QUEST
Professional Center

دورة تدريبية احترافية

رقم الدورة 1985

دورة إدارة معلومات وأحداث الأمن السيبراني

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 إدارة معلومات وأحداث الأمن السيبراني إطاراً عملياً متكاملاً لفهم وتطبيق وتشغيل وتحسين حلول إدارة معلومات وأحداث الأمن السيبراني داخل البيئات التقنية الحديثة. وتركز الدورة على كيفية جمع البيانات الأمنية مركزياً، وربط الأحداث وتحليلها، واكتشاف الأنشطة المشبوهة، والتحقيق في التهديدات، ودعم الاستجابة الأمنية في الوقت المناسب.

يتعرف المشاركون على البنية الأساسية وآليات تشغيل حلول إدارة معلومات وأحداث الأمن السيبراني، بما يشمل جمع السجلات واستقبال البيانات وتوحيدها وتحليلها وفهرستها وربط الأحداث وإنشاء التنبيهات ولوحات المعلومات وإعداد التقارير. كما تركز الدورة على اختيار مصادر البيانات المناسبة وتحقيق رؤية أمنية متكاملة عبر الشبكات والأجهزة والتطبيقات والهويات والبيئات السحابية والبنية التحتية الحيوية.

ويطور البرنامج قدرات عملية في اكتشاف التهديدات والتحقيق فيها باستخدام أنظمة إدارة معلومات وأحداث الأمن السيبراني. ويتعلم المشاركون كيفية بناء حالات الاستخدام الأمنية، وتطوير قواعد الربط، وتحليل التنبيهات، والتحقيق في تسلسل الأحداث، وتحديد مؤشرات الاختراق، وتقليل التنبيهات غير الصحيحة، والاستفادة من السياق الأمني للتمييز بين الأنشطة المشروعة والتهديدات الفعلية.

كما تتناول الدورة حوكمة أنظمة إدارة معلومات وأحداث الأمن السيبراني، وقياس الأداء التشغيلي، ودمج معلومات التهديدات، وربط عمليات المراقبة بالاستجابة للحوادث، وإعداد تقارير الالتزام، والتحسين المستمر. ومن خلال التمارين العملية وتحليل السجلات وسيناريوهات الكشف وحالات التحقيق ومحاكاة عمليات الأمن، يطور المشاركون المهارات اللازمة لتعظيم قيمة أنظمة إدارة معلومات وأحداث الأمن السيبراني وتعزيز المراقبة والاستجابة الأمنية للمؤسسة.

أهداف الدورة

- بنهاية الدورة، سيتمكن المشاركون من:
- شرح بنية ومكونات ومبادئ تشغيل أنظمة إدارة معلومات وأحداث الأمن السيبراني.

- تقييم متطلبات المؤسسة لإدارة الأحداث الأمنية بصورة مركزية.
- تحديد مصادر السجلات والأحداث الأمنية وترتيب أولوياتها.
- تصميم عمليات فعالة لجمع البيانات الأمنية وإدخالها إلى النظام.
- تطبيق أساليب توحيد السجلات وتحليلها وفهرستها وإثرائها.
- تطوير حالات استخدام للمراقبة والكشف الأمني.
- إنشاء قواعد لربط الأحداث واكتشاف الأنشطة المشبوهة.
- تحليل التنبيهات الأمنية وترتيب أولوياتها وفقاً للمخاطر والخطورة.
- التحقيق في الأحداث الأمنية وإعادة بناء التسلسل الزمني للهجمات المحتملة.
- دمج معلومات التهديدات مع عمليات المراقبة والكشف.
- تقليل التنبيهات غير الصحيحة وتحسين جودة التنبيهات الأمنية.
- تعزيز تكامل أنظمة إدارة الأحداث الأمنية مع عمليات الاستجابة للحوادث.
- تطوير لوحات معلومات وتقارير أمنية فعالة.
- تقييم أداء النظام وجودة البيانات وتغطية الكشف الأمني.
- إنشاء إطار فعال لحوكمة وتشغيل أنظمة إدارة الأحداث الأمنية.
- إعداد خارطة طريق للتحسين المستمر ونضج قدرات إدارة الأحداث الأمنية.

الفئة المستهدفة

تستهدف الدورة متخصصي الأمن السيبراني، ومحللي عمليات الأمن، ومديري ومشغلي أنظمة إدارة معلومات وأحداث الأمن السيبراني، ومتخصصي المراقبة الأمنية، ومتخصصي الاستجابة للحوادث، ومحللي اكتشاف التهديدات، ومهندسي الأمن، ومتخصصي أمن المعلومات المسؤولين عن مراقبة وتحليل الأحداث الأمنية.

