المقدمة:

في ظل تصاعد الهجمات الإلكترونية وازدياد وتيرة الجرائم الرقمية، بات من الضروري تطوير منظومة الاستجابة للحوادث الأمنية وتعزيز الضوابط والإجراءات الخاصة بالتحقيقات الرقمية. ومع تعقّد أنماط اختراق البيانات وتطور أساليب الهجمات الإلكترونية، أصبح من الضروري وجود آليات رقابية داخلية قوية تعتمد على تقنيات متقدمة.

تُقدّم هذه الدورة التدريبية إطارًا شاملًا يمكّن المشاركين من التعامل بفعالية مع التحقيقات المتعلقة بالجرائم والمخالفات الرقمية، سواء كانت داخلية أو خارجية، من خلال تطبيق إجراءات راسخة للاستحواذ على الأدلة الرقمية من مختلف الأجهزة مثل الهواتف المحمولة وأجهزة الحاسوب، بما يتماشى مع المعايير المعتمدة لحماية المواد الثبوتية.

كما توفّر الدورة فرصة عملية للمشاركين لتطبيق أفضل الممارسات في الحفاظ على سلامة البيانات الرقمية خلال مراحل التحقيق المختلفة. وتتناول أيضًا متطلبات مراكز العمليات الأمنية (SOC) وفِرَق الاستجابة لحوادث أمن المعلومات (CSIRT)، مع تزويد المشاركين بالمهارات اللازمة في مجال التحقيقات الرقمية الحديثة.

الفئات المستهدفة:

المتخصصون في تكنولوجيا المعلومات.

محققو الاحتيال ومدققو الحسابات وأعضاء فرق الاستجابة لحوادث أمن المعلومات (CSIRT).

محللو مراكز العمليات الأمنية (SOC) العاملون في بيئات مهددة بهجمات إلكترونية.

أفراد الشرطة، والعسكريون، وضباط مراقبة السلوك، وغيرهم من أفراد الأمن المكلّفين بالتحقيقات الرقمية.

جميع من يشعر بحاجة إلى تطوير مهاراته وخبراته في هذا المجال ويرغب بالانخراط فيه.

الأهداف التدريبية:

بنهاية هذه الدورة التدريبية، سيتمكن المشاركون من:

تطبيق منهجيات التحليل الجنائي الرقمي ضمن بيئات تشغيلية مختلفة.

تطوير استراتيجيات فعالة لتحديد وتنفيذ إطار استجابة للجنائيات الرقمية.

إجراء تحقيقات في الوسائط الرقمية، تشمل وسائل التواصل الاجتماعي والبرمجيات الخبيثة والفيروسات.

إدارة مسرح الجريمة الرقمية وجمع وتحليل الأدلة الرقمية والآثار ذات الصلة.

التحقيق في الأجهزة المحمولة ووسائط التخزين التي قد تحتوي على أدلة رقمية أو مواد أثرية.

استخدام تقنيات فعالة لاستخراج الصور والمعلومات من أنظمة تحتوي على بيانات أثرية رقمية.

الكفاءات المستهدفة:

فهم شامل للتشريح الجنائي الرقمي، بما يشمل الخلفيات القانونية والمعلومات التقنية ذات الصلة.

الإلمام بالقوانين والتشريعات المتعلقة بالجرائم الرقمية.

المهارة في جمع الأدلة الرقمية وتحليلها ومعالجتها بطريقة تضمن سلامتها.

الإلمام بنظام أسماء النطاقات (DNS) ودوره في التحقيقات.

القدرة على التعامل مع التحقيقات في كل من الجرائم الرقمية الداخلية والخارجية.

استخدام تقنيات OSINT (معلومات المصادر المفتوحة) في دعم عمليات التحليل الجنائي الرقمي.

محتوى الدورة التدريبية:

الوحدة الأولى: الجنائي الرقمي - الخلفية والمعلومات القانونية

مقدمة حول علم الجنائيات الرقمية.

شرح المصطلحات والتعريفات الأساسية.

دراسة تسلسل الجرائم الرقمية.

استعراض الخلفية والتاريخ المرتبط بالجرائم الرقمية، مع حالات واقعية.

قوانين وتشريعات الجنائيات الرقمية.

المعايير الدولية المتعلقة بالأدلة الرقمية.

المبادئ الأساسية في علم الجنائيات الرقمية.

أبرز المخاطر التي تواجه المؤسسات في العالم الرقمي.

هيكلية إطار الاستجابة للتحقيقات الرقمية.

تجهيز أدوات المستجيب الرقمي الأول.

إدارة المشهد في الجرائم الرقمية.

نظرة على مراكز العمليات الأمنية (SOC).

فريق الاستجابة لحوادث أمن الحاسوب (CSIRT): الأدوار والمسؤوليات.

تنفيذ إطار عمل فعال لإدارة التحقيقات الرقمية.

تقنيات إدارة الحالات.

الوحدة الثانية: جمع ومعالجة الأدلة الرقمية

فهم دور نظام أسماء النطاقات (DNS) في التحقيقات الرقمية.

نظرة على البنية التحتية للأمن الموسّع.

التحقيق في تقنيات الأجهزة المحمولة.

خطوات الاستحواذ على الأدلة الرقمية.

كيفية التعامل مع الأدلة الرقمية وتجهيزها بشكل سليم.

بروتوكولات إدارة القضايا الرقمية.

بروتوكولات الاتصالات اللاسلكية ودورها في التحقيقات.

تقنيات الدعم الفني ذات الصلة.

إعداد التقارير والممارسات المرتبطة بها.

الوحدة الثالثة: التحقيقات في الجرائم الرقمية الداخلية والخارجية

توظيف معلومات المصادر المفتوحة (OSINT) في دعم عمليات التحقيق.

الفرق بين الجرائم الداخلية والخارجية من حيث المفهوم والممارسة.

التعامل مع البرمجيات الخبيثة وتطبيقات الفدية (Ransomware).

التعرف على القدرات الرقمية المطلوبة لمكافحة الجرائم.

دور التحقيقات الجنائية الرقمية في مكافحة الإرهاب والتهديدات السيبرانية المعقدة.