یوزیت

چشم پنهان امنیت سازمان ها

YUZIT.IR

امنیت هوشمند زیرساخت‌های سازمانی

پلتفرم امنیتی یوزیت با استفاده از الگوریتم های پیشرفته هوش مصنوعی امکان تشخیص، کنترل و شناسایی تهدیدات امنیت سایبری، درون و برون سیستمی را با سرعت بالا ممکن می‌سازد.

https://yuzit.ir

برخی از چالش‌های مدیریت امنیت در سازمان‌ها

با گسترش زیر ساخت های دیجیتال سازمانها، حجم داده های امنیتی نیز به سرعت افزایش یافته و تحلیل آنها بدون ابزارهای دقیق و هوشمند به یک فرآیند پیچیده و زمان بر تبدیل شده است.

از لاگ های سرور و رویدادهای شبکه گرفته تا فعالیت کاربران. تحلیل این داده‌ها بدون ابزارهای پیشرفته بسیار دشوار و همین موضوع باعث تهدیدات امنیتی جدی می‌شود.

تشخیص فعالیت‌های غیر معمول

بسیاری از رفتارهای مخرب در لایه‌های عمیق رخ می‌دهند اما در ظاهر عادی به‌نظر می‌رسند. آنها بدون تحلیل هوشمند قابل شناسایی نیستند.

کنترل دسترسی‌های غیر مجاز

سوءاستفاده از دسترسی‌های داخلی یکی از رایج‌ترین تهدیدات است. موضوعی که بدون پایش رفتاری و نظارت لحظه‌ای قابل تشخیص نیست.

حجم بالای لاگ‌های امنیتی

زیرساخت‌های سازمانی روزانه هزاران رویداد امنیتی تولید می‌کنند. تحلیل دستی داده‌ها شناسایی تهدیدات را غیرممکن و پرخطا می‌سازد.

مدیریت دسترسی‌های پراکنده

پراکنده بودن اطلاعات امنیتی در سیستم‌های مختلف مانع ایجاد یک نقطه دید واحد، تشخیص تهدیدات را دشوار و زمان‌بر می‌نماید.

پلتفرم امنیتی یوزیت مبتنی بر شبکه عصبی هوش مصنوعی با معماری متمرکز باعث شده تمامی تهدیدات به سرعت کشف و خنثی گردد.

راهکار ما

مانیتورینگ هوشمند داده های امنیتی مبتنی بر هوش مصنوعی

- راهکار یوزیت بر پایه رویکرد مدرن Security Data Analysis طراحی شده است؛ رویکردی که با تحلیل الگوهای رفتاری، بررسی رویدادهای امنیتی و پایش هوشمند زیرساخت، تهدیدات پنهان و فعالیت‌های مشکوک را پیش از ایجاد خسارت شناسایی می‌کند.

- این پلتفرم با ترکیب AI و یادگیری الگوهای رفتاری کاربران، به‌همراه پایش یکپارچه زیرساخت، امکان تشخیص تهدیدات پیچیده، حملات تدریجی و رفتارهای غیرعادی را فراهم می‌سازد.

- یکی از ویژگی‌های مهم این راهکار امکان استقرار در زیرساخت داخلی سازمان است (On premise deployment) موضوعی که از خروج داده‌های حساس جلوگیری کرده و امنیت سازمان را به‌طور چشمگیری افزایش می‌دهد.

برای مشاهده دمو با ما در ارتباط باشید

خدمات یوزیت

ارائه راهکارهای پیشرفته و نوین امنیت زیرساخت های سازمانی

تحلیل کاربران

تحلیل رفتار کاربران یا (User behavior analytics – UBA)

در بسیاری از حملات سایبری، مهاجم از طریق دسترسی یک کاربر قانونی وارد سیستم می‌شود. به همین دلیل بررسی رفتار کاربران یکی از مهم‌ترین روش‌های شناسایی تهدیدات امنیتی است.
این موضوع به طیف وسیعی از دسترسی های درون سازمانی و برون سازمانی و هر امکانی که ورود به سیستم را ایجاد می نماید مرتبط می گردد.
این سیستم توسط الگوریتم های پیچیده هوش مصنوعی رفتار کاربران را بررسی و در صورت مشاهده فعالیت های غیر معمول طبق پروتکل ها، دستورالعمل های لازم را انجام می دهد.

