معرفی دوره آموزشی

عنوان دوره:

فارسی: **دفاع فعال سایبری**

انگلیسی: **Cyber Active Defence**

درباره دوره:

امروزه با گسترش تهدیدات و مخاطرات امنیتی، حتی سازمان‌هایی با بهترین زیرساخت‌های امنیتی هم نمی‌توانند تضمین کنند که اقدامات یا عملیات بدخواهانه بر روی شبکه آنها رخ نخواهد داد. هنگامی که حوادث امنیتی به وقوع می‌پیوندند، برای یک سازمان، حیاتی است که راهکار مؤثری برای دفاع و همچنین پاسخگویی به آن حملات داشته باشد. سرعت تشخیص، تحلیل و پاسخگویی سازمان به حوادث امنیتی علاوه بر این که می‌تواند خسارت ناشی از حادثه را محدود سازد، هزینه بازیابی از آن حادثه را نیز به شدت کاهش می‌دهد.

در این دوره آموزشی، مخاطبان ضمن آشنایی با حملات پیشرفته سایبری، مهارت‌های مورد نیاز را جهت طراحی، پیاده‌سازی و مدیریت اجزای کلیدی امنیت شبکه‌های سازمانی، فرا گرفته و می‌توانند از سازمان‌ها در برابر مخاطرات و تهدیدهای امنیتی پیشرفته محافظت کنند.

اهداف دوره:

۱- آشنایی با روش‌های استحکام بخشی اجزای شبکه به منظور دفاع متمرکز و فعال در برابر حملات سایبری

۲- آشنایی با روش‌های جلوگیری و کاهش تأثیر انواع حملات سایبری

۳- آشنایی با روش‌های کشف و پاسخ به حملات سایبری

۴- آشنایی با روش‌های طراحی و پیکربندی امن شبکه‌های رایانه‌ای سازمانی

مخاطبان دوره:

- ✓ مدیران، راهبران و کارشناسان فناوری اطلاعات و امنیت

- ✓ مشاوران امنیت اطلاعات
- ✓ سایر علاقمندان به مباحث امنیت اطلاعات

مدت زمان دوره:

۱۶ ساعت (۲ روز)

محتویات دوره:

- آشنایی با مفاهیم کلیدی امنیت اطلاعات
- آشنایی با حملات سایبری و روش‌های نفوذ به سازمان‌ها
- آشنایی با اصول دفاع سایبری
- روش‌های ارزیابی فناوری‌های دفاع سایبری
- چگونگی تدوین، توسعه و پیاده‌سازی خط‌مشی‌های امنیتی
  - نحوه رعایت تعادل میان مخاطرات و نیازمندی‌های سازمان
  - نحوه شناسایی اهداف تضمین امنیتی
  - نحوه انتخاب فناوری‌های امنیتی
- راهکارهای انتخاب فناوری‌های امنیتی مناسب برای سازمان
- روش‌های نصب و پیکربندی فناوری‌های امنیتی
  - دیواره آتش
    - چگونگی پیکربندی دیواره آتش برای پشتیبانی از خدمات بیرونی
      - پشتیبانی از خدمات عمومی (HTTP & SMTP)
      - پالایش و مسدودسازی محتوای خطرناک
      - پالایش ترافیک‌های رمزنگاری شده
      - مدیریت سرویس‌های پیچیده (VOIP, Audio & Video)
    - سازوکار ارایه خدمات ایمن بیرونی
      - پیاده‌سازی سرویس دهنده‌های عمومی قابل دسترس
      - ایجاد یک معماری امن برای مناطق نه چندان حفاظت شده (DMZ)
    - روش‌های مجوزدهی دسترسی به خدمات داخلی

- سفارشی‌سازی سرویس نام دامنه (DNS) برای معماری‌های دیواره آتش
- پیکربندی سرویس ترجمه آدرس شبکه (NAT)
- ایجاد لیست‌های کنترل دسترسی برای برنامه‌های کاربردی و کاربران

o سیستم‌های تشخیص و جلوگیری از نفوذ

➢ بکارگیری سیستم‌های تشخیص و جلوگیری از نفوذ

- مکان‌یابی سیستم‌های تشخیص و جلوگیری از نفوذ در معماری شبکه سازمان
- قراردهی حسگرهای عملیاتی در حالت پنهان

➢ کشف نفوذ در سازمان

- طراحی سیستم‌های تشخیص و جلوگیری از نفوذ سلسله مراتبی چند لایه‌ای در شبکه سازمان
- مدیریت یکپارچه سیستم‌های تشخیص و جلوگیری از نفوذ توزیع شده

➢ هشدارهای امنیتی

- کاهش خطاهای مثبت و منفی
- اعتباربخشی رویدادها و تشخیص حملات

➢ فرایندهای پاسخ فعال به رویدادها و حوادث

o ضد بدافزار

o ضد ویروس

- پیکربندی کاربران راه دور شبکه‌های خصوصی مجازی (VPN)

➢ ایجاد تونل‌های VPN

- پشتیبانی از کاربران راه دور با پروتکل تونل زنی لایه ۲ (L2TP)
- اتصال سایت‌های راه دور با پروتکل تونل زنی لایه ۳ (IPSec)

➢ توسعه راه حل‌های کاربری

- ارزیابی کاربران راه دور VPN
- پیاده‌سازی سازوکارهای هویت‌سنجی کاربران راه دور VPN

➢ الگوریتم‌های احراز هویت تونل‌های VPN

➢ الگوریتم‌های رمزنگاری و درهم‌سازی تونل‌های VPN

➢ ارزیابی امنیتی پروتکل‌های تونل زنی

➢ روش‌های حفاظت از تونل‌های VPN

➢ فناوری‌ها و تجهیزات سخت افزاری VPN

- مدیریت گواهینامه‌های دیجیتال از طریق PKI

- اصول یکپارچه‌سازی اجزای دفاعی سازمان
- روش‌های کاهش تأثیر حملات سایبری
- بررسی معماری‌های امنیتی شبکه
- روش‌های دفاع عمقی
- روش‌های اجرایی مقاوم‌سازی سیستم‌های عملیاتی سازمان

ویژگی‌های دوره:

- ✓ امکان صدور گواهینامه معتبر حضور در دوره آموزشی
- ✓ برخورداری از ۱۰٪ تخفیف در صورت ثبت نام گروهی