
Razban
Atlas
Fanavaran

معرفی و چشم انداز

اطلس فناوران رازبان حاصل سال‌ها تجربه‌ی فردی و ســـپس همکاری تیمی متخصصان در حوزه‌های متنوع فناوری و مدیریت بحران اســـت. این مجموعه از سال 1395 با فعالیت‌های مستقل آغاز شد، در سال 1401 به شـــکل یک تیم منسجم درآمد و طی سال‌های 1402 تا 1404 زیرســـاخت‌ها و ساختارهای خود را پایه‌گذاری و تثبیت کرد. امروز رازبان به‌عنوان برندی رســـمی و معتبر، وارد دوره‌ای نوین از رشد و نوآوری شده و راهکارهایی پایدار، استاندارد و قابل اتکا برای سازمان‌ها و کسب‌وکارها ارائه می‌دهد.

در دنیای پرشتاب امروز، رشد سازمان‌ها تنها با نوآوری و بهره‌گیری از فناوری ممکن است؛ اما این مسیر بدون لایه‌های ایمنی و پایداری دوام نخواهد داشت. رازبان پیش از هر چیز شرایط واقعی هر سازمان را می‌سنجد و بر همان اســـاس راهکارهایی متناســـب طراحی می‌کند؛ راهکارهایی که همگام با سرعت تغییرات، امنیت و اســـتمرار را نیز تضمین می‌کنند. در ادامه، رویکردها و روش‌هایی را معرفـــی می‌کنیم که این نگاه را به عمل تبدیل می‌کنند

Razban
ATLAS FANAVARAN

چرخه عملکرد امنیتی

Identify (شناسایی)

- مدیریت هویت و دسترسی (Identity & Access Management – IAM): پیاده‌سازی احراز هویت چندعاملی (MFA)، ورود یکپارچه (SSO)، مدیریت چرخه عمر حساب‌ها و اعمال سیاست حداقل دسترسی (Least Privilege).
- انطباق و حاکمیت (Governance & Compliance): هم‌راستاسازی با استانداردهای ISO/IEC 27001، NIST CSF و الزامات افتا؛ طراحی نقشه راه ارتقای بلوغ امنیتی.
- مدیریت ریسک و دارایی‌ها: شناسایی دارایی‌های حیاتی، ممیزی‌های دوره‌ای و تحلیل ریسک برای اولویت‌بندی اقدامات امنیتی.

Protect (محافظت)

- امنیت زیرساخت و شبکه
  سخت‌سازی سیستم‌ها و Active Directory، مدیریت دسترسی ممتاز (PAM)، استقرار EDR/XDR، استانداردسازی لاگ‌ها و استفاده از معماری‌های Secure-by-Design و Zero Trust. استقرار فایروال‌های نسل جدید، IDS/IPS، کنترل NAC و رمزنگاری ترافیک حیاتی.
- امنیت کاربران و محیط کار
  استفاده از دسکتاپ مجازی (VDI) برای جلوگیری از نشت داده، وصله‌گذاری یکپارچه و سیاست‌های کاهش ریسک در دستگاه‌ها و کاربران.
- امنیت ایمیل، برنامه و داده
  محافظت از ایمیل و دامنه با SPF/DKIM/DMARC و تحلیل لینک‌ها و پیوست‌ها. امنیت وب‌اپ و API با WAF، تست نفوذ و مدیریت آسیب‌پذیری. طبقه‌بندی و رمزگذاری داده‌ها با KMS/HSM.
- امنیت ابر و توسعه نرم‌افزار
  پایش و ایمن‌سازی سرویس‌های ابری (CSPM/CWPP)، امنیت کانتینر و Kubernetes. ادغام امنیت در چرخه توسعه (DevSecOps) با اسکن کد و پایش زنجیره تأمین نرم‌افزار.
- فرهنگ‌سازی و آموزش
  برگزاری آموزش‌های نقش‌محور، شبیه‌سازی حملات فیشینگ و سنجش بلوغ امنیتی برای نهادینه سازی فرهنگ امنیت.

