Carrier Digit
کاریار ارقام

مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی

و برگزارکننده دوره های آموزشی

Designed by
دوره طراحی شده ویژه کاریار ارقام
Carrier Digit

دوره ویژه امنیت SANS - SANS (SEC 566)

پیاده سازی و ارزیابی 20 کنترل حیاتی امنیت
Implementing and Auditing the Critical Security Controls In-Depth (20 Controls)

مدت(ساعت): 32	پیش نیاز: + SECURITY	اعتبار دهنده: SANS

معرفی دوره :

در سال 2013 آژانسهای امنیتی اروپا و امریکا بدلیل تهدیدات پیشرفته سایبری در قالب یک پروژه مشترک با حضور افرادوشرکتهایی متخصص در این حوزه، مبادرت به تدوین چارچوبی مناسب، جامع و عملکردی در مورد چگونگی اجرای کنترل های امنیتی بحرانی با رویکرد مبتنی بر ریسک امنیت را طراحی کردند.
این چارچوب تحت سندی جامع ودر20 کنترل حیاتی خلاصه گشت که بهترین راه برای جلوگیری از حملات شناخته شده و کاهش آسیب از حملات موفق است واکنون توسط نهادهای امنیتی ، دولتها، دانشگاه ها وشرکتهای خصوصی وسازمانی تصویب واجرا میگردد.
شرکت SANS براین اساس دوره ای به نام 566 طراحی کرد که کلیه این کنترل ها در آن بررسی و آنالیز میگردد.

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

مخاطبان دوره :

- فعالین حوزه امنیت سازمانها که به دنبال چارچوبهای عملکردی و کاربردی با رویکرد فنی در حوزه امنیت هستند، بطوریکه با پیاده سازی این کنترلها علاوه بر نظامند سازی سیستم امنیت، ارتباط منطقی مابین الزامات فنی و عملیاتی امنیت از یک سو و کنترلهای مدیریتی امنیت از سوی برقرار شود.

اهداف دوره :

- آشنایی با مفاهیم، نحوه پیاده سازی واستقرار کنترلهای مرتبط (به‌عنوان سرویس امنیتی)
- تشریح هریک ازمفاهیم ونحوه بکارگیری آنها در سیستمهای عملیاتی سازمانها بصورت واقعی
- ایجاد یک چارچوب منطقی، ساختارمند و قابل مدیریت جهت نظارت مدیران امنیت بر سیستمها و کارشناسان

Accredited by CARRIER DIGIT Computer Software LLC
EC-Council
تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک 242 تلفن مستقیم آموزش: 8 ،88062203 فاکس :88065222

Carrier Digit

کاریار ارقام

مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی

و برگزارکننده دوره های آموزشی

محتوای دوره :

1) تشریح تاریخچه و ساختار و نحوه تدوین کنترلها

2) ساختار سلسله مراتبی چارچوب کنترلها، رویکردهای تدوین شده

3) تشریح الگوی زنجیره مخرب حملات، انواع حملات و رفتارهایی که نفوذگران از خود بروز می دهند و همچنین تبیین مفهوم "Offence Informs Defense"

4) تقسیم بندی کنترلها و اولویت پیاده سازی هریک از زیرکنترلها (بهبودهای سریع، بهبودهای ملموس و اثرگذار، بهبود نهادینه و ماندگار، بهبودهای پیشرفته)

5) تشریح هریک از کنترلها و مزایای اجرا آنها (توضیح کلی کنترل، تهدیدات ناشی از فقدان کنترل، مثالهایی از ابزار نفوذگران که منجر به نفوذ می شود، سناریوهای واقعی نفوذ، اهداف پدافند سایبری، طراحی سنسورهای لازم جهت کنترل، مثالی از اسکریپت های خودکارساز)

6) مروری بر کنترلهای 20 گانه :

a) موجودی تجهیزات مجاز و غیرمجاز

b) موجودی نرم افزارهای مجاز و غیرمجاز

c) پیکربندی امنیتی سخت افزارها و نرم افزارهای: موبایل، سرورها لپ‌تاپها وکامپیوترها

d) پویش مداوم آسیب‌پذیریها و راهکارهای مقابله

e) نظارت بر اعطای دسترسی های راهبران و کاربران ویژه

f) بررسی و تجزیه و تحلیل حوادث

g) حفظ و مراقبت بر مرورگرهای وب و Email

h) مقابله با بدافزار

i) محدودسازی و نظارت بر پروتکلها، سرویسها و پورتها

j) تسهیلات بازیابی داده ها

Course Outline :

k) تنظیمات امنیتی بر روی تجهیزات شبکه مانند فایروالها،روتر ها و سوییچها

l) کنترل ترافیک شبکه

m) پاسداری و مراقبت از شبکه ها

n) اعطای دسترسی براساس نیاز

o) کنترل دسترسی بر روی شبکه های بیسیم

p) نظارت بر حسابهای کاربری

q) مهارتهای امنیتی و آموزشهای موردنیاز جهت بطرف نمودن کمبودها

r) امنیت نرم افزار های کاربردی

s) مدیریت پاسخگوئی به حوادث

t) آزمونهای نفوذ

7) اهمیت و جایگاه کنترلها در ساختار امنیت فآوا

8) مقایسه کنترلهای حساس امنیتی (CSC) با الزامات مندرج در NIST SP 800-53

9) مقایسه کنترلهای حساس امنیتی (CSC) با سایر الزامات امنیتی معروف

10) نحوه ممیزی و ارزیابی (متدلوژی) کنترلهای حساس امنیتی (CSC) پس از پیاده سازی در سازمان

11) رویکرد پنجگانه پیاده سازی کنترلها به منظور حفظ اثربخشی آنها (شناسایی الگوی حملات نفوذگران، اولویت بندی پیاده سازی کنترلها، شاخصهای کنترل اثربخشی، ممیزی و پایش مستمر و دفاع خودکار و اتوماتیک)

12) نحوه ریشه یابی مشکلات و خرابیها

Accredited by CARRIER DIGIT Computer Software LLC

EC-Council

تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک 242 تلفن مستقیم آموزش: 8 ،88062203 فاکس :88065222