



بسمه تعالی

سامانه هوشمند یکپارچه امنیت سازمانی

Sehyas: Samaneh-ye Hooshmand-e Yekparcheh-ye)

(Amniyat-e Sazmani

با بهره گیری از معماری پیشرفته
XDR (Extended Detection and
(Response



فهرست مطالب

بخش	عنوان	صفحه
۱	خلاصه اجرایی و ارزش پیشنهادی منحصر به فرد	۳
۲	معرفی، چشم انداز و مأموریت سامانه	۵
۳	تحلیل عمیق ضرورت و نیازسنجی	۶
۴	اهداف کلان راهبردی و عملیاتی پروژه	۷
۵	معماری XDR؛ قلب تپنده سامانه سهیاس	۸
۶	سه رکن کلیدی سامانه سهیاس (امنیت، یکپارچگی، هوشمندی)	۱۰
۷	ساختار و مؤلفه های تفصیلی سامانه	۱۲
۸	قابلیت های پیشرفته کنترل امنیت نظارتی (VMS)	۱۴
۹	رکن دوم: کنترل نشد داده (DLP) و هوشمندی آن	۱۷
۱۰	معماری فنی و زیرساخت نسل نوین	۱۹
۱۱	مزایا، دستاوردها و بازگشت سرمایه (ROI)	۲۱
۱۲	برنامه زمانبندی تفصیلی و روش اجرا	۲۳
۱۳	برآورد بودجه و منابع انسانی	۲۵
۱۴	جمع بندی و پیشنهاد راهبردی	۲۶
۱۵	ضمائم و مستندات فنی	۲۷



ردیف	ویژگی کلیدی	شرح جامع
۱	معماری XDR پیشرفته	جمع آوری، نرمال سازی و همبستگی خودکار داده های امنیتی از تمامی منابع (دوربینها، شبکه، نقاط پایانی، ایمیل، برنامه ها، DLP، و سرورها) در یک پلتفرم واحد برای تشخیص تهدیدات چندمرحله ای و ترکیبی .
۲	سه رکن کلیدی (سهیاس)	امنیت (فیزیکی، شبکه، اطلاعات)، یکپارچگی (در پنج لایه سخت افزاری، نرم افزاری، دادهای، فرایندی و مدیریتی)، و هوشمندی (هوش مصنوعی و یادگیری ماشین).
۳	یکپارچگی کامل و بومی	طراحی کاملاً بومی با قابلیت شخصی سازی عمیق، بررسی کد منبع، و اتصال هوشمندانه به تمامی تجهیزات و سامانه های موجود سازمان.
۴	هوش مصنوعی نسل جدید (Agentic AI)	تشخیص، پیش بینی و واکنش خودکار به تهدیدات با دقت بالای ۹۸٪. استفاده از دستیار هوش مصنوعی برای خودکارسازی تحلیل و ارائه سناریوهای پاسخ .
۵	کاهش هشدارهای کاذب	کاهش ۸۰٪ هشدارهای کاذب با استفاده از الگوریتمهای پیشرفته همبستگی و تحلیل رفتاری، جلوگیری از خستگی تیم امنیتی.
۶	دید ۳۶۰ درجه و داشبورد یکپارچه	ارائه یک تصویر منسجم و واحد از وضعیت امنیت سازمان در یک داشبورد مدیریتی واحد، با قابلیت نمایش روایت کامل زنجیره حمله.
۷	واکنش خودکار و هماهنگ	قابلیت واکنش خودکار به تهدیدات در کمتر از ۱ ثانیه، از طریق اجرای پلیبوک های امنیتی و هماهنگی بین لایه های فیزیکی، شبکه ای و اطلاعاتی.

جدول تحلیل چالش‌ها و راه‌حل‌های سامانه سهیاس

ردیف	چالش اساسی	شرح چالش	راه‌حل منحصر به فرد سهیاس
۱	تهدیدات ترکیبی و چندوجهی	حملات مدرن از جبهه‌های فیزیکی، شبکه و اطلاعات به صورت همزمان و هماهنگ اجرا میشوند.	معماری XDR با جمع‌آوری و همبستگی داده‌های تمامی منابع، امکان شناسایی همزمان و ارتباط‌دهی این تهدیدات را فراهم میکند.
۲	حجم عظیم هشدارهای کاذب	تیم‌های امنیتی با سیل هشدارهای روزانه (بیش از ۹۰٪ کاذب) مواجه‌اند که تحلیل را مختل میکند.	همبستگی هوشمند و اولویت‌بندی ریسک بر اساس هوش مصنوعی، هشدارهای واقعی را از کاذب تفکیک کرده و بر اساس شدت، اولویت‌بندی میکند.
۳	عدم یکپارچگی سامانه‌های امنیتی	سامانه‌های امنیتی (فیزیکی، شبکه‌ای، اطلاعاتی) به صورت جزیره‌ای و بدون ارتباط با یکدیگر مدیریت میشوند.	XDR با یکپارچه‌سازی داده‌های تمامی سامانه‌ها، یک تصویر واحد و منسجم از وضعیت امنیت ارائه میدهد و سیل‌های اطلاعاتی را حذف می‌کند.
۴	نیاز به واکنش پیشدستانه و آنی	روشهای سنتی مبتنی بر واکنش پس از وقوع حادثه هستند که خسارت جبران‌ناپذیری به بار می‌آورند.	تحلیل الگوهای رفتاری و شناسایی ناهنجاریها توسط XDR ، پیش از وقوع حادثه هشدار داده و اقدامات خودکار را آغاز میکند.
۵	ناتوانی در تشخیص حملات پیشرفته	حملات امروزی پیچیده، چندمرحله‌ای و با تکنیک‌های پنهانسازی هستند که توسط ابزارهای سنتی قابل شناسایی نیستند.	همبستگی داده‌های متنوع و استفاده از هوش مصنوعی در معماری XDR ، امکان شناسایی حملات پیشرفته و زنجیره حمله را فراهم میسازد.



