Padvish®

Padvish OT

راهکار امنیت عملیاتی Padvish OT برای محیط‌های کنترل صنعتی (ICS/OT)

حوادث سایبری مهم در دو دهه اخیر همچون حمله سایبری به سه شرکت فولاد (۱۴۰۱)، حملات سایبری به جایگاه‌های سوخت (۱۴۰۰ و ۱۴۰۲)، انفجار خطوط انتقال گاز (۱۴۰۲) و آلودگی‌های بدافزاری در صنایع کشور، اهمیت تهدیدات سایبری و بدافزاری علیه صنایع کشور (حوزه OT) را بیش ازپیش نشان می‌دهد.

پادویش OT، راهکاری اختصاصی برای سیستم‌های کنترل صنعتی با رویکرد دفاع در عمق است که برای حفظ در دسترس بودن (Availability) و صحت (Integrity) سیستم‌های کنترل صنعتی (ICS/SCADA) در برابر تهدیدات بدافزاری و باج‌افزاری، بدون تأثیر منفی بر عملکرد این سیستم‌های حساس، طراحی شده است.

این راهکار، امنیت را بدون نیاز به تغییر در نرم‌افزارهای بهره‌برداری و لاجیک سیستم کنترل و با حداقل سربار بر سیستم‌های مهندسی (ES) و سیستم‌های بهره‌برداری (HMI/OT/OS) و سرورهای لاگ تأمین می‌کند.

۱ لایه محافظت سیستم میزبان صنعتی (OT Host-based Protection Core)

محافظت بلادرنگ پیشرفته

حملات پیشرفته به زیرساخت‌های صنعتی در چند سال اخیر نشان می‌دهد که صرف استفاده از روش‌های مبتنی بر امضا درپیشگیری از حملات به شبکه‌های کنترل صنعتی کافی نیست، لذا پادویش OT از ترکیب موتورهای مبتنی بر امضا (Signature-Based) و تحلیل رفتاری (Behavioral Analysis) و هوش‌مصنوعی برای شناسایی تهدیدات شناخته‌شده و ناشناخته (Zero-Day) با تمرکز بر جلوگیری از اختلال در سرویس‌های حیاتی استفاده می‌نماید.

پشتیبانی از AMSI

برای مقابله با تهدیدات اسکریپتی
در سیستم‌های OS، ES

کنترل حافظه‌های جانبی (USB)

اعمال سیاست‌های امنیتی برای شناسایی و جلوگیری از نفوذ تهدیدات از طریق حافظه‌های USB در سیستم‌های کنترل صنعتی ESD، DCS، رولیاژ، تله‌متری، دیسپاچینگ و ...

موتور هوشمند ضد باج‌افزار چندلایه

در سیستم‌های OS، ES و سیستم‌های لاگ صنعتی (Historian, SOE, ...)

- **لایه محافظت در برابر دستکاری** (Tamper Protection): جلوگیری از رمزنگاری فایل‌ها توسط باج‌افزارها.
- **محافظت از سکتور راه‌انداز** (MBR Protection): در برابر تهدیداتی که فرایند بوت سیستم‌های ES و OS را هدف می‌گیرند.
- **تشخیص مبتنی بر فایل‌های طعمه** (Bait Mechanism): استقرار فایل‌های طعمه در مسیرهای حساس سیستم‌های کنترل صنعتی برای شناسایی و مهار زودهنگام فعالیت باج‌افزارها.

این مؤلفه دارای گواهی تشخیص ۱۰۰% باج‌افزارها از آزمایشگاه AV-Test آلمان است.

لایه‌های معماری

لایه‌های معماری

۲ لایه محافظت برنامه‌ها و شبکه کنترل صنعتی (OT Applications & Network Control)

کنترل ابزار (Device Control)

مدیریت دسترسی ابزارها

کنترل دسترسی به تجهیزات صنعتی از طریق وب (Web-based Control)

کنترل دسترسی به آدرس‌های وب در تجهیزات جدید صنعتی قابل پیکربندی و نظارت از طریق وب

شبکه‌های مورد اعتماد (Trusted Network)

امکان تعریف شبکه های مورد اعتماد، بسته به محل اتصال کاربر، محدودسازی اتصال به شبکه، و تهیه گزارش جامع از نقض سیاست های تعریف شده در شبکه های مورد اعتماد

فایروال (Firewall)

دو لایه محافظتی برای کنترل کامل ترافیک ورودی و خروجی:
لایه ۳: کنترل بسته‌ها در سطح هسته سیستم
لایه ۷: کنترل اتصال‌ها بر پایه برنامه

کنترل برنامه‌ها (Applications Control)

پیشگیری از اجرای برنامه‌های غیرمجاز بر اساس نرم‌افزار، سازنده و محتوا در سیستم‌های کنترل صنعتی
Mitsubishi، Honeywell، Emerson، HIMA، ABB، Yokogawa، Siemens و ...

