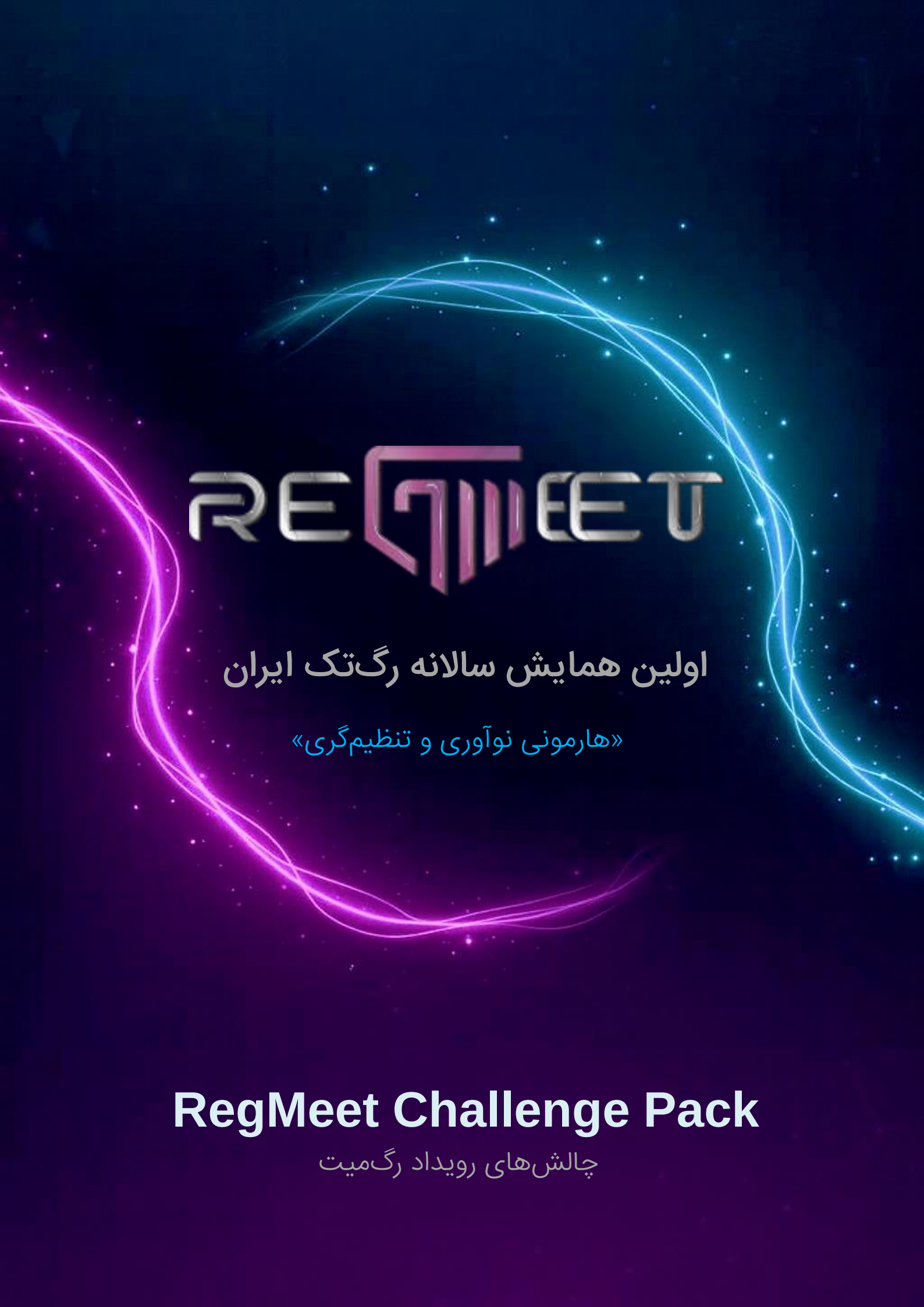

REGMEET
اولین همایش سالانه رگ‌تک ایران
«هارمونی نوآوری و تنظیم‌گری»
RegMeet Challenge Pack
چالش‌های رویداد رگ‌میت

RegMeet Challenge Pack

چالش‌های رویداد رگ‌میت

- Regulatory Change Management (RCM)
- Regulatory Reporting (RR)
- Anti Money Laundering (AML)
- Transaction Monitoring (TM)
- Identity and Access Management (IAM)

