



(رویداد ملی سپر نوآوری)  
مرکز رشد واحدهای فناور نوشهر  
"فرم معرفی ایده یا طرح خلاقانه"



۱- **عنوان ایده : نام محصول/سرویس: نام خلاقانه و مرتبط با ایده‌ی هوش مصنوعی شما: (کوتاه و رسا):**

سامانه هشدار هوشمند سروش (Soroush AI Early Warning System) - سیستم هشدار زودهنگام هوشمند برای پدافند سایبری و غیرعامل

سروش یک سامانه‌ی هوش مصنوعی مبتنی بر تحلیل داده‌های رفتاری شبکه و محیط است که می‌تواند پیش از وقوع بحران سایبری یا اختلال فیزیکی، هشدار زودهنگام (Early Warning) صادر کند. برخلاف سیستم‌های پیچیده دفاعی، سروش با استفاده از الگوهای یادگیری سبک (Lightweight Machine Learning) و تحلیل الگوهای غیرعادی در ترافیک شبکه، رفتار کاربران و شرایط محیطی (دما، ولتاژ، دسترسی‌ها و...)، تهدیدهای احتمالی را چند ساعت تا چند روز قبل از بروز حادثه شناسایی می‌کند.

ویژگی جذاب این ایده:

- کاملاً کاربردی و کم‌هزینه است. (نیاز به سرور یا شبکه‌ی گسترده ندارد، حتی روی یک شبکه‌ی داخلی کوچک قابل نصب است).
- در ایران نمونه مشابه ندارد. ولی مشابه ساده‌اش در برخی کشورها (مثل ژاپن و فنلاند) برای پدافند غیرعامل شهری استفاده شده.
- برای اجرا نیاز به مجوز امنیتی سطح بالا ندارد، چون فقط تحلیل داده می‌کند، نه کنترل سیستم‌ها.
- می‌تواند به‌صورت یک محصول نرم‌افزاری کوچک برای صنایع، سازمان‌ها یا حتی شهرداری‌ها ارائه شود.

هوش مصنوعی سروش با بررسی داده‌های رفتاری سیستم (مثلاً افزایش خطای ولتاژ، افت ترافیک شبکه، یا دسترسی مشکوک)، الگوهای خطر را شناسایی کرده و به مدیران هشدار می‌دهد — مثل یک پیش‌بینی‌گر بحران قبل از وقوع. فرض کنید در یک مرکز داده‌ی بانکی، در ۲۴ ساعت گذشته تعداد خطاهای لاگین ناموفق افزایش یافته، دمای سرور یکی از رک‌ها بالا رفته، و همزمان ترافیک خروجی غیرعادی شده. سروش این همبستگی رو تشخیص می‌دهد، تشخیص می‌دهد احتمال حمله یا نقص در سیستم خنک‌کننده وجود دارد و پیش از وقوع بحران هشدار می‌فرستد. سروش در واقع یک سیستم هشدار هوشمند پیشگیرانه برای حوزه‌های سایبری و فیزیکی است که می‌تواند در پروژه‌های پدافند غیرعامل شهری، صنعتی و نظامی به کار گرفته شود.

۲- **معرفی تیم کاری:**

نام و نام خانوادگی ارائه دهندگان (کامل)	تاریخ تولد	مقطع و رشته تحصیلی	پست الکترونیکی	تلفن همراه	محل اشتغال	استان
سحر پاسیار	1368	دکتر-افیزیک حالت جامد	<a href="mailto:Saharpasyar.uni@gmail.com">Saharpasyar.uni@gmail.com</a>	۰۹۱۴۳۹۴۵۸۲۴	شرکت فناوری های پیشرفته پاسیار	آذربایجان شرقی
صبا شاکر	1378	دکتر- مهندسی نفت	<a href="mailto:shakerrsabaa@gmail.com">shakerrsabaa@gmail.com</a>	0914259227 2	دانشگاه صنعتی تبریز	آذربایجان شرقی

### ۳- تعریف مسئله (Problem Statement)

در شرایط کنونی، زیرساخت‌های حیاتی کشور — از مراکز داده و نیروگاه‌ها گرفته تا شبکه‌های شهری و صنعتی — در معرض حملات سایبری، نقص‌های فنی، و اختلالات محیطی هستند که اغلب بدون هیچ هشدار قبلی اتفاق می‌افتند. در اغلب موارد، مدیران امنیتی یا فنی زمانی از بروز بحران مطلع می‌شوند که حادثه رخ داده و خسارت ایجاد شده است. در حالی که در بسیاری از کشورهای پیشرفته، سامانه‌های هشدار زودهنگام مبتنی بر هوش مصنوعی (AI Early Warning Systems) توانسته‌اند با تحلیل الگوهای رفتاری شبکه، وقوع بحران را قبل از وقوع پیش‌بینی کنند، چنین سامانه‌ای در ایران وجود ندارد.