- ورود کاربران در زمان یا مکان غیرعادی (Abnormal login pattern)
- دسترسی غیرمعمول به اطلاعات یا فایل‌های حساس (Data access anomaly)
- انتقال حجم غیرعادی از داده‌ها (Data exfiltration detection)
- تغییر الگوی فعالیت کاربر در سیستم (Behavior deviation)

تحلیل سیستم ها

تحلیل رفتار سیستم‌ها (System Behavior Analytics – SBA)

سرویس‌ها، پردازش‌ها و سرورها دارای الگوهای رفتاری مشخصی هستند. انحراف از این الگوها می‌تواند نشانه نفوذ یا اختلال عملکرد باشد.
این قابلیت رفتار واقعی سرویس‌ها و پردازش‌ها را با الگوی طبیعی آن‌ها مقایسه کرده و موارد غیرمعمول را شناسایی می‌کند.

- رفتار غیرعادی پردازش‌ها یا سرویس‌ها (Process/Service Anomaly)
- فعالیت‌های غیرمعمول در سطح سرور (Server Activity Outlier)
- افزایش غیرعادی مصرف منابع سیستم (Suspicious Resource Utilization)
- تغییرات ناگهانی در الگوهای ترافیک داخلی (Internal Traffic Deviation)

تحلیل رویدادهای امنیتی

تحلیل رویدادهای امنیتی (Security Event Analysis)

سیستم‌ها روزانه هزاران رویداد امنیتی تولید می‌کنند که تحلیل آن‌ها برای شناسایی تهدیدات ضروری است.
این قابلیت با اولویت‌بندی رویدادهای مهم، تهدیدات واقعی را از هشدارهای کم‌اهمیت جدا می‌کند.

- شناسایی الگوهای حمله در رویدادها (Attack Pattern Recognition)
- تحلیل رفتار سرویس‌ها و پردازش‌ها (Service Behavior Analysis)
- اولویت‌بندی رویدادهای حیاتی امنیتی (Event Risk Scoring)
- تشخیص رفتار غیرعادی در سرویس‌ها (Service Anomaly)

شناسایی ناهنجاری‌ها

شناسایی ناهنجاری‌ها (Anomaly Detection)

مدل‌های یادگیری ماشین با شناسایی انحرافات رفتاری، فعالیت‌های مشکوک را حتی بدون تعریف قبلی الگوهای حمله کشف می‌کنند.
این قابلیت در همه لایه‌ها از کاربران تا سیستم و شبکه مورد استفاده قرار می‌گیرد.

- تشخیص ناهنجاری در ترافیک شبکه (Network Traffic Anomaly)
- شناسایی فعالیت‌های غیرعادی در سرورها (Server Anomaly Detection)
- کشف الگوهای رفتاری غیرمتعارف (Behavioral Anomaly)
- یافتن روندهای غیرطبیعی در داده‌های امنیتی (Trend Outliers)

وضعیت امنیت و اعلان‌ها

وضعیت امنیت و اعلان‌ها (Security Status & Alerting)

این بخش وضعیت لحظه‌ای امنیت سازمان را نمایش داده و اعلان‌ها را بر اساس اولویت و سطح ریسک ارائه می‌کند.
با این قابلیت تیم امنیتی همیشه یک دید جامع و دقیق از وضعیت تهدیدات فعال خواهد داشت.

- نمایش وضعیت لحظه‌ای امنیت (Real-Time Security Overview)
- اعلان‌های هوشمند و اولویت‌بندی‌شده (Intelligent Alerts)
- نمایش تهدیدات فعال در سیستم (Active Threat Visibility)
- تحلیل روندها و وضعیت امنیت (Security Trends)

یکپارچه‌سازی داده‌های امنیتی

یکپارچه‌سازی داده‌های امنیتی (Security Data Aggregation)

داده‌های امنیتی در منابع مختلف ذخیره می‌شوند. این قابلیت همه داده‌ها را جمع‌آوری و استانداردسازی می‌کند.
نتیجه این فرآیند ایجاد یک دید واحد برای تحلیل امنیت و تشخیص تهدیدات پنهان است.

