QUEST
Professional Center

دورة تدريبية احترافية

رقم الدورة 1987

دورة إدارة وتشغيل مركز عمليات 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 وتشغيل مركز عمليات الأمن السيبراني إطاراً عملياً متكاملاً لتصميم وإدارة وتشغيل وتطوير مراكز عمليات الأمن السيبراني الحديثة. وتركز الدورة على بناء قدرات فعالة للعمليات الأمنية تتيح الرؤية المستمرة للبيئة التقنية، والمراقبة الأمنية، والكشف عن التهديدات، وتحليل الأحداث، والاستجابة للحوادث، وإدارة المخاطر السيبرانية.

يتناول البرنامج المكونات التنظيمية والتشغيلية والتقنية لمركز عمليات الأمن السيبراني، بما يشمل نماذج التشغيل والهياكل التنظيمية والأدوار والمسؤوليات ومسارات العمل وإجراءات التصعيد وعمليات المراقبة وإدارة التنبيهات والتعامل مع الحوادث ومعلومات التهديدات وقياس الأداء. ويركز على كيفية تكامل هذه العناصر لبناء قدرة تشغيلية أمنية فعالة وموجهة نحو المخاطر.

ويولي البرنامج اهتماماً خاصاً للعمليات اليومية لمركز عمليات الأمن السيبراني، حيث يتعلم المشاركون كيفية إدارة التنبيهات الأمنية وتنفيذ الفرز الأولي والتحقيق في الأنشطة المشبوهة وتنسيق الاستجابة للحوادث وإدارة إجراءات التشغيل وتحقيق التوازن في أعباء العمل وتعزيز التعاون بين محللي الأمن وفرق الاستجابة للحوادث وتقنية المعلومات وفرق المخاطر والإدارة. كما يتناول الاستخدام الفعال للمراقبة الأمنية المركزية والأتمتة والتقنيات الأمنية في العمليات اليومية.

كما تتناول الدورة حوكمة مركز عمليات الأمن السيبراني وإدارة الأداء وجودة الخدمات وتخطيط القوى العاملة والمرونة التشغيلية والتحسين المستمر. ومن خلال السيناريوهات العملية والمحاكاة التشغيلية وتمارين التحقيق في الحوادث وقياس الأداء وورش تصميم مراكز العمليات، يطور المشاركون القدرات اللازمة لبناء مركز عمليات أمن سيبراني ناضج وقابل للقياس ومستدام.

أهداف الدورة

- بنهاية الدورة، سيتمكن المشاركون من:
- شرح الدور الاستراتيجي والوظائف الأساسية لمركز عمليات الأمن السيبراني.

- تقييم المتطلبات المؤسسية لإنشاء أو تطوير قدرات مركز عمليات الأمن السيبراني.
- تصميم نماذج تشغيل وهياكل تنظيمية مناسبة لمركز العمليات.
- تحديد الأدوار والمسؤوليات ومسارات العمل وإجراءات التصعيد.
- إنشاء عمليات فعالة للمراقبة الأمنية وإدارة التنبيهات.
- تطبيق منهجيات منظمة لفرز التنبيهات الأمنية والتحقيق فيها.
- تنسيق عمليات مركز الأمن السيبراني مع الاستجابة للحوادث وإدارة الأزمات.
- دمج معلومات التهديدات في عمليات المراقبة والكشف الأمني.
- تحسين استخدام أنظمة إدارة معلومات وأحداث الأمن السيبراني ضمن عمليات المركز.
- تقييم فرص الأتمتة وتحسين مسارات العمل الأمنية.
- إنشاء مؤشرات أداء ومقاييس فعالة لقياس أداء مركز العمليات.
- إدارة أعباء عمل المحللين والأولويات والعمليات القائمة على المناوبات.
- تعزيز حوكمة مركز العمليات والتوثيق والضوابط التشغيلية.
- تقييم مستوى نضج المركز وتحديد الفجوات التشغيلية والقدرات المطلوبة.
- تطوير مبادرات للتحسين المستمر ورفع فعالية العمليات الأمنية.
- إعداد خارطة طريق استراتيجية لتطوير وتشغيل مركز عمليات الأمن السيبراني.

