BLACKBIRD FOR TRAINING

دورة الاستجابة للحوادث والتحقيق الجنائي الرقمي

November 2027 19 – 15

ليون (فرنسا)



دورة الاستجابة للحوادث والتحقيق الجنائي الرقمي

المرجع: 201667_3255278 **التاريخ:** 15 – 19 November 2027 **المكان:** ليون (فرنسا) **الرسوم:** GBP 5900

مقدمة

في عالم رقمي يشهد تزايداً مستمراً في الهجمات السيبرانية، لم يعد السؤال هو هل ستتعرض المؤسسة لهجوم؟ بل متى سيحدث ذلك؟. ومع هذا الواقع الجديد، أصبحت الاستجابة للحوادث والتحقيق الجنائي الرقمي من الركائز الأساسية لأي استراتيجية فعالة في مجال الأمن السيبراني. فهي تمكّن المؤسسات من اكتشاف الهجمات بسرعة، احتوائها، استعادة الأنظمة المتضررة، وتحليل الأدلة الرقمية لضمان عدم تكرار الحادثة.

تهدف هذه الدورة إلى تزويد المشاركين بالمعرفة العميقة والمهارات العملية اللازمة للتعامل مع الحوادث الأمنية الرقمية بأسلوب احترافي ومنهجي. تجمع الدورة بين المفاهيم النظرية وأفضل الممارسات العالمية في الاستجابة للحوادث، إلى جانب تطبيقات عملية في مجال التحقيق الجنائي الرقمي لتحليل الأدلة وتتبع الأنشطة الخبيثة بدقة.

تستهدف هذه الدورة المتخصصين في الأمن السيبراني، ومديري تقنية المعلومات، ومحللي مراكز العمليات الأمنية SOC، وكل من يسعى إلى تطوير قدراته في مواجهة التهديدات الإلكترونية وتحليل الحوادث الرقمية بفعالية.

أهداف الدورة

بنهاية هذه الدورة، سيتمكن المشاركون من:

- فهم المبادئ الأساسية ودورة حياة الاستجابة للحوادث الرقمية.
- تطوير وتنفيذ خطة فعالة لإدارة الحوادث الأمنية.
- اكتشاف مؤشرات الاختراق وتحليل الأنشطة المشبوهة.
- تطبيق تقنيات التحقيق الجنائي الرقمي في جمع الأدلة وتحليلها.
- تحليل الأنظمة المتضررة واستخلاص النتائج الفنية.
- استخدام أدوات متقدمة في الفحص الجنائي الرقمي وتوثيق النتائج.
- إعداد تقارير مهنية دقيقة تُستخدم في التحقيقات الفنية والقانونية.
- تعزيز جاهزية المؤسسة في التعامل مع التهديدات والهجمات المستقبلية.



محاور الدورة

اليوم الأول: مقدمة في الاستجابة للحوادث والتهديدات السيبرانية

- المفاهيم الأساسية للاستجابة للحوادث الرقمية.
- أنواع الحوادث الأمنية الشائعة وأسبابها.
- دورة حياة الاستجابة للحوادث: التحضير، الاكتشاف، الاحتواء، المعالجة، الاستعادة، والدروس المستفادة.
- الأدوار والمسؤوليات داخل فريق الاستجابة للحوادث.
- بناء سياسة فعالة لإدارة الحوادث الرقمية.

اليوم الثاني: اكتشاف وتحليل الحوادث الأمنية

- مؤشرات الاختراق وكيفية رصدها مبكراً.
- تحليل السجلات والأحداث الأمنية واستخراج الأنماط.
- استخدام أنظمة مراقبة المعلومات الأمنية SIEM لاكتشاف التهديدات.
- التفريق بين الإنذارات الزائفة والحوادث الحقيقية.
- دمج المعلومات الاستخباراتية في عملية التحليل الأمني.

اليوم الثالث: أساسيات التحقيق الجنائي الرقمي

- تعريف التحقيق الجنائي الرقمي ومراحله الأساسية.
- جمع الأدلة الرقمية والحفاظ على سلامتها القانونية.
- إنشاء النسخ الجنائية Imaging للبيانات والأقراص.
- تحليل نظم الملفات واستخراج البيانات المخفية.
- التعرف على أدوات التحقيق الجنائي الرقمية الشائعة.

اليوم الرابع: التحليل المتقدم للحوادث واحتواؤها

- تحليل الأنظمة المصابة واسترجاع الملفات المحذوفة.
- تحليل البرمجيات الخبيثة وتتبع نشاط المهاجمين.
- الفحص الشبكي وتحليل حركة البيانات للكشف عن الاختراقات.
- استراتيجيات الاحتواء والمعالجة الآمنة للحوادث.
- تنسيق جهود الاستجابة بين الفرق التقنية والإدارية.



اليوم الخامس: إعداد التقارير والتعافي من الحوادث

- إعداد التقارير الفنية والجنائية بشكل احترافي.
- توثيق الأدلة والنتائج لاستخدامها في الإجراءات القانونية.
- التواصل الفعال مع الأطراف الإدارية والتنظيمية.
- تطوير خطط التعافي واستعادة الأنظمة المتضررة.
- مراجعة ما بعد الحادث واستخلاص الدروس لتحسين الأداء المستقبلي.

لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- فهم متكامل لدورة حياة الاستجابة للحوادث من الاكتشاف إلى الاستعادة.
- اكتساب مهارات تحليل الأدلة الرقمية باستخدام أدوات احترافية.
- تطوير قدرات عملية في التعامل مع الحوادث الأمنية المعقدة.
- تعزيز التعاون بين فرق الأمن والتقنية لضمان استجابة فعالة.
- رفع جاهزية المؤسسة في مواجهة الهجمات المستقبلية.
- ضمان الامتثال للمعايير التنظيمية ومتطلبات الأمن السيبراني.
- بناء قدرة على اتخاذ قرارات سريعة أثناء الحوادث الأمنية.
- تحسين جودة التقارير الفنية والدروس المستفادة بعد الحوادث.

الخاتمة

تشكل دورة الاستجابة للحوادث والتحقيق الجنائي الرقمي محوراً أساسياً في تطوير قدرات المؤسسات على مواجهة التهديدات السيبرانية الحديثة. فهي لا تقتصر على معالجة الحوادث بعد وقوعها، بل تهدف إلى بناء ثقافة استباقية قائمة على التحليل، الفهم، والاستعداد الدائم.

تجمع هذه الدورة بين المعرفة النظرية والممارسات العملية لتزويد المشاركين بقدرات احترافية في كشف الهجمات، احتوائها، وتحليل الأدلة الرقمية بطريقة دقيقة وقانونية.

في زمن تتسارع فيه التهديدات الإلكترونية، يصبح امتلاك مهارات الاستجابة والتحقيق الرقمي عاملاً حاسماً في حماية الأصول الرقمية وضمان استمرارية الأعمال. هذه الدورة تمنح المشاركين القدرة على تحويل كل حادثة أمنية إلى فرصة لتعزيز الدفاعات وتحسين الاستراتيجيات المستقبلية.