۱. خلاصه اجرایی و ارزش پیشنهادی منحصر به فرد

سامانه سهیاس (سامانه هوشمند یکپارچه امنیت سازمانی) یک پلتفرم امنیتی نسل نوین است که با تلفیق دو حوزه حیاتی امنیت فیزیکی (نظارت تصویری هوشمند) و امنیت اطلاعات (کنترل نشت داده DLP) در یک بستر کاملاً یکپارچه و مبتنی بر معماری XDR و هوش مصنوعی (AI)، راهکاری جامع، خودکار و هوشمند برای مدیریت تمام‌جانبه امنیت سازمان ارائه می‌دهد.

ارزش پیشنهادی کلیدی (KPIها):

هدف	شرح	شاخص کلیدی عملکرد (KPI)
ارتقاء سطح بلوغ امنیتی	افزایش قابلیت‌های سازمان در شناسایی، پیش‌گیری و پاسخ‌دهی به تهدیدات	افزایش ۴۰٪ در شاخص بلوغ امنیتی (بر اساس مدل CMMI)
یکپارچه‌سازی سامانه‌های امنیتی	ایجاد یک بستر واحد مبتنی بر XDR برای مدیریت تمامی لایه‌های امنیتی	کاهش ۷۰٪ در تعداد سامانه‌های مدیریتی جداگانه
هوشمندسازی و خودکارسازی فرایندها	کاهش وابستگی به تصمیمات انسانی و خودکارسازی تشخیص و واکنش	افزایش ۶۰٪ در خودکارسازی فرایندهای امنیتی
کاهش زمان تشخیص تهدید (MTTD)	کاهش میانگین زمان شناسایی تهدیدات از ۴۵ دقیقه به کمتر از ۲ دقیقه	کاهش از ۴۵ دقیقه به کمتر از ۲ دقیقه
کاهش زمان واکنش به تهدید (MTTR)	کاهش میانگین زمان مهار و خنثی‌سازی تهدیدات از ۳ ساعت به کمتر از ۱۵ دقیقه	کاهش از ۳ ساعت به کمتر از ۱۵ دقیقه
کاهش هشدارهای کاذب	کاهش تعداد هشدارهای غیرواقعی با استفاده از الگوریتم‌های پیشرفته	کاهش ۸۰٪ در هشدارهای کاذب
افزایش دقت تشخیص	افزایش نسبت تشخیص صحیح تهدیدات واقعی به بیش از ۹۸٪	افزایش به بیش از ۹۸٪ دقت تشخیص



۲. معرفی، چشم انداز و مأموریت سامانه

۲-۱. معرفی

سامانه **سپاس** با بهره‌گیری از **معماری پیشرفته XDR** و سه رکن **کلیدی امنیت، یکپارچگی و هوشمندی**، مرزهای سنتی امنیت سازمانی را جابه‌جا میکند. این سامانه با اتصال هوشمندانه دوربینهای مدار بسته، سیستمهای کنترل تردد، سنسورهای محیطی، سامانه کنترل نشست داده (DLP)، شبکه، سرورها، نقاط پایانی و برنامه‌های کاربردی، یک **مرکز عملیات امنیت یکپارچه (Integrated SOC)** ایجاد میکند که تمامی تهدیدات را در یک نما پایش، تحلیل و مهار مینماید.

۲-۲. چشم‌انداز

"ایجاد یک اکوسیستم امنیتی خودکار، هوشمند و هماهنگ مبتنی بر معماری **XDR** که با تحلیل داده‌های لحظه‌ای از تمامی منابع، تهدیدات را پیش‌بینی، تشخیص و مهار نماید".

۲-۳. مأموریت

"تحول در مدیریت امنیت سازمان از طریق یکپارچه‌سازی هوشمندانه **لایه‌های امنیتی فیزیکی، شبکه‌ای و اطلاعاتی** با بهره‌گیری از معماری **XDR** و الگوریتمهای یادگیری ماشین".

۳. تحلیل عمیق ضرورت و نیازسنجی

سازمان‌های امروزی با تهدیدات پیچیده و چندوجهی مواجه اند که سامانه‌های سنتی قادر به پاسخگویی به آنها نیستند. سامانه **سپاس** با تکیه بر معماری **XDR** و هوش مصنوعی، پاسخگوی این چالشهاست.

