معرفی دوره‌های

سازمانی امنیت شبکه

راهکارهای آموزشی ارتقای تاب‌آوری سایبری سازمان

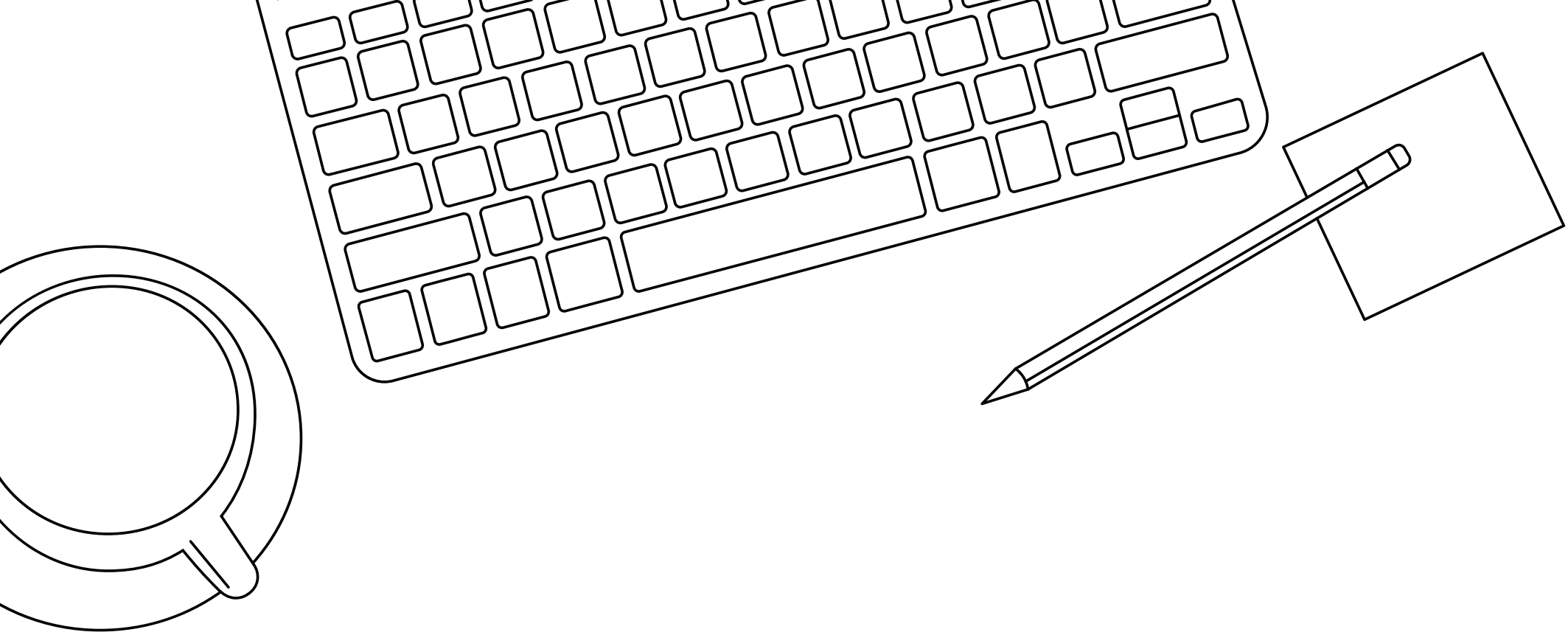
Cyberland
ناوک ارتباط هوشمند اوراسیا

سایبرلند

سایبرلند با بیش از یک دهه تجربه در حوزه امنیت شبکه، تلاش کرده است در کنار سازمان‌ها و صنایع مختلف، نقش کوچکی در ارتقای سطح امنیت سایبری ایفا کند. ما باور داریم امنیت پایدار تنها با ابزارها و فناوری‌های پیشرفته به دست نمی‌آید، بلکه آگاهی و توانمندسازی منابع انسانی در همه سطوح سازمان اهمیت حیاتی دارد. به همین دلیل، سایبرلند علاوه بر ارائه خدمات و راهکارهای امنیتی، در زمینه آموزش امنیت سایبری نیز فعالیت می‌کند تا با ترکیب تجربه عملی و دانش به‌روز، بستری برای افزایش آمادگی سازمان‌ها در برابر تهدیدات فراهم شود. اعتماد مجموعه‌ای از سازمان‌های خصوصی و دولتی در حوزه‌هایی همچون نفت و گاز، کشاورزی، صنایع هوایی، مخابرات و... برای ما ارزشمندترین سرمایه بوده است و ما همچنان خود را متعهد می‌دانیم با ارائه آموزش‌ها و راهکارهای کاربردی، در مسیر افزایش تاب‌آوری سایبری کشور همراه باشیم.

آکادمی سایبرلند

آکادمی سایبرلند با رویکردی متعهدانه در مسیر ارتقای امنیت سایبری سازمان‌ها فعالیت می‌کند. ما باور داریم آموزش، یکی از مؤثرترین ابزارها برای مقابله با تهدیدات روزافزون است. بر همین اساس، آکادمی مجموعه‌ای از دوره‌های حرفه‌ای امنیت سایبری را در سطوح مختلف از کارکنان اجرایی تا مدیران ارشد، طراحی و ارائه می‌کند تا سازمان‌ها بتوانند ضمن افزایش آگاهی، آمادگی و تاب‌آوری خود را در برابر مخاطرات سایبری ارتقا دهند.



ضرورت آموزش امنیت سایبری برای سازمان‌ها

