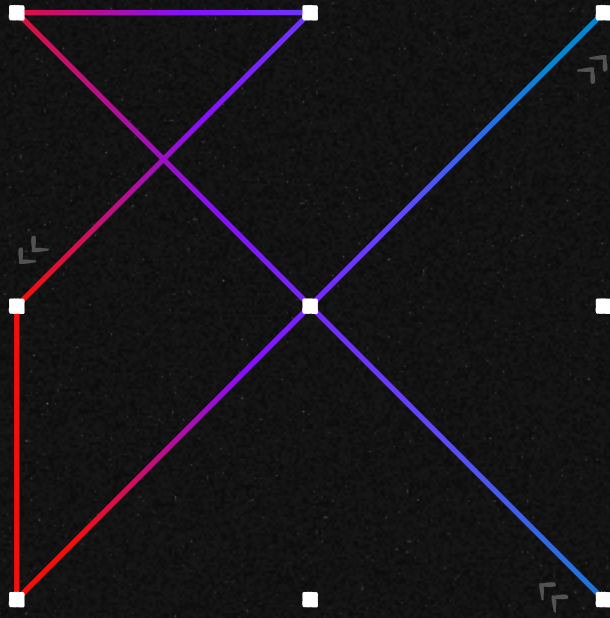


ورود بہ دنیاے امنیت سائبرے



ENTERING THE 0118



آکادمی سائبر سکیورٹی

CYBER SECURITY WORLD

فهرست

۰۱	پیش‌گفتار
۰۲	امنیت سایبری چیست؟
۰۵	نقش امنیت سایبری در دنیای امروز چیست؟
۰۷	اشتغال در زمینه‌ی امنیت سایبری
۰۹	چشم‌انداز بازار کار در امنیت سایبری
۱۱	مشاغل موجود در امنیت سایبری
۱۳	پیشرفت شغلی در امنیت سایبری
۲۶	مهارت‌های غیر فنی مورد نیاز در امنیت سایبری
۳۵	چطور مسیر امنیت سایبری را شروع کنیم؟
۴۱	چطور امنیت سایبری را فرا بگیریم؟



Intro

پیش‌گفتار

اگر درس یا دانشگاه خود را به تازگی تمام کرده و به دنبال ورود به بازار کار باشید یا اگر در تلاش برای تغییر مسیر شغلی فعلی خود هستید؛ همواره تصمیم برای شروع یک مسیر جدید می‌تواند دله‌ره‌آور باشد. طی سال‌های اخیر، محبوبیت اشتغال در زمینه‌ی امنیت سایبری، هم با توجه به اهمیت آن برای دنیای امروز ما و هم به دلیل وجود یک بازار کاری داغ در سراسر دنیا، به‌طور قابل توجهی افزایش یافته است. اما امنیت سایبری چیست؟ برای افرادی که به دنبال شروع کردن یک حرفه در امنیت سایبری هستند، کدام مسیرهای شغلی در دسترس است؟ این افراد به چه مهارت‌هایی نیاز خواهند داشت و در مورد انتخاب شغل درست با چه چالش‌هایی روبرو خواهند بود؟

در این کتابچه تلاش کرده‌ایم تا جای ممکن به تمام این سوالات پاسخ دهیم. بنابراین، اگر تمایل دارید در زمینه‌ی امنیت سایبری شروعی حرفه‌ای و در امن‌سازی کردن دنیای جدید دیجیتالی که در آن زندگی می‌کنیم نقشی موثر داشته باشید، مطالعه‌ی این کتابچه می‌تواند به شما کمک کند.



امنیت سایبرے چیست؟

WHAT IS
CYBER SECURITY?



امنیت سایبری اصطلاحی در جامعه‌ی مدرن است که از رسانه‌های خبری تا دنیای سیاست و تجارت، در زندگی اغلب ما به گوشمان می‌خورد. بنابراین یافتن پاسخ قطعی برای درک امنیت سایبری در میان این همه بحث و بررسی، می‌تواند کمی دشوار یا شاید حتی گیج‌کننده باشد.

صورت سوال به ظاهر ساده است: امنیت سایبری چیست؟ اما به طور کلی هیچ تعریف مطلوب و یکسانی بین مراجع مختلف وجود ندارد. با این حال، اکثریت موافق هستند که امنیت سایبری، گسترش چیزی است که اغلب از آن به عنوان حفاظت از اطلاعات یا دارایی‌های اطلاعاتی یاد می‌شود. برای درک بهتر، نگاهی به تاریخچه‌ی امنیت سایبری می‌اندازیم. در سال ۱۹۶۱ اولین سامانه‌ی محافظت شده با رمز عبور، توسط محققان دانشگاه MIT ایجاد شد. امروزه این سامانه به نام سامانه‌ی اشتراک زمان سازگار یا CTSS شناخته می‌شود. به نظر بسیاری از متخصصان، این نقطه از تاریخ را می‌توان زادگاه امنیت اطلاعات در نظر گرفت. استفاده از رمز عبور که عمل محافظت از اطلاعات و سیستم‌های الکترونیکی را انجام داده و از دسترسی غیرمجاز به آن جلوگیری می‌کند.

پس از گذشت حدود یک دهه از آن روزها، محققان شروع به اتصال شبکه‌های رایانه‌ای به شبکه‌ی ARPANET کردند. این شبکه به شکلی طراحی شده بود که به شبکه‌های کامپیوتری دیگر در مناطق جغرافیایی بزرگ اجازه می‌داد تا به طور سریع و قابل اطمینان با هم ارتباط برقرار کنند و داده‌ها را به اشتراک بگذارند. همان‌گونه که مشخص است، ARPANET شروعی بوده است برای آن‌چه که ما امروزه به اسم اینترنت می‌شناسیم.

پس از آن در سال ۱۹۸۸، سه سال قبل از این‌که اینترنت در دسترس همه قرار بگیرد، محقق‌ی به نام رابرت موریس تصمیم گرفت مخاطرات امنیتی که متوجه رایانه‌های تحقیقاتی متصل به اینترنت بود را بررسی و به دیگران معرفی کند. در همین راستا نرم‌افزاری طراحی کرد که خود را در سراسر سیستم‌های رایانه‌ای متصل به اینترنت پخش کند.

این نرم افزار از برخی نقص های امنیتی موجود در سیستم عامل یونیکس برای نصب و ادامه ی تکرار خود بهره برداری می کرد. در واقع موريس برای رسیدن به اهداف خود، اولین کرم اینترنتی را ایجاد کرده بود. البته دامنه ی گسترش این کرم اینترنتی از دست موريس خارج و سبب شد تعداد زیادی از سیستم های آلوده، غیرقابل استفاده شوند. این کار نه تنها باعث شد موريس اولین فردی باشد که طبق قانون کلاه برداری و سواستفاده رایانه ای در سال ۱۹۸۶ به جرم سایبری محکوم می شود، بلکه سبب ایجاد یک تیم واکنش سریع رایانه ای (CERT) در دانشگاه Carnegie Mellon، تحت حمایت مالی دولت فدرال ایالات متحده شد.

ایجاد این تیم پاسخگویی به حوادث رایانه ای یا همان CERT را می توان تولد چیزی دانست که اکنون ما آن را با نام امنیت سایبری می شناسیم. بنابراین، اگر بخواهیم یک تعریف مطلوب از امنیت سایبری داشته باشیم می گوییم، امنیت سایبری شامل مجموعه ای از تحقیقات، فناوری ها و فرآیندهایی است که در زمینه ی محافظت از سامانه های متصل به هم، داده ها و افراد در برابر حملات سایبری، استفاده ی غیرمجاز و آسیب یا اختلال، کاربرد دارند.

معنی لغوی امنیت سایبری سازمانی را می توان به این صورت نیز تعریف کرد: «حفاظت از اطلاعات الکترونیکی، شبکه و سیستم های کامپیوتری یا به طور کلی هر گونه اطلاعات محرمانه در برابر سرقت یا افشا و تغییر غیرقانونی و همچنین حفاظت از دسترس پذیری سرویس های سازمان». با توجه به ضریب بالای نفوذ فناوری اطلاعات در جوامع امروزی، امنیت سایبری برای تمام اقشار جامعه از سازمان های دولتی گرفته تا شرکت های بزرگ و کسب و کارهای کوچک، کارمندان و حتی افراد داخل منزل هم از اهمیت بالایی برخوردار شده است.

نقش امنیت سایبرے در دنیاے امروز چیست؟

WHAT IS THE ROLE OF
CYBER SECURITY IN
TODAY'S WORLD?



هدف امنیت سایبری، تا حد قابل توجهی به زمینه‌ای بستگی دارد که قرار است در آن اعمال شود. زمانی که در رسانه‌ها از امنیت سایبری صحبت می‌شود، اغلب از دیدگاه حفاظت از کسب و کارها و جلوگیری از نفوذ مجرمان سایبری به سازمان‌ها، به آن نگاه می‌شود. با این حال، موضوع امنیت سایبری در حقیقت بخش‌های مختلف یک جامعه‌ی دیجیتالی را شامل می‌شود. به عبارت دیگر این موضوع از امنیت در انتخابات و امنیت ملی گرفته تا حفاظت از حریم خصوصی آنلاین هر فرد در فضای مجازی را در بر می‌گیرد. می‌توان گفت امنیت سایبری مسئول تضمین عملکرد بدون اختلال و امن در تمام جنبه‌های یک جامعه‌ی سایبری است. امروزه امنیت سایبری تا اندازه‌ای در زندگی ما نقش دارد که گاه حتی دیگر وجود آن به چشمان نمی‌آید.

