

دورة معتمدة بأمن الشبكات ISO 27033 لتأمين شبكاتك بفعالية

17 – 21 يناير 2027

نيروبي

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

دورة معتمدة بأمن الشبكات ISO 27033 لتأمين شبكاتك بفعالية

المرجع: 99175_103600302 **التاريخ:** 17 – 21 يناير 2027 **المكان:** نيروبي **الرسوم:** Euro 6000

نظرة عامة على الدورة:

صُممت الدورة المعتمدة بأمن الشبكات ISO/IEC 27033: تأمين شبكات تكنولوجيا المعلومات بفعالية، خصيصًا لتزويد محترفي تكنولوجيا المعلومات بالخبرة المتقدمة في أمن الشبكات، والتدريب على الأمن السيبراني، والتنفيذ العملي لمعايير أمن الشبكات. تتناول هذه الدورة موضوعات رئيسية تشمل أمن الشبكات الافتراضية الخاصة VPN، وأمن الشبكات اللاسلكية، وبوابات الأمان، والاستراتيجيات المتقدمة للحماية من التهديدات السيبرانية. سيتقن المشاركون تقنيات مثل إدارة مخاطر الشبكة، واستراتيجيات تقييم مخاطر أمن الشبكة، والتدابير الأمنية المتقدمة لشبكات المؤسسات.

مع التركيز على تطبيق معيار ISO/IEC 27033 للأمن السيبراني، توجه هذه الدورة التدريبية المتعلمين خلال التنفيذ التدريجي لأمن الشبكات، وتعلمهم أفضل الممارسات للامتثال لأمن الشبكات، ومنع الوصول غير المصرح به، وتأمين الاتصالات اللاسلكية للأعمال. سيستكشف المشاركون أيضًا استراتيجيات أمن جدار الحماية، وإدارة الضوابط الأمنية، وتعزيز مرونة الأمن السيبراني. تضمن هذه الدورة الشاملة أن يتمكن المشاركون من تطبيق الإرشادات بفعالية لتصميم بنية شبكة آمنة وحماية شبكات الأعمال من التهديدات السيبرانية.

الجمهور المستهدف:

- مديرو أمن الشبكات
- محترفو أمن تكنولوجيا المعلومات
- محللو الأمن السيبراني
- مديرو الشبكات
- مسؤولو الامتثال في تكنولوجيا المعلومات
- مسؤولو أمن المعلومات

AGILE LEADERS
Training Center

الإدارات التنظيمية المستهدفة:

- إدارات أمن تكنولوجيا المعلومات والأمن السيبراني
- عمليات الشبكات
- إدارة البنية التحتية لتكنولوجيا المعلومات
- الامتثال وإدارة المخاطر
- استمرارية الأعمال والتعافي من الكوارث

القطاعات المستهدفة:

- تكنولوجيا المعلومات والخدمات
- القطاع المصرفي والمالي
- الرعاية الصحية والصناعات الدوائية
- الاتصالات
- الحكومة والإدارة العامة
- التصنيع والأتمتة الصناعية

مخرجات الدورة:

بنهاية هذه الدورة، سيتمكن المشاركون من:

- تطبيق معايير شهادة أمن الشبكات ISO/IEC 27033
- إجراء استراتيجيات فعالة لتقييم مخاطر أمن الشبكة
- حماية شبكات الأعمال من التهديدات السيبرانية باستخدام تدابير أمنية متقدمة
- استخدام تقنيات تشفير الشبكة لحماية البيانات
- تطوير وإدارة حلول أمن الشبكات الافتراضية الخاصة VPN والشبكات اللاسلكية الآمنة
- وضع استراتيجيات قوية لأمن جدار الحماية
- تطبيق الضوابط الأمنية التقنية لشبكات المؤسسات
- تعزيز حوكمة أمن الشبكات في بيئات تكنولوجيا المعلومات التنظيمية

منهجية التدريب:

تستخدم هذه الدورة التدريبية منهجيات متنوعة، بما في ذلك المحاضرات التفاعلية، والتمارين العملية، والمناقشات الجماعية، ودراسات الحالة العملية. سيشارك المتدربون في جلسات تفاعلية مصممة حول سيناريوهات واقعية لأمن الشبكات لتطبيق تقنيات إدارة مخاطر الشبكة بفعالية. تسلط دراسات الحالة حول الحماية من التهديدات السيبرانية وخروقات البيانات الضوء على أهمية المرونة السيبرانية الاستباقية والامتثال. تتيح الأنشطة الجماعية وورش العمل للمشاركين استكشاف الاتصالات اللاسلكية الآمنة للأعمال واستراتيجيات أمن جدار الحماية بشكل تعاوني، مما يعزز التعلم من خلال التمارين العملية. تضمن جلسات التقييم المنتظمة تجارب تعلم مخصصة، مع التركيز على التنفيذ التدريجي لأمن الشبكات والتدابير الأمنية المتقدمة لشبكات المؤسسات. يعزز هذا النهج التدريبي التفاعلي القدرة على تطبيق معيار ISO/IEC 27033 بفعالية، مما يضمن أن يكون المشاركون مجهزين جيدًا لإدارة تهديدات الأمن السيبراني وتحديات الامتثال في مؤسساتهم.