نبود این زیرساخت پیشگیرانه باعث می‌شود:

- زمان واکنش به بحران (Response Time) بسیار بالا باشد،
- خسارت‌های سایبری و صنعتی افزایش یابد،
- و هماهنگی بین واحدهای امنیتی و فنی کاهش پیدا کند.

طبق آمار مرکز ماهر، طی سال‌های اخیر، میانگین زمان تشخیص حملات سایبری در ایران بیش از ۵ روز بوده است، در حالی که سیستم‌های هشدار هوشمند در کشورهای توسعه‌یافته این زمان را به کمتر از ۶ ساعت کاهش داده‌اند.

بنابراین، مسئله‌ی اصلی، فقدان سامانه‌ای بومی و هوشمند برای پیش‌بینی زودهنگام تهدیدات سایبری و فیزیکی است که بتواند بر اساس داده‌های واقعی و آنی، پیش از وقوع بحران، هشدار دقیق صادر کند و فرصت تصمیم‌گیری به‌موقع را برای مدیران فراهم آورد.

### ۴- راه‌حل (Solution)

سامانه سروش (Soroush AI Early Warning System) با بهره‌گیری از هوش مصنوعی و تحلیل داده‌های چندمنبعی، به‌صورت هوشمند رفتار شبکه، تجهیزات و کاربران را رصد می‌کند تا الگوهای غیرعادی را پیش از تبدیل شدن به بحران تشخیص دهد. سروش مانند یک "رادار هوشمند" عمل می‌کند که به جای تمرکز بر حملات لحظه‌ای، تغییرات تدریجی و رفتارهای مشکوک را شناسایی می‌کند — یعنی همان نشانه‌هایی که معمولاً پیش از وقوع بحران یا حمله سایبری دیده می‌شوند.

نحوه عملکرد سامانه:

#### ۱. جمع‌آوری داده‌ها:

- از لاگ‌های سیستم‌ها، ترافیک شبکه، حسگرهای محیطی (دما، ولتاژ، رطوبت)، و رفتار کاربران.

#### ۲. تحلیل الگوها با هوش مصنوعی:

- استفاده از الگوریتم‌های یادگیری ماشین سبک (Lightweight ML) برای تشخیص رفتار غیرعادی (Anomaly Detection).

- بهره‌گیری از یادگیری بدون ناظر (Unsupervised Learning) برای کشف الگوهای جدید تهدید که قبلاً تعریف نشده‌اند.
- ترکیب داده‌های سایبری و محیطی با مدل‌های یادگیری چندوجهی (Multimodal AI) جهت تحلیل جامع وضعیت.

#### ۳. تشخیص و هشدار:

- در صورت مشاهده روند خطرناک (مثل افت ناگهانی ترافیک، افزایش دما، یا خطاهای دسترسی مشکوک)، سامانه با تحلیل همبستگی داده‌ها (Data Correlation) احتمال وقوع بحران را تخمین می‌زند.
- هشدار سطح‌بندی‌شده (کم، متوسط، بحرانی) برای مدیران امنیت و نگهداری صادر می‌شود.

#### ۴. بازخورد و یادگیری مستمر:

- سروش با مرور عملکرد گذشته و صحت هشدارهای خود، به‌صورت خودآموز (Self-Learning) دقت پیش‌بینی‌ها را بهبود می‌دهد.

فناوری‌ها و الگوریتم‌های مورد استفاده:

- Isolation Forest و Autoencoder Neural Networks برای تشخیص ناهنجاری‌ها.
- Reinforcement Learning برای بهبود واکنش‌های هوشمند و کاهش هشدارهای کاذب.
- Federated Learning برای یادگیری از چند سازمان بدون نیاز به انتقال داده‌های محرمانه.

