الدورة التدريبية للمحترف المعتمد في إدارة الأمن السيبراني

3 – 7 أكتوبر 2027

عمان

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

الدورة التدريبية للمحترف المعتمد في إدارة الأمن السيبراني

المرجع: 98876_103600296 **التاريخ:** 3 – 7 أكتوبر 2027 **المكان:** عمان **الرسوم:** Euro 6000

نظرة عامة على الدورة التدريبية

تزود الدورة التدريبية للمحترف المعتمد في إدارة الأمن السيبراني المشاركين بالمعرفة العملية والمهارات الاستراتيجية والتقنيات الإدارية اللازمة لقيادة وإدارة برامج الأمن السيبراني بفعالية. يمزج هذا التدريب الشامل في إدارة الأمن السيبراني بين المعرفة التأسيسية والاستراتيجيات المتقدمة، مما يضمن تزويد المشاركين بالقدرة على تطوير وتنفيذ وإدارة برامج أمن سيبراني قوية تتماشى مع الأطر الدولية مثل التدريب على الأمن السيبراني وفقًا لمعيار iso/iec 27032 والتدريب على إطار عمل الأمن السيبراني من nist.

يركز هذا التدريب للحصول على شهادة في الأمن السيبراني على التدريب على الاستجابة للحوادث وإدارة المخاطر، والتدريب على إطار حوكمة الأمن السيبراني، والتدريب على تنفيذ برامج الأمن السيبراني. ويسلط الضوء على أفضل الممارسات في التدريب على المرونة السيبرانية وتخفيف المخاطر، مع التركيز على كيفية تطوير سياسات وإجراءات الأمن السيبراني، وإجراء تقييمات المخاطر، وإدارة الحوادث، وإجراء عمليات المراجعة من أجل التحسين المستمر. سيكتسب المشاركون خبرة في التدريب على التواصل والتوعية في مجال الأمن السيبراني، وتقنيات دورة تخفيف التهديدات وإدارة الثغرات الأمنية، والتدريب على دورة حياة تطوير البرمجيات الآمنة للتوافق مع التحديات التنظيمية الحديثة.

من خلال إكمال دورة إدارة أمن المعلومات هذه، سيكون المشاركون مستعدين أيضًا للحصول على شهادة الأساس في الأمن السيبراني من PECB والتدريب على مدير الأمن السيبراني الرائد، مما يؤهلهم للتطوير الوظيفي والتقدم المهني في مجال قيادة الأمن السيبراني المتطور.

الجمهور المستهدف

- كبار مسؤولي أمن المعلومات
- مديرو الأمن السيبراني
- مديرو أمن تكنولوجيا المعلومات
- مديرو المخاطر ومسؤولو الامتثال
- قادة فرق الاستجابة للحوادث
- مديرو استمرارية الأعمال
- المراجعون الداخليون والخارجيون
- الاستشاريون الذين يستعدون للتدريب على مدير الأمن السيبراني الرائد

AGILE LEADERS
Training Center

الإدارات التنظيمية المستهدفة

- إدارات أمن المعلومات والأمن السيبراني
- فرق إدارة مخاطر وحوكمة تكنولوجيا المعلومات
- فرق الامتثال والشؤون التنظيمية
- فرق استمرارية الأعمال والتعافي من الكوارث
- إدارات المراجعة الداخلية وحوكمة الشركات
- المكاتب القانونية ومكاتب خصوصية البيانات

القطاعات المستهدفة

- الخدمات المالية والمصرفية
- الرعاية الصحية والصناعات الدوائية
- القطاع الحكومي والعام
- التكنولوجيا والاتصالات
- الصناعات التحويلية وسلاسل التوريد
- البنية التحتية الحيوية والمرافق العامة
- التجارة الإلكترونية والمنصات عبر الإنترنت
- الخدمات الاستشارية والمهنية