جدول تحلیل نیازها و پاسخ سامانه سپاس:

نیاز کلیدی	شرح نیاز	پاسخ سامانه سپاس
همبستگی داده‌های فیزیکی و سایبری	ارتباطدهی هوشمند بین رویدادهای امنیت فیزیکی (تصاویر دوربین، تردد) و رویدادهای امنیت سایبری (نشست داده، حملات شبکه) برای شناسایی تهدیدات ترکیبی.	موتور همبستگی XDR با تحلیل همزمان داده‌ها، الگوهای حمله ترکیبی را کشف میکند.
تشخیص حملات چندمرحله‌ای	شناسایی حملاتی که از چندین جبهه و در چندین مرحله اجرا میشوند (مثلاً نفوذ فیزیکی + نشست داده).	XDR با گردآوری داده‌های پراکنده، روایت منسجمی از کل زنجیره حمله ارائه میدهد.

کاهش زمان تشخیص و واکنش	نیاز به کاهش چشمگیر زمان شناسایی و پاسخ‌دهی به تهدیدات برای جلوگیری از خسارت .	با همبستگی خودکار و واکنشهای از پیش تعریف‌شده، زمان MTTR و MTTD به شدت کاهش می‌یابد.
ارائه روایت منسجم از حملات	تبدیل داده های پراکنده به یک روایت منسجم برای درک کامل و مستندسازی حمله .	XDR داده های پراکنده را به یک روایت منسجم از یک حمله تبدیل کرده و دید کاملی از زنجیره حمله ارائه می‌دهد.
افزایش بهره‌وری تیم امنیتی	کاهش حجم هشدارها و ارائه اطلاعات مفید و همبسته شده برای تمرکز بر تهدیدات واقعی .	با کاهش هشدارهای کاذب و اولویت‌بندی هوشمند، تیم امنیتی بر روی تهدیدات واقعی متمرکز میشود.

۴. اهداف کلان راهبردی و عملیاتی پروژه

۴-۱. اهداف راهبردی

لایه امنیتی	شرح جامع
امنیت فیزیکی	نظارت تصویری هوشمند، کنترل تردد، تشخیص حریم، تشخیص اشیاء و رفتارهای مشکوک.
امنیت شبکه	پایش ترافیک شبکه، تشخیص نفوذ (IDS/IPS)، کنترل دسترسی شبکه و تحلیل پروتکلها.
امنیت اطلاعات	کنترل نشت داده (DLP)، پایش کانال‌های خروجی اطلاعات، رمزنگاری و مدیریت دسترسی.
امنیت ترکیبی (XDR)	همبستگی رویدادهای فیزیکی، شبکه‌ای و اطلاعاتی برای شناسایی تهدیدات ترکیبی و ارائه پاسخ یکپارچه .

۴-۲. اهداف عملیاتی

مؤلفه XDR	شرح
جمع آوری داده (Data Ingestion)	جمع‌آوری خودکار و نرم‌السازی داده‌های امنیتی از تمامی منابع: دوربینها، شبکه، سرورها، نقاط پایانی، ایمیل، برنامه های کاربردی، DLP و سامانه های فیزیکی .



ارتباط‌دهی هوشمند بین رویدادهای پراکنده برای کشف الگوهای پیچیده حمله و شناسایی روابط پنهان.	همبستگی (Correlation)
استفاده از هوش مصنوعی (Agentic AI) و یادگیری ماشین برای شناسایی تهدیدات پیچیده، ناهنجاریها و پیشبینی ریسک .	تحلیل پیشرفته (Advanced Analytics)
هماهنگی خودکار واکنش بین لایه های مختلف امنیتی (فیزیکی، شبکه ای و اطلاعاتی) از طریق اجرای پلیبوک‌های امنیتی (Security Playbook).	پاسخ یکپارچه (Unified Response)
ارائه روایت منسجم از حملات، تولید گزارشهای تحلیلی و مستندسازی برای ممیزی و تحلیل.	گزارش‌گیری و مستندسازی

۵. معماری XDR؛ قلب تپنده سامانه سهیاس

۵-۱. مفهوم XDR و مزایای آن

XDR (Extended Detection and Response) یک پلتفرم یکپارچه امنیتی است که اطلاعات و لاگهای مرتبط با تهدیدات را از منابع مختلف (نقاط پایانی، شبکه، ایمیل، سرورها، برنامه ها و...) جمع آوری کرده و با استفاده از تحلیل های پیشرفته و هوش مصنوعی، آنها را همبسته نموده و به یک روایت منسجم از یک حمله تبدیل میکند. برخلاف راه حل‌های نقطه ای (مثل EDR یا NDR)، XDR دیدی جامع و یکپارچه از کل محیط فناوری اطلاعات ارائه میدهد .

۵-۲. مزایای پیاده سازی XDR در سامانه سهیاس

- **تشخیص تهدیدات پیشرفته و چندمرحله‌ای:** با همبستگی داده‌ها، حملات پیچیده‌ای که از چندین نقطه عبور میکنند، قابل شناسایی هستند .
- **کاهش چشمگیر زمان تشخیص و پاسخ (MTTD/MTTR):** خودکارسازی فرایندها و هماهنگی بین لایه ها، زمان واکنش را از ساعتها به چند دقیقه کاهش میدهد .
- **کاهش هشدارهای کاذب و افزایش دقت:** الگوریتمهای هوش مصنوعی با تحلیل داده‌های متنوع، هشدارهای واقعی را با دقت بالا تشخیص میدهند .
- **ارائه دید ۳۶۰ درجه و روایت منسجم از حملات:** یک داشبورد واحد، تصویری کامل از وضعیت امنیت و زنجیره حمله ارائه میدهد .