Detect (تشخیص)

- مرکز عملیات امنیت (Security Operations Center – SOC): جمع‌آوری و همبستگی رویدادها از شبکه، سرورها، ایمیل و کاربران؛ ایجاد دید 360 درجه بر تهدیدات.
- هوش مصنوعی و تحلیل رفتاری: بهره‌گیری از AI برای شناسایی تهدیدات ناشناخته و کشف الگوهای غیرعادی.
- شکار تهدیدات (Threat Hunting): تحلیل پیشگیرانه و جستجوی فعال برای کشف حملات پیچیده قبل از وقوع.

Respond (پاسخ‌گویی)

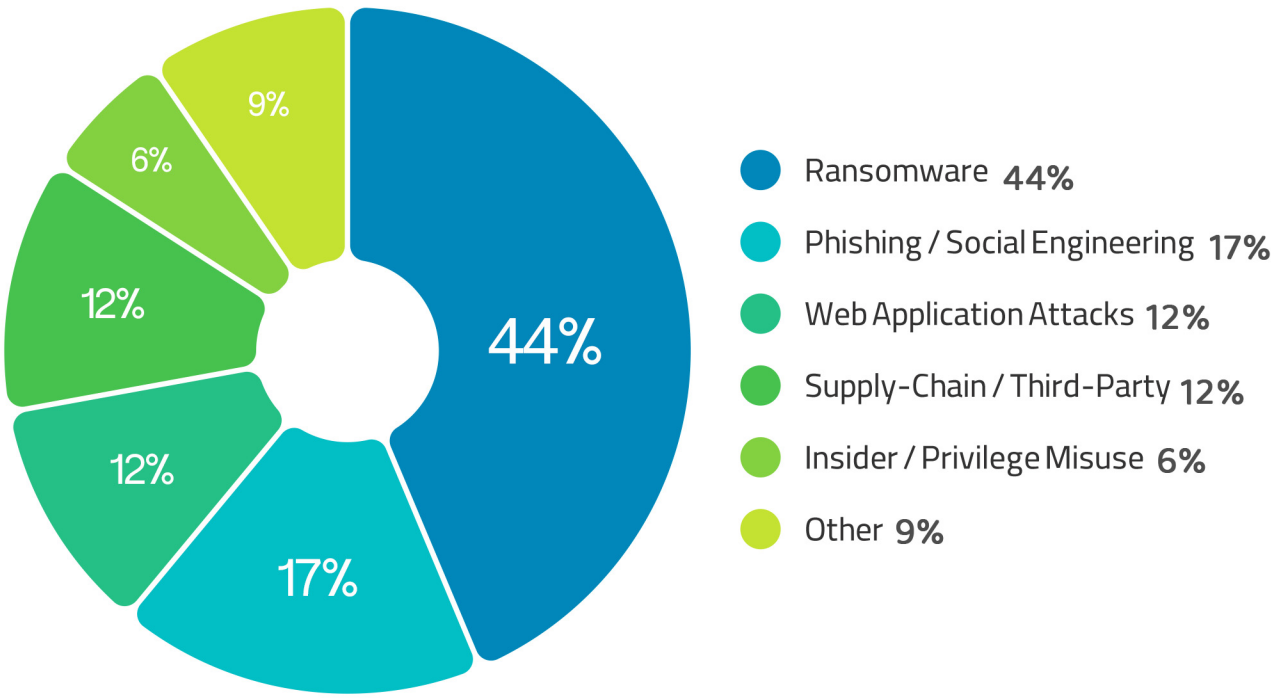
- پلی‌بوک‌های واکنش سریع: سناریوهای اختصاصی رازبان برای پاسخ خودکار و کاهش چرخه کشف تا پاسخ.
- مدیریت رخداد (Incident Response): رویه‌های مستند برای کنترل، مهار و اطلاع‌رسانی رخدادها.
- ارتباطات بحران: برنامه ارتباطی داخلی و خارجی در زمان حادثه برای کاهش آسیب های اعتباری و تجاری.