ما در جهانی با حجم ارتباطات بی‌سابقه زندگی می‌کنیم. هر سال وسایل و تجهیزات بیشتری را می‌بینیم که به اینترنت متصل می‌شوند و این در حالیست که تقریباً تمام بخش‌های زندگی ما به صورت الکترونیکی در حال ردیابی است. به عنوان مثال می‌توان به سوابق پزشکی ما، اطلاعات مالی، مصرف انرژی، چیزی که می‌پوشیم، ساعتی که به منزل می‌رسیم، جایی که به آن سفر می‌کنیم و هزاران مورد دیگر اشاره کرد. با استفاده از اطلاعات صحیح، ماشین‌ها می‌توانند با ایجاد پروفایل‌ها، درک بهتری از زندگی ما داشته باشند حتی ممکن است ما را بهتر از خودمان بشناسند. بنابراین میزان اهمیت محافظت از این اطلاعات در برابر دسترسی غیرمجاز توسط افراد سودجو (و خرابکار) به یک موضوع حیاتی تبدیل شده است.

از طرف دیگر با توجه به این که حملات سایبری امروزی، پتانسیل بالایی در آسیب زدن یا حتی از بین بردن یک کسب و کار دارند لذا بسیاری از سازمان‌ها، فراگیری دانش امنیت سایبری و جذب نیروهای متخصص در این زمینه را در اولویت‌های بالای خود قرار داده‌اند. خلاصه‌ی همه‌ی آن‌چه که تا این جا گفته شد این است: امروزه تقاضای سازمان‌ها و شرکت‌ها برای جذب متخصص امنیت سایبری نسبت به هر زمانی در گذشته، بیشتر بوده و حجم این تقاضا کماکان رو به رشد است.

اشتغال در زمینه امنیت سایبر

EMPLOYMENT IN THE FIELD
OF CYBER SECURITY



در این بخش نوبت آن رسیده است که به مشاغل موجود در حوزه امنیت سایبری بپردازیم و به این سوال پاسخ دهیم که آیا همه ی افراد علاقه مند (حتی آن هایی که سابقه ی کاری در سایر زمینه های فناوری اطلاعات ندارند) می توانند به این حوزه وارد شوند؟

نکته ی مهم اول که باید به آن توجه کنیم این است که در نظر گرفتن کل امنیت سایبری به عنوان یک مسیر شغلی خاص، دیدگاه اشتباهی است. در حقیقت امنیت سایبری شامل ده ها مسیر تخصصی مختلف می شود که هر کدام، به یک موقعیت شغلی مشخص منتهی خواهد شد. نیاز به متخصصان مختلف امنیت روز به روز در حال افزایش است و هیچ نشانه ای مبنی بر عدم نیاز یا کم شدن آن در آینده ی نزدیک مشاهده نمی شود. بلکه برعکس، برای افرادی که به دنبال یادگیری این مسیرهای تخصصی هستند، می توان آینده ای روشن را متصور بود.

اگر فکر می کنید که برای اشتغال در امنیت سایبری حتما به یک یا چند مدرک آموزشی و چند سال سابقه در یکی از زمینه های فنی نیاز دارید، باید دیدگاه خود را اصلاح کنید. البته در برخی از نقش های کاری مانند امنیت شبکه، داشتن سابقه ی کار در زمینه های غیر امنیتی مانند مدیریت یا پیاده سازی شبکه می تواند بسیار مفید باشد، اما این موضوع در خصوص تمام رشته های امنیت سایبری صدق نمی کند. علاوه بر آن یک تیم کامل امنیتی به ترکیب متفاوتی از دانش های مختلف مانند حقوقی، فنی، مدیریت مخاطرات و دانش سازمانی احتیاج خواهد داشت. به همین دلیل در امنیت سایبری، گستره ی وسیعی از انواع فرصت های شغلی هم برای متخصصین فنی و هم برای متخصصین غیر فنی وجود دارد.

Andy Ellis مدیر ارشد امنیت سایبری شرکت Akamai می گوید: «اغلب افراد، تنها اپراتورهای فنی و مهندسان پشتیبان را به عنوان مسیرهای شغلی اصلی در امنیت می شناسند، اما امنیت سایبری به مدیر برنامه، توسعه دهنده ی نرم افزار، متخصص ارتباطات، متخصص تحلیل داده، تحلیل گر سیستم، مدیر پروژه و بسیاری از تخصص های دیگر نیز احتیاج دارد». به این موارد می توان عناوین دیگری مانند معمار امنیت، مهندس فروش و غیره را نیز اضافه کرد.

چشم انداز بازار کار در امنیت سایبر

JOB MARKET OUTLOOK IN
CYBERSECURITY



با توجه به حجم فزاینده‌ی تقاضا برای امنیت دیجیتال، جای تعجب نیست که پتانسیل مشاغل موجود در امنیت سایبری دنیا از همیشه بیشتر شده است. چشم انداز بازار کار برای متخصصان صنعت امنیت سایبری در بسیاری از کشورها بسیار امیدوار کننده است به طوری که در حال حاضر اغلب صنایع دیگر، چنین چشم اندازی را در پیش روی خود ندارند.

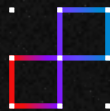
گزارشات ارایه شده توسط دفتر «آمار کار آمریکا» نشان می دهد که رشد مشاغل موجود در امنیت سایبری بین سال های ۲۰۱۸ تا ۲۰۲۸ از میانگین صنایع دیگر بسیار بیشتر خواهد بود. در حالی که میانگین رشد برای بقیه ی حرفه ها در آمریکا ۵٪ است، این رشد برای تحلیل گران امنیت حدود ۳۲٪ پیش بینی شده است. در همین راستا مطالعه ی انجام شده درباره ی نیروی کار امنیت سایبری توسط موسسه ISC2 در سال ۲۰۱۹ نشان می دهد تعداد جایگاه های پر نشده ی شغلی در آن سال ۴ میلیون و در سال گذشته ۲/۹۳ میلیون بوده است.

در ایران نیز با توجه به رشد فناوری اطلاعات در سازمان ها و افزایش تعداد شرکت های بزرگ فناوری محور از یک سو و گسترش چشم گیر حملات سایبری رخ داده در سال های اخیر از سوی دیگر، استخدام متخصصین امنیت، رشد بسیار بالایی را در این سال ها تجربه کرده است. به گونه ای که تعداد جایگاه های شغلی بسیار بیشتر از تعداد متخصصین امنیت سایبری بوده و همین امر چالش هایی را برای سازمان ها و شرکت های مختلف به وجود آورده است.

پیامدهای کمبود نیروی متخصص امنیت سایبری، برای سازمان ها می تواند بسیار شدید باشد. با رشد روز افزون فناوری اطلاعات و ارتباطات در کسب و کار سازمان ها و شرکت ها، مقابله و محافظت از دارایی های آن ها در برابر تهدیدات سایبری، همواره به عنوان یکی از چالش های اساسی هر کسب و کاری خواهد بود. اگر شما به دنبال شغلی هستید که بتوانید به صورت مشخص تاثیرات کار خود را در محیط اطرافتان مشاهده کرده و از چالش های کاری نیز استقبال می کنید، شروع به یادگیری در مسیر تخصص های امنیت سایبری می تواند برای شما مسیر مناسبی باشد.

مشاغل موجود در امنیت سایبرے

CAREERS IN CYBER SECURITY



از آنجایی که صنعت امنیت سایبری بسیار گسترده است، مسیرهای شغلی متفاوتی برای مبتدیان در این راه وجود دارد. بازه‌ی حقوقی این مشاغل بر اساس نوع شغل و نقش مورد نظر بسیار متفاوت است که از عوامل تاثیر گذار بر روی این مساله می‌توان به سطح تخصص مورد نیاز، پیچیدگی و سطح حساسیت کار، سازمان استخدام کننده، حجم تقاضای سازمان‌ها و غیره اشاره کرد.

به طور کلی تخصص‌های امنیت سایبری را می‌توان به سه گروه **امنیت دفاعی و امنیت تهاجمی و ترکیبی از این دو** تقسیم کرد. گروه اول با رنگ آبی، گروه دوم با رنگ قرمز و گروه سوم با رنگ بنفش نمایش داده می‌شود. **متخصصین گروه آبی** وظیفه‌ی امن سازی، شناسایی تهدیدات سایبری و پاسخ‌گویی به این تهدیدات را بر عهده دارند. در مقابل **گروه قرمز** (مانند متخصص تست نفوذ و عملیات تیم قرمز) وظیفه دارند تا با شبیه‌سازی رفتار نفوذگر یا هکر، آسیب‌پذیری‌ها و نقاط ضعف سایبری موجود در سازمان را شناسایی و گزارش کنند. **گروه بنفش** نیز جایگاهی بین دو گروه قبلی داشته و بخش از وظایف هر دو گروه را به همراه وظیفه‌ی ایجاد ارتباط بین آن دو، بر عهده دارند.

با توجه به موارد ذکر شده مشاغل موجود در زمینه‌ی امنیت سایبری می‌تواند در هر سازمان متفاوت باشد اما در این جا به برخی از متداول‌ترین آن‌ها اشاره می‌کنیم:

کارشناس امنیت عمومی General Security Operator



شخصی که همه‌ی کارهای مربوط به امنیت را در شرکت‌های کوچک‌تر بر عهده دارد. این فرد باید در زمینه‌های مختلف امنیت سایبری دانش سطحی داشته باشد تا بتواند امنیت نسبی کسب و کار را تامین یا بخشی از آن را برون‌سپاری کند.

تحلیل‌گر بدافزار Malware Analyst



تلاش می‌کنند تا با ابزارها و دانش‌های مختلف (مانند مهندسی معکوس) ماهیت و رفتار یک بدافزار مانند ویروس، تروجان، کرم و غیره را تحلیل کرده و همچنین شاخصه‌های آن را به منظور امکان شناسایی موارد مشابه در آینده، استخراج می‌کنند.

