تشخیص حمله، شکار تهدید و هوش تهدید

Threat Detection, Hunting and Intelligence

مدت(ساعت): 40

معرفی دوره :

صرف نظر از اینکه در کدام زمینه امنیت -دفاع یا نفوذ- فعالیت می کنید، یادگیری مفاهیم Threat Hunting و Threat Intelligence امری ضروری است.

یک متخصص امنیت نمی تواند بدون دانش کامل از تکنیکهای نفوذ، از سازمان در برابر حملات سایبری محافظت کند. به همین صورت، دانستن تکنیک های تشخیص حمله هم برای یک تست نفوذگر حرفه ای الزامی است.

امروزه سازمانهایی با سطح بلوغ امنیتی بالا، در کنار راهکارهای سنتی امنیت، قسمت زیادی از تمرکزشان را به کشف فعالیت های پس از نفوذ و شکار تهدید یا Threat Hunting اختصاص داده اند. در این دوره آموزشی بعد از مرور مفاهیم مهم تشخیص حمله، شکار تهدید و هوش تهدید، به بررسی استراتژی ها و تکنیک ها و ابزارهای مختلف شکار تهدید می پردازیم. در این دوره، دانشجو با تکنیکهای پس از نفوذ و روشهای تشخیص آنها به طور عملی آشنا می شود.

اهداف دوره :

بعد از گذراندن این دوره قادر خواهید بود:

- برنامه‌ی Threat Hunting خود را با رویکرد دفاع فعال تدوین کنید.
- آشنایی کامل از فعالیت های پس از نفوذ، تهدیدات درون شبکه‌ی سازمان را به طور فعال شکار کنید.
- استراتژی های تدافعی سازمانتان را به طور مداوم و بر اساس آخرین تکنیک ها و تاکتیک های نفوذگران بهبود داده و تنظیم کنید.
- از فیدهای هوش تهدید و IOC برای شکار تهدیدات شناخته شده استفاده کنید.
- با تحلیل ترافیک شبکه، فعالیت های غیرعادی و حملات را شناسایی کنید.
- از ابزارهایی مانند osquery، Sysmon و ELK برای جمع آوری و تحلیل رخدادها، و کشف الگوهای حمله استفاده کنید.

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

پیش نیاز های دوره :

- آشنایی کامل با مفاهیم شبکه و پروتکل های شبکه از جمله DNS و HTTP
- آشنایی کامل با مفاهیم امنیت اطلاعات
- آشنایی با ابزارها و روشهای تست نفوذ (در سطح متوسط تا پیشرفته)
- آشنایی ابتدایی با Splunk / Elasticsearch و ابزارها و مفاهیم مدیریت لاگ

مخاطبان دوره :

این دوره آموزشی برای تحلیلگران امنیت و SOC که به طور فعال به دنبال تشخیص حملات و تهدیدات امنیتی هستند، طراحی شده است.

- مهندسان و تحلیلگران مراکز عملیات امنیت (SOC)
- متخصصان تست نفوذ و Red Team
- مهندسان امنیت شبکه
- اعضای تیم پاسخ به حوادث سایبری (IR)
- مشاوران امنیت اطلاعات
- مدیرانی که قصد راه اندازی تیم های کشف / شکار تهدیدات سایبری و Threat Intelligence را دارند.
- تمام علاقه مندان به مباحث Threat Intelligence و Hunting

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