عنوان دوره:

فارسی: **مدیریت حوادث سایبری (نحوه راه‌اندازی عملی تیم‌های امداد رایانه‌ای)**
انگلیسی: **Incident Management (CSIRT Implementation)**

درباره دوره:

با پیشرفت و گسترش روز افزون فناوری اطلاعات و ارتباطات در دنیای امروز، بحث حفاظت از داده‌ها اهمیت ویژه‌ای یافته است. هر چه راه‌های دسترسی و روش‌های ارتباطی افزایش می‌یابد مسئله حفاظت از امنیت اطلاعات نیز مهم‌تر و پیچیده‌تر می‌شود. وجود حفره‌ها و نقص‌های امنیتی در سیستم‌های فناوری اطلاعات، همواره مورد توجه افراد سودجو بوده است به طوری که در مقاطعی از زمان، سرعت افزایش تعداد حملات صورت گرفته، از سرعت پیشرفت و گسترش سیستم‌ها بسیار بیشتر است. بنابراین با نگاهی به آمار منتشر شده و وضعیت فعلی پیشرفت فناوری اطلاعات، وجود مراکزی مستقل برای تأمین امنیت فضای تبادل اطلاعات (افتا) در سازمان‌ها امری حیاتی و ضروری به نظر می‌رسد.

امروزه بیشتر سازمان‌ها دریافته‌اند که یک راهکار امنیتی واحد برای فراهم‌آوری امنیت سیستم‌ها وجود ندارد بلکه باید از استراتژی امنیتی چند لایه بهره گرفت. یکی از لایه‌هایی که بیشتر سازمان‌ها در راهبرد امنیتی خود در نظر می‌گیرند ایجاد یک مرکز مدیریت رخدادهای امنیتی و تشکیل تیم پاسخگویی به رخدادهای امنیتی رایانه است که در سازمان‌های ایرانی با نام «گوهر» شناخته می‌شود. هدف از ایجاد مرکز مدیریت رخدادهای امنیتی و تشکیل این تیم، تأمین قابلیت ارزیابي، پاسخگویي و آموختن از رخدادهاي امنیت اطلاعات است. این مرکز با مدیریت صحیح رخدادهای امنیتی در سازمان می‌تواند کمک شایانی را به سازمان‌ها در کاهش صدمات مالی و مهمتر از همه، وجهه و شهرت آن سازمان کند.

در این دوره آموزشی، مخاطبان ضمن آشنایی با چارچوب‌ها و اصول ایجاد تیم‌های امداد رایانه‌ای در سازمان‌های ایرانی، با روش‌های اجرایی طراحی، تشکیل و راه‌اندازی این تیم‌ها به صورت کامل آشنا شده

و می‌توانند تیم‌های امداد رایانه‌ای را در سازمان‌های خویش پیاده‌سازی کنند.

اهداف دوره:

1- کاهش و به حداقل رساندن بروز حادثه امنیتی در سازمان‌ها
2- کاهش و به حداقل رساندن زمان پاسخ به حوادث رایانه‌ای در سازمان‌ها
3- کاهش و به حداقل رساندن میزان خسارت حوادث رایانه‌ای در سازمان‌ها

مخاطبان دوره:

- ✓ مدیران، راهبران و کارشناسان فناوری اطلاعات و امنیت
- ✓ مدیران و کارشناسان تیم‌های امداد و گروه‌های پاسخ به حوادث امنیتی رایانه‌ای
- ✓ سایر علاقمندان به مباحث امنیت اطلاعات

مدت زمان دوره:

16 ساعت (2 روز)

محتویات دوره:

- تشکیل و راه‌اندازی مرکز گوهر
  - معرفی مرکز گروه واکنش هماهنگ رخداد (گوهر)
  - اسناد بالادستی الزام‌آور کشور در خصوص تشکیل مرکز گوهر در سازمان‌ها
  - اهداف راه‌اندازی مرکز گوهر
  - مزایای راه‌اندازی مرکز گوهر
  - مأموریت‌ها و وظایف مرکز گوهر
  - سطوح پیاده‌سازی مرکز گوهر

