

تقييم وإدارة مخاطر الأمان السيبراني



GENTEX®
TRAINING CENTER



المقدمة

في المشهد الرقمي المتتطور باستمرار، تشكل التهديدات السيبرانية تحديًّا مستمراً للمؤسسات من جميع الأحجام. يعد اتباع نهج استباقي لتقدير وإدارة مخاطر الأمان السيبراني أمرًا ضروريًّا لحماية البيانات الحساسة، وحماية البنية التحتية الحيوية، وضمان استمرارية الأعمال. يزود هذا البرنامج المكثف الذي يستمر خمسة أيام، والذي يقدمه مركز جينتكس للتدريب، المشاركين بالمعرفة والمهارات العملية اللازمة لتقدير مخاطر الأمان السيبراني بشكل فعال، وتطوير استراتيجيات تخفيف قوية، وتنفيذ إطار شامل لإدارة المخاطر. ومن خلال الاستكشاف الشامل لمنهجيات تقييم المخاطر الرئيسية وأفضل ممارسات الصناعة والتمارين العملية، يكتسب المشاركون القدرة على تحديد نقاط الضعف وتحديد أولويات المخاطر وبناء وضع قوي للأمن السيبراني داخل مؤسساتهم.

أهداف دورة تقييم وإدارة مخاطر الأمان السيبراني:

- إتقان المبادئ الأساسية لتقدير وإدارة مخاطر الأمان السيبراني.
- فهم مشهد التهديدات السيبرانية والأنواع المختلفة من الهجمات السيبرانية التي تواجهها المؤسسات.
- تحديد وتحليل نقاط الضعف في الأمان السيبراني داخل البنية التحتية لتقنيولوجيا المعلومات وأنظمة البيانات في المؤسسة.
- تطبيق منهجيات تقييم المخاطر المت الموافقة مع معايير الصناعة لتقدير احتمالية التهديدات السيبرانية وتأثيرها.
- وضع خطة شاملة لإدارة المخاطر لتحديد أولويات المخاطر وتحصين الموارد وتنفيذ استراتيجيات التخفيف.



- استكشف أفضل الممارسات للاستجابة للحوادث والتعافي من الكوارث و التخطيط لاستمرارية الأعمال في حالة وقوع هجوم إلكتروني.
- الاستفادة من الأطر القانونية والتنظيمية ذات الصلة بإدارة مخاطر الأمن السيبراني.
- تحليل دراسات الحالة الواقعية لعمارات إدارة مخاطر الأمن السيبراني الناجحة وغير الناجحة.
- قم بصياغة خطة عمل مخصصة لتقدير وإدارة مخاطر الأمن السيبراني داخل مؤسستك.

منهجية الدورة

يستخدم هذا البرنامج التفاعلي نهجاً يركز على المشاركين. فهو يعزز بين محاضرات خبراء الأمان السيبراني وورش العمل التفاعلية ودراسات الحالة الواقعية والمناقشات الجماعية والتمارين العملية. يشارك المشاركين بنشاط في إجراء تقييمات المخاطر، وتطوير خطط إدارة المخاطر، ومحاكاة سيناريوهات الاستجابة للحوادث، وصياغة خطط عمل لمعالجة مخاطر الأمن السيبراني المحددة داخل مؤسساتهم. من خلال التعلم التجريبي، يكتسب المشاركون المهارات العملية والمعرفة النظرية الضرورية ليصبحوا أبطال إدارة مخاطر الأمن السيبراني داخل مؤسساتهم، مما يضمن بيئة رقمية أكثر أماناً وموثوقة.

الفئات المستهدفة

- يسعى متخصصو أمن تكنولوجيا المعلومات ومسؤولو الأنظمة ومهندسو الشبكات إلى تعزيز مهاراتهم في تقييم مخاطر الأمن السيبراني وإدارتها.
- مدورو الأعمال ومديرو المشاريع وصناع القرار المسؤولون عن حماية الأصول التنظيمية والتخفيض من مخاطر الأمن السيبراني.



- يسعى مسؤولو الامتثال ومتخصصو إدارة المخاطر إلى دمج اعتبارات الأمان السيبراني في إطار إدارة المخاطر الشاملة الخاصة بهم.

- أي شخص مهتم بالفهم والمساهمة في بناء وضع قوي للأمن السيبراني لمؤسساته.

محتوى دورة تقييم وإدارة مخاطر الأمان السيبراني:

اليوم الأول: فهم المشهد: تحديد نقاط الضعف في الأمان السيبراني

- إزالة الغموض عن مخاطر الأمان السيبراني: المفاهيم الأساسية، ومشهد التهديد، وأنواع الهجمات السيبرانية

- تحديد نقاط الضعف وتحليلها: البنية التحتية للشبكة، وأنظمة البيانات، والعوامل البشرية

اليوم الثاني: تقييم المخاطر: منهجيات تقييم المخاطر المتواقة مع معايير الصناعة

- استكشاف منهجيات تقييم المخاطر: AEMF (AEMF TSIN FSC) إطار المعهد الوطني للمعايير والتكنولوجيا للأمن السيبراني

- إجراء تقييمات المخاطر وتقييم احتمالية وتأثير التهديدات السيبرانية



اليوم الثالث: بناء دفاع قوي: وضع خطة شاملة لإدارة المخاطر

- تحديد أولويات المخاطر وتحصيص الموارد: وضع خطة لإدارة المخاطر مع استراتيجيات التخفيف

- ضوابط التنفيذ: الضمانات الفنية والإدارية والعادية لمعالجة نقاط الضعف

اليوم الرابع: ما بعد الخرق: الاستجابة للحوادث، والتعافي من الكوارث، واستمرارية الأعمال

- التخطيط لما هو غير متوقع: تطوير خطة الاستجابة للحوادث واستراتيجية التعافي من الكوارث

- ضمان استمرارية الأعمال: تقليل وقت التوقف عن العمل والحفاظ على العمليات الحيوية بعد الهجوم

الإلكتروني

اليوم الخامس: بناء مستقبل آمن: الاعتبارات القانونية وأفضل الممارسات وتحطيط العمل

- فهم الأطر القانونية والتنظيمية المتعلقة بالأمن السيبراني

- استكشاف أفضل الممارسات لإدارة المخاطر المستمرة والتحسين المستمر

- صياغة خطة عمل مخصصة لتنفيذ تقييم مخاطر الأمن السيبراني وإدارتها داخل مؤسستك



الخاتمة:

من خلال إكمال هذا البرنامج الشامل الذي يقدمه مركز جينتكس للتدريب بنجاح، يكتسب المشاركون المعرفة والمهارات العملية الالزمة للتنقل في العالم المعقد لتقدير وإدارة مخاطر الأمن السيبراني. وسيكونون مجهزين لتحديد ومعالجة الخروقات الأمنية المحتملة، وتحديد أولويات المخاطر السيبرانية بشكل فعال، والمساهمة في بناء وضع أمني سيبراني قوي ومرن داخل مؤسساتهم. وتمكنهم هذه المعرفة المعززة من أن يصبحوا مدافعين استباقيين في مكافحة التهديدات السيبرانية، وحماية الأصول القيمة وضمان استمرارية الأعمال في العصر الرقمي اليوم.