SKILLSLAB
Training Provider

كتيب الدورة

ضوابط الأمن السيبراني وإدارة المخاطر– متقدمة لحماية المعلومات والحوكمة وإدارة التهديدات الرقمية استراتيجيات

Professional Training Course

Skillslab Training Provider
Skills for Tomorrow's World

info@skillslab-training.com | +966 55 965 3447 | www.skillslab-training.com

وصف الدورة

المقدمة

لتنفيذ عملياتها الأساسية على التقنيات المترابطة والمنصات السحابية والخدمات تعتمد المؤسسات بصورة متزايدة المتنامي على التكنولوجيا إلى زيادة التعرض وتقديم خدماتها بكفاءة. ويؤدي هذا الاعتماد الرقمية وأنظمة المعلومات وتوفر ضوابط الخدمات أو اختراق المعلومات الحساسة أو إلحاق للتهديدات السيبرانية التي قد تتسبب في تعطيل التهديدات وحماية الأصول الأمن السيبراني وإدارة المخاطر منهجية منظمة خسائر مالية وأضرار بالسمعة المؤسسية. المبادئ والأطر والتقنيات العملية اللازمة لإنشاء المعلوماتية الحيوية. يقدم هذا البرنامج التدريبي لتحديد الثغرات وتقييم والمتطلبات المخاطر. كما يستعرض العلاقة بين حوكمة أمن منظومة متكاملة لإدارة الأمن السيبراني قائمة على تقييم التهديدات السيبرانية التنظيمية والأهداف الاستراتيجية للمؤسسات. ويتعرف المعلومات ومستويات تقبل المخاطر التقنية والإدارية والمادية المناسبة. ويتناول واكتشاف نقاط الضعف الأمنية واختيار الضوابط المشاركون على أساليب العملية كيفية إعداد الأمنية وإدارة الحوادث ومراقبة الأداء الأمني البرنامج تقييم المخاطر السيبرانية وتنفيذ الضوابط الإدارة بمستويات التعرض سجلات المخاطر وتقييم الضوابط الأمنية وتطوير خطط بصورة مستمرة. وتوضح التطبيقات التطبيقية يطور المشاركون قدراتهم على إدارة للتهديدات. ومن خلال التعلم المنظم ودراسات الحالة المعالجة وإبلاغ أهداف الدورة المخاطر السيبرانية بصورة استباقية وتحسين مستوى

سيتمكن المشاركون من تحقيق النضج الأمني داخل مؤسساتهم.

فهم المبادئ الأساسية الأهداف التالية بنهاية هذه الدورة التدريبية

- تطبيق الأطر والمعايير المعلومات والأصول الرقمية لإدارة المخاطر السيبرانية وأهميتها في حماية التدريبية:
- تحديد الدولية للأمن السيبراني وممارسات الحوكمة الأمنية المؤسسية.
- منظمة المحتملة التي تؤثر على العمليات التهديدات الإلكترونية والثغرات الأمنية والمخاطر في البيئات المؤسسية.

إجراء تقييمات

- تصميم وتنفيذ الضوابط للمخاطر السيبرانية باستخدام أساليب التحليل النوعي التشغيلية.
- تقييم فعالية الأمنية الوقائية والكاشفة والتصحيحية وفقاً والكمي.
- إعداد سجلات ضوابط أمن المعلومات وتحديد فرص التحسين وتعزيز لأولويات المخاطر.
- تعزيز إدارة الهوية المخاطر السيبرانية وخطط المعالجة ومؤشرات قياس مستويات الحماية.

- تطوير إجراءات وصلاحيات الوصول وحماية البيانات وإدارة مخاطر الأداء الأمني.
- تحسين التواصل فعالة للاستجابة للحوادث واستمرارية الأعمال وتعزيز الأطراف الخارجية.
- الفئة بشأن المخاطر السيبرانية ودعم التحسين المستمر المرونة السيبرانية.

يستهدف هذا البرنامج التدريبي لقدرات الأمن المؤسسي.

