Carrier Digit
کاریار ارقام

مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی

و برگزارکننده دوره های آموزشی

شکار تهدیدات سایبری

Threat Hunting & Intelligence

مدت(ساعت): ۳۵ | **پیش نیاز:** CEH | **اعتبار دهنده:** ندارد

معرفی دوره :

در این دوره روش‌های نوین تشخیص تهدیدات پیشرفته سایبری به صورت تئوری و عملی (با پلتفرم‌های Splunk و ELK) مورد بررسی قرار می‌گیرد. دانشجویان در این دوره با روش‌های مختلف نفوذ پیشرفته و همچنین نحوه بررسی و تحلیل داده‌های امنیتی با رویکرد تشخیص تهدیدات آشنا خواهند شد.

اهداف دوره :

- آشنایی با روش‌های سنتی تشخیص تهدیدات سایبری
- فراگیری رویکردها و روش‌های تشخیص تهدیدات پیشرفته سایبری
- فراگیری پلتفرم‌های مطرح Splunk و ELK به‌صورت عملیاتی
- فراگیری عملیاتی جدیدترین متدهای تحلیل لاگ
- فراگیری عملیاتی روش‌های تشخیص نفوذ تهدیدات سایبری

امتیازات دوره :

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

مخاطبان دوره :

- تحلیلگران امنیت
- کارشناسان مرکز عملیات امنیت
- مدیران سیستم و شبکه
- مدیران امنیتی فنی
- کارشناسان تحلیل نفوذ و حملات سایبری

محتوای دوره :

مروری بر معماری و راهکارهای سنتی امنیت شبکه (Firewall، NIDS، HIDS و ...)

مروری بر حملات لایه شبکه و وب

بررسی راهکارهای سنتی تشخیص تهدیدات

مروری بر منابع داده

- بررسی ساختار بسته‌ها و پروتکل‌های مختلف شبکه
- بررسی ساختار لاگ‌های مختلف تجهیزات امنیتی

معرفی روش‌های نوین تشخیص تهدیدات سایبری

- Threat Hunting
- Threat Intelligence
- مروری بر APT ها و مکانیزم های تشخیص APT
- معرفی مدل Kill Chain و MITRE ATT@CK
- بررسی یک نمونه تهدید پیشرفته APT با استفاده از Threat Intelligence و مدل MITRE

معرفی SIEM

- معرفی پلتفرم تحلیل داده Splunk

Course Outline :

- نصب و برپاسازی Splunk
- معرفی SPL و ماژول‌های مختلف Splunk
- معرفی پلتفرم تحلیل داده ELK Stack (ElasticSearch)
- نصب و برپاسازی ELK

تشخیص و تحلیل گام‌های نفوذ مهاجمین با پلتفرم Splunk و ELK

- تشخیص و تحلیل **Lateral Movement**
- تشخیص و تحلیل کانال کنترل و فرمان C۲
- تشخیص و تحلیل نمونه باج افزار
- تشخیص و تحلیل **Privilege Escalation**
- تشخیص و تحلیل **Data Exfiltration**
- بصری سازی (**Virtualization**) در **Splunk** و **ELK**
- ساخت داشبوردهای مختلف در **Splunk** و **ELK**

بررسی پیشرفته تهدیدات محتمل در سازمان ها با رویکرد Threat Hunting

تحلیل ترافیک با استفاده از Wireshark

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