مهندس امنیت شبکه Network Security Engineer



نقشی که در سازمان‌های بزرگتر وجود دارد. این افراد در زمینه‌ی مدیریت امنیت زیرساخت شبکه شامل سخت‌افزار و نرم‌افزار از Firewall گرفته تا سیستم‌عامل‌ها و راهکارهای ارتباط از راه دور، فعالیت دارند.

متخصص امنیت نرم‌افزارهای کاربردی و پایگاه‌های داده Database Security Specialist



این افراد وظیفه دارند تا با ترکیب مهارت‌های خود در زمینه‌های نرم‌افزاری و سخت‌افزاری، امنیت مربوط به نرم‌افزارهای کاربردی، سرویس‌ها و پایگاه‌های داده‌ی سازمان را تامین کنند.

تحلیل‌گر مرکز عملیات امنیت SOC Analyst



متخصصان امنیت سایبری هستند که به عنوان بخشی از تیم SOC در راستای نظارت و مقابله با تهدیدات زیرساخت فناوری اطلاعات یک سازمان، ارزیابی سامانه‌ها، اقدامات امنیتی برای شناسایی و بهبود نقاط ضعف، پاسخ به تهدیدات شناسایی شده و غیره فعالیت می‌کنند. وظایف تحلیل‌گران SOC با توجه به سطح دانش و تجربه‌ی آن‌ها در سه سطح مختلف تعریف می‌شود.

مهندس امنیت ابری Cloud Security Engineer



همان طور که از عنوان این شغل برمی آید، این افراد امنیت سایبری را در زیرساخت ها و پلتفرم های ابری تامین می کنند. این سمت شغلی هنوز در داخل ایران چندان شناخته شده نیست، اما توسعه ی آن در آینده ی نزدیک اجتناب ناپذیر خواهد بود.

ارزیاب امنیت سایبری Cyber Security Auditor



این متخصصان بهره وری ساختار امنیت سایبری سازمان را ارزیابی کرده و راه حل هایی را برای بهبود آن پیشنهاد می دهند. نقش این افراد با متخصصان تست نفوذ متفاوت است، به گونه ای که آن ها اغلب با بهره برداری از استانداردهای سطح بالا و شناخته شده، امنیت سازمان یا یک سامانه را بررسی و تحلیل می کنند.

متخصص پاسخ به رخداد های سایبری Cyber Incident Responder



در صورت شناسایی هرگونه رخداد سایبری، این افراد اولین کسانی هستند که وظیفه ی بررسی، اقدام مناسب در راستای مقابله با تهدید و رفع و کاهش آثار رخداد را بر عهده دارند.

متخصص ردیابی مهاجم سایبری Digital Forensic Specialist



در صورت شناسایی یک حمله یا خراب کاری سایبری، این فرد وظیفه دارد تا با جمع آوری و تحلیل مدارک موجود به ردیابی فرد (یا تیم) خراب کار و مهاجم پرداخته و در صورت نیاز این مدارک را به مراجع قانونی ارائه دهند.

متخصص رمزنگاری Encryption Specialist



این افراد وظیفه‌ی رمزنگاری اطلاعات سازمان را به منظور حفظ محرمانگی و یکپارچگی داده‌ها در برابر افراد خراب‌کار و سودجو بر عهده دارند. این موارد شامل رمزنگاری داده‌های ذخیره شده و داده‌های در حال انتقال می‌شود.

کارشناس ارزیابی مخاطرات سایبری Cyber Risk Auditor



این افراد اطلاعات دارایی‌های سازمان را جمع‌آوری کرده و مخاطرات سایبری که متوجه هر یک از این دارایی‌ها هست را شناسایی، تحلیل و مستندسازی می‌کنند تا به تصمیم‌گیری سازمان در راستای اولویت‌بندی و امن‌سازی آن‌ها کمک کند.

شکارچی تهدیدات سایبری Cyber Threat Hunter



متخصصان امنیت ماهره‌ی که به صورت فعال در زیرساخت فناوری اطلاعات سازمان به دنبال ردپایی از هکرها هستند تا تهدیدات سایبری را قبل از ایجاد مشکلات جدی در زیرساخت سازمان، شناسایی و خنثی کنند.

متخصص تست نفوذ وب، موبایل یا شبکه Penetration Testing Specialist



این افراد با شبیه‌سازی رفتار هکر، تلاش می‌کنند تا به صورت قانونی به یک سامانه نفوذ کرده و آسیب‌پذیری‌های احتمالی موجود در یک سرویس نرم‌افزاری یا زیرساخت ارتباطی را شناسایی و گزارش کنند.

متخصص تیم قرمز Red Team Specialist



با شبیه سازی رفتار تیم های APT (تیم های مهاجمی که اغلب تحت حمایت دولت ها فعالیت می کنند) تلاش می کنند تا نقاط ضعف امنیتی موجود در زیر ساخت و افراد سازمان را شناسایی نمایند. این تخصص تا حدی مشابه تخصص تست نفوذ است، با این تفاوت که در سطحی بالاتر و اغلب با همکاری تیمی از متخصص های مختلف امنیتی انجام می شود.

علاوه بر موارد ذکر شده، تعداد بسیاری زیادی از عناوین شغلی دیگر در زمینه ی امنیت را نیز می توان تعریف کرد که به دلیل پیش گیری از طولانی شدن بحث، از ذکر تمام آن ها خودداری شده است. در اینجا تنها به تعدادی از مهم ترین و پرمخاطب ترین عناوین شغلی موجود، به منظور آشنایی اولیه اشاره کردیم. در صورت علاقه، با یک جستجوی ساده در اینترنت می توانید با سایر سمت های شغلی نیز آشنا شوید.

عناوینی که تا این جا به شرح آن ها پرداختیم اغلب به صورت شغل های تمام وقت هستند، اما در امنیت سایبری عناوین شغلی نیز وجود دارند که بدون نیاز به استخدام در یک سازمان مشخص می توان به آن ها مشغول شد و کسب درآمد کرد. در حالت کلی به این مشاغل، شغل های Freelance و به افرادی که به این صورت کار می کنند Freelancer گفته می شود. یکی از پرمخاطب ترین مشاغل نیمه وقت یا Freelance در امنیت سایبری، شکارچی باگ یا Bug Hunter است که در برنامه های باگ بانتری (Bug Bounty) شرکت می کند.

باگ بانتری نام فرآیندی است که طی آن، شما سرویس ها یا نرم افزارهای یک سازمان را به صورت قانونی از بیرون ارزیابی کرده و برای شناسایی آسیب پذیری های احتمالی موجود در آن ها تلاش می کنید. در صورت شکار آسیب پذیری یا باگ، آن را به شرکت واسط یا خود سازمان مربوطه (بستگی به برنامه ی باگ بانتری

دارد که در آن شرکت کرده‌اید) گزارش کرده و در صورت تایید آسیب‌پذیری، مبلغی را به عنوان جایزه دریافت می‌کنید. برخی از شرکت‌های بین‌المللی و ایرانی که می‌توانید با ثبت نام در آن‌ها، مسیر باگ‌بانتی خود را شروع کنید به شرح زیر است:



hackerone.com



ravro.ir



bugcrowd.com



bugdasht.ir

افراد بسیاری به صورت تمام وقت به باگ‌بانتی مشغول هستند، برخی دیگر نیز در کنار شغل اصلی خود به شرکت در این برنامه‌ها می‌پردازند. شرکت در برنامه‌های باگ‌بانتی علاوه بر کسب درآمد، یک روش بسیار مناسب برای تمرین و ارزیابی توانمندی‌های شخصی نیز برای متخصصین تست نفوذ به حساب می‌آید. علاوه بر باگ‌بانتی می‌توان به مشاغل پاره وقت دیگری مانند مشاوره، آموزش، و غیره نیز در زمینه‌ی امنیت سایبری اشاره کرد.

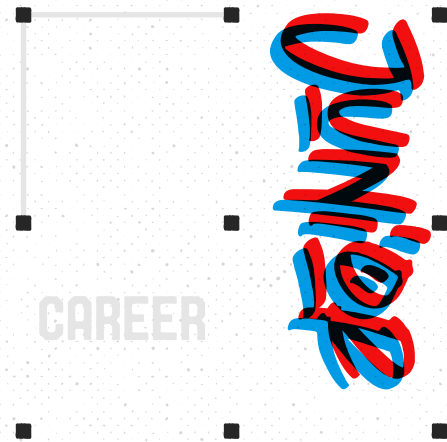
پیشرفت شغلے در امنیت سایبرے

CAREER ADVANCEMENT IN
CYBER SECURITY



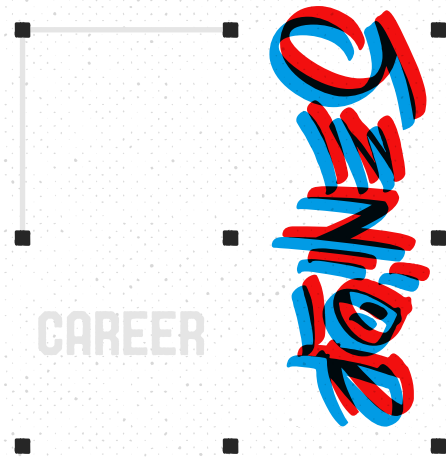
وقتی درباره‌ی پیشرفت شغلی صحبت می‌کنیم، منظورمان این است که به مرور زمان از جایگاه‌های شغلی در سطوح تخصصی پایین به سمت جایگاه‌های با تخصص بالاتر، حرکت کنیم. برای درک بهتر این پیشرفت، بهتر است مهارت‌های کلیدی و اصلی مورد نیاز برای افرادی که در جایگاه‌های شغلی مختلف امنیت فعالیت می‌کنند را بررسی کرده و بشناسیم.

