MERCURY

إدارة عمليات البحث الجنائي

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

إدارة عمليات البحث الجنائي

المقدمة:

في ظل التطور المتسارع للجرائم الإلكترونية وارتفاع أعداد اختراقات الإنترنت، كان لزامًا على المشرعين تطوير متطلبات استجابة قوية للحوادث الرقمية وضوابط إجراءات الجنايات الإلكترونية. حيث أن اختراق البيانات أصبح أكثر تعقيدًا، مما يستدعي وجود آليات تحكم إلكتروني داخلي قوية.

تهدف دورة إدارة عمليات البحث الجنائي، إلى تزويد المشاركين بالمهارات اللازمة للتعامل مع التحقيق في الجرائم والمخالفات الرقمية التي تحدث داخل المؤسسات أو خارجها. كما تشمل تطبيق الإجراءات المعتمدة لاستخلاص الأدلة الرقمية من مختلف الأجهزة الإلكترونية مثل الهواتف المتحركة وأجهزة الكمبيوتر، بما يتماشى مع أفضل الممارسات العالمية لضمان تأمين وحفظ المواد الثبوتية.

تغطي الدورة التدريبية في إدارة عمليات البحث الجنائي، أيضًا متطلبات فرق الاستجابة لحوادث الأمن السيبراني SOC و CSIRT وتزود المشاركين بالمهارات اللازمة لإجراء التحقيقات الرقمية وفقًا للمعايير الدولية.

الفئات المستهدفة:

- متخصصو تكنولوجيا المعلومات.
- محققو الاحتيالات، مدققو الحسابات وفرق CSIRT.
- محللو مركز العمليات الآمنة SOC في الشركات المعرضة للهجمات الرقمية.
- أفراد الشرطة والجيش، ضباط مراقبة السلوك وأفراد الأمن المتعاملين مع التحقيقات الإلكترونية.
- أي شخص يرغب في تطوير مهاراته في التحقيق الجنائي الرقمي.

الأهداف التدريبية:

في نهاية هذا البرنامج، سيكون المشاركون قادرين على:

- تطبيق منهجية الطب الجنائي الرقمي في بيئات العمل المختلفة.
- وضع استراتيجيات لتحديد إطار استجابة الجنائي الرقمي.
- إجراء تحقيقات في وسائل الإعلام الاجتماعية، البرمجيات الخبيثة، والفيروسات.
- إدارة مشهد الجريمة الرقمية وحفظ الأدلة الرقمية والأثرية.
- التحقيق في التكنولوجيات المتنقلة ووسائط الإعلام الأخرى التي قد تحتوي على الأدلة الجنائية.
- تطبيق تقنيات لاستخراج الصور من أنظمة القطع الأثرية.

الكفاءات المستهدفة:

- التشريح الجنائي الرقمي، مع التركيز على المعلومات القانونية.
- قوانين وتشريعات الجنائية الرقمية.
- جمع ومعالجة الأدلة الرقمية بشكل آمن.
- نظام اسم النطاق DNS واعتباره أداة حيوية في التحقيقات.
- التحقيقات في الجرائم الرقمية الداخلية والخارجية.
- تقنيات OSINT تبادل معلومات المصادر المفتوحة واستخدامها في التحقيقات الجنائية.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

محتوى الدورة:

الوحدة الأولى: الجنائي الرقمي، الخلفية والمعلومات القانونية:

- مقدمة في العلم الجنائي الرقمي: تعريف المفاهيم الأساسية للطب الجنائي الرقمي وأهميته.
- المصطلحات والتعاريف: التعرف على المصطلحات المتعلقة بالجنائي الرقمي.
- سلسلة الجرائم الرقمية: من بداياتها إلى شكلها الحالي.
- خلفية تاريخية عن الجرائم الرقمية: كيف تطورت الجرائم الرقمية مع مرور الوقت.
- قوانين الجنائية الرقمية: القوانين الخاصة بالتحقيقات الجنائية الرقمية، وكذلك التشريعات المتعلقة بها.
- معايير الأدلة الجنائية الرقمية: كيفية معالجة الأدلة الرقمية لتكون مقبولة في المحكمة.
- أساسيات الجنائية الرقمية: المبادئ الأساسية التي يجب اتباعها أثناء التحقيقات.
- المخاطر التي تواجهها المنظمات: التحليل الشامل للمخاطر الرقمية التي قد تواجه المؤسسات.
- إطار استجابة الجنائيات الرقمية: كيفية وضع وتنفيذ خطط استجابة فعالة للحوادث الرقمية.
- أدوات المستجيب الجنائي الرقمي الأول: الأدوات الأساسية التي يجب أن يكون مستجيب الحوادث الرقمي على دراية بها.
- مشهد من إدارة الجريمة الرقمية: كيفية إدارة المشهد الرقمي بعد وقوع الجريمة.
- مركز العمليات الأمنة SOC: الدور الهام لمراكز العمليات في ضمان الأمن الرقمي.
- .الأمنية الحوادث مع التعامل في المتخصصة الفرق :الحاسوب أمن لحوادث الاستجابة فريق CSIRT
- الأدوار والمسؤوليات: كيفية توزيع المسؤوليات بين الفرق المعنية.
- تنفيذ إطار عمل: كيفية تطبيق خطة استجابة متكاملة.
- إدارة الحالة: كيفية متابعة التحقيقات وأدواتها.