• **Dashboard** هوشمند مبتنی بر NLP برای تحلیل هشدارها به زبان طبیعی توسط مدیران. به بیان ساده، سروش همان نقشی را در امنیت سایبری ایفا می‌کند که سامانه آریانا در پدافند فیزیکی داشت — یعنی پیش‌بینی بحران پیش از وقوع آن، اما این بار در فضای دیجیتال. با این ساختار، سروش به یک ابزار ساده ولی بسیار قدرتمند تبدیل می‌شود که می‌تواند در هر سازمان یا مرکز داده‌ای نصب شود و هشدارهای زود هنگام و دقیق ارائه دهد — بدون نیاز به زیرساخت پیچیده یا نیروی انسانی زیاد.

## ۵. ارزش پیشنهادی (Value Proposition)

- چه مزیت‌هایی راه‌حل شما نسبت به راه‌حل‌های موجود دارد؟
- چرا مشتریان یا کاربران باید از راه‌حل شما استفاده کنند؟

سروش یک سامانه‌ی هوشمند هشدار زود هنگام است که ارزش اصلی آن در پیش‌بینی بحران قبل از وقوع و کاهش خسارت با هزینه‌ای بسیار پایین نهفته است. برخلاف سامانه‌های سنتی که فقط در زمان حمله یا خرابی واکنش نشان می‌دهند، سروش با استفاده از الگوریتم‌های یادگیری ماشین، می‌تواند چند ساعت تا چند روز زودتر از وقوع بحران، هشدار دقیق و تحلیلی صادر کند. مزیت‌های کلیدی سروش نسبت به راه‌حل‌های موجود:

۱. پیش‌بینی به‌جای واکنش:

- اکثر سیستم‌های امنیتی فعلی فقط در زمان وقوع تهدید فعال می‌شوند.
- سروش با مدل‌های رفتاری و تحلیل هوشمند، بحران را قبل از رخداد شناسایی می‌کند.

۲. هزینه پایین و پیاده‌سازی ساده:

- نیاز به سخت‌افزار پیشرفته یا شبکه پیچیده ندارد.
- روی یک سرور محلی یا حتی به‌صورت نرم‌افزار سبک ابری (Cloud Lite) قابل اجراست.

۳. قابلیت استفاده در چند حوزه هم‌زمان:

- هم در پدافند سایبری (مثل مراکز داده، شبکه‌های سازمانی)،
- و هم در پدافند غیرعامل صنعتی (مثل نیروگاه، پالایشگاه، کارخانه) قابل استفاده است.

۴. بومی و قابل شخصی‌سازی:

- داده‌ها در داخل سازمان پردازش می‌شوند؛ نیازی به ارسال بیرونی نیست.
- الگوریتم‌ها بر اساس نوع صنعت یا زیرساخت قابل تنظیم‌اند.

۵. کاهش خطای انسانی:

- با استفاده از داشبورد هوشمند و تحلیل بلادرنگ، تصمیم‌گیری مدیران سریع‌تر و دقیق‌تر انجام می‌شود.

۶. افزایش تاب‌آوری سازمانی:

- با هشدارهای زود هنگام، فرصت واکنش هدفمند ایجاد می‌شود؛ این یعنی افزایش پایداری، کاهش توقف عملیات، و حفظ امنیت داده‌ها.

سروش، یک دستیار هوشمند پیش‌بینی بحران است که با هزینه‌ای کم، امنیت سایبری و پایداری زیرساختی را چند برابر می‌کند — بدون نیاز به تغییر ساختار موجود یا خرید تجهیزات جدید.

## ۶. تحلیل بازار (Market Analysis)

- مخاطبان هدف شما چه کسانی هستند؟
- اندازه بازار چگونه است؟ چقدر پتانسیل رشد وجود دارد؟

مخاطبان هدف: (Target Audience)

محصول سروش برای سازمان‌ها و مجموعه‌هایی طراحی شده که امنیت، پایداری و تاب‌آوری در آن‌ها حیاتی است، از جمله:

۱. نهادهای حیاتی و زیرساختی کشور:
  - نیروگاه‌ها، پالایشگاه‌ها، مراکز داده، شرکت‌های آب، برق و گاز.
۲. سازمان‌های دولتی و دفاعی:
  - مراکز فناوری اطلاعات، پدافند غیرعامل، و شبکه‌های ارتباطی ملی.
۳. بانک‌ها و شرکت‌های پرداخت الکترونیک:
  - جهت پیش‌بینی حملات سایبری یا نقص در سرویس‌های مالی.
۴. صنایع تولیدی و پتروشیمی:
  - برای جلوگیری از خرابی تجهیزات یا اختلال در فرآیندهای صنعتی.
۵. شهرداری‌ها و مراکز مدیریت بحران شهری:
  - در راستای پدافند غیرعامل شهری و پایش زیرساخت‌های هوشمند.

