



الجنائيات والتحقيقات الرقمية



الجنائيات والتحقيقات الرقمية

المقدمة:

نتيجة للاختراقات والجرائم الالكترونية في عالم الانترنت اضطر المشرعون إلى تطوير متطلبات الاستجابة للحوادث التشغيلية وضوابط واجراءات الجنائيات الرقمية، كما أن اختراق البيانات تطور بصورة أكثر تعقيدا مما دعت الحاجة لوجود تحكم الكتروني داخلي قوي، هذه الدورة التدريبية ستمكن المشاركين فيها من التعامل مع التحقيق في الجرائم والمخالفات الرقمية الداخلية والخارجية وتطبيق عمليات وإجراءات قوية يمكن من الاستحواذ الرقمي للصور والوسائط المتعددة من أجهزة الهواتف المتحركة والكمبيوتر تماشيا مع العمليات التي أثبتت جدواها لتأمين المواد الثبوتية، كما ستعطي هذه الدورة التدريبية للمشاركين الفرصة لتطبيق أفضل الممارسات لضمان الحفاظ على سلامة البيانات الرقمية، تغطي هذه الدورة أيضاً متطلبات SOC وCSIRT وتزود المشاركين بالمهارات التي يحتاجون إليها في التحقيق الرقمي.

الفئات المستهدفة:

- متخصصي تكنولوجيا المعلومات.
- محققي الاحتيالات ومدققي الحسابات وCSIRT.
- محلي مركز العمليات الآمنة SOC الذين يعملون في شركات معرضة للهجمات الرقمية.
- أفراد الشرطة والجيش وضباط مراقبة السلوك وغيرهم من أفراد الأمن الذين يتعاملون مع التحقيقات الالكترونية.
- كل من يجد في نفسه الحاجة لهذه الدورة ويرغب بتطوير مهاراته وخبراته.

الأهداف التدريبية

في نهاية هذا البرنامج، سيكون المشاركون قادرين على:

- 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 المشهد في 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.

الكفاءات المستهدفة:

- التشريح الجنائي الرقمي، الخلفية والمعلومات القانونية.
- قوانين الجناية الرقمية.
- تشريعات الجناية الرقمية.
- جمع ومعالجة الأدلة الرقمية.
- نظام اسم النطاق DNS.
- التحقيقات في الجرائم الرقمية الداخلية والخارجية.
- OSINT تبادل معلومات المصادر المفتوحة.

محتوى الدورة

الوحدة الأولى، 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 الجناية الرقمية
- تشريعات الجناية الرقمية
- معايير الأدلة الجناية الرقمية
- أساسيات الجناية الرقمية
- المخاطر التي تواجه المنظمات
- إطار استجابة الجنايات الرقمية
- مجموعة أدوات المستجيب الجنائي الرقمي الأول
- مشهد من إدارة الجريمة الرقمية
- مركز العمليات الآمنة SOC
- CSIRT فريق الاستجابة لحوادث أمن الحاسوب
- الأدوار والمسؤوليات
- تنفيذ إطار عمل
- إدارة الحالة

الوحدة الثانية، 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

الوحدة الثالثة، التحقيقات في الجرائم الرقمية الداخلية والخارجية:

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