آموزش امنیت سایبری برای تمامی سطوح سازمان، از کارکنان غیرتخصصی تا مدیران ارشد، ضرورتی استراتژیک محسوب می‌شود؛ زیرا انسان همواره ضعیف‌ترین حلقه امنیت است و بی‌توجهی یا خطای کوچک می‌تواند دروازه ورود تهدیدات جدی مانند حملات فیشینگ و باج‌افزار باشد. ایجاد آگاهی در میان کارکنان نه تنها احتمال وقوع رخدادهای امنیتی را کاهش می‌دهد، بلکه موجب بهینه‌سازی تصمیم‌گیری‌های مدیریتی، انطباق با الزامات قانونی و استانداردهای بین‌المللی، و در نهایت کاهش هزینه‌های سنگین ناشی از حملات سایبری می‌شود. به همین دلیل، سرمایه‌گذاری در آموزش امنیت سایبری را باید نه یک هزینه اضافی، بلکه اقدامی ضروری برای حفاظت از دارایی‌ها، اعتبار و تداوم کسب‌وکار دانست.

تهدیدات بالقوه که امنیت سازمان شما را به خطر می‌اندازند:

امنیت سایبری در سازمان‌ها تنها به ابزارها و فناوری محدود نمی‌شود، بلکه رفتار و آگاهی تمامی افراد از کارکنان عادی تا مدیران ارشد نقشی تعیین‌کننده در میزان ایمنی دارد. خطاهای سهوی، بی‌توجهی به سیاست‌های امنیتی یا تصمیمات ناآگاهانه می‌توانند به اندازه حملات هدفمند خارجی، سازمان را در معرض تهدید قرار دهند. از این رو شناسایی و طبقه‌بندی تهدیدات بالقوه در تمامی سطوح، پیش‌شرطی اساسی برای طراحی راهکارهای دفاعی مؤثر و ایجاد یک فرهنگ امنیتی پایدار در سازمان است.

۱. ریسک‌های ناشی از کارکنان:

کارکنان در سطوح عملیاتی به دلیل بی‌احتیاطی در انجام فعالیت‌های روزمره، مانند باز کردن پیام‌های مشکوک، دانلود فایل‌های آلوده یا استفاده از گذرواژه‌های ضعیف، می‌توانند زمینه‌ساز بروز رخدادهای امنیتی شوند. این تهدیدات به دلیل فراگیری و سهولت وقوع، از اهمیت ویژه‌ای برخوردارند.