#### اندازه و پتانسیل بازار: (Market Size & Growth Potential)

- طبق برآوردهای جهانی، بازار سیستم‌های هشدار زودهنگام هوش مصنوعی تا سال ۲۰۳۰ بیش از ۱۵ میلیارد دلار رشد خواهد داشت.
- در ایران، حدود ۳۵۰ سازمان و نهاد زیرساختی به‌صورت مستقیم مشمول الزامات پدافند غیرعامل هستند؛ اگر تنها ۳۰٪ از آن‌ها سامانه سروش را به‌کار گیرند، بازار بالقوه‌ای معادل ۵۰ تا ۷۰ میلیون دلار فقط در سطح داخلی ایجاد می‌شود.
- علاوه بر آن، نسخه سبک‌تر سروش می‌تواند در شرکت‌های خصوصی و مراکز داده کوچک نیز استفاده شود که پتانسیل بازار را چند برابر می‌کند.

#### پتانسیل رشد: (Growth Potential)

- در سطح ملی: الزام قانونی برای ارتقای پدافند غیرعامل در دستگاه‌های اجرایی و صنعتی، فضای مناسبی برای پذیرش این سامانه ایجاد کرده است.
- در سطح منطقه‌ای: کشورهای همسایه با چالش‌های مشابه در حوزه امنیت سایبری مواجه‌اند و به سامانه‌های بومی‌سازی شده علاقه‌مندند؛ بنابراین امکان صادرات فناوری به کشورهای منطقه (مثل عراق، ارمنستان، آذربایجان و عمان) نیز وجود دارد.
- در سطح تکنولوژیک: قابلیت توسعه سروش به‌عنوان پلتفرم ابری ملی هشدار زودهنگام می‌تواند آن را به بخشی از شبکه هوشمند پدافند کشور تبدیل کند.

بازار سروش نه تنها در بخش امنیت سایبری بلکه در حوزه پدافند غیرعامل شهری و صنعتی نیز پتانسیل رشد بالایی دارد. این محصول با هزینه‌ی پایین، قابلیت پیاده‌سازی سریع و مقیاس‌پذیری بالا، می‌تواند به یکی از اولین محصولات بومی هوش مصنوعی در حوزه هشدار زودهنگام بحران در ایران و منطقه تبدیل شود.

#### ۷. مزیت رقابتی (Competitive Advantage)

- چه عواملی شما را از رقبای متمایز می‌کند؟
- ویژگی‌های منحصر به فرد محصول یا خدمات شما چیست؟

سامانه‌ی سروش به‌عنوان نخستین سیستم بومی هشدار زودهنگام مبتنی بر هوش مصنوعی در حوزه پدافند سایبری و غیرعامل، دارای مجموعه‌ای از ویژگی‌های منحصر به فرد است که آن را از سایر راه‌حل‌های موجود متمایز می‌کند.

۱. هوش پیش‌بینی‌گر، نه صرفاً واکنشی  
برخلاف سامانه‌های امنیتی سنتی (که پس از وقوع تهدید واکنش نشان می‌دهند)، سروش بر پایه‌ی مدل‌های پیش‌بینی رفتاری (Behavioral Forecasting) طراحی شده و می‌تواند قبل از وقوع حادثه هشدار دهد. این رویکرد از پایه با همه‌ی محصولات فعلی در بازار متفاوت است.

۲. بومی، امن و مستقل از سرویس‌های خارجی  
سروش به‌طور کامل در داخل کشور قابل توسعه و استقرار است و به هیچ سرویس ابری یا پایگاه داده خارجی وابسته نیست.  
در نتیجه:

- خطر نشت داده وجود ندارد،
- تطابق کامل با الزامات پدافند غیرعامل دارد،
- و برای نهادهای حساس، گزینه‌ای مطمئن و قابل اعتماد محسوب می‌شود.

۳. یادگیری خودکار و انطباق با محیط‌های مختلف  
الگوریتم‌های سروش به‌صورت Self-Learning عمل می‌کنند؛  
یعنی با گذشت زمان و مشاهده‌ی الگوهای واقعی هر سازمان، خود را با آن سازگار می‌کنند.  
این ویژگی باعث می‌شود سامانه در هر محیط صنعتی یا اداری، دقت بالاتری نسبت به راه‌حل‌های ثابت خارجی داشته باشد.

