Carrier Digit
کاریار ارقام

مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی

و برگزارکننده دوره های آموزشی

دوره تکمیلی مرکز عملیات امنیت SANS (FOR 508)

Advanced Digital Forensics, Incident Response and Threat Hunting
GCFA

مدت(ساعت): ۴۰ | **پیش نیاز:** SANS FOR 500 | **اعتبار دهنده:** SANS

معرفی دوره :

طی چند سال اخیر شاهد حملات پیشرفته و پیچیده بوده‌ایم که زیرساخت‌های حیاتی و سازمان‌ها را هدف قرار داده‌اند. این دسته از حملات، توانسته‌اند حجم زیادی از اطلاعات را سرقت کرده و خسارت‌های مالی و اعتباری زیادی را به کشورمان تحمیل نمایند. در دنیای امنیت به این حملات Advanced Persistent Threat یا APT گفته می‌شود.

برای شناسایی و مقابله با این حملات نیاز است تا کارشناسان امنیت دانش گسترده‌ای در مورد روش‌های پاسخ به حوادث امنیتی، روش‌های پیشرفته فارنزیک، روش‌های پیچیده نفوذ داشته باشند. در این دوره مهارت‌های لازم جهت شناسایی، پاسخ و مقابله با تهدیدات پیشرفته و پیچیده‌ی امروزی، ارائه خواهد شد.

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
- برگزاری لابراتوارهای دوره مبتنی بر Workshop رسمی دوره
- بهره گیری از اساتید مجرب و تأیید شده با سابقه حضور در پروژه‌های ملی

اهداف دوره :

- آشنایی با تهدیدات پیشرفته و پیچیده
- شناسایی اینکه یک حمله چگونه و چه زمانی رخ داده است.
- شناسایی سیستم‌های آلوده شده یا تحت تاثیر قرار گرفته
- شناسایی اینکه مهاجمین چه داده‌هایی را بدست آورده یا تغییر داده‌اند
- روش‌های کاهش تاثیر یا مقابله با تهدیدات جدید
- آشنایی با منابع و روش‌های ایجاد هوش امنیتی

مخاطبان دوره :

- کارشناسان تیم امداد رایانه‌ای
- کارشناسان مرکز عملیات امنیت
- مدیر مرکز عملیات امنیت
- کارشناسان جرائم رایانه‌ای
- مدیران شبکه
- مدیرات امنیت سازمان

Course Outline :

SEC 508

1: Enterprise Incident Response
2: Memory Forensics in Incident Response
3: Timeline Analysis
4: Deep Dive Forensics And Anti-Forensics Detection
5: Adversary and Malware Hunting
6: The APT Incident Response Challenge

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