۲. ریسک‌های ناشی از مدیران میانی و ارشد:

مدیران سازمان نیز در صورت نداشتن آگاهی کافی از الزامات امنیتی، ممکن است با تصمیمات نادرست مانند کاهش بودجه امنیت، نادیده گرفتن به‌روزرسانی‌ها یا بی‌توجهی به سیاست‌های حفاظتی، ناخواسته ریسک‌های جدی برای سازمان ایجاد کنند. همچنین استفاده از تجهیزات و شبکه‌های غیرایمن در مأموریت‌ها می‌تواند پیامدهای پرخطری به همراه داشته باشد.

۳. ریسک‌های فنی و سیستمی:

وجود نقص‌ها و آسیب‌پذیری‌های نرم‌افزاری که به‌موقع برطرف نمی‌شوند، و همچنین اعطای دسترسی‌های بیش از نیاز به کاربران، از جمله تهدیدات فنی محسوب می‌شوند که می‌توانند بستر مناسبی برای نفوذ و سوءاستفاده مهاجمان فراهم سازند. مدیریت مناسب این حوزه نقش حیاتی در کاهش ریسک های سازمان دارد.

آموزش امنیت سایبری برای کلیه کارکنان

پیشنهاد ما برای ارتقای سطح آگاهی و ایجاد فرهنگ امنیتی در سازمان، برگزاری دوره CSCU (Certified Secure Computer User) برای کلیه کارکنان است. این دوره به‌طور ویژه برای افرادی طراحی شده که ممکن است تخصص فنی در حوزه فناوری اطلاعات نداشته باشند، اما در فعالیت‌های روزمره خود با داده‌ها، سیستم‌ها و اینترنت در تعامل هستند. سرفصل‌های این دوره شامل آموزش امنیت در کار با اینترنت و ایمیل، مدیریت صحیح گذرواژه‌ها، شناسایی و مقابله با حملات فیشینگ و مهندسی اجتماعی، حفاظت از داده‌های شخصی و سازمانی، رعایت اصول امنیت در شبکه‌های اجتماعی و دستگاه‌های همراه، و روش‌های جلوگیری از آلودگی به بدافزارها و باج‌افزارها است. با گذراندن این دوره، کارکنان قادر خواهند بود نقش فعالی در پیشگیری از تهدیدات ایفا کرده و به تقویت امنیت کلی سازمان کمک نمایند.

فهرست مباحث دوره آشنایی با امنیت سایبری - به مدت ٦ ساعت

- آگاهی عمومی کاربر
- اصول بنیادی امنیت داده
- امنیت فضای ابری
- امنیت رمز عبور
- اقدامات مقابله‌ای در برابر مهندسی اجتماعی
- کاهش جرائم هویت انسانی
- امنیت ایمیل
- امنیت در مرورگرهای اینترنتی
- امنیت سیستم‌عامل
- امنیت پست الکترونیک
- امنیت دستگاه تلفن همراه
- پشتیبان‌گیری از داده
- امنیت شبکه‌های اجتماعی
- حفاظت توسط آنتی‌ویروس
- بازیابی در شرایط بحران
- امنیت در اینترنت
- امنیت کارت‌های اعتباری و بانکی
- نظارت آنلاین بر فرزندان
- امنیت شبکه خانگی و بی‌سیم
- فیشینگ , مقابله با آن

آموزش امنیت سایبری برای مدیران میانی و ارشد

برای مدیران ارشد و تصمیم‌گیرانی که ممکن است دانش تخصصی در حوزه امنیت سایبری نداشته باشند، شرکت در دوره CRISC (Certified in Risk and Information Systems Control) گزینه‌ای مناسب و کاربردی است. این دوره بر شناسایی و مدیریت ریسک‌های مرتبط با فناوری اطلاعات و انطباق آن‌ها با اهداف کلان سازمان تمرکز دارد و کمک می‌کند تا مدیران درک روشنی از تأثیر تهدیدات سایبری بر کسب‌وکار پیدا کنند. محتوای آموزشی این دوره به جای ورود به مباحث پیچیده فنی، بر اصول مدیریت ریسک، کنترل‌های اطلاعاتی و تصمیم‌گیری مبتنی بر ریسک تأکید دارد و زمینه‌ساز ارتقای تاب‌آوری سازمان و حفاظت مؤثر از دارایی‌های اطلاعاتی خواهد بود.

