



سامانه فدرال مانور و رزمایش سایبری حاکمیت، ریسک و انطباق

طراحی، اجرا و ارزیابی رزمایش IT/OT

ممیزی SCADA و مراکز کنترل

دوقلوی دیجیتال مکانی و صنعتی

کنسول فرماندهی ملی

سکوی بومی، تمام برون خط

Air-Gap — بدون هیچ وابستگی به سرویس ابری خارجی

معرفی اجمالی محصول

چند پروژه در قالب یک محصول

سامانه مانور و مدیریت تا آوری

مجموعه های از پروژه های وابسته به مدیریت امنیت سایبری حوزه های فناوری اطلاعات و حوزه عملیاتی (OT) میباشد :

۱- سامانه حاکمیت، ریسک و انطباق (GRC - Governance, Risk, and Compliance)

۲- اجرای مانور سایبری در حوزه IT و OT در یک محیط شبیه سازی شده کاملاً ایزوله

۳- مدیریت دارایی های سایبری حوزه IT و OT (Asset Discovery and Management)

۴- مدیریت ریسک و آسیب پذیری ها مراکز داده ، اتاق های فرمان ، مراکز دیسپاچینگ ، مراکز تلمتری و SCADA از یک نقطه

۵- کارتابل مکاتبات امن (کاملاً رمزنگاری شده و امن)

۶- دریافت راهنمای امن سازی (اولیه) از سیستم



امروز آمادگی با «مستندات» سنجیده می‌شود، نه با «شواهد»

چهار شکاف، یک ریشه: نبود یک منبع واحد حقیقت

وضعیت امروز	با این سامانه
 پرونده‌های پراکنده چند فایل و صورت جلسه	 پروندهٔ زندهٔ انطباق پیوسته به‌روز، نه سالی یک‌بار
 چک لیست بله/خیر بدون شاهد، بدون تاریخ اعتبار	 شاهد تغییر ناپذیر هش، متولی، روش، بازه، طبقه‌بندی
 رزمایش دستی مشاهدات ثبت‌نشده و تکرار ناپذیر	 رزمایش مهندسی شده تزریق زمان‌بندی شده و ارزیاب مستقل
 ابزار خارجی و ابری تحریم‌پذیر، غیرقابل استقرار ایزوله	 بومی و کاملاً برون خط بدون هیچ اتصال به اینترنت
 آمادگی اثبات شده با شاهد، نه با ادعا	 دید واحد از دارایی نقشه، توپولوژی، ریسک
 انطباق زنده پیوسته، نه سالانه	 حاکمیت ملی بدون تمرکز دادهٔ خام

ویژگی متمایزکننده

چرا راه‌حل‌های نقطه‌ای کافی نیستند

این سامانه از ابتدا برای محیط ایزوله و بدون اتصال به اینترنت (Air-Gap) طراحی شده است. هیچ وابستگی به سرویس ابری خارجی یا اینترنت نداشته، هیچ بارگذاری امضاء یا نقشه از اینترنت، و هیچ به‌روزرسانی کنترل‌نشده وجود ندارد. این یک تصمیم معماری در روز اول است، نه وصله‌ای بعدی.

می‌توان برای هر شکاف یک ابزار جدا خرید: یک سامانهٔ GRC، یک محیط Range، یک سامانهٔ GIS، یک ابزار مدیریت دارایی. اما مسئلهٔ اصلی خود ابزارها نیستند؛ مسئله این است که خروجی هیچ‌کدام ورودی دیگری نمی‌شود. یافتهٔ رزمایش به‌صورت خودکار به یافتهٔ GRC تبدیل نمی‌شود، و دارایی روی نقشه همان دارایی‌ای نیست که در پروندهٔ ریسک ثبت شده است. این سامانه دقیقاً روی همین اتصال‌ها بنا شده است.

