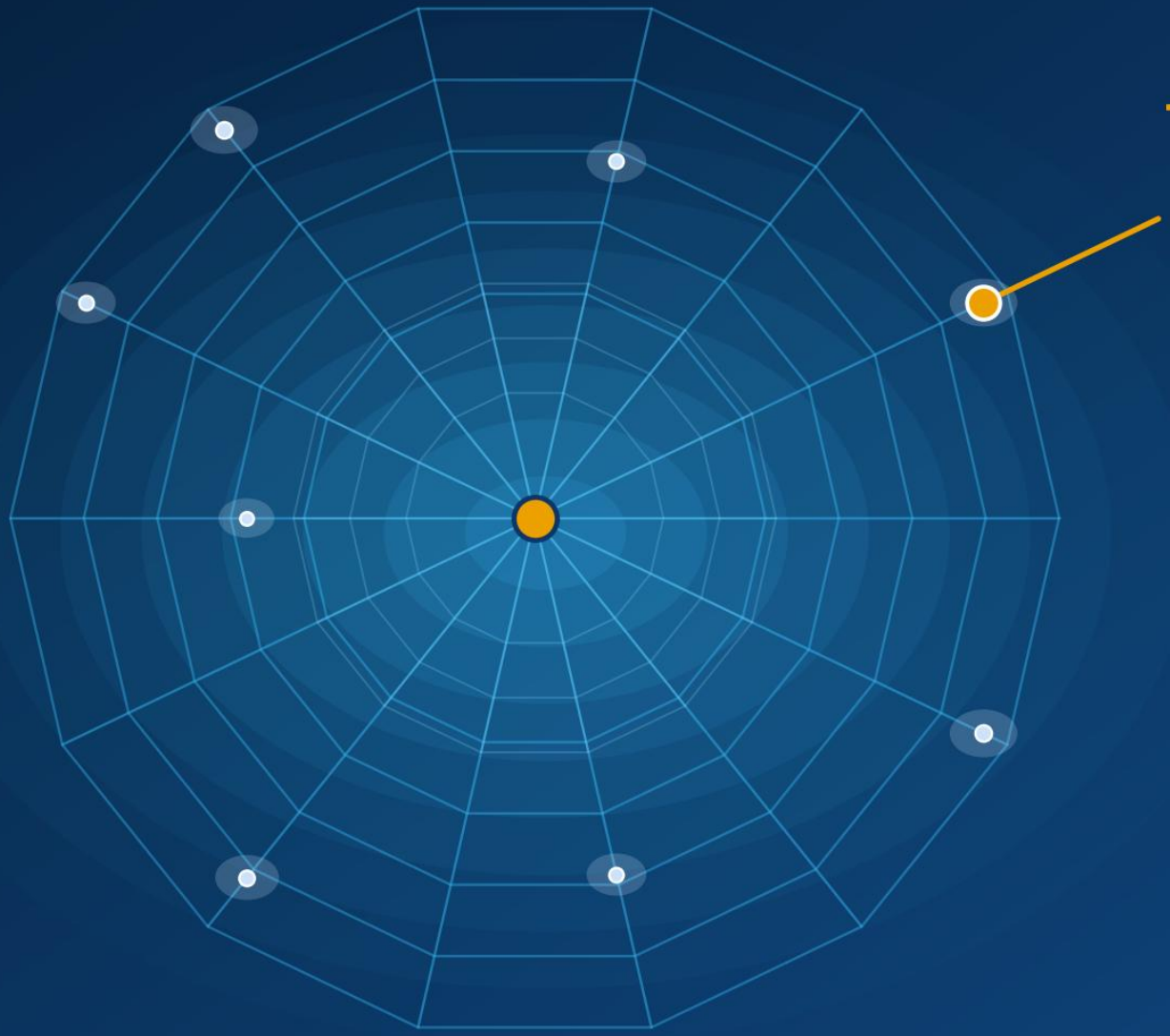


EAOS

Enterprise AI Operating System

دام‌تار

DĀMTĀR · EAOS Spider v2

سامانهٔ فریب سایبری صنعتی و سازمانی

دارایی فریبنده در IT و OT/ICS

کشف زودهنگام مهاجم، پیش از دارایی واقعی

گراف حمله، شاهد تغییرناپذیر و هوش تهدید

ایمنی OT به‌عنوان تصمیم روز اول

تار می‌تنیم تا مهاجم دیده شود

هیچ مسیر نوشتنی به فرآیند واقعی — در قرارداد، نه در متن

چرا دام‌تار وجود دارد؟

۰۱

مهاجمی که وارد شده است، با ابزارهای امروز ماه‌ها دیده نمی‌شود

مهاجم داخل شبکه است و هیچ‌کس خبر ندارد

چهار شکاف، یک ریشه: کشف بر پایهٔ نویز، نه بر پایهٔ طعمه

وضعیت امروز	با دام‌تار
کشف با امضا و آستانه هزاران هشدار، بیشترشان بی‌ربط	**سیگنال با اطمینان بالا** تماس با دارایی‌ای که هیچ کاربری نباید لمس کند
شبکهٔ OT را نمی‌توان اسکن کرد ابزار IT روی PLC یعنی ریسک تولید	**طعمه به‌جای اسکن** هیچ بسته‌ای به سمت فرآیند واقعی فرستاده نمی‌شود
حرکت جانبی دیده نمی‌شود اعتبارنامهٔ سرقتی مثل کاربر عادی است	**اعتبارنامهٔ طعمه** نخستین گام حرکت جانبی، خودش هشدار است
شاهد پس از حادثه بازسازی می‌شود لاگ ناقص، زنجیرهٔ حضانت مخدوش	**ضبط از لحظهٔ اول** نشست، PCAP و فرمان، با اثر انگشت رمزنگاری‌شده

هشدار کم‌نویز
تعامل با طعمه، رخداد بی‌ابهام است

بدون اثر بر تولید
حس‌گر منفعل، Decoy در Zone جدا

دید بر مسیر مهاجم
گراف حمله از تعامل مشاهده‌شده

قابل استقرار ایزوله
بدون وابستگی اینترنتی در زمان اجرا

چرا یک Honeypot تنها کافی نیست

یک تلهٔ سنتی یک ماشین جدا با یک سرویس باز است؛ مهاجم حرفه‌ای آن را در چند ثانیه از روی پاسخ غیرواقعی‌اش تشخیص می‌دهد و کنارش می‌گذارد. دام‌تار یک تله نیست، یک لایه است: هر پروفایل پاکت رفتاری دستگاهی را که تقلید می‌کند اعلام می‌کند، اعتبارنامه و فایل طعمه داخل دارایی واقعی کاشته می‌شود، و هر تعامل هم‌زمان به یک شاهد تغییرناپذیر و یک گره در گراف حمله تبدیل می‌شود.

