Carrier Digit
کاریارارقام

مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی

و برگزارکننده دوره های آموزشی

بسته مقدماتی مرکز عملیات امنیت
SOC + SIEM

Security Operation Center (SOC)
Security Information and Event Management (SIEM)

مدت(ساعت): ۱۶ | **پیش نیاز:** CEH | **اعتبار دهنده:** SANS

معرفی دوره:

- هر روزه در اخبار مشاهده می‌کنیم که روزانه تعداد داده‌های فاش شده، حملات سایبری و خراب‌کاری‌های اینترنتی در حال افزایش است. حملات به صورت مداوم هم از لحاظ کمی و هم از لحاظ کیفی در حال افزایش است. سازمان‌ها برای جلوگیری و کاهش تهدیدات، از تکنولوژی‌های متعددی در سطوح مختلف بهره می‌گیرند. استفاده از این تکنولوژی‌ها تیم‌های امنیت سازمان را با سیل عظیمی از اطلاعات و رویدادهای امنیتی مواجه خواهد کرد که چنین حجمی بیش از اندازه ای است که توسط نیروی انسانی قابل کنترل و تحلیل باشد.
- نتیجه ی این موضوع این می شود که زمان و تخصص و هزینه ای که برای مدیریت داده های امنیتی در گستره ی تشکیلات، مورد استفاده قرار میگیرد، به طور مداوم افزایش می یابد بدون اینکه ضریب امنیت کسب و کار پیشرفت چشمگیری داشته باشد.
- در برابر این چالش‌ها، کسب و کارها(شرکت و سازمان بهتره) به این سوال می‌رسند که بهترین راه برای محافظت از فعالیت‌ها و دارایی‌های حیاتی چیست؟ راه مناسب برای پیاده‌سازی سیاست‌های امنیتی کدام است؟ چگونه باید به اطلاعات مربوط به امنیت که از ابزارهای مختلف امنیتی در سطح سازمان جمع‌آوری می‌شود پرداخته شود؟ با وجود تمام گستردگی و ناهماهنگی اطلاعات، چگونه باید مسئولیت و یکپارچگی در سطح مدیریت را حفظ نمود؟
- لذا برای بهبود راهبردهای فعلی مدیریت حوادث امنیتی و فرآیندهای امن‌سازی کسب و کار، مدیران امنیتی به پایش و نظارت بلادرنگ و متمرکز وضعیت امنیت سازمان نیازمند هستند. مرکز عملیات امنیت، با پایش شبانه‌روزی اتفاقات امنیتی، تحلیل پیشرفته، و با استفاده از زنگ خطرهای خودکار، ارائه‌ی گزارشات مشروح رویکرد پیشگیرانه به امنیت را تحقق می‌بخشد.

اهداف دوره:

آشنایی با موضوعات زیر:

- دفاع فعال
- تحلیل هوشمند
- پایش مداوم امنیت
- پایش امنیتی میزبان‌ها و شبکه‌ها
- معیارهای یک مرکز عملیات امنیت موفق
- یکپارچه‌سازی تکنولوژی‌های امنیت سازمان
- طراحی، راه‌اندازی و مدیریت تیم مدیریت حوادث
- راه‌حل‌های طراحی و راه‌اندازی یک مرکز عملیات امنیت موثر

امتیازات دوره :

- اعطای مدرک فارسی و انگلیسی با مجوز رسمی از :
  - مجوز از اداره کل نظام مدیریت امنیت اطلاعات (نما)
  - سازمان مدیریت و برنامه ریزی کشور (معاونت توسعه مدیریت و سرمایه انسانی رئیس جمهوری سابق)
  - شورای عالی انفورماتیک
  - قابلیت ترجمه وتایید قوه قضاییه وامور خارجه
- بهره گیری از اساتید مجرب و تأیید شده با سابقه حضور در پروژه‌های ملی
- طراحی شده توسط تیم اساتید کاریار ارقام

مخاطبان دوره:

- مدیران فناوری اطلاعات سازمان
- مدیران امنیت سازمان
- کارشناسان ارشد امنیت
- تحلیل‌گران مرکز عملیات امنیت
- کارشناسان امنیت تیم CSIRT

Accredited by CARRIER DIGIT Computer Software LLC
EC-Council
تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳،۸ فاکس :۸۸۰۶۵۲۲۲

محتوای دوره :	Course Outline :
SOC:	**SIEM:**
• ضرورت و نیاز به SOC	• تاریخچه SIEM
• معرفی اجزای SOC	• معرفی پروتکل‌ها، استانداردها و تکنولوژی‌های Log Management
• ساختار سازمانی SOC و ارائه پیشنهاداتی برای انتخاب ساختار سازمانی بهینه متناسب با کسب و کار سازمان	• ارتباط SIEM با دیگر ابزارهای امنیت سازمان
• معرفی فرآیندها و رویه‌های SOC	• معرفی اجزای SIEM
• بیان راه‌کارهای طراحی موثر رویه‌ها و ایجاد ارتباط با دیگر رویه‌های سازمان	• معرفی روش‌ها و ابزارهای نرمال‌سازی و همبستگی
• راه‌کارهایی موثر برای استخدام، حفظ و آموزش نیروی انسانی SOC	• ویژگی‌های یک SIEM بالغ
• معرفی مهارت‌های فنی و غیر فنی نیروی انسانی SOC	• مقایسه SIEMهای معتبر و ارائه شاخص‌هایی برای انتخاب بهترین راه‌کار
• معرفی ابزارها و تکنولوژی‌های SOC	• راه‌اندازی یک SIEM و دموی تمام بخش‌های مهم آن
• روش‌ها و تکنولوژی‌های تحلیل و شناسایی تهدیدات پیشرفته پایدار (APT)	• تولید حمله و پیمایش رویه مدیریت حوادث به صورت عملی
• اقدامات و کارهای لازم برای طراحی، راه‌اندازی و بهره‌برداری یک SOC کارا	
• نشانه‌های یک SOC بالغ و راه‌کارهای تعیین سطح بلوغ SOC	
• نکات فنی تهیه مستنداتی مانند RFP، پروپوزال و ... برای SOC	

Accredited by CARRIER DIGIT Computer Software LLC
EC-Council
تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳، ۸ فاکس :۸۸۰۶۵۲۲۲