4 روشی که موجب تاثیر هوش‌مصنوعی مولد (GenAI) بر CISOها و تیم‌های آنها می‌شود

ChatGPT و مدل‌های زبان بزرگ نشانه‌های اولیه این هستند که چگونه هوش مصنوعی مولد بسیاری از فرآیندهای تجاری را شکل می‌دهد. رهبران امنیت و مدیریت ریسک، به‌ویژه CISOها و تیم‌های آن‌ها باید از نحوه ساخت و مصرف هوش‌مصنوعی مولد (GenAI) سازمانشان مطمئن باشند و تأثیرات آن بر امنیت سایبری را بررسی کنند.

مرور

اثرات:

- گسترش اعلامیه‌های هوش‌مصنوعی مولد (GenAI) در بازارهای امنیتی و مدیریت ریسک هنوز هم می‌تواند باعث بهبود بهره‌وری و دقت تیم‌های امنیتی شود، اما همچنین باعث اتلاف و ناامیدی می‌شود.

- مصرف برنامه‌های GenAI، مانند مدل‌های زبان بزرگ (LLMs)، از آزمایش‌های کسب و کار و مدیریت نشده، پذیرش کارکنان موقت، سطوح حمله جدید و خطرات مربوط به حریم خصوصی فردی، داده‌های حساس و مالکیت معنوی سازمانی را ایجاد می‌کند.

- بسیاری از کسب و کارها عجله دارند تا از مالکیت معنوی خود استفاده کنند و برنامه‌های کاربردی Gen AI خود را توسعه دهند و الزامات جدیدی برای امنیت برنامه‌های هوش مصنوعی ایجاد کنند.

- مهاجمان از هوش‌مصنوعی مولد (GenAI) استفاده خواهند کرد. آنها با ایجاد محتوای به ظاهر معتبرتر، طعمه‌های فیشینگ و جعل هویت انسان در مقیاس شروع کرده‌اند. عدم اطمینان در مورد اینکه چگونه و تا چه حدی آن‌ها می‌توانند هوش‌مصنوعی مولد (GenAI) را برای حملات پیچیده‌تر استفاده کنند، نیاز به نقشه‌های راه امنیت سایبری انعطاف پذیرتر دارد.

توصیه‌ها:

برای پرداختن به تأثیرات مختلف هوش مصنوعی مولد بر برنامه‌های امنیتی سازمان خود، مدیران ارشد امنیت اطلاعات (CISOs) و تیم‌های آنها باید:

- آزمایش‌های هوش‌مصنوعی مولد (GenAI) را با دستیاران چت برای مرکز عملیات امنیت (SOC) و امنیت برنامه‌ها آغاز کنید.

- با همتایان سازمانی که دارای علایق فعال در هوش‌مصنوعی مولد (GenAI) هستند، مانند موارد قانونی و انطباق، و خطوط تجاری برای تدوین خط‌مشی‌های کاربر، آموزش و راهنمایی کار کنید. این کمک می‌کند تا استفاده‌های غیرمجاز از هوش‌مصنوعی مولد (GenAI) به حداقل برسد و خطرات نقض حریم خصوصی و کپی رایت کاهش یابد.

- از چارچوب اعتماد هوش مصنوعی، مدیریت ریسک و امنیت (AI TRiSM) هنگام توسعه برنامه های شخص اول جدید یا مصرف برنامه‌های شخص ثالث جدید که از LLM و GenAI استفاده می کنند، استفاده کنید.

- تقویت روش‌هایی برای چگونگی ارزیابی قرار گرفتن در معرض تهدیدات غیر قابل پیش‌بینی و اندازه‌گیری تغییرات در اثربخشی کنترل‌های خود، زیرا آنها نمی‌توانند حدس بزنند که آیا و چگونه بازیگران مخرب ممکن است از GenAI استفاده کنند.

فرضیات برنامه ریزی استراتژیک

تا سال 2027، هوش مصنوعی مولد به کاهش 30 درصدی نرخ های مثبت کاذب برای آزمایش امنیت برنامه و تشخیص تهدید کمک خواهد کرد و نتایج حاصل از تکنیک‌های دیگر را برای دسته‌بندی رویدادهای بدخیم از دیگر روش‌ها اصلاح می کند.