۴. معماری سبک، قابل استقرار سریع و کم‌هزینه  
درحالی‌که اغلب سامانه‌های امنیتی نیاز به زیرساخت سخت‌افزاری گسترده دارند،  
سروش به‌صورت نرم‌افزار سبک (Lightweight AI Agent) طراحی شده و در کمتر از چند ساعت قابل نصب، تنظیم و استفاده است.  
این یعنی هزینه پیاده‌سازی پایین، بدون نیاز به تغییر زیرساخت موجود.

۵. قابلیت اتصال هم‌زمان به داده‌های سایبری و فیزیکی  
سروش ترکیبی از پدافند سایبری و غیرعامل است؛  
یعنی علاوه بر شبکه و سیستم‌ها، می‌تواند داده‌های محیطی (مثل دما، ولتاژ، فشار و...) را هم تحلیل کند و ارتباط بین خطاهای فنی و حملات  
احتمالی را تشخیص دهد.  
چنین ترکیبی در ایران و منطقه تاکنون وجود نداشته است.

۶. قابلیت تجاری‌سازی سریع و مقیاس‌پذیری بالا  
طراحی ماژولار سروش اجازه می‌دهد نسخه‌های مختلف آن (صنعتی، شهری، اداری) به‌صورت جداگانه عرضه شوند.  
این یعنی محصول هم برای نهادهای بزرگ دولتی و هم برای شرکت‌های خصوصی کوچک مناسب است — مزیتی که رقبا معمولاً ندارند.  
مزیت اصلی سروش در ترکیب هوش مصنوعی سبک، پیش‌بینی بلادرنگ، و استقلال از سرویس‌های خارجی است.  
این سامانه می‌تواند به‌عنوان اولین پلتفرم هشدار زودهنگام بومی در ایران، نقش کلیدی در افزایش تاب‌آوری سایبری و صنعتی کشور ایفا کند.

## ۸. مدل کسب و کار (Business Model)

مدل کسب‌وکار سامانه‌ی سروش بر پایه‌ی فروش سرویس هوشمند به سازمان‌ها و صنایع حساس، همراه با مدل اشتراکی و پشتیبانی بلندمدت  
طراحی شده است. هدف، ایجاد جریان درآمدی پایدار و مقیاس‌پذیر در حوزه‌ی امنیت و پدافند سایبری است.

### ۱. فروش مجوز نرم‌افزار (License Sale)

سروش در سه نسخه‌ی اصلی عرضه می‌شود:

- نسخه سازمانی (Enterprise): برای وزارتخانه‌ها، زیرساخت‌های حیاتی، نیروگاه‌ها و مراکز صنعتی بزرگ.
- نسخه شرکتی (Corporate): برای بانک‌ها، شرکت‌های IT و صنایع متوسط.
- نسخه سبک (Lite): ویژه‌ی شرکت‌های کوچک یا مراکز آموزشی.

هر نسخه با هزینه مجوز اولیه (Setup License) فروخته می‌شود که شامل نصب، آموزش و راه‌اندازی است.

### ۲. درآمد اشتراکی ماهانه (Subscription Model)

پس از نصب اولیه، سازمان‌ها اشتراک ماهانه یا سالانه برای دریافت موارد زیر پرداخت می‌کنند:

- به‌روزرسانی الگوریتم‌های هوش مصنوعی
- پشتیبانی ۷/۲۴
- مانیتورینگ مرکزی تهدیدات
- تحلیل‌های دوره‌ای عملکرد سیستم

این بخش مهم‌ترین منبع درآمد پایدار سروش است.

### ۳. خدمات سفارشی‌سازی (Customization Services)

هر صنعت ویژگی‌های خاص خود را دارد (مثلاً پتروشیمی با بانک تفاوت دارد).

سروش قابلیت شخصی‌سازی ماژول‌ها را دارد، و برای هر پروژه‌ی خاص هزینه جداگانه‌ی سفارشی‌سازی دریافت می‌شود.

### ۴. همکاری با نهادهای حاکمیتی و دانشگاه‌ها

سروش می‌تواند از طریق قراردادهای همکاری (B2G) با سازمان‌های پدافند غیرعامل، شرکت‌های دانش‌بنیان، و دانشگاه‌های صنعتی توسعه یابد.

در این مدل، سروش به‌عنوان پلتفرم پایه‌ی ملی هشدار زودهنگام مورد استفاده قرار می‌گیرد و هزینه توسعه یا خدمات از محل پروژه‌های مشترک تأمین می‌شود.