ویژگی متمایزکننده

این سامانه از روز اول برای شبکهٔ صنعتی و محیط بدون اتصال به اینترنت (Air-Gap) طراحی شده است. ایمنی OT در متن ادعا نمی‌شود؛ در طرح‌وارهٔ قرارداد pin شده و یک سوئیت آزمون ثابت می‌کند که واقعاً رد می‌کند. تفاوت میان «pin موجود است» و «pin گاز می‌گیرد» واقعی است: یک قید که هرگز آزموده نشود، از یک پیش‌فرض که در یک merge جایش را گرفته قابل تشخیص نیست.

محصول در یک نگاه

۰۲

نُه دامنهٔ قابلیت — از کارخانهٔ فریب تا موتور سیاست و تأیید انسانی

نُه دامنهٔ قابلیت

هر دامنه با مالک، قرارداد و خروجی مشخص

کارخانهٔ دارایی فریبنده

قالب امضاشده، چرخهٔ عمر،
هماهنگ‌ساز و وضعیت مطلوب

پروفایل‌های IT

پوستهٔ راه دور، اشتراک فایل،
وب و API، پایگاه‌داده، دایرکتوری

پروفایل‌های OT/ICS

پروتکل کنترل صنعتی، سریال،
و پروتکل لایهٔ دو

طعمه و شیء عسلی

Honeytoken، اعتبارنامه،
فایل و راز جعلی

حس‌گر منفعل و سلول لبه

TAP/SPAN، بافر رمزنگاری‌شده،
Kill Switch محلی

خط لولهٔ رخداد و شاهد

پاکت، حذف تکرار، هش،
زنجیرهٔ حضانت

گراف حمله و DNA سایبری

دوخت نشست، همبستگی،
اثر انگشت رفتاری

تحلیل‌گر هوشمند

خلاصه، درجهٔ اطمینان،
استناد به شاهد، ATT&CK

سیاست، تأیید و پاسخ

موتور سیاست، approval،
SIEM · SOAR · STIX

چند سایت و چند مستأجر
Hub-and-Spoke، فدرال، گسسته

نوار زمانی نشست
بازگشت به هر لحظه از تعامل

قرارداد پیش از کد
OpenAPI، AsyncAPI، Protobuf

Kill Switch محلی
بدون وابستگی به WAN عمل می‌کند

◄ **فریب به‌جای اسکن:** دام‌تار هیچ بسته‌ای به سمت دارایی واقعی نمی‌فرستد و هیچ agentی روی HMI، Engineering Workstation یا کنترلر نصب نمی‌کند. سیگنال از تماس مهاجم با دارایی جعلی می‌آید، نه از کاوش دارایی واقعی — که هم الزام ایمنی است و هم شرط باقی‌ماندن پشتیبانی سازنده.

