش را می‌پاید و جایی که نتواند، با دلیل روشن به شما می‌گوید.

راه‌اندازی اولیه، هدایت‌شده

۱ — نصب در رک
دستگاه 2U را در رک می‌گذارید و برق و اتصال به شبکه‌های امن، ناامن و مدیریت را وصل می‌کنید.

۲ — باز کردن کنسول
کنسول را در مرورگر باز می‌کنید. کدی که روی نمایشگرِ خودِ دستگاه می‌بینید ثابت می‌کند شما کنار آن هستید.

۳ — راه‌اندازی هدایت‌شده
گام‌ها به‌ترتیب اجرا می‌شوند و هر گام خودش را می‌آزماید: سخت‌افزار، زمان، نشانی‌های شبکه و نخستین مدیر.

۴ — پذیرش
بسته‌ی مدرکِ امضاشده‌ی راه‌اندازی را می‌گیرید و دستگاه آماده‌ی کار است.

رویه ترتیبی و اجباری است. رمز بازیابیِ دیسک فقط یک بار، روی همان صفحه‌ی راه‌اندازی، به کسی که کنار دستگاه است نشان داده می‌شود.

به‌روزرسانی و بازگشت

- **بسته‌ها امضاشده و آفلاین‌اند.** بسته‌ی بدون امضای معتبر یا با شماره‌ی نسخه‌ی پایین‌تر رد می‌شود (ضد بازگشت)؛ تنزل نسخه‌ی عادی ممنوع است.
- **دو اسلات.** به‌روزرسانی در اسلات دیگر نوشته می‌شود، یک‌بار آزمایشی بوت می‌شود و فقط پس از سلامت‌سنجی قطعی می‌گردد؛ در غیر این صورت دستگاه خودکار به نسخه‌ی قبلی برمی‌گردد.
- **داده جدا از نرم‌افزار.** امضای ClamAV، قاعده‌های YARA و طرح‌واره‌های اعتبارسنجی در بسته‌ی داده‌ی جداگانه می‌آیند که فقط داده است و نرم‌افزاری را عوض نمی‌کند.

خودترمیمی

دستگاه فرض می‌کند هیچ‌کس به آن دسترسی ندارد؛ پس خودش را درست می‌کند. روی آن ایستگاه کاری، صفحه‌نمایش و SSH معمولی نیست و هر بازیابی‌ای که به رسیدن به دستگاهِ خراب نیاز داشته باشد، طراحی نمی‌شود.

سطح	چه می‌کند	چه می‌ماند
بازنشانی نرم	نرم‌افزار را به آخرین حالت سالم برمی‌گرداند؛ همان سازوکار بازگشتِ به‌روزرسانی است.	هویت، پیکربندی، گزارش‌ها و ممیزی
بازنشانی سخت	دستگاه را به پیش از راه‌اندازی اولیه برمی‌گرداند و پاک می‌کند، نه بازیابی.	هیچ؛ پیش از آن ممیزی را خروجی بگیرید

جایگزینی و بازیابی

وضعیت	مسیر درست
خرابی یک دیسک	جایگزینی طبق دستورالعمل؛ حجم سالم یا قابل‌بازسازی می‌ماند.
منبع تغذیه یا فن	تعمیر طبق رویه‌ی سازنده در حالت نگهداری و بررسی دوباره‌ی آمادگی.
برد اصلی یا تراشه‌ی امنیتی	دستگاه یک‌بار رمز بازیابی را در محل می‌خواهد؛ هویت، پیکربندی و مجوز خود را نگه می‌دارد.
از دست رفتن کل دستگاه	دستگاه جایگزین: راه‌اندازی اولیه‌ی تازه، وارد کردن فایل پیکربندی، ورود دوباره‌ی رمزها و برقراری دوباره‌ی نقاط پایانی. هویت دستگاه قبلی کلون نمی‌شود.

فایل پیکربندی ARP همه‌ی مسیرها و سیاست‌ها را حمل می‌کند و رمزها را نه. پس از وارد کردنش، فقط کلیدهای SSH باید دوباره وارد و میزبان‌ها دوباره پین شوند.

دستگاه و نصب

بخش	توضیح
دستگاه	یک اپلاینس رک‌مونت 2U با همه‌چیز آماده. لازم نیست سرور، سیستم‌عامل یا نرم‌افزار جانبی انتخاب یا نصب کنید.
جا و برق	2U فضا در رک استاندارد و برق.
شبکه	اتصال به شبکه‌ی امن، شبکه‌ی ناامن و شبکه‌ی مدیریت. دو شبکه‌ی اول هیچ‌گاه به هم وصل نمی‌شوند.
کار روزمره	فقط یک مرورگر. کنسول به چهارده زبان است، از جمله فارسی.
اینترنت	لازم نیست؛ مجوز، به‌روزرسانی و امضاها آفلاین و امضاشده‌اند.

دستگاهی که باید در جایی بی‌دسترس کار کند، باید بتواند خودش را درست کند و بداند چه زمانی نباید ادامه دهد.

کاتالوگ‌های دیگر این محصول

کاتالوگ ۱	کاتالوگ ۲	کاتالوگ ۳
معرفی محصول	مسیر و سیاست	بازرسی و قرنطینه

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

مشخصات ممکن است بدون اطلاع قبلی تغییر کند.