

نشریه تخصصی فناوری اطلاعات و امنیت

امنیت در عصر یکپارچگی

چرا نگاه جزیره‌ای دیگر کافی نیست؟

از فروش تجهیزات تا ارائه راهکار

گفت‌وگو با مدیرعامل
آریو مروارید ایمن

هارد استوک در پروژه‌های نظارت تصویری

صرفه جویی یا انتقال ریسک؟

هوش مصنوعی و آینده حفاظت الکترونیک

از تشخیص رویداد
تا تصمیم‌سازیSECURITY
TECHNOLOGY
RESILIENCE
FOR A
SMARTER
TOMORROWزیرساخت امروز
آرامش فرداSECURE
CONNECTED
SUSTAINABLE

امنیت



زیرساخت



فناوری

ساینا

نشریه

نشریه تخصصی فناوری اطلاعات و امنیت

درباره نشریه ساینا

ساینا روایت یک نگاه مهندسی و سیستماتیک به فناوری اطلاعات، امنیت، زیرساخت و ایمنی در پروژه‌های صنعتی و سازمانی است؛ نگاهی که بر این باور است فناوری زمانی ارزش آفرین خواهد بود که به صورت پیکارچه طراحی شود، مبتنی بر تحلیل مهندسی باشد و در خدمت ایمنی، پایداری و تصمیم‌سازی آگاهانه قرار گیرد.

شرکت شبکه گستر ساینا، به عنوان طراح، مشاور و ناظر پروژه‌های فناوری، نظارت تصویری و زیرساخت، تلاش کرده است با گردهم‌آوردن مجموعه‌ای از شرکت‌های تخصصی و هم‌راستا، تصویری واقع‌بینانه از الزامات فنی، امنیتی و اجرایی پروژه‌های حیاتی ارائه دهد؛ تصویری که در آن، امنیت و پایداری حاصل طراحی صحیح، تصمیم‌سازی آگاهانه و نظارت حرفه‌ای است، نه انتخاب‌های مقطعی و واکنشی.

این ویژه‌نامه با همین نگاه منتشر شده است؛ دعوتی به بازنگری در شیوه مواجهه با فناوری و پروژه‌های حساس، نگاهی که به جای راه‌حل‌های جزیره‌ای، بر معماری پیکارچه، استانداردمحور و آینده‌نگر تکیه دارد و فناوری را نه یک هدف مستقل، بلکه ابزاری برای ارتقای کیفیت تصمیم‌گیری، کاهش ریسک و تضمین موفقیت پروژه‌ها می‌داند.

دانش،
تجربه،
امنیت پایدار...

فناوری
امنیت
زیرساخت
آینده‌ای مطمئن‌تر

شناسنامه نشریه

نام نشریه	نشریه ساینا
شماره	۹
تاریخ انتشار	مهرماه ۱۴۰۵
دوره انتشار	ماهنامه
صاحب امتیاز	شرکت شبکه گستر ساینا
مدیرمسئول	مهندس اسماعیل اکبری
وبسایت	www.SainaMag.ir
تلفن	۰۲۶۳۲۶۲۰۰۰۰
همراه (ارسال اخبار، مقاله و رپورتاژ)	۰۹۲۰۴۶۰۶۹۹۱



امنیت پایدار



زیرساخت مطمئن



فناوری هوشمند



تصمیم آگاهانه

امنیت در عصر یکپارچگی؛ چرا نگاه جزیره‌ای دیگر کافی نیست؟

امنیت یکپارچه؛ یعنی دیدن تصویر بزرگ‌تر

در یک معماری یکپارچه، حفاظت فیزیکی، حفاظت الکترونیکی، شبکه، نرم‌افزار، نیروی انسانی و فرآیندهای سازمانی، اجزای جدا از هم نیستند؛ بلکه بخش‌های مختلف یک زنجیره امنیتی هستند. ضعف در هر یک از این حلقه‌ها می‌تواند عملکرد کل مجموعه را تحت تأثیر قرار دهد.

برای مثال، پیاده‌سازی دوربین مداربسته نیز اگر در محل نامناسب نصب شود، طراحی شبکه درستی نداشته باشد، ذخیره‌سازی آن متناسب با نیاز پروژه انتخاب نشود یا تصاویر آن به درستی مدیریت و تحلیل نگردند، نه‌نهایتاً ارتقای امنیت کمکی نمی‌کند، بلکه می‌تواند منابع سازمان را هدر دهد.

نقش کاربران در امنیت پایدار

یکی از چالش‌های مهم صنعت، توجه کافی به نقش کاربران و نیروی انسانی است. در بسیاری از پروژه‌ها مشاهده می‌شود که حتی بهترین تجهیزات نیز به دلیل نبود آموزش، عدم آگاهی یا نبود فرآیندهای مشخص، کارایی لازم را ندارند. امنیت پایدار زمانی شکل می‌گیرد که فناوری، فرایند و انسان به صورت هماهنگ در کنار هم قرار گیرند.

مسیر آینده، مسیر تجهیزات منفرد نیست؛

مسیر اتصال انسان، فناوری و فرایند برای
برای ساختن یک راهکار امنیتی قابل اعتماد است.

مهندس اسماعیل اکبری

مدیرعامل شرکت شبکه گستر ساینما
مدیرمسئول نشریه ساینما

امنیت، فراتر از مجموعه‌ای از تجهیزات مستقل

سال‌ها نگاه به حوزه حفاظت و امنیت، عمدتاً بر انتخاب و نصب تجهیزات متمرکز بود؛ دوربین، سامانه کنترل تردد، دزدگیر، اعلام سرقت و... هر کدام به عنوان یک راهکار مستقل تعریف و اجرا می‌شدند. اما امروز با رشد فناوری و پیچیده‌تر شدن تهدیدها، این رویکرد دیگر پاسخگوی نیاز سازمان‌ها و جوامع نیست.

امروز یک پروژه امنیتی موفق، تنها با خرید تجهیزات مناسب شکل نمی‌گیرد. آنچه اهمیت دارد، شناخت صحیح مسئله، ارزیابی ریسک، طراحی متناسب، انتخاب فناوری مناسب، اجرای اصولی، یکپارچه‌سازی و در نهایت ایجاد ارتباط میان اجزای مختلف سامانه است.

از محصول به راهکار

ورود هوش مصنوعی، تحلیل ویدئو، سامانه‌های مدیریت تصویر کنترل تردد هوشمند و تجهیزات تحت شبکه، سرعت تغییرات در این صنعت را به شکل چشمگیری افزایش داده است. در چنین شرایطی، نگاه صرف به «محصول» کافی نیست و باید به سمت ارائه «راهکار» حرکت کنیم. راهکاری که در معماری صحیح، پاسخگوی نیاز واقعی مشتری باشد و برای حل یک مسئله مشخص طراحی شود.

آینده‌ای که با همکاری ساخته می‌شود

صنعت حفاظت و امنیت در ایران، طویقت بسیار بالایی برای رشد و توسعه دارد. تحقق این آینده، نیازمند همکاری همه بازیگران این صنعت است؛ از تولیدکنندگان، وارکنندگان و شرکت‌های فعال، تا اتحادیه‌ها، مراکز آموزشی و نهادهای نظارتی.

در نشریه ساینما، تلاش می‌کنیم با نگاهی جامع، مفهوم امنیت در عصر یکپارچگی را از زوایای مختلف بررسی کنیم و برای گفت‌وگو، تبادل تجربه و هم‌افزایی میان فعالان این مسیر فراهم آوریم.

“

امنیت یکپارچه
تنها با اتصال
فناوری‌ها محقق
نمی‌شود؛
بلکه نیازمند
دید کل‌نگر،
مدیریت ریسک
و همکاری همه
بازیگران صنعت است.

”



انسان
محوریت



فرایند
هوشمند



فناوری
پیشرفته



امنیت
یکپارچه



امنیت یکپارچه؛ وقتی همه اجزا باید با هم کار کنند

از تجهیزات مستقل تا معماری یکپارچه؛
نگاهی به ارتباط حفاظت فیزیکی، حفاظت الکترونیک،
شبکه، نرم افزار و نیروی انسانی

امنیت یکپارچه
فراتر از تجهیزات،
یک نگرش است.