تا سال 2025، حملاتی که از هوش مصنوعی مولد (GenAI) استفاده می‌کنند، سازمان‌های هوشیار امنیتی را مجبور می‌کنند تا آستانه‌های پایین‌تری برای شناسایی فعالیت‌های مشکوک، ایجاد هشدارهای نادرست بیشتر، و در نتیجه نیاز به پاسخ‌های انسانی بیشتر و نه کمتر داشته باشند.

4 روشی که موجب تاثیر هوش‌مصنوعی مولد (GenAI) بر CISOها و تیم‌های آنها می‌شود

معرفی

سطح تبلیغات، مقیاس و سرعت پذیرش ChatGPT آگاهی کاربر نهایی را از LLMها افزایش داده است که منجر به استفاده‌های کنترل نشده از برنامه‌های کاربردی LLM شده است. همچنین دریچه‌هایی برای آزمایش‌های تجاری و موجی از استارت‌آپ‌های مبتنی بر هوش مصنوعی را بازکرده است که نوید منحصربه فرد را می‌دهند.

گزاره ارزش از برنامه‌های جدید LLM و GenAI بسیاری از تیم‌های پروژه کسب و کار و فناوری اطلاعات در حال حاضر ابتکارات GenAI را راه اندازی کرده اند یا به زودی شروع خواهند شد.

CISOها و تیم‌های امنیتی باید برای تأثیرات هوش مصنوعی مولد در چهار نوع مختلف آماده شوند:

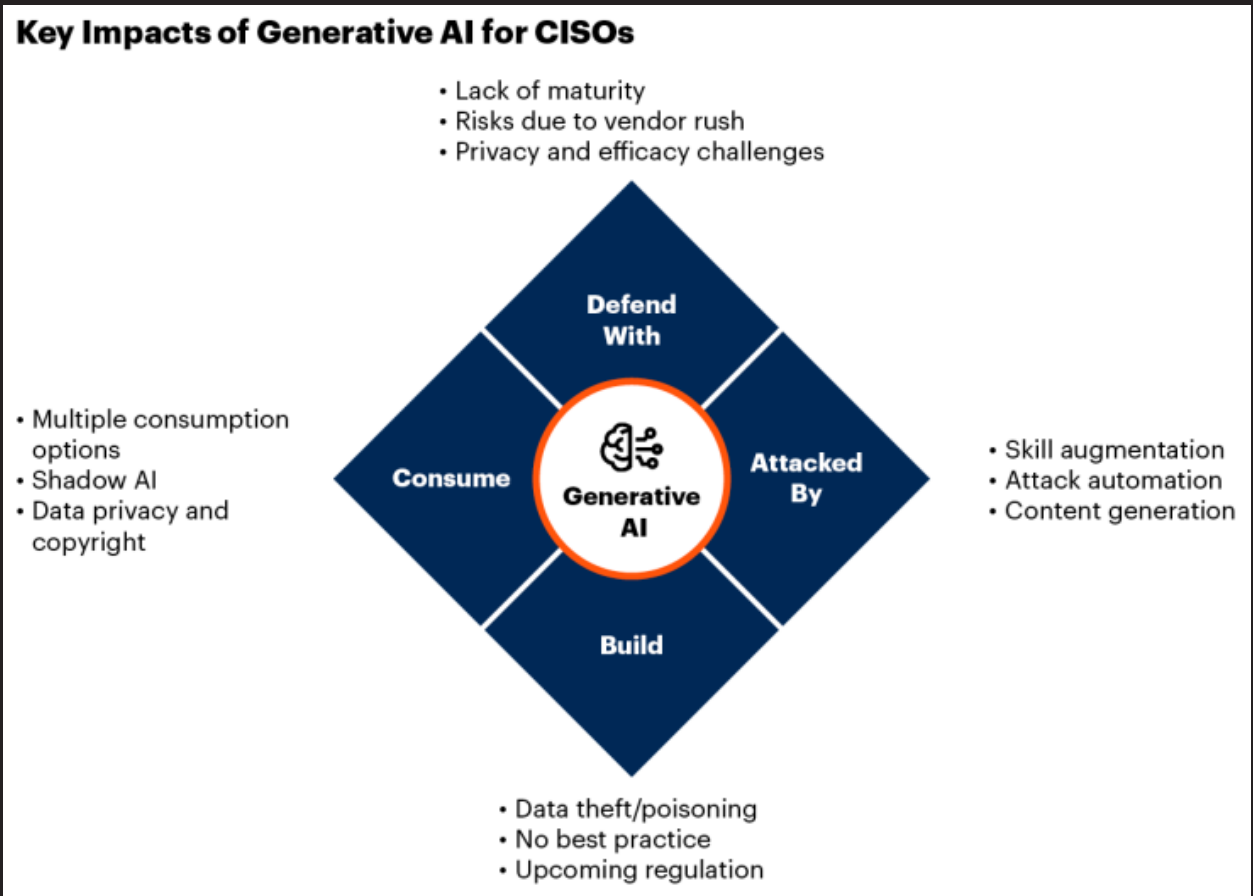
مناطق (همچنین به شکل 1 مراجعه کنید):