- **بهبود کارایی تیم امنیتی:** با اولویت‌بندی هوشمند و خودکارسازی، تیم امنیتی می‌تواند بر روی مهمترین تهدیدات تمرکز کند.

۳-۵. یکپارچگی XDR با سه رکن سهیاس

معماری XDR به عنوان هسته مرکزی، سه رکن کلیدی را به هم متصل می‌کند:

- **هوشمندی: XDR + داده** های جمع آوری شده از تمام منابع، توسط موتور تحلیل و همبستگی XDR پردازش شده و با استفاده از هوش مصنوعی، به تهدیدات قابل درک و قابل پاسخ تبدیل میشوند.
- **یکپارچگی XDR: XDR + به‌عنوان** لایه یکپارچه ساز، داده های پراکنده از لایه های مختلف (سخت افزاری، نرم افزاری، داده‌ای، فرایندی و مدیریتی) را در یک بستر واحد تجمیع می‌کند.
- **امنیت XDR: XDR +** با ایجاد یک لایه امنیتی ترکیبی، پوشش دهی امنیت را از لایه فیزیکی تا اطلاعاتی یکپارچه کرده و امکان واکنش هماهنگ را فراهم می‌سازد.

۶. سه رکن کلیدی سامانه سهیاس

۱-۶. رکن اول: هوشمندی (هوش مصنوعی XDR +)

هوش مصنوعی در سامانه سهیاس به صورت بومی و با معماری Agentic AI پیاده سازی شده است، بدین معنا که خودکار، تطبیق پذیر و توانایی برنامه‌ریزی و اجرای اقدامات پیچیده را دارد. قابلیت‌های آن شامل:

حوزه	قابلیت‌های هوش مصنوعی XDR +
تشخیص چهره	تشخیص و تطابق چهره با پایگاه داده، حتی با تغییرات ظاهری، نوری و پوشش جزئی.
تشخیص اشیاء	تشخیص بیش از ۵۰ نوع شیء (انسان، خودرو، حیوان، سلاح و...) با دقت بالا.
تشخیص رفتار	تشخیص حرکات مشکوک (دویدن، تجمع، رهاسازی اشیاء، غش کردن و...).
تشخیص دود و آتش	شناسایی انواع دود و شعله در مراحل اولیه، حتی در محیط‌های باز.
پلاکخوانی	تشخیص و خواندن پلاک خودروها در شرایط مختلف نوری و آب و هوایی.
پیش بینی تهدید	تحلیل الگوهای رفتاری و پیش بینی رویدادهای امنیتی احتمالی.
تشخیص ناهنجاری (UEBA)	شناسایی انحراف از الگوهای عادی در محیط، شبکه و رفتار کاربران.



دستیار هوش مصنوعی	کمک به تحلیلگران امنیتی برای تحلیل سریعتر رویدادها و ارائه سناریوهای پاسخ .
-------------------	---

۶-۲. رکن دوم: یکپارچگی (یکپارچه سازی XDR +)

لایه یکپارچگی	شرح
سخت افزاری	اتصال و مدیریت یکپارچه دوربینها، کنترل تردد، سنسورها و تجهیزات شبکه در یک بستر واحد.
نرم افزاری	اتصال و هماهنگی VMS ، DLP ، ابزارهای شبکه، SIEM و سرورها در یک پلتفرم. XDR
داده‌ای	جمع آوری و تجمیع داده های امنیتی از تمامی منابع در یک پایگاه داده متمرکز. XDR
فرایندی	هماهنگی و یکپارچه سازی فرایندهای امنیتی فیزیکی، شبکه ای و اطلاعاتی.
مدیریتی	ارائه داشبورد واحد و یکپارچه برای مدیریت تمامی لایه ها و نمایش روایت منسجم از حملات.

۶-۳. رکن سوم: امنیت (حفاظت جامع XDR +)

حوزه امنیتی	شرح
امنیت فیزیکی	تأمین امنیت محیطی از طریق نظارت تصویری، کنترل تردد، تشخیص حریم و اشیاء.
امنیت شبکه	حفاظت از زیرساخت شبکه در برابر حملات، نفوذ و دسترسی های غیرمجاز.
امنیت اطلاعات	حفاظت از دادههای حساس سازمان در برابر نشت، سرقت و دسترسی غیرمجاز. (DLP)
امنیت ترکیبی	ایجاد یک لایه امنیتی هماهنگ و یکپارچه که از تمامی زوایا از سازمان محافظت میکند.

۷. ساختار و مؤلفه‌های تفصیلی سامانه

سامانه سهیاس از سه لایه اصلی تشکیل شده است که در یک بستر یکپارچه XDR با یکدیگر تعامل دارند:

۷-۱. لایه XDR (Extended Detection and Response)

- جمع آوری داده: (Data Ingestion) جمع‌آوری خودکار داده ها از منابع مختلف با استفاده از Apache

Kafka و Fluentd



• همبستگی و تحلیل (Correlation & Analytics): پردازش و همبستگی داده ها با Apache Spark و Elasticsearch.

• پاسخ یکپارچه (Unified Response): موتور واکنش خودکار مبتنی بر پلیبوکهای امنیتی (Security Playbook).

• دستیار هوش مصنوعی: XDR کمک به تحلیلگران برای بررسی و پاسخ سریعتر به تهدیدات.