◄ **شاهد به‌جای لاگ:** هر تعامل با هش، متولی، روش جمع‌آوری، بازهٔ زمانی و طبقه‌بندی ثبت می‌شود و در نگهداشت تغییرناپذیر می‌نشیند. همین پرونده بدون بازسازی دستی به SIEM، به پروندهٔ پاسخ به حادثه و به شواهد کنترل GRC تحویل می‌شود.

۰۳ کارخانهٔ فریب

چه چیزی جعل می‌شود، با چه سطحی از تعامل، و مرزی که پیکربندی‌پذیر نیست

چه چیزی جعل می‌شود

پروفایل‌ها بر اساس نحوهٔ مهارشدنشان گروه‌بندی شده‌اند، نه بر اساس صنعت

فناوری اطلاعات	OT مسیریابی‌شونده	OT غیرقابل‌مسیریابی	سریال و طعمه
مهار: Zone جدا، خروجی محدود	مهار لایهٔ ۳ — بدون route به فرآیند	مهار لایهٔ ۲ — دامنهٔ انتشار جدا	tap سریال منفعل، bus اختصاصی
SSH / Telnet	Modbus/TCP	IEC 61850 MMS	Modbus RTU (RS-485)
SMB / File Share	IEC 60870-5-104	GOOSE (فقط شنود)	DNP3 serial
Web / API	S7comm	Sampled Values (فقط شنود)	Honey Credential
Database	EtherNet/IP (CIP)	PROFINET RT (فقط شنود)	Honey File
RDP	OPC UA	PROFINET DCP (ممنوع)	Fake Secret
LDAP / Directory	DNP3		Honeytoken
Cloud API key	BACnet/IP		
	Historian · HMI		

قاعدهٔ مشترک هر پروفایل — پاکت رفتاری اعلام‌شده

یک PLC واقعی چند اتصال هم‌زمان می‌پذیرد و روی چرخهٔ اسکن خودش پاسخ می‌دهد. Decoyی که صدها اتصال بپذیرد و در کسری از میلی‌ثانیه جواب دهد، پیش از آنکه کسی را فریب دهد شناسایی می‌شود — پس سقف نشست هم‌زمان و پنجرهٔ تأخیر پاسخِ هر پروفایل در قرارداد اعلام می‌شود.

◄ **پروفایل SIS — کنترلر ایمنی، BMS، ESD و رلهٔ حفاظتی — هرگز ساخته نمی‌شود. ولیدیتور بسته، پروفایلی را که نشانهٔ SIS دارد رد می‌کند.**

◄ **سه سطح تعامل:** L0 فقط سرویس و بنر است، L1 پاسخ پروتکلی با وضعیت داخلی می‌دهد و L2 محیط قابل کاوش. سقف مجاز در OT تولیدی L1 است و این سقف در manifest اعلام شده، نه در راهنمای بهره‌برداری.

◄ **طعمه داخل دارایی واقعی کاشته می‌شود:** اعتبارنامه، فایل و راز جعلی روی سامانه‌های واقعی می‌نشینند تا نخستین گام حرکت جانبی خودش هشدار بسازد؛ خودِ Decoy همیشه در ناحیهٔ جدا می‌ماند.

یک Non-Goal دائمی، نه کارِ فاز بعد

پروفایل SIS — کنترلر ایمنی، BMS، ESD و رلهٔ حفاظتی — هرگز ساخته نمی‌شود. چون «نام پروفایل» یک رشتهٔ آزاد است، ولیدیتور بسته هر پروفایلی را که نشانهٔ SIS دارد رد می‌کند؛ بدون این بررسی، یک facade از کنترلر ایمنی کاملاً معتبر بود. این پوشش محصول را در پالایشگاه و نیروگاه محدود می‌کند و همین‌جا اعلام می‌شود تا مشتری بداند چه نمی‌گیرد.

ایمنی OT — قولی که در قرارداد اثبات می‌شود

۰۴

دو بُعد مهار، یک کف، و شواهدی که پیش از استقرار خواسته می‌شود

جایگاه مجاز استقرار

مدل Purdue — و کفی که گزینهٔ پیکربندی نیست

۵	شبکهٔ سازمانی — سطح ۵ و ۴	Decoy مجاز
۳٫۵	ناحیهٔ فریب و OT DMZ	Decoy مجاز
۳	عملیات و کنترل مرکزی	Decoy مجاز
۲	نظارت و HMI	فقط با ارزیابی ریسک ویژه

کف مجاز — پایین‌تر از سطح ۲ در قرارداد قابل بیان نیست

۱	کنترل — PLC، RTU، IED	در قرارداد قابل بیان نیست
۰	میدان — سنسور و محرک	در قرارداد قابل بیان نیست

۹ **سامانهٔ ابزاردقیق ایمنی (SIS)**
نه شبیه‌سازی، نه استقرار در Zone آن، نه TAP شبکه‌اش

دو ادعا، نه یکی

«بدون مسیر به فرآیند» تا نسخه‌های اخیر تنها ادعای مهار بود و برای پروتکل‌های لایهٔ دو یک حفرهٔ واقعی می‌ساخت: IEC 61850 GOOSE و PROFINET RT اصلاً IP ندارند، پس شرط «route ندارد» برایشان بدیهی برقرار است در حالی که هیچ چیز مهار نشده — یک IED واقعی در همان دامنهٔ انتشار می‌تواند فریم Decoy را دریافت کند، و GOOSE به‌صورت پیش‌فرض احراز اصالت ندارد.