مخرجات الدورة التدريبية

بنهاية هذه الدورة، سيتمكن المشاركون من

- تطوير وتنفيذ برامج أمن سيبراني شاملة باستخدام التدريب على تنفيذ برامج الأمن السيبراني
- مواءمة الاستراتيجيات التنظيمية مع التدريب على إطار حوكمة الأمن السيبراني والتدريب على الأمن السيبراني وفقًا لمعيار iso/iec 27032
- إدارة التهديدات والحوادث والثغرات السيبرانية باستخدام التدريب على الاستجابة للحوادث وإدارة المخاطر
- تطبيق أفضل الممارسات من دورة إدارة مخاطر الأمن السيبراني ودورة تخفيف التهديدات وإدارة الثغرات الأمنية
- وضع سياسات وإجراءات للأمن السيبراني تتماشى مع الأطر التنظيمية من خلال التدريب المخصص لذلك
- إجراء تدريب على تقييم مخاطر الأمن السيبراني وضمان الامتثال من خلال التدريب على مراجعة وتدقيق برامج الأمن السيبراني
- دمج إدارة الحوادث مع عمليات استمرارية الأعمال والتدريب على الأمن السيبراني
- بناء واستدامة برامج التوعية بالأمن السيبراني باستخدام تقنيات التدريب على التواصل والتوعية في مجال الأمن السيبراني

منهجية التدريب

تستخدم الدورة التدريبية للمحترف المعتمد في إدارة الأمن السيبراني نهج التعلم المدمج للجمع بين المحاضرات التي يقودها الخبراء والتمارين الجماعية التعاونية وتحليل دراسات الحالة. يطبق المشاركون بفاعلية المفاهيم المستمدة من التدريب على إدارة الأمن السيبراني وسيناريوهات دورة إدارة مخاطر الأمن السيبراني على أمثلة من العالم الواقعي، مما يضمن تطوير المهارات العملية.

تركز المناقشات الجماعية على مواءمة التدريب على إطار حوكمة الأمن السيبراني مع الاستراتيجيات التنظيمية، بينما تعزز تمارين دراسات الحالة تقنيات دورة تخفيف التهديدات وإدارة الثغرات الأمنية وعمليات التدريب على الاستجابة للحوادث وإدارة المخاطر. يعمل المشاركون في فرق لتصميم خطط التدريب على إدارة حوادث الأمن السيبراني وإجراء تمارين محاكاة بناءً على حوادث فعلية.

لتعزيز التعلم، يطور المشاركون برامج أمن سيبراني وهمية، ويجرون مراجعات داخلية باستخدام مبادئ التدريب على مراجعة وتدقيق برامج الأمن السيبراني، ويقدمون نتائجهم للزملاء والمدربين. تدعم التغذية الراجعة المستمرة عملية التعلم، بينما تساعد التمارين التفاعلية التي تستخدم التدريب على قياس أداء الأمن السيبراني وأدوات تتبع المقاييس والأداء المشاركين على تقييم فعالية البرنامج. يختتم البرنامج بالتحضير لامتحان شهادة الأساس في الأمن السيبراني من PECB لمساعدة المشاركين على الحصول على شهادة مهنية.

مجموعة أدوات الدورة التدريبية

- دليل التدريب على إدارة الأمن السيبراني
- نماذج التدريب على تقييم مخاطر الأمن السيبراني
- إرشادات التدريب على إدارة حوادث الأمن السيبراني
- أدلة التدريب على إطار حوكمة الأمن السيبراني
- قوائم التحقق للتدريب على الاستجابة للحوادث وإدارة المخاطر
- نماذج التدريب على سياسات وإجراءات الأمن السيبراني
- دراسات حالة لتمارين دورة تخفيف التهديدات وإدارة الثغرات الأمنية
- قوائم التحقق للتدريب على مراجعة وتدقيق برامج الأمن السيبراني
- نماذج لأدوات التدريب على قياس أداء الأمن السيبراني
- دليل التحضير لامتحان شهادة الأساس في الأمن السيبراني من PECB

