آکادمی فنافزا

معرفی دوره‌ها

امنیت سایبری (CS)

هوش مصنوعی (AI)

نیمه اول

۱۴۰۴

مهارت‌آموزی و مهارت‌افزایی در مسیر شغلی

درباره ما

آکادمی فن‌افزا با درک عمیق از نیاز کشور به نیروی متخصص در حوزه فناوری‌های نو، آموزش مبتنی بر مسیر شغلی را کلید زده است. در این آکادمی مبتنی بر استانداردهای بین‌المللی و نیازهای بومی کشور، مسیرهای آموزش امنیت سایبری و هوش مصنوعی طراحی شده است. ما به علاقمندان و متخصصان فناوری اطلاعات کمک می‌کنیم تا با توسعه مهارت‌های خود همگام با توسعه علم، رشد و موفقیت شغلی را تجربه کنند. از آنجا که آموزش مهارت‌های نرم مدیریتی جزو لاینفک عملکرد بهتر نیروهای متخصص بوده و در دانشگاه به صورت ویژه به آن توجه نمی‌شود؛ در کنار آموزش‌های تخصصی، در هر دوره متناسب با نیاز مخاطب کارگاه‌های مدیریتی و توسعه فردی نیز در این موسسه تعریف شده‌اند.

حامیان

فن‌آسا
صندوق پژوهش و فناوری

صندوق نوآوری و شکوفایی

اینوستک
سرمایه‌گذار و سرمایه‌پذیر هوشمند

فهرست

هوش مصنوعی (AI)

امنیت سایبری (CS)

AI

۳

مدیر ارشد هوش مصنوعی (CAIO)

Chief AI Officer

امروزه نقش CAIO فراتر از جنبه‌های فنی هوش مصنوعی، به‌عنوان یکی از مهم‌ترین نقش‌های راهبردی در سازمان‌ها مطرح شده است. این مدیر باید بتواند استراتژی‌های هوش مصنوعی را با اهداف کسب‌وکار هم‌راستا کرده، پروژه‌های ارزش‌آفرین را شناسایی و زیرساخت داده‌ای مناسب برای پیاده‌سازی موفقیت‌آمیز آن‌ها فراهم کند. او همچنین مسئول اطمینان از رعایت ملاحظات اخلاقی، حریم خصوصی و الزامات قانونی مرتبط با AI خواهد بود. آشنایی با جدیدترین تکنولوژی‌ها و روندهای هوش مصنوعی در کنار تقویت مهارت‌هایی همچون طراحی مدل‌های تحول دیجیتال، هدایت تیم‌های بین‌رشته‌ای و برقراری ارتباط مؤثر با سایر اعضای ارشد سازمان از ویژگی‌های یک رهبر تحول‌آفرین در حوزه هوش مصنوعی است .

مدت زمان: ۲ روز
تاریخ برگزاری: نیمه دوم تیرماه

مخاطبان دوره

- ✓ مدیر ارشد فناوری اطلاعات
- ✓ مدیرعامل
- ✓ تحلیل‌گران داده و مهندسان AI
- ✓ مدیر پروژه هوش مصنوعی

محورهای تخصصی
دوره CAIO

۱ توسعه استراتژی و هم‌راستایی سازمانی

- مبانی AI و رهبری در عصر دیجیتال
- طراحی نقشه راه AI
- تجزیه و تحلیل تاثیر کسب و کار

۲ یکپارچه‌سازی فنی، اجرا و مدیریت ریسک

- حاکمیت هوش مصنوعی در سازمان و مدیریت ریسک
- تصمیم‌گیری مبتنی بر داده و ارزیابی تأثیر کسب‌وکار
- آمادگی فنی و ترویج استفاده سازمانی از هوش مصنوعی
- امنیت سایبری در AI

۳ رهبری، تحول و چشم‌انداز آینده

- بهره‌گیری از GenAI برای نوآوری در کسب‌وکار
- رهبری راهبردی
- بهره‌گیری از GenAI برای گزینش نیروی مناسب
- کارگاه عملی (طراحی یک استراتژی واقعی AI برای سازمان)