وقتی فردی به دنبال یک مسیر شغلی جدید است، اغلب قبل از شروع کار خود به اهداف بزرگ فکر می‌کند. به عبارت دیگر افرادی که به دنبال شغل جدید هستند، ابتدا خود را در 5 یا 15 سال آینده تصور می‌کنند که در صورت موفقیت شغلی در کجا قرار خواهند داشت. آینده‌نگر بودن برای هر کسی که در یک مسیر شغلی جدید قرار می‌گیرد بسیار مهم است. آینده‌نگر بودن به ما اجازه می‌دهد مسیری را برای خود تصور و سپس اهداف کوتاه مدت خود را تعیین کنیم، تا بتوانیم وضعیت خود را در طول مسیر مورد سنجش قرار دهیم. همچنین به ما انگیزه می‌دهد تا به عنوان یک فرد حرفه‌ای به تلاش و پیشرفت در مسیر شغلی خود ادامه دهیم. در همین راستا نگاهی به سطوح مختلف شغلی در صنعت امنیت سایبری خواهیم داشت.



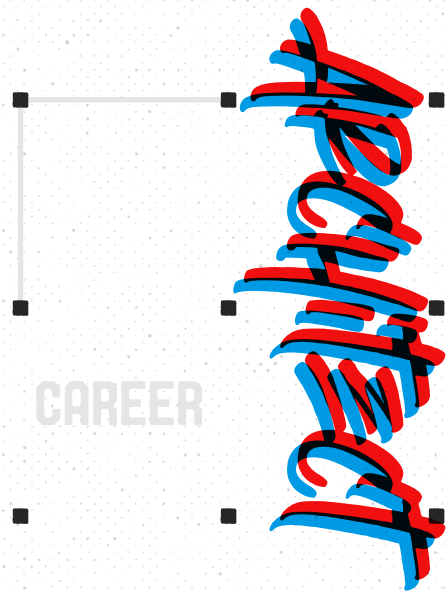
مشاغل سطح پایه

مشاغل سطح پایه را می‌توان نقطه‌ی شروع اشتغال در هر مسیر شغلی در نظر گرفت. در واقع این جایگاه‌های شغلی، مسیر ورود شما به دنیای امنیت سایبری هستند. در اینجا، انتظارات زیادی در خصوص تجربه‌ی کاری شما وجود ندارد و در عوض تمرکز بیشتر بر روی مجموعه‌ی مهارت‌های اصلی که در این جایگاه نیاز است و همچنین استعداد شما در یادگیری، معطوف خواهد بود. البته در صنعت امنیت سایبری، با توجه به حساسیت بالای آن در سازمان‌ها، پیدا کردن مشاغل پایه که بدون وجود تجربه‌ی کار به شما اعتماد کنند شاید کمی دشوارتر از سطوح شغلی دیگر باشد.



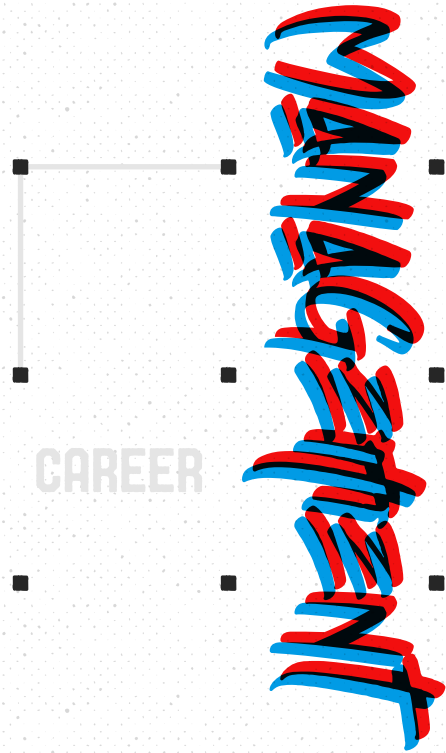
جایگاه‌های شغلی ارشد

زمانی که متخصصان امنیتی در طول مسیر شغلی خود تجربه‌ی کافی را کسب می‌کنند، به سمت عناوین شغلی که اغلب به عنوان موقعیت‌های سطح ارشد شناخته می‌شود، حرکت خواهند کرد. بسته به جایگاه شغلی، کارفرمایان ممکن است بین پنج تا هشت سال تجربه کاری مرتبط را برای استخدام در یک جایگاه ارشد، مدنظر قرار دهند. فردی که یک جایگاه ارشد قرار می‌گیرد مسئولیت بیشتری خواهد داشت. این افراد ممکن است نقش رهبری را در برخی پروژه‌های خاص بر عهده گرفته یا به عنوان مربی برای سایر افراد کم‌تجربه‌تر در سازمان عمل می‌کنند. اگر به موقعیت‌های شغلی موجود در بازار امنیت نگاه کنیم، خواهیم دید که یکی از رایج‌ترین موقعیت‌های موجود برای استخدام، همین نقش‌های ارشد هستند.



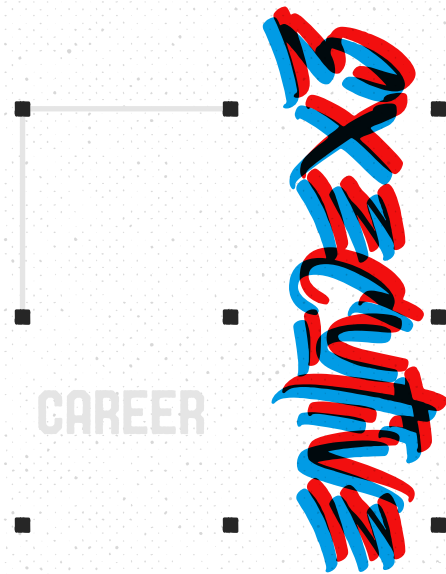
جایگاه شغلی معمار

جایگاه معمار امنیت، به دانشی فراتر از تخصص امنیتی در یک حوزه‌ی خاص نیاز دارد. در واقع قرار گرفتن در این جایگاه شغلی، مستلزم مجموعه‌ی وسیعی از دانش امنیت سایبری شامل آشنایی با فناوری‌های مختلف، اصول امنیتی آن‌ها و همچنین آشنایی با محدودیت‌ها و مشکلات سازمانی است. معماران، مسئول طراحی امنیت در سطح بالا هستند. آن‌ها باید فناوری‌های مختلف را مد نظر داشته و راهکارهایی را به وجود بیاورند که تکنیک‌های دفاعی متنوعی را در خود جای داده است. در نتیجه این جایگاه می‌تواند بسیار پرحاشیه باشد و به همین دلیل برای تصدی آن نیاز است تا تجربه‌ی کاری حداقل 10 سال یا بیشتر را در نظر گرفت. در صنعت امنیت سایبری کمتر به استخدام در این موقعیت شغلی بر خواهید خورد.



راهبری امنیتی

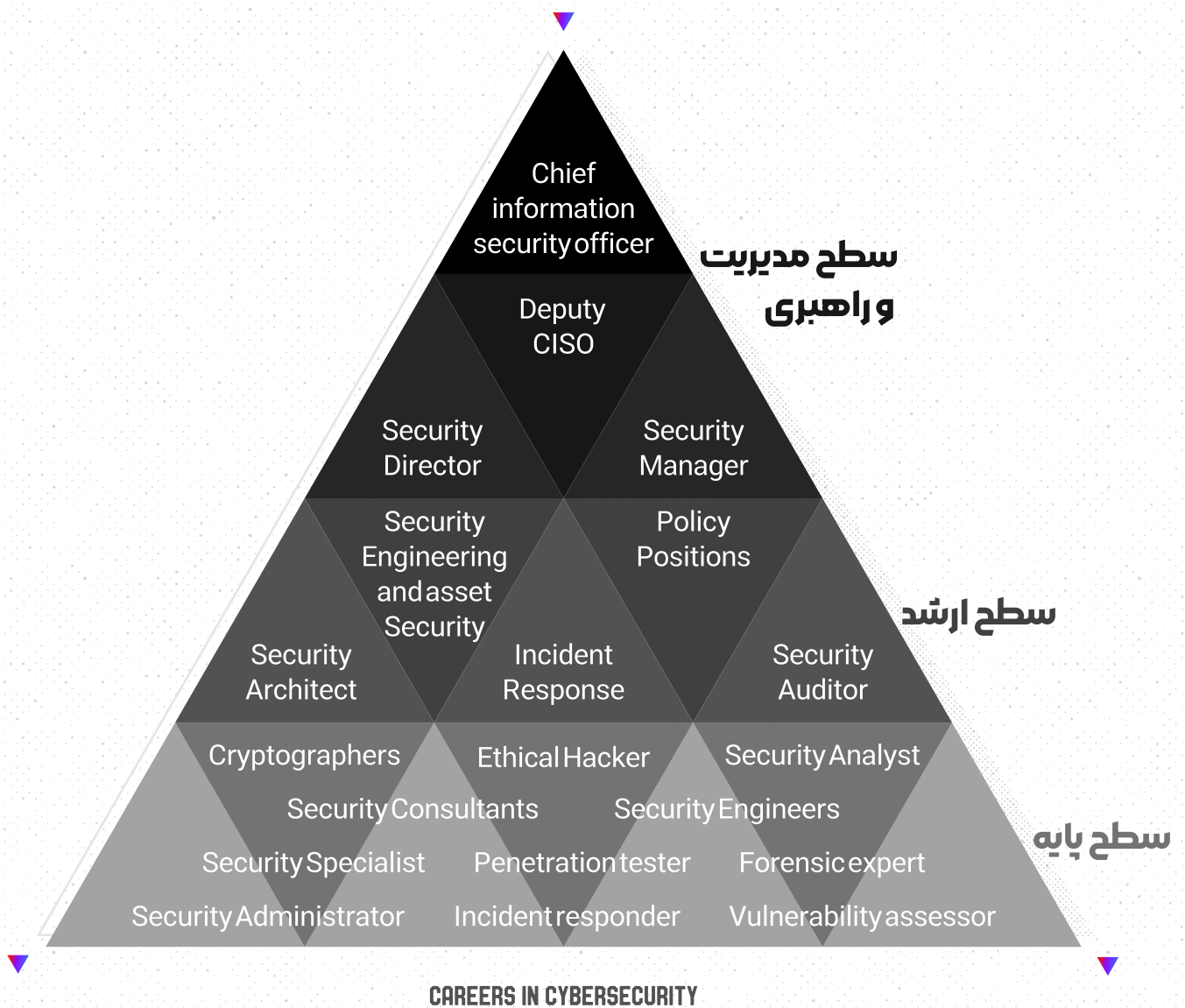
حرکت از جایگاه یک بازیگر فردی در امنیت به سمت جایگاهی که شامل همکاری و نظارت بر دیگر متخصصان است را می‌توان یک هدف شغلی یا نقطه‌ی عطفی در نظر گرفت که بسیاری از افراد به دنبال آن هستند. حرکت به سمت جایگاه مدیریتی می‌تواند اشکال مختلفی داشته باشد و این مسیر در یک سازمان نسبت به سازمان دیگر متفاوت است اما در اغلب موارد، گام اول از رهبری یک تیم شروع می‌شود. این نقش اغلب اوقات یک عنوان رسمی ندارد. در عوض ممکن است به یک فرد ارشد یا یک متخصص، نقش رهبری تیمی داده شود، اگرچه شاید عنوان شغلی آن‌ها تغییری نکند. این جایگاه رهبری، با توجه به استعداد و دانش فرد می‌تواند با گذشت زمان به سمت رهبری تیم‌های بزرگتر یا بیشتر حرکت کند.