1. "دفاع با" هوش مصنوعی امنیت سایبری مولد: دریافت حکم برای بهره‌برداری از فرصت‌های GenAI برای بهبود امنیت و مدیریت ریسک، بهینه‌سازی منابع، دفاع در برابر تکنیک‌های حمله در حال ظهور یا حتی کاهش هزینه‌ها.
2. "حمله توسط" GenAI: انطباق با بازیگران مخرب در حال تحول تکنیک‌های خود و یا حتی بهره‌برداری از بردارهای حمله جدید به لطف توسعه ابزار و تکنیک های GenAI.
3. ابتکارات سازمانی ایمن برای «ساخت» برنامه‌های کاربردی GenAI: برنامه‌های هوش مصنوعی سطح حمله گسترده‌ای دارند و خطرات بالقوه جدیدی را ایجاد می‌کنند که نیازمند تعدیل رویه‌های امنیتی برنامه‌های کاربردی موجود است.
4. مدیریت و نظارت بر نحوه "مصرف" GenAI توسط سازمان: ChatGPT اولین نمونه بود. دستیارهای تعبیه شده GenAI در برنامه های موجود بعدی خواهند بود. همه این برنامه‌ها دارای الزامات امنیتی منحصر به فردی هستند که توسط کنترل های امنیتی قدیمی برآورده نمی‌شوند.

کسب و کارها بدون در نظرگرفتن امنیت، از هوش مصنوعی مولد استقبال خواهند کرد.

این تحقیق از طریق تبلیغات شفافیت را ارائه می‌کند و توصیه‌های عملی را برای هر یک از این چهار حوزه تاثیرگذاری ارائه می‌کند، که به سازمان‌ها و تیم‌های آنها امکان می‌دهد به سرعت با این سرعت سریع تغییر سازگار شوند.

شکل 1: تاثیرات کلیدی هوش مصنوعی مولد برای CISO



تاثیرات و توصیه‌ها

اعلامیه‌های بیش از حد خوش بینانه GenAI در مدیریت امنیت و ریسک می‌تواند باعث پیشرفت شود، اما همچنین منجر به اتلاف و ناامیدی شود.

گارتنر هوش مصنوعی امنیت سایبری مولد را به عنوان تکنیک های GenAI تعریف می‌کند که نمایشی از مصنوعات را از داده های موجود (امنیت سایبری) یا از طریق عوامل شبیه‌سازی می‌آموزد و سپس از آن برای تولید مصنوعات جدید استفاده می‌کند.

همانطورکه از نام آن پیداست، هوش مصنوعی امنیت سایبری مولد موارد استفاده اصلی خود را از GenAI گرفته است.

گارتنر بیش از 30 اطلاعیه ارائه دهندگان امنیتی را بررسی کرده است. دو مورد از رایج ترین موارد استفاده از هوش مصنوعی امنیت سایبری، دستیاران توسعه برنامه امن و چت‌بات‌های عملیات امنیتی هستند.

دستیاران توسعه برنامه ایمن

ابزارهای تولید کد (به عنوان مثال، GitHub Copilot، Amazon Code Whisperer) ویژگی‌های امنیتی را تعبیه کرده‌اند، و ابزارهای امنیتی برنامه در حال حاضر از برنامه‌های LLM استفاده می‌کنند.