نُه دامنه قابلیت

هر دامنه با مالک، قرارداد و خروجی مشخص

فدراسیون مرز اعتماد، مستاجر، تبادل امضاشده • موجود / در حال ساخت	رزمایش MSEL، تزریق، ارزیاب، گزارش پس از رزمایش • موجود / در حال ساخت	حاکمیت، ریسک، انطباق کنترل، ریسک، یافته، برنامه اقدام اصلاحی • موجود / در حال ساخت
دوقلوی دیجیتال سایت، ناحیه، دارایی، وابستگی‌ها • موجود / در حال ساخت	نقشه و مکان لایه ملی، شرکتی، سایت، راهروی اثر حادثه • موجود / در حال ساخت	شبیه‌سازی توپولوژی، طرح حمله، بازپخش قطعی ○ در دست پیاده‌سازی
بانک دانش استاندارد ۱۵۹ استاندارد، نگاشت متقابل، پروفایل کنترل • موجود / در حال ساخت	هوشمندی و شواهد تله‌متری، سیگنال ریسک، روند ○ در دست پیاده‌سازی	کنسول مرکزی وضعیت امنیتی، آمادگی، تجمیع ملی ○ در دست پیاده‌سازی

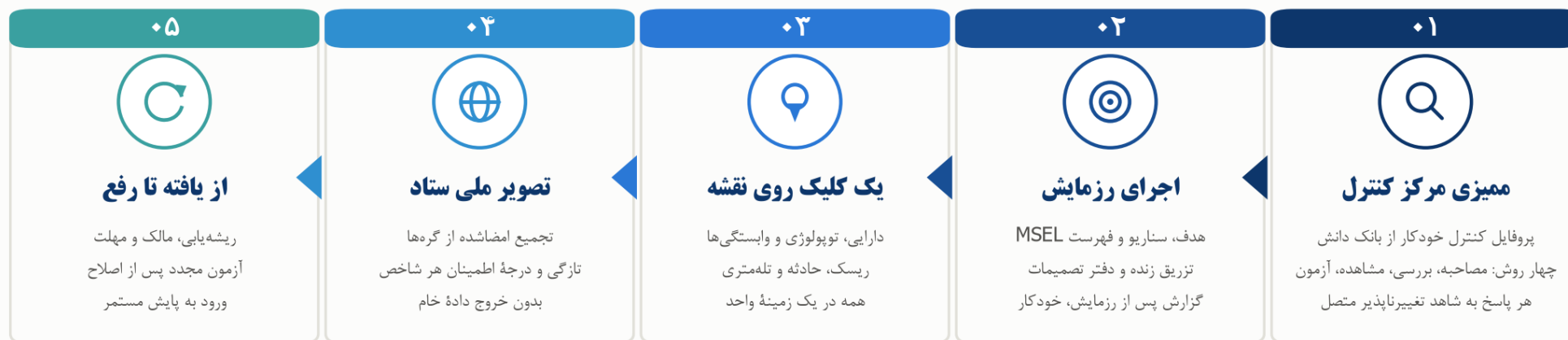
جست‌وجوی دوزبانه فارسی و انگلیسی، با امضای هر بند	امتیازدهی هفت‌بُعدی به‌جای یک نمره واحد	نوار زمانی بازگشت به هر لحظه رزمایش	کار در حالت گسسته قطع ملی، عملیات برقرار
--	--	--	---

➤ **ارزیابی در برابر همه استانداردها:** نگاشت‌آگاه اجرا می‌شود؛ یک الزام مشترک میان چند استاندارد فقط یک‌بار امتیاز می‌گیرد و پوشش، تعارض و حوزه صلاحیت جداگانه نمایش داده می‌شود.

➤ **ایمنی چک‌لیست:** پاسخ به/خیر به‌تنهایی شاهد نیست؛ «مشمول نیست» نیازمند توجیه و تأیید است؛ کنترل جبرانی باید تاریخ انقضا و ریسک باقیمانده داشته باشد.