چارچوب محتوای آموزشی CRISC (مطابق ISACA) - به مدت ۱۸ ساعت

۱. شناسایی ریسک (IT Risk Identification)

- شناسایی دارایی‌ها و منابع حیاتی سازمان
- تحلیل تهدیدات داخلی و خارجی
- شناسایی آسیب‌پذیری‌ها و نقاط ضعف
- درک نیازهای قانونی و مقرراتی مرتبط با ریسک

۲. ارزیابی ریسک (IT Risk Assessment)

- تحلیل سناریوهای ریسک و احتمال وقوع آن‌ها
- ارزیابی تأثیر ریسک بر اهداف کسب‌وکار
- مدل‌سازی و سنجش سطح ریسک سازمان
- اولویت‌بندی ریسک‌ها برای تخصیص منابع

۳. پاسخ‌گویی و کاهش ریسک (Risk Response and Mitigation)

- طراحی و پیاده‌سازی کنترل‌های امنیتی متناسب
- تدوین سیاست‌ها و چارچوب‌های مدیریت ریسک
- اقدامات اصلاحی برای کاهش احتمال یا اثر تهدیدات
- ارزیابی اثربخشی کنترل‌ها و اقدامات امنیتی

۴. پایش و گزارش‌دهی ریسک (Risk and Control Monitoring & Reporting)

- نظارت مستمر بر وضعیت ریسک‌ها و کنترل‌ها
- تحلیل شاخص‌های کلیدی ریسک (KRI)
- تهیه گزارش‌های مدیریتی برای تصمیم‌گیری
- بهبود مستمر فرآیند مدیریت ریسک در سازمان

آموزش‌های پیشرفته امنیت شبکه

دوره‌های تخصصی سازمانی در حوزه امنیت شبکه با هدف تربیت نیروهای حرفه‌ای طراحی شده‌اند تا سازمان‌ها بتوانند در برابر طیف گسترده‌ای از تهدیدات سایبری واکنش سریع، دقیق و مؤثر داشته باشند. این آموزش‌ها بر توسعه مهارت‌های عملی در پایش، تحلیل و مدیریت رخدادهای امنیتی متمرکز بوده و شرکت‌کنندگان را برای کار با سامانه‌های پیشرفته مانیتورینگ و تحلیل داده آماده می‌سازند. رویکرد این دوره‌ها ترکیبی از دانش نظری و تمرین‌های عملی است تا فراگیران بتوانند علاوه بر درک مفاهیم کلیدی، توانایی به‌کارگیری ابزارهای تخصصی و اجرای فرآیندهای استاندارد در محیط واقعی سازمان را نیز کسب کنند. نتیجه این آموزش‌ها، افزایش تاب‌آوری سایبری سازمان و ایجاد تیم‌هایی کارآمد برای پاسخ به حوادث و مدیریت مداوم امنیت شبکه خواهد بود.

دوره مقدماتی

Core Techniques

۱۴۰ ساعت

این دوره، مبانی امنیت شبکه را به صورت ساخت‌یافته پوشش داده و ضمن آموزش روش‌های شناسایی تهدیدات، مهارت‌های بنیادین در مدیریت امنیت زیرساخت‌های سازمانی را فراهم می‌سازد.

بر اساس سرفصل‌های:

SANS SEC 401
SANS SEC 504
Security+

دوره متوسط

SOC Tier 1

۱۲۰ ساعت

دوره SOC Tier-1 بر آموزش مبانی مرکز عملیات امنیت متمرکز است و فراگیران را با پایش رویدادها، شناسایی تهدیدات اولیه و اصول پاسخ‌گویی سریع به حوادث سایبری آشنا می‌سازد.