Recover (بازیابی)

- برنامه تداوم کسب‌وکار (Business Continuity Plan – BCP): طراحی معماری پایدار و مسیرهای افزونه (Redundant) برای استمرار خدمات حیاتی.
- برنامه بازیابی از فاجعه (Disaster Recovery Plan – DRP): پشتیبان‌گیری و تست دوره‌ای سناریوهای بازیابی عملیاتی.
- بازبینی پس از رخداد (Post-Incident Review): تحلیل درس‌آموخته‌ها و به‌روزرسانی رویه‌ها برای پیشگیری از رخدادهای مشابه.

در سال 2024، حملات باج افزاری در هر دقیقه حدود 80 هزار دلار خسارت وارد کرده و مجموع زیان جهانی کسب وکارها را به بیش از 42 میلیارد دلار رسانده است

نمودار پراکندگی و
سهم حملات سایبری در سال 2024



پنج نوع حمله اول
از منظر حجم و آسیب در ایران

1. Ransomware / باج‌افزار

حملات گسترده به بانک‌ها (IRLeaks) و بخش مالی.

ویژگی: رمزگذاری داده + درخواست باج.

2. Phishing / Spear-Phishing (فیشینگ و مهندسی اجتماعی)

عمدتاً توسط APTها برای دسترسی اولیه و سرقت اعتبار.

ویژگی: ایمیل/لینک‌های جعلی برای فریب کاربران و گرفتن لاگین.

3. DDoS (Distributed Denial of Service)

مخصوصاً توسط گروه‌های هکتیویستی برای از کار انداختن سامانه‌ها و سرویس‌های آنلاین.

ویژگی: ایجاد اختلال در دسترسی به سرویس‌ها.

4. Web Application Exploits (حملات به وب‌اپلیکیشن‌ها)

سوءاستفاده از ضعف‌های اپلیکیشن‌های بانکی، دولتی و دانشگاهی.

ویژگی: تزریق کد (SQLi، XSS)، نفوذ به وب‌سایت‌ها، Defacement.

5. Supply-Chain / Infrastructure Attacks (زنجیره تأمین و زیرساخت)

شامل نفوذ به سامانه سوخت، PLCها و بخش‌های صنعتی/حیاتی (Predatory Sparrow).

ویژگی: اثرگذاری فراتر از یک سازمان منفرد و ایجاد اختلال در زیرساخت ملی.

ماهیت جدید امنیت
در ایران و منطقه

واقعیت این است که **حملات سایبری بدون توجه به اندازه و نوع کسب‌وکار، همـــه را هدف می‌گیرند**؛ از کارخانه‌ای با چند خط تولید گرفته تا شـــرکت‌های بازرگانی و اســـتارتاپ‌های در حال رشـــد. برای صنایع متوسط ، یک باج‌افزار می توانـــد **خط تولید را متوقف کند** , **اطلاعات مالی حســـابداری را ناپدید کند** و زیان مالی ســـنگین به بار آورد. **برای شرکت‌های بازرگانی، فیشینگ و سرقت ایمیل کافی اســـت تا قراردادهای حیاتی یا تراکنش‌های مالی از دست برود**. حتی سازمان‌های کوچک نیز در امان نیستند؛ **نشت ساده اطلاعات مشتریان می‌تواند به ســـرعت اعتبارشـــان را نابود کند** و در بازار رقابتی به معنای مرگ زودرس باشد.

تهدیدات ســـایبری در ایران ابعاد اقتصادی، عملیاتی و اعتباری دارند. **خسارت مستقیم هر حمله معمولاً چندین برابر هزینه پیشگیرانه است**؛ توقف کسب وکار می‌تواند هفته‌ها طول بکشد، و بازسازی اعتماد مشتری **گاهی غیرممکن است**. مهاجمان از تکنیک‌های جدید مثل جعل هویت هوشمند با کمک هوش مصنوعی، باج‌افزارهای دو مرحله‌ای و نفوذ از طریق پیمانکاران کوچک استفاده می‌کنند. به همین دلیل است که دیگر نمی‌توان امنیت را به آینده موکول کرد. ســـرمایه‌گذاری در امنیت یعنـــی خریدن آرامش و تداوم. برای یک ســـازمان صنعتی، امنیت برابر با جلوگیری از توقف تولید است. برای یک شرکت بازرگانی، یعنی حفظ اعتبـــار و قراردادها. برای یک مجموعه کوچک، یعنی زنده ماندن در بازار رقابتی. **امنیت سایبری دیگر هزینه جانبی نیست؛ ستون فقرات بقای هر کسب‌وکار در ایران امروز است**.