- مراحل تکامل مراکز گوهر

- گام‌های راه‌اندازی و تشکیل مرکز گوهر در سازمان
  - جایگاه مرکز گوهر در چارت سازمان و ارتباط آن با سایر واحدها
  - ساختار مرکز گوهر و تیم‌های آن
  - نقش‌ها و مسئولیت‌های افراد
  - تعیین مکان فیزیکی مرکز گوهر
- تعاملات مرکز گوهر
  - نحوه تعامل مرکز گوهر با مرکز عملیات امنیت (SoC)
  - نحوه تعامل مرکز گوهر با سایر گوهرها
  - نحوه تعامل مرکز گوهر با مراکز ماهر و آپا
  - نحوه تعامل مرکز گوهر با ذی‌نفعان سازمان (همکاران، مشتریان، بیمه‌گذاران، اشخاص سوم و غیره)
  - نحوه تعامل مرکز گوهر با سازمان‌های بالادستی، نهادهای امنیتی و قانون‌گذار
- سرویس‌های امنیتی مرکز گوهر
  - خدمات پیشگیرانه
  - خدمات واکنشی
  - خدمات مدیریت کیفی امنیت
- فراهم‌آوری امنیت مرکز گوهر
  - امنیت شبکه
  - امنیت فیزیکی
  - امنیت منابع انسانی
- ابزارها و نرم افزارهای مورد استفاده در مرکز گوهر
- مدیریت رویدادها و حوادث امنیتی در گوهر
  - چرخه مدیریت رخدادها و حوادث امنیتی در گوهر
  - چگونگی گردش کار بین تیم‌های گوهر
  - نحوه رصد و تشخیص نفوذ به سازمان
  - نحوه شناسایی رخدادهای امنیتی در سازمان

- نحوه شناسایی آسیب پذیری‌ها
- نحوه جمع‌آوری گزارشات و هشدارها از تجهیزات شبکه و سامانه‌های امنیتی

- ارزیابی و تصمیم‌گیری درباره رویدادها و حوادث امنیتی در گوهر
  - نحوه تعیین متدولوژی رسیدگی به حوادث امنیتی
  - نحوه تدوین طرح ارزیابی و تصمیم اولیه
  - نحوه تدوین طرح ارزیابی و تأیید رویدادهای امنیتی
  - نحوه تدوین طرح رده‌بندی رویدادهای امنیتی
- پاسخگویی به رویدادها و حوادث امنیتی در گوهر
  - نحوه تدوین طرح پاسخگویی به حوادث امنیتی
  - نحوه تعیین اقدامات لازم در خصوص پاسخگویی فوری به حوادث امنیتی
  - نحوه تعیین اقدامات لازم در خصوص پاسخگویی ثانویه به حوادث امنیتی
  - نحوه تعیین اقدامات لازم در خصوص پاسخگویی‌ها با موقعیت‌های ویژه
  - نحوه تعیین طرح محدودسازی اثرات نامطلوب حوادث امنیتی
  - چگونگی طراحی زیرساخت‌های سازمانی مطلوب و مورد نیاز برای پاسخگویی به رویدادهای امنیتی
  - نحوه تدوین طرح استمرار کسب و کار
  - نحوه تعیین متدولوژی مناسب جهت روز آمد کردن اطلاعات رویدادهای امنیتی
  - نحوه تعیین کنترل‌های امنیتی در رابطه با رویدادهای امنیتی
  - نحوه تعیین متدولوژی ارزیابی کنترل‌های امنیتی بکار گرفته شده
  - نحوه تعیین روش تحلیل امور قانونی امنیت اطلاعات
- نحوه اعلام هشدار در مورد رخدادهای امنیتی
- نحوه تهیه فرم‌های مورد نیاز مرکز گوهر
- فرایندهای ترمیم و بازیابی از حوادث در گوهر
- چگونگی اشتراک‌گذاری اطلاعات و پایگاه دانش حوادث

- گزارش‌دهی رویدادها و حوادث امنیتی در گوهر
  - نحوه گزارش‌دهی رخدادهای امنیتی به گوهر
  - نحوه گزارش‌دهی رخدادهای امنیتی از گوهر به سایر نهادها
- یادگیری از رویدادها و حوادث امنیتی در گوهر
  - نحوه تدوین برنامه‌های آموزشی و آگاهی‌رسانی
  - نحوه تدوین متدولوژی مستندسازی رویدادهای امنیتی
  - نحوه تدوین روش بازنگری‌های مدیریتی امنیت اطلاعات
  - نحوه تدوین طرح‌واره بهبود در کاربرد نظارت امنیت اطلاعات
- ویژگی‌ها و ساختار پرتال سازمانی مرکز گوهر
- روش‌های ارزیابی و ممیزی عملکرد مرکز گوهر
- معرفی بهترین الگوها و استانداردهای جهانی در خصوص راه‌اندازی و تشکیل مرکز گوهر

ویژگی‌های دوره:

- ✓ امکان صدور گواهینامه معتبر حضور در دوره آموزشی