راهبری اجرایی امنیت

جایگاه شغلی راهبری اجرایی امنیت سایبری، اغلب به جایگاه مدیر ارشد یا معاونت در سازمان و نقش‌های تخصصی مانند CISO اشاره دارد. بسیاری از کسانی که در زمینه‌ی امنیت سایبری کارشان را آغاز کرده‌اند، به جایگاه CISO به عنوان هدف نهایی در مسیر شغلی خود نگاه می‌کنند. برای گرفتن این جایگاه، علاوه بر دانش امنیت سایبری باید با تخصص‌های دیگری مانند مدیریت پروژه، برنامه‌ریزی و استراتژی و مواردی از این دست نیز آشنایی داشته باشید.

به طور کلی، می‌توان سطوح مختلف مسیر شغلی در امنیت سایبری را در شکل زیر به صورت خلاصه مشاهده کرد.



مہارت ہائے غیر فنی مورد نیاز در امنیت سایبرے

SOFT SKILLS REQUIRED IN
CYBER SECURITY



مهارت‌های فنی در یافتن شغل امنیتی، یک موضوع بسیار مهم به حساب می‌آید اما این تمام ماجرا نیست. توانایی‌های دیگری نیز برای یافتن شغل و رشد در مسیر شغلی اهمیت دارد که خیلی فنی نیستند. این مهارت‌ها را به عنوان مهارت‌های نرم یا Soft Skills می‌شناسند. این توانایی‌ها ارتباطی به یک فناوری یا سامانه‌ی خاص ندارند، بلکه در تمام رشته‌ها مشابه هستند. به عنوان مثال می‌توان به شیوه‌ی ارتباط فرد با همکاران یا شیوه‌ی مدیریت وظایف کاری اشاره کرد. با این‌که ممکن است برخی سازمان‌های استخدام‌کننده، تمرکز خود را بر روی مهارت‌های فنی کارجو گذاشته و نسبت به مهارت‌های غیر فنی، کم‌توجهی کنند، اما در واقعیت تاثیر بالای این توانمندی‌ها در رشد شغلی شما، انکارناپذیر است.

به همین دلیل، بسیار مهم است که شما نه تنها برای چگونگی توسعه‌ی مهارت‌های فنی خود برنامه‌ریزی کنید، بلکه اطمینان حاصل کنید که مهارت‌های نرم خود را نیز به صورت مستمر بهبود خواهید بخشید. برخی مهارت‌های نرم می‌توانند شبیه به استعدادهای ذاتی باشند اما در واقع با تمرین و مطالعه می‌توان آن‌ها را تقویت کرد. در ادامه، مهم‌ترین مهارت‌های غیر فنی که در پیشرفت شغلی شما در مسیر امنیت سایبری موثر خواهند بود، به صورت خلاصه بررسی شده است.

RESEARCH Skills

مهارت تحقیق

توانایی تمرکز بر روی مساله‌ای که قصد دارید آن را بهتر درک کنید و تبدیل آن بخش‌های کوچک‌تر یا ساده‌تر به منظور پیدا کردن پاسخ برای آن‌ها، توانمندی بسیار مهمی در امنیت و به خصوص در امنیت دفاعی به حساب می‌آید. بهترین متخصصان امنیتی، افرادی هستند که یک موضوع یا موقعیت را تنها آن‌گونه که به نظر می‌رسد نمی‌پذیرند، بلکه به جای آن تلاش دارند تا درک درستی از ریشه و دلایل وجودی آن به دست آورند. این نوع از کنجکاوی، میل ما را برای تحقیق در مورد یک موضوع در راستای ایجاد درک عمیق‌تر از آن، تقویت می‌کند. در نتیجه زمانی که یک وضعیت را به طور کامل درک کنیم، خلاقیت و روحیه‌ی نوآورانه‌ی ما می‌تواند ایده‌های جدیدی در ذهنمان پیروارند. در خصوص اهمیت این موضوع باید بگوییم بدون مهارت تحقیق، نمی‌توانید به رشد بالا در مسیر امنیت سایبری امید زیادی داشته باشید.

PROBLEM SOLVING SKILLS

حل مساله

همان‌گونه که در بخش قبل نیز شرح داده شد، مهارت‌های حل مساله و تحقیق ممکن است شبیه به هم به نظر برسند، اما در واقع فقط مفاهیم مرتبطی هستند که یکی به دیگری منتهی می‌شود. بسیاری از افراد در تحقیق توانمند هستند اما نمی‌توانند یک مساله‌ی پیچیده را تجزیه و تحلیل کنند. بنابراین، مهم است که این دو مهارت را مجزا دانسته و توانایی‌های خود را در هر دو زمینه تقویت کنید.

COLLABORATION Skills

همکاری

توانایی کار کردن با سایر افراد در سراسر سازمان، برای کارشناسان امنیت سایبری، یک توانمندی حیاتی به حساب می‌آید. اهمیت این همکاری تا اندازه‌ای است که می‌تواند مرز بین ایجاد بهبود در امنیت سازمان یا گیر افتادن در یک نبرد قدرت همیشگی با افراد دیگر، در نظر گرفته شود. همکاری موثر مستلزم آن است که افرادی را که امکان همکاری با آن‌ها وجود دارد را شناسایی کرده و در انجام کار با آن‌ها به صورت موثر همراه شویم.

EMPATHY . EMOTIONAL INTELLIGENCE Skills

همدلی / هوش عاطفی

همدلی به معنی توانایی درک احساسات، انتظارات و نگرانی‌های فرد دیگر است. برای تاثیرگذاری بر دیگران، شما باید همدلی را با هوش هیجانی همراه کنید. این مهارت‌ها هنگام همکاری با دیگران، به شما اطمینان می‌دهند که بتوانید حمایت و همکاری کسانی که دوست دارید با آن‌ها کار کنید را با درک احساسات آن‌ها به دست آورید.

MULTITASKING AND ORGANIZATIONAL SKILLS

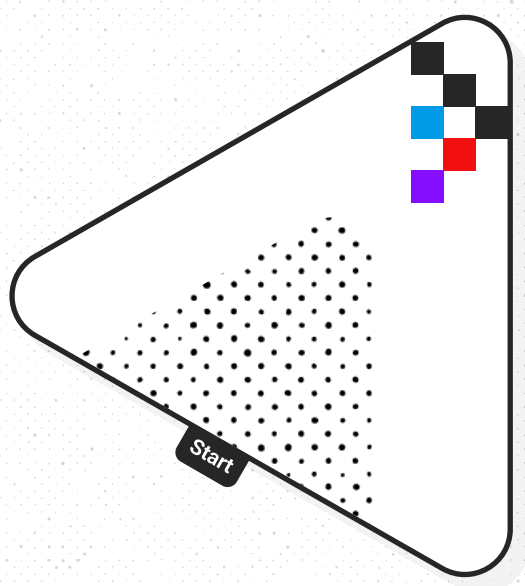
مهارت چند وظیفه‌ای بودن و سازمان‌دهی امور

شاید غیرممکن باشد که کسی را در یک جایگاه امنیت سایبری پیدا کنید و این احساس را نداشته باشد که هر روز مجبور است با فهرستی از وظایف متفاوت سروکله بزند. در هر شغل امنیتی شما با کارهای متعدد و اولویت‌های مختلف روبرو خواهید بود که باید به‌طور موازی روی آن‌ها کار شود. توانایی دریافت طیف گسترده‌ای از ورودی‌ها، سازمان‌دهی و اولویت‌بندی آن‌ها و سپس انجامشان یکی از مهارت‌های مهم در مشاغل امنیت سایبری است.