در دنیای امروز، تهدیدها پیچیده تر، هوشمندتر و سازمان یافته تر شده اند. دیگر نمی توان با نکیه بر یک دوربین، یک سیستم کنترل تردد یا یک نگهبان فیزیکی، امنیت یک مجموعه را تضمین کرد. امنیت واقعی زمانی محقق می شود که تمام اجزا، - از تجهیزات فیزیکی تا سامانه های الکترونیک، شبکه، نرم افزار و نیروی انسانی در قالب یک معماری منسجم و هدفمند طراحی و مدیریت شوند.

اجزای اصلی امنیت یکپارچه

حفاظت فیزیکی، حفاظت الکترونیک، شبکه و ارتباطات، نرم افزار و مدیریت مرکزی و نیروی انسانی، هر کدام نقش مهمی در ایجاد یک ساختار امنیتی کارآمد دارند.

مزایای رویکرد یکپارچه

افزایش سطح امنیت، کاهش هزینه های عملیاتی، مدیریت متمرکز، پاسخ سریع تر به تهدیدها و امکان تحلیل و گزارش گیری جامع، از مهم ترین مزایای امنیت یکپارچه هستند.

از طراحی تا بهره برداری

موفقیت در پیاده سازی امنیت یکپارچه، نیازمند طراحی معماری مناسب، انتخاب تجهیزات سازگار، اجرای استاندارد، آموزش مستمر و نگهداری حرفه ای است.

امنیت یک پروژه نیست؛

یک مسیر بلندمدت است که با نگاه یکپارچه
به فناوری، انسان و فرآیند، به نتیجه می رسد.



امنیت، حاصل
هم افزایی انسان،
فناوری و فرآیند
است؛ نه مجموعه ای
از تجهیزات جداگانه.

محافظةت هوشمند
از دارایی ها

افزایش بهره وری
سازمان

تصمیم گیری دقیق
و مبتنی بر داده

کاهش هزینه ها
در بلندمدت

پایداری و
تاب آوری بیشتر

داده ها
دید بهتری می دهند؛
یکپارچگی
تصمیم های بهتری.



حفاظت فیزیکی؛ اولین لایه دفاعی در معماری امنیت

از موانع و کنترل دسترسی تا نظارت و واکنش؛
چرا امنیت واقعی به چند لایه مکمل نیاز دارد؟

در دنیای امروز، حفاظت فیزیکی همچنان یکی از ارکان اصلی امنیت سازمان‌ها، زیرساخت‌ها و دارایی‌های حساس است. هرچند فناوری‌های نوین مانند دوربین‌های مداربسته، کنترل دسترسی و سیستم‌های هوشمند نقش بسزایی در افزایش سطح امنیت دارند، اما بدون یک زیرساخت فیزیکی مناسب و طراحی اصولی محیط، این فناوری‌ها به تنهایی نمی‌توانند امنیت پایدار ایجاد کنند.

لایه‌های حفاظت فیزیکی



امنیت واقعی
از ترکیب هوشمندانه
محیط، تجهیزات
و انسان شکل
می‌گیرد.

SECURE
ENVIRONMENTS
STRONGER
ORGANIZATIONS

چرا حفاظت فیزیکی اهمیت دارد؟

- ✓ کاهش احتمال وقوع تهدیدات
- ✓ ایجاد بازدارندگی مؤثر
- ✓ حفاظت از دارایی‌های فیزیکی
- ✓ کنترل دسترسی افراد و وسایل نقلیه
- ✓ ایجاد بستر مناسب برای عملکرد تجهیزات الکترونیکی
- ✓ افزایش آمادگی در شرایط بحران



حفاظت فیزیکی
سرمايه‌گذاری در
آرامش و تداوم کسب‌وکار است.

اجزای اصلی حفاظت فیزیکی

- محوطه و پیرامون**
حصارکشی، روشنایی، محوطه‌سازی و دید مناسب
- ورودی‌ها و خروجی‌ها**
گیت‌ها، درب‌های امن و مسیرهای کنترل شده
- کنترل دسترسی**
مدیریت تردد افراد، وسایل نقلیه و محموله‌ها
- نیروی انسانی**
نگهبانی، گشت‌های منظم و رویه‌های عملیاتی
- پشتیبانی و نگهداری**
بازبینی‌های دوره‌ای و به‌روزرسانی زیرساخت‌ها

نکته کلیدی:

یک محیط امن، نتیجه طراحی دقیق، اجرای استاندارد و مدیریت مستمر است.



حفاظت الکترونیک؛ وقتی تجهیزات باید یک مسئله را حل کنند

از دوربین و کنترل تردد تا اعلام سرقت و سنجش محیطی؛
نقش تجهیزات الکترونیکی در معماری امنیت پیکارچه

حفاظت الکترونیک مجموعه‌ای از سیستم‌ها و تجهیزات هوشمند است که با استفاده از فناوری‌های نوین، امکان پایش، کنترل، تشخیص و واکنش سریع را فراهم می‌کند. اما ارزش واقعی این تجهیزات زمانی مشخص می‌شود که در یک، معماری پیکارچه، با طراحی صحیح و متناسب با نیاز هر سازمان به کار گرفته شوند.

فناوری،
وقتی معنا دارد
که امنیت ایجاد کند.



نظارت تصویری
بیش از یک دوربین؛
تحلیل، تشخیص
و تصمیم‌سازی



کنترل تردد
مدیریت هوشمند ورود
و خروج افراد و وسایل
نقلیه



**اعلام سرقت
و تشخیص نفوذ**
هشدار سریع
برای واکنش به موقع



**سنسورها
و تجهیزات محیطی**
پایش شرایط محیطی
برای امنیت پایدار



شبکه و نرم‌افزار
اتصال، پیکارچه‌سازی
و مدیریت مرکزی



داده، دید بهتر می‌دهد.
پیکارچی، امنیت بیشتری.



طراحی
متناسب با نیاز



نصب و راه‌اندازی
استاندارد



تنظیمات
و بهینه‌سازی



پشتیبانی
و خدمات پس از فروش

“

مگاپیکسل
همه چیز نیست؛
مهم‌تر از آن،
این است
که تجهیزات
چه مسئله‌ای را
برای شما
حل می‌کنند.

”

**مگاپیکسل مهم است،
اما کافی نیست!**

در انتخاب دوربین و سایر تجهیزات، فقط به اعداد و مشخصات فنی نگاه نکنید. کیفیت تصویر در شرایط نوری، مختلف، نوع لنز، قابلیت‌های تحلیلی، سازگاری با نرم‌افزار مدیریت و خدمات پس از فروش، همگی در کارایی واقعی یک سیستم تأثیرگذارند.



**تفاوت فروش تجهیز
با طراحی راهکار**

فروش تجهیز، تنها بخشی از کار است. طراحی یک راهکار امنیتی، شامل نیازسنجی، انتخاب تجهیزات مناسب، پیکارچه‌سازی، سیستم‌ها، برنامه‌ریزی اجرا و پشتیبانی مداوم است. یک راهکار درست، هزینه‌های آینده را کاهش می‌دهد و امنیت را پایدار می‌کند.

**جایگاه حفاظت الکترونیک
در امنیت پیکارچه**

حفاظت الکترونیک در کنار حفاظت فیزیکی و با انکابه زیرساخت‌های شبکه، نیروی انسانی و فرآیندهای مدیریتی، یک لایه کلیدی در معماری امنیت پیکارچه است. این لایه، اطلاعات دقیق و لحظه‌ای از محیط را فراهم می‌کند و زمینه‌ساز تصمیم‌گیری سریع و موثر می‌شود.

امنیت هوشمند
برای فردایی مطمئن‌تر



هارد استوک

در پروژه‌های نظارت تصویری؛ صرفه جویی یا انتقال ریسک؟

کامران محمدزاده

کارشناس ارشد سیستم‌های ذخیره‌سازی
و زیرساخت نظارت تصویری

در پروژه‌های نظارت تصویری، هارد دیسک قلب ذخیره‌سازی و یکی از مهمترین اجزای سیستم است. استفاده از هارد استوک، به دلیل قیمت پایین‌تر، در برخی پروژه‌ها مورد توجه قرار می‌گیرد؛ اما آیا این انتخاب واقعاً مقرون به صرفه است یا می‌تواند ریسک‌های جدی به همراه داشته باشد؟ در این مقاله به بررسی این موضوع می‌پردازیم.