پنج کاربرد واقعی

از ممیزی یک مرکز کنترل تا تصویر ملی صنعت



ذی‌نفع	آنچه به دست می‌آورد	ذی‌نفع	آنچه به دست می‌آورد
مدیرعامل و هیئت مدیره	تصویر مدیریتی از ریسک و آمادگی، قابل دفاع در برابر نهاد ناظر	مدیر رزمایش	چرخه کامل با تزریق زمان‌بندی‌شده، ارزیاب مستقل و گزارش خودکار
مدیر امنیت (CISO)	اتصال مستقیم رزمایش، ممیزی، ریسک و اقدام اصلاحی در یک پرونده	تیم عملیات SOC/OT	دسترسی فوری به توپولوژی، وابستگی‌ها و محدودیت ایمنی هر تجهیز
مالک ریسک	ریسک متصل به دارایی، کنترل و شاهد واقعی، با ریسک باقیمانده	مهندس SCADA	تضمین معماری: هیچ آزمون خودکاری روی تجهیز زنده نمی‌نویسد
ممیز و ممیزی داخلی	چرخه ممیزی با پرونده‌ای که سال بعد قابل بازتولید است	ستاد و نهاد ناظر	تجمیع امضاشده با تازگی و اطمینان مشخص، بدون تصاحب داده خام

بانک دانش استاندارد

استاندارد به‌عنوان «داده» نگهداری می‌شود، نه متن ثابت درون کد



خانواده‌های اصلی



استانداردهای ملی — در همین بانک

- افتا: امنیت فضای تولید و تبادل اطلاعات
 - پدافند غیرعامل: الزامات سازمان پدافند غیرعامل
- در کنار چارچوب‌های بین‌المللی، با نگاشت متقابل

نگاشت متقابل — یک ارزیابی، چند استاندارد

- یک الزام مشترک میان چند استاندارد، یک‌بار امتیاز می‌گیرد
- پوشش، تعارض و حوزه صلاحیت جداگانه دیده می‌شود
- هر بند نسخه، تاریخ اعتبار، منبع و امضا دارد
- افزودن استاندارد ملی جدید = عملیات داده‌ای، نه بازنویسی

افتا و پدافند غیرعامل

بومی، نه ترجمه

۱۴۹ حقیقت مشترک

پشت ۱۲۰۶ کنترل، اهرم ۸٫۱ برابر

۴۸۳ کنترل با مشاهده خودکار

بقیه با سند تأیید شده

۱۰۰٪ کنترل‌ها بسته به «حقیقت»

۱۵۹۴ از ۱۵۹۴

آنچه ادعا نمی‌کنیم

از ۱۵۹۴ کنترل، ۴۸۳ کنترل امروز از مشاهده خودکار تصمیم می‌گیرند؛ بقیه به سند تأیید شده متکی‌اند و همین‌طور هم گزارش می‌شوند. «سند» برای کنترل‌های حاکمیتی پاسخ درست است، نه یک کمبود — اما جای مشاهده زنده را نمی‌گیرد و ما آن را جای مشاهده جا نمی‌زنیم.