مديرو الأمن السيبراني المهنيين الراغبين في تطوير معارفهم المستهدفة

- مسؤولو أمن المسؤولون عن حماية الأنظمة والشبكات والمعلومات ومهاراتهم:
- مديرو المعلومات المشرفون على الحوكمة الأمنية والامتثال الحساسة داخل المؤسسات.
- المعلومات الإلكترونية ومستويات التعرض المخاطر والمحللون المعنيون بتقييم التهديدات وإدارة المخاطر السيبرانية.

مديرو تقنية

- المدققون المسؤولون عن أمن البنية التحتية والأنظمة السحابية للمخاطر.
- والامتثال وممارسات إدارة المخاطر والامتثال الداخليون المكلفون بتقييم الضوابط الأمنية والمرونة التشغيلية.

مسؤولو الحوكمة

- مديرو استمرارية الأعمال المشاركون في تطوير السياسات والأطر التنظيمية لأمن التنظيمي.
- مديرو المشاريع المسؤولون عن الاستعداد للحوادث السيبرانية المعلومات.
- القيادات التنفيذية الرقمية المعنيون بمتطلبات الأمن السيبراني وحماية والتعافي منها.
- المستشارون المشرفة على الاستثمارات الأمنية والمخاطر التقنية المعلومات.
- المحتوى والمتخصصون في تطوير النضج الأمني وتحسين ضوابط الاستراتيجية.

فهم مبادئ الأمن السيبراني السيبراني والحوكمة وأطر إدارة التدريبياليوم الأول: أساسيات الأمن الحماية المؤسسية.

- استعراض مشهد التهديدات وأهدافه ومسؤوليات حماية المعلومات المخاطر
- تحديد الأصول المعلوماتية السيبرانية المتطور والتحديات الأمنية المؤسسية.
- التعرف على الأطر الحيوية والعمليات التشغيلية التي تتطلب الناشئة.
- فهم هياكل الحوكمة والمعايير الدولية لإدارة الأمن السيبراني الحماية.
- تحديد شهية المخاطر الأمنية والسياسات وآليات المساءلة والمخاطر.
- توزيع الأدوار والمسؤوليات السيبرانية ومستويات تحملها ومعايير المؤسسية.
- دمج حوكمة الأمن المتعلقة بإدارة المخاطر والأمن قبولها.
- تطوير السياسات السيبراني مع إدارة المخاطر المؤسسية والأهداف السيبراني.
- تمرين عملي لإنشاء إطار والإجراءات والوثائق المنظمة لإدارة أمن الاستراتيجية.

- اليوم الثاني: تحديد متكامل لحوكمة الأمن السيبراني وإدارة المعلومات.

تحديد مصادر المخاطر السيبرانية وتقييم التهديدات وإدارة المخاطر.

- فهم أساليب الهجمات التهديدات السيبرانية الداخلية والخارجية التي الثغرات الأمنية
- تقييم الثغرات الأمنية في الإلكترونية الشائعة وتأثيراتها المحتملة على تواجه المؤسسات.
- إعداد قوائم الأصول الشبكات والتطبيقات والأجهزة والبيئات الأعمال.
- تطبيق منهجيات منظمة المعلوماتية وتحديد الاعتماديات الأمنية السحابية.
- تحليل احتمالية التهديدات لتحديد المخاطر السيبرانية الحيوية.
- استخدام مصفوفات المخاطر وشدة الثغرات وحجم التأثير على وتقييمها.
- إعداد سجلات شاملة لتصنيف التهديدات وتحديد أولويات الأعمال.
- تقييم مخاطر الأمن السيبراني للمخاطر السيبرانية وتحديثها بصورة المعالجة.
- ورشة تطبيقية لإجراء المرتبطة بالموردين والأطراف دورية.
- اليوم الثالث: تصميم تقييم متكامل للمخاطر السيبرانية في بيئة الخارجية.

فهم الضوابط الأمنية الضوابط الأمنية وتنفيذها وتقييم مؤسسية.

- تصميم ضوابط أمنية الوقائية والكاشفة والتصحيحية فعاليتها
- تطبيق مبادئ إدارة الهوية تقنية وإدارية ومادية قائمة على تقييم والتعويضية.
- تعزيز آليات المصادقة وصلاحيات الوصول والحد الأدنى من المخاطر.
- تنفيذ ضوابط أمن الشبكات والتحقق من الهوية وإدارة الصلاحيات الامتيازات.
- تطبيق تصنيف البيانات وإجراءات التهيئة الآمنة الحساسة.
- إدارة الثغرات الأمنية من والتشفير وضوابط حماية المعلومات للأنظمة.
- تقييم ضوابط الأمن السحابي خلال التحديثات والمعالجات والإصلاحات الحساسة.
- اختبار تصميم الضوابط ومتطلبات المسؤولية الدورية.
- تمرين عملي لإعداد الأمنية وفعاليتها التشغيلية ومدى الامتثال المشتركة.
- اليوم الرابع: معالجة مصفوفة الضوابط الأمنية وتقييم مستوى للمتطلبات.

تطوير استراتيجيات معالجة المخاطر السيبرانية والاستجابة للحوادث والمرونة فعاليتها.

- تطبيق أساليب تجنب المخاطر السيبرانية بما يتوافق مع الأولويات المؤسسية
- تقييم الاستثمارات الأمنية المخاطر وتخفيفها ونقلها المؤسسية.

- إنشاء إجراءات اكتشاف باستخدام تحليل خفض المخاطر والتكاليف وقبولها.
- تحديد الأدوار والمسؤوليات الحوادث الأمنية والإبلاغ عنها وتصعيدها والاستجابة والمنافع.
- إعداد خطط الاستجابة وآليات التواصل أثناء إدارة الحوادث لها.
- دمج إدارة المخاطر للحوادث الإلكترونية وإجراءات التعافي السيبرانية.
- تقييم الاستعداد لهجمات السيبرانية ضمن خطط استمرارية التشغيلي.
- إدارة المخاطر المتبقية الفدية وحماية النسخ الاحتياطية وقدرات الأعمال.
- ورشة تطبيقية لإعداد خطة وقياس فعالية إجراءات المعالجة الاستعادة.
- اليوم الخامس: المراقبة معالجة المخاطر السيبرانية والاستجابة الأمنية.

إنشاء عمليات مستمرة الأمنية والامتثال وإعداد التقارير والتحسين للحوادث.

- تطوير مؤشرات المخاطر لمراقبة المخاطر السيبرانية ومراجعة الضوابط المستمر
- مراقبة الأحداث الأمنية الرئيسية ومقاييس الأداء في الأمن الأمنية.
- تنفيذ تقييمات الضوابط والثغرات والتهديدات الإلكترونية السيبراني.
- تقييم الامتثال الأمنية وعمليات التدقيق الداخلي للأمن الناشئة.
- إعداد تقارير المخاطر للتشريعات واللوائح والمعايير الأمنية المعمول السيبراني.
- تطوير لوحات متابعة توضح السيبرانية للإدارة العليا ولجان بها.
- تقييم مستوى النضج الوضع الأمني ومستويات التعرض الحوكمة.
- إعداد خطط التحسين المستمر السيبراني المؤسسي وتحديد أولويات للمخاطر.
- تمرين ختامي لإعداد وعرض وبرامج التوعية بالأمن التحسين.
- مدة الدورة استراتيجية متكاملة للضوابط الأمنية وإدارة المخاطر السيبراني.

يُنفذ هذا البرنامج التدريبي على السيبرانية.

يومياً، وبإجمالي خمس وعشرين ساعة تدريبية. يجمع مدار خمسة أيام متتالية، بواقع خمس ساعات تدريبية التدريبية ودراسات الحالة الواقعية. التطبيقية وتمارين تقييم المخاطر السيبرانية البرنامج بين المحاضرات التفاعلية وورش العمل وأطر الحوكمة وخطط الاستجابة ويعمل المشاركون على إعداد سجلات المخاطر ومصفوفات والمناقشات الجماعية برامج تدريبية داخلية مخصصة وفقاً لاحتياجات للحوادث. ويمكن تقديم البرنامج حضورياً أو عن بُعد تقييم الضوابط الأمنية يقدم المؤسسات ومستويات الخبرة المهنية أو ضمن

معلومات المدرب

وتعزيز واستشارية واسعة في حوكمة الأمن السيبراني وإدارة البرنامج خبير معتمد دولياً يتمتع بخبرة عملية للمشاركين.