WRITING AND PRESENTATION Skills

مهارت نوشتن و ارائه مطلب

یک مهارت نرم دیگر که باید در نظر گرفته شود نوشتن است. چه شما یک ارزیاب امنیت باشید، چه پاسخ دهنده‌ی به رخداد یا حتی یک معمار امنیتی، باید بتوانید ایده‌ها، پیشنهادها و یافته‌هایتان را به شکل نوشتاری به دیگران منتقل کنید. مهارت نوشتن برای جلب حمایت دیگران بسیار حیاتی است. یک فرد فعال در زمینه‌ی پاسخ به رخداد که نمی‌تواند گزارشی قابل درک از یک رخداد امنیتی را به مدیران خود ارائه دهد تا تصمیم‌گیری در مورد استراتژی آینده‌ی امنیت سازمان را برای آن‌ها ممکن کند، در تاثیرگذاری نقش خود شکست خورده است. این موضوع برای اغلب جایگاه‌های شغلی امنیت سایبری صدق می‌کند.



اما فارغ از سمت شغلی، اگر
بخواهیم به دنیای امنیت سایبری
وارد شویم، از کجا باید شروع کنیم؟

چطور مسیر امنیت سایبرے را شروع کنیم؟

HOW TO START THE PATH OF
CYBER SECURITY?



راه‌های زیادی برای ورود به دنیای امنیت سایبری وجود دارد. برخی توصیه می‌کنند که از همان ابتدا باید کار را به صورت عملی شروع کرد و در حین اجرای عملی پروژه‌ها و ابزارها، دانش مورد نیاز را هم فرا گرفت. برخی هم توصیه می‌کنند که قبل شروع کار عملی، حتما باید یک سری از پیش‌نیازها را به صورت نظری آموخت. به نظر ما بسته به شرایط فرد، هر یک از دو حالت ذکر شده می‌تواند درست یا غلط باشد. فارغ از هر چیز، یک حقیقت غیرقابل انکار وجود دارد و این که تنها یک مسیر مشخص و جادویی برای ورود به دنیای امنیت وجود ندارد که همه افراد بتوانند از آن مسیر به متخصص امنیت تبدیل شوند. در ادامه به صورت خلاصه به چند سوال متداول در این زمینه پاسخ می‌دهیم:

آیا برای ورود به دنیای امنیت، حتما باید سابقه‌ی کار قبلی در زمینه‌ی فناوری اطلاعات داشته باشم؟



خیر، شما می‌توانید امنیت سایبری را به عنوان اولین مسیر آموزش یا شغلی خود انتخاب کنید. اگر چه سابقه‌ی کار قبلی در سایر زمینه‌های فناوری اطلاعات می‌تواند به شما کمک کند، اما الزامی نیست.

آیا برای موفقیت در دنیای امنیت سایبری، داشتن مدرک دانشگاهی یا یک مدارک تخصصی موجود در بازار الزامی است؟



خیر، بسیاری از افراد پیش‌رو در امنیت سایبری جهان، هیچ مدرک تجاری یا تخصصی ندارند. در خصوص مدرک دانشگاهی هم وضع به همین گونه است. به جای دریافت مدارک به منظور اثبات توانمندی، شما می‌توانید در پروژه‌های Open Source شرکت کرده یا در کنفرانس‌های معتبر، آخرین یافته‌های خود را ارائه دهید. البته بسیاری از شرکت‌های بزرگ، داشتن مدرک دانشگاهی را به عنوان یک الزام و مدارک تخصصی را به عنوان یک امتیاز در استخدام در نظر می‌گیرند، اما این موارد به این معنی نیست که بدون داشتن مدرک نمی‌توانید در یک شرکت بزرگ مشغول به کار شوید.

به چه مهارت‌هایی برای اشتغال در این زمینه نیاز داریم؟



مهارت‌هایی که باید آن‌ها را فرا بگیرید به جایگاه شغلی یا تخصصی که به دنبال آن هستید بستگی دارد. اما به طور کلی یک سری از مهارت‌ها فارغ از نوع تخصص شما در امنیت سایبری، مورد نیاز است که در بخش‌های بعد در خصوص آن‌ها بیشتر توضیح داده شده است.

چگونه باید در امنیت سایبری، تجربه کسب کنم؟



با مشارکت در پروژه‌های Open Source، حضور در برنامه‌های Bug Bounty، حضور در شرکت‌ها به عنوان کارآموز، ارائه‌ی پروژه‌های تحقیقاتی و توسعه‌ی ابزار و انتشار آن در کنفرانس‌ها، پلتفرم Github و سایر موارد مشابه می‌توان تجربه (و حتی شهرت) خوبی در زمینه‌ی امنیت سایبری به دست آورد. حضور در کلاس‌های آموزشی نیز می‌تواند در انتقال تجربه از دیگران، به شما کمک کند.

یک مسیر شغلی در امنیت سایبری را انتخاب کنید.

یکی از موارد هیجان‌انگیز درباره‌ی امنیت سایبری این است که ده‌ها مسیر متفاوت شغلی برای انتخاب وجود دارد و همان‌طور که در مطالب قبلی نیز به آن اشاره شد، برای ورود به آن‌ها نیازی به داشتن تجربه‌ی قبلی در سایر زمینه‌های فناوری نیست. اولین قدم برای انتخاب مسیر شغلی مناسب در حیطه‌ی امنیت سایبری این است که بر اساس تجربیات گذشته‌ی زندگی خود، نقاط قوت و ضعف‌تان را به همراه مهارت‌ها و علایق خود مشخص کنید. به عنوان مثال از خود بپرسید که آیا شخصی اجتماعی هستید؟ یا ترجیح می‌دهید توسعه دهنده‌ی برنامه باشید یا متخصص شبکه؟ و ده‌ها سوال دیگر.

فهرست کردن علایق و مهارت‌ها به شما کمک می‌کند تا نوع تخصصی که احتمال می‌دهید در آن بهترین عملکرد را خواهید داشت، راحت‌تر انتخاب کنید. زمانی که شما شروع به نوشتن گزینه‌های موجود می‌کنید، بهتر است که زمینه‌ی مورد علاقه‌ی خود را با جزییات کامل ارزیابی کرده و درباره‌ی آن به خوبی تحقیق کنید. می‌توانید کتاب‌ها یا مقالاتی را در آن زمینه‌ها خوانده (مانند کتاب‌های انتشارات no starch، Wiley، Packt و غیره) یا در سایت‌های کاریابی، شرح شغل و انتظارات کارفرماها را مطالعه کنید (مانند وبسایت indeed.com). در این خصوص می‌توانید از خدمات مشاوره‌ی آکادمی راوین نیز استفاده کنید.

مهارت‌های اصلی برای شروع یادگیری امنیت سایبری چیست؟

مانند اغلب شاخه‌های دیگر فناوری، یادگیری مهارت‌های اصلی برنامه‌نویسی می‌تواند نقطه‌ی شروع بسیار خوبی باشد. نیازی نیست شما حتما به یک متخصص برنامه‌نویسی تبدیل شوید، بلکه همین اندازه که قادر به خواندن و درک یک زبان برنامه‌نویسی باشید مزیت بسیار خوبی محسوب می‌شود. سایر مهارت‌های کلی که فارغ از تخصص مورد انتخاب، توصیه می‌شود یاد بگیرید به شرح زیر است:

دانش اولیه‌ی شبکه‌های کامپیوتری: درک ارتباطات کامپیوتری و شیوه‌ی انتقال اطلاعات در شبکه‌ها و اینترنت به شما در درک و اجرای پروژه‌های امنیتی کمک خواهد کرد. این موارد شامل آشنایی با لایه‌های شبکه، مسیریابی در لایه‌های مختلف، تجهیزات متداول در شبکه و سایر مفاهیم اولیه‌ی شبکه می‌شود.

آشنایی با پروتکل‌های پرکاربرد: برای درک شیوه‌ی عملکرد سرویس‌ها و ارزیابی یا امن‌سازی آن‌ها نیاز است تا با پروتکل‌های متداول TCP/IP و شیوه‌ی عملکرد آن‌ها آشنا باشید. برای فراگیری دانش اولیه‌ی شبکه‌های کامپیوتری و آشنایی با پروتکل‌های پرکاربرد می‌توانید از دوره‌ی آموزشی **Security Essentials** آکادمی راوین که به صورت رایگان در اختیار شما قرار گرفته است، استفاده کنید.

شناخت انواع حملات سایبری: حتی اگر قصد نداشته باشید در زمینه‌های امنیت تهاجمی مانند تست نفوذ فعالیت داشته باشید، باز هم آشنایی با تعاریف و ساختار انواع متداول حملات سایبری برای شما مورد نیاز خواهد بود. برای آشنایی با حملات سایبری مختلف می‌توانید ویدیوی دوره‌های **CEH Plus** و **Hack With Kali** را که به رایگان توسط آکادمی راوین عرضه شده، تماشا کنید.

درک مفاهیم پایه‌ی سیستم‌عامل: برای فعالیت در هر یک از زمینه‌های امنیت سایبری، لازم است تا آشنایی کافی با سیستم‌عامل‌های ویندوز و لینوکس داشته باشید. البته ممکن است با توجه به شغل انتخابی شما، نیاز به سطوح متفاوتی از میزان آشنایی با این سیستم‌عامل‌ها وجود داشته باشد.