۳ لایه پایش و تحلیل رفتار (Behavior Monitoring & Detection)

پایش دسترسی به رجیستری
(Registry Access Monitoring)

تشخیص اتصال‌های غیرمجاز به اینترنت و اینترانت (شبکه IT) و شبکه‌های بالادستی

Unauthorized Connection Detection
شناسایی تلاش‌های ارتباطی غیرمجاز یا غیرمنتظره از سیستم‌های DCS و ESD

ارزیابی مستمر آسیب‌پذیری‌های سیستم عامل با حفظ پایداری سیستم‌های OT

برای شناسایی وصله‌های مفقود شده (Missing Patches) و پیکربندی‌های ناامن در سیستم‌های قدیمی (Legacy Systems).

لایه‌های معماری

۴ لایه امنیت تخصصی صنعتی (OT-Specific Security)

پشتیبانی کامل از محیط‌های کاملاً ایزوله (Air-Gapped Mode)

با امکان مدیریت و به‌روزرسانی کاملاً آف‌لاین.

پیکربندی‌های آماده (Out-of-the-Box Profiles)

برای نرم‌افزارهای رایج صنعتی (مانند WinCC، STEP 7 و ...).

کمک به انطباق (Compliance Assistance)

سنجش انطباق با الزامات امنیتی مبتنی بر استانداردهای مرجع نظیر، ISA/IEC 62443
NIST 800-82، AGA، API، NERC- CIP، IAEA

۵ لایه مدیریت متمرکز و پاسخ (Centralized Management & Response)

کنسول مدیریت متمرکز (Padvish Management Console)

- امکان پشتیبانی از ساختار سلسله‌مراتبی محیط عملیاتی برای گروه‌بندی کلاینت‌های تحت مدیریت در شبکه‌های صنعتی مطابق با معماری Purdue و Zero Trust.
- سیستم گزارش‌گیری جامع با قابلیت سفارشی‌سازی.
- امکان شناسایی و مشاهده دارایی‌های شبکه صنعتی.

حالت صرفاً شناسایی (Detection-Only Mode)

- با توجه به شناخت و تجربه کامل نسبت به دغدغه‌های شبکه‌های صنعتی در تیم طراحی محصول، جهت کاهش ریسک اختلال ناخواسته در سیستم‌های کنترل صنعتی و حفظ پایداری کامل شبکه و فرایند کنترل صنعتی، امکان استقرار ابتدایی عامل امنیتی صرفاً در حالت پایش، برای ارزیابی ریسک و شناسایی تهدیدات پیش از اعمال سیاست‌های محدود کننده دیده شده است.

قابلیت یکپارچه‌سازی با خدمات مدیریت‌شده (MDR/MSSP) امن‌پرداز به شکل امن

- امکان ارسال امن رویدادهای امنیتی به سرویس امن‌پرداز برای تحلیل پیشرفته و پاسخ مدیریت شده توسط متخصصین مجرب امنیت سایبری OT با رعایت اصول محافظت و اتصال امن و با اخذ مجوز از نهادهای ذی‌صلاح توسط تیم خدمات تخصصی امنیت سایبری OT

دامنه پوشش عملیاتی

- **سیستم‌عامل‌های قدیمی (Legacy)**
  - سازگار و بهینه‌شده برای سیستم‌های مبتنی بر Windows 7 SP1+، Windows XP SP3+ و نسخه‌های بعدی، با درنظرگیری محدودیت منابع و قدیمی بودن سخت‌افزار IPC ها
- **محیط‌های حساس و real-time عملیاتی**
  - مناسب برای زیرساخت‌های حیاتی (Critical Infrastructure)، شبکه‌های کاملاً ایزوله (Air-Gapped)
  - با حفظ ویژگی‌های observability، reliability، stability و resiliency در شبکه‌های صنعتی، مناسب سیستم‌های کنترل بلادرنگی که تحمل هیچ‌گونه توقف عملیاتی را ندارند.

قابلیت‌های کلیدی

حفظ در دسترس‌بودن (Availability)

تأثیر ناچیز بر زمان پاسخ (Latency) سیستم‌های بلادرنگ صنعتی.