- تجمیع لاگ‌ها از منابع گوناگون (Log Consolidation)
- استانداردسازی داده‌های امنیتی (Data Normalization)
- ایجاد دید واحد برای تیم امنیت (Unified Security View)
- کشف تهدیدات با همبستگی داده‌ها (Correlated Insights)

مزایا

الگوریتم‌های هوش مصنوعی سفارشی

دقت بالا در تشخیص و کاهش ریسک نشت اطلاعات

تشخیص سریع در واکنش به تهدیدات امنیتی

تسلط کامل تیم فناوری اطلاعات به فعالیت ها

هزینه مناسب نسبت به راهکارهای خارجی

پشتیبانی مستقیم و سریع از تیم فنی ما

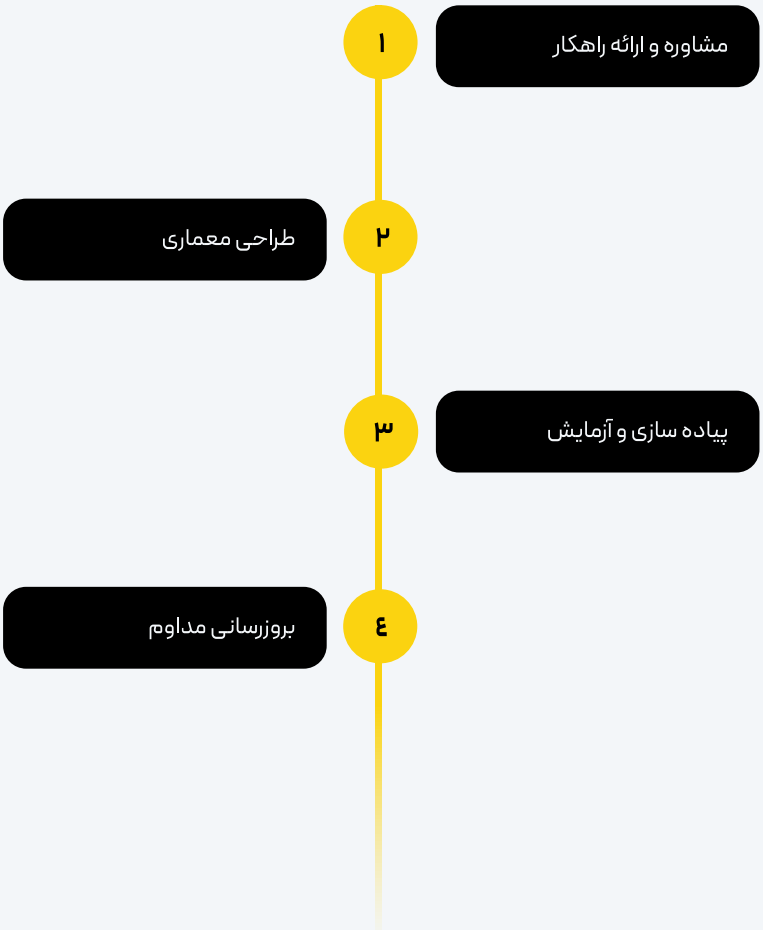
چرا ما؟

پلتفرم یوزیت راهکاری بومی و هوشمند برای افزایش امنیت اطلاعات سازمان‌ها و شرکت‌ها. ما به‌عنوان یک شرکت فناورانه با سابقه در زمینه هوش مصنوعی، راهکارهایی سفارشی و کاملاً انحصاری ارائه می‌دهیم که نه تنها با سیستم‌های داخلی هر سازمان سازگار هستند، بلکه به‌خوبی با نیازهای خاص آن بهینه‌سازی می شوند.

در طول سال‌های گذشته، ما به‌عنوان یکی از پیشگامان فناوری‌های پیشرفته در کشور، در زمینه‌های مختلفی از جمله هوش مصنوعی پزشکی و فناوری اطلاعات، فعالیت‌های گسترده‌ای در سطح داخلی و بین‌المللی انجام داده‌ایم. تجربه ما در توسعه سیستم‌های هوشمند و موفقیت‌های علمی در حوزه‌های حساس، ما را به یک گزینه قابل اعتماد و معتبر در این عرصه تبدیل کرده است.

تطبیق‌پذیری بالا، امنیت بیشتر و هزینه مناسب نسبت به راهکارهای خارجی را می توان برخی از مزیت های ما دانست. این سیستم نه تنها با ساختارهای داخلی سازمان‌ها سازگار هستند، بلکه با پشتیبانی سریع و مداوم، اطمینان حاصل می‌شود که هرگونه نیاز فنی به‌خوبی پوشش داده می‌شود.

فرآیند همکاری



الگوریتم های امنیتی پیشرفته بومی هوش مصنوعی یوزیت
ضامن افزایش امنیت و سرعت در جلوگیری از بروز تهدیدات امنیتی

ارتباط با ما

تهران

۰۲۱۸۱۶۴۰۲۶۵

۰۹۱۲۶۷۰۲۸۵۷

https://yuzit.ir