تصاویر
شاید تکرار شوند،
اما فرصت بازیابی
همیشه تکرار
نمی‌شود.



هارد استوک چیست؟



هارد استوک، هارد دیسکی است که قبلاً در سیستم‌های دیگری (مثلاً دیتاسترها یا تجهیزات سازمانی) استفاده شده و مجدداً وارد بازار می‌شود. این هاردها معمولاً کارکرد مشخصی داشته و ساعت روشن بودن (Power On Hours) آنها قابل بررسی است.

چرا وارد پروژه‌ها می‌شود؟

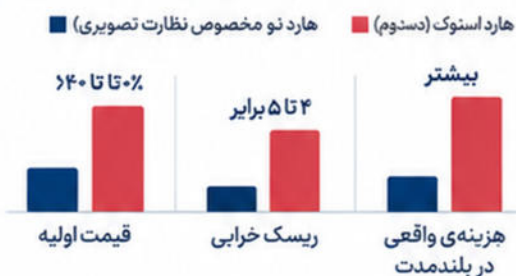


- قیمت پایین‌تر نسبت به هارد نو
- دسترسی سریع در بازار
- ظاهر سالم و تست اولیه بدون خطا
- جذابیت اقتصادی در پروژه‌های با بودجه محدود

در نظارت تصویری،

هزینه واقعی زمانی مشخص می‌شود
که به تصاویر نیاز داشته باشید
و در دسترس نباشند.

مقایسه هارد نو و استوک



مسیر ذخیره‌سازی در یک پروژه نظارتی



ریسک‌های استفاده از هارد استوک



- ✓ احتمال بالاتر خرابی و از دست رفتن اطلاعات
- ✓ کارکرد نامشخص و ساعات روشن بودن بالا
- ✓ عدم تناسب با Workload سنگین ضبط ۱۴/۲
- ✓ تأثیر منفی بر عملکرد VMS و NVR
- ✓ افزایش هزینه‌های نگهداری و تعویض
- ✓ ریسک عدم گارانتی معتبر
- ✓ از دست رفتن شواهد و پیامدهای حقوقی

قبل از خرید هارد، این ۶ مورد را بررسی کنید

۱. نوع هارد (مخصوص نظارت تصویری - Surveillance)
۲. کارفیت مورد نیاز و مدت نگهداری (Retention)
۳. میزان Workload و تطابق با شرایط پروژه
۴. سلامت هارد (بررسی SMART و ساعات کارکرد)
۵. گارانتی معتبر و اصالت کالا
۶. شرایط محیطی (دما، تهویه و محل نصب)

نکات فنی مهم



- ✓ استفاده از هاردهای سری Surveillance / Enterprise
- ✓ توجه به میزان Workload (معمولاً ۱۸۰ تا ۵۵۰ ترابایت در سال)
- ✓ استفاده از RAID و پیکاب در پروژه‌های حساس
- ✓ بایش سلامت هارد و هشداردهی هوشمند
- ✓ توجه به دمای محیط و تهویه مناسب رک

جمع‌بندی



هارد استوک ممکن است در نگاه اول باعث صرفه‌جویی در هزینه‌ها شود، اما در پروژه‌های نظارت تصویری می‌تواند ریسک‌های جدی و هزینه‌های پنهان زیادی به همراه داشته باشد. انتخاب صحیح هارد، بخشی از طراحی حرفه‌ای و تضمین‌کننده پایداری سیستم است.

در امنیت تصویری،
هیچ چیز جایگزین
اطلاعات از دست رفته نمی‌شود.

هارد مناسب پروژه را چگونه انتخاب کنیم؟

از تعداد دوربین تا مدت نگهداری تصاویر؛ پارامترهایی که ظرفیت و نوع ذخیره سازی را تعیین می کنند

انتخاب صحیح ذخیره سازی در پروژه های نظارت تصویری، تأثیر مستقیم بر پایداری سیستم، دسترسی به تصاویر و هزینه های بلندمدت دارد. در این صفحه، مهم ترین پارامترهای مؤثر در محاسبه ظرفیت و انتخاب نوع هارد به صورت کاربردی بررسی می شوند.

ذخیره سازی مطمئن، پایه تداوم امنیت است.

مسیر محاسبه ظرفیت ذخیره سازی



تفاوت انواع هارد در کاربردهای نظارتی

ویژگی	هارد دسکتاپ (Consumer)	هارد نظارتی (Surveillance)	هارد سازمانی (Enterprise)
میزان کارکرد (Workload)	کم	تا ۱۸۰ ترابایت در سال	بالای ۵۵۰ ترابایت در سال
مناسب برای	کاربری شخصی	سیستم های نظارت تصویری	دیتاستر و پروژه های بزرگ
پایداری و دوام	متوسط	بالا	بسیار بالا
مقاومت در کار مداوم ۲۴/۷	محدود	مناسب	بسیار مناسب
قیمت	پایین تر	متوسط	بالا

پارامترهای کلیدی در انتخاب ذخیره سازی

تعداد دوربین ها و رزولوشن (2MP / 4MP / 8MP)	نرخ فریم و بیت ریت (FPS / Kbps)	کدک فشرده سازی H.264 / H.265	نوع ضبط Motion/Event دانم
مدت نگهداری (Retention)	ظرفیت واقعی و ضریب رشد پروژه	Workload هارد	استفاده از RAID در پروژه های حساس

مثال محاسباتی یک پروژه واقعی



پروژه: مجتمع اداری

تعداد دوربین: ۶۴ عدد
رزولوشن: ۴ مگاپیکسل
نرخ فریم: ۲۵ فریم بر ثانیه
بیت ریت متوسط هر دوربین: ۴ Mbps
مدت نگهداری: ۳۰ روز

- حجم روزانه هر دوربین: ۴ Mbps ≈ ۴۳ GB/Day
- حجم کل روزانه: ۶۴ × ۴۳ ≈ ۲۷۵۲ GB ≈ ۲.۷ TB
- حجم مورد نیاز برای ۳۰ روز: ۲.۷ × ۳۰ ≈ ۸۱ TB
- با در نظر گرفتن ۲۰٪ ظرفیت اضافه: ۹۶ TB حدود

پیشنهاد: استفاده از ۴ عدد هارد ۲۴ ترابایتی در RAID 5

چک لیست نهایی انتخاب هارد

- ✓ برآورد دقیق تعداد دوربین و رزولوشن
- ✓ تعیین نرخ فریم و بیت ریت واقعی
- ✓ محاسبه حجم مورد نیاز بر اساس مدت نگهداری
- ✓ در نظر گرفتن حداقل ۲۰٪ ظرفیت اضافه
- ✓ انتخاب هارد مناسب با Workload مورد نیاز
- ✓ استفاده از RAID در پروژه های حساس
- ✓ بررسی گارانتی و اصالت کالا
- ✓ توجه به شرایط محیطی (دما و تهویه)

نکات مهم

- ✓ همیشه از هاردهای مخصوص نظارت تصویری استفاده کنید.
- ✓ در پروژه های حیاتی از RAID استفاده کنید.
- ✓ ظرفیت را بر اساس بدترین شرایط (بیشترین بیت ریت) محاسبه کنید.
- ✓ به رشد آینده پروژه توجه کنید.
- ✓ صرفه جویی در ظرفیت ذخیره سازی می تواند منجر به از دست رفتن تصاویر مهم شود.

داده ها دارایی سازمان شما هستند. در انتخاب ذخیره سازی هوشمندانه تصمیم بگیرید.

انتخاب درست ذخیره سازی، فقط یک تصمیم فنی نیست؛ یک سرمایه گذاری بلندمدت در امنیت و آرامش است.



از فروش تجهیزات تا ارائه راهکار

صنعت حفاظت الکترونیک در مسیر یکپارچگی

گفت‌وگو با مهندس محمدعلی احمدی
مدیرعامل شرکت آریو مروارید ایمن

در این شماره از نشریه ساینا، با مهندس محمدعلی احمدی، مدیرعامل شرکت آریو مروارید ایمن، درباره مسیر توسعه صنعت حفاظت الکترونیک، نقش فناوری‌های نوین در ارتقای امنیت، چالش‌های بازار و ضرورت حرکت از فروش تجهیزات به سمت ارائه راهکارهای یکپارچه گفت‌وگو کرده‌ایم.

