

كتيب الدورة

المؤسسية والتعافي وتعزيز المرونة الرقمية الاستجابة

Professional Training Course

Skillslab Training Provider

Skills for Tomorrow's World 



وصف الدورة

المقدمة

المؤسسات على الاستعداد للحوادث السيبرانية السيبراني برنامجًا تدريبًا مهنيًا متقدمًا طمّم يُعد برنامج إدارة أزمات الأمن القرار في البرنامج القيادات التنفيذية وقادة الأمن السيبراني عالية التأثير وإدارتها والتعافي منها بكفاءة. يزود لمساعدة للاستجابة الفعالة لهجمات القطاع العام بالقدرات الاستراتيجية والفنية ومتخصصي المخاطر ومديري العمليات وصناع الداخلية وهجمات سلاسل الإمداد وغيرها برمجيات الفدية واختراقات البيانات وتعطل الخدمات والحوكمة اللازمة تتمثل القيمة والتهديدات من نشاط فني محدود إلى قدرة مؤسسية التنفيذة للبرنامج في تحويل الاستجابة للحوادث من حالات الطوارئ الرقمية. والوفاء حماية العمليات الحرجة واتخاذ القرارات في الوقت متكاملة لإدارة الأزمات. ويتعلم المشاركون كيفية السيبرانية والقانونية والتشغيلية بالالتزامات التنظيمية واستعادة الخدمات الأساسية المناسب والمحافظة على ثقة المعنيين من خلال المحاكاة الواقعية مع الحد من الأضرار المالية التنفيذ، يدرس المشاركون هياكل قيادة الحوادث وسيناريوهات الأزمات وتمارين اتخاذ القرار وورش والسمعة المؤسسية. ومخاطر الأطراف التحقيقات الرقمية واستمرارية الأعمال والاتصال السيبرانية وبروتوكولات الاستجابة التنفيذية وتنسيق بصورة خاصة للجهات الحكومية الخارجية وتخطيط التعافي والتحسين بعد الحوادث. أثناء الأزمات والإبلاغ التنظيمي الحرجة والشركات الكبرى الساعية إلى تعزيز والوزارات ومؤسسات القطاع العام ومشغلي البنى ويُعد البرنامج مناسبًا بنهاية المرونة السيبرانية والجاهزية التحية أهداف الدورة

فهم الأبعاد برنامج إدارة أزمات الأمن السيبراني، سيتمكن المؤسسية.

- التمييز بين الحوادث المرتبطة بالأزمات الاستراتيجية والتشغيلية والقانونية والسمعة المشاركون من:
- إنشاء حوكمة فعالة للأزمات السيبرانية وحالات الطوارئ المؤسسية السيبرانية.
- تحديد الكبرى.
- تنسيق جهود الأمن الأدوار والمسؤوليات وحدود التصعيد وصلاحيات القرار وهياكل واضحة لقيادة الحوادث.
- تقييم أثر برمجيات والتقنية والقانون والمخاطر والاتصال التنفيذي.
- اتخاذ قرارات قائمة على الفدية والاختراقات والتعطل وفقدان والعمليات.

- تطوير استراتيجيات فعالة الأدلة في ظل الغموض والضغط البيانات.
- دمج الاستجابة للحوادث للاتصال الداخلي والخارجي والتنظيمي الزمني.
- إدارة اعتماديات الموردين مع استمرارية الأعمال والتعافي من والإعلامي.
- إجراء مراجعات منظمة بعد والأطراف الخارجية والبنية التحتية الكوارث.
- إعداد خارطة عملية لإدارة الحوادث وتحديد فرص تحسين الحرجة.
- محتوى الدورة اليوم الأزمات السيبرانية والاستجابة المرونة.

فهم طبيعة الأزمات الأول: حوكمة الأزمات السيبرانية والاستعداد لها.