- **مهار لایهٔ ۳** — بدون هیچ مسیر مسیریابی‌شده میان ناحیهٔ فریب و کنترل واقعی
- **مهار لایهٔ ۲** — بدون دامنهٔ انتشار مشترک — با پیکربندی سوییچ اثبات می‌شود، نه با ادعا
- **پروتکل غیرقابل‌مسیریابی** — روی سایت فقط شنود؛ انتشار تنها داخل آزمایشگاه دوقلو
- **سطح Purdue** — کف مجاز سطح ۲؛ سطح ۱ و ۰ در طرح‌واره قابل بیان نیست
- **Kill Switch محلی** — بدون وابستگی به WAN عمل می‌کند

شواهد لازم پیش از استقرار: نقشهٔ شبکه، نگاشت VLAN و پیکربندی trunk، اثبات فایروال و جدول مسیریابی، آزمون مهار لایهٔ ۲، محدودهٔ آدرس و VLAN مربوط به SIS، آزمون fail-open روی TAP، گزارش مقایسهٔ اثر انگشت با دستگاه مرجع، و امضای بهره‌برداری، شبکه و ایمنی فرآیند.

الزامی که با یک جدول مسیریابی اثبات نمی‌شود

اتصال حس‌گر به لینک تولید باید fail-open باشد. دستگاه مانیتورینگی که با قطع تغذیه‌اش لینک فرآیندی را ببندد، خودش همان اختلالی می‌شود که این معماری ادعا می‌کند ایجاد نمی‌کند. روی باس RS-485 چندنقطه‌ای هیچ SPAN portی وجود ندارد و ضبط با tap سریال منفعل انجام می‌شود؛ آنجا این الزام مهم‌تر است، نه کمتر.

معماری مرجع

۰۵

چهار لایه، چهارده مؤلفه، و یک مرز که هیچ‌وقت عبور نمی‌کند

سلول لبه در دنیای واقعی

سلول لبه در بسیاری از سایت‌ها در کابینت پست یا اتاق کنترل می‌نشیند، نه در رک مرکز داده. مشخصات باید با محل نصب بخواند، وگرنه طراحی روی کاغذ درست است و در سایت نصب نمی‌شود:

- **نصب روی ریل DIN** — رک ۱۹ اینچی در کابینت پست وجود ندارد
- **بدون فن** — فن در محیط گردوغبار صنعتی یک نقطهٔ خرابی است
- **تغذیهٔ ۲۴ ولت مستقیم** — برق کابینت معمولاً DC است، نه ۲۳۰ ولت متناوب
- **دمای کاری منفی ۲۰ تا مثبت ۶۰** — کابینت بیرونی در تابستان از این فراتر می‌رود
- **مقاوم به ارتعاش، با پوشش محافظ** — محیط پالایشگاه و نیروگاه

اگر سایت منطقهٔ خطرناک دارد، تجهیز باید گواهی متناظر داشته باشد؛ در غیر این صورت آن نقطهٔ نصب حذف می‌شود، نه اینکه با تخفیف پذیرفته شود.

پنجرهٔ تغییر در OT، نه در IT

استقرار، ارتقا و بازگشت نباید نیازمند توقف فرآیند باشد. در OT پنجرهٔ تغییر واقعی می‌تواند تعمیرات اساسی سالانه باشد، نه بازهٔ شبانهٔ IT — پس هر کاری که توقف بخواهد عملاً یک سال معطل می‌ماند.

از تعامل تا تصمیم

۰۶

هفت گام، پنج ویژگی که شاهد را شاهد می‌کند، و شاخص‌هایی که باید در محیط مشتری baseline شوند

از تعامل تا تصمیم

هفت گام؛ آخرین گام همیشه یک انسان است، نه یک مدل

شاهدی که این پنج ویژگی را نداشته باشد، شاهد نیست

- اثر انگشت رمزنگاری‌شده
- متولی و مالک
- روش جمع‌آوری
- بازهٔ زمانی
- طبقه‌بندی

رخداد روی گذرگاه مشترک EAOS منتشر می‌شود، نه روی یک گذرگاه داخلی — تعریف گذرگاه دوم در گیت G۶ پورتفولیو معیار رد است.

