مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی

و برگزارکننده دوره های آموزشی

SIEM و رو شهای تحلیل داده SANS (SEC 555)

SIEM With Tactical Analytics

مدت(ساعت): ۵۰ | **پیش نیاز:** SANS 504 | **اعتبار دهنده:** SANS

معرفی دوره :

در این دوره مهارت های لازم جهت کار با سیستم های تحلیل و مدیریت داده های امنیتی (SIEM) ارایه خواهد شد. دانشجویان در این دوره علاوه بر شناخت نسبتا کامل از SIEM و انواع مختلف لاگ، تکنیک ها و روش های نوین تحلیل تهدیدات سایبری را نیز فرا می گیرند. این دوره تلفیقی از مباحث تئوری و عملی است و کار با بسترهای تحلیل داده امنیتی نظیر Splunk و ELK و همچنین سناریوهای عملیاتی تشخیص تهدیدات سایبری به دانشجویان آموزش داده می شود.

اهداف دوره :

- آشنایی با مفاهیم SIEM، SOC و لاگ
- آشنایی کامل با معماری سیستمی عملیاتی مراکز عملیات امنیت و SIEM ها
- فراگیری عملیاتی SIEM و جمع آوری لاگ
- فراگیری عملیاتی جدیدترین متدهای تحلیل لاگ
- فراگیری عملیاتی روش های تشخیص تهدیدات سایبری با استفاده از SIEM

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
- 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 :

- Methods of collection
- Adding additional logging
- Windows filtering and tuning
- Analyze critical events based on attacker patterns
- Host-based firewall logs
- Credential theft and reuse
- Monitor PowerShell

Baselining and User Behavior Monitoring
- Identify authorized and unauthorized assets
- Identify authorized and unauthorized software
- Baseline data

Tactical SIEM Detection and Post-Mortem Analysis
- Centralize NIDS and HIDS alerts
- Analyze endpoint security logs
- Augment intrusion detection alerts
- Analyze vulnerability information
- Correlate malware sandbox logs with other systems to identify victims across enterprise
- Monitor Firewall Activity
- SIEM tripwires
- Post mortem analysis

Course Outline :

SIEM Architecture, SOF-ELK
- State of the SOC/SIEM
- Log Monitoring
- Logging architecture
- SIEM platforms
- Planning a SIEM
- SIEM Architecture
- Ingestion techniques and nodes
- Data queuing and resiliency
- Storage and speed
- Analytical reporting

Service Profiling with SIEM
- Detection methods and relevance to log analysis
- Analyzing common application logs that generate tremendous amounts of data
- Apply threat intelligence to generic network logs
- Active Dashboards and Visualizations

Advanced Endpoint Analytics
- Understanding value

تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳،۸ فاکس: ۸۸۰۶۵۲۲۲