چرا این عدد اهمیت دارد

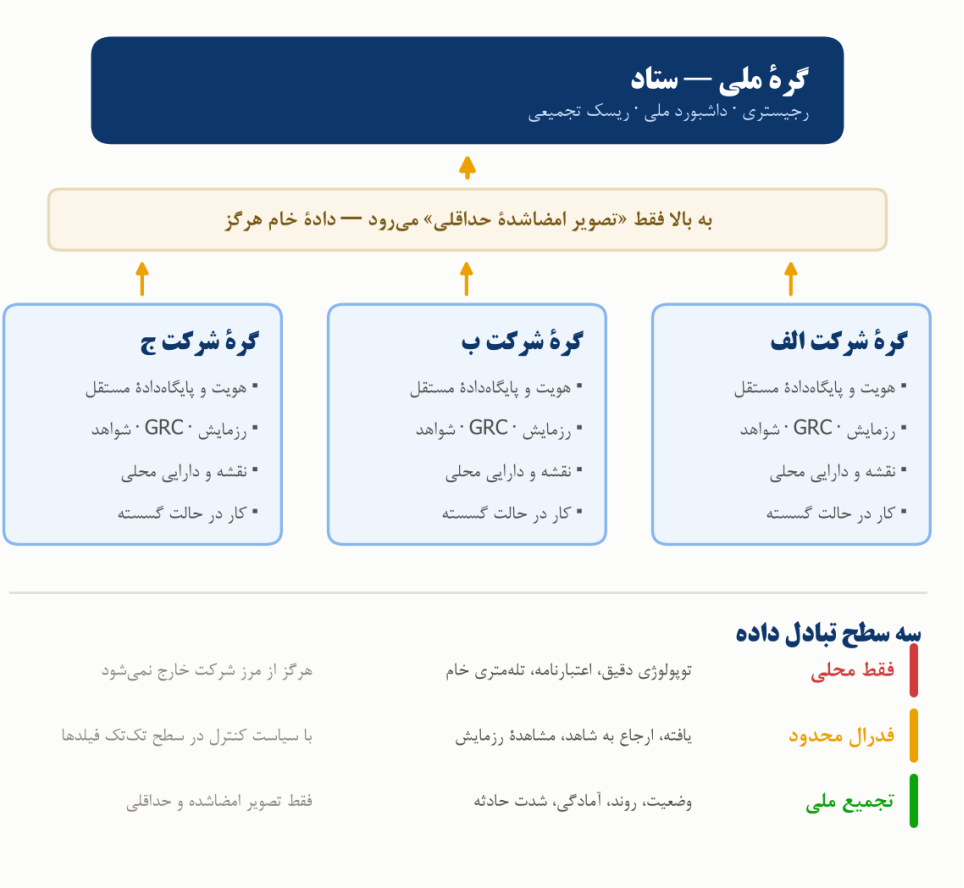
ارزیابی در برابر ۱۵۹ استاندارد بدون نگاشت متقابل یعنی امتیازدهی تکراری به یک الزام مشترک. سامانه یک ستون فقرات ۲۶ دامنه‌ای دارد و هر کنترل به یک «حقیقت» قابل اندازه‌گیری بسته شده است؛ به همین دلیل یک بار ارزیابی، پوشش چند استاندارد را هم‌زمان گزارش می‌کند.

هر شرکت خانه خودش را دارد؛ ستاد فقط پنجره‌ای رو به آن خانه‌ها دارد، نه کلید در ورودی

چهارده سرویس مستقل

هر سرویس مالک داده، قرارداد، سیاست، آزمون و استقرار خودش است: توسعه موازی توسط چند تیم ممکن می‌شود و هر بخش بدون بازنویسی کل سامانه ارتقا می‌یابد.

- دروازه تجربه کاربری — پوسته کاربری و جریان «کلیک روی مرکز»
- هویت و سیاست — فدراسیون هویت انسانی و سرویس، اعمال مجوز
- محیط نقشه (GIS) · توپولوژی — دارایی، لایه مکانی، چیدمان داخل مرکز
- مأموریت و رزمایش — چرخه رزمایش، MSEL، تزریق، امتیاز و گزارش
- GRC · استانداردها — ارزیابی، ریسک، یافته، نگاشت متقابل
- شواهد و ممیزی — نگهداری تغییرناپذیر شواهد و دفتر ممیزی
- آداپتور شبیه‌سازی · عامل‌ها — اتصال ایمن به شبیه‌ساز، اجرای کنترل‌شده
- تاب‌آوری · تصویر فدرال · گزارش — what-if، انتشار امضاشده، اعلان



قاعده مرزبندی

هیچ سرویسی حق نوشتن مستقیم در پایگاه‌داده سرویس دیگر را ندارد، و دسترسی به جزئیات (Drill-Down) تنها با مجوز صریح شرکت و با تعیین هدف مشخص انجام می‌شود.