- التمييز المؤسسي
- تحديد التهديدات بين الحوادث والطوارئ والاضطرابات والأزمات السيبرانية ومراحل تطورها.
- تعريف حوكمة الأزمات السيبرانية الرئيسية وسيناريوهات المؤسسية.
- إنشاء هياكل أثرها.
- توزيع والمسائلة التنفيذية.
- وضع حدود التصعيد ومعايير المسؤوليات بين الفرق الفنية وغير القيادة والتوجيه والتنسيق.
- تقييم الجاهزية الفنية.
- تطوير السياسات والخطط المؤسسية ومستوى النضج في تفعيل الأزمة.
- مواومة المرونة.
- اليوم الثاني: قيادة الاستجابة السيبرانية مع إدارة المخاطر وإجراءات الاستجابة.
- إنشاء إطار لقيادة الحوادث الحوادث وصنع القرار والتنسيق المؤسسية.
- إدارة المعلومات التشغيلي
- ترتيب حماية الأفراد الناقصة والمتعارضة والمتغيرة والسيطرة عليها.
- تنسيق فرق الأمن والتقنية والخدمات والأنظمة والبيانات بسرعة.
- إعداد والأصول.
- إدارة اجتماعات الأزمة تقارير الموقف والإحاطات والقانون والمخاطر والأعمال.
- تقييم التنفيذية.
- المحافظة على سلامة قرارات الاحتواء والعزل والإيقاف ومتابعة الإجراءات والمسائلة.
- التنسيق مع جهات إنفاذ الأدلة ودعم التحقيقات والاستمرارية.
- إدارة الرقمية.

- اليوم الثالث: برمجيات الحوادث الممتدة وإجهاد فرق القانون والخبراء الخارجيين.

فهم أنماط هجمات برمجيات الفدية واختراق البيانات وتعطل القيادة.

- تقييم الخدمات

- دراسة الخيارات القانونية سيناريوهات التشفير وسرقة البيانات والابتزاز الفدية وأثرها المؤسسي.

- إدارة اكتشاف اختراق والأخلاقية والمالية والتشغيلية والتعطّل.

- تحديد نطاق الأنظمة والمعلومات البيانات واحتوائه والإبلاغ للاستجابة.

- حماية الخدمات عنه.

- تقييم موثوقية النسخ والدرجة والمحافظة على العمليات الحساسة المتضررة.

- تنسيق التحقيقات الاحتياطية وأولويات الأساسية.

- إدارة الاستعادة.

- معالجة الحوادث المرتبطة التهديدات الداخلية واختراق الحسابات ذات والتعافي واستمرارية الأعمال.

- اليوم الصلاحيات.

تطوير اتصال داخلي واضح الرابع: الاتصال أثناء الأزمات وإدارة المعنيين بالموردين وسلاسل الإمداد.

- إحاطة والامتثال

- التواصل مع العملاء القيادات والمجالس والجهات التنظيمية خلال الأزمة السيبرانية.

- إدارة الاهتمام الإعلامي والمواطنين والشركاء والموظفين.

- تجنب التكهّنات والتناقض والبيانات العامة ومخاطر والموردين.

- مواجهة الاتصال مع السمعة.

- إعداد رسائل الإخطار المتطلبات القانونية والإفصاح المبكر.

- إدارة والتنظيمية.

- المحافظة على ثقة المعنيين المعلومات المضللة والشائعات وضغوط المنصات للجهات والأفراد المتأثرين.

- توثيق الرقمية.

- اليوم الخامس: التعافي القرارات والاعتمادات والاتصالات والإجراءات خلال فترات التعطل الممتدة.

تحديد التنظيمية.

- التحقق من سلامة الأنظمة أولويات الاستعادة الأمانة للأنظمة والمرونة ومحاكاة الأزمات

- إدارة التعافي المرحلي والبيانات والصلاحيات والخدمات.

- مراقبة والضوابط.
- إجراء مراجعات منظمة إعادة الاختراق والاستمرارية والهجمات وقرارات العودة إلى التشغيل.
- تحديد الثانوية.
- تحديث الخطط والسياسات إخفاقات الضوابط وفجوات العمليات ونقاط واستخلاص الدروس المستفادة.
- قياس الضعف.
- تنفيذ محاكاة تنفيذية المرونة السيبرانية وأداء إدارة والتدريب والضوابط التقنية.
- إعداد الأزمات.
- الفئة خارطة تطوير للجاهزية والمرونة متكاملة لأزمة سيبرانية.

طعم برنامج إدارة أزمات الأمن المؤسسية.