۲-۷. لایه های منابع داده (Data Sources)

دسته منابع	منابع داده	نوع داده
امنیت فیزیکی	دوربینها (VMS)، کنترل تردد، سنسورها، فنس های مجازی	تصاویر، رویدادهای تردد، هشدارهای حریم
شبکه	فایروالها، IDS/IPS، روترها، سوئیچها	ترافیک شبکه، لاگهای اتصال، هشدارهای شبکه، NetFlow
نقاط پایانی	کامپیوترها، لپتاپ ها، سرورها، دستگاههای همراه	لاگهای سیستمی، رویدادهای امنیتی، فعالیتهای کاربر
برنامه های کاربردی	ایمیل، وبپلیکیشن ها، پایگاه دادهها	لاگهای دسترسی، رویدادهای ایمیل، تراکنشها
امنیت اطلاعات	DLP، سیستمهای رمزنگاری، مدیریت دسترسی	رویدادهای نشت داده، تلاشهای غیرمجاز

۸. قابلیت های تفصیلی کنترل امنیت نظارتی

۸-۱. تشخیص چهره و احراز هویت

سامانه سهیاس با بهره گیری از پیشرفته ترین فناوریهای تشخیص چهره، قادر است:

- چهره افراد را حتی با تغییرات اساسی در ظاهر (گذر سن، چرخش سر، تغییرات نورپردازی) با دقت بسیار بالا تشخیص دهد.
- هویت افراد را در شرایط مختلف (چرخش سر، پوشش جزئی صورت) شناسایی کند.



- لیستی از کارکنان یا افراد مجاز تعریف کرده و نسبت به افراد ناشناس حساس شود.
- چندین نفر را به طور همزمان شناسایی کند.
- اشخاص ناشناس را ثبت و هشدارهای لازم را صادر نماید.
- امکان جستجوی چهره‌های مشابه در انبوهی از تصاویر را فراهم کند.
- **همبستگی با XDR:** ارتباط رویدادهای تشخیص چهره با رویدادهای شبکه و DLP برای شناسایی تهدیدات ترکیبی .

۸-۲. تشخیص اشیاء و اهداف

سامانه سهیاس توانایی تشخیص بیش از ۵۰ نوع شیء مختلف را دارد:

دسته	اشیاء قابل تشخیص
انسان	تشخیص حضور انسان در حریم های ممنوعه
چهار پا	تشخیص ورود حیوانات به مناطق حساس
پرنده	تشخیص پرندگان و تفکیک از پهبادهای
وسایل نقلیه	تشخیص خودرو، موتورسیکلت، کامیون، اتوبوس
سلاح	تشخیص انواع سلاحهای متداول (اسلحه گرم، سرد)
پهباد	شناسایی پهبادهای و هلیشاتها در شرایط جوی مختلف

۸-۳. برپایی فنس مجازی

امکان برپایی فنسهای مجازی با چند کلیک ساده:

- تعریف فنسهای مجازی در میدان دید دوربین بدون نیاز به تجهیزات سخت افزاری.
- امکان تعریف چندین فنس برای هر دوربین.
- قابلیت تار کردن حریمهای خصوصی.
- امکان برعکس کردن فنس (نظارت بر اطراف حریم به جای خود حریم).
- قابلیت تعیین حساسیت نسبت به نوع شیء شناسایی شده.



۸-۴. تشخیص پلاک و پلاکخوانی

- تشخیص و خواندن پلاک خودروها در شرایط مختلف روشنی.
- تعریف خودروهای مجاز و شناسایی خودروهای ناشناس.
- ارائه آمار از ورود، خروج و مدت زمان توقف خودروها.
- قابلیت تعریف محدودیت حضور خودروها در نواحی خاص.

۸-۵. سایر قابلیت‌های پیشرفته

- تشخیص دود و آتش: شناسایی انواع دود و شعله، ارسال هشدار برای جلوگیری از آتشسوزی.
- تشخیص کلاه ایمنی: شناسایی کارگران بدون کلاه ایمنی در محیط‌های صنعتی.
- شمارش افراد و تشخیص تجمع: شمارش دقیق افراد و تشخیص تجمعات بیش از حد مجاز.
- تشخیص ترک پست نگهبانی: پایش حضور یا عدم حضور افراد در پست‌های نگهبانی.
- ردیابی و شمارش اشیاء: ردیابی و شمارش افراد و وسایل نقلیه، تهیه نقشه حرارتی تردد.

۹. رکن دوم: کنترل نشت داده (Data Loss Prevention - DLP)

سامانه سپاس با یکپارچه سازی سامانه کنترل نشت داده (DLP) و همبستگی آن با سایر داده‌های امنیتی از طریق معماری XDR، لایه دوم امنیت اطلاعاتی را نیز پوشش می‌دهد.

۹-۱. مؤلفه های اصلی DLP

مؤلفه	شرح
شناسایی و طبقه بندی داده های حساس	با استفاده از الگوریتم های یادگیری ماشین، داده های حساس سازمان شناسایی و طبقه بندی میشوند.
پایش کانالهای خروجی	نظارت بر ایمیل، حافظه های جانبی، پیام رسانها، چاپگرها، ترافیک شبکه و بسترهای ابری.