AI

دوره LLMx

دوره LLMx یا همان LLM experienced، دیدی عمیق از دنیای مدل‌های زبانی بزرگ در اختیار مخاطب قرار می‌دهد. از انتخاب مدل مناسب، آموزش آن‌ها، و سازگار کردن‌شان با محتوای اختصاصی خود گرفته تا مقایسه بین مدل‌های تجاری و متن‌باز، همگی در برنامه آموزشی این دوره گنجانده شده‌اند. بررسی تفاوت‌های استراتژیک بین مدل‌های مختلف به مهارت‌آموزان کمک می‌کند تا تصمیم‌گیری دقیق‌تری در انتخاب ابزار داشته باشند.

مدت زمان: ۱ روز
تاریخ برگزاری: ۳ مرداد
۲ شهریور

مخاطبان دوره

- ✓ کارآفرینان و صاحبان کسب‌وکار
- ✓ مدیران و کارشناسان ارشد سازمان‌ها
- ✓ اساتید و محققان دانشگاهی
- ✓ طراحان و متخصصان خلاقیت
- ✓ هر علاقمندی که میخواهد قدم در راه LLMها بگذارد

محورهای تخصصی

دوره LLMx

۱ معرفی هوش مصنوعی

- آشنایی با تعاریف هوش مصنوعی
- درک کاربردهای عملی و مفاهیم اساسی مانند پرامپت‌ها و مدل‌ها.

۲ استراتژی‌های بهبود عملکرد کارآمد

- شناسایی سناریوهای مناسب برای بهره‌وری مؤثر
- تکنیک‌های طراحی مؤثر پرامپت‌ها و بهینه‌سازی تکنیک‌های مهندسی پرامپت.

۳ تولید متن

- بررسی قابلیت‌های مدل‌های محبوب مانند ChatGPT، Claude و Llama.
- تسلط بر استراتژی‌های پرامپت و جریان‌های کاری GenAI
- استفاده از ابزارهایی برای خودکارسازی و بهبود مهندسی پرامپت.

۴ تولید تصویر و پادسازی هوش مصنوعی

- مرور توانایی‌های مدل‌های برجسته برای تولید تصویر – مانند DALL·E، Stable Diffusion، Mid-Journey.
- مهندسی پرامپت در طراحی‌های خلاقانه.
- کاربردهای واقعی در سناریوهای عملی.

۵ کارگاه عملی و پروژه نهایی دوره

- انجام پروژه‌های عملی با استفاده از مدل‌ها و ابزارهای AI
- پرورش تفکر طراحی در ارائه راهکارهای هوش مصنوعی در سناریوهای واقعی.

AI

LLM++

برنامه‌نویس ارشد LLM

در این دوره هدف تربیت نیروهای متخصص و برجسته در حوزه داده و هوش مصنوعی در سطح سازمان است. آن‌ها دارای تخصص فنی پیشرفته هستند و بیشتر نقش رهبری تیم‌های توسعه‌دهنده و دانش فنی بالا را دارند. تمرکز اصلی این افراد، توسعه و پیاده‌سازی سیستم‌های پیشرفته داده‌محور و مدل‌های زبانی بزرگ است.

مخاطبان دوره

- ✓ مهندسان یادگیری ماشین
- ✓ برنامه‌نویسان

مدت زمان: ۲ روز
تاریخ برگزاری: نیمه دوم مرداد

محورهای تخصصی

دوره LLM++

۱ مقدمه‌ای بر مدل‌های زبانی بزرگ (LLM)

- آموزش و ساختار مدل‌ها
- تعداد پارامترها و تأثیر عملی آن‌ها
- نیازمندی‌های سرور، سخت‌افزار و زیرساخت
- استفاده از مدل‌های زبانی با داده‌های اختصاصی سازمان

۲ آزمون عملی با استفاده از پرامپت‌ها

- مقایسه پاسخ مدل‌های مختلف از نظر خلاقیت، ارتباط و درک محتوا
- آزمون سوگیری: بررسی مواجهه مدل‌ها با موضوعات بحث‌برانگیز برای شناسایی سوگیری‌های احتمالی
- ارزیابی با معیارهای انسجام، دقت و سوگیری‌های شناسایی‌شده در رتبه‌بندی مدل‌ها

