

پک تحلیلگر امنیت سایبری (Cybersecurity Analyst)

مروری بر دوره

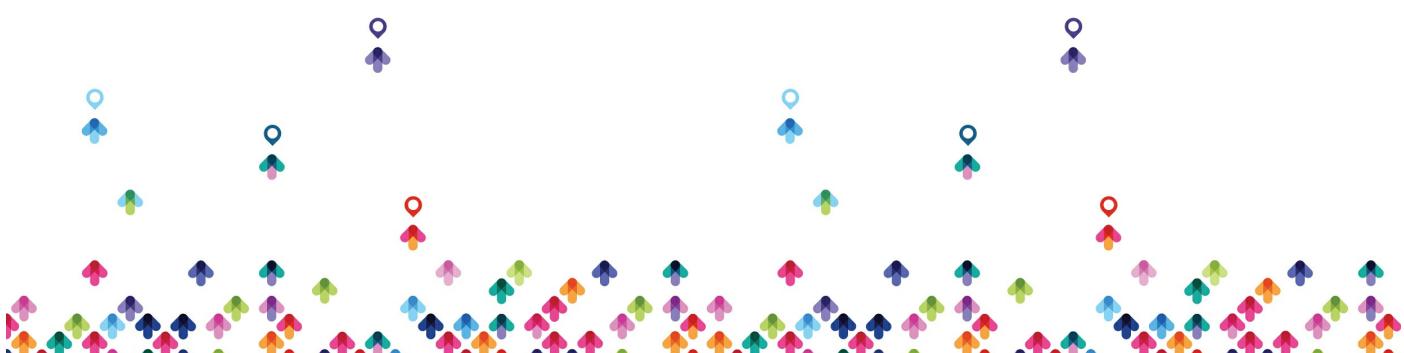
انتخاب مسیر شغلی به عنوان یک تحلیلگر امنیت سایبری (Cybersecurity Analyst) می‌تواند فرصت‌های شغلی زیادی را در حوزه فناوری اطلاعات برای شما فراهم کند. با توجه به رشد روزافزون تهدیدات سایبری، این شغل از جایگاه بالایی برخوردار است و نیازمند مهارت‌های خاصی است. در ادامه به نکات کلیدی و مهم در انتخاب این مسیر شغلی پرداخته‌ایم:

آشنایی با حوزه امنیت سایبری و نقش تحلیلگر امنیت

- ابتدا باید با مفاهیم پایه امنیت سایبری و تهدیدات مختلف در فضای مجازی آشنا شوید. تحلیلگر امنیت سایبری مسئول شناسایی، تحلیل، و پاسخ به تهدیدات امنیتی برای حفاظت از داده‌ها و سیستم‌های اطلاعاتی است.
- نقش تحلیلگر امنیت شامل نظارت بر رویدادهای امنیتی، انجام تحلیل تهدید، مدیریت رخدادهای امنیتی و همچنین پیشنهاد راهکارهای امنیتی برای کاهش آسیب‌پذیری‌ها است.
- در Package آموزشی ارزنگ سعی شده است که مطالب بالا بصورت مناسب تحت پوشش قرار بگیرند.

مهارت‌های فنی مورد نیاز

- برای موفقیت در این مسیر، نیازمند تسلط بر شبکه‌ها و سیستم‌های کامپیوتری، آشنایی با ابزارهای مانیتورینگ و تحلیل امنیتی و همچنین درک مفاهیم رمزنگاری و کنترل دسترسی هستید.
- مهارت‌هایی مانند کار با ابزارهای امنیتی (مثل SIEM)، تحلیل لاغ‌ها، شناسایی بدافزارها، و مقابله با حملات شبکه‌ای از جمله مهارت‌های مهم در این حوزه هستند.
- آشنایی با زبان‌های برنامه‌نویسی مانند Bash و Python نیز می‌تواند در اتوماتیک‌سازی فرایندها و تحلیل تهدیدات کمک کند. این بخش، بخش Python در بسته تعریف شغلی امنیت ارزنگ وجود ندارد، اما کلاس‌های کاملی جهت



خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۰۵۰ - ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

همپوشانی این مطلب در ارزنگ برگزار می شود.