شاخص	دروازهٔ پایلوت	هدف نسخهٔ نهایی
نرخ ثبت تعامل مجاز در آزمون	دست‌کم ۹۹ درصد	دست‌کم ۹۹٫۹ درصد
تأخیر تا هشدار در سایت (صدک ۹۵)	حداکثر ۱۰ ثانیه	حداکثر ۵ ثانیه
نرخ مثبت کاذب روی خط پایهٔ تأییدشده	حداکثر ۲ درصد	حداکثر ۱ درصد
فرار Decoy در آزمون · مسیر Decoy به کنترل واقعی	صفر	صفر

اعداد بالا هدف طراحی‌اند، نه ادعای عملکرد پیش از سنجش. شاخص‌ها باید در محیط مشتری و روی خط پایهٔ همان سایت اندازه‌گیری شوند.

۰۷ هوش مصنوعی: مشاور، نه تصمیم‌گیرنده

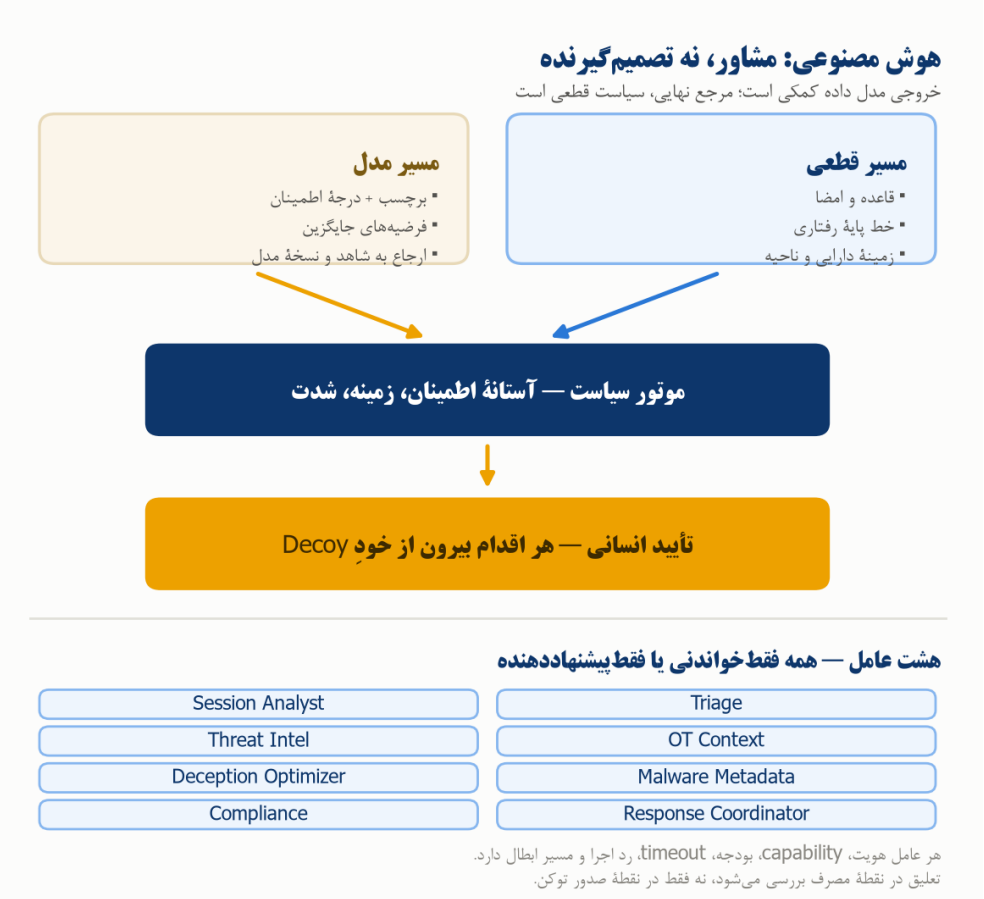
هر خروجی مدل با درجهٔ اطمینان، فرضیهٔ جایگزین و ارجاع به شاهد می‌آید

اصل تفکیک

خروجی مدل یک دادهٔ کمکی است. شدت نهایی و هر اقدام را سیاست قطعی، آستانهٔ اطمینان، زمینهٔ دارایی و تأیید انسانی تعیین می‌کند. این یک تصمیم ثبت‌شدهٔ معماری است و درخواست تغییرش با یک ADR رد می‌شود، نه با یک feature flag.

- **مدل به نمونهٔ خام دسترسی ندارد** — فقط فراداده و گزارش تحلیل جعبهٔ ایمن
- **ابزارها allowlist شده‌اند** — prompt و خروجی ابزار در دفتر ممیزی ثبت می‌شود
- **هر خروجی نسخه‌دار است** — نسخهٔ ویژگی، نسخهٔ مدل و نسخهٔ نگاشت ATT&CK
- **اقدام خودکار وجود ندارد** — مسدودسازی و تغییر قاعده بدون تأیید انجام نمی‌شود

نکته‌ای که از تجربهٔ پلتفرم برمی‌آید: صدور توکن سیاست اجرا نمی‌کند. توکن یک عامل معلق تا انقضا معتبر می‌ماند، پس تعلیق باید در نقطهٔ مصرف بررسی شود، نه فقط در نقطهٔ صدور.