اجرای سیاستهای امنیتی	اعمال سیاستهای مسدودسازی، رمزگذاری، هشدار، قرنطینه و هدایت مجدد.
پایش لحظه ای و گزارشگیری	پایش رویدادها به صورت لحظ های و تولید گزارشهای تحلیلی.
همبستگی با XDR	ارتباط رویدادهای DLP با رویدادهای فیزیکی و شبکه برای شناسایی تهدیدات ترکیبی .

۹-۲. قابلیت های هوش مصنوعی در DLP

قابلیت هوش مصنوعی	کاربرد عملیاتی
طبقه بندی هوشمند داده ها	شناسایی و دسته بندی خودکار داده های حساس بدون نیاز به تعریف دستی.
تشخیص ناهنجاریهای رفتاری (UEBA)	تحلیل رفتار کاربران و شناسایی انحراف از الگوی عادی.
تشخیص دادههای مشابه و مشتق شده	تشخیص دادههایی که تغییر شکل دادهاند (مانند تغییر فرمت فایل).
پیشبینی ریسک نشت داده	تحلیل الگوهای انتقال داده و پیشبینی احتمال نشت اطلاعات.
تشخیص محتوای پنهان	شناسایی دادههای پنهان در تصاویر و فایل های چندرسانه ای (استگانوگرافی).
یادگیری تطبیقی	بهرورزسانی بویای سیاستهای امنیتی بر اساس الگوهای جدید.

۱۰. معماری فنی و زیرساخت نسل نوین

مؤلفه	مشخصات و توضیحات
معماری کلی	مبتهی بر معماری Microservices با قابلیت استقرار متمرکز یا توزیع شده (Hybrid & Multi-Cloud).
لایه XDR	جمع آوری داده از تمامی منابع با استفاده از Apache Kafka و Fluentd ؛ همبستگی با Apache Spark Streaming و Elasticsearch .

شبکه های عصبی عمیق (CNN, RNN, Transformers) برای پردازش ویدئو؛ مدل های یادگیری ماشین (Random Forest, XGBoost) برای تشخیص نشت داده و ناهنجاری ها .	موتور هوش مصنوعی (Agentic AI)
معماری ESB با استفاده از Apache Kafka و RabbitMQ؛ پشتیبانی از REST API، WebSocket و GraphQL.	لایه یکپارچه سازی
PostgreSQL (داده های ساختاریافته)، InfluxDB (داده های زمان محور)، Elasticsearch (جستجوی سریع و تحلیل)، MinIO (ذخیره سازی تصاویر و فایل ها).	پایگاه داده
استفاده از Apache Spark Streaming و Flink برای تحلیل بلادرنگ رویدادها.	زیرساخت پردازش بلادرنگ
سیستم ذخیره سازی توزیع شده (Ceph / MinIO) با رمزنگاری AES-256 و بایگانی طولانی مدت.	ذخیره سازی
رمزنگاری TLS 1.3 برای تمامی ارتباطات؛ احراز هویت دو مرحله ای (MFA) برای دسترسی به سامانه؛ رمزگذاری داده ها در حالت ذخیره. (Encryption at Rest)	امنیت ارتباطات
مدیریت تا ۵۰۰۰۰ دوربین، ۲۰۰۰۰ درب کنترل تردد و بیش از ۱ میلیون کاربر.	مقیاس پذیری
پشتیبانی از خوشه بندی، Failover خودکار و Load Balancing برای تضمین ۹۹/۹۹٪ در دسترس بودن.	دسترس پذیری بالا
استفاده از توان پردازشی GPU برای افزایش سرعت و کارایی پردازش های هوش مصنوعی.	پشتیبانی از GPU
ONVIF (پروفایل های S و G)، RTSP، Modbus، SNMP، MQTT، Syslog، NetFlow.	پروتکل های پشتیبانی شده



۱۱. مزایا، دستاوردها و بازگشت سرمایه (ROI)

۱۱-۱. مزایای عملیاتی

حوزه	مزایای مستقیم ناشی از هوش مصنوعی	مزایای مستقیم ناشی از یکپارچگی و XDR
تشخیص تهدید	دقت بالای ۹۸٪ در تشخیص تهدیدات واقعی؛ کاهش ۸۰٪ هشدارهای کاذب	تشخیص تهدیدات ترکیبی و چندمرحله‌ای که هر سامانه به تنهایی قادر به شناسایی آنها نیست .
زمان واکنش	واکنش خودکار در کمتر از ۱ ثانیه با کمک Agentic AI	کاهش زمان پاسخ دهی از ساعتها به چند دقیقه از طریق هماهنگی خودکار بین لایه ها
هزینه ها	کاهش ۶۰٪ وابستگی به نیروی انسانی؛ بهینه‌سازی مصرف منابع	صرفه جویی ۳۰-۴۰٪ در هزینه های نگهداری و یکپارچه سازی سامانه های موازی
مدیریت ریسک	پیشبینی تهدیدات قبل از وقوع با تحلیل الگوهای رفتاری	ارائه تصویر کامل از وضعیت امنیت سازمان و روایت منسجم از حملات

۱۱-۲. مزایای راهبردی

ردیف	مزیت راهبردی	شرح
۱	افزایش بلوغ امنیتی سازمان	ارتقاء از حالت واکنشی به پیشدستانه و خودکار
۲	کاهش ریسک شهرت	پیشگیری از حوادث امنیتی و نشت داده که به اعتبار سازمان آسیب میزند
۳	افزایش اعتماد ذینفعان	مشتریان، شرکا و نهادهای نظارتی به سازمانی با سامانه امنیتی پیشرفته اعتماد بیشتری دارند
۴	پایداری کسبوکار	اطمینان از تداوم عملیات سازمان در مواجهه با تهدیدات امنیتی
۵	بومی بودن و امنیت داده	اطمینان از عدم نشت اطلاعات به خارج از کشور و قابلیت بررسی کدهای منبع
۶	بازگشت سرمایه (ROI)	بازگشت سرمایه کمتر از ۱۸ ماه با در نظر گرفتن کاهش هزینهها و ریسکها



۱۲. برنامه زمانبندی تفصیلی و روش اجرا

مرحله	عنوان	شرح فعالیتهای کلیدی	مدت زمان (هفته)	خروجیها
۰	مطالعه و نیازسنجی	برگزاری جلسات با ذینفعان، شناسایی نقاط حساس و منابع داده، تحلیل شکاف، تدوین مستندات نیازمندیها و طراحی سطح بالای معماری XDR	۴	مستند نیازمندیها، نقشه نقاط حساس، تحلیل شکاف، طراحی معماری سطح بالا
۱	طراحی معماری تفصیلی	طراحی معماری فنی یکپارچه، تعیین سناریوهای همبستگی و واکنش خودکار، انتخاب الگوریتمهای هوش مصنوعی، طراحی داشبورد مدیریت یکپارچه XDR	۴	مستند معماری فنی، سناریوهای کاربری، طراحی رابط کاربری، مستند انتخاب تکنولوژی
۲	تأمین زیرساخت	تأمین سرورهای GPU و زیرساخت XDR، خرید و نصب دوربینهای هوشمند، پیادهسازی لایه جمعآوری داده، نصب و پیکربندی پایگاه دادهها	۶	تجهیزات نصبشده، زیرساخت شبکه و XDR راهاندازیشده
۳	پیاده سازی و یکپارچه سازی	نصب نرمافزار VMS، DLP و ابزارهای XDR، یکپارچه سازی تمامی منابع داده، اتصال به دایرکتوری سازمانی، پیکربندی سناریوهای همبستگی و واکنش	۶	سامانه یکپارچه XDR راهاندازیشده، اتصال به تمامی منابع
۴	آموزش و بهینه سازی هوش مصنوعی	آموزش مدلهای هوش مصنوعی با دادههای سازمان، ثبت نام اشخاص و خودروها، تنظیم دقیق الگوریتمها، برگزاری کارگاههای آموزشی برای تیم امنیتی و کاربران	۴	مدلهای هوش مصنوعی آموزششده، تیم آموزششده، مستندات کامل



۵	تست، استقرار و بهره برداری	اجرای تستهای یکپارچگی و پیکربندی (UAT)، بهینه سازی نهایی، استقرار رسمی سامانه و انتقال به بهره برداری، آغاز دوره پشتیبانی و نگهداری	۳	سامانه عملیاتی، گزارش تست ها، انعقاد قرارداد پشتیبانی
۶	پایش و بهبود مستمر	پایش عملکرد هوش مصنوعی و بهروزرسانی مدلها، پایش عملکرد لایه XDR و بهینه سازی همبستگی ها، ارائه پشتیبانی فنی سطح ۱، ۲ و ۳، بهروزرسانی های دوره های	مستمر	گزارشهای عملکرد ماهانه، بهروزرسانیهای نرمافزاری

۱۳. برآورد بودجه و منابع انسانی

۱۳-۱. برآورد هزینهها (ارقام تقریبی)

ردیف	اقلام هزینه	برآورد هزینه (تومان/دلار)	توضیحات
۱	تجهیزات سختافزاری		سرورهای GPU، دوربینهای IP، تجهیزات شبکه، سرورهای ذخیرهسازی و پردازش XDR
۲	مجوزهای نرمافزاری		مجوز VMS، DLP، پایگاه داده، سیستمعاملها، ابزارهای XDR و پردازش بلادرنگ
۳	توسعه و پیادهسازی		هزینه تیم توسعه، یکپارچهسازی، پیکربندی و راهاندازی لایه XDR
۴	آموزش و انتقال دانش		برگزاری کارگاهها، تهیه مستندات، آموزش تیم امنیتی و کاربران
۵	پشتیبانی و نگهداری (سال اول)		پشتیبانی فنی، بهروزرسانیها، نگهداری زیرساخت XDR
۶	پشتیبانی و نگهداری (سالهای بعد)		هزینه تمدید مجوزها و پشتیبانی

		مجموع هزینه پروژه (فازهای ۰ تا ۵)	
		مجموع هزینه سالانه (فاز ۶)	