حفاظت یکپارچه (Unified Protection)

تلفیق کنترل‌های امنیت مرسوم IT (مانند آنتی‌ویروس، فایروال) با ملاحظات و کنترل‌های حیاتی OT (مانند کنترل برنامه‌ها و دستگاه) در یک پلتفرم یکپارچه با حفظ ویژگی‌های observability، reliability، stability و resiliency در شبکه‌های صنعتی جزیره‌ای PLC ـ مبنا، شبکه‌های توزیع‌شده DCS و شبکه‌های صنعتی متصل.

افزایش تاب‌آوری عملیاتی (Operational Resilience)

تقویت توانایی سیستم‌های ICS برای ادامه ارائه سرویس در مواجهه با حوادث سایبری و بازیابی سریع.

مدیریت متمرکز ریسک (Centralized Risk Management)

ایجاد دید و کنترل یکپارچه از دارایی‌های صنعتی پراکنده در نواحی (Zones) و مجراها (Conduits)، برای تصمیم‌گیری متمرکز و واکنش سریع.

طراحی و توسعه محصول منطبق با استانداردهای بین‌المللی و اسناد بالادستی ملی حوزه امنیت OT

بسیاری از استانداردها و اسناد بالادستی امنیت سایبری در حوزه OT نظیر ISA/IEC 62443، اسناد مرکز راهبردی افتا و سازمان پدافند غیرعامل، استفاده از راهکارهای امنیتی خاص و تخصصی که شامل آنتی‌ویروس‌های OT است را به‌عنوان الزام معرفی می‌کنند. طراحی محصول در قالب الزامات ISA/IEC 62443-4-1 اطمینان از فرایند SDLC را ایجاد می‌نماید.

تطابق با نیازهای خاص OT صنایع کشور

آنتی‌ویروس‌های عمومی IT ممکن است به دلیل تشخیص نادرست، فایل‌های برنامه‌های مهندسی و بهره‌برداری OT را به‌عنوان تهدید شناسایی کرده و باعث توقف یا اختلال در فرآیندها شوند. آنتی‌ویروس تخصصی OT که براساس تجربه میدانی از صنایع کشور طراحی و پیاده‌سازی شده، این ریسک را کاهش می‌دهد.

چرا Padvish OT؟

۱. **طراحی ویژه و آگاه به محدودیت‌های OT**
معماری سبک، حساسیت به پروتکل‌های صنعتی، آن را از راهکارهای عمومی IT متمایز می‌کند.

۲. **سازگاری عمیق با سامانه‌های قدیمی (Legacy)**
پشتیبانی مؤثر از سیستم‌عامل‌ها (تا آخرین نسخه ویندوز) و نرم‌افزارهای صنعتی که امکان ارتقاء یا تعویض ندارند.

۳. **انعطاف در مدل عملیاتی**
قابلیت اجرا به‌صورت مستقل (Standalone) توسط تیم داخلی یا تحت نظارت و مدیریت (Managed) مرکز عملیات امنیت (SOC) اختصاصی.

۴. **توسعه مبتنی بر تجربه میدانی**
شکل گرفته بر پایه درک واقعی از چالش‌های امنیتی، معماری شبکه و الزامات عملیاتی محیط‌های صنعتی داخلی.

۵. **تطابق با نیازهای خاص OT**
آنتی‌ویروس تخصصی OT برای سامانه‌های کنترل صنعتی، قابلیت‌های انطباق با پروتکل‌ها و نرم‌افزارهای خاص این سامانه‌ها را دارد، درحالی که آنتی‌ویروس‌های عمومی IT نمی‌توانند به درستی در محیط‌های حساس OT عمل کنند و می‌توانند مشکلات و خساراتی را برای صنایع به همراه داشته باشند.

۶. **آگاهی از بردارهای خاص OT در حملات به صنایع کشور**
حملات هدفمند و بدافزارهای ساخته شده برای سامانه‌های کنترل صنعتی کشور، نیازمند راهکارهای امنیتی خاص هستند که تنها در آنتی‌ویروس و EDR تخصصی بومی یافت می‌شود.

"شرکت نرم افزاری امن پرداز محصولات و خدمات متنوعی را با نام تجاری پادویش جهت مقابله با طیف گسترده تهدیدات و حملات سایبری در بخش خانگی و سازمانی و اکنون در حوزه صنعتی (OT) ارائه می نماید."

شرکت نرم افزاری امن پرداز®

پادویش®

www.padvish.com
info@amnpardaz.com