QUEST
Professional Center

دورة تدريبية احترافية

رقم الدورة 1984

دورة المراقبة الأمنية والكشف عن التهديدات والاستجابة للحوادث

العمليات الأمنية والاستجابة للحوادث
تقنية المعلومات والأمن السيبراني

المدة
5 أيام

طريقة التقديم
حضوري

شركة كويست ترينينج

quest-training.com

نظرة عامة على الدورة

تقدم دورة المراقبة الأمنية والكشف عن التهديدات والاستجابة للحوادث إطاراً عملياً متكاملاً لمراقبة البيئات الرقمية، واكتشاف الأنشطة المشبوهة، والتعرف على التهديدات السيبرانية، وتنسيق الاستجابات الأمنية بفاعلية. وتهدف الدورة إلى تعزيز قدرة المؤسسات على تحقيق رؤية أمنية مستمرة عبر الشبكات وأجهزة المستخدمين والهويات والتطبيقات والبيئات السحابية والأنظمة الحيوية.

يتناول البرنامج دورة المراقبة الأمنية بدءاً من جمع السجلات والأحداث وتحليلها، مروراً بإدارة التنبيهات واكتشاف التهديدات وفرز الحوادث والتحقيق فيها وتصعيدها، وصولاً إلى تنفيذ الاستجابة المناسبة. ويركز على قدرة المشاركين على التمييز بين التهديدات الأمنية الحقيقية والأنشطة التشغيلية الطبيعية، وتحديد أولويات التنبيهات وفقاً لمستوى الخطورة والتأثير على الأعمال والمخاطر المحتملة.

كما يركز البرنامج على تطوير قدرات الكشف الأمني من خلال تحليل الأحداث والمؤشرات الأمنية وأنماط السلوك المشبوه وقواعد الكشف ومعلومات التهديد وتقنيات الربط بين الأحداث. ويتعرف المشاركون على دور منصات المراقبة الأمنية المركزية وقدرات إدارة معلومات وأحداث الأمن في جمع البيانات من مصادر متعددة وتحليلها لدعم الكشف المبكر واتخاذ القرارات المناسبة.

ومن خلال سيناريوهات عملية وتمارين تحليل السجلات والتحقيق في التنبيهات وتطوير حالات الكشف ومحاكاة أنشطة الاستجابة، يطور المشاركون القدرة على الانتقال من الإشارة الأمنية الأولية إلى التحقيق المنظم والاستجابة المناسبة. كما تتناول الدورة قياس أداء المراقبة والكشف، وتقليل التنبيهات غير الدقيقة، وتحديد فجوات الكشف، وتحسين التنسيق بين الفرق بصورة مستمرة.

أهداف الدورة

- بنهاية الدورة، سيتمكن المشاركون من:
- شرح مبادئ وأهداف المراقبة والكشف والاستجابة في الأمن السيبراني.
- تقييم مستوى الرؤية الأمنية عبر الشبكات والأجهزة والهويات والتطبيقات والبيئات السحابية.

- تحديد الأحداث الأمنية والمؤشرات المرتبطة بالأنشطة المشبوهة.
- تحليل السجلات والتنبيهات الأمنية لتحديد التهديدات المحتملة.
- تطبيق منهجيات منظمة لفرز التنبيهات وتحديد أولوياتها.
- تطوير حالات كشف أمنية وسيناريوهات فعالة للمراقبة.
- تطبيق تقنيات الربط بين الأحداث لاكتشاف أنماط الأنشطة الخبيثة.
- التمييز بين التنبيهات غير الصحيحة والأنشطة الطبيعية والتهديدات الأمنية الحقيقية.
- التحقيق في الأحداث المشبوهة وتحديد مسارات التصعيد المناسبة.
- دمج معلومات التهديد في عمليات المراقبة والكشف الأمني.
- تعزيز التنسيق بين فرق المراقبة والاستجابة للحوادث وتقنية المعلومات والمخاطر.
- تقييم تغطية الكشف وتحديد فجوات المراقبة الأمنية.
- تحسين جودة التنبيهات وتقليل الإشعارات الأمنية غير الضرورية.
- وضع مؤشرات مناسبة لقياس أداء المراقبة والكشف.
- تطوير إجراءات عملية للتحسين المستمر للمراقبة الأمنية.
- تعزيز جاهزية المؤسسة لاكتشاف التهديدات السيبرانية المتطورة والاستجابة لها.

