SEMATEC
IT Training Center

For500 Windows Forensics

خلاصه دوره:

FOR500 دانش جامع جرم یابی دیجیتال را در مورد سیستم عامل های مایکروسافت ویندوز ایجاد می کند که ابزارهایی برای بازیابی، تجزیه و تحلیل و تأیید اعتبار داده های جرم یابی، ردیابی فعالیت کاربر در شبکه، و سازماندهی یافته ها برای استفاده در پاسخ به حادثه، بررسی های سیستم داخلی، بررسی سرقت مالکیت معنوی و مدنی ارائه می دهد. از این دانش برای اعتبارسنجی ابزارهای امنیتی، افزایش ارزیابی آسیب‌پذیری، شناسایی تهدیدات داخلی، ردیابی هکرها و بهبود سیاست‌های امنیتی استفاده می شود .

مدت دوره: 30 ساعت

پیش نیاز دوره: CHFI, CEH

مخاطب دوره:

- تحلیلگران امنیت
- کارشناسان جرم یابی سایبری
- کارشناسان شکارتهدیدات

اهداف دوره:

در انتهای این دوره دانشجویان قادر خواهند بود:

- قابلیت استفاده از تکنیک های بررسی شده با تمرکز بر روی ویندوز 7، ویندوز 8.1/8، ویندوز 10، ویندوز 11 و محصولات ویندوز سرور، تجزیه و تحلیل عمیق را استفاده کنند.
- انجام "جرم یابی سریع" برای ارزیابی و تریاژ سریع سیستم ها برای ارائه پاسخ های سریع را انجام دهند.
- شناسایی رفتار کاربر و فعالیت های انجام شده را شناسایی کنند.

سرفصل دوره:

- Digital Forensics and Advanced Data Triage
- Registry Analysis, Application Execution, and Cloud Storage

- Shell Items and Removable Device Profiling
- Email Analysis, Windows Search, SRUM, and Event Logs
- Web Browser Forensics

منبع درسی:

https://www.sans.org/cyber-security-courses/windows-forensic-analysis/