BLACKBIRD FOR TRAINING

دورة تدريبية في عمليات الفريق الأحمر (CRTO)

May 2027 6 – 2

عمّان (الأردن)



دورة تدريبية في عمليات الفريق الأحمر (CRTO)

المرجع: 326056_3254925 **التاريخ:** 2 – 6 May 2027 **المكان:** عمان (الأردن) **الرسوم:** GBP 4900

مقدمة

في عصر يتزايد فيه خطر الهجمات السيبرانية وتتعاظم فيه تحديات حماية البيانات، أصبحت المؤسسات بحاجة إلى خبراء قادرين على تقويم دفاعاتها الأمنية وتحصينها ضد التهديدات. تأتي هنا أهمية شهادة العمليات الحمراء المعتمدة، التي تعد من أقوى البرامج التدريبية المخصصة لمحاكاة الهجمات الرقمية الواقعية، وتقييم نقاط الضعف وتعزيز الدفاعات الإلكترونية.

تستهدف هذه الدورة جميع المستويات الوظيفية داخل المؤسسات، من الموظفين الجدد ومتوسطي الخبرة، إلى القيادات العليا، مما يجعلها خياراً مثالياً لتعزيز الخبرات التقنية والإدارية في مجال الأمن السيبراني. صممت الدورة خصيصًا لتخدم مختلف القطاعات مثل النفط والغاز، البنوك والخدمات المالية، الاتصالات، القطاع الحكومي، الموارد البشرية، إدارة المشاريع، التسويق والمبيعات، وغيرها.

من خلال التدريب على محاكاة الهجمات السيبرانية واكتشاف نقاط الضعف الفعلية، تساعد هذه الدورة المشاركين على تعزيز الثقة والجاهزية لمواجهة التهديدات الأمنية، ودعم أهداف الأداء المؤسسي المستدام.

أهداف الدورة

في ختام هذه الدورة، سيكون المشاركون قادرين على:

- فهم المبادئ الأساسية لعمليات الفريق الأحمر وأهميتها في مجال الأمن السيبراني.
- تطوير مهارات استخدام الأدوات المتقدمة لمحاكاة الهجمات وتحليل الثغرات الأمنية.
- تطبيق أساليب وتقنيات الاختراق الأخلاقي وفق أفضل الممارسات العالمية.
- تحليل نتائج عمليات المحاكاة وصياغة تقارير تقييم شاملة وفعالة.
- صياغة خطط شاملة لعمليات الفريق الأحمر تتماشى مع أهداف المؤسسة.
- تعزيز التعاون مع فرق الدفاع الداخلية لتحقيق أفضل مخرجات أمنية.
- تحديد الثغرات الأمنية في البنية التحتية الرقمية واقتراح حلول عملية لمعالجتها.
- مواكبة التطورات وأحدث الأدوات المستخدمة في محاكاة الهجمات وعمليات الفريق الأحمر.



محاور الدورة

اليوم الأول: مقدمة في عمليات الفريق الأحمر

- تعريف عمليات الفريق الأحمر ومفاهيمها الأساسية.
- التمييز بين عمليات الفريق الأحمر واختبار الاختراق التقليدي.
- استعراض أهداف المؤسسات من استراتيجية الفريق الأحمر.
- التعرف على التهديدات الحالية وأساليب المهاجمين.
- عرض الأدوات المستخدمة في الفريق الأحمر وأهم خصائصها.
- مناقشة الاعتبارات الأخلاقية والقانونية المرتبطة بعمليات الفريق الأحمر.

اليوم الثاني: أدوات وتقنيات محاكاة الهجمات

- استكشاف الشبكات وأنظمة جمع المعلومات المبدئية.
- تقنيات جمع المعلومات وتحليلها لاستهداف الأنظمة.
- وسائل تجاوز نظم الكشف والحماية.
- استعراض أدوات محاكاة الهجمات مثل أدوات التحكم في الجلسات.
- أساليب إدارة الثغرات والتحكم في نتائج الهجمات.
- تمارين عملية لتطبيق أساليب محاكاة الهجمات.