بر اساس سرفصل‌های:

SANS SEC 504
SANS SEC 450
Splunk Fundamentals

دوره پیشرفته

SOC Tier 2

۱۴۰ ساعت

دوره SOC Tier-2 مهارت‌های پیشرفته تحلیل رویدادها، شناسایی تهدیدات پیچیده و پاسخ به حملات هدفمند را آموزش می‌دهد و کارشناسان را برای مدیریت حوادث در سطح حرفه‌ای توانمند می‌سازد.

بر اساس سرفصل‌های:

SANS SEC 503
SANS SEC 511
SANS SEC 555

دوره جامع

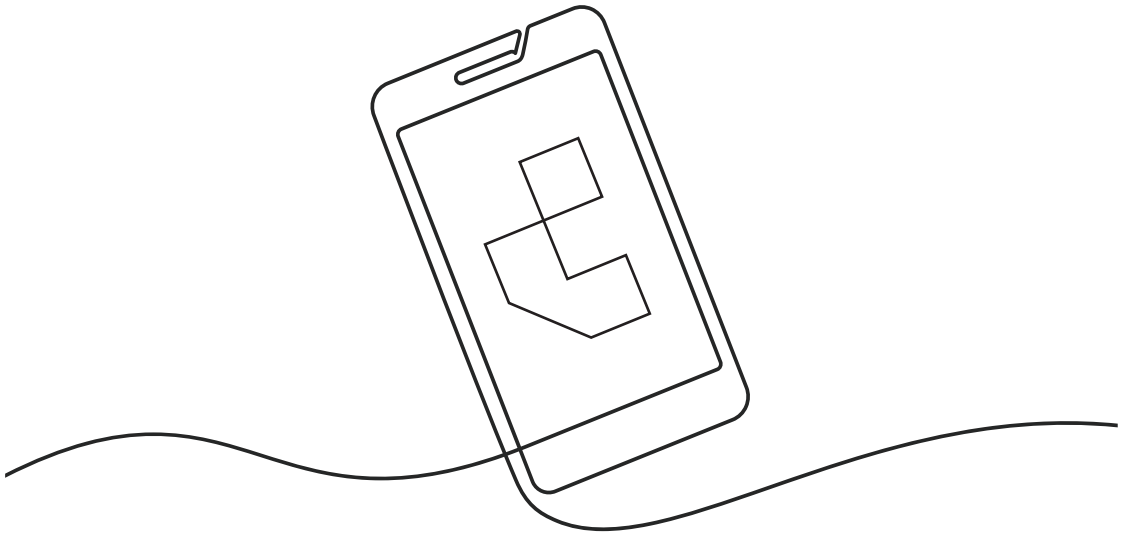
Splunk ES

۲۰+۴۰+۴۰ ساعت

دوره Splunk ES مهارت استفاده از این SIEM پیشرفته را آموزش می‌دهد؛ شامل پیکربندی، تحلیل داده‌های امنیتی، مدیریت هشدارها و شناسایی تهدیدات برای ارتقای کارایی مرکز عملیات امنیت سازمان.

بر اساس سرفصل‌های:

Splunk ES



ارتباط با ما

امنیت سایبری امروز یکی از نیازهای جدی هر سازمان است و نقش مهمی در کاهش ریسک‌ها و تداوم کسب‌وکار دارد. آموزش نیروی انسانی می‌تواند تأثیر قابل‌توجهی در افزایش سطح آمادگی و ارتقای توانمندی‌های عملیاتی سازمان‌ها داشته باشد.

در این معرفی نامه مجموعه‌ای از دوره‌های آموزشی مطرح شدند که با هدف پاسخگویی به نیازهای واقعی صنایع طراحی شده‌اند. در صورتی که این دوره‌ها می‌تواند برای سازمان شما مفید باشد، خوشحال می‌شویم فرصتی برای هماهنگی بیشتر و ارائه توضیحات تکمیلی در اختیارمان قرار دهید.

برای کسب اطلاعات بیشتر و برنامه‌ریزی دوره‌های آموزشی متناسب با نیاز سازمان، لطفاً با شماره تماس زیر با ما در ارتباط باشید:

تلفن تماس: ۵۷۸۱۴-۰۲۱
www.cyberland.ir