تعریف چالش

چالش تک‌اسپرینت
۱
مدیریت تغییرات مقررات

چالش شماره ۱

شما عضوی از شرکت فرضی در حوزه پرداخت الکترونیکی هستید. ناظر به تازگی مقررات جدیدی برای سامانه‌های پرداخت و خدمات مالی دیجیتال اعلام کرده است. شرکت شما باید سامانه‌ای طراحی کند که تغییرات مقرراتی را به سرعت تحلیل، ترجمه به قوانین داخلی سیستم و اعمال کند، بدون اینکه عملکرد سیستم دچار اختلال شود.

هدف چالش

فرآیند مدیریت تغییرات، به‌صورت خودکار یا نیمه‌خودکار، امن، و قابل رصد برای ناظر اجرا شود:

- دسته‌بندی به قوانین قابل اجرا در سیستم، و شناسایی بخش‌های فنی آسیب‌پذیر
- برای هر تغییر تصمیم بگیرد: اعمال در سیستم (Apply)، نیاز به بررسی دستی (Review)، مغایرت با سیاست فعلی یا ریسک بالا (Flag)
- ثبت لاگ و ارائه گزارش برای ممیزی ناظر

ویژگی‌های خروجی مورد انتظار

سطح ۱: طرح

- طراحی مدل مفهومی RCM
- نقشه جریان تصمیم: چگونه تغییر مقررات به سیستم‌های داخلی منتقل می‌شود
- مثال Policy یا Rule sample

سطح ۲: نمونه اولیه MVP

- ساخت یک سرویس ساده API یا Rule Engine که مقررات را دریافت کرده و تغییرات را اعلام می‌کند
- ثبت لاگ و گزارش خلاصه
- امکان تست با نمونه‌های واقعی

سطح ۳: محصول آماده عرضه

- Policy Engine پیکربندی‌پذیر با مدیریت نسخه قوانین
- اعلان خودکار در صورت مغایرت یا ریسک
- مستند فنی و دموی قابلیت تغییر قوانین در سیستم زنده

تعریف چالش

چالش تک‌اسپرینت
۲
گزارش‌دهی به رگولاتور

RR
Regulatory Reporting

چالش شماره ۲

در سال‌های اخیر، فین‌تک‌های جدیدی در کشور ظهور کرده‌اند که هنوز رگوله نشده‌اند و چارچوب مشخصی برای نظارت بر آن‌ها وجود ندارد. از سوی دیگر، نهاد ناظر به داده‌های این بخش‌ها نیاز دارد تا بتواند رفتار بازار را درک کند، بدون آنکه مانع رشد نوآوری شود. در چنین فضایی، برخی از فین‌تک‌ها مایلند که به‌صورت داوطلبانه و امن، داده‌های کلیدی خود را با ناظر به اشتراک بگذارند و اعتمادسازی کنند.
این چالش از شما می‌خواهد، راهکاری طراحی کنید که فین‌تک‌های غیررگوله بتوانند گزارش‌های داوطلبانه و استاندارد خود را ثبت کنند، ناظر بتواند آن‌ها را تحلیل کند و در مقابل، مشوق‌هایی برای شفافیت و رفتار مسئولانه به این فین‌تک‌ها اختصاص داده شود.

هدف چالش

هدف چالش طراحی یک مدل فناورانه اعتمادساز است که هم فین‌تک‌ها را به شفافیت ترغیب کند و هم ناظر را به داده‌های واقعی و قابل اعتماد مجهز سازد. تیم‌ها باید نشان دهند که راهکارشان چگونه می‌تواند:

- فرآیند جمع‌آوری، استانداردسازی و ارسال داده‌ها را برای فین‌تک‌ها ساده و کم‌هزینه کند،
- ابزارهای تحلیل و نمایش داده را برای ناظر فراهم آورد،
- مشوق‌های انگیزشی و مدل اعتمادسازی میان فین‌تک و نهاد ناظر را در طراحی خود بگنجاند.

