Carrier Digit
کاریار ارقام

مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی

و برگزارکننده دوره های آموزشی

Designed by
طراحی شده توسط
کاریار ارقام
Carrier Digit

دوره پایه مرکز عملیات امنیت
Security Operation Center (SOC)

Hacker Techniques, Exploits & Incident Handling (SEC 504)

مدت(ساعت): ۴۰ | **پیش نیاز:** مبانی اولیه امنیت | **اعتبار دهنده:** SANS

معرفی دوره :

فضای اینترنتی سرشار از ابزار های مختلف هکینگ و طیف وسیعی از افراد بدخواه میباشد .

اگر سازمان شما به اینترنت متصل میباشد و در بین کارکنان شما افراد ناراضی وجود دارند احتمال وقوع حمله برای شما بالاست و از این رو آشنایی با ابزار ها و تکنیک های مرسوم نفوذ به منظور دفاع در مقابل آنها امری ضروری به نظر میرسد.

این دوره پیشرفته (با رویکرد جامعیت، کاربردی بودن و چالاکی) از بهترین محتواهای آموزشی دنیا مانند: SANS، EC-Council، Cisco و بهروشهای موجود در دنیا برگرفته شده است. گزینش مطالب همراه با رعایت اصول کاربردی بودن و پیوستگی مطالب و همچنین با تاکید بر نیاز های روز جامعه متخصصین ایران ، بومی سازی شده و به شما کمک می کند تا با درکی مناسب از تاکتیک ها و استراتژی های مهاجمان در جزئیات یک حمله آشنا شوید، آسیب پذیری های خود را شناسایی نمایید، نفوذ گران را پیدا کنید و از همه مهمتر اینکه به منظور مواجه مناسب با رویداد های امنیتی Incident Handling & Response Strategy داشته باشید. از مزایای این دوره، تمرکز بر تلفیق فرآیند IH&R با SOC بوده و این فرآیند به عنوان قابلیتی بنیادین در SOC تشریح و تدریس می شود.

در این دوره آموزشی، شما به صورت سلسله مراتبی با ابزارهایی که مهاجمان با استفاده آنها تلاش می نمایند تا به فضای سایبری شما نفوذ کنند، آشنا میشوید، نحوه تجزیه و تحلیل راهکارهای مقابله با آنها را فرا میگیرید و با طریقه عملکرد تیمها در قالب Incident Response آشنا شده و چگونگی مدیریت آنها در از طریق فرآیند Incident Handling را فرا خواهید گرفت.

این دوره مناسب متخصصانی است که یا جزئی از تیم پاسخگوئی به حوادث یا SOC، هستند و یا قصد رهبری این تیمها را دارند، همچنین این دوره برای مدیران راهبری سیستم های کامپیوتری و متخصصان شبکه و حتی معماران امنیتی شبکه دوره ای بسیار مفید است زیرا از ویژگی های بارز این دوره میتوان به درک مناسب نسبت به منظور پیشگیری و Design, Build and Operate به چگونگی پروسه تشخیص و پاسخ گویی مناسب به رخداد های امنیتی استفاده نمود.

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
- طراحی شده توسط تیم اساتید کاریار ارقام

مخاطبان دوره :

- کارشناسان امنیت شبکه (زیرساخت)
- راهبران تجهیزات دیواره آتش
- تحلیلگران شبکه
- هکرهای کلاه سفید
- کارشناسان جرم‌شناسی رایانه‌ای

اهداف دوره :

- چگونه خود را برای برخورد با حملات ناخواسته امنیتی آماده کنیم
- چگونگی ایجاد و توسعه Incident Handling Process و آماده سازی تیم IR به منظور مقابله با حملات
- چگونگی انجام دفاع فعال و واکنش گرا در مقابل حملات
- چگونگی شناسایی حملات فعال در شبکه
- آشنایی با آخرین Attack Vector ها و چگونگی مقابله با آنها
- آشنایی با تکنیک ها و ابزارهای نفوذ
- آشنایی با استراتژی و ابزارهای تشخیص نفوذ

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 :
۱. آشنایی با مفاهیم Incident Handlin & Response، متدلوژیهای و الگوهای حملات در دیدگاه IH&R	9- Computer and Network Hacker Exploits - Part 1
۲. SOC requirement for IH&R، معماری SOC در حوزه IH&R و نحوه تعامل با سایر اجزا SOC	• Reconnaissance
۳. تشریح فرآیندهای مدیریت: آسیب پذیری، تهدیدات و نهایتا مدیریت ریسک و همچنین رویکردهای پیشرفته جهت شناسایی آنها	• Scanning
۴. مراحل مختلف فرآیندهای IH&R، طریقه استقرار و پیاده سازی در ساختارهای امنیت اطلاعات سازمانها	• Envisioning Concept
۵. تشریح کامل تیمهای IH&R و نقشها هریک از تیمها، نحوه تیم سازی و چینش کارشناسان و آموزش و نگهداشت منابع انسانی در تیم (با رویکرد SOC)	10- Computer and Network Hacker Exploits - Part 2
۶. تشریح تعاملات فرآیندهای Forensic Analysis and Incident Response	• Network-Level Attacks
۷. نحوه گزارش و مستندسازی IH&R و نحوه انطباق با قوانین	• Operating System and Application-level Attacks
۸. مروری بر فرآیندهای Recovery و Continuity در فرآیند IH&R و اصول طراحی برنامه های مرتبط در قالب SOC	11- Computer and Network Hacker Exploits - Part 3
	• Password Cracking
	• Web Application Attacks
	• Denial-of-Service Attacks
	12- Computer and Network Hacker Exploits - Part 4
	• Maintaining Access
	• Covering the Tracks

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