استراتيجيات معالجة المرونة المؤسسية. يمتلك المدرب خبرة تطبيقية في أمن المعلومات وتقييم المخاطر الإلكترونية

وتطبيق الأطر والمعايير الدولية لأمن المخاطر والامتثال الأمني والتخطيط للاستجابة تصميم الضوابط الأمنية وتطوير

على تحويل المهنية ودراسات الحالة الواقعية والتمارين المعلومات. ويركز أسلوب التدريب على المنهجيات للحوادث

لإدارة المخاطر داخل المعارف المكتسبة إلى ضوابط أمنية فعالة وممارسات التطبيقية بما يضمن قدرة المشاركين

ما الهدف الرئيسي من دورة مؤسساتهم.الأسئلة متقدمة

1. وتعزيز إلى تطوير المهارات العملية لتحديد المخاطر ضوابط الأمن السيبراني وإدارة المخاطر؟ تهدف الدورة الشائعة
   هل الدورة مناسبة للمهنيين قدرة المؤسسات على مواجهة التهديدات السيبرانية وتطبيق الضوابط الأمنية الفعالة
2. وتحليل السيبراني؟ نعم، يبدأ البرنامج بالمفاهيم الأساسية الذين لا يمتلكون خبرة تقنية متقدمة في الأمن الرقمية.
   ما الأطر والمعايير الضوابط وتطبيقات إدارة الأمن ثم ينتقل تدريجياً إلى تقييم المخاطر
3. الدولية إطار الأمن السيبراني الصادر عن المعهد الوطني الأمنية التي يتناولها البرنامج؟ يستعرض البرنامج السيبراني.
   هل تتضمن الدورة تمارين لإدارة أمن المعلومات وإدارة مخاطر أمن الأمريكي للمعايير والتكنولوجيا والمواصفات
4. التطبيقات إعداد سجلات المخاطر وتقييم الضوابط عملية لتقييم المخاطر السيبرانية؟ نعم، تشمل المعلومات.
   ما المؤسسات الأمنية وتطوير خطط المعالجة وتحليل سيناريوهات
5. الجهات الحكومية والمؤسسات المالية وشركات التي يمكن أن تستفيد من هذا البرنامج؟ يناسب الاستجابة للحوادث.
   تمثل ضوابط معلومات رقمية الطاقة ومزودي الخدمات التقنية والمؤسسات التي تدير البرنامج

الخاتمة

حماية الأصول المعلوماتية وضمان استمرارية العمليات الأمن السيبراني وإدارة المخاطر عنصراً أساسياً في حساسة.

تساعد المهنيين على تحديد المتطورة. يوفر هذا البرنامج التدريبي منهجيات وتعزيز المرونة المؤسسية في البيئات الرقمية

الضوابط الأمنية المناسبة. ويطور المشاركون قدراتهم التهديدات السيبرانية وتقييم الثغرات وتنفيذ منظمة وأدوات عملية

والاستجابة المعالجة الفعالة ودعم الامتثال والحوكمة الأمنية. على تقييم المخاطر الإلكترونية وإعداد استراتيجيات

للأمن السيبراني. ومن خلال تطبيق للحوادث والتواصل واتخاذ القرارات اللازمة للإدارة كما يعزز البرنامج مهارات المراقبة

مستويات التعرض للمخاطر وتحسين الأداء الأمني المعارف والتقنيات المكتسبة تستطيع المؤسسات تقليل الاستباقية

الاستدامة التشغيلية. وتعزيز قدرتها على مواجهة التهديدات وتحقيق

تواصل معنا

الأسعار الجماعية، يُرجى التواصل معنا: للاستفسار عن التسجيل أو المواعيد القادمة أو

الموقع الإلكتروني www.skillslab-training.com

البريد الإلكتروني info@skillslab-training.com

واتساب +966 559 653 447

Generated by Skillslab Training

info@skillslab-training.com | واتساب: +966 559 653 447

www.skillslab-training.com