أدوات الدورة:

- مواد دراسية وكتيبات عمل رقمية شاملة
- قوائم تحقق ونماذج لأمن الشبكات
- إرشادات للامتثال لأمن الشبكات
- موارد عبر الإنترنت للمرونة السيبرانية
- أمثلة ورؤى حول شهادة أمن الشبكات ISO/IEC 27033

جدول أعمال الدورة:

اليوم الأول: مقدمة في أمن الشبكات ومعيار ISO/IEC 27033

- الموضوع 1: نظرة عامة على معايير أمن الشبكات والامتثال لمعيار ISO/IEC 27033
- الموضوع 2: أهمية أمن الشبكات في البنية التحتية لتكنولوجيا المعلومات
- الموضوع 3: إرشادات لتصميم بنية شبكة آمنة
- الموضوع 4: أساسيات إدارة مخاطر الشبكة
- الموضوع 5: منع الوصول غير المصرح به إلى الشبكات
- مراجعة وتأمل: النقاط الرئيسية في أمن الشبكات وإدارة المخاطر

اليوم الثاني: تطبيق ضوابط أمن الشبكات الفعالة

- الموضوع 1: الضوابط الأمنية التقنية لشبكات المؤسسات
- الموضوع 2: أفضل الممارسات للامتثال لأمن الشبكات
- الموضوع 3: إدارة الضوابط الأمنية في بيئات الشبكات
- الموضوع 4: بوابات الأمان واستراتيجيات أمن جدار الحماية
- الموضوع 5: التنفيذ التدريجي لأمن الشبكات
- مراجعة وتأمل: استراتيجيات فعالة لبيئات تكنولوجيا المعلومات الآمنة

اليوم الثالث: تقنيات أمن الشبكات المتقدمة

- الموضوع 1: تقنيات تشفير الشبكة لأمن البيانات
- الموضوع 2: استراتيجيات الحماية من التهديدات السيبرانية واكتشافها
- الموضوع 3: تأمين الاتصالات الرقمية باستخدام معيار ISO/IEC 27033
- الموضوع 4: أمن الشبكات الافتراضية الخاصة VPN وتأمين شبكات الوصول عن بعد
- الموضوع 5: حماية البيانات الشخصية من خلال الشبكات الآمنة
- مراجعة وتأمل: رؤى حول أساليب حماية الشبكات المتقدمة

اليوم الرابع: أمن الشبكات اللاسلكية والأمن السحابي

- الموضوع 1: أمن الشبكات اللاسلكية لبيئات الأعمال
- الموضوع 2: تدابير أمن الشبكات السحابية للشركات
- الموضوع 3: تعزيز مرونة الأمن السيبراني من خلال أمن الشبكات
- الموضوع 4: حماية شبكات الوصول عن بعد بشكل آمن
- الموضوع 5: أفضل ممارسات استمرارية الأعمال وأمن الشبكات
- مراجعة وتأمل: توحيد أفضل ممارسات أمن الشبكات

اليوم الخامس: الحوكمة وإدارة مخاطر أمن الشبكات

- الموضوع 1: حوكمة أمن الشبكات للمؤسسات
- الموضوع 2: تطبيق إدارة المخاطر السيبرانية لمحترفي تكنولوجيا المعلومات
- الموضوع 3: حلول امتثال تكنولوجيا المعلومات لأمن الشبكات
- الموضوع 4: منع خروقات البيانات بأمن شبكات قوي
- الموضوع 5: الاتجاهات والابتكارات المستقبلية في التدريب على الأمن السيبراني
- مراجعة وتأمل: مراجعة شاملة للدورة واستراتيجيات التنفيذ

AGILE LEADERS
Training Center

الأسئلة الشائعة:

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

يجب أن يكون لدى المشاركين معرفة أساسية بالبنية التحتية للشبكات، ومبادئ الأمن السيبراني، وخبرة عمل سابقة في مجال تكنولوجيا المعلومات.

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

تستمر كل جلسة يومية عادةً لمدة تتراوح بين 4 و5 ساعات، شاملة فترات الراحة والأنشطة التفاعلية. وتمتد الدورة بأكملها على مدى أسبوع، بإجمالي 20 إلى 25 ساعة تدريبية تقريبًا.

هل يضمن تطبيق معايير ISO/IEC 27033 حماية كاملة ضد التهديدات السيبرانية؟

بينما يوفر معيار ISO/IEC 27033 أطرًا قوية لتأمين الشبكات، فإن الحماية الكاملة تعتمد على التطبيق المستمر والتقييم المتواصل والتحديث الدائم للممارسات الأمنية.

بماذا تختلف هذه الدورة عن دورات ISO/IEC 27033 المعتمدة الأخرى:

تركز الدورة المعتمدة بأمن الشبكات ISO/IEC 27033 بشكل فريد على استراتيجيات التنفيذ العملية والقابلة للتطبيق والمصممة خصيصًا لشبكات تكنولوجيا المعلومات الآمنة. على عكس دورات شهادات أمن تكنولوجيا المعلومات القياسية، فهي تجمع بين المعرفة النظرية بمعايير أمن الشبكات والتجارب العملية، مما يضمن اكتساب المشاركين فهمًا عميقًا لمنهجيات التدريب على الأمن السيبراني. تغطي الدورة بشكل مميز سيناريوهات شاملة مثل أمن الشبكات الافتراضية الخاصة VPN، وأمن الشبكات اللاسلكية، والتقنيات المتقدمة للحماية من التهديدات السيبرانية، مما يزود المتعلمين بنهج واقعية لمنع الوصول غير المصرح به وحماية البيانات الحساسة. كما أن استخدامها المكثف لدراسات الحالة العملية والتفاعلات الجماعية والمراجعات التأملية يميزها عن غيرها من عروض الشهادات المماثلة. سيستكشف المشاركون استراتيجيات مفصلة لإدارة الضوابط الأمنية، وتطبيق الضوابط الأمنية التقنية لشبكات المؤسسات، وتحقيق الامتثال لأمن الشبكات بفعالية، مما يوفر ميزة تنافسية واضحة على دورات أمن الشبكات المماثلة.