الفئة المستهدفة

تستهدف الدورة متخصصي الأمن السيبراني، ومتخصصي عمليات الأمن، ومحللي المراقبة الأمنية، ومحللي الأمن، ومتخصصي الاستجابة للحوادث، ومتخصصي اكتشاف التهديدات، ومهندسي الأمن، ومتخصصي تقنية المعلومات المسؤولين عن مراقبة البيئات التقنية في المؤسسات.

كما تناسب مديري الأمن السيبراني ومديري أمن المعلومات ومتخصصي معلومات التهديدات ومتخصصي إدارة الثغرات ومديري ومشرفي الشبكات والأنظمة ومتخصصي أمن البيئات السحابية وفرق المخاطر والالتزام وقادة

التقنية الذين يتولون إدارة أو الإشراف على قدرات المراقبة والكشف الأمني.

وتعد الدورة مناسبة بصورة خاصة للجهات الحكومية والوزارات والمصارف والمؤسسات المالية وشركات النفط والغاز وشركات الاتصالات ومشغلي البنية التحتية الحيوية والشركات التقنية والمؤسسات متعددة الجنسيات والمؤسسات الكبرى التي تسعى إلى تعزيز الرؤية الأمنية والكشف عن التهديدات وفعالية المراقبة والمرونة التشغيلية للأمن السيبراني.

مخرجات التعلم

- بنهاية الدورة، سيكون المشاركون قادرين على:
- إنشاء منهج منظم للمراقبة الأمنية عبر البيئات التقنية الحيوية.
- تحديد مصادر البيانات الأكثر أهمية لعمليات المراقبة الأمنية.
- تفسير السجلات والأحداث الأمنية لاكتشاف السلوكيات المشبوهة.
- فرز التنبيهات الأمنية وتحديد أولوياتها وفق مستوى المخاطر وتأثير الأعمال.
- التحقيق في الحوادث الأمنية المحتملة باستخدام أساليب تحليل منظمة.
- تطوير سيناريوهات كشف تستند إلى التهديدات والمخاطر المؤسسية.
- ربط الأحداث القادمة من أنظمة متعددة لاكتشاف أنماط الهجمات.
- التعرف على مؤشرات الاختراق والسلوكيات غير الطبيعية.
- التمييز بين الأنشطة الخبيثة والأنشطة المشروعة والمتوقعة.
- دمج معلومات التهديدات في أنشطة المراقبة والكشف.
- تحديد نقاط الضعف في تغطية الكشف وعمليات المراقبة الحالية.
- تحسين دقة التنبيهات وتقليل التنبيهات غير الصحيحة.

- إنشاء إجراءات واضحة للتصعيد وتسليم الحالات بين فرق الأمن.
- قياس أداء المراقبة والكشف باستخدام مؤشرات مناسبة.
- إعداد توصيات عملية لتعزيز قدرات المراقبة الأمنية.
- تطوير خارطة طريق لتحسين نضج عمليات الكشف والاستجابة.
- المحاور التدريبية

محاور الدورة

اليوم الأول

أسس المراقبة الأمنية والرؤية على التهديدات

- مبادئ المراقبة الأمنية في الأمن السيبراني.
- دور المراقبة الأمنية في حماية المؤسسة.
- الرؤية الأمنية وعلاقتها بإدارة المخاطر.
- مراقبة الشبكات والأجهزة والهويات والتطبيقات والبيئات السحابية.
- السجلات والأحداث والبيانات الأمنية.
- مصادر بيانات المراقبة الأمنية.
- جمع السجلات وتوحيدها.
- فهم الأنشطة الطبيعية وغير الطبيعية.
- تصنيف الأحداث الأمنية وتحديد أولوياتها.
- مراقبة الأصول الحيوية والبيئات عالية المخاطر.
- تحديات المراقبة الأمنية وفجوات الرؤية.
- بناء إطار متكامل للمراقبة الأمنية.

اليوم الأول — تابع

- التطبيق العملي: إعداد خريطة للأصول الحيوية ومصادر البيانات الأمنية في مؤسسة مختارة وتحديد متطلبات المراقبة ذات الأولوية.