كما تناسب مديري الأمن السيبراني وقادة مراكز عمليات الأمن ومديري تقنية المعلومات ومسؤولي الشبكات

والأنظمة ومتخصصي معلومات التهديدات وإدارة الثغرات وفرق المخاطر والالتزام والمدققين الداخليين وقادة التقنية المسؤولين عن الإشراف على المراقبة الأمنية وإعداد التقارير.

وتعد الدورة مناسبة بصورة خاصة للجهات الحكومية والوزارات والمصارف والمؤسسات المالية وشركات النفط والغاز وشركات الاتصالات ومشغلي البنية التحتية الحيوية والمؤسسات التقنية والشركات متعددة الجنسيات والمؤسسات الكبرى التي تسعى إلى تعزيز المراقبة الأمنية المركزية واكتشاف التهديدات والتحقيق في الحوادث وحوكمة الأمن السيبراني.

مخرجات التعلم

- بنهاية الدورة، سيكون المشاركون قادرين على:
- وصف البنية الوظيفية المتكاملة لبيئة إدارة معلومات وأحداث الأمن السيبراني.
- تحديد مصادر البيانات المؤسسية التي ينبغي ربطها بالنظام.
- تحديد وتقييم متطلبات جمع السجلات الأمنية.
- تقييم جودة البيانات الأمنية المجمعة واكتمالها وموثوقيتها.
- تطبيق الأساليب المناسبة لتحليل البيانات وتوحيدها وإثرائها.
- تطوير حالات استخدام أمنية تتوافق مع تهديدات ومخاطر المؤسسة.
- إنشاء وتحسين منطق ربط الأحداث لاكتشاف التهديدات.
- تحليل التنبيهات الأمنية وتحديد أولويات التحقيق المناسبة.
- ربط الأحداث من مصادر متعددة لاكتشاف أنماط الهجمات المحتملة.
- إعادة بناء الحوادث الأمنية باستخدام بيانات الأحداث والتسلسل الزمني.
- استخدام معلومات التهديدات لتحسين عمليات الكشف والتحقيق.
- تحديد التنبيهات غير الصحيحة وتقليلها دون التأثير في جودة الكشف.

- تطوير لوحات معلومات وتقارير فعالة للمراقبة الأمنية.
- قياس أداء النظام وتغطية الكشف باستخدام مؤشرات مناسبة.
- دمج عمليات إدارة الأحداث الأمنية مع الاستجابة للحوادث والتصعيد.
- إعداد خارطة طريق عملية لتحسين فعالية ونضج إدارة معلومات وأحداث الأمن السيبراني.
- المحاور التدريبية

محاور الدورة

اليوم الأول

أساسيات إدارة معلومات وأحداث الأمن السيبراني والبنية الأمنية

- مفهوم إدارة معلومات وأحداث الأمن السيبراني ودورها.
- دور النظام في عمليات الأمن السيبراني الحديثة.
- البنية الأساسية ومكونات النظام.
- جمع الأحداث الأمنية وإدخال البيانات.
- مصادر السجلات والبيانات الأمنية.
- بيانات الشبكات والأجهزة والتطبيقات والهويات والبيئات السحابية.
- أساليب جمع السجلات ومسارات نقل البيانات.
- تحليل السجلات وتوحيدها.
- فهرسة البيانات وتخزينها وإدارة فترات الاحتفاظ بها والبحث فيها.
- جودة البيانات واكتمالها.
- متطلبات الرؤية الأمنية والمراقبة.
- اعتبارات تطبيق وتشغيل النظام.

اليوم الأول — تابع

- التطبيق العملي: تصميم بنية أولية لنظام إدارة معلومات وأحداث الأمن السيبراني لمؤسسة مختارة وتحديد الأنظمة ومصادر البيانات ذات الأولوية للربط.