الفئة المستهدفة

تستهدف الدورة مديري مراكز عمليات الأمن السيبراني وقادة الفرق ومحللي العمليات الأمنية ومتخصصي المراقبة الأمنية ومتخصصي الاستجابة للحوادث ومحللي اكتشاف التهديدات ومهندسي الأمن ومتخصصي أمن المعلومات المشاركين في العمليات الأمنية.

كما تناسب مديري الأمن السيبراني ومسؤولي أمن المعلومات ومديري تقنية المعلومات ومتخصصي معلومات

التهديدات وفرق إدارة الثغرات والمخاطر والالتزام ومتخصصي استمرارية الأعمال وقادة التقنية المسؤولين عن إنشاء أو إدارة أو الإشراف على عمليات الأمن السيبراني.

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 إنشاء أو تطوير أو تحسين قدرات مركز عمليات الأمن السيبراني.

مخرجات التعلم

- بنهاية الدورة، سيكون المشاركون قادرين على:
- تقييم مستوى النضج والفعالية التشغيلية لمركز عمليات الأمن السيبراني.
- اختيار نموذج التشغيل المناسب وفق احتياجات المؤسسة.
- تحديد الهيكل التنظيمي والأدوار والمسؤوليات وخطوط التقارير.
- إنشاء مسارات عمل فعالة للمراقبة والكشف والتحقيق والاستجابة.
- تطوير إجراءات منظمة لفرز التنبيهات وتصعيدها.
- التحقيق في الأحداث الأمنية وتحديد إجراءات الاستجابة المناسبة.
- تنسيق عمليات مركز الأمن السيبراني مع الاستجابة للحوادث والوظائف الأمنية الأخرى.
- دمج معلومات التهديدات في المراقبة الأمنية واتخاذ القرارات التشغيلية.
- تحسين استخدام أنظمة إدارة معلومات وأحداث الأمن السيبراني وتقنيات المراقبة.
- تحديد الأنشطة المتكررة التي يمكن أتمتتها داخل مركز العمليات.
- إدارة أعباء العمل والأولويات والمناوبات والطاقة التشغيلية.
- تطوير مؤشرات أداء وتقارير إدارية فعالة لمركز العمليات.

- تحديد الفجوات في الأفراد والعمليات والتقنية والحوكمة.
- إنشاء آليات لضمان جودة العمليات والتحسين المستمر.
- تعزيز المرونة التشغيلية واستمرارية خدمات مركز العمليات.
- إعداد خارطة طريق عملية لتطوير نضج وقدرات مركز عمليات الأمن السيبراني.
- المحاور التدريبية

محاور الدورة

اليوم الأول

استراتيجية مركز عمليات الأمن السيبراني وهياكل التشغيل

- الدور والأهمية الاستراتيجية لمركز عمليات الأمن السيبراني.
- الوظائف الأساسية ومسؤوليات العمليات الأمنية.
- نماذج تشغيل مراكز عمليات الأمن السيبراني.
- نماذج التشغيل الداخلي والخارجي والمختلط.
- الأدوار والمسؤوليات ومتطلبات الكفاءات.
- متطلبات المراقبة والرؤية الأمنية.
- إجراءات العمل ومسارات العمليات الأمنية.
- تحديد أولويات الأصول ومصادر البيانات.
- التكامل مع حوكمة الأمن السيبراني وإدارة المخاطر.
- سياسات وإجراءات وتوثيق عمليات المركز.
- هياكل التصعيد وقنوات الاتصال.
- تصميم إطار تشغيلي فعال لمركز العمليات.

اليوم الأول — تابع

- التطبيق العملي: تصميم نموذج تشغيلي أولي لمركز عمليات الأمن السيبراني لمؤسسة مختارة، يشمل الوظائف والأدوار ومسارات العمل وإجراءات التصعيد وأولويات المراقبة.

اليوم الثاني

المراقبة الأمنية وإدارة التنبيهات والكشف عن التهديدات

- مبادئ المراقبة الأمنية والرؤية التشغيلية.
- إدارة الأحداث والسجلات الأمنية.
- دور أنظمة إدارة معلومات وأحداث الأمن السيبراني في عمليات المركز.
- إنشاء التنبيهات الأمنية وإدارتها.
- تصنيف التنبيهات وتحديد أولوياتها.
- إجراءات فرز التنبيهات والتحقيق فيها.
- تحديد مؤشرات الاختراق.
- اكتشاف السلوكيات المشبوهة للمستخدمين والأجهزة والشبكات.
- حالات الاستخدام الأمنية وقواعد ربط الأحداث.
- إدارة التنبيهات غير الصحيحة وتحسين قواعد الكشف.
- دمج معلومات التهديدات.
- تحسين تغطية الكشف وفعالية المراقبة.
- التطبيق العملي: تحليل مجموعة من التنبيهات الأمنية وترتيب أولوياتها وفق المخاطر وتنفيذ التحقيق الأولي وتحديد إجراءات التصعيد المناسبة.