۲-۱۳. منابع انسانی مورد نیاز

نقش	تعداد	شرح مسئولیت
مدیر پروژه	۱	مدیریت کلی پروژه، هماهنگی بین تیمها، ارتباط با کارفرما
معمار سیستم (XDR)	۱	طراحی معماری XDR، یکپارچهسازی، انتخاب فناوریها
مهندس هوش مصنوعی	۲	توسعه و آموزش مدل‌های یادگیری ماشین، بهینه سازی الگوریتمها
مهندس داده (XDR)	۱	پیداهسازی لایه جمع‌آوری و همبستگی دادهها، مدیریت پایگاه داده
توسعه دهنده بک‌اند	۲	توسعه سرویسهای سمت سرور، یکپارچهسازی با سامانههای ثالث
توسعه دهنده فرانت‌اند	۱	پیداهسازی داشبورد مدیریت یکپارچه و رابط کاربری XDR
کارشناس شبکه و زیرساخت	۱	نصب و پیکربندی تجهیزات شبکه، دوربینها و سرورها
کارشناس امنیت	۱	تعیین سیاستهای امنیتی، پیکربندی DLP و سناریوهای امنیتی
کارشناس دوربین و نظارت تصویری	۱	نصب و تنظیم دوربینها، تنظیمات زاویه و پارامترهای تصویری
تکنسین پشتیبانی	۲	پشتیبانی فنی، عیبیابی و نگهداری روزانه
مربی و مدرس	۱	آموزش کاربران و تیم امنیتی، تهیه مستندات آموزشی
مجموع	۱۴	

۱۴. جمع‌بندی و پیشنهاد راهبردی

سامانه **سیاس** با تکیه بر **معماری پیشرفته XDR** و سه رکن **کلیدی امنیت، یکپارچگی و هوشمندی**، تحولی اساسی در مدیریت امنیت سازمانی ایجاد میکند:



✓ **هوشمندی** به سامانه توانایی تشخیص دقیق (با دقت بالای ۹۸٪)، پیشبینی هوشمند و واکنش خودکار (کمتر از ۱ ثانیه) را میدهد و با بهره‌گیری از **Agentic AI**، وابستگی به تصمیمات انسانی را به حداقل می‌رساند.

✓ **یکپارچگی** موجب حذف سیلوهای اطلاعاتی، ایجاد دید ۳۶۰ درجه و هماهنگی بینظیر بین لایه‌های امنیتی فیزیکی، شبکه‌ای و اطلاعاتی میشود و یک مرکز عملیات امنیت یکپارچه (SOC) را ایجاد میکند.

✓ **معماری XDR** با جمع‌آوری داده از تمامی منابع، همبستگی هوشمند و ارائه روایت منسجم از حملات، امکان شناسایی تهدیدات ترکیبی و چندمرحله‌ای را فراهم میکند که توسط سامانه‌های سنتی قابل تشخیص نیستند.

✓ **امنیت** در سه لایه فیزیکی، شبکه‌ای و اطلاعاتی به صورت همزمان و با رویکردی ترکیبی تأمین میشود.

امتیازات ویژه سامانه سهیاس:

#	امتیاز ویژه	شرح
۱	بومی و دانش بنیان	طراحی کاملاً بومی با قابلیت شخصی سازی و بررسی کد منبع
۲	معماری XDR پیشرفته	جمع آوری، همبستگی و تحلیل داده از تمامی منابع امنیتی
۳	معماری انعطافپذیر	پشتیبانی از معماری متمرکز، توزیعشده و Hybrid Cloud
۴	پشتیبانی از انواع دوربینها	پشتیبانی از پروتکل ONVIF و برندهای مختلف
۵	پشتیبانی از GPU	افزایش سرعت و کارایی با استفاده از توان پردازشی GPU
۶	رابط کاربری فارسی	طراحی کاربرپسند و کاملاً فارسی
۷	سازگاری با Windows و Linux	قابلیت اجرا در محیطهای نرم افزاری متنوع
۸	دسترس پذیری بالا	پشتیبانی از خوشه‌بندی و Failover برای تضمین پایداری

پیشنهاد نهایی

با توجه به اهمیت راهبردی امنیت سازمانی، پیچیدگی تهدیدات امروزی و نیاز به رویکردی یکپارچه و هوشمند، استقرار سامانه **سهیاس** با معماری **XDR** به عنوان یک پروژه **اولویت‌داد و سرمایه گذاری راهبردی** به سازمان محترم پیشنهاد میگردد. این سامانه ضمن



تأمین امنیت فیزیکی، شبکه‌های و اطلاعاتی، زمینه‌ساز تحول دیجیتال در حوزه مدیریت امنیت سازمان و ارتقاء سطح بلوغ امنیتی به بالاترین درجه خواهد بود.

امید است با تأیید و حمایت جنابعالی، نسبت به آغاز فاز مطالعاتی و نیازسنجی پروژه اقدام گردد.

۱۵. ضمائم (پیشنهادی)

- **ضمیمه الف:** مستند نیازمندیهای سطح بالا (فهرست کامل نیازمندیهای عملکردی و غیرعملکردی)
- **ضمیمه ب:** نقشه نقاط حساس سازمان (شناسایی اولیه نقاط بحرانی برای استقرار تجهیزات)
- **ضمیمه ج:** تحلیل شکاف (مقایسه وضعیت موجود با مطلوب)
- **ضمیمه د:** سناریوهای کاربری و همبستگی XDR (شرح دقیق سناریوهای امنیتی و نحوه همبستگی داده‌ها)
- **ضمیمه ه:** مشخصات فنی تجهیزات (دیتاشیت دوربینها، سرورها، تجهیزات شبکه و نرمافزارها)
- **ضمیمه و:** قرارداد پشتیبانی (پیش نویس تعهدات پشتیبانی و سطح خدمات SLA)
- **ضمیمه ز:** معماری تفصیلی XDR (مستندات معماری لایه های جمع آوری، همبستگی و پاسخ)