گزارش توصیه‌های امنیتی

(Security Recommendations Report)

۱. نقش مدل در امنیت شبکه (Model Role in Network Security)

مدل طراحی‌شده در این پروژه به عنوان یک **سامانه پشتیبان تصمیم (Decision-Support System)** برای تیم امنیت شبکه عمل می‌کند.
این مدل با استفاده از داده‌های ترافیک شبکه، نوع رفتار را به یکی از چهار کلاس اصلی تقسیم می‌کند: **drop**, **deny**, **allow**, و **reset-both**.

هدف اصلی، شناسایی **فعالیت‌های غیرعادی یا تهدیدات بالقوه** است که معمولاً در میان داده‌های حجیم و عادی شبکه پنهان می‌مانند.

با دقت کلی **۹۹٫۸٪** و نرخ **تشخیص تهدید ۸۴٪**، این مدل می‌تواند به عنوان یک **لایه تشخیص اولیه (Early Threat Detection Layer)** در سیستم‌های امنیتی سازمان مورد استفاده قرار گیرد.

۲. اهمیت معیارهای امنیتی (Security Metrics Significance)

- **دقت کلی (Accuracy)** بالا نشان می‌دهد که مدل توانایی کلی خوبی در طبقه‌بندی ترافیک دارد.
- اما از دید امنیت شبکه، **Recall کلاس‌های deny و drop** مهم‌تر است؛ زیرا این معیار مشخص می‌کند چند تهدید واقعی واقعاً شناسایی شده‌اند.
- هر کاهش در Recall برای کلاس‌های امنیتی می‌تواند منجر به **False Negative** شود، یعنی تهدید واقعی‌ای که نادیده گرفته می‌شود — این خطرناک‌ترین حالت در سامانه‌های دفاعی است.

بنابراین مدل باید طوری تنظیم شود که حتی با کمی کاهش در **Recall**، Precision **امنیتی بالا باقی بماند** تا هیچ تهدیدی از دید سیستم پنهان نماند.

۳. تحلیل عملکرد مدل از دید امنیتی (Model Security Impact)

- مدل فعلی با Recall کلی **۰٫۸۴** برای کلاس‌های امنیتی عملکرد بسیار خوبی دارد.
- این مقدار نسبت به قبل از بالانس‌سازی حدود **۳۵٪ بهبود** یافته است.
- مدل توانسته تهدیدات کم‌نمونه (rare attacks) را با دقت قابل قبول شناسایی کند.
- کلاس **reset-both** که پیش‌تر تقریباً نادیده گرفته می‌شد، اکنون در مدل لحاظ شده و رفتار آن توسط SMOTE بازتولید شده است.

با این حال، هرچند مدل Recall بالایی دارد، **وابستگی زیاد به الگوهای گذشته** ممکن است در برابر تهدیدات جدید (zero-day attacks) محدودیت ایجاد کند.

۴. توصیه‌های کلیدی امنیتی (Core Recommendations)

الف. برای تیم امنیت شبکه

1. مدل را به عنوان **سیستم هشدار اولیه (Early Warning System)** در کنار IDS/SIEM به کار ببرید، نه جایگزین کامل آن.

2. هشدارهای مدل با **سیاست‌های فایروال و لاگ‌های سیستم** تلفیق شود تا صحت تشخیص‌ها افزایش یابد.
3. برای جلوگیری از کاهش Recall در طول زمان، داده‌های آموزشی باید **هر سه ماه به‌روزرسانی شوند**.
4. توجه ویژه به **False Negatives (ویژگی‌های خطرناک)** داشته باشید؛ زیرا ممکن است برخی بسته‌های مخرب به‌عنوان allow طبقه‌بندی شوند.

ب. برای تیم توسعه داده

1. گسترش دیتاست با حملات واقعی و داده‌های شبیه‌سازی‌شده (adversarial) جهت افزایش مقاومت مدل.
2. آموزش مجدد با داده‌های شبکه‌ی زنده در محیط کنترل‌شده.
3. افزودن ویژگی‌های رفتاری جدید (behavioral features) مثل نرخ ارتباط، زمان پاسخ، یا توالی پکت‌ها.
4. استفاده از الگوریتم‌های ترکیبی (Ensemble) برای افزایش پایداری عملکرد امنیتی.

۵. جمع‌بندی امنیتی (Security Summary)

مدل کنونی توانسته با دقت کلی **۹۹٫۸٪** و Recall امنیتی **۰٫۸۴**، تعادل قابل‌توجهی بین **عملکرد کلی و دقت امنیتی** برقرار کند.
اما مهم‌تر از اعداد، این است که سیستم به تیم امنیتی کمک می‌کند **تهدیدات نادر و کم‌نمونه را سریع‌تر شناسایی کند** — تهدیداتی که معمولاً از دید روش‌های سنتی پنهان می‌مانند.

در نتیجه:

این مدل یک ابزار پشتیبان قوی برای تحلیل رفتار شبکه است، اما نیازمند **بازآموزی دوره‌ای و نظارت انسانی** برای حفظ دقت و کاهش خطاهای امنیتی است.