موارد استفاده نمونه برای این دستیاران کد ایمن عبارتند از:

1. **هدف قراردادن دردرجه اول تیم های امنیتی برنامه:**

■**تشخیص آسیب‌پذیری**: مشکلات موجود در قطعه کد وارد شده در پیام‌ها یا با انجام اسکن کد منبع را برجسته می‌کند.

■**کاهش مثبت کاذب**: این ویژگی به عنوان یک لایه تأیید برای سایر تکنیک‌های تجزیه و تحلیل کد استفاده می‌شود، این ویژگی هشدار و کد مربوطه را تجزیه و تحلیل می‌کند و به زبان مکالمه نشان می‌دهد که چرا ممکن است مثبت کاذب (False Positive) باشد.

■**دستیار اصلاح**: به‌روزرسانی‌هایی را در کد پیشنهاد می‌کند تا شناسایی‌شده را برطرف کند.

آسیب‌پذیری‌ها به عنوان بخشی از خلاصه‌ای که تولید می‌شود.

2. هدف قراردادن دردرجه اول تیم های توسعه، نه پرسنل امنیتی:

■**تولید کد:** اسکریپت/کد را از ورودی توسعه‌دهندگان شامل نظرات یا دستورالعمل‌های زبان طبیعی ایجاد می‌کند یا به عنوان یک ابزار تکمیل کد پیشرفته عمل می‌کند. برخی از ابزارها همچنین می‌توانند نشان دهند که آیا کد تولید شده شبیه یک پروژه منبع باز است یا می‌تواند به تأیید اعتبار کد (تولید شده یا نوشته شده توسط انسان) با شیوه‌های امنیتی استاندارد صنعت کمک کند.

■**ایجاد تست واحد:** مجموعه‌ای از آزمایش‌ها را برای یک تابع ارسال شده پیشنهاد می‌کند تا مطمئن شود رفتار آن مطابق انتظار است و در برابر ورودی‌های مخرب مقاوم است.

■**مستندات کد:** توضیحاتی را درباره کاری که یک قطعه کد انجام می دهد یا تأثیر تغییر کد ایجاد می کند.

در حالی که شناسایی موارد استفاده آسان است، هنوز برای اندازه گیری کیفی مرتبط با این دستیاران خیلی زود است. در حالی که برخی از ارزیابی‌های موقت ChatGPT نیاز به احتیاط دارند، ارائه‌دهندگان تخصصی منابع زیادی را روی این ابزارها سرمایه‌گذاری می‌کنند و گارتنر پیش‌بینی می‌کند در آینده پذیرش گسترده‌ای داشته باشد.

یکپارچه سازی ابزار عملیات امنیتی

ابزارهای GenAI راه خود را به تعدادی از ابزارهای عملیات امنیتی از فروشندگانی مانند Microsoft، Google، SentinelOne، CrowdStrike و Cisco باز کرده اند. این ابزارها پتانسیل بهبود بهره‌وری و مجموعه مهارت مدیران عادی و بهبود نتایج امنیتی و ارتباطات را دارند.

با ما درتماس باشید

شرکت "داده پردازی هوشمند کندو" درسال 1402 به منظور ارائه خدمات فناوری اطلاعات و ارتباطات به ویژه در حوزه امنیت اطلاعات تاسیس گردید. هدف اصلی ما ارائه راهکارهای جامع امنیت، جهت حفاظت از اطلاعات و دارایی‌های دیجیتال سازمان‌ها می‌باشد. در تلاش هستیم با خدمات مشاوره، اجرا، پیاده‌سازی و راهبری پروژه‌ها و همچنین ارائه راهکارهای نوآورانه و انعطاف پذیر، به نیازها و انتظارات بازار پاسخ دهیم. ما با توسعه دانش و مهارت کارکنان خود، به افزایش بهره‌وری و ارزش آفرینی می‌پردازیم.

شعار شرکت:

"سپر امنیتی ما، همراهی قدرتمند برای آینده‌ی شما"

www.csdpc.ir

info@csdpc.ir