ویژگی‌های خروجی مورد انتظار

سطح ۱: طرح

- مدل مفهومی پلتفرم گزارش‌دهی داوطلبانه
- مدل داده‌ها و تعیین شاخص‌های کلیدی گزارش‌دهی
- فرآیند جریان اطلاعات بین فین‌تک‌ها و ناظر
- طراحی نظام مشوق‌ها

سطح ۲: نمونه اولیه MVP

- توسعه یک نمونه داشبورد ارسال گزارش
- طراحی یک API ساده برای ارسال داده‌ها
- توسعه یک محیط نمایشی برای ناظر با قابلیت مشاهده، تحلیل و امتیازدهی به گزارش‌ها

سطح ۳: محصول آماده عرضه

نسخه عملیاتی یک پلتفرم کامل با قابلیت:

- احراز هویت
- رمزنگاری داده
- سطح‌بندی دسترسی
- تولید خودکار گزارش‌ها
- اتصال به سایر فین‌تک‌ها
- تحلیل داده‌های تراکنشی
- پنل مشترک ناظر–فین‌تک

تعریف چالش

چالش تک‌اسپرینت
۳
راهکار OSINT در حوزه مقابله با پولشویی

چالش شماره ۳

شما عضوی از مجموعه مانیتورینگ یک موسسه مالی هستید و مدیر مؤسسه متوجه شده است که برخی از گروه‌های متخلف، اخیرا در حال بازاریابی و شبکه‌سازی برای سوء استفاده از هویت دیگران، مجوزهای صوری و شرکت‌های کاغذی هستند. بدین نحو که به صورت خواسته یا ناخواسته به نام فرد دیگری نزد مؤسسه شما ثبت نام کرده و خدمات دریافت می‌کنند. شرکت در حال حاضر یک سامانه مانیتورینگ برای تحلیل تراکنش‌های مالی دارد ولی از شما خواسته شده که با تحلیل اطلاعات منابع آزاد (OSINT)، کمک کنید از مؤسسه شما سوء استفاده نشود.

۱- در صورت دریافت هشدار یا داده‌های برچسب‌دار از سامانه مانیتورینگ (مثلا افرادی که گردش یا حجم معاملات بالایی دارند) موتور OSINT می‌بایست به تکمیل پروفایل و تحلیل عملکرد اشخاص و روابط اقدام کند.
۲- بدون دریافت داده برچسب‌دار از سوی سامانه مانیتورینگ به شناسایی مصادیق جدید رفتارهای مشکوک صرفاً براساس منابع آزاد بپردازد.

هدف چالش

۱. شناسایی دقیق‌تر و سریع‌تر روابط پرریسک و نیز صحه‌گذاری بر روابط شناسایی شده
۲. غنی‌سازی، طبقه‌بندی و تهیه پروفایل اشخاص با استفاده از کلیه اطلاعات موجود
۳. تهیه سیستم بلادرنگ ارزیابی، تطبیق و گزارش ریسک افراد و شبکه‌های مشکوک
۴. کمک به تصمیم‌سازی و تهیه گزارش جهت شناسایی و مدیریت ریسک سوء استفاده از خدمات مؤسسه

ویژگی‌های خروجی مورد انتظار

سطح ۱: طرح

- معماری، مدل مفهومی و جریان تبادل اطلاعات بین سامانه‌ها و منابع مختلف
- کلیدواژه‌ها، الگوریتم‌ها و شاخص‌های ریسک و امتیازدهی
- ساختار پروفایل اشخاص و روابط بدون وابستگی به نوع منبع

سطح ۲: نمونه اولیه MVP

- طراحی جزئی، شامل تکنولوژی‌ها یا ابزارها
- ربات‌ها و خزنده‌ها با قابلیت شخصی‌سازی کامل (به عنوان مثال تعیین کلمه کلیدی برای ربات جهت جستجو در منابع و پلتفرم‌های مختلف) حداقل در ۲ منبع تخصصی

سطح ۳: محصول آماده عرضه

- موتور یکپارچه OSINT با قابلیت تعامل با سامانه مانیتورینگ، قابلیت تعریف منابع جدید (عام و تخصصی) و همچنین امکان مستندسازی و ارائه گزارشات قابل استناد
- داشبوردسازی و هشداردهی
- به‌روزرسانی خودکار پروفایل براساس مدل‌های یادگیرنده