AGILE LEADERS
Training Center

جدول أعمال الدورة التدريبية

اليوم الأول: مقدمة في إدارة وحوكمة الأمن السيبراني

- الموضوع 1: مقدمة في التدريب على إدارة الأمن السيبراني وأهداف الدورة
- الموضوع 2: نظرة عامة على التدريب على الأمن السيبراني وفقًا لمعيار iso/iec 27032 والتدريب على إطار عمل الأمن السيبراني من nist
- الموضوع 3: تحديد الأدوار التنظيمية باستخدام التدريب على أدوار ومسؤوليات فريق الأمن السيبراني
- الموضوع 4: تأسيس أسس البرنامج باستخدام التدريب على تنفيذ برامج الأمن السيبراني
- الموضوع 5: التدريب على إطار حوكمة الأمن السيبراني ومواءمة السياسات
- تأمل ومراجعة: مراجعة مفاهيم دورة حوكمة وقيادة الأمن السيبراني

اليوم الثاني: إدارة مخاطر الأمن السيبراني وتخفيف التهديدات

- الموضوع 1: إجراء تدريب على تقييم مخاطر الأمن السيبراني وتحديد الثغرات الأمنية
- الموضوع 2: إدارة المخاطر باستخدام تقنيات دورة إدارة مخاطر الأمن السيبراني
- الموضوع 3: تطوير استراتيجيات دورة تخفيف التهديدات وإدارة الثغرات الأمنية
- الموضوع 4: ربط استمرارية الأعمال والتدريب على الأمن السيبراني من أجل المرونة
- الموضوع 5: وضع سياسات وإجراءات للأمن السيبراني من خلال التدريب المخصص لذلك
- تأمل ومراجعة: مراجعة دمج إدارة المخاطر والتهديدات مع التدريب على إطار حوكمة الأمن السيبراني

اليوم الثالث: إدارة الحوادث والاستجابة لها

- الموضوع 1: بناء عمليات استجابة فعالة باستخدام التدريب على إدارة حوادث الأمن السيبراني
- الموضوع 2: تفعيل فرق الاستجابة للحوادث باستخدام التدريب على الاستجابة للحوادث وإدارة المخاطر
- الموضوع 3: كشف الحوادث وتقييمها وتصعيدها باستخدام الإبلاغ عن حوادث الأمن السيبراني والتحقيق فيها
- الموضوع 4: إجراء تحليل ما بعد الحادث والدروس المستفادة باستخدام التدريب على إدارة حوادث الأمن السيبراني
- الموضوع 5: دمج إدارة الحوادث مع التدريب على مقارنة إطار عمل iso/iec 27032 مقابل إطار عمل nist
- تأمل ومراجعة: مراجعة سيناريوهات الحوادث وإدارتها باستخدام دراسات حالة من العالم الواقعي

اليوم الرابع: الامتثال والمراجعات وأداء البرنامج

- الموضوع 1: التدريب على الامتثال والتنظيم في الأمن السيبراني للأطر والمعايير
- الموضوع 2: إجراء مراجعات داخلية باستخدام التدريب على مراجعة وتدقيق برامج الأمن السيبراني
- الموضوع 3: مراقبة نجاح البرنامج باستخدام التدريب على قياس أداء الأمن السيبراني
- الموضوع 4: استخدام مقاييس الأمن السيبراني وتتبع الأداء من أجل التحسين المستمر
- الموضوع 5: ضمان التوافق مع متطلبات التدريب على الأمن السيبراني وفقًا لمعيار iso/iec 27032
- تأمل ومراجعة: مراجعة فعالية البرنامج ومواءمة الامتثال باستخدام دراسات الحالة