### ۵. مدل درآمدی بلندمدت (Long-term Revenue Stream)

در چشم‌انداز سه‌ساله، سروش می‌تواند با ایجاد مرکز ملی هشدار هوشمند سایبری (Smart Cyber Defense Hub)،

به سایر کشورهای منطقه نیز خدمات ارائه دهد و از صادرات فناوری بومی درآمد ارزی ایجاد کند.

جدول ۱ چشم‌انداز سه‌ساله سروش

منبع درآمد	توضیح	پایداری
فروش مجو اولیه	نصب و راه‌اندازی اولیه سامانه	یکباره
اشتراک ماهانه / سالانه	پشتیبانی و به‌روز رسانی مداوم	پایدار
سفارشی‌سازی صنعتی	توسعه ماژول‌های اختصاصی	پروژه‌ای
قرارداد همکاری با نهادها	توسعه ملی و بین‌سازمانی	بلند مدت

### ۹. نقشه راه (Roadmap)

- مراحل توسعه محصول از حال حاضر تا زمان عرضه به بازار
- چشم‌انداز آینده برای گسترش و بهبود محصول چیست؟

#### مرحله ۱ - تحقیق و طراحی اولیه (۰ تا ۳ ماه)

- تشکیل تیم فنی و تحقیقاتی (متشکل از متخصصان هوش مصنوعی، امنیت سایبری و نرم‌افزار).
- جمع‌آوری داده‌های واقعی از محیط‌های صنعتی، شهری و اداری جهت آموزش مدل‌ها.
- طراحی الگوریتم پایه‌ی پیش‌بینی تهدید (Threat Forecast Model).
- خروجی: نمونه مفهومی (Concept Prototype) از سامانه‌ی سروش.

#### مرحله ۲ - توسعه نسخه آزمایشی (۴ تا ۹ ماه)

- پیاده‌سازی داشبورد مدیریتی و هسته هوش مصنوعی.
- تست عملکرد در یک محیط واقعی (مثلاً در یک مرکز صنعتی یا شهرداری منتخب).

دبیرخانه مسابقات : استان مازندران - نوشهر - خیابان رازی- خیابان ۲۲ بهمن - کوچه مسجد- ساختمان مرکز رشد و نوآوری نوشهر

تلفن و نمابر دبیرخانه : ۰۱۱-۵۲۱۴۱۱۷۳ کسب اطلاعات بیشتر با رئیس دبیرخانه رویداد : مهندس ترابی: ۰۹۱۱۳۹۵۱۹۷۹

لطفاً فایل تکمیل شده در دو قالب Word و PDF و PDF در وبسایت [separnoavari.ir](http://separnoavari.ir) ارسال فرمائید.

- دریافت بازخورد از کاربران و بهینه‌سازی رابط کاربری و مدل‌های یادگیری.

خروجی: نسخه‌ی آزمایشی قابل نصب. (Beta Version)

مرحله ۳ – تجاری‌سازی محدود (۱۰ تا ۱۸ ماه)

- اخذ مجوزهای لازم از مراجع ذی‌ربط (سازمان پدافند غیرعامل، وزارت ارتباطات).
- عرضه نسخه‌ی سازمانی برای ۳ مشتری آزمایشی. (Pilot Clients)
- تدوین مدل اشتراک‌گذاری و پشتیبانی فنی.
- خروجی: نسخه‌ی رسمی اولیه برای سازمان‌ها و صنایع حساس.

مرحله ۴ – توسعه زیرساخت ملی (۱۸ تا ۳۶ ماه)

- راه‌اندازی مرکز هشدار هوشمند سروش (Soroush Defense Hub) برای تحلیل داده‌های ملی در سطح کلان.
- گسترش دامنه استفاده به سایر استان‌ها، صنایع انرژی، مخابرات، بانک‌ها و شرکت‌های بزرگ.
- توسعه ماژول‌های جدید شامل:

○ تحلیل رفتار تهدیدات داخلی (Insider Threat Detection)

○ تحلیل هم‌زمان داده‌های فیزیکی و سایبری

○ نسخه سبک برای SME ها و ادارات کوچک

خروجی: سروش به‌عنوان پلتفرم ملی هشدار زودهنگام و تاب‌آوری سایبری.

چشم‌انداز آینده (۳ تا ۵ سال بعد)

- اتصال سروش به سامانه‌های بین‌المللی هشدار بحران برای پیش‌بینی حملات فرامرزی.
- ایجاد نسخه ابری با قابلیت استفاده چندسازمانی. (Cloud-based Defense Platform)
- صادرات فناوری بومی سروش به کشورهای منطقه (ترکیه، عراق، قطر، عمان).
- بهره‌گیری از داده‌های کلان و شبکه‌های عصبی پیشرفته برای پیش‌بینی تهدیدات در سطح ملی.