اليوم الثاني

الكشف الأمني وإدارة التنبيهات والتحليل

- مبادئ اكتشاف التهديدات السيبرانية.
- أساليب الكشف والمؤشرات الأمنية.
- مؤشرات الاختراق ومؤشرات السلوك المشبوه.
- قواعد الكشف وسيناريوهات المراقبة.
- الربط بين الأحداث والتحليل السياقي.
- الكشف القائم على السلوك واكتشاف الحالات غير الطبيعية.
- إنشاء التنبيهات الأمنية وتصنيفها.
- تحديد مستوى خطورة التنبيهات وأولوياتها.
- إدارة التنبيهات غير الصحيحة وحالات عدم الكشف.
- تغطية الكشف وتحديد فجوات المراقبة.
- تطوير حالات كشف فعالة.
- تحسين جودة التنبيهات وارتباطها بالمخاطر.
- التطبيق العملي: تحليل مجموعة من التنبيهات الأمنية وتصنيف مستوى خطورتها وتحديد التهديدات المحتملة وترتيب أولويات التحقيق.

اليوم الثالث

تحليل الأحداث الأمنية والتحقيق في الحوادث

- مفاهيم المراقبة الأمنية المركزية.
- قدرات إدارة معلومات وأحداث الأمن.
- دمج السجلات من مصادر تقنية متعددة.
- البحث في الأحداث الأمنية وتحليلها.
- بناء التسلسل الزمني للحوادث.
- التحقيق في أنشطة الدخول والمصادقة المشبوهة.
- اكتشاف الحالات غير الطبيعية في الأجهزة والشبكات.
- التحقيق في سلوك المستخدمين غير المعتاد.
- الربط بين الأحداث عبر الأنظمة المختلفة.
- تحديد أنماط الهجمات والمؤشرات المرتبطة بها.
- توثيق نتائج التحقيقات الأمنية.
- الانتقال من الكشف إلى الاستجابة للحوادث.
- التطبيق العملي: تنفيذ تحقيق أمني افتراضي باستخدام مصادر متعددة للأحداث لإعادة بناء تسلسل الهجوم وتحديد مسار التصعيد المناسب.

اليوم الرابع

هندسة الكشف ومعلومات التهديد وتنسيق الاستجابة

- بناء استراتيجيات كشف قائمة على التهديدات.
- استخدام معلومات التهديدات لتحسين قدرات الكشف.
- ربط التهديدات بالتقنيات وأساليب تنفيذ الهجمات.

اليوم الرابع — تابع

- تطوير حالات الكشف الأمنية وإدارتها.
- ترتيب أولويات الكشف وفق المخاطر المؤسسية.
- تنسيق العمل بين فرق المراقبة والاستجابة للحوادث.
- تصعيد التنبيهات وتسليم الحالات.
- إجراءات الاستجابة بعد تأكيد التهديد.
- مراقبة التهديدات الناشئة والمتطورة.
- اختبار فعالية قدرات الكشف.
- إدارة التغييرات في قواعد وحالات الكشف.
- التحسين المستمر لقدرات الكشف الأمني.
- التطبيق العملي: تطوير حالة كشف قائمة على تهديد محدد، تشمل مصادر البيانات ومنطق الكشف ومعايير التنبيه وخطوات التحقيق ومتطلبات التصعيد وإجراءات الاستجابة.

اليوم الخامس

أداء عمليات الأمن والتحسين المستمر

- قياس فعالية المراقبة الأمنية.
- مؤشرات الأداء والتشغيل لعمليات المراقبة والكشف.
- حجم التنبيهات وأوقات الاستجابة وجودة التحقيق.
- قياس تغطية الكشف وفعالية الضوابط الأمنية.
- قياس معدلات التنبيهات غير الصحيحة وكفاءة التنبيهات.
- تحديد نقاط الضعف المتكررة في عمليات المراقبة.
- حوكمة المراقبة الأمنية وتحديد المسؤوليات.
- إعداد تقارير المراقبة الأمنية للإدارة.

اليوم الخامس — تابع

- تحسين إجراءات العمل والتنسيق بين الفرق.
- مراجعة قدرات الكشف في ضوء التهديدات المتغيرة.
- بناء منهج للتحسين المستمر.
- إعداد خارطة طريق لنضج المراقبة الأمنية.
- الورشة الختامية: تطوير إطار متكامل للمراقبة الأمنية والكشف عن التهديدات والاستجابة للحوادث لمؤسسة مختارة، يشمل مصادر المراقبة وحالات الكشف وفرز التنبيهات والتحقيق ومعلومات التهديدات والتصعيد وتنسيق الاستجابة وقياس الأداء والحوكمة والتحسين المستمر.

للتسجيل أو لطلب مزيد من المعلومات

صفحة الدورة: https://quest-training.com/courses/security-monitoring-detection-response-training-course

الموقع الإلكتروني: https://quest-training.com

البريد الإلكتروني: info@quest-training.com

الهاتف: +905016771440