اليوم الثالث

الاستجابة للحوادث والتنسيق التشغيلي

- مسؤوليات مركز العمليات خلال دورة حياة الحادث.
- تحديد الحوادث وتقييمها الأولي.
- فرز الحوادث الأمنية وتصنيفها.
- التحقيق وجمع الأدلة.
- تصعيد الحوادث وتسليم الحالات.
- التنسيق بين مركز العمليات وفرق الاستجابة للحوادث.
- دعم عمليات الاحتواء والاستجابة.
- إدارة الحوادث الأمنية عالية الخطورة.
- التنسيق مع تقنية المعلومات والبنية التحتية والمخاطر والشؤون القانونية والالتزام وفرق الأعمال.
- توثيق الحوادث وإدارة الحالات.
- الاتصالات أثناء الحوادث الأمنية.
- المراجعة بعد الحادث والدروس المستفادة.
- التطبيق العملي: تنفيذ محاكاة لحادث أمني داخل مركز العمليات تبدأ من التنبيه الأولي، مروراً بالتحقيق والتصعيد وتنسيق الاستجابة، وصولاً إلى المراجعة بعد الحادث.

اليوم الرابع

إدارة مركز العمليات والأتمتة وقياس الأداء

- إدارة محللي الأمن والفرق التشغيلية.
- إدارة المناوبات والتغطية التشغيلية المستمرة.
- توزيع أعباء العمل وترتيب الأولويات.

اليوم الرابع — تابع

- تطوير مهارات المحللين وإدارة الكفاءات والأداء.
- الأتمتة وتحسين مسارات العمل الأمنية.
- أتمتة مهام المراقبة والاستجابة المتكررة.
- تحسين الكفاءة التشغيلية.
- جودة الخدمات والضوابط التشغيلية.
- مؤشرات الأداء والتشغيل الرئيسية.
- قياس أداء معالجة التنبيهات والاستجابة.
- لوحات المعلومات والتقارير الإدارية.
- إدارة المخاطر التشغيلية واستمرارية الخدمات.
- التطبيق العملي: تطوير إطار لقياس أداء مركز العمليات يشمل احتياجات القوى العاملة وإدارة أعباء العمل والمؤشرات التشغيلية وجودة الخدمات وفرص الأتمتة والتقارير الإدارية.

اليوم الخامس

حوكمة مركز العمليات والنضج والتحسين المستمر

- حوكمة مركز عمليات الأمن السيبراني والمساءلة.
- سياسات ومعايير العمليات الأمنية.
- تقييم نضج وقدرات مركز العمليات.
- تحديد الفجوات في الأفراد والعمليات والتقنية والحوكمة.
- تقييم قدرات الكشف والاستجابة.
- ضمان الجودة والمراجعات التشغيلية.
- قياس ومقارنة أداء مركز العمليات.
- التحسين المستمر ورفع الكفاءة.

اليوم الخامس — تابع

- تحسين فعالية المحللين ومسارات العمل.
- تعزيز المرونة التشغيلية لمركز العمليات.
- التطوير الاستراتيجي والتحول التشغيلي.
- إعداد خارطة طريق طويلة المدى لنضج مركز العمليات.
- الورشة الختامية: تطوير إطار متكامل لإدارة وتشغيل مركز عمليات الأمن السيبراني لمؤسسة مختارة، يشمل نموذج التشغيل والهيكل التنظيمي والمراقبة والكشف وإدارة التنبيهات والاستجابة للحوادث ومعلومات التهديدات والأتمتة والقوى العاملة وقياس الأداء والحوكمة وتقييم النضج والتحسين المستمر.

للتسجيل أو لطلب مزيد من المعلومات

صفحة الدورة:

https://quest-training.com/courses/security-operations-center-soc-management-operations-training-course

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

البريد الإلكتروني: info@quest-training.com

الهاتف: +905016771440