همچنین فارغ از این که در چه زمینه ای از امنیت متخصص هستید، کلید اصلی اغلب پروژه های امنیتی، درک سیستم مورد نظر است. زمانی که با یک تکنولوژی جدید مواجه می شوید سعی کنید تا یک نمای کلی از سیستم را ترسیم کنید، با طرح سوالاتی از قبیل: چه چیزی در سیستم در حال رخ دادن است که من نمی توانم به صورت مستقیم آن را ببینم؟ طراحان سیستم و صاحبان آن چه اهدافی از طراحی آن داشته اند؟ چه نوع تهدیدات سایبری برای این سامانه وجود دارد؟ این تهدیدات چگونه ممکن است رخ دهند؟ و بسیاری سوالات مشابه دیگر که پاسخ آن ها می تواند درک شما را از سامانه ی در حال امن سازی (یا در حال ارزیابی)، افزایش دهد.

امنیت

چطور امنیت سایبرے را فرا بگیریم؟

HOW TO LEARN CYBER
SECURITY?



به دلیل پیچیدگی‌های موجود در تخصص امنیت سایبری و همچنین کمبود آموزش‌های مفید و کاربردی در این زمینه، اگر موفق شوید این تخصص را به خوبی کسب کنید به راحتی در شرکت‌ها و سازمان‌های مختلف استخدام خواهید شد، فارغ از این‌که این تخصص را با گذراندن دوره‌های آموزشی به دست آورده یا به صورت خودآموز یاد گرفته باشید. به عبارت دیگر در شرایط کنونی اغلب سازمان‌ها و شرکت‌ها به دنبال افراد متخصص در زمینه‌ی امنیت سایبری هستند (تا افراد دارای مدرک و گواهینامه). اما از کجا باید شروع کرد و از چه منابعی می‌توان برای کسب دانش امنیت سایبری بهره برد؟ این‌که چه منابعی برای شما مناسب‌تر هستند تا حد زیادی بستگی به انتخاب مسیر شما و این‌که چقدر می‌خواهید بر روی آن وقت بگذارید یا پیشرفت کنید دارد. در حالت کلی می‌توان موارد زیر را برای آموزش امنیت سایبری معرفی کرد:

- حضور در دوره‌های آموزش حضوری و آنلاین موسسه‌های معتبر
- دوره‌های ویدیویی رایج شده توسط موسسه‌های مختلف داخلی و بین‌المللی
- مطالعه‌ی کتاب‌های منتشر شده (توصیه می‌شود کتاب‌های جدید و زبان اصلی را مطالعه کنید)
- مشاهده و مطالعه‌ی ویدیوها و مقالات رایج شده در کنفرانس‌های امنیتی معتبر
- تماشای ویدیوهای رایگان موجود در پایگاه‌های اینترنتی مانند YouTube
- گشت‌وگذار در پلتفرم GitHub و مطالعه‌ی مطالب و کدهای به اشتراک گذاشته شده توسط سایر متخصصین

ممکن است ترجمه‌ی منابع ذکر شده نیز در دسترس شما باشد اما با توجه به پویایی بالای دانش امنیت، قبل از مطالعه، اطمینان حاصل کنید که این مطالب به روز هستند. بهره‌گیری از مسیرهای آموزشی رایج شده توسط متخصصین و موسسه‌های آموزشی می‌تواند شما را در انتخاب منابع و مسیر یادگیریتان کمک کند. مسیرهای آموزشی آکادمی راوین را نیز می‌توانید در بخش بعد مطالعه کنید.

در پایان می‌توان گفت برای هر کسی که به دنبال داشتن یک شغل ارزشمند و در عین حال به همراه ماجراجویی است، امنیت سایبری می‌تواند یکی از بهترین گزینه‌ها باشد. Brian Witten مدیر امنیت شرکت United Technologies Corporation درباره‌ی اشتغال در امنیت سایبری می‌گوید: «هر روز صبح با این فکر که شما نقش کوچکی در بهتر کردن جهان دارید از خواب بیدار می‌شوید و هر شب قبل از خواب به این نکته فکر می‌کنید که امروز از اطلاعات میلیون‌ها و شاید میلیارد‌ها نفر محافظت کرده‌اید، امیدوارم این نوع از شادمانی را همه بتوانند تجربه کنند».

آخرین توصیه‌ای که می‌توانیم به شما بکنیم این است که، جامعه‌ی امنیت سایبری مجموعه‌ی شگفت‌انگیزی از افراد بسیار باتجربه و ماهر است. با ورود به دنیای امنیت می‌توانید افتخار کنید که به بخشی از این جامعه‌ی شگفت‌انگیز تبدیل شده‌اید و بخشی از مسئولیت امن‌سازی این دنیای دیجیتالی بر روی دوش شما خواهد بود. همچنین با کمک به رشد یکدیگر، کل جامعه‌ی خود را بهبود داده و دنیای خود را به محیطی امن‌تر از دیروز تبدیل خواهید کرد.

مسیرہائے آموزشے آکادمیے راوین





تحلیل گر SOC لایه ۱

SOC TIER 1

مرکز عملیات امنیت (SOC) در واقع تیمی از بخش امنیت سازمان است، که وظیفه‌ی نظارت و تجزیه و تحلیل وضعیت امنیتی آن سازمان (به صورت مداوم) را بر عهده دارد. هدف اصلی یک تیم SOC را می‌توان شامل شناسایی، تجزیه و تحلیل و پاسخ به رخدادهای امنیت سایبری با استفاده از ترکیب راهکارهای مبتنی بر فناوری و مجموعه‌ای قدرتمند از فرآیندها دانست. یک مرکز عملیات امنیت اغلب از تعدادی تحلیل‌گر و متخصص امنیت و همچنین از مدیرانی که بر عملیات امنیت نظارت می‌کنند، تشکیل شده است.

«تحلیل‌گر SOC لایه ۱» یک جایگاه عملیاتی است که نظارت بر رویدادهای امنیتی به صورت در لحظه و بررسی رخدادهای امنیتی مشکوک را بر عهده دارد. به عبارت دیگر شما به عنوان یک تحلیل‌گر لایه ۱، به طور فعال تهدیدات امنیتی و مخاطرات مربوط به زیرساخت سازمان را رصد خواهید کرد.

در حالت کلی، مسئولیت‌های کلیدی این جایگاه شغلی به شرح زیر است:

زیرساخت‌های سازمان را با هدف شناسایی رخدادهای امنیتی به صورت مداوم پایش می‌کند

هشدارهای امنیتی را بررسی و ارزیابی می‌کند

در صورت نیاز، داده‌ها و مفاهیم لازم برای انتقال رخداد موردنظر به تحلیل‌گر لایه ۲ را جمع‌آوری و ارائه می‌کند

تا حد ممکن به رخدادهای امنیتی پاسخ می‌دهد

بر روی سلامت حس‌گرهای امنیتی سازمان و همچنین زیرساخت SIEM، نظارت می‌کند

گزارش‌های برنامه‌ریزی شده به صورت دوره‌ای و گزارش‌های موردی درخواست شده را ارائه می‌دهد

همکاری نزدیکی با متخصصین لایه ۲ و لایه ۳ در جهت بهبود مستمر خدمات دارد



کارشناس تست نفوذ

PENETRATION TESTER

تست نفوذ (Penetration Testing) یک حمله‌ی شبیه‌سازی شده‌ی قانونی است که بر روی یک سامانه یا زیرساخت شبکه در راستای ارزیابی امنیت آن انجام می‌شود. کارشناس تست نفوذ از ابزارها، تکنیک‌ها و فرآیندهای مشابه مهاجمان برای یافتن و ارزیابی تاثیرات آسیب‌پذیری‌های موجود در یک سامانه استفاده می‌کنند. تست‌های نفوذ اغلب انواع حملاتی را شبیه‌سازی می‌کنند که یک کسب‌وکار را تهدید می‌کند. آن‌ها می‌توانند بررسی کنند که آیا یک سامانه به اندازه‌ی کافی امن است تا بتواند در برابر حملات سایبری مختلف مقاومت کند؟

تست نفوذ اغلب با مرحله‌ی شناسایی شروع می‌شود که طی آن یک هکر اخلاقی زمان را صرف جمع‌آوری داده‌ها و اطلاعاتی می‌کند که از آن‌ها برای برنامه‌ریزی حمله‌ی شبیه‌سازی شده‌ی خود بهره خواهد برد. پس از آن، بر روی دستیابی و حفظ دسترسی به سامانه‌ی هدف تمرکز می‌کند که البته برای انجام آن به مجموعه‌ی وسیعی از ابزارها نیاز دارد. هکر قانونی پس از انجام تست نفوذ، یافته‌های خود را با تیم امنیت شرکت هدف به اشتراک می‌گذارد تا از این اطلاعات در راستای ارتقای امنیت سازمان و رفع آسیب‌پذیری‌های کشف شده در طول ارزیابی، استفاده کنند.

در حالت کلی، مسئولیت‌های کلیدی این جایگاه شغلی به شرح زیر است:

تست نفوذ و فعالیت‌های ارزیابی آسیب‌پذیری در خصوص برنامه‌های کاربردی تحت وب و Desktop، سیستم‌های عامل، انواع شبکه‌های سیمی و بی‌سیم و برنامه‌ها یا دستگاه‌های تلفن همراه

توسعه و اجرای برنامه‌های مدون تست امنیت

خودکارسازی تست نفوذ و سایر تست‌های امنیتی در شبکه‌ها، سامانه‌ها و برنامه‌های کاربردی

تعریف معیارهای معنادار به منظور انعکاس وضعیت واقعی امنیت، که به سازمان اجازه دهد تا تصمیمات موثری را بر اساس مخاطرات موجود اتخاذ کند

نگارش گزارش‌های جامع از نتایج تست‌های امنیتی انجام شده

همکاری با تیم‌های دفاعی سازمان و سایر متخصصین فناوری اطلاعات در راستای بهبود امنیت زیرساخت و سامانه‌ها



کارشناس تیم قرمز

RED TEAM SPECIALIST

بر خلاف کارشناس تست نفوذ که قصد دارد نقاط ضعف و آسیب‌پذیری‌های یک سامانه یا زیرساخت سازمان را تا جای ممکن شناسایی کند، هدف تیم قرمز شبیه‌سازی رفتار تیم‌های APT در تمام مراحل فعالیت آن‌هاست. شرکت FireEye، تیم APT را این‌گونه تعریف می‌کند: «شامل گروهی از نفوذگران است که تلاش می‌کنند داده‌های محرمانه را سرقت کنند، سرویس‌های حیاتی را مختل کنند یا به زیرساخت سازمان آسیب رسانند». برخلاف سایر مجرمین سایبری، یک تیم APT شاید ماه‌ها برای دستیابی به اهداف خود (شامل زیرساخت سازمان‌های قربانی) و حفظ این دسترسی‌ها زمان صرف کند. در واقع تیم‌های APT با بهره‌برداری از تکنیک‌های مختلف تلاش می‌کنند دسترسی خود را برای طولانی‌مدت در زیرساخت سازمان‌های قربانی حفظ کنند.

عملیات تیم قرمز مانند این است که یک بانک، شخصی را استخدام می‌کند تا لباس سارقین را پوشیده و نهایت تلاش خود برای نفوذ به ساختمان آن‌ها را انجام دهد. اگر موفق به ورود به بانک یا خزانه شود، آن‌گاه بانک تحت ارزیابی، اطلاعات ارزشمندی در مورد چگونگی تشدید تدابیر امنیتی خود، به دست خواهد آورد.

در واقع کارشناسان تیم قرمز باید بتوانند رفتار تیم‌های APT را در تمام مراحل نفوذ، گسترش دسترسی، نگهداری دسترسی و دستیابی به دارایی‌های حساس سازمان شبیه‌سازی کنند. بنابراین کارشناس تیم قرمز برای انجام این فعالیت‌ها به دانش‌های مختلفی مانند برنامه‌نویسی، نفوذ به زیرساخت، مهندسی اجتماعی، اکسپلویت‌نویسی و غیره نیاز دارد. البته باید به این نکته دقت داشت که خدمات تیم قرمز، همان‌گونه که از نامش برمی‌آید یک کار تیمی بوده و نیاز نیست تا همه‌ی این تخصص‌ها در یک نفر جمع شده باشد. بنابراین شما می‌توانید در یک تا تعدادی از این موارد، تخصص و تجربه کسب کنید.

این جایگاه شغلی مستلزم درک خوب از فناوری‌ها، ابزارها، تاکتیک‌ها، تکنیک‌ها و رویه‌هایی است که توسط مهاجمین سایبری برای نفوذ به سازمان‌های قربانی استفاده می‌شود. بنابراین توانایی تحقیق و مطالعه‌ی مستمر از اهمیت بالایی در این جایگاه شغلی برخوردار است.

در حالت کلی، مسئولیت‌های کلیدی این جایگاه شغلی به شرح زیر است:

یافتن راه‌های خلاقانه برای نفوذ به شبکه‌ی یک سازمان (استفاده از مهندسی اجتماعی، اکسپلویت و غیره)

توانایی تفکر مشابه مهاجمین سایبری به منظور شبیه‌سازی رفتار هکرهای سطح بالا و دستیابی به اهداف خاص تعریف شده در پروژه‌ی تیم قرمز

حرکت مخفیانه در زیرساخت سازمان به گونه‌ای که اطمینان داشته باشیم هیچ هشدار یا ایجاد نمی‌شود

انجام تحقیق و توسعه‌ی مستمر به منظور بهبود ابزارها و تکنیک‌های خود

اشتراک نتایج تحقیقات انجام شده با کارشناسان تیم آبی

شناسایی نقاط ضعف امنیتی سازمان و تبدیل آن به توصیه‌های امنیتی برای تیم‌های دفاعی

همکاری با تیم بنفش و آموزش تیم‌های دفاعی در راستای تقویت توانمندی سازمان در شناسایی تاکتیک‌ها، تکنیک‌ها و رویه‌هایی (TTP) که توسط مهاجمین استفاده می‌شود



کارشناس تیم بنفش

PURPLE TEAM SPECIALIST

برای از بین بردن احساس رقابت بین تیم‌های قرمز و آبی و بهبود تمرکز بر روی تقویت وضعیت امنیت سازمان، می‌توان از تیم بنفش استفاده کرد. در واقع یک تیم بنفش، تیم‌های قرمز و آبی را که به‌طور سنتی از هم جدا هستند، به هم مرتبط کرده و توانمندی‌های آن را در راستای ارتقای امنیت سازمان، گرد هم می‌آورد.

با توجه به موارد ذکر شده می‌توان گفت فعالیت تیم بنفش، یک فرآیند امنیتی است که در آن تیم‌های قرمز و آبی برای به حداکثر رساندن قابلیت‌های سایبری سازمان، با استفاده از بازخورد مستمر از یکدیگر و انتقال دانش به هم، همکاری می‌کنند. تیم بنفش می‌تواند به تیم‌های امنیتی برای بهبود اثربخشی در زمینه‌های مختلف مانند شناسایی آسیب‌پذیری، شکار تهدیدات سایبری و نظارت بر شبکه و غیره با شبیه‌سازی دقیق سناریوهای تهدید رایج و تسهیل طراحی تکنیک‌های جدید برای پیش‌گیری و شناسایی انواع تهدیدهای جدید کمک کند.

در حالت کلی، مسئولیت‌های کلیدی این جایگاه شغلی به شرح زیر است:

* تست و بررسی سناریوهای تهدید علیه زیرساخت سازمان با استفاده از ابزارها، تاکتیک‌ها و تکنیک‌های تهاجمی روز دنیا

* اجرای دوره‌ای حملات سایبری پیچیده به منظور آزمایش و بهبود مستمر قابلیت‌های مرکز عملیات امنیت سازمان و تیم‌های پاسخ به رخداد سایبری

* ارزیابی وضعیت دفاع سایبری سازمان و تقویت سامانه‌های حیاتی در جهت کاهش مخاطرات سایبری آینده

* شناسایی فعالیت‌های مخرب پیشرفته‌ای که از دید راهکارهای شناسایی تهدیدات سنتی سازمان دور مانده است

* توسعه و نگهداری از مستندات و راهنماهای مربوط به فرآیندهای امنیت در سازمان

* اعضای تیم بنفش باید بدون توجه به اینکه در حال انجام فعالیت‌های تهاجمی (تیم قرمز) یا دفاعی (تیم آبی) هستند، بتوانند در کنار هم کار کنند



کارشناس شکار تهدیدات سایبر

THREAT HUNTER

شکار تهدیدات سایبری یک جستجوی امنیتی فعال و پیش‌گیرانه در سراسر شبکه، نقاط پایانی و مجموعه داده‌های موجود با هدف شکار فعالیت‌های مخرب، مشکوک یا مخاطره‌آمیزی است که از دید ابزارهای شناسایی موجود در سازمان، دور مانده‌اند. بنابراین، بین شناسایی تهدید سایبری و شکار تهدید سایبری تمایز وجود دارد. شناسایی تهدید یک رویکرد تا حدی منفعلانه برای نظارت و پایش بر روی داده‌ها و سامانه‌ها در راستای تشخیص تهدیدات امنیتی بالقوه است. اما در شکار تهدیدات سایبری، فرد متخصص به صورت فعالانه تمام بخش‌های زیرساخت را به دنبال یافتن سر نخ‌ی از حضور یک فرد خرابکار یا مهاجم، جستجو می‌کند.

در واقع شکارچی تهدیدات سایبری، یک عنصر انسانی را به امنیت سازمان وارد و عملکرد سامانه‌های خودکار شناسایی تهدیدات را تکمیل می‌کند. به عبارت دیگر آن‌ها متخصصان امنیت ماهر هستند که تهدیدها را قبل از ایجاد مشکلات جدی در زیرساخت سازمان شناسایی و خنثی می‌کنند.

به‌طور خلاصه شکارچیان تهدید داده‌های امنیتی را بررسی و تحلیل می‌کنند. آنها به دنبال بدافزارها یا مهاجمان پنهان و الگوهای فعالیت مشکوکی می‌گردند که ممکن است سامانه‌های امنیتی خودکار از قلم انداخته باشند. آنها همچنین به اصلاح زیرساخت و معماری امنیتی یک سازمان به منظور پیش‌گیری از تکرار تهدیدات شناخته‌شده نیز کمک می‌کنند.

در حالت کلی، مسئولیت‌های کلیدی این جایگاه شغلی به شرح زیر است:

به طور فعال به دنبال تاکتیک‌ها، تکنیک‌ها و رویه‌های APT در شبکه و در نقاط پایانی زیرساخت سازمان است

بهبود مکانیزم‌های شناسایی سازمان با اجرای تکنیک‌هایی برای جستجوی تهدیدات با تکیه بر گزارش‌های Threat Intelligent و دانش خود در خصوص TTPها

کمک به تحقیقات اولیه در تیم امنیت سازمان در مورد رخدادهای احتمالی

بهبود مستمر زیرساخت Threat Intelligent و ایجاد و نگهداری از یک چشم‌انداز کامل در خصوص دامنهی تهدیدات سایبری موجود در کسب‌وکار سازمان

تهیه‌ی گزارش از رخدادها و موارد شناسایی‌شده در طول فرآیند شکار تهدید، که می‌تواند در راستای بهبود وضعیت کلی امنیت سازمان استفاده شود

GOOD
LUCK