قاعده‌ای که از حلقهٔ بازخورد جلوگیری می‌کند

برای جلوگیری از حلقهٔ خودکارسازی، هر رخداد مبدأ و زنجیرهٔ علیت دارد؛ رخدادی که خودِ سامانه باعثش بوده دوباره وارد صف تصمیم نمی‌شود.

استانداردها و یکپارچگی

۰۸

چهارده مرجع با شاهد متناظر، و درزهایی که مالکشان دام‌تار نیست

استانداردها و جای دام‌تار در پورتفولیو

این ماتریس «هم‌راستایی طراحی» است و ادعای گواهی‌نامه نیست

چهارده مرجع، هرکدام با شاهد متناظر

- **NIST SP 800-82r3** — ایمنی و توپولوژی OT
- **NIST CSF 2.0** — شش کارکرد حاکمیتی
- **NIST SP 800-207** — Zero Trust و هویت بار کاری
- **MITRE D3FEND** — نگاشت اقدام متقابل
- **ISO/IEC 27001/2** — سامانهٔ مدیریت امنیت
- **ISO 22301** — تداوم کسب‌وکار
- **OWASP ASVS / API** — امنیت رابط و API
- **ISA/IEC 62443** — ناحیه و مجرا، دفاع در عمق
- **NIST SP 800-53r5** — کنترل فنی و سازمانی
- **MITRE ATT&CK ICS** — نگاشت TTP و پوشش
- **STIX 2.1 / TAXII** — تبادل هوش تهدید
- **ISO/IEC 27035** — چرخهٔ عمر حادثه
- **CIS Controls v8** — کنترل‌های اولویت‌دار
- **افتا · پدافند غیرعامل** — الزامات ملی، در همان نگاشت

درز با ماژول‌های EAOS

هر ردیف مالک بیرونی دارد؛ دام‌تار در هیچ‌کدام مالک نیست

AEON Kernel · Trust Fabric — هویت کاربر و بار کاری	مصرف‌کننده
Platform Services · Event Bus — انتشار روی گذرگاه مشترک	تولیدکننده
aeon-evidence — ثبت شاهد سازمانی	تولیدکننده
EAOS-Manovr-GRC — نگاشت شواهد کنترل	تأمین‌کننده
CyberTwin · Industrial Twin — اعتبارسنجی پروفایل OT	مصرف‌کننده
EAOS-Aegis-Sandbox — گزارش تحلیل نمونه	مصرف‌کننده
SIEM · SOAR — مقصد صدور رخداد	تولیدکننده

◄ **قرارداد پیش از کد:** OpenAPI، AsyncAPI و Protobuf به‌همراه هفت طرح‌وارهٔ JSON در همین بسته منجمد شده‌اند و یک سرور ساختگی تحویل می‌شود تا دوازده تیم بدون انتظار برای یکدیگر شروع کنند. تغییر ناسازگار در قرارداد یک تصمیم اعلام‌شده است، نه یک اتفاق.

◄ **رخداد روی گذرگاه مشترک، نه گذرگاه خودمان:** نام‌ها در قالب رسمی پلتفرم نوشته شده‌اند و ترتیب کار عمدی است: اول در کاتالوگ مرکزی ثبت می‌شوند، بعد تولیدکننده اعلامشان می‌کند. نوع ثبت‌نشده در انتشار رد می‌شود، و تعریف یک گذرگاه دوم معیار ردِ گیت است.

آنچه تا امروز تولید شده

۰۹

بستهٔ طراحی و تحویل — سنجیده با ابزار، نه اعلام‌شده در متن

آنچه تا امروز تولید شده — سنجیده، نه اعلام‌شده

بستهٔ طراحی و تحویل، نسخهٔ ۲,۲۰,۰ — اندازه‌گیری‌شده در ششم مرداد ۱۴۰۵

۲۳۴	۳۱۸	۷	۹	۱۴
فایل تألیفی	بررسی خودکار	طرحوارهٔ JSON	تصمیم معماری (ADR)	تصمیم ثبت‌شده

بررسی‌های خودکاری که امروز اجرا می‌شوند و سبزند

نردبان گیت پلتفرم EAOS — نتیجهٔ سنجیده، صادقانه قرمز

آنچه اثبات شده است

- ۸ از ۸ در کیت انطباق مالک قرارداد (Aegis)
- ۳۰ بررسی سرتاسری آزمایشگاهی، بدون خطا
- ۱۴ از ۱۵ جهش عمدی، توسط سوئیت گرفته شد