اليوم الثالث: استغلال الثغرات وتحليل البيانات

- تقنيات تصعيد الامتيازات داخل الشبكات المستهدفة.
- طرق تجاوز الضوابط الأمنية والتعامل مع نظم الحماية.
- تشغيل أدوات الإدارة عن بعد للوصول إلى الأنظمة الحساسة.
- تحليل الثغرات والتعرف على مواطن الضعف في الأنظمة.
- دراسة تأثير الهجمات على أنظمة المؤسسة وتحليل النتائج.
- جلسة عملية لمحاكاة سيناريو متكامل لاختبار قدرات الفريق.



اليوم الرابع: إدارة العمليات وتحسين التعاون

- بناء خطة شاملة لعمليات الفريق الأحمر داخل المؤسسة.
- تكامل الفريق الأحمر مع فرق الدفاع الداخلية لتعزيز التنسيق.
- إدارة البيانات والوثائق الخاصة بنتائج المحاكاة.
- تحليل الأداء وقياس فعالية العمليات المنفذة.
- تقديم التوصيات النهائية لتحسين الوضع الأمني.
- استعراض دراسات حالة لتطبيق المفاهيم في بيئات واقعية.

اليوم الخامس: ختام الدورة والتقييم الشامل

- إدارة مشروع شامل للفريق الأحمر من البداية إلى النهاية.
- توزيع الأدوار والمسؤوليات داخل الفريق لتحقيق أفضل النتائج.
- توثيق نتائج المحاكاة وتحضير تقارير شاملة لأصحاب المصلحة.
- مناقشة التحديات المحتملة وسبل التغلب عليها.
- تقييم الأداء النهائي من خلال تمرين عملي تطبيقي.
- تقديم الشهادات وختام الدورة بمناقشة شاملة لأهم النتائج المستفادة.

لماذا يجب عليك حضور هذه الدورة؟ الإيجابيات والسلبيات

- بناء معرفة متقدمة في تقنيات محاكاة الهجمات الواقعية.
- اكتساب خبرة عملية في استخدام الأدوات والتقنيات الحديثة.
- تحسين القدرة على اكتشاف الثغرات ومعالجتها بطرق فعالة.
- تعزيز مهارات التعاون بين الفرق الأمنية داخل المؤسسة.
- رفع الكفاءة الشخصية والمهنية في مجال الأمن السيبراني.
- الحصول على شهادة معتمدة تعزز المصداقية والجاهزية المهنية.
- مواكبة أحدث الممارسات العالمية في عمليات الفريق الأحمر.
- الاستفادة من أمثلة عملية ودراسات حالة تعزز الفهم التطبيقي.
- من التحديات المحتملة: الحاجة إلى أساس قوي في الأمن السيبراني لاستيعاب محتوى الدورة بالكامل.
- إمكانية مواجهة صعوبة في تطبيق نتائج الدورة دون دعم إداري متكامل.



الخاتمة

تشكل شهادة العمليات الحمراء المعتمدة خيارًا استراتيجيًا للراغبين في تطوير مهاراتهم الأمنية واكتساب خبرة عملية شاملة في مجال الأمن السيبراني. فهي تمنح المشاركين القدرة على تقييم نظم الحماية الحالية وتحليل الثغرات وإيجاد حلول عملية لها. تعد هذه الدورة فرصة مثالية للمديرين التنفيذيين وقادة الفرق والمتخصصين لتعزيز كفاءتهم في مجال الأمن السيبراني، وتحقيق مستويات أعلى من الحماية الرقمية التي تدعم الأداء المؤسسي وتقلل المخاطر المحتملة.

إذا كنت تسعى لتكون جزءًا من منظومة أمنية متكاملة قادرة على مواجهة التهديدات بفعالية، فإن هذه الدورة ستمكنك من تحقيق هذا الهدف من خلال المعرفة المتقدمة والتدريبات العملية الشاملة.