تحصیلات و مدارک مورد نیاز

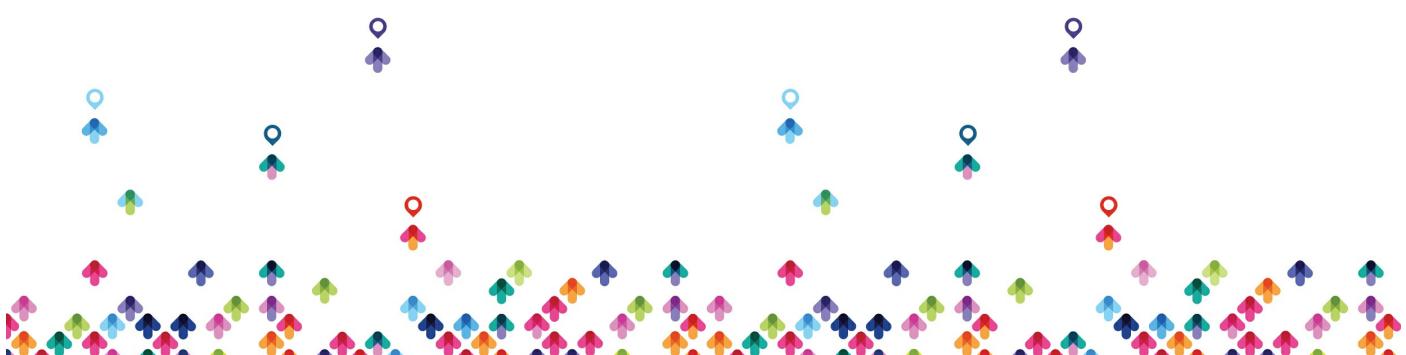
- برای ورود به این حوزه، معمولاً داشتن مدرک کارشناسی در رشته‌هایی مثل امنیت اطلاعات، فناوری اطلاعات، علوم کامپیوتر یا مهندسی کامپیوتر توصیه می‌شود. البته دقت شود داشتم مدارک دانشگاهی مناسب اما شرط لازم و کافی نمی‌باشد.
- علاوه بر تحصیلات دانشگاهی، مدارک حرفه‌ای امنیتی به مانند دوره‌های ISMS, SANS, Cisco Security و Pack پیشنهاد داده می‌شود. پیشنهادی ارزنگ پوشش کاملی از دوره‌هی SANS می‌باشد که باعث تجهیز شدن دانشجو به دانش لازم جهت اخذ این حرفه است.

مهارت‌های ارتباطی و تحلیل

- تحلیلگر امنیت سایبری باید توانایی گزارش‌دهی دقیق و انتقال مفاهیم پیچیده امنیتی به زبان ساده برای تیم‌های غیرفنی را داشته باشد.
- مهارت‌های تحلیلی قوی برای شناسایی الگوها و رفتارهای غیرمعمول در سیستم‌ها و پیش‌بینی و جلوگیری از حملات، ضروری هستند.
- جهت این دو مهم پیشنهاد داده می‌شود، دانشجو دوره‌های SoftSkill ارزنگ را حتماً جهت افزایش مهارت‌های غیر فنی در نظر داشته باشد.

یادگیری مداوم و به‌روز بودن

- دنیای امنیت سایبری بسیار پویاست و تهدیدات و روش‌های حمله دائمًا تغییر می‌کنند. بنابراین، یادگیری مداوم و به‌روز نگهداشت دانش و مهارت‌ها امری ضروری است.
- شرکت در دوره‌های آموزشی آنلاین، خواندن مقالات و گزارش‌های امنیتی، و تعامل با جامعه امنیت سایبری به شما کمک می‌کند تا با تهدیدات جدید آشنا شوید و مهارت‌های خود را تقویت کنید.



خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۰۵۰ - ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

فرصت‌های شغلی و رشد در حوزه امنیت سایبری

- تحلیلگر امنیت سایبری یکی از مشاغل پر تقاضا و با فرصت‌های شغلی متنوع است. از صنایع مالی و بانکی گرفته تا بهداشت و درمان، دولتی و فناوری اطلاعات، همگی به تحلیلگران امنیت نیاز دارند.
- در این مسیر شغلی می‌توانید پس از کسب تجربه به سطوح بالاتری مانند مدیر امنیت اطلاعات، مهندس امنیت شبکه یا حتی مدیر امنیت سایبری ارتقا پیدا کنید.

سطح درآمد و مزايا

- با توجه به اهمیت این شغل در سازمان‌ها و تقاضای بالای آن، تحلیلگران امنیت سایبری معمولاً از سطح درآمد مناسبی برخوردار هستند. میزان درآمد بسته به میزان تجربه، مدارک و مهارت‌های شما و همچنین نوع سازمان متفاوت است.

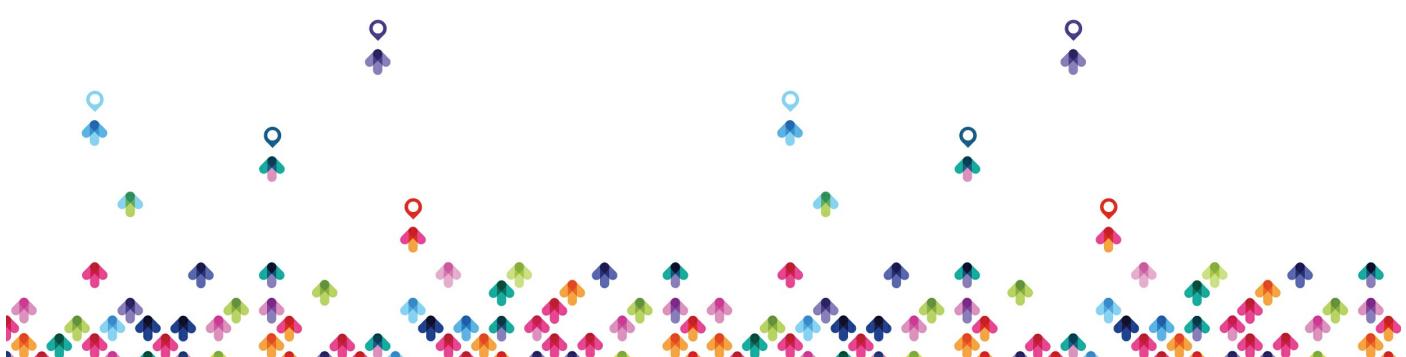
پذیرش مسئولیت‌های زیاد و استرس کاری

- یکی از چالش‌های اصلی این مسیر شغلی، پذیرش مسئولیت زیاد و همچنین استرس ناشی از مقابله با تهدیدات امنیتی و وقوع رخدادهای امنیتی است. شما باید آمادگی برخورد با شرایط بحرانی و اضطراری را داشته باشید و توانایی مقابله با فشارهای کاری را تقویت کنید. با تمام این شرایط باز تاکید می‌شود جدا از Pack امنیت که باعث تجهیز دانشجو به دانش فنی می‌شود حتما دوره‌های Soft Skill ارزشگ را نیز دانشجو شرکت کند و خود را به مهارت‌های کنترل شرایط بحران تجهیز کند.

آمادگی برای کار تیمی و همکاری بین‌بخشی

- تحلیلگر امنیت سایبری غالب با تیم‌های مختلف از جمله تیم توسعه، شبکه، و مدیریت همکاری می‌کند تا استراتژی‌های امنیتی سازمان را پیاده‌سازی و نظارت کند. بنابراین مهارت کار تیمی و همکاری بین‌بخشی برای این موقعیت بسیار حائز اهمیت است.

آنچه در این دوره خواهید آموخت



خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۰۵۰ - ۸۸۹۹۵۳۴۸ | ۰۷۵ - ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- مفاهیم امنیتی (Firewalls, IDS/IPS)
- امنیت شبکه و اطلاعات
- مدیریت ریسک و حوادث