الوحدة الثانية: جمع ومعالجة الأدلة الرقمية:

- نظام اسم النطاق DNS: فهم دور DNS في التحقيقات الجنائية الرقمية.
- البنية التحتية الأمنية الموسعة: التعامل مع البنية التحتية لحماية البيانات خلال عملية التحقيق.
- التحقيق في التكنولوجيات المتنقلة: كيفية التعامل مع الأدلة الموجودة على الهواتف المتحركة.
- الاستحواذ على الأدلة الرقمية: التقنيات المستخدمة لاستخلاص الأدلة.
- الأدوات المستخدمة في التعامل مع الأدلة الرقمية: أدوات وتقنيات تتبع الأدلة الرقمية.
- تجهيز الأدلة الرقمية: كيفية تحضير الأدلة الرقمية للاستخدام في التحقيقات.
- بروتوكولات إدارة الحالة: الخطوات الأساسية في إدارة التحقيقات الرقمية.
- بروتوكولات لاسلكية: التقنيات المستخدمة للتعامل مع الأدلة الرقمية عبر الشبكات اللاسلكية.
- تقنيات الدعم: دعم التحقيقات الجنائية الرقمية بالأدوات والتقنيات الحديثة.
- ممارسات كتابة التقارير: كيفية توثيق نتائج التحقيقات بشكل دقيق.

الوحدة الثالثة: التحقيقات في الجرائم الرقمية الداخلية والخارجية:

- دور OSINT في التحقيقات الجنائية الرقمية: استخدام المصادر المفتوحة في جمع الأدلة.
- تعريف الجرائم الداخلية والخارجية: الفرق بين الجرائم الداخلية التي تحدث داخل المؤسسة والخارجية.
- التطبيقات الخبيثة: كيف تؤثر التطبيقات الخبيثة على التحقيقات.
- برامج الفدية: كيفية مكافحة البرامج الخبيثة التي تطلب فدية.
- قدرات المكافحة الجنائية: تقنيات مكافحة الجنائيات الرقمية.
- الجرائم الرقمية والإرهاب الإلكتروني: تأثير الجريمة الرقمية على الأمن العالمي.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

الوحدة الرابعة: استجابة فعالة للحوادث الرقمية:

- بناء خطة استجابة لحوادث الأمن السيبراني: كيفية التخطيط للتعامل مع الهجمات الرقمية.
- أدوات الاستجابة السريعة: الأدوات المستخدمة لتحديد مصدر الهجوم وحجمه.
- التنسيق بين الفرق الفنية والأمنية: العمل الجماعي أثناء التعامل مع الحوادث الرقمية.
- التحليل بعد الحادث: كيفية تحليل الأدلة بعد وقوع الهجوم.

الوحدة الخامسة: التطبيقات العملية في التحقيق الجنائي الرقمي:

- محاكاة التحقيقات الرقمية: تطبيق نظريات التحقيق الجنائي الرقمي في بيئات محاكاة.
- تحليل الأدلة الرقمية: طرق تحليل الأدلة المستخلصة من الأجهزة الرقمية.
- تقنيات استرجاع الصور والبيانات: استخدام تقنيات متقدمة لاستخراج الصور والبيانات من الأجهزة.
- تقنيات تأمين وحفظ الأدلة: كيفية ضمان أن الأدلة التي تم جمعها تظل سليمة وغير معدلة.

الوحدة السادسة: عمليات البحث الجنائي:

- أهداف وأهمية عمليات البحث الجنائي.
- التخطيط الفعال لعمليات البحث الجنائي.
- تنظيم وتوزيع عمليات البحث الجنائي.
- قيادة فرق عمليات البحث الجنائي.
- الأخطاء الشائعة في إدارة عمليات البحث الجنائي.

الوحدة السابعة: التحريات الجنائية:

- مصادر جمع التحريات الجنائية.
- إدارة المصادر البشرية بكفاءة.
- اليات المراقبة الأمنية ومتطلباتها وأدواتها الفعالة.
- تسخير التكنولوجيا لخدمة التحقيق الأمني.
- تقنيات المناقشة التفصيلية للمشتبه بهم والمتهمين.