آنچه ادعا نمی‌کنیم

- هیچ کدی نوشته نشده — و در این مرحله نباید می‌شد
- G۱ تا G۸ بدون پیاده‌سازی قابل عبور نیستند
- ۵ شکاف اعلام‌شده در نامتغیرهای ایمنی، باز و مستند

چرا یک سطر قرمز را در کاتالوگ فروش چاپ می‌کنیم

سامانه‌ای که مأموریتش سنجش آمادگی بر پایهٔ شواهد است، نمی‌تواند وضعیت خودش را بدون شاهد اعلام کند. سطر گیت پلتفرم برای این محصول امروز قرمز است و این درست‌ترین خواندن ممکن است: بسته کد ندارد و در این مرحله نباید داشته باشد. ماژولی که اصلاً سنجیده نشود بدترین حالت است، چون برخلاف یک گیت قرمز، سطری در جدول ندارد و نبودش به چشم نمی‌آید.

نقشهٔ راه

۱۰

هشت فاز، دوازده بستهٔ کار موازی، و ترتیبی که با موازی‌شدن تیم‌ها موازی نمی‌شود

هشت فاز تا GA

تا گیت هر فاز امضا نشود، فاز بعد آغاز نمی‌شود

دوازده بستهٔ کار موازی — تیم‌ها فقط از قرارداد منجمدشده استفاده می‌کنند

WP-01 قرارداد و معماری	WP-02 لایهٔ کنترل	WP-03 زمان اجرای لبه	WP-04 فریب IT	WP-05 فریب OT	WP-06 رخداد و شاهد
WP-07 گراف و همبستگی	WP-08 هوش مصنوعی	WP-09 تجربهٔ کاربری	WP-10 یکپارچگی‌ها	WP-11 DevSecOps	WP-12 راستی‌آزمایی و ایمنی

- **موازی‌سازی تیم‌ها، نه موازی‌سازی گیت‌ها:** فریب IT و فریب OT پس از بنیان پلتفرم می‌توانند با دو تیم مستقل جلو بروند و هوشمندی روی دادهٔ مصنوعی آغاز می‌شود؛ ولی ترتیب امضای گیت‌ها حفظ می‌شود. مدت‌ها برآورد اولیه‌اند و به تعداد پروتکل، تعداد سایت و اندازهٔ تیم بستگی دارند.
- **دو نردبان که نباید قاطی شوند:** گیت فاز می‌پرسد «این فاز تمام شده و قابل امضاست؟» و گیت پلتفرم می‌پرسد «این ماژول واقعاً بخشی از پلتفرم است؟». نسخهٔ نهایی محصول، عبور از گیت پذیرش پلتفرم را تضمین نمی‌کند؛ این دو، چیزهای مختلفی می‌سنجند.

گام بعدی و مرزهای اعلام‌شده

۱۲

آنچه برای آغاز لازم است، و آنچه این محصول صریحاً انجام نمی‌دهد

آنچه برای شروع لازم است

- تعیین حامی اجرایی و مالک محصول — گیت‌ها به مرجع تصمیم‌گیرندهٔ مشخص نیاز دارند.
- تصویب رسمی منشور فاز نخست و تصمیم‌های معماری.
- انتخاب سایت مرجع و تعیین مرجع تأییدکنندهٔ ایمنی آن.
- طراحی ناحیهٔ فریب: نگاشت VLAN، اثبات مهار لایهٔ ۲ و نقطهٔ TAP.
- تعیین سیاست نگهداشت، طبقه‌بندی داده و مسیر صدور به SIEM.
- تأمین زیرساخت استقرار ایزوله و مخزن داخلی artifact.
- تصمیم دربارهٔ نگاشت شناسهٔ شاهد سازمانی — مالکش نه ما هستیم و نه سازندهٔ جعبهٔ ایمن.

آنچه در محدودهٔ این سامانه نیست

- اجرای حمله به سامانهٔ واقعی — نه اسکن، نه بهره‌جویی، نه حرکت جانبی.
- کنترل یا تغییر فرآیند صنعتی؛ هیچ مسیر نوشتنی به کنترلر واقعی وجود ندارد.
- اقدام خودکار بدون انسان؛ خروجی مدل پیشنهاد است.
- جایگزینی SIEM، SOAR، EDR یا فایروال.
- اجرای نمونهٔ بدافزار؛ فقط فراداده و گزارش تحلیل پردازش می‌شود.
- حس‌گر درون‌مسیر — حالت inline اصلاً پیاده نمی‌شود تا در دسترس نبودنش تصادفی نباشد.
- شبیه‌سازی سامانهٔ ابزاردقیق ایمنی، و استقرار در سطح Purdue یک و صفر.