همکاری‌های متنوع رازبان با سازمان‌ها و صنایع مختلف

بانک‌ها و مؤسسات مالی

پایش متمرکز و واکنش سریع در برابر تهدیدات پیچیده، همراه با توسعه زیرساخت‌های ارتباطی و بهبود سامانه‌های بکاپ و تداوم خدمات

صنایع تولیدی و کارخانه‌ها

حفاظت از خطوط تولید و دستگاه‌های کنترل صنعتی، بازطراحی شبکه و زیرساخت فیزیکی، و ایجاد لایه‌های پایدار برای مدیریت دسترسی و مانیتورینگ

بازرگانی‌ها و خرده‌فروشی‌های آنلاین

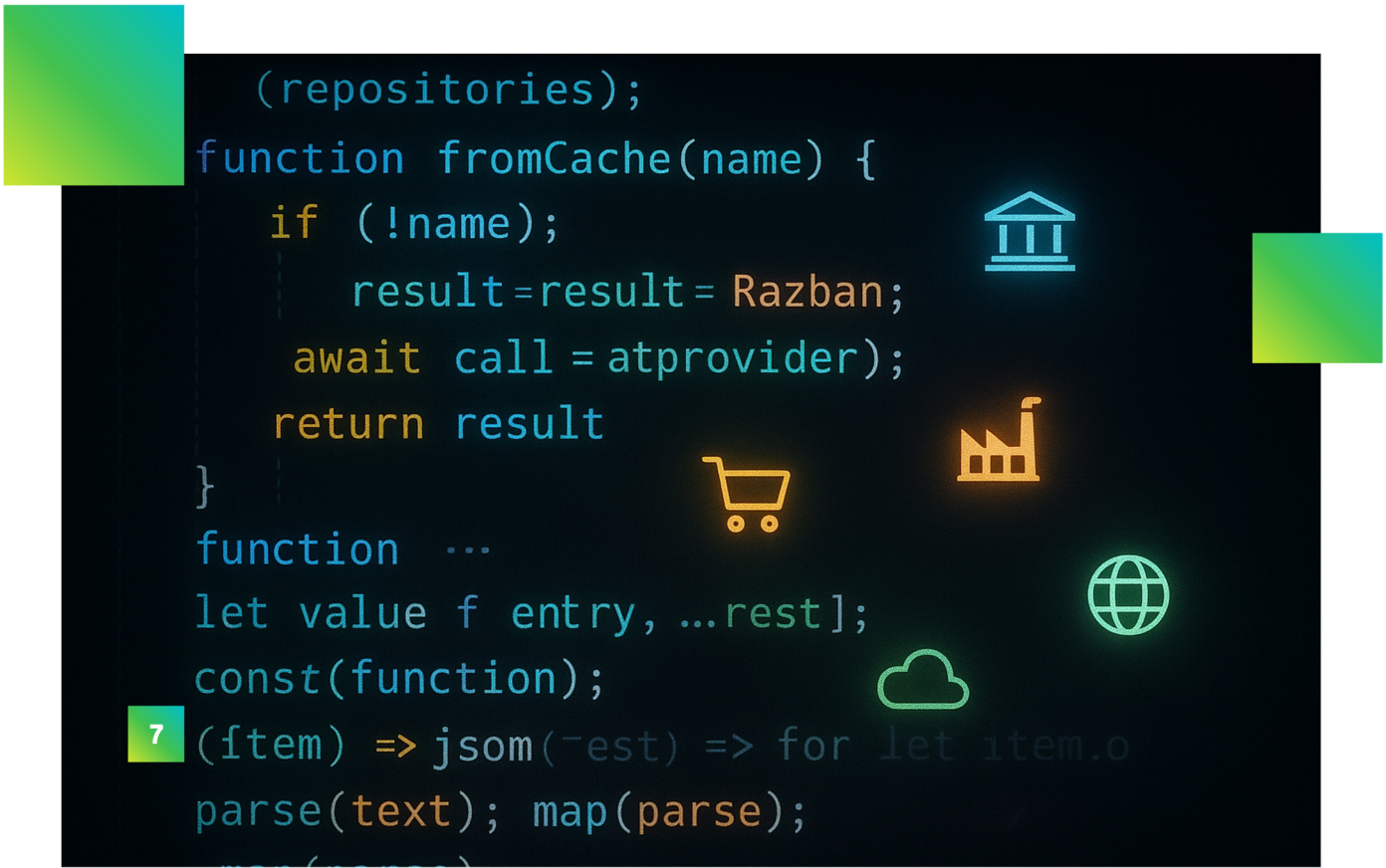
طراحی و پیاده‌سازی نرم‌افزارهای اختصاصی برای مدیریت فرآیندهای فروش و زنجیره تأمین، در کنار ایمن‌سازی زیرساخت فروش آنلاین بهبود تجربه مشتری