نقشه راه سروش نشان می‌دهد این پروژه نه تنها فنی و نوآورانه است، بلکه دارای مسیر توسعه‌ی گام‌به‌گام، قابل اجرا و متناسب با اهداف پدافند غیرعامل کشور است. سروش در سه سال می‌تواند از یک نمونه آزمایشی دانشگاهی به پلتفرم ملی هشدار زودهنگام تبدیل شود.

## ۱۰. چالش‌ها و ریسک‌ها

- چالش‌های فنی، عملیاتی یا بازاریابی که ممکن است با آن مواجه شوید.

- برنامه شما برای غلبه بر این چالش‌ها چیست؟

هر پروژه نوآورانه در حوزه‌ی پدافند سایبری و هوش مصنوعی، با موانع و چالش‌هایی همراه است. سروش نیز از این قاعده مستثنی نیست؛ با این تفاوت که برای هر چالش، راه‌حل مشخص و عملیاتی در نظر گرفته شده است.

۱. چالش فنی: کمبود داده‌های بومی و واقعی برای آموزش هوش مصنوعی

ریسک: در حوزه امنیت سایبری، بسیاری از داده‌های واقعی محرمانه هستند و دسترسی به آن‌ها دشوار است.

راه‌حل:

- همکاری با مراکز دانشگاهی و پژوهشی دارای مجوز پدافند غیرعامل برای تولید داده‌های شبیه‌سازی شده. (Synthetic Data)
- ایجاد محیط تست ملی (National Cyber Sandbox) برای تولید و اعتبارسنجی داده‌های واقعی در شرایط کنترل شده.

۲. چالش امنیتی: اطمینان از محرمانگی کامل اطلاعات کاربران

ریسک: سامانه‌هایی که داده‌های حساس را تحلیل می‌کنند، خودشان ممکن است هدف حمله قرار گیرند.

راه‌حل:

- استفاده از رمزنگاری چندلایه (Multi-layer Encryption) و تفکیک داده‌ها در سطح کلاینت و سرور.

دبیرخانه مسابقات: استان مازندران – نوشهر – خیابان رازی – خیابان ۲۲ بهمن – کوچه مسجد – ساختمان مرکز رشد و نوآوری نوشهر

تلفن و نمابر دبیرخانه: ۰۱۱-۵۲۱۴۱۱۷۳ کسب اطلاعات بیشتر با رئیس دبیرخانه رویداد: مهندس ترابی: ۰۹۱۱۳۹۵۱۹۷۹

لطفاً فایل تکمیل شده در دو قالب Word و PDF در وبسایت [separnoavari.ir](http://separnoavari.ir) ارسال فرمائید.

- پیاده‌سازی سیاست “Zero Trust Architecture” که در آن هیچ سطح دسترسی‌ای به‌صورت پیش‌فرض امن نیست.

۳. چالش عملیاتی: استقرار سامانه در سازمان‌های بزرگ و پیچیده

ریسک: برخی نهادهای صنعتی یا دولتی دارای زیرساخت قدیمی هستند و پیاده‌سازی هوش مصنوعی در آن‌ها دشوار است.

راه‌حل:

- طراحی ماژولار سرویس به‌صورت Agent-based تا بتواند بدون تغییر زیرساخت، به‌صورت افزونه (Plug-in) نصب شود.
- ارائه تیم فنی برای استقرار در محل و آموزش پرسنل جهت کاهش مقاومت سازمانی در برابر فناوری جدید.

۴. چالش اقتصادی: هزینه اولیه بالا برای توسعه و جذب سرمایه‌گذار

ریسک: توسعه الگوریتم‌های هوش مصنوعی و امنیتی نیازمند سرمایه‌گذاری اولیه قابل توجه است.

راه‌حل:

- همکاری با مراکز رشد و شتاب‌دهنده‌های حوزه فناوری دفاعی و سایبری.
- تعریف پروژه‌های مشترک با نهادهای دولتی (B2G) به‌عنوان سرمایه‌گذار اولیه.
- طراحی مدل درآمدی اشتراکی برای بازگشت سریع سرمایه پس از عرضه نسخه اولیه.