انطباق با چارچوب‌های مرجع

- NIST SP ۸۰۰-۸۴ — طراحی، اجرا و ارزیابی رزمایش و آمادگی پاسخ
- CISA CTEP — نقش‌ها و آرتیفک‌های رزمایش
- MITRE ATT&CK for ICS — طراحی تزریق‌ها و سنجش پوشش تاکتیک‌ها
- NIST SP ۸۰۰-۸۲۳ — الزامات ایمنی محیط عملیاتی (OT)
- NIST CSF ۲.۰ و RMF — پیوند حاکمیت با مدیریت ریسک و پایش مستمر
- OSCAL — قالب ماشین‌خوان کنترل، ورود و خروج داده
- IEC ۶۲۴۴۳۰ ISO/IEC ۲۷۰۰۱ — خط پایه امنیت ICS و مدیریت امنیت اطلاعات
- افتا ۰ پدافند غیرعامل — الزامات ملی، در همان بانک و با نگاشت متقابل



شاهدی که این پنج ویژگی را نداشته باشد، شاهد نیست:

روش جمع‌آوری

متولی

اثر انگشت رمزنگاری‌شده

طبقه‌بندی

بازه زمانی

جایگاه هوش مصنوعی

هوش مصنوعی در این سامانه یک دستیار است، نه یک تصمیم‌گیرنده. هر قابلیت هوشمند از یک دروازه رسمی عبور می‌کند؛ نتیجه آن همیشه جدا از نتیجه قطعی و همراه با درجه اطمینان نمایش داده می‌شود، و تصمیم امنیتی نهایی همواره بر عهده انسان است.



وضعیت امروز و نقشه راه

آنچه ساخته شده، آنچه در حال ساخت است، و آنچه ادعا نمی‌کنیم

شش موج تحویل

تا شرط خروج هر موج اثبات نشود، موج بعد آغاز نمی‌شود



نه دروازه کیفیت — پیشرفت با درصد اعلام نمی‌شود، با دروازه اثبات می‌شود

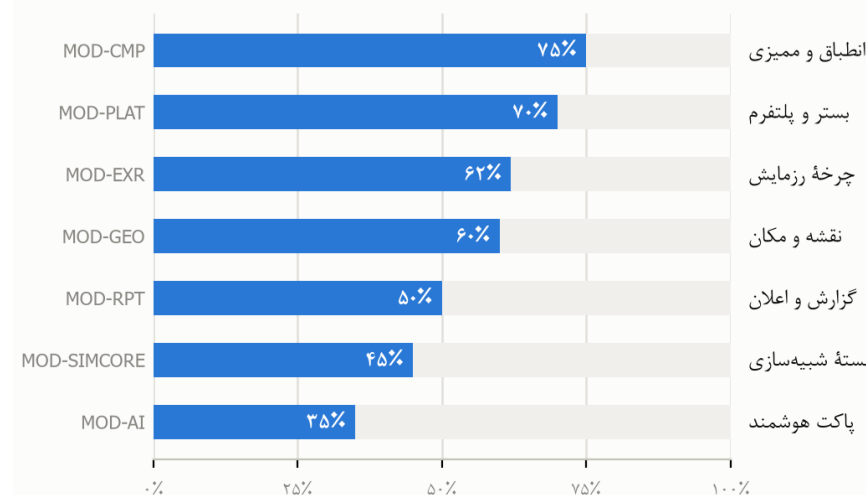


آنچه هنوز ادعا نمی‌شود

- ▶ پیاده‌سازی کامل زمان اجرای همه چهارده سرویس
- ▶ آزمون یکپارچگی سرتاسری، نفوذ و کارایی در مقیاس عملیاتی
- ▶ آزمون انطباق فدراسیون میان دو گره واقعی
- ▶ تصویب نهایی تصمیم‌های معماری توسط کارفرما

سامانه‌ای که مأموریتش سنجش آمادگی بر پایه شواهد است، نمی‌تواند وضعیت خودش را بدون شاهد اعلام کند. درصدها از ممیزی داخلی مازول‌ها آمده‌اند، نه از خوداظهاری.

