

# الأدلة الجنائية والتحقيقات الرقمية

## لمحة عامة

- نتيجة للاختراقات والجرائم الالكترونية في عالم الانترنت اضطر المشرعون إلى تطوير متطلبات الاستجابة للحوادث التشغيلية وضوابط واجراءات الجنايات الرقمية. كما أن اختراق البيانات تطور بصورة أكثر تعقيداً مما دعت الحاجة لوجود تحكم الكتروني داخلي قوي.
- هذه الدورة تمكن المشاركين من التعامل مع والتحقيق في الجرائم والمخالفات الرقمية الداخلية والخارجية وتطبيق عمليات وإجراءات قوية يمكن من الاستحواذ الرقمي للصور والوسائط المتعددة من أجهزة الهواتف المتحركة والكمبيوتر تماشياً مع العمليات التي أثبتت جدواها لتأمين المواد الثبوتية
- تعطيهذه الدورة التدريبية للمشاركين الفرصة لتطبيق أفضل الممارسات لضمان الحفاظ على سلامة البيانات الرقمية. كما توفر الدورة تدريباً عملياً وواقعياً مدعوماً بهياكل أكاديمية وقانونية تشكل الأساس لعلوم الطب الجنائي.
- تغطي هذه الدورة أيضاً متطلبات (SOC) و (CSIRT) وتزود المشاركين بالمهارات التي يحتاجون إليها في التحقيق الرقمي.

## المنهجية

- تتضمن هذه الدورة جلسات عملية ومناقشات جماعية بعد حضور أشرطة الفيديو بالإضافة إلى العروض التطبيقية الحية.

## أهداف الدورة

سيتمكن المشاركون في نهاية الدورة من:

- تطبيق منهجية الطب الجنائي الرقمي في بيئة تشغيلية
- وضع إستراتيجية لتحديد إطار استجابة الطب الجنائي الرقمي
- إجراء تحقيقات في وسائل الاعلام الاجتماعية والبرمجيات الخبيثة والفيروسات
- إدارة مشهد-من الجريمة الرقمية والأدلة الرقمية والأثرية
- التحقيق في التكنولوجيات المتنقلة ووسائل الإعلام الأخرى التي قد تحمل المواد الثبوتية والأثرية
- تطبيق تقنيات لاستخراج الصور من أنظمة القطع الأثرية

## الفئات المستهدفة

- تم تصميم هذه الدورة لمتخصصي تكنولوجيا المعلومات ومحققي الاحتيالات ومدققي الحسابات و CSIRT ومحللي مركز العمليات الامنة SOC الذين يعملون في شركات معرضة للهجمات الرقمية. كما تفيد أفراد الشرطة والجيش وضباط مراقبة السلوك وغيرهم من أفراد الأمن الذين يتعاملون مع التحقيقات الالكترونية.

## المحاور العلمية

- الاستجابة للحوادث
- فهم الطب الجنائي الرقمي
- إجراء التحقيق في الجرائم الرقمية
- تطبيق العلم الجنائي

## التشريح الجنائي الرقمي – الخلفية والمعلومات القانونية

- مقدمة في العلم الجنائي
- المصطلحات والتعاريف
- سلسلة الجرائم الرقمية
- خلفية عن الجرائم الرقمية
- تاريخها حالة من حالات واقع الحياة
- قوانين الجنائية الرقمية
- تشريعات الجنائية الرقمية
- معايير الأدلة الجنائية الرقمية
- أساسيات الجنائية الرقمية
- المخاطر التي تواجهه المنظمات

## اطار استجابة الجنائيات الرقمية

- مجموعة أدوات المستجيب الجنائي الرقمي الأول
- مشهد من إدارة الجريمة الرقمية
- مركز العمليات الآمنة (SOC)
- (CSIRT) فريق الاستجابة لحوادث أمن الحاسوب
- الادوار والمسؤوليات
- تنفيذ إطار عمل
- إدارة الحالة

## جمع ومعالجة الأدلة الرقمية

- نظام اسم النطاق (DNS)
- البنية التحتية الأمنية الموسعة
- التحقيق في التكنولوجيات المتنقلة
- الاستحواذ على الأدلة الرقمية والأدوات
- التعامل مع الأدلة الرقمية والأدوات
- تجهيز الأدلة الرقمية والأدوات
- بروتوكولات إدارة الحالة
- بروتوكولات لاسلكية
- تقنيات الدعم
- ممارسات التقارير

## التحقيقات في الجرائم الرقمية الداخلية والخارجية

- OSINT (تبادل معلومات المصادر المفتوحة)
- دورها في تحقيقات الطب الجنائي الرقمي
- تعريف الجرائم الداخلية
- تعريف الجرائم الخارجية
- استغلال الأطفال والتحقيقات
- التطبيقات الخبيثة
- الفدية
- قدرات مكافحة الجنايات
- الجنايات الرقمية والإرهاب