اليوم الثاني

إعداد النظام وربط الأحداث وتطوير حالات الاستخدام

- إدخال مصادر البيانات وإدارتها.
- تحديد متطلبات المراقبة الأمنية الفعالة.
- تطوير حالات الاستخدام الأمنية.
- مفاهيم ربط الأحداث والعلاقات بينها.
- منطق القواعد وشروط الكشف.
- مراقبة المصادقة والوصول.
- كشف أنشطة الأجهزة والبرمجيات الخبيثة.
- مراقبة أحداث أمن الشبكات.
- اكتشاف السلوكيات المشبوهة للمستخدمين.
- اكتشاف تصعيد الصلاحيات واختراق الحسابات.
- مؤشرات الوصول إلى البيانات واستخراجها بصورة غير مصرح بها.
- تطوير حالات استخدام قائمة على التهديدات.
- اختبار قواعد الكشف وتحسينها.
- التطبيق العملي: تطوير مجموعة من حالات الاستخدام الأمنية وقواعد ربط الأحداث لسيناريوهات سيبرانية مختارة.

اليوم الثالث

تحليل التنبيهات والكشف عن التهديدات والتحقيق

- إنشاء التنبيهات الأمنية وإدارتها.
- تصنيف التنبيهات وتحديد مستوى خطورتها.
- فرز التنبيهات الأمنية وتحديد أولويات التحقيق.
- التمييز بين الأنشطة المشروعة والسلوكيات المشبوهة.
- التنبيهات غير الصحيحة وحالات عدم الكشف.
- ربط الأحداث والتحليل السياقي.
- بناء التسلسل الزمني للأحداث الأمنية.
- التحقيق في الحسابات المخترقة.
- التحقيق في أنشطة البرمجيات الخبيثة والأجهزة.
- التحقيق في السلوكيات المشبوهة عبر الشبكات.
- تحديد مؤشرات الاختراق.
- توثيق نتائج التحقيق.
- تصعيد الحوادث الأمنية المؤكدة.
- التطبيق العملي: التحقيق في حادث أمني افتراضي باستخدام أحداث من مصادر متعددة وإعادة بناء تسلسل الهجوم وتحديد الإجراءات المناسبة للتصعيد.

اليوم الرابع

معلومات التهديدات والاستجابة وعمليات إدارة الأحداث الأمنية

- دمج معلومات التهديدات مع النظام.
- مؤشرات الاختراق والسياق المرتبط بالتهديد.

اليوم الرابع — تابع

- إثراء الأحداث الأمنية بالمعلومات الداخلية والخارجية.
- ربط النظام بإجراءات الاستجابة للحوادث.
- تصعيد التنبيهات وإدارة الحالات.
- تنسيق العمل بين محللي النظام وفرق الاستجابة للحوادث.
- دعم إجراءات الاحتواء والاستجابة.
- لوحات المعلومات والرؤية التشغيلية.
- إعداد التقارير الأمنية للإدارة التنفيذية.
- تقارير الالتزام والتدقيق.
- التحكم في الوصول والحوكمة التشغيلية.
- إدارة أداء النظام والتحديات التشغيلية.
- التطبيق العملي: بناء مسار متكامل للاستجابة الأمنية يربط معلومات التهديدات بتحليل التنبيهات والتحقيق والتصعيد والاستجابة وإعداد التقارير وإخطار الإدارة.

اليوم الخامس

تحسين النظام وقياس الأداء والتحسين المستمر

- قياس فعالية النظام والأداء التشغيلي.
- تغطية الكشف وفعالية حالات الاستخدام.
- جودة البيانات وموثوقية مصادرها.
- حجم التنبيهات وعبء العمل على المحللين.
- تقليل التنبيهات غير الضرورية وتحسين كفاءة الكشف.
- متابعة أداء التحقيق والاستجابة.
- حوكمة النظام وتحديد المسؤوليات.

اليوم الخامس — تابع

- مراجعة فجوات الكشف في ضوء التهديدات المتطورة.
- صيانة حالات الاستخدام وتحديثها.
- الضبط والتحسين المستمر.
- تقييم مستوى نضج قدرات إدارة معلومات وأحداث الأمن السيبراني.
- إعداد خارطة طريق استراتيجية لتحسين النظام.
- الورشة الختامية: تطوير إطار تشغيلي متكامل لإدارة معلومات وأحداث الأمن السيبراني لمؤسسة مختارة، يشمل البنية ومصادر البيانات وإدخالها وحالات الاستخدام والكشف وربط الأحداث وإدارة التنبيهات والتحقيق ومعلومات التهديدات والاستجابة وإعداد التقارير والحوكمة وقياس الأداء والتحسين المستمر.

للتسجيل أو لطلب مزيد من المعلومات

صفحة الدورة:

https://quest-training.com/courses/security-information-event-management-siem-training-course

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

البريد الإلكتروني: info@quest-training.com

الهاتف: +905016771440