پیشرفت مازول‌ها — اندازه‌گیری‌شده در ممیزی داخلی، نه خوداظهاری



آنچه پیشنهاد می‌شود، خرید یک ابزار دیگر نیست.

پیشنهاد این است که سازمان روش سنجش آمادگی خودش را عوض کند:

از اتکا به مستندات، به اتکا به شواهد.



رزمایش

طراحی، اجرا و ارزیابی IT/OT



ممیزی

SCADA و مراکز کنترل، با شاهد



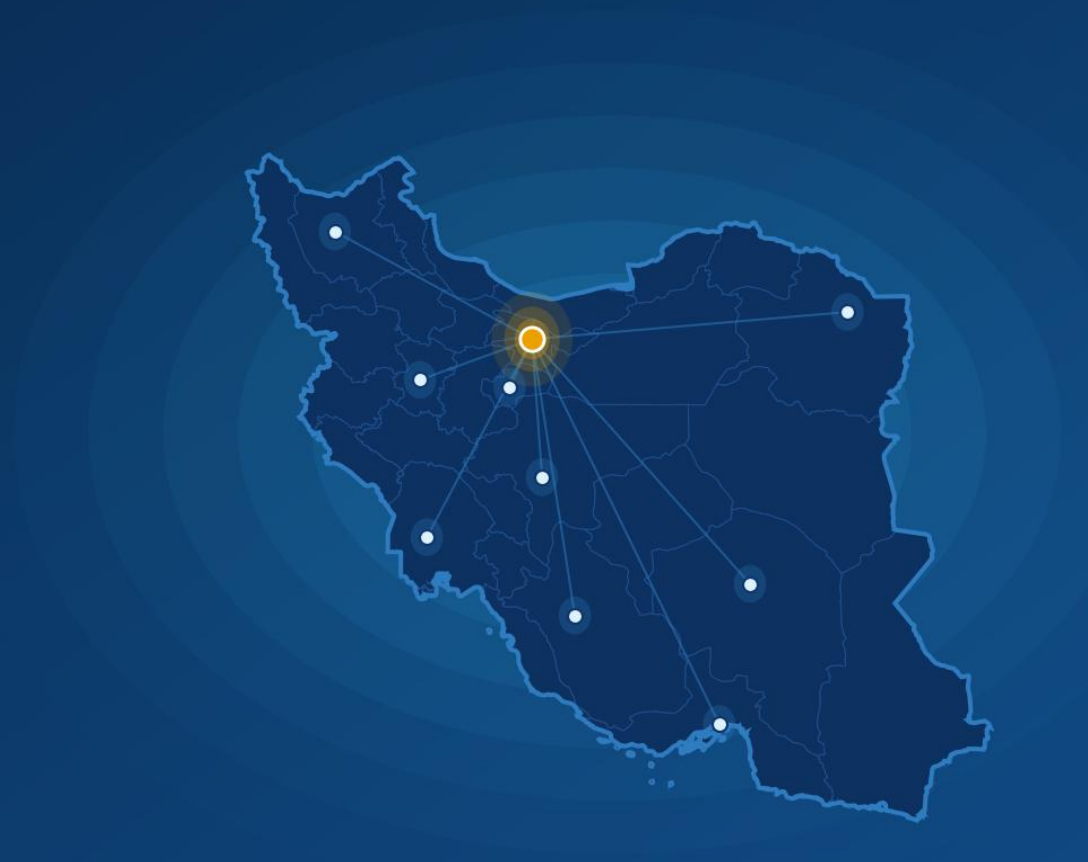
دارایی

دوقلوی دیجیتال مکانی و صنعتی



نقشه

از سایت تا تصویر ملی



گام بعدی

یک نشست فنی-مدیریتی و انتخاب شرکت مرجع برای گره نمونه

EAOS

Enterprise AI Operating System