حالت استقرار	چه چیزی را حل می‌کند	حالت استقرار	چه چیزی را حل می‌کند
تک‌سایتی	یک لایهٔ کنترل و یک سلول لبه — حالت پایلوت	متمرکز و شعاعی	لایهٔ کنترل مرکزی و یک سلول لبه در هر سایت، تاب‌آور در قطع ارتباط
ایزوله	بدون هیچ وابستگی اینترنتی در زمان اجرا؛ تبادل فقط با بستهٔ امضاشده	فدرال	هر سازمان لایهٔ کنترل مستقل دارد؛ تنها هوش تهدید و تجمیع مبادله می‌شود
سایت گسستهٔ OT	کار مستقل در قطع کامل ارتباط با مرکز	آزمایشگاه	اعتبارسنجی اثر انگشت و ایمنی پروفایل، پیش از استقرار در سایت

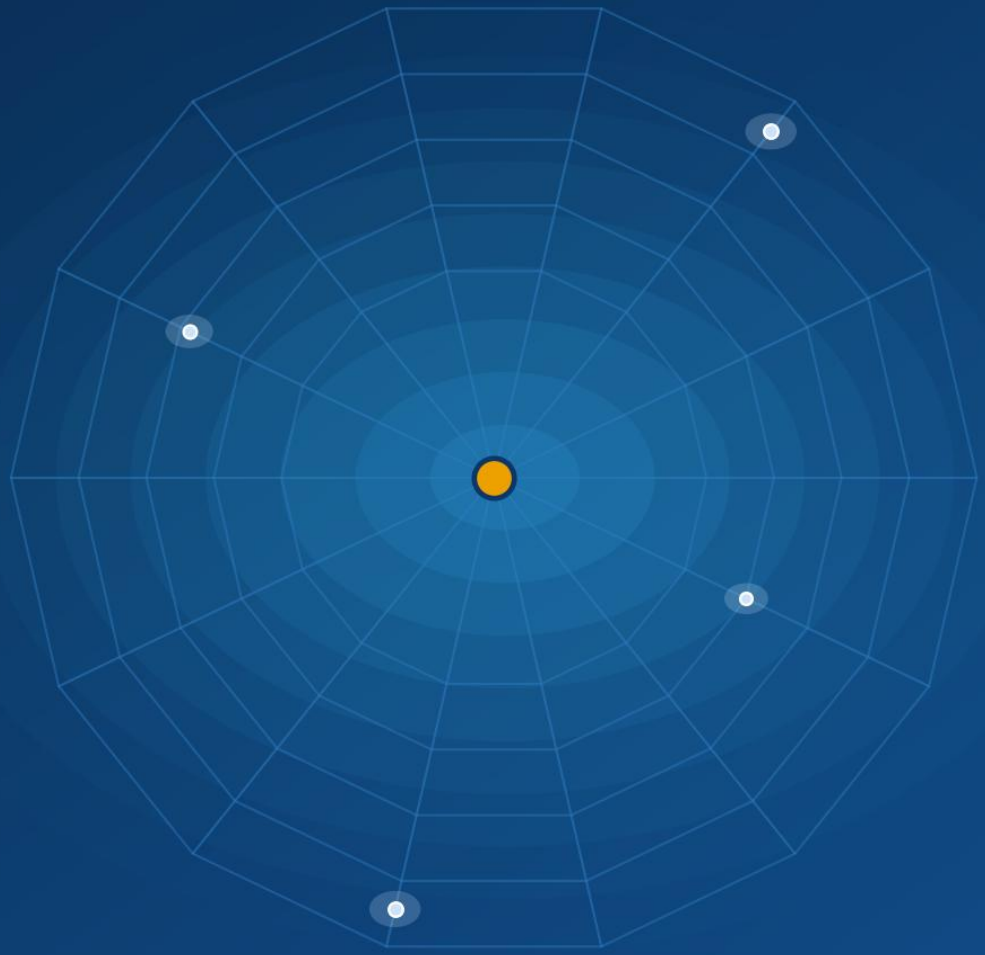
پیشنهاد گام بعدی

یک نشست فنی-مدیریتی برای مرور تصمیم‌های معماری و مدل ایمنی، و انتخاب یک سایت مرجع برای آزمایشگاه — پروفایل IT روی محیط جدا، پیش از آنکه هر تصمیمی دربارهٔ OT گرفته شود.

آنچه پیشنهاد می‌شود، یک حس‌گر دیگر نیست.

پیشنهاد این است که سازمان یک دارایی بسازد که هیچ کاربر مجازی

به آن دست نمی‌زند — و هر تماس با آن را به شاهد تبدیل کند.



فریب — دارایی جعلی در IT و OT/ICS

کشف — سیگنال کم‌نویز، پیش از دارایی واقعی

شاهد — تغییرناپذیر، قابل ممیزی، قابل صدور

ایمنی — بدون هیچ مسیر نوشتنی به فرآیند

گام بعدی

یک آزمایشگاه مرجع، و امضای منشور فاز نخست

دام‌تار

EAOS

Enterprise AI Operating System