۵. چالش بازاریابی و اعتمادسازی در بازار داخلی

ریسک: سازمان‌ها معمولاً نسبت به محصولات امنیتی جدید بومی بی‌اعتماد هستند و ترجیح می‌دهند از نرم‌افزارهای خارجی استفاده کنند.

راه‌حل:

- اجرای پروژه‌های آزمایشی (Pilot Projects) در چند نهاد منتخب جهت اثبات کارایی.
- دریافت گواهی‌نامه امنیتی از مراکز رسمی (مرکز ماهر، سازمان پدافند غیرعامل).
- برگزاری کارگاه‌ها و نمایش‌های تخصصی برای معرفی مزیت‌های فنی و اقتصادی سرویس.

۶. چالش نیروی انسانی متخصص در هوش مصنوعی امنیتی

ریسک: متخصصان AI در زمینه امنیت سایبری در کشور محدود هستند.

راه‌حل:

- ایجاد برنامه همکاری دانشگاهی با دانشجویان کارشناسی ارشد و دکتری در حوزه یادگیری ماشین و امنیت.
- آموزش نیروی داخلی از طریق کارگاه‌های تخصصی تحت پروژه سرویس.

هرچند سرویس با چالش‌های فنی، اقتصادی و نهادی روبه‌روست، اما با طراحی ماژولار، توسعه داده‌های مصنوعی، رمزنگاری چندلایه و مدل درآمدی پایدار، ریسک‌های آن به‌صورت مؤثر کنترل‌پذیر هستند و مسیر توسعه آن کاملاً واقع‌بینانه و اجرایی است.

## ۱. نتیجه‌گیری و درخواست (Closing and Ask)

سامانه‌ی سرویس پاسخی بومی، هوشمند و آینده‌نگر به یکی از حیاتی‌ترین نیازهای کشور است: تشخیص و پیش‌بینی تهدیدات سایبری و غیرعامل پیش از وقوع بحران. در دنیایی که حملات سایبری و اختلالات زیرساختی به‌صورت هم‌زمان رخ می‌دهند، سرویس با ترکیب یادگیری ماشین، تحلیل پیش‌گویانه، و پدافند غیرعامل دیجیتال می‌تواند نقش «رادار هوشمند» برای سازمان‌ها و صنایع حیاتی کشور را ایفا کند. سرویس نه تنها یک ابزار هوشمند برای امنیت سایبری است، بلکه گامی مهم در مسیر خودکفایی دفاعی دیجیتال، افزایش تاب‌آوری ملی و پدافند غیرعامل هوشمند در کشور محسوب می‌شود. این سامانه:

- کاملاً بومی، امن و مستقل از زیرساخت‌های خارجی است،
- با هزینه پایین و سرعت بالا قابل استقرار در سازمان‌های مختلف می‌باشد،
- و با الگوریتم‌های یادگیرنده، به مرور دقیق‌تر و هوشمندتر می‌شود.

درخواست: (Ask)

دبیرخانه مسابقات: استان مازندران - نوشهر - خیابان رازی - خیابان ۲۲ بهمن - کوچه مسجد - ساختمان مرکز رشد و نوآوری نوشهر

تلفن و نمابر دبیرخانه: ۰۱۱-۵۲۱۴۱۱۷۳ - کسب اطلاعات بیشتر با رئیس دبیرخانه رویداد: مهندس ترابی: ۰۹۱۱۳۹۵۱۹۷۹

لطفاً فایل تکمیل شده در دو قالب Word و PDF در وبسایت [separnoavari.ir](http://separnoavari.ir) ارسال فرمائید.

برای عبور از مرحله ایده تا پیاده‌سازی ملی، نیاز به:

۱. حمایت مالی اولیه (Seed Funding) جهت توسعه نمونه صنعتی فروش،
  ۲. دسترسی به محیط‌های تست سازمانی (برای آزمایش الگوریتم در داده‌های واقعی)،
  ۳. و همکاری استراتژیک با سازمان پدافند غیرعامل و مراکز دانشگاهی کشور داریم.
- هدف ما این است که در کمتر از ۱۸ ماه، نسخه‌ی سازمانی فروش را به‌صورت عملیاتی در یکی از صنایع کلیدی کشور راه‌اندازی کنیم و از آن به‌عنوان اولین سامانه هشدار زود هنگام بومی ایران رونمایی شود.

آیا نمونه اولیه ایده یا طرح خود را ساخته اید؟ ☐ بلی ☐ خیر

آیا آمادگی ارائه نمونه اولیه محصول یا خدمت خود را جهت بررسی داوران دارید؟ ☐ بلی ☐ خیر