تعریف چالش

چالش تک‌اسپرینت
۴
کشف ناهنجاری در گراف تراکنش‌های بانکی
TM
Transaction Monitoring

چالش شماره ۴

در شبکه پرداخت کشور، روزانه میلیون‌ها تراکنش کارت‌به‌کارت میان حساب‌های بانکی انجام می‌شود. در ظاهر، این تراکنش‌ها بخشی از روند طبیعی تبادل پول میان شهروندان است، اما در پشت پرده بخشی از این تراکنش‌ها به فعالیت‌هایی مانند پولشویی، حساب‌های اجاره‌ای، جابجایی پول‌های کلاهبرداری، فرار مالیاتی و قمار آنلاین اختصاص دارد. سیستم‌های مبتنی بر قواعد سنتی تنها زمانی هشدار می‌دهند که مبلغ یا تعداد تراکنش غیرعادی باشد؛ در حالی‌که الگوهای شبکه‌ای این متخلفان همچنان پنهان باقی می‌ماند.

هدف چالش

طراحی و پیاده‌سازی یک سامانه کشف ناهنجاری و تحلیل تراکنش‌ها که بتواند:

- ناهنجاری های شبکه را کشف کند
- الگوهای جالب توجه در شبکه را پیدا کند
- گره‌ها در شبکه را طبقه‌بندی کند

داده های ورودی

داده‌های مورد استفاده در این چالش شامل داده‌های واقعی یک بانک خارجی و همچنین داده‌های شبیه‌سازی شده است

ویژگی‌های خروجی مورد انتظار

سطح ۱: طرح

- ساخت گراف تراکنش‌ها و پیدا کردن نودهای مشکوک
- نمایش ساده شبکه‌های مشکوک روی گراف

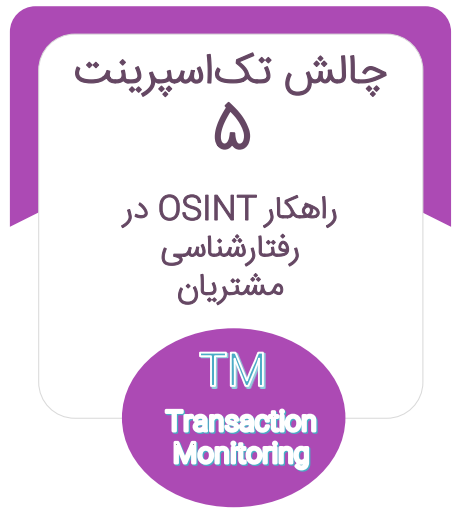
سطح ۲: نمونه اولیه MVP

- Risk Score ساده برای حساب‌ها و گروه‌ها
- داشبورد پایه برای دیدن روابط و هشدارها

سطح ۳: محصول آماده عرضه

- کشف لحظه‌ای الگوهای مشکوک
- اتصال به سیستم‌های AML و گزارش‌دهی خودکار

تعریف چالش



چالش شماره ۵

شما عضوی از واحد تحلیل بازار یک موسسه مالی هستید. مدیر مؤسسه، فهرست تراکنش‌های یک مشتری برای یک بازه زمانی مشخص را به شما ارائه می‌کند از شما می‌خواهد که در خصوص این مشتری به تحلیل اطلاعات منابع آزاد (OSINT) بپردازید. به این نحو که با بررسی اخبار، رخدادها، معاملات اتاق‌های شیشه‌ای (نظیر تالارهای بورس، پلتفرم‌های رمزارزی که دسترسی عمومی دارند و ...)، نرخ ارز، روندهای اقتصادی و تجاری (اعم از داخل کشور یا خارج کشور) و اطلاعاتی از این دست، مشخص کنید که رفتار واقعی مشتری با کدامیک تناظر دارد و استراتژی تجاری و موضوع فعالیت اصلی مشتری چیست.