۳ سفارشی‌سازی و توسعه مدل‌های موجود

- آموزش مدل با داده‌های اختصاصی
- آماده‌سازی و یکپارچه سازی داده‌ها
- تنظیم دقیق (Fine-Tuning) و توسعه مدل‌های سفارشی‌شده

۴ تکنیک های پیشرفته

- ادغام داده‌های سازمانی در مدل‌های هوش مصنوعی
- بهبود عملکرد هوش مصنوعی از طریق تأمین هدفمند داده‌ها و تنظیم مدل
- نقش RAG در بازیابی و پردازش هوشمند داده‌ها

۵ کارگاه عملی از صفر تا صد یک پروژه Agentic AI

FAN AFZA ACADEMY

AI

دوره LLMOps

این دوره مهندسین هوش مصنوعی را برای طراحی، پیاده‌سازی و مدیریت زیرساخت‌های سخت‌افزاری و بک‌اند مدل‌های زبانی بزرگ آماده می‌کند. مسئولیت یک مهندس LLMOps شامل انتخاب و بهینه‌سازی سخت‌افزار مناسب، طراحی سیستم‌های مقیاس‌پذیر و پایدار برای آموزش و سرویس‌دهی مدل‌ها است. او باید از ابزارهای مدرن برای آموزش توزیع‌شده، استقرار امن و پایدار مدل‌ها و مدیریت هزینه‌های عملیاتی استفاده کند. همچنین بر روی عملکرد سیستم، تضمین امنیت داده‌ها و رعایت استانداردهای قانونی و اخلاقی نظارت داشته باشد.

مدت زمان: ۲ روز
تاریخ برگزاری: ۲۱ و ۲۸ تیرماه

مخاطبان دوره
مهندسان DevOps

محورهای تخصصی

دوره LLMOps

۱ مبانی زیرساخت‌های LLM

- معرفی مدل‌های زبان بزرگ و نیازهای عملیاتی آنها
- اجزای اصلی زیرساخت LLM
- زبان برنامه‌نویسی مورد نیاز

۲ طراحی سخت‌افزار برای LLM

- معماری‌های GPU و TPU و نقش آنها در عملکرد LLM
- مدیریت و بهینه‌سازی حافظه، موازی‌سازی مدل
- مدیریت هزینه سخت‌افزار و انتخاب منابع بهینه

۳ سیستم‌های بک‌اند و استقرار مدل

- معماری‌های سرویس‌دهی و پردازش دسته‌ای APIها
- تکنیک‌های آموزش توزیع‌شده DeepSpeed، FSDP و Ray
- CI/CD برای مدل‌های LLM و مدیریت نسخه‌ها

۴ عملیات و پایش LLM

- چارچوب‌های LLMOps و پیاده‌سازی عملیات پایش، لاگ‌گیری و هشدارها
- بهینه‌سازی عملکرد، تعادل بار و مقیاس‌پذیری خودکار
- امنیت و رعایت قوانین و ملاحظات اخلاقی

۵ موضوعات پیشرفته و کاربردهای عملی

- معماری بازیابی و تولید (RAG) و پیاده‌سازی آن
- استقرار مدل‌ها روی دستگاه‌های Edge، کمینه‌سازی و فشرده‌سازی مدل
- روندهای آینده و نوآوری‌های زیرساخت LLM

AI

Prompt parties:

توانمندسازی شرکت‌کنندگان در زمینه‌ی مهندسی پرامپت (Prompt Engineering) به شیوه‌ای تعاملی و خلاق به منظور آشنایی عملی با ابزارهای هوش مصنوعی (مثل ChatGPT، Gemini، Claude) و توسعه‌ی تفکر مسئله‌محور برای کاربردهای واقعی.