سرویس‌دهندگان داده و اینترنت

ارزیابی امنیتی شبکه، اصلاح پیکربندی‌های پرریسک و ایجاد بستر امن برای ارائه خدمات ، همراه با توسعه زیرساخت مانیتورینگ چندلایه

راهکارهای مشترک

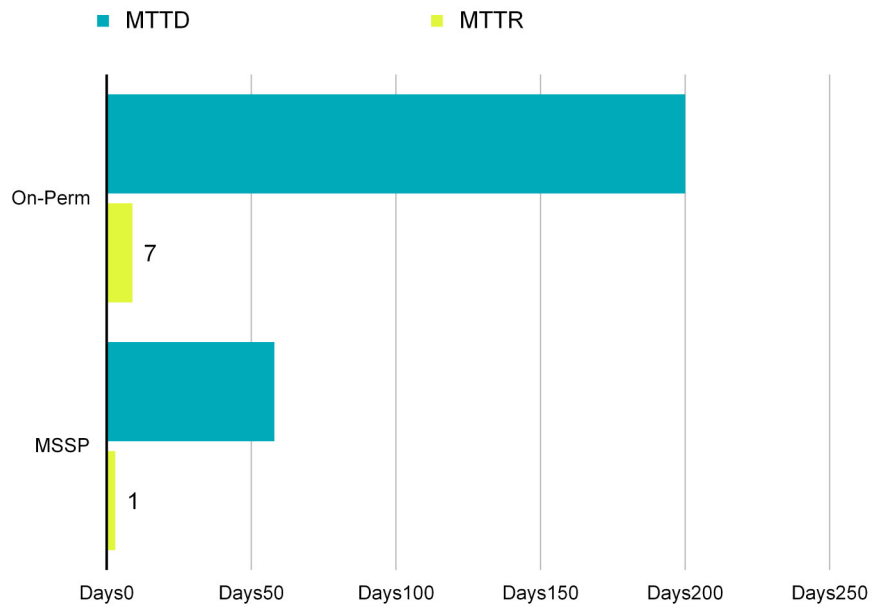
یکپارچه‌سازی و امن‌سازی ارتباط بین شعب، توسعه سایت‌های بحران و بکاپ، ارتقای دسترسی از راه دور، و همچنین طراحی و استقرار نرم افزارهای پشتیبان عملیات



ابزار های مورد استفاده

در رازبان ما از ترکیبی از ابزارهای نرم‌افزاری و سخت‌افزاری پیشرفته استفاده می‌کنیم که شامل سامانه‌های پایش تهدید (SIEM/SOAR)، پلتفرم‌های EDR/XDR برای حفاظت نقطه پایانی، فایروال‌های نسل جدید (NGFW)، تجهیزات تحلیل ترافیک شبکه، سامانه‌های مدیریت هویت (IAM/PAM) و زیرساخت‌های امن‌سازی ابری و کانتینر است. این ابزارها به ما امکان می‌دهند نه‌تنها تهدیدات شناخته‌شده را مسدود کنیم، بلکه حملات پیچیده و ناشناخته را هم در مراحل اولیه شناسایی کنیم.