هدف چالش

۱. رفتارشناسی و تکمیل اطلاعات مشتریان
۲. برنامه‌ریزی استراتژیک جهت هدفمندسازی بازاریابی
۳. برنامه‌ریزی استراتژیک جهت توسعه محصولات و خدمات جدید
۴. شناسایی روندهای پر سود در طول زمان و تنظیم نظام کارمزدی متناسب با هر مشتری

داده‌های ورودی

۱. مجموعه تراکنش‌های مشتری (در گذشته یا در ایام جاری)
۲. برخی اطلاعات مشتری نظیر استان محل فعالیت و تاریخ ثبت‌نام (پذیرش) مشتری

ویژگی‌های خروجی مورد انتظار

سطح ۱: طرح

- معماری، مدل مفهومی و جریان تبادل اطلاعات بین سامانه‌ها و منابع مختلف
- تعریف، ارزیابی استنادپذیری و رتبه‌بندی منابع
- الگوریتم‌های تحلیل و شیوه‌های گزارش‌دهی
- ساختار پروفایل اشخاص بدون وابستگی به نوع منبع

سطح ۲: نمونه اولیه MVP

- طراحی جزئی، شامل تکنولوژی‌ها یا ابزارها
- ربات‌ها و خزنده‌ها با قابلیت شخصی‌سازی کامل حداقل در ۲ منبع تخصصی
- توسعه داشبورد و بصری‌سازی میزان تناظر بین داده‌های تراکنشی و OSINT

سطح ۳: محصول آماده عرضه

- موتور یکپارچه OSINT با قابلیت تعریف منابع جدید (عام و تخصصی) و همچنین امکان مستندسازی و ارائه گزارشات قابل استناد
- پایش تراکنش‌ها در لحظه جهت شناسایی موج‌های جدید رفتار مشتریان

تعریف چالش

چالش تک‌اسپرینت
۶

مدیریت هویت و دسترسی در شبکه پرداخت

IAM
Identity & Access Management

چالش شماره ۶

شبکه پرداخت شامل کاربران متنوع است که این تنوع هویتی و پیچیدگی تعاملات، چالش‌های جدی در مدیریت هویت ایجاد می‌کند. هر یک از محورها یک بُعد ضروری از یک سیستم IAM مدرن، امن و مقیاس‌پذیر را نشان می‌دهد که باید به صورت هم‌زمان در طراحی و پیاده‌سازی آن لحاظ شود.

محورهای چالش

مدیریت هویت چندگانه
- چگونه می‌توان هویت‌ها را به طور یکپارچه و امن مدیریت کرد؟

تأمین امنیت
- چه روش‌ها و فناوری‌هایی می‌توانند امنیت IAM را تقویت کنند؟

رعایت قوانین و مقررات
- چگونه سیستم IAM را طراحی کنیم که با تغییر قوانین و مقررات جدید سازگار باشد؟

مدیریت دسترسی
- چه رویکردهایی دسترسی غیرمجاز را کاهش می‌دهند؟

مدیریت هویت‌های موقت
- چه راهکارهایی برای مدیریت هویت‌های موقت مؤثر هستند؟

تجربه کاربری
- چگونه می‌توان UX سیستم‌های IAM را بهبود داد؟

ویژگی‌های خروجی مورد انتظار

سطح ۱: طرح
- شناسایی مسائل اصلی IAM و مدل مفهومی اولیه شامل:
- لیست مشکلات اصلی مدیریت هویت فعلی
- شناسایی نقاط ضعف در دسترسی‌ها و امنیت
- تشخیص نیازهای اولیه برای بهبود سیستم IAM

سطح ۲: نمونه اولیه MVP
- نمونه عملیاتی اولیه از سیستم IAM شامل:
- جریان احراز هویت و دسترسی برای سناریوهای واقعی
- نمونه سیاست‌های دسترسی (RBAC/ABAC)
- مدیریت هویت‌های موقت
- نمونه تحلیل و گزارش‌دهی
- شبیه‌سازی بهبود امنیت و کنترل دسترسی
- یکپارچگی اولیه با سایر سیستم‌ها
- نمایش مقیاس‌پذیری و تجربه کاربری

سطح ۳: محصول آماده عرضه
- یک چارچوب کامل و قابل پیاده‌سازی IAM شامل:
- معماری جامع IAM
- مدیریت کامل دسترسی‌ها و سیاست‌ها
- مدیریت هویت‌های موقت و چرخه عمر کامل کاربران
- امنیت پیشرفته و Zero Trust
- یکپارچگی با سایر سیستم‌ها و سرویس‌ها
- تحلیل و گزارش‌دهی پیشرفته
- مقیاس‌پذیری و عملکرد در سطح سازمانی
- بهبود تجربه کاربری