سازمان نظام صنفی رایانه ای استان تهران	**کارگاه مقدماتی فورنسیک دیجیتال در رسیدگی به رخدادهای امنیتی**	سازمان نظام صنفی رایانه ای کشور استان تهران
کمیسیون افتا		

عنوان فارسی وبینار:
کارگاه دیجیتال فورنسیک

عنوان انگلیسی وبینار:
Digital Forensic in Incident Response

دسته بندی دوره: Forensic	**مدت کل:** ۳ ساعت	**مدت تئوری: ۷۵ دقیقه**	**مدت عملی: ۳۰ دقیقه**

معرفی و کاربرد وبینار:

در این رویداد، شرکت‌کنندگان با کاربرد و فرآیند رسیدگی به رخداد و فورنسیک دیجیتال آشنا می گردند. رویکردی روشمند برای انجام فورنسیک دیجیتال که شامل جستجو و اکتساب، نگهداری، تحلیل و گزارش شواهد دیجیتال است، ارائه می گردد. ضمن اشاره به روش های جمع آوری اطلاعات، فراگیران با ابزارهای مورد نیاز جهت انجام فورنسیک و شیوه استفاده از برخی آنها آشنا می گردند.

اهداف وبینار:

- آشنایی با فرآیند رسیدگی به رخداد
- آشنایی با فرآیند فورنسیک
- آشنایی با فورنسیک سیستم‌ها، سیستم‌های عامل، شبکه‌ها و برنامه های کاربردی تحت وب
- آشنایی با چگونگی اکتساب و تحلیل داده‌ها
- آشنایی با ابزارهای فورنسیک

سرفصل مطالب:

- **آماده سازی و حضور افراد (۱۰ دقیقه)**
- **نشست اول: (۶۰ دقیقه)**
  - مفاهیم رخداد امنیتی، مدیریت رخداد و رسیدگی به رخداد امنیتی --- ۱۰ دقیقه
  - فرآیند رسیدگی به رخداد --- ۱۵ دقیقه
  - مفهوم فورنیسک (فارنزیک) و ارتباط آن با رسیدگی به رخداد --- ۱۰ دقیقه
  - فرآیند فورنیسک --- ۱۰ دقیقه
  - جمع آوری اطلاعات و ملاحظات آن --- ۱۵ دقیقه
- **پرسش و پاسخ نشست اول** --- ۱۵ دقیقه
- **نشست دوم (۶۰ دقیقه)**
  - معرفی ابزارهای فورنسیک --- ۱۵ دقیقه
  - فورنسیک سیستم عامل (اشاره به جمع آوری شواهد از سیستم عامل) --- ۱۵ دقیقه
  - فورنسیک حافظه (انجام دامپ حافظه و بررسی آن) --- ۱۵ دقیقه
  - فورنسیک شبکه (اشاره به منابع جمع آوری لاگ در شبکه و تحلیل یک لاگ نمونه) --- ۱۵ دقیقه
- **پرسش و پاسخ نشست دوم** --- ۱۵ دقیقه

رویداد دوم: تحلیل فورنسیک رجیستری ویندوز

مخاطبان دوره:

- اعضای تیم‌های واکنش به رخداد و مراکز عملیات امنیت
- مدیران امنیت اطلاعات
- کارشناسان و مدیران فناوری اطلاعات
- مهندسان شبکه/ سیستم‌ها
- کارشناسان رسیدگی به جرایم سایبری

پیش نیازهای دوره:

- آشنایی با مبانی امنیت سایبری

مدرس:

- مهندس محمد سیفی
  - کارشناس ارشد امنیت اطلاعات
  - مدرس دوره های مدیریت رخداد و فورنسیک

زمان بندی پیشنهادی:

رسمیت یافتن جلسه: ۱۰ دقیقه

نشست اول: ۶۰ دقیقه

استراحت: ۱۰ دقیقه

نشست دوم: ۶۰ دقیقه

- پرسش و پاسخ: ۳۰ دقیقه