یکی از سرویس‌های متمایز رازبان، MMSP (Managed Modern Security Platform) است؛ پلتفرمی مدیریت‌شده که ابزارهای پیشرفته امنیتی را در اختیار کسب‌وکارهای کوچک و متوسط قرار می‌دهد، بدون نیاز به سرمایه‌گذاری سنگین در سخت‌افزار یا تیم‌های بزرگ امنیتی. در این مدل، پایش، تحلیل و حتی واکنش خودکار توسط تیم تخصصی رازبان انجام می‌شود. نتیجه، دسترسی به سطح امنیتی هم‌تراز سازمان‌های بزرگ با هزینه کمتر و سرعت شناسایی و پاسخ چندبرابر سریع‌تر از راهکارهای سنتی است.



رازبان با خدمات مدیریت شده (MSSP) توانسته چرخه شناسایی و پاسخ را بطور چشم گیری کوتاه کند و تهدید هایی که ماه ها پنهان می ماندند در عرض چند ساعت شناسایی کرده و پاسخ دهد .

این مهم به کمک پایگاه داده‌ی به روز بدافزارها و الگوهای حمله , بهره گیری از کارشناسان با تجربه و همچنین ابزار های پیشرفته محقق شده است

نمونه ای از تجربه ها و خدمات جاری ما

- **زیرساخت و شبکه**

طراحی و پیاده‌سازی زیرساخت‌های سروری و مراکز داده (اکتیو و پسیو)، توسعه بسترهای مجازی‌سازی، ارتباط امن بین شعب و بهینه‌سازی تجهیزات شبکه

- **نرم‌افزار و سامانه‌ها**

داشبورد ،CRM ،ERP ،اتوماسیون) توسعه نرم‌افزارهای اختصاصی VDI و راه‌اندازی سرویس‌های سازمانی مانند ایمیل، دامین و (مدیریتی برای دورکاری امن

- **پایش و تداوم خدمات**

ایجاد سامانه‌های مانیتورینگ، طراحی راهکارهای بکاپ‌گیری و و استقرار سایت‌های جایگزین برای تداوم عملیات Disaster Recovery حیاتی

- **امنیت و ریسک**

سخت‌سازی زیرساخت، تست نفوذ دوره‌ای، مدیریت دسترسی کاربران، شبیه‌سازی حملات و تدوین سیاست‌های مدیریت داده

- **خدمات ابری و تجارت آنلاین**

طراحی بسترهای ابری و هاستینگ امن و مقیاس‌پذیر، همراه با توسعه و ایمن‌سازی وب‌سایت‌ها و فروشگاه‌های اینترنتی

هوش مصنوعی در امنیت

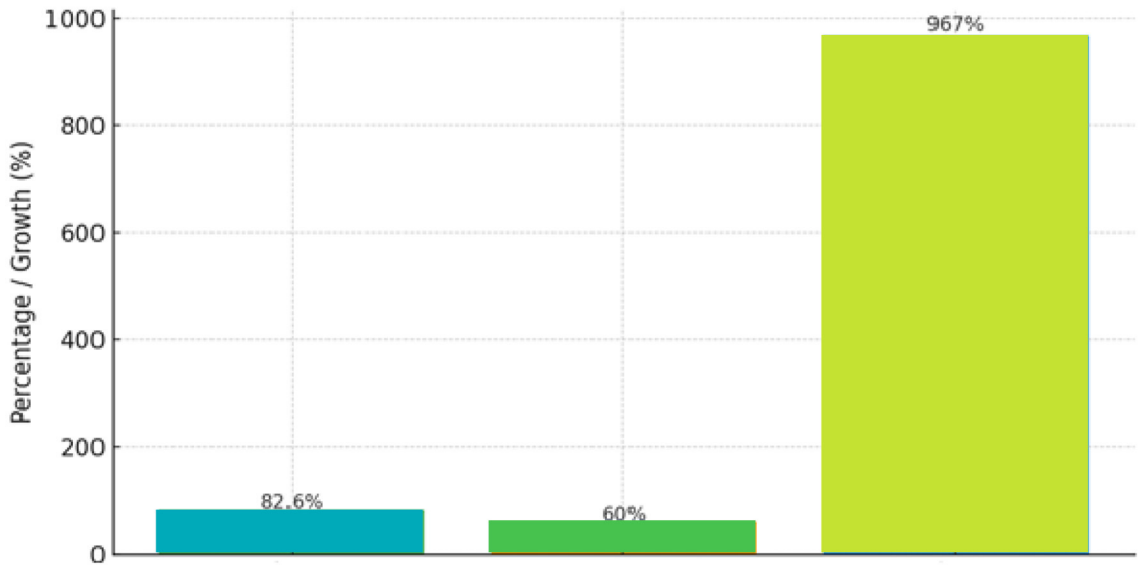
امروز هوش مصنوعی به یکی از اصلی‌ترین ابزارهای مهاجمان ســـایبری تبدیل شده است. آن‌ها با کمک AI می توانند ایمیل‌های فیشـــینگ طبیعی و شخصی‌سازی‌شده تولید کنند، بدافزارهایی بسازند که رفتارشان را تغییر می‌دهند و از شناسایی فرار می‌کنند، یا حتی با دیپ‌فیک هویت‌های جعلی خلق کنند. این یعنی حملاتی که روزی به‌سادگی قابل تشخیص بودند، حالا می‌توانند بسیار هوشمندانه، دقیق و گمراه‌کننده باشند.

