1 **predictive maintenance**

حفاظت از زیرساخت های حیاتی: نقش هوش مصنوعی در امنیت OT

حفاظت از زیرساخت‌های حیاتی برای حفظ عملکرد روان خدمات ضروری مانند پست برق، پالایشگاه نفت، تصفیه آب و سیستم‌های حمل و نقل ضروری است. با افزایش ادغام فناوری عملیاتی (OT) و افزایش تهدیدات سایبری پیچیده، نقش هوش مصنوعی (AI) در امنیت OT اهمیت فزاینده ای پیدا کرده است. هوش مصنوعی می‌تواند نقش مهمی در افزایش امنیت زیرساخت‌های حیاتی با شناسایی و پاسخگویی به تهدیدات سایبری در زمان واقعی، بهبود قابلیت‌های واکنش به حادثه، و امکان نگهداری پیش‌بینی‌کننده برای جلوگیری از خرابی سیستم ایفا کند.

برخی از مزایای کلیدی وجود دارد که در آنها هوش مصنوعی به امنیت OT کمک می کند:

- **تشخیص تهدید و تشخیص ناهنجاری**

سیستم‌های مجهز به هوش مصنوعی می‌توانند حجم زیادی از داده‌های تولید شده توسط شبکه‌های OT، از جمله ترافیک شبکه، گزارش‌های سیستم و داده‌های حسگر را تجزیه و تحلیل کنند تا الگوهای غیرعادی و نقض‌های امنیتی احتمالی را شناسایی کنند. الگوریتم‌های یادگیری ماشینی می‌توانند از داده‌های تاریخی بیاموزند تا ناهنجاری‌ها و فعالیت‌های مخربی را که از رفتار عادی منحرف می‌شوند، شناسایی کنند و تشخیص زودهنگام تهدید را ممکن می‌سازند.

- **اقدامات امنیتی تطبیقی**

هوش مصنوعی می تواند به صورت پویا اقدامات امنیتی را بر اساس تهدیدات در حال تحول و تغییر شرایط سیستم تنظیم کند. با یادگیری مداوم از داده‌های جدید، الگوریتم‌های هوش مصنوعی می‌توانند سیاست‌های امنیتی، کنترل‌های دسترسی و پیکربندی‌ها را برای کاهش خطرات نوظهور و تقویت وضعیت کلی امنیتی تطبیق داده و به‌روزرسانی کنند.

- **نظارت در زمان واقعی و پاسخ به حادثه**

هوش مصنوعی می‌تواند نظارت بر زمان واقعی سیستم‌های OT را فراهم کند و به پرسنل امنیتی در مورد فعالیت‌های مشکوک یا حملات سایبری احتمالی هشدار دهد. الگوریتم‌های هوش مصنوعی می‌توانند داده‌ها را از منابع متعدد برای شناسایی شاخص‌های سازش (IoC) تجزیه و تحلیل و مرتبط کنند و با پیشنهاد اقدامات کاهش مناسب، از تلاش‌های واکنش به حادثه پشتیبانی کنند.

- **مدیریت آسیب پذیری**

هوش مصنوعی می‌تواند به شناسایی و اولویت‌بندی آسیب‌پذیری‌ها در سیستم‌های OT کمک کند. الگوریتم‌های هوش مصنوعی با اسکن شبکه‌ها، تجزیه و تحلیل پیکربندی‌های سیستم و ارزیابی نسخه‌های نرم‌افزار، می‌توانند نقاط ضعف بالقوه‌ای را که می‌توانند توسط مهاجمان سایبری مورد سوء استفاده قرار گیرند، مشخص کنند. این اطلاعات به تیم‌های امنیتی کمک می‌کند تا ابتدا منابع خود را بر روی حساس‌ترین آسیب‌پذیری‌ها متمرکز کنند.

021-88109330
www.navak-ai.ir 0933-6889690 info@navak-ai.ir

ناوک هوشمند پویان
Edge Intelligent Enterprise

2 **predictive maintenance**

- **تجزیه و تحلیل رفتار کاربر**

هوش مصنوعی می‌تواند رفتار کاربر در شبکه‌های OT را برای شناسایی فعالیت‌های غیرعادی یا مشکوک که ممکن است نشان‌دهنده تهدیدات داخلی باشد، تجزیه و تحلیل کند. سیستم‌های هوش مصنوعی با ایجاد خطوط پایه رفتار عادی کاربر و نظارت مستمر برای انحرافات، می‌توانند خطرات امنیتی بالقوه را علامت‌گذاری کنند و مداخله به موقع را امکان‌پذیر کنند.

شرکت لنر در ارائه شبکه افزارهای امنیتی سخت جان، که می تواند هوش مصنوعی را در امنیت OT فعال کند، متخصص است. با استفاده از ابزارهای هوش مصنوعی لبه شرکت لنر، سازمان ها می توانند قابلیت های امنیتی OT خود را با استقرار الگوریتم های هوش مصنوعی به طور مستقیم در لبه شبکه های خود افزایش دهند. این امر تشخیص تهدید در زمان واقعی را تقویت می کند، زمان پاسخ را بهبود می بخشد، حفظ حریم خصوصی داده ها را تضمین می کند، استفاده از پهنای باند را بهینه می کند، و انعطاف پذیری را در محیط های عملیاتی چالش برانگیز فراهم می کند.