مدت: نیم روز
بنا به نیاز کارفرما، برگزاری سازمانی

مخاطبان دوره

تمامی کارمندان مجموعه در قالب گروه‌های حداکثر ۳۰ نفره

امکان شخصی سازی کارگاه بر اساس حوزه کاری مجموعه کارفرما و نقش شغلی مد نظر

محورها

۱ آموزش اصول اولیه طراحی پرامپت مؤثر

- ساختار پرامپت (دستور، زمینه، مثال).
- نقش‌پذیری در پرامپت
- نکات و ترفندهای بهینه‌سازی پرامپت.
- سوگیری و مخاطرات احتمالی

۲ تمرین عملی و رقابت تیمی برای نوشتن پرامپت‌های بهتر

- نمونه چالش‌ها:
  - خلاصه‌سازی یک گزارش تخصصی.
  - تحلیل یک آسیب‌پذیری امنیتی
  - تولید داستان خلاقانه با محدودیت خاص.

۳ اصول استفاده مسئولانه از هوش مصنوعی.

مدیر ارشد امنیت سایبری (CISO)

Chief Information Security Officer

CISO پل ارتباطی بین مدیران و مهندسان است که راهبردهای امنیتی سازمان را متناسب با اهداف و چشم‌اندازهای آن طراحی می‌کند. او باید جزئیات کنترل‌های فناوری و چارچوب‌های انطباق را دنبال کرده و فراتر از ایجاد امنیت عملیاتی، توسعه‌دهنده و هدایت‌گر برنامه‌های امنیتی بلندمدت باشد. داشتن دانش کافی در حوزه حاکمیت امنیت اطلاعات، مدیریت ریسک، پاسخ به تهدیدات و برنامه‌ریزی راهبردی برای موفقیت در این نقش ضروری است.

مدت زمان: ۵ روز
تاریخ برگزاری: نیمه دوم تیرماه

مخاطبان دوره

- ✓ کارشناسان امنیت با تجربه
- ✓ مدیران ارشد امنیت
- ✓ مدیران علاقمند به فناوری
- ✓ سرپرستان امنیت سازمان
- ✓ مدیران فناوری اطلاعات

محورهای تخصصی

دوره CISO

۱ اصول مدیریت و حاکمیت در امنیت سایبری

- مدیریت و حاکمیت امنیت اطلاعات
- برنامه‌ریزی راهبردی امنیت اطلاعات
- بسترسازی فرهنگ و اخلاق امنیت سایبری در سازمان

۲ نقش روزانه CISO

- ارزیابی، مدیریت و ایجاد امنیت اطلاعات
- شایستگی‌ها و نقش‌های مدیریتی
- ایجاد تعادل بین امنیت اطلاعات و اهداف سازمان
- برنامه‌ریزی و توسعه تیم

۳ دانش فنی و شایستگی‌های CISO

- حملات فزاینده سایبری و راهبردهای نوین دفاعی
- معماری امنیت شبکه نسل جدید
- مفاهیم اولیه هوش مصنوعی در امنیت سایبری
- مدل بلوغ امنیت نرم‌افزار

۴ کنترل‌های مدیریت اطلاعات و مدیریت ریسک

- مفاهیم کنترل امنیت اطلاعات
- استانداردها و چارچوب‌های امنیت اطلاعات
- مدیریت ریسک امنیت اطلاعات

۵ راهبردهای تجربه‌محور در امنیت سایبری

- بودجه پروژه‌های امنیتی
- مدیریت قراردادها و فرآیندهای تدارکاتی
- تداوم کسب و کار
- تاب‌آوری سایبری

کارگاه مهارت نرم مدیریتی

مدیر حفاظت از زیرساخت‌های حیاتی (CIP)

Critical Infrastructure Protection

CIP شامل حفاظت از دارایی‌های فیزیکی و دیجیتالی، سامانه‌ها و شبکه می‌شود. دوره مدیر حفاظت از زیرساخت‌های حیاتی کشور یک رویکرد هماهنگ برای الویت‌بندی و تعیین اهداف و الزامات برای کاهش مخاطرات حاصل از رویدادها و حملات دشمن در اختیار قرار می‌دهد. این برنامه هر سه جنبه فیزیکی، سایبری و انسانی را در نظر گرفته و الزامات لازم جهت پیاده‌سازی برنامه‌های حفاظتی و راهبردهای تاب‌آورانه را شامل می‌شود.

مخاطبان دوره

- ✓ مدیران شبکه و سرور
- ✓ تحلیل‌گران امنیت سایبری
- ✓ مهندسان امنیت سایبری
- ✓ سرپرست‌های امنیت سایبری

مدت زمان: ۵ روز
تاریخ برگزاری: نیمه دوم تیرماه

محورهای تخصصی

دوره CIP

۱ اهمیت حفاظت از زیرساخت‌های حیاتی

- درک اهمیت زیرساخت‌های حیاتی و انواع آن
- تحلیل برنامه فعلی سازمان برای CIP
- سیاست‌های ملی و بین‌المللی موجود
- روندهای آینده در CIP
- مطالعات موردی و کاربردهای دنیای واقعی

۲ امنیت سایبری و فیزیکی برای زیرساخت‌های حیاتی

- امنیت فیزیکی برای زیرساخت‌های حیاتی
- محیط‌های امنیت الکترونیکی
- درک وابستگی متقابل امنیت فیزیکی و سایبری
- پیاده‌سازی راهبرد

۳ ارزیابی ریسک

- درک اصول ارزیابی ریسک و اجرای آن
- توسعه استراتژی‌های کاهش ریسک
- بررسی مطالعات موردی و انتخاب بهترین شیوه‌ها
- ارزیابی و بهبود مستمر

۴ شناسایی تهدیدات و بررسی آمادگی ذینفعان

- درک فرآیندهای THIRA و SPR
- شناسایی تهدیدات و خطرات
- تعیین اهداف زیرساخت
- انجام بررسی آمادگی ذینفعان

۵ تاب‌آوری و چرخه هوشمند اطلاعاتی

- تاب آوری
- تدوین یک نقشه تاب‌آورانه و چرخه هوشمند تداوم عملکرد
- بهره‌گیری از چرخه هوشمند اطلاعات

CS

متخصص سیستم‌های امنیت اطلاعات (ISSP)

Information Security Systems professional

این برنامه آموزشی ویژه برای افزایش دانش امنیت سایبری رهبران تیم‌های امنیتی بوده و عمدتاً بر اجرای عملی امنیت سایبری و مدیریت تیم متمرکز است. مخاطب دوره مهارت‌های فنی و دانش عملی و کاربردی در نقش‌های عملیاتی فناوری اطلاعات داشته و بعد از طی کردن این دوره تخصص کافی برای پیاده‌سازی، نظارت و مدیریت زیرساخت‌های فناوری اطلاعات را به دست می‌آورد. این تخصص مطابق با سیاست‌ها و رویه‌های امنیت اطلاعات است که از محرمانگی، یکپارچگی و در دسترس بودن داده‌ها اطمینان حاصل می‌کند. از این دوره می‌توان به عنوان شروعی برای مسیر اخذ گواهی CISSP نام برد.

مدت: ۵ روز
تاریخ برگزاری: ۱ مرداد

مخاطبان دوره

- ✓ تحلیل‌گر امنیت
- ✓ مهندس امنیت IT
- ✓ مشاور امنیت
- ✓ مدیر امنیت اطلاعات
- ✓ کارشناسان ارشد امنیت

محورهای تخصصی

دوره ISSP

۱

کنترل دسترسی

- پیاده‌سازی و نگهداری روش‌های احراز هویت
- پشتیبانی از معماری‌های اعتماد بین‌شبکه‌ای
- مشارکت در چرخه عمر مدیریت هویت
- پیاده‌سازی کنترل‌های دسترسی

۲

عملیات امنیتی و مدیریت

- درک مفاهیم امنیتی
- مستندسازی، پیاده‌سازی و نگهداری کنترل‌های امنیتی
- مشارکت در مدیریت دارایی‌ها
- پیاده‌سازی کنترل‌های امنیتی و ارزیابی ریسک

۳

شناسایی، نظارت و تحلیل ریسک

- درک فرآیند مدیریت ریسک
- انجام فعالیت‌های ارزیابی امنیتی
- مدیریت، نگهداری و تحلیل نتایج سیستم‌های نظارتی

۴

پاسخ به حوادث و بازیابی

- پشتیبانی از چرخه حیات حادثه
- درک و پشتیبانی از تحقیقات فارنزیک

۵

فناوری

- اهمیت رمزنگاری
- ترندهای هوش مصنوعی
- استفاده از ابر در سازمان

۶

امنیت شبکه و ارتباطات

- درک و اعمال مفاهیم پایه‌ای شبکه
- درک حملات شبکه و اقدامات مقابله‌ای
- مدیریت کنترل دسترسی شبکه

۷

امنیت سامانه‌ها و برنامه‌ها

- شناسایی و تحلیل کد و فعالیت‌های مخرب
- پیاده‌سازی و مدیریت امنیت دستگاه‌های پایانی

کارگاه تداوم کسب و کار

محوریت کارگاه استاندارد ISO ۲۲۳۰۱ هست. ایجاد یک برنامه مدیریت تداوم کسب و کار بر اساس ISO ۲۲۳۰۱ می‌تواند به سازمان‌ها کمک کند تا به سمت درک و مدیریت حوادث و خطرات پیشرفت کنند. از این رو این دوره آموزشی به منظور ارائه دانش و مهارت لازم به شرکت‌کنندگان برای پیاده‌سازی سیستم مدیریت تداوم کسب و کار (BCMS) بر اساس الزامات ISO ۲۲۳۰۱ طراحی شده است. ایجاد چارچوبی مبتنی بر این استاندارد سازمان را قادر می‌سازد که اثربخشی عملیاتی مستمر سازمان را در طول رویدادهای مخرب تضمین کند.

مدت: یک روز
تاریخ برگزاری :نیمه دوم تیر ماه و نیمه اول مرداد

مخاطبان دوره

- ✓ مدیران و کارشناسان بخش IT سازمان
- ✓ متخصصان امنیت سایبری
- ✓ سیاست‌گذاران تداوم کسب و کار سازمان
- ✓ مدیران ریسک و امنیت
- ✓ متخصصان بازیابی و امداد حادثه

CS

محورهای تخصصی

- ❖ مقدمه‌ای بر تداوم کسب و کار و تاب‌آوری سایبری
- ❖ آشنایی با استاندارد ISO۲۲۳۰۱ به عنوان مرجع سیستم مدیریت استمرار کسب و کارو الزامات آن
- ❖ ارزیابی ریسک و تحلیل تأثیر کسب و کار (BIA)
- ❖ توسعه برنامه تداوم کسب و کار (BCP)

CS

اتاق فرار سایبری

تجربه‌ای کاملاً تعاملی که تهدیدات واقعی سایبری را در محیطی ایمن و کنترل‌شده شبیه‌سازی می‌کند. این برنامه با هدف افزایش آگاهی و دانش کارمندان مجموعه و ایجاد تجربه تعاملی به همراه بازی‌وارسازی (گیمیفیکیشن) با تلفیق بخش‌های آموزشی و مهارتی طرح ریزی شده است.

مخاطبان دوره

تمامی کارمندان مجموعه

در هر سری اجرا تیم‌های ۴ نفره وارد اتاق شده و حداکثر نیم ساعت فرصت حل چالش ها را دارند.

در نهایت آموزش آگاهی رسانی سایبری به تیم‌های حاضر در جلسه داده می‌شود.

مدت: نیم روز
بنا به نیاز کارفرما، برگزاری سازمانی

محورهای تخصصی اتاق فرار

- مدیریت هویت و دسترسی
- پیشگیری از نشت اطلاعات
- حاکمیت اطلاعات و مدیریت ریسک
- امنیت فیزیکی
- مدیریت اعتبارنامه‌ها
- مهندسی اجتماعی
- رمزنگاری پایه
- حفظ تمامیت داده

FANAFZA ACADEMY

شرکت‌های حاضر در دوره‌های پیشین

آدرس:
تهران، خیابان آزادی، بعد از دانشگاه صنعتی شریف، بلوار جواد اکبری، بن‌بست گل، پلاک ۱

www.fanafza.ir
info@fanafza.ir
02166013109
LinkedIn: fanafza

آکادمی فنافزا