Carrier Digit
کاریار ارقام

مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی

و برگزارکننده دوره های آموزشی

دوره تکمیلی مرکز عملیات امنیت SANS (FOR 500) (Formerly 408)

Windows Forensic Analysis
GCFE

مدت(ساعت): ۴۰ | **پیش نیاز:** SANS SEC 504 | **اعتبار دهنده:** SANS

معرفی دوره :

شما نمی‌توانید چیزی را که نمی‌شناسید محافظت کنید. لذا قابلیت‌ها و دانش فارنزیک کامپوننت اصلی امنیت اطلاعات محسوب می‌شود. در این دوره مهارت‌های لازم جهت فارنزیک سیستم عامل ویندوز ارائه خواهد شد. روش‌های بازیابی، تحلیل و تصدیق اصالت داده‌های فارنزیک در سیستم عامل ویندوز در این دوره به دانشجویان آموزش داده خواهد شد. همچنین در این دوره روش مانیتور کردن رفتار کاربران در شبکه و روش سازمان‌دهی یافته‌ها برای استفاده در پاسخ به حوادث و شیوه ارائه آن‌ها در دعاوی قانونی شرح داده 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
- تدریس توسط مدرس دارای مدرک بین المللی CEI
- 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 روش‌های فارنزیک در سیستم عامل‌های Windows 7/8/8.1/10 و Windows Server 2008/2012
- روش‌های شناسایی شواهد حادثه و پاسخ به سوالات حیاتی مانند برنامه‌های اجرا شده، دسترسی به فایل‌ها، داده‌های دزیده شده، فایل‌های دانلود شده و ...
- تمرکز بر توانایی و قالبیت تحلیل به جای شیوه استفاده از یک ابزار خاص
- آشنایی با Windows Registry و روش‌های فارنزیک آن
- آشنایی با روش‌های فارنزیک مرورگرهای پرکاربرد وب مانند Internet Exlporer و Firefox، Chrome

مخاطبان دوره :

- کارشناسان تیم امداد رایانه‌ای
- کارشناسان مرکز عملیات امنیت
- کارشناسان جرائم رایانه‌ای
- مدیران شبکه

Course Outline :

FOR 500

1: Windows Digital Forensics and Advanced Data Triage
2: Core Windows Forensics Part I: Registry and USB Device analysis
3: Core Windows Forensics Part II-E-Mail Forensics
4: Core Windows Forensics Part III - Windows Artifact and Log File Analysis
5: Core Windows Forensics Part IV: Web Browser Forensics- Firefox, Internet Explorer, and Chrome
6: Windows Forensic Challenge

EC-Council

تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳،۸ فاکس: ۸۸۰۶۵۲۲۲