مهندس محمدعلی احمدی
مدیرعامل شرکت آریو مروارید ایمن

”امنیت، تنها یک محصول نیست؛
یک تجربه، یک اعتماد و
یک تعهد بلندمدت است.“

۳ مهندسين چالش‌های اصلی فعالان این صنعت در حال حاضر چیست؟

یکی از چالش‌های اصلی، رقابت قیمتی غیرمنطقی و حضور شرکت‌های غیرمتخصص در بازار است که باعث کاهش کیفیت پروژه‌ها و بی‌اعتمادی کارفرمایان می‌شود. چالش، دیگر، نبود استانداردهای الزام‌آور و ضعف در فرهنگ‌سازی نسبت به اهمیت طراحی و اجرای اصولی است. همچنین کمبود نیروی انسانی متخصص و به‌روز، از دیگر مسائل مهم صنعت ماست. برای عبور از این چالش‌ها، نیازمند همکاری بیشتر میان فعالان حرفه‌ای، حمایت نهادهای صنفی و ارتقای سطح دانش و آگاهی در بازار هستیم.

۲ به نظر شما مهم‌ترین تغییر در صنعت حفاظت الکترونیک در سال‌های اخیر چه بوده است؟

به باور من، مهم‌ترین تغییر، حرکت از فروش صرف تجهیزات به سمت ارائه راهکارهای یکپارچه است. امروز دیگر مشتری‌ای به دنبال خرید چند دوربین با یک دستگاه NVR نیستند؛ بلکه انتظار دارند یک سیستم کامل شامل طراحی مبتنی بر نیاز، انتخاب صحیح تجهیزات، نرم‌افزارهای مدیریتی، تحلیل هوشمند تصویر و پشتیبانی بلندمدت دریافت کنند. همچنین ورود فناوری‌هایی مانند هوش مصنوعی و تحلیل ویدئو، تعریف جدیدی از نقش دوربین‌ها در پروژه‌ها ایجاد کرده و آن‌ها را به یک سنسور هوشمند در زیرساخت‌های امنیتی تبدیل کرده است.

۱ لطفاً ابتدا درباره شرکت آریو مروارید ایمن و حوزه فعالیت‌های آن توضیح دهید.

شرکت آریو مروارید ایمن با هدف ارائه راهکارهای تخصصی در حوزه سیستم‌های حفاظت الکترونیک، نظارت تصویری و فناوری‌های امنیتی فعالیت می‌کند. تمرکز ما بر ارائه راهکارهای کامل بر اساس نیاز واقعی مشتریان است؛ از مشاوره و طراحی تا تأمین تجهیزات، اجرا و خدمات پس از فروش. تلاش ما همیشه بر این بوده که با تکیه بر دانش فنی، تجربه اجرایی و همکاری با برندهای معتبر بین‌المللی، راهکارهایی قابل اعتماد و پایدار برای پروژه‌های مختلف ارائه دهیم.

راهکارهای هوشمند
برای دنیایی امن‌تر



BUILDING
A SAFER
TOMORROW

”با تکیه بر دانش، تجربه و فناوری
به سوی آینده‌ای امن‌تر حرکت می‌کنیم.“

آریو مروارید ایمن
ارائه‌دهنده راهکارهای جامع امنیت و نظارت الکترونیک

”

آینده این صنعت در
گرو ترکیب دانش،
فناوری و انسان‌های
متخصص است.

مهندس محمدعلی احمدی
مدیرعامل شرکت آریو مروارید ایمن



از تجهیزات تا راهکار پایدار

ادامه گفت‌وگو با مهندس محمدعلی احمدی
مدیرعامل شرکت آریو مروارید ایمن

در بخش نخست این گفت‌وگو، درباره مسیر توسعه شرکت آریو مروارید ایمن، تغییر نگاه بازار و ضرورت ارائه راهکارهای یکپارچه صحبت کردیم. در ادامه، به موضوعاتی مانند نقش هوش مصنوعی، اهمیت خدمات پس از فروش، چالش‌های بازار و چشم‌انداز آینده صنعت حفاظت الکترونیک می‌پردازیم.

۴ نقش هوش مصنوعی را در آینده صنعت حفاظت الکترونیک چگونه می‌بینید؟

هوش مصنوعی و تحلیل تصویر، دوربین مداربسته را از یک ابزار صرفاً نظارتی به یک سنسور هوشمند تبدیل کرده است. امروز می‌توانیم علاوه بر ضبط و مشاهده تصویر، از داده‌های ویدئویی برای تحلیل رفتار، تشخیص رویدادها، مدیریت ترافیک و افزایش بهره‌وری استفاده کنیم. این فناوری اگر به‌درستی در پروژه‌ها پیاده‌سازی شود، ارزش افزوده واقعی برای کارفرما ایجاد خواهد کرد.

۵ خدمات پس از فروش چه جایگاهی در موفقیت یک پروژه دارد؟

خدمات پس از فروش، بخش جدایی‌ناپذیر یک پروژه موفق است. بسیاری از کارفرمایان پس از اجرا با مشکلات نگهداری و پشتیبانی مواجه می‌شوند. ما در آریو مروارید ایمن همواره تلاش کرده‌ایم با ارائه قراردادهای پشتیبانی، تأمین قطعات و پاسخ‌گویی سریع، اعتماد مشتریان را در بلندمدت حفظ کنیم. به باور من، یک پروژه زمانی واقعاً موفق است که سال‌ها پس از اجرا نیز، سیستم پایدار و قابل اتکا باقی بماند.

۶ به نظر شما مهم‌ترین چالش فعالی فعالان این صنعت چیست؟

یکی از چالش‌های اصلی، حضور شرکت‌ها و افراد غیرمتخصص در بازار است که با رقابت قیمتی، کیفیت و اعتبار صنعت را زیر سؤال می‌برند. چالش دیگر، نیاز به به‌روزرسانی مستمر دانش فنی و هماهنگ شدن با فناوری‌های نوین است. همچنین استانداردسازی، نظارت دقیق‌تر و تعامل بیشتر میان شرکت‌ها، اتحادیه و نهادهای دولتی می‌تواند به بهبود شرایط بازار کمک کند.

۷ برای شرکت‌هایی که قصد ورود به این صنعت را دارند، چه توصیه‌ای دارید؟

توصیه من این است که با نگاه بلندمدت و حرفه‌ای وارد این حوزه شوند. صرفاً فروش تجهیزات کافی نیست؛ باید دانش فنی، توان طراحی راهکار، تیم اجرایی متخصص و توان خدمات پس از فروش داشت. همچنین آشنایی با استانداردها، قوانین و روندهای جهانی و سرمایه‌گذاری در آموزش نیروی انسانی، از الزامات موفقیت در این صنعت است.

۸ چشم‌انداز آینده صنعت حفاظت الکترونیک در ایران را چگونه می‌بینید؟

با توجه به رشد تقاضا، توسعه زیرساخت‌های شهری و صنعتی و ورود فناوری‌های نوین مانند هوش مصنوعی، اینترنت اشیا و تحلیل داده، آینده روشنی برای این صنعت در ایران متصور هستم. اگر بتوانیم بر توسعه دانش فنی، تولید داخلی و ارائه راهکارهای یکپارچه تمرکز کنیم، ضمن کاهش وابستگی به واردات، می‌توانیم در سطح منطقه نیز به یک بازیگر مهم تبدیل شویم.

۹ و در پایان، چه پیامی برای فعالان این صنعت دارید؟

این صنعت، تنها یک بازار اقتصادی نیست؛ بلکه نقش مهمی در امنیت جامعه، آرامش مردم و توسعه پایدار کشور دارد. از همه فعالان، به‌ویژه نسل جوان و متخصص، دعوت می‌کنم با تعهد، اخلاق حرفه‌ای و همکاری بیشتر، برای ارتقای جایگاه صنعت حفاظت الکترونیک در ایران تلاش کنیم.

ARIO
SECURITY SOLUTIONS
FOR A SMARTER TOMORROW

راهکارهای یکپارچه
برای دنیایی امن‌تر



امنیت
فناوری
اعتماد
آینده روشن‌تر

توسعه بازار، با دانش و اعتماد ممکن است

ادامه گفت‌وگو با مهندس محمدعلی احمدی، مدیرعامل شرکت آریو مروارید ایمن

در بخش پایانی گفت‌وگو، با مهندس محمدعلی احمدی درباره آینده صنعت، نقش شرکت‌های ایرانی در زنجیره ارزش، اهمیت همکاری میان فعالان این حوزه و پیام ایشان به نسل جدید متخصصان صحبت کردیم.

”
با همکاری،
استاندارد و
تعهد، می‌توانیم
آینده‌ای امن‌تر
برای جامعه
بسازیم.

مهندس محمدعلی احمدی
مدیرعامل شرکت
آریو مروارید ایمن

۱۲ آیا شرکت آریو مروارید ایمن برنامه‌ای برای حضور در بازارهای منطقه‌ای دارد؟

بله، با توجه به ظرفیت‌های فنی و تجربی شرکت، حضور در بازارهای منطقه‌ای یکی از اهداف ما در سال‌های آینده است. باور داریم که محصولات و راهکارهای ایرانی در صورت رعایت استانداردها و ارائه خدمات حرفه‌ای می‌توانند در بازارهای منطقه نیز رقابتی باشند در حال حاضر، بررسی و برنامه‌ریزی برای این مسیر در دستور کار ما قرار دارد.

۱۰ به نظر شما مهم‌ترین چالش‌های فعلی صنعت چیست؟

از مهم‌ترین چالش‌ها می‌توان به نوسانات ارزی، واردات غیررسمی و کالاهای غیراستاندارد، ضعف در آموزش تخصصی، نبود حمایت‌های کافی از تولید و همچنین رقابت ناسالم در برخی بخش‌های بازار اشاره کرد. رفع این چالش‌ها نیازمند همکاری جدی میان دولت، اتحادیه‌ها و فعالان صنعت است.

۱۱ نقش اتحادیه‌ها و نهادهای صنفی را در توسعه صنعت چگونه ارزیابی می‌کنید؟

اتحادیه‌ها می‌توانند نقش بسیار مهمی در ساماندهی بازار، ارتقای استانداردها، حمایت از شرکت‌های معتبر و ایجاد بستر مناسب برای آموزش و تبادل تجربه داشته باشند. هرچه تعامل میان شرکت‌ها و نهادهای صنفی قوی‌تر باشد، مسیر رشد و توسعه صنعت هموارتر خواهد شد.

۱۵ چه توصیه‌ای به نسل جدید فعالان این صنعت دارید؟

توصیه من به نسل جدید این است که همواره به‌روز باشند، دانش فنی خود را تقویت کنند و تنها به فروش تجهیزات بسنده نکنند. این صنعت ترکیبی از فناوری، مدیریت، ارتباط با مشتری و تعهد است. با یادگیری مستمر، صداقت در کار و رعایت اصول حرفه‌ای می‌توانند آینده روشنی در این حوزه داشته باشند.

۱۴ چشم‌انداز شما از آینده صنعت حفاظت الکترونیک در ایران چیست؟

من آینده این صنعت را روشن می‌بینم. با رشد شهرنشینی، افزایش نیاز به امنیت و توسعه فناوری‌های نوین مانند هوش مصنوعی و تحلیل داده، بازار حفاظت الکترونیک در ایران ظرفیت بسیار بالایی دارد. اگر زیرساخت‌های لازم، استانداردسازی و آموزش به‌درستی تقویت شود می‌توانیم شاهد توسعه پایدار و حضور پررنگ‌تر شرکت‌های ایرانی در این حوزه باشیم.

۱۳ چه نقشی برای همکاری میان شرکت‌های فعال در این حوزه قائل هستید؟

همکاری میان شرکت‌ها به بویژه در زمینه تبادل تجربه، اجرای پروژه‌های مشترک و توسعه استانداردها، می‌تواند به ارتقای کل صنعت کمک کند. رقابت سالم در کنار همکاری، باعث رشد بازار، افزایش اعتماد مشتریان و بهبود سطح خدمات خواهد شد. ما در آریو مروارید ایمن همواره از هم‌افزایی با سایر شرکت‌های معتبر استقبال می‌کنیم.



SECURITY
PEOPLE
TECHNOLOGY
TRUST
A SAFER
TOMORROW

پیام پایانی

مهندس محمدعلی احمدی
به فعالان صنعت حفاظت الکترونیک

امنیت، یک نیاز اساسی برای جامعه امروز است و ما در این صنعت، مسئولیتی فراتر از یک کسب‌وکار داریم. با دانش، تعهد، رعایت استانداردها و همکاری، می‌توانیم سهم مؤثری در ساختن جامعه‌ای امن‌تر و هوشمندتر داشته باشیم. از همه همکاران، مشتریان و فعالان این عرصه که با اعتماد و حمایت خود در کنار ما هستند، صمیمانه سپاسگزارم.

مهندس محمدعلی احمدی
مدیرعامل شرکت آریو مروارید ایمن

فناوری برای زندگی امن‌تر



ARIO
SECURITY SOLUTIONS
FOR A SMARTER TOMORROW

یکپارچگی، آینده امنیت از تجهیزات تا مدیریت هوشمند

در دنیای امروز، امنیت تنها به معنای نصب چند دوربین یا تجهیز یک مرکز کنترل نیست؛ امنیت یک اکوسیستم یکپارچه است که از تجهیزات، زیرساخت، نرم افزار، داده و انسان تشکیل می شود. سازمان ها و شهرهای هوشمند برای مقابله با تهدیدهای پیچیده امروز، نیازمند رویکردی جامع و یکپارچه در حوزه امنیت فیزیکی و الکترونیکی هستند.

امنیت پایدار،
نتیجه نگاه یکپارچه
و تصمیم گیری مبتنی
بر داده است.

فناوری،
زیرساخت امن
برای فردای بهتر



امنیت سابری

حفاظت از داده ها،
دستگاه ها و زیرساخت ها
در برابر تهدیدهای
سابری



مدیریت یکپارچه

تجمیع سامانه ها
و مدیریت متمرکز
برای افزایش کارایی
و کاهش هزینه ها



هوش مصنوعی

تحلیل هوشمند تصاویر
و داده ها برای تشخیص
سریع تر و تصمیم گیری
دقیق تر



تحول دیجیتال

حرکت به سمت
زیرساخت های هوشمند
و سازمان های داده محور

فرصت ها و چالش های پیش رو

- رشد تقاضا برای شهرها و ساختمان های هوشمند
- افزایش حجم داده ها و نیاز به تحلیل سریع
- ضرورت یکپارچه سازی سامانه های ناهمگون
- نیاز به نیروی متخصص و آموزش های کاربردی
- رعایت الزامات قانونی و حریم خصوصی
- مدیریت تهدیدهای نوظهور در فضای فیزیکی و سایبری



داده
دید بهتر
تصمیم هوشمندتر

از نظارت سنتی
تا مدیریت هوشمند

راهکارهای یکپارچه برای سازمان های آینده

با ترکیب تجهیزات نوین، نرم افزارهای هوشمند، زیرساخت پایدار و تیم های متخصص، می توان مسیری مطمئن برای افزایش امنیت، بهره وری و توسعه پایدار سازمان ها و شهرها ایجاد کرد.



طراحی و مشاوره
تخصصی



پیاده سازی
و اجرا



پشتیبانی
و نگهداری



آموزش و
توانمندسازی

امروز امن تر،
فردا هوشمندتر

پرونده ویژه

هوش مصنوعی در حفاظت الکترونیک

از تشخیص تا تصمیم گیری هوشمند

هوش مصنوعی در سال های اخیر تحولی اساسی در صنعت حفاظت الکترونیک ایجاد کرده است. این فناوری با تحلیل داده های تصویری، شناسایی الگوها و یادگیری مداوم، دقت، سرعت و کارایی سیستم های نظارتی را به سطحی جدید رسانده و امکان تصمیم گیری هوشمند و پیشگیرانه را فراهم می کند.

AI
VISION
A SAFER
TOMORROW

فناوری
در خدمت
امنیت هوشمند



تشخیص افراد و چهره

شناسایی افراد
شتخیص چهره
ردیابی هوشمند



تشخیص پلاک (LPR)

کنترل تردد
مدیریت پارکینگ
مراجعه های هوشمند



تحلیل رفتار غیرعادی

تشخیص تجمع
رفتار مشکوک
اعلان های هوشمند



تحلیل داده های ویدئویی

آمار و گزارش های تحلیلی
بهینه سازی منابع
پیش بینی رخدادها



یکپارچه سازی سیستم ها

VMS هوشمند
اتصال به سایر سامانه ها
تصمیم گیری یکپارچه

کاربردهای عملی در دنیای واقعی



امنیت شهری

پایش معابر، تشخیص تجمع،
مدیریت بحران



صنایع و زیرساخت های حیاتی

پایش محیط های صنعتی،
تشخیص نفوذ، هشدارهای پیشگیرانه



سازمان ها و مراکز تجاری

کنترل دسترسی، تحلیل رفتار
مشتریان، افزایش امنیت



حمل و نقل و ترافیک

تشخیص پلاک، مدیریت تردد،
تحلیل جریان ترافیک



هوش مصنوعی
دوربین ها را از یک ابزار
ثبت تصویر، به یک
دستیار هوشمند برای
تصمیم گیری تبدیل
کرده است.



چالش ها و ملاحظات

- حفظ حریم خصوصی افراد
- امنیت داده ها و جلوگیری از سوءاستفاده
- دقت در تشخیص و کاهش خطاهای کاذب
- نیاز به زیرساخت پردازشی مناسب
- استانداردسازی و قوانین استفاده از AI

آینده هوش مصنوعی در امنیت

- تحلیل پیش بینیانه و پیشگیری از رخدادها
- ادغام با اینترنت اشیا (IoT)
- استفاده از مدل های یادگیری عمیق پیشرفته
- اتوماسیون کامل فرآیندهای نظارتی
- شهرها و سازمان های کاملاً هوشمند

امنیت هوشمند
آینده ای امن تر

فناوری امروز
آرامش فردا



امنیت سایبری
بخشی از
امنیت فیزیکی است.

امنیت سایبری در پروژه‌های حفاظت الکترونیک

از دوربین و NVR تا شبکه و دسترسی از راه دور؛
چطور یک زیرساخت حفاظتی امن طراحی کنیم؟

با گسترش اتصال تجهیزات نظارتی به شبکه و اینترنت، امنیت سایبری به یکی از ارکان اصلی در طراحی، اجرا و بهره‌برداری از سیستم‌های حفاظت الکترونیک تبدیل شده است. بی‌توجهی به اصول امنیتی می‌تواند منجر به دسترسی غیرمجاز، افشای اطلاعات و اختلال در سرویس‌ها شود.

۷ اصل امنیتی که باید رعایت کنیم

- تغییر رمزهای پیش فرض**
استفاده از رمزهای قوی و منحصر به فرد
- مدیریت حساب‌های کاربری**
تعریف سطوح دسترسی و حذف کاربران غیرضروری
- تفکیک شبکه‌ها**
جداسازی شبکه تجهیزات نظارتی از شبکه سازمان
- به‌روزرسانی مداوم**
به‌روزرسانی Firmware و نرم‌افزارها
- محدودسازی دسترسی از راه دور**
استفاده از VPN و غیرفعال کردن سرویس‌های غیرضروری
- پایش و ثبت رویدادها**
مانیتورینگ لاگ‌ها و بررسی رفتارهای مشکوک
- تهیه نسخه پشتیبان**
Backup منظم و تست فرآیند بازیابی

معماری امن یک سیستم نظارت تصویری



اشتباهات رایج در پروژه‌ها

- استفاده از رمزهای پیش فرض کارخانه
- اتصال مستقیم تجهیزات به اینترنت
- عدم تفکیک شبکه نظارتی از شبکه سازمان
- بروزرسانی نکردن Firmware
- فعال بودن سرویس‌های غیرضروری
- استفاده از P2P بدون کنترل امنیتی
- عدم پایش و بررسی لاگ‌ها

چک‌لیست امنیتی پروژه

- تغییر تمام رمزهای پیش فرض
- تعریف سطوح دسترسی کاربران
- پیکربندی VLAN و فایروال
- بروزرسانی Firmware تجهیزات
- غیرفعال‌سازی سرویس‌های غیرضروری
- استفاده از VPN برای دسترسی از راه دور
- فعال‌سازی لاگ و مانیتورینگ
- تهیه نسخه پشتیبان منظم
- انجام تست نفوذ و بررسی دوره‌ای امنیت

آکادمی ساینا
پاهوش تیر و سریش تیر و پیتیر

یادگیری حرفه‌ای،
بخشی از امنیت پروژه است.

در آکادمی ساینا، آموزش صرفاً انتقال مفاهیم نیست؛
هدف ما، تبدیل دانش فنی به توانایی اجرای پروژه است.
مسیرهای آموزشی با تمرکز بر نیاز واقعی صنعت طراحی شده‌اند.

دوره‌های مرتبط با امنیت سایبری در آکادمی ساینا



مبانی شبکه
و امنیت شبکه



امنیت در
سیستم‌های نظارتی



پیکربندی
تجهیزات شبکه



مدیریت و نگهداری
سیستم‌های نظارتی

SainaSoft.com

آموزش تخصصی برای متخصصان صنعت حفاظت و امنیت

HIKVISION®

See Farther, Safer World

راهکارهای جامع نظارت تصویری

برای دنیایی امن‌تر

- کیفیت بالاتر
- فناوری پیشرفته
- پشتیبانی مطمئن



انتخاب حرفه‌ای‌ها
در سراسر جهان

SECURITY
INTELLIGENCE
FOR A
BETTER
TOMORROW

AI

هوش مصنوعی

تحلیل هوشمند
و تشخیص دقیق



دوربین‌های تحت شبکه

تصویر شفاف
در هر شرایط



NVR / DVR

مدیریت حرفه‌ای
تصاویر



کنترل تردد

راهکارهای یکپارچه
مدیریت دسترسی



نرم‌افزار مدیریت

نظارت متمرکز
و مقیاس‌پذیر



پشتیبانی و خدمات

مشاوره، آموزش
و خدمات پس از فروش

امنیت

زیرساختی مطمئن‌تر

برای فردایی روشن‌تر

HIKVISION

TECHNOLOGY
BUILDS A SAFER
TOMORROW

شبکه گستر ساین

شرکت فناوری اطلاعات و ارتباطات



نماینده رسمی هایک‌ویژن در ایران



۰۲۶ ۳۲۶۲۰۰۰۰



www.SainaSoft.com



با ما در ارتباط باشید

کیفیت، نوآوری و اعتماد

See Farther, Safer World

از طراحی تا اجرا آناتومی یک پروژه حرفه‌ای حفاظت الکترونیک

چرا موفقیت یک پروژه فقط به انتخاب تجهیزات وابسته نیست؟

یک پروژه حرفه‌ای حفاظت الکترونیک، حاصل ترکیب دانش فنی، تحلیل دقیق نیازها، طراحی مهندسی، اجرای استاندارد و پشتیبانی مستمر است.

در این صفحه، مسیر اجرای یک پروژه موفق را به صورت گام به گام بررسی می‌کنیم.



SECURITY

DESIGN
IMPLEMENT
SUPPORT

پروژه موفق
نتیجه نگاه جامع است
نه فقط انتخاب تجهیزات

10 نگهداری و پشتیبانی



- بازدیدهای دوره‌ای
- به‌روزرسانی نرم‌افزار و فریمور
- پشتیبانی فنی و رفع اشکال
- ارائه SLA و قرارداد نگهداری

2 بازدید و برداشت اطلاعات



- بازدید میدانی
- برداشت نقشه و ابعاد
- بررسی زیرساخت موجود
- مستندسازی شرایط محیطی

3 طراحی معماری سیستم



- تعیین جانمایی تجهیزات
- طراحی توپولوژی شبکه
- انتخاب نرم‌افزار مدیریت تصویر
- طراحی پیکارچه با سیستم‌های دیگر

9 آموزش کاربر



- آموزش اپراتورهای سیستم
- آموزش مدیریت و گزارش‌گیری
- ارائه راهنمای کاربری
- انتقال دانش فنی به تیم بهره‌بردار

4 انتخاب تجهیزات مناسب



- دوربین‌های متناسب با سناریو
- NVR و سرورهای ذخیره‌سازی
- تجهیزات شبکه و PoE
- تجهیزات جانبی (UPS، رک و ...)

8 تست، مستندسازی و تحویل



- تست عملکرد کامل سیستم
- تنظیم گزارش نهایی
- ارائه مستندات فنی
- تحویل و تایید کارفرما

5 طراحی شبکه و زیرساخت



- طراحی ساختار شبکه
- تفکیک VLAN و امنیت شبکه
- محاسبه پهنای باند
- تعیین مسیر کابل‌کشی و فیبر نوری

8 تست، مستندسازی و پیرز



- تست عملکرد کامل سیستم
- تنظیم گزارش نهایی
- ارائه مستندات فنی
- تحویل و تایید کارفرما

7 اجرا و پیکربندی



- نصب تجهیزات
- پیکربندی نرم‌افزار و دستگاه‌ها
- تنظیمات امنیتی
- راه‌اندازی و تست اولیه

6 محاسبات ذخیره‌سازی و پهنای باند



- تعیین مدت زمان ذخیره‌سازی
- محاسبه ظرفیت هارد و RAID
- برآورد پهنای باند مورد نیاز
- بهینه‌سازی باس‌های کدک و رزولوشن

اشتباهات پرهزینه در پروژه‌ها



- ✗ انتخاب دوربین صرفاً بر اساس مگاپیکسل
- ✗ عدم توجه به شرایط نور و سناریوی واقعی
- ✗ طراحی ضعیف شبکه و زیرساخت
- ✗ برآورد نادرست ذخیره‌سازی
- ✗ عدم مستندسازی و آموزش کاربر
- ✗ نبود برنامه نگهداری و پشتیبانی

امنیت
یک محصول نیست؛
یک فرایند است.

People
Process
Technology
A Safer Tomorrow

در پروژه‌های امنیتی، اشتباهات کوچک می‌توانند هزینه‌های بزرگی داشته باشند.

آکادمی ساینا

با هوش تر سریع تر و بهتر

مسیر حرفه‌ای ورود

به پروژه‌های حفاظت الکترونیک

در آکادمی ساینا، دانش روز صنعت، تجربه عملی و نیازهای واقعی پروژه‌ها در قالب دوره‌های تخصصی به شما منتقل می‌شود.



اطلاعات دوره‌ها



مدارک معتبر



استاد مجرب



آموزش کاربردی

www.SainaSoft.com

آموزش؛

مسیر ساختن نسل حرفه‌ای صنعت

نگاهی به اهمیت آموزش در صنعت حفاظت الکترونیک و مسیر پیش رو

سال‌ها فعالیت در صنعت حفاظت الکترونیک و فناوری اطلاعات، یک واقعیت مهم را بیش از گذشته برای من روشن کرده است؛ تجهیزات و فناوری به‌تثایی نمی‌توانند یک صنعت حرفه‌ای بسازند؛ آنچه به فناوری ارزش می‌دهد، دانش، تجربه و انسانی هستند که بتوانند از آن به درستی استفاده کنند.

با همین باور، آکادمی ساینا را راه‌اندازی کردم؛ با هدف ایجاد بستری برای انتقال دانش تخصصی، تجربه‌های واقعی پروژه و مهارت‌های کاربردی که مستقیماً در محیط کار قابل استفاده باشند، تلاش ما این است که آموزش از فضای صرفاً تئوری فاصله بگیرد و به سمت مهارت‌محوری، پروژه‌محوری و نیاز واقعی بازار حرکت کند.

هدف؛ تربیت نیروی توانمند برای صنعت

هدف من در آکادمی ساینا صرفاً برگزاری دوره‌های آموزشی، نیست؛ بلکه تربیت نیرویی است که بتواند مسئله را تحلیل کند، راهکار ارائه دهد، طراحی انجام دهد، پروژه را اجرا کند و در برابر نتیجه کار خود مسئول باشد.

نقش آموزش در توسعه صنعت

یکی از مهم‌ترین دغدغه‌های من، فاصله میان آموزش و نیاز واقعی صنعت است. صنعت حفاظت الکترونیک برای رشد و حرفه‌ای‌تر شدن به نیروی انسانی متخصص، به‌روز و دارای مهارت‌های عملی نیاز دارد. آموزش، سرمایه‌گذاری برای آینده این صنعت است.

چرا در کمیسیون آموزش؟

حضور من در کمیسیون آموزش اتحادیه صنف الکترونیک و رایانه و اطلاع‌رسانی کرج به‌عنوان رئیس کمیسیون و همچنین در اتحادیه سراسری شرکت‌های فنی و مهندسی حفاظت الکترونیک، ادامه همین مسیر است. هدف، کمک به تدوین و توسعه دوره‌های تخصصی، استانداردسازی آموزش‌ها، شناسایی نیازهای واقعی بازار و ایجاد ارتباط مؤثر بین فعالان صنعت و مراکز آموزشی است.



با هم، برای صنعتی حرفه‌ای‌تر



مهندس اسماعیل اکبری

مدیر و مؤسس آکادمی ساینا

- رئیس کمیسیون آموزش اتحادیه صنف الکترونیک و رایانه و اطلاع‌رسانی کرج
- عضو کمیسیون آموزش اتحادیه سراسری شرکت‌های فنی و مهندسی حفاظت الکترونیک
- مدیرعامل شرکت شبکه گستر ساینا
- مدرس سازمان فنی و حرفه‌ای کشور
- بیش از ۲۰ سال تجربه در حوزه شبکه، امنیت و حفاظت الکترونیک

“

اگر قرار است صنعت حفاظت الکترونیک آینده‌ای حرفه‌ای‌تر داشته باشد، باید از امروز برای دانش و نیروی انسانی آن سرمایه‌گذاری کنیم.

مهندس اسماعیل اکبری

”



دوربین مناسب را چگونه انتخاب کنیم؟

از مگاپیکسل تا لنز، نور، DORI و تحلیل تصویر؛ انتخاب دوربین باید از سناریو شروع شود، نه از کاتالوگ.

انتخاب دوربین مدار بسته، صرفاً مقایسه چند عدد در کاتالوگ نیست. هر پروژه نیازها، محدودیت‌ها و شرایط خاص خود را دارد. در این راهنما، مهم‌ترین مؤلفه‌هایی که باید در انتخاب یک دوربین مناسب در نظر بگیرید، مرور می‌کنیم.

انتخاب
هوشمندانه
تصویری مطمئن‌تر
از آینده

۱. هدف تصویربرداری

ابتدا مشخص کنید هدف شما از تصویربرداری چیست: مشاهده کلی، تشخیص، شناسایی یا صرفاً ثبت رخداد؟ هر هدف، نیازمند رزولوشن، لنز و قابلیت‌های متفاوتی است.

۳. لنز و زاویه دید

لنز ثابت، وریفوکال یا موتورایز؟ زاویه دید مناسب باید بر اساس محیط، فاصله و محدوده تحت پوشش انتخاب شود.

۵. DORI

مگاپیکسل به تنهایی کافی نیست. باید بدانید دوربین در چه فاصله‌ای توانایی Detection، Observation و Identification دارد. (DORI معیار واقعی عملکرد است).

۷. قابلیت‌های هوشمند

امروزه قابلیت‌هایی مانند تشخیص انسان و خودرو، عبور از خط، Intrusion، شمارش افراد، LPR و سایر تحلیل‌های هوشمند به افزایش کارایی سیستم کمک می‌کنند.

۹. ذخیره‌سازی

مدت زمان نگهداری تصاویر، رزولوشن، بیت‌ریت و تعداد دوربین‌ها، ظرفیت هارد و نوع ذخیره‌سازی (NVR، سرور یا فضای ابری) را تعیین می‌کند.

۲. فاصله تا سوژه

فاصله نصب دوربین و فاصله مورد نیاز برای شناسایی مستقیماً بر انتخاب لنز و رزولوشن اثر دارد. برای فاصله‌های زیاد، استفاده از لنزهای موتورایز و دوربین‌های با رزولوشن بالاتر توصیه می‌شود.

۴. شرایط نوری

عملکرد دوربین در نور روز، شب، نور پس‌زمینه و شرایط نوری دشوار بسیار مهم است. قابلیت‌هایی مانند WDR، دید در شب (IR) و سنسورهای متخصص، کیفیت تصویر را تضمین می‌کنند.

۶. نرخ فریم و فشرده‌سازی

تعداد فریم بر ثانیه (FPS) و روش فشرده‌سازی مانند H.265+ / H.265 بر کیفیت تصویر، مصرف پهنای باند و ظرفیت ذخیره‌سازی تأثیر مستقیم دارد.

۸. شبکه و زیرساخت

نوع اتصال (PoE)، پهنای باند مورد نیاز، VLAN و ظرفیت NVR/VMS باید با تعداد و کیفیت دوربین‌ها متناسب باشد.

۱۰. سازگاری با معماری پروژه

دوربین باید بخشی از یک راهکار یکپارچه باشد. سازگاری با سایر تجهیزات، نرم‌افزار مدیریت و الزامات پروژه را در نظر بگیرید.

نمونه سناریوهای رایج



فضای داخلی
دوربین دام، زاویه دید وسیع



پارکینگ
فشار نوری متغیر، WDR قوی



ورودی
تشخیص چهره، کنترل دسترسی



محیط بیرونی
مقاومت در برابر شرایط جوی



نکته آکادمی ساینا



دوربین خوب، لزوماً گران‌ترین دوربین نیست؛ دوربینی است که برای سناریوی موردنظر، تصویر قابل استفاده تولید کند.



ساینا در مسیر توسعه؛ از صنعت تا آموزش و نیروی انسانی

با نگاه به آینده
در کنار فعالان
صنعت
حفاظت الکترونیک

مروری بر مهم‌ترین فعالیت‌ها، برنامه‌ها و دستاوردهای شبکه گستر ساینا در ماه‌های اخیر

تجربه
دانش
هم‌افزایی
توسعه



توسعه آکادمی ساینا

حرکت به سمت آموزش‌های تخصصی، مهارت‌محور و پروژه‌محور در حوزه حفاظت الکترونیک، شبکه و فناوری‌های نوین، با هدف تربیت نیروی متخصص و پاسخ به نیاز واقعی صنعت.

محورهای آموزشی:

- ✓ نظارت تصویری و ویدئو آنالیتیکس
- ✓ شبکه و زیرساخت
- ✓ طراحی و اجرای پروژه
- ✓ مهارت‌های حرفه‌ای و کسب‌وکار

→ **Saina Academy**
Learning Today
A Safer Tomorrow



برگزاری دوره‌های تخصصی

برگزاری دوره‌های کاربردی و تخصصی از مبانی شبکه و نصب دوربین تا طراحی، اجرا و عیب‌یابی سیستم‌های حفاظت الکترونیک، متناسب با نیاز بازار و پروژه‌های واقعی.

نمونه دوره‌ها:

- ✓ حفاظت الکترونیک (سطح مقدماتی)
- ✓ انز ۳۶۰ درجه تا فروش و مذاکره حرفه‌ای
- ✓ طراحی و اجرای پروژه‌های نظارت تصویری
- ✓ آمادگی آزمون‌های تخصصی



توسعه مسیرهای شغلی و استخدام

ایجاد فرصت همکاری و جذب نیروهای متخصص در حوزه‌های فروش، فنی، پشتیبانی، آموزش و فعالیت‌های تخصصی، با هدف توسعه سرمایه انسانی و رشد پایدار مجموعه.

- ✓ محیط حرفه‌ای و پویا
- ✓ فرصت یادگیری و رشد
- ✓ همکاری بلندمدت



فعالیت کمیسیون آموزش

مشارکت فعال در کمیسیون آموزش اتحادیه صنف الکترونیک و رایانه و اطلاع‌رسانی کرج و همکاری در تدوین و برگزاری دوره‌های آموزشی تخصصی برای ارتقای دانش و مهارت فعالان صنفی.

- ✓ تدوین سرفصل‌های آموزشی
- ✓ برگزاری دوره‌های تخصصی
- ✓ انتقال تجربه و دانش عملی
- ✓ هم‌افزایی با سازمان‌های مرتبط



توسعه محتوای تخصصی

ترجمه و ویراستاری منابع معتبر بین‌المللی مانند کتاب Intelligent Network Video و تولید محتوای فنی و آموزشی در قالب مقالات، ویدئوها و نشریه ساینا.

- ✓ ترجمه و بومی‌سازی منابع تخصصی
- ✓ تولید محتوای آموزشی و فنی
- ✓ انتشار نشریه ساینا
- ✓ اشتراک‌گذاری دانش با جامعه تخصصی



«از تجربه پروژه تا انتقال دانش؛
ساینا تلاش می‌کند بخشی از مسیر
توسعه حرفه‌ای صنعت باشد.»



صنعت
پروژه‌های واقعی



آموزش
انتقال تجربه



نیروی انسانی
رشد و فرصت



توسعه
آینده‌ای پایدار

S A I N A
A SAFER, SMARTER TOMORROW

امنیت یعنی یکپارچگی

از زیرساخت تا انسان،
از فناوری تا مدیریت،
در مسیر سازمانی امن تر و هوشمندتر

فناوری
انسان
فرآیند
امنیت پایدار

A SAFER
SMARTER
TOMORROW

۴ تداوم و توسعه

نگاهی به فردا



امنیت یک مقصد ثابت نیست، بلکه مسیر مداوم پیشرفت است. با بهره‌گیری از فناوری‌های نوین و رویکردی یکپارچه، می‌توان سازمان‌هایی هوشمندتر، ایمن‌تر و آمادتر برای آینده ساخت.

۳ دانش و نیروی انسانی

سرمایه اصلی صنعت



فناوری بدون انسان متخصص ارزش واقعی خود را نشان نمی‌دهد. آموزش، توسعه مهارت‌ها، انتقال تجربه و جذب نیروهای توانمند، ضامن امنیت پایدار و رشد صنعت است.

۲ طراحی یکپارچه

از زیرساخت تا بهره‌برداری



یکپارچگی در طراحی، انتخاب فناوری‌ها، زیرساخت، شبکه، ذخیره‌سازی، نرم‌افزار و فرآیندهای عملیاتی، کلید دستیابی به سیستمی کارآمد، قابل اعتماد و آینده‌نگر است.

۱ شناخت دقیق‌تر مسئله

نگاهی جامع به امنیت امروز



امنیت پایدار با درک صحیح از تهدیدها، تحلیل واقع‌بینانه شرایط و نگاه سیستمی آغاز می‌شود. نگاه جزیره‌ای دیگر پاسخگو نیست و امروز، امنیت نیازمند دیدی یکپارچه و فراتر از نصب تجهیزات است.

“**امنیت، نتیجه نگاه یکپارچه است؛ نه مجموعه‌ای از راهکارهای جداگانه.**”

در دنیایی که فناوری، انسان و داده بیش از هر زمان دیگری به هم متصل شده‌اند، امنیت تنها با یک نگاه جامع، همکاری و تداوم در مسیر دانش، فرآیند و مدیریت تحقق می‌یابد.

سخن پایانی

در این شماره تلاش کردیم با نگاهی جامع، ابعاد مختلف امنیت در عصر یکپارچگی را بررسی کنیم؛ از فناوری و زیرساخت تا انسان، فرآیند و مدیریت. امیدواریم مطالب این شماره بتواند برای فعالان صنعت حفاظت الکترونیک، شبکه و فناوری اطلاعات، الهام‌بخش مسیرهای جدید و تصمیم‌گیری‌های موثر باشد.

از همه نویسندگان، متخصصان، همکاران و خوانندگانی که با همراهی خود به انتشار این شماره کمک کردند، صمیمانه سپاسگزاریم.

در مسیر دانش و امنیت پایدار، همراه شما هستیم.

نشریه ساینا

مهرماه ۱۴۰۵

با هم
برای آینده‌ای
ایمن‌تر...

ساینا

همراه مسیر توسعه

دانش
تجربه
امنیت پایدار
آینده روشن‌تر

PEOPLE
TECHNOLOGY
SECURITY
A SMARTER
TOMORROW



نشریه تخصصی فناوری اطلاعات و امنیت

امنیت در عصر یکپارچگی



SainaMag.ir



۰۲۶۳۲۶۲۰۰۰۰



۰۹۲۰۴۶۰۶۹۹۱

فناوری زمانی ارزش آفرین است که در خدمت امنیت، پایداری و تصمیم‌سازی آگاهانه باشد.

SECURE CONNECTED SUSTAINABLE