القيادات المستهدفة

- قادة الأمن السيبراني التنفيذية المسؤولة عن المرونة المؤسسية والمخاطر السيبراني للفئات التالية:
 - رؤساء ومديرو الاستراتيجية.
 - مسؤولو الجهات وحماية المعلومات.
 - فرق الاستجابة الحكومية والوزارات المشرفون على الأمن الرقمي تقنية المعلومات.
 - مديرو المخاطر والحوكمة للحوادث ومراكز العمليات والاستمرارية.
 - متخصصو استمرارية الأمنية.
 - المتخصصون القانونيون الأعمال والتعافي من والامثال.
 - قادة الاتصال المؤسسي والتنظيميون وحماية الخصوصية الكوارث.
 - مديرو البنى والبيانات.
 - المدققون الداخليون التحية الحرجة والتقنيات والعلاقات العامة.
 - فرق إدارة الأزمات التشغيلية.
 - مسؤولو إدارة ومتخصصو الضمان.
 - المستشارون الداعمون الموردين ومخاطر الأطراف والاستجابة للطوارئ.
 - متطلبات للمرونة السيبرانية والاستجابة الخارجية.

لا تتطلب الدورة معرفة متقدمة للحوادث.

الأعمال للأمن السيبراني أو المخاطر المؤسسية أو تقنية البرمجة. ويُفضل أن يمتلك المشاركون فهمًا عامًا للدورة يُنصح المعلومات أو إدارة الأزمات أو استمرارية الأزمات أو ترتيبات استمرارية المشاركون بإحضار أمثلة عن خطط الاستجابة للحوادث أو الامتثال أو صنع القرار التنفيذي. السيبرانية لاستخدامها في بعض التمارين. كما يُنصح الأعمال أو إجراءات التصعيد أو سيناريوهات المخاطر أو هياكل إدارة تجمع السيناريوهات ورسم الاستجابة وإعداد رسائل الاتصال بإحضار جهاز حاسوب محمول لأنشطة التخطيط وتحليل منهجية التدريب

الأزمات والتخطيط العملي وصنع القرار التشاركي. وقد منهجية التدريب بين التعليم التنفيذي ومحاكاة وتخطيط التنفيذ. يتضمن والانضباط اللزمين لإدارة حالات الطوارئ طُفمت الدورة لمساعدة المشاركين على بناء الثقة

عروضًا متخصصة تستند إلى السيبرانية ضمن بيئات مؤسسية واقعية.

- دراسات حالات واقعية الممارسات الحديثة في الأمن البرنامج;
- سيناريوهات السيبراني.
- تمارين لاتخاذ القرارات للاستجابة لبرمجيات الفدية واختراقات لأزمات سيبرانية.
- ورشًا لقيادة البيانات.
- أنشطة التنفيذية تحت الضغط.
- تمارين لاستمرارية للاتصال أثناء الأزمات وإحاطة الحوادث والتنسيق بين الفرق.
- سيناريوهات المعنيين.
- محاكاة الأعمال وتخطيط التعافي.
- ورشًا لمراجعة الحوادث مكتوبة تشارك فيها فرق متعددة للإبلاغ التنظيمي والتوثيق.
- تخطيطًا فرديًا التخصصات.
- تمكن هذه المنهجية التطبيقية وتطوير الإجراءات.
- الفجوات وتطوير تحسينات عملية قابلة للتنفيذ داخل المشاركين من اختبار قدراتهم الحالية وتحديد ومؤسسيًا للتنفيذ. مخرجات

عند إتمام البرنامج بنجاح، سيتمكن مؤسساتهم.

التعرف على الحالات التعلم

- إنشاء ترتيبات فعالة التي تتطلب تفعيل إدارة الأزمة المشاركون من:

- إدارة المؤسسية.
- ترتيب احتياجات الخدمات القرارات السيرانية في ظل الغموض والضغط للقيادة والحوكمة والتنسيق.
- تنسيق الاستجابة الفنية والأنظمة والمعلومات التشغيلي.
- الاستجابة والمعنيين.
- التواصل بوضوح مع القيادات الفعالة لبرمجيات الفدية والاختراقات والتعطل مع الاستمرارية والتعافي.
- إدارة الجوانب القانونية والموظفين والجهات التنظيمية الرقمي.
- تقييم مخاطر الموردين والتنظيمية والخصوصية والجمهور.
- قيادة التعافي المنظم والأطراف الخارجية أثناء والسمعة.
- تعزيز الأزمات.
- إعداد خطة عملية لتنفيذ المرونة السيرانية والجاهزية والتحسين بعد الحوادث.
- ملف منظومة إدارة الأزمات المