

دوره تربیت مدیر ارشد امنیت سایبری (سطح ۱)

فهرست

معرفی آکادمی	۳
CISO چه کسی است؟	۴
مخاطبان دوره	۴
ضرورت وجود CISO در سازمان چیست؟	۵
اهداف دوره	۵
محورهای تخصصی محتوای دوره	۶
اساتید دوره	۸
زمانبندی دوره	۱۰
هزینه دوره	۱۱
مکان برگزاری	۱۲

حامیان



معرفی آکادمی

امنیت سایبری آینده، تهدید از جنس منابع انسانی و نیروی متخصص است. هرچند پیش‌بینی شده است که تا سال ۲۰۲۵ تهدیدات سایبری منجر به بیش از ۱۰.۵ تریلیون خسارت شود؛ اما نبود نیروی متخصص به عنوان یکی از ۵ چالش بزرگ این صنعت بیان می‌شود. بیش از ۷۰ درصد مدیران امنیت سایبری ادعا می‌کنند که عدم توانایی و نبود دانش کافی در تیم امنیت سایبری منجر به خسارات غیرقابل جبران در سازمان آنها شده است. به همین دلیل صنعت امنیت سایبری به سمت دو هدف در حال پیش‌رفتن است: بازنگری مهارتی و مهارت‌افزایی. فن‌افزا یک موسسه آموزش عالی امنیت سایبری با رویکرد تربیت نیروی متخصص آماده به کار و در قالب چارچوب آموزشی تعریف شده بومی هست. چارچوب آموزشی تعریف شده در این موسسه مبتنی بر نیاز کشور و براساس چارچوب‌های آزموده شده جهانی و به کمک متخصصان دانشگاه صنعتی شریف تدوین شده است. ما به علاقمندان و متخصصان فناوری اطلاعات و امنیت سایبری 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 آموزش امنیت سایبری، دوره‌های مدیریتی نیز در این موسسه تعریف شده‌اند. هدف ما ارتقا سطح امنیت سایبری شرکت‌های بزرگ و بعد در قدم بعدی شرکت‌های میانه و کوچک است.

مدیر ارشد امنیت سایبری 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. دانش در حوزه حاکمیت امنیت اطلاعات، مدیریت ریسک، پاسخ به تهدیدات و برنامه‌ریزی راهبردی برای موفقیت در این نقش ضروری است.

CISO چه کسی است؟



مخاطبان دوره

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

این دوره برای مدیران ارشد و میانی و کارشناسان ارشدی مفید است که در تصمیم‌گیری‌ها نقش مهم دارند. بنابراین دوره قابل استفاده برای CISOهای فعلی و مدیران فناوری اطلاعات سازمان‌ها است که وظیفه پشتیبانی از برنامه‌های امنیت اطلاعات را داشته و قصد مهارت‌افزایی و کسب دانش روز را دارند. در کنار این‌ها متخصصان ارشد امنیت، ممیزان امنیت و معماران امنیتی که در صدد ارتقای شغلی به سمت مدیر امنیت هستند می‌توانند برای تسهیل مسیر خود از محتوای این دوره بهره ببرند.

ضرورت وجود CISO در سازمان چیست؟

صرف نظر از اینکه پیش‌زمینه مدیر امنیت سایبری فنی باشد یا مدیریتی، نیاز به کسب مهارت‌های راهبردی همراستا با راهبرد سازمان دارد. بنابراین او باید ریسک کسب‌وکار را درک کند. چرا که وظیفه او تنها حفاظت از فناوری اطلاعات نبوده، بلکه محافظت از کسب‌وکار در برابر تهدیدات سایبری به زیرساخت‌های فناوری اطلاعات وظیفه مهمتری است.



اهداف دوره

- ۱ شناخت مفاهیم پایه و کلیدی در مدیریت و حاکمیت امنیت اطلاعات
- ۲ شناسایی، تجزیه و تحلیل و ارزیابی ریسک‌های امنیتی با استفاده از رویکرد سیستماتیک و شناخت مفاهیم کنترل‌های امنیتی
- ۳ شناخت کاربرد فناوری‌های نوین مثل هوش مصنوعی در امنیت سایبری
- ۴ درک نقش و مسئولیت‌های CISO و ملاحظات اخلاقی مرتبط با آن و شناخت راهکار مناسب رویایی با چالش‌های این نقش
- ۵ طراحی و توسعه یک برنامه موثر امنیت سایبری متناسب با نیازهای سازمان و با رویکرد تاب‌آوری سایبری و تداوم کسب و کار
- ۶ تقویت مهارت نرم مدیران با یادگیری تکنیک مهارت مکالمه صریح و چگونگی ترویج فرهنگ صراحت در داخل سازمان

محورهای تخصصی

محتوای دوره

محور اول

اصول مدیریت و حاکمیت در امنیت سایبری

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

محور دوم

نقش روزانه CISO

- ارزیابی، مدیریت و ایجاد امنیت اطلاعات
- شایستگی‌ها و نقش‌های مدیریتی
- ایجاد تعادل بین امنیت اطلاعات و اهداف فناورانه سازمان
- برنامه‌ریزی و توسعه تیم در راستای برنامه امنیت اطلاعات
- سخنرانی کلیدی تجربه زیست مدیر امنیت سایبری

محور سوم

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



محور چهارم

کنترل‌های مدیریت اطلاعات و مدیریت ریسک

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

محور پنجم

راهبردهای تجربه‌محور در امنیت سایبری

- تامین و تخصیص منابع مالی، پایش و پیش‌بینی و گزارش‌دهی بودجه
- ادغام الزامات امنیتی در قراردادهای و فرآیندهای تدارکاتی، معرفی ابزارها
- تداوم کسب و کار
- تاب‌آوری سایبری
- کارگاه مهارت نرم: گفتگوی صریح

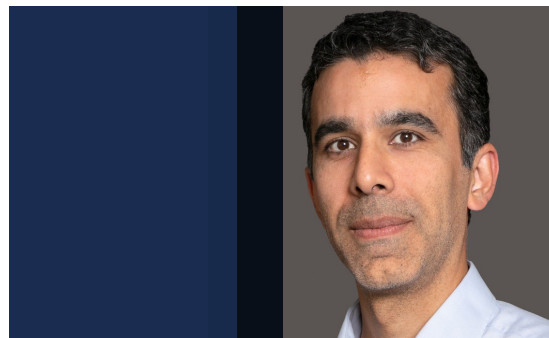


اساتید دوره



مهندس وحید خدابخشی

- مدیر ریسک و امنیت شرکت شاپرک
- رئیس کمیته ریسک و امنیت نظام پرداخت کشور
- بیش از ۱۰ سال سابقه فعالیت در حوزه امنیت شبکه و اطلاعات
- مدرس مدعو دانشگاه صنعتی شریف
- دانش آموخته کارشناسی ارشد امنیت شبکه و
- اطلاعات از دانشگاه صنعتی شریف



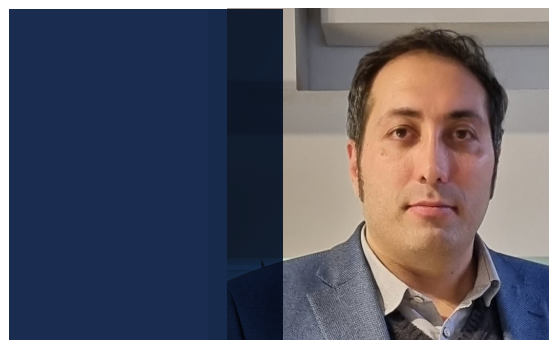
دکتر محمدرضا سهی زاده

- دانش آموخته مخابرات رمز از دانشگاه صنعتی شریف در مقطع کارشناسی ارشد و امنیت فضای تبادل اطلاعات از دانشگاه برگن نروژ در مقطع دکترا
- بیش از ۱۵ سال تجربه در زمینه مشاوره امنیت فضای تبادل اطلاعات در داخل و خارج از کشور و همکاری با شرکت‌های مشاوره‌ای بین‌المللی در زمینه امنیت اطلاعات از جمله Accenture و PwC



دکتر محمدحسین نقوی

- مدیر مدرسه مدیریت ناول و نماینده موسسه بین‌المللی Coaching Ourselves
- مترجم و مولف چندین کتاب
- مدرس مربی و تسهیلگر بیش از ۱۵۰ کارگاه آموزشی مدیریتی در سازمانهای بزرگ کشور
- پژوهشگر و مشاور سیاستگذاری و رهبری نوآوری
- مشاور روشهای نوین توسعه و یادگیری مدیران



دکتر سید علیرضا مهدوی

- مشاور ارشد امنیت اطلاعات
- مدیر عامل شرکت داده پردازان آبشار
- بیش از ۱۵ سال سابقه مشاوره حوزه کنترل امنیت اطلاعات
- نویسنده کتاب
- مشاوره مدیریت تداوم کسب و کار



دکتر هاشم حبیبی

- سابقه بیش از ۲۵ سال مدیریت امنیت سایبری
- مدیرعامل و عضو هیئت مدیره امن افزار گستر شریف
- دانش‌آموخته مهندسی کامپیوتر دانشگاه صنعتی شریف



دکتر محمود اقوامی‌پناه

- دانش‌آموخته دکتری امنیت داده و شبکه از دانشگاه صنعتی شریف
- محقق در دانشگاه KTH سوئد
- مدیرعامل شرکت دانش‌بنیان ناد فعال در حوزه امنیت سایبری



دانستن تفاوت‌های رهبری و مدیریت در کنار لایه‌های امنیت اطلاعات از لایه فنی تا لایه راهبردی جزو بایسته‌های یک مدیر خوب است. **CISO** باید استانداردهای مرتبط با هر لایه، مولفه‌های حاکمیت امنیت سایبری و نحوه دستیابی به اهداف راهبردی را بداند.

زمانبندی دوره

مدت دوره: ۵ روز - ۴۲ ساعت

ساعت / تاریخ	۱۰ خرداد	۱۷ خرداد	۲۳ خرداد	۲۴ خرداد	۳۱ خرداد
۸:۳۰ تا ۹:۴۵	ارزیابی و مدیریت امنیت اطلاعات (مهندس خدابخشی)	تهدیدات و راهبردهای نوین دفاعی (مهندس خدابخشی)	شبکه سازی بین مدیران (دکتر نقوی)	سیستم کنترل مدیریت امنیت اطلاعات (دکتر مهدوی)	مدل بلوغ امنیت نرم افزار (مهندس خدابخشی)
۱۰ تا ۱۱:۱۵	شایستگی ها و نقش های مدیریتی (مهندس خدابخشی)	معماری امنیت شبکه نسل جدید (مهندس خدابخشی)	کارگاه مهارت گفتگوی صریح ۱ (دکتر نقوی)	استانداردهای امنیت اطلاعات (دکتر مهدوی)	بودجه بندی پروژه های امنیتی (مهندس خدابخشی)
۱۱:۳۰ تا ۱۲:۴۵	برنامه ریزی و توسعه تیم در راستای اهداف امنیتی (مهندس خدابخشی)	مدیریت امنیت کلان داده (مهندس خدابخشی)	کارگاه مهارت گفتگوی صریح ۲ (دکتر نقوی)	استاندارد جدید (دکتر مهدوی)	پایش و گزارش دهی بودجه (مهندس خدابخشی)
۱۳:۴۵ تا ۱۵:۱۵	تجربه زیست سال مدیریت امنیت (دکتر حبیبی)	حاکمیت و مدیریت امنیت اطلاعات (دکتر سهی زاده)	سخرانی کلیدی	مدیریت ریسک امنیت اطلاعات (دکتر مهدوی)	فرآیندهای تدارکاتی پروژه های امنیتی (مهندس خدابخشی)
۱۵:۳۰ تا ۱۷	ایجاد تعادل بین امنیت اطلاعات و اهداف فناورانه (مهندس خدابخشی)	برنامه ریزی راهبردی (دکتر سهی زاده)	کاربرد هوش مصنوعی در امنیت سایبری (دکتر اقوامی پناه)	تداوم کسب و کار (دکتر سهی زاده)	تاب آوری سایبری (دکتر سهی زاده)



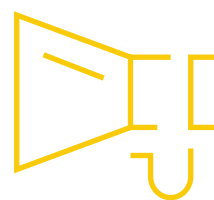
مدیر ارشد امنیت سایبری باید ریسک کسب و کار را درک کند، چرا که وظیفه او تنها حفاظت از فناوری اطلاعات نبوده، بلکه محافظت از کسب و کار در برابر زیرساخت های فناوری اطلاعات، وظیفه مهم تری است.

هزینه دوره

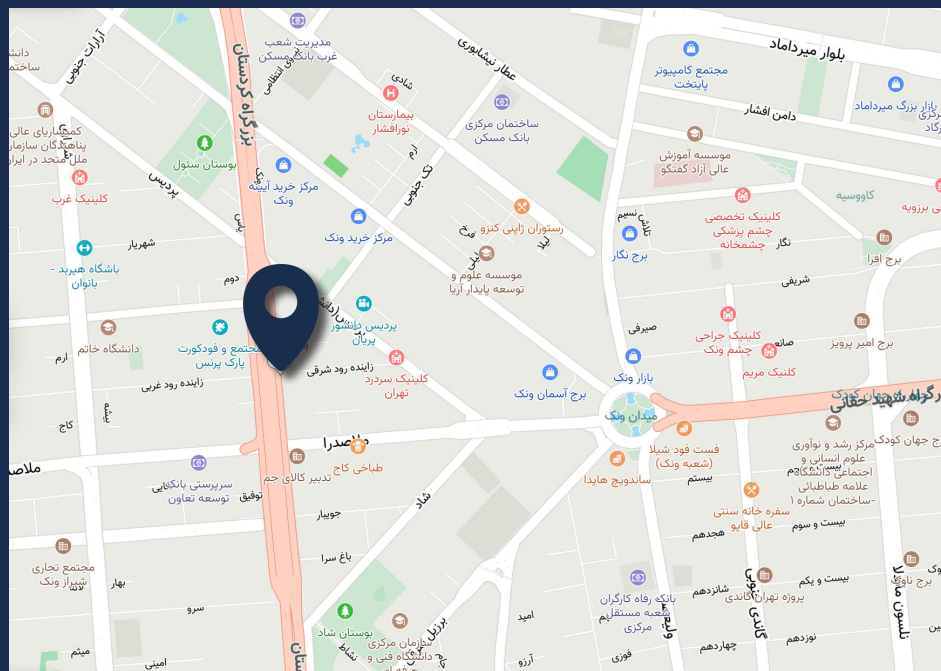
نحوه شرکت	میزان تخفیف	هزینه نهایی*
انفرادی و آزاد	-	۲۵/۰۰۰/۰۰۰
گروهی دو نفره	۱۰ درصد	۲۲/۵۰۰/۰۰۰
گروهی بیش از سه نفر	۱۵ درصد	۲۱/۲۵۰/۰۰۰
شرکت‌های دانش‌بنیان	۳۵ درصد	۱۶/۲۵۰/۰۰۰
ثبت نام زودهنگام (تا پایان فروردین ماه)	۱۵ درصد	۲۱/۲۵۰/۰۰۰

* واحد قیمت‌ها به تومان است.

CISO باید بتواند ارتباط خوبی با اعضای ارشد، هیئت مدیره، تامین‌کننده‌ها و تیم خود داشته باشد تا به ساده‌ترین و قابل فهم‌ترین روش مسائل فنی مرتبط با ریسک‌های **امنیت سایبری** و اهداف تجاری را توضیح دهد.



مکان برگزاری



تهران، میدان ونک، خیابان ملاصدرا، خیابان پردیس، خیابان زاینده‌رود شرقی، شماره ۲۴، صندوق نوآوری و شکوفایی، سالن همایش‌های شیخ بهایی

میزان توجه و سرمایه‌گذاری شرکت‌ها بر روی امنیت سایبری با توجه به اندازه سازمان و اهمیت حفظ دارایی‌های دیجیتال آن متفاوت بوده و نیاز به مدیریت دارد. یکی از مهمترین افرادی که باید شایستگی‌های فنی لازم را داشته و امنیت سایبری سازمان را کنترل و مدیریت کند، CISO است.





FANAFZA ACADEMY



1st Floor, No. 29, Paradis Bldg, North Kamranijeh, Tehran, Iran



+9821 2228 7541



fanafza



www.fanafza.ir