اليوم الخامس: التواصل والتوعية والتحضير للشهادة

- الموضوع 1: بناء الوعي باستخدام التدريب على التواصل والتوعية في مجال الأمن السيبراني
- الموضوع 2: تطوير خطط التواصل باستخدام التدريب على استراتيجية التواصل في الأمن السيبراني
- الموضوع 3: دمج الأمن مع العمليات باستخدام دمج الأمن السيبراني مع استمرارية الأعمال
- الموضوع 4: المراجعة النهائية والاختبار التجريبي باستخدام التحضير لامتحان شهادة الأساس في الأمن السيبراني من PECB
- الموضوع 5: امتحان الشهادة
- تأمل ومراجعة: مراجعة عروض المشاركين وخطط العمل الشخصية للتطوير الوظيفي والحصول على الشهادة في مجال الأمن السيبراني

الأسئلة الشائعة

ما هي المؤهلات أو المتطلبات المسبقة المحددة اللازمة للمشاركين قبل التسجيل في الدورة؟

لا توجد متطلبات مسبقة رسمية للدورة التدريبية للمحترف المعتمد في إدارة الأمن السيبراني، ولكن سيستفيد المشاركون الذين لديهم خبرة سابقة في الأمن السيبراني أو إدارة المخاطر أو حوكمة تكنولوجيا المعلومات بشكل أكبر. هذا التدريب مثالي للمهنيين الذين يستعدون لشهادة الأساس في الأمن السيبراني من PECB والتدريب على مدير الأمن السيبراني الرائد.

كم تبلغ مدة الجلسة اليومية، وهل هناك عدد إجمالي من الساعات المطلوبة للدورة بأكملها؟

تستمر كل جلسة يومية بشكل عام لمدة تتراوح بين 4 إلى 5 ساعات، مع فترات راحة وأنشطة تفاعلية. تمتد مدة الدورة الإجمالية على مدى خمسة أيام، أي ما يقرب من 20 إلى 25 ساعة من التدريس.

AGILE LEADERS
Training Center

كيف تعد هذه الدورة المشاركين للأدوار القيادية في مجال الأمن السيبراني؟

تدمج الدورة التدريب المتقدم في قيادة واستراتيجية الأمن السيبراني مع التدريب العملي على إدارة الأمن السيبراني، مما يسمح للمشاركين بتطوير الفهم التقني ومهارات اتخاذ القرار على المستوى التنفيذي، وهي أمور ضرورية لبناء برامج الأمن السيبراني والحفاظ عليها.

كيف تختلف هذه الدورة التدريبية عن غيرها من دورات المحترف المعتمد في إدارة الأمن السيبراني

تقدم الدورة التدريبية للمحترف المعتمد في إدارة الأمن السيبراني أكثر من مجرد مهارات تقنية، فهي تزود المشاركين بالخبرة الاستراتيجية والتشغيلية على حد سواء. تمزج هذه الدورة بين التدريب على إدارة الأمن السيبراني وتقنيات دورة إدارة مخاطر الأمن السيبراني، مما يضمن قدرة المشاركين على تصميم وتنفيذ وتحسين برامج أمنية شاملة.

على عكس البرامج الأخرى، تربط هذه الدورة التدريب على إطار حوكمة الأمن السيبراني بأهداف العمل والاحتياجات التنظيمية. كما أنها تركز على التدريب على الاستجابة للحوادث وإدارة المخاطر، وتغطي دورة حياة الحادث بأكملها بدءًا من الكشف وحتى الدروس المستفادة. تتيح التمارين العملية باستخدام دراسات حالة من العالم الواقعي للمشاركين تطبيق التدريب على إدارة حوادث الأمن السيبراني، والتدريب على سياسات وإجراءات الأمن السيبراني، والتدريب على تقييم مخاطر الأمن السيبراني مباشرة في سيناريوهات العمل.

مع التركيز الإضافي على التدريب على التواصل والتوعية في مجال الأمن السيبراني والتحضير لشهادة الأساس في الأمن السيبراني من PECB، يخرج المشاركون ليس فقط بالمعرفة التقنية ولكن أيضًا بالمهارات القيادية لدفع استراتيجيات الأمن والتقدم في حياتهم المهنية.