Carrier Digit
کاریارارقام

مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی

و برگزارکننده دوره های آموزشی

دوره اصلی مرکز عملیات امنیت
Security Operation Center (SOC I)

Continuous Monitoring and Security Operations (SEC 511)

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

معرفی دوره :

یکی از معضلات اصلی تیم های امنیتی و مرکز عملیات امنیت شناسایی حملات امنیتی می باشد. برای اینکه عملیات شناسایی به درستی انجام شود و بتوان حملات را شناسایی کرد نیاز است تا طراحی و سیاست های نظارتی مانیتورینگ مناسب وجود داشته باشد تا بتوان توسط یک ابزار مناسب فعالیت نفوذگران را شناسایی کرد.

دوره **SEC 511** برای افزایش قدرت تیم های عملیات امنیتی طراحی شده است. در این دوره، مفاهیم TTP یا همان Tactics، Techniques و Procedure ها که در واقع همان تاکتیک ها و تکنیک های هکر ها می باشند مورد بررسی قرار می گیرند و روش های نظارت مستمر (Continues Monitoring) و دفع با کاهش اثر ها (Mitigation Techniques) مورد بررسی قرار می گیرند. یکی از اصول دفاع سایبری در حال حاضر بر پایه بروز رسانی دانش TTP بنا شده است. در چند سال گذشته استفاده از یک فایروال و سامانه تشخیص نفوذ به تنهایی برای محافظت از دارایی ها امنیتی اکتفا می کرد. اما در زمان حال، هکرها از تکنیک های متفاوت و پیچیده ای نظیر Client Attacks، حملات تحت وب و Application های ناشناخته استفاده می کنند که دیگر با ابزار سنتی امنیت قابل شناسایی نیستند. در واقع این دوره برای تقویت تیم های Blue Team در سازمان ها طراحی شده است که وظیفه آنها شناسایی و دفع حملات، گاهی به صورت همزمان و Real-time می باشد.

اهداف دوره :

- مقایسه ساختار حملات نسل جدید با حملات سنتی
- آشنایی با روش های شناسایی حملات مبتنی بر نظارت بر تجهیزات شبکه ای
- آشنایی با روش های شناسایی حملات سیستمی
- آشنایی با روش های نظارت مستمر

عنوان شغلی دوره :

- کارشناس تحلیل و آنالیز حملات

امتیازات دوره :

- اعطای مدرک فارسی و انگلیسی با مجوز رسمی از :
  - مجوز از اداره کل نظام مدیریت امنیت اطلاعات (نما)
  - 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 :

- کارشناس تحلیل و آنالیز حملات
- کارشناس مرکز عملیات امنیت
- عضو تیم Cert
- آنالیزور و تشخیص نفوذ
- مدیر و کارشناس امنیت سایبری

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

Carrier Digit

کاریار ارقام

مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی

و برگزار کننده دوره های آموزشی

ویژگی های دوره :

- ارائه جزوه Customize دوره
- ارائه ابزار های مورد استفاده در طول دوره
- به اشتراک گذاری تجربیات بومی مدرسان دوره به منظور کاربردی نمودن هرچه بیشتر دوره

محتوای دوره :

Course Outline :

SEC 511

Current State Assessment, SOCs, and Security Architecture

- Traditional Security Architecture
- Modern Security Architecture Principles
- Security Architecture - Key Techniques/Practices
- Security Operations Center (SOC)

SOCs and Defensible Network Security Architecture

- SOCs/Security Architecture - Key Infrastructure Devices
- Traditional and Next Generation Firewalls, and NIPS
- Web Application Firewall
- Malware Detonation Devices
- HTTP Proxies, Web Content Filtering, and SSL Decryption
- SIMs, NIDS, Packet Captures, and DLP
- Honeypots/Honeynets
- Network Infrastructure - Routers, Switches, DHCP, DNS
- Mobile Devices and Wireless Access Points
- Threat Intelligence

SOCs and Defensible Endpoint Security Architecture

- Security Architecture - Endpoint Protection
- Antimalware
- Host-based Firewall, Host-based IDS/IPS
- Application Whitelisting, Application Virtualization
- Privileged Accounts, Authentication, Monitoring, and UAC
- Whole Disk Encryption
- Virtual Desktop Infrastructure
- Browser Security
- EMET
- Dangerous Endpoint Applications
- Patching
- Current Architectural Challenges

Network Security Monitoring

- Continuous Monitoring Overview
- Network Security Monitoring (NSM)
- Evolution of NSM
- The NSM Toolbox
- NIDS Design
- Analysis Methodology
- Understanding Data Sources

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