در نقطه مقابل، همین فناوری به ابزاری قدرتمند در دســـت مدافعان تبدیل شـــده است. سامانه‌های امنیتی مبتنی بر AI می‌توانند رفتار کاربران و ترافیک شبکه را تحلیل کرده و الگوهای ناشناخته را سریع‌تر شناسایی کنند، تهدیدات پیچیده را در لحظه تشـــخیص دهند و حتی واکنش خودکار داشته باشـــند. این پیشرفت باعث شده سرعت و دقت دفاع سایبری به سطحی برسد که با روش‌های سنتی غیرممکن بود.

رازبان نیز بـــا درک این واقعیت، هوش مصنوعـــی را در فرآیندهای خود به‌کار گرفته اســـت؛ از تحلیل داده‌ها و همبســـتگی رویدادها در SOC، تا طراحی پلی‌بوک‌های هوشمند و واکنش ســـریع به رخدادها. به همین دلیل سرویس‌های ما نه‌تنها در برابر تهدیدات امروز مقاوم‌اند، بلکه آماده مقابله با حملات فردا نیز هستند.

نکته کلیدی این است که نباید از این تحولات غافل شد یا عقب ماند. هرچه مهاجمان سریع‌تر از هوش مصنوعی بهره بگیرند، فاصله‌ی آن‌ها با سازمان‌هایی که هنوز بر روش‌های سنتی تکیه کرده‌اند بیشتر می‌شود. به‌کارگیری AI در امنیت سایبری امروز دیگر یک انتخاب نیست؛ بلکه ضرورتی برای بقا و حفظ رقابت در بازار است.

میزان استفاده از هوش مصنوعی در حملات فیشینگ



- ایمیل های ساخته شده توسط هوش مصنوعی
- کاربرانی که روی لینک‌های فیشینگ هوش مصنوعی کلیک کرده‌اند
- رشد در فیشینگ اطلاعات هویتی

خدمات اطلس فناوران رازبان

- طراحی و اجرای زیرساخت و شبکه امن
- توسعه نرم‌افزارها و سامانه‌های سازمانی
- خدمات جامع امنیت سایبری و مشاوره
- راهکارهای پشتیبان‌گیری مدیریت بحران و تداوم کسب‌وکار

امنیت یعنی ادامه مسیر. رازبان در یک مشاوره رایگان جایگاه امروز و مسیر فردای امن تر را به شما نشان می‌دهد

RazbanSec.com/per/contact

+98-21-91304514

Contact@RazbanSec.com

رازبان
اطلس فناوران

اصفهان، بلوار آتشگاه،
جنب خیابان وحدت، مجتمع هفت آسمان،
طبقه 4، واحد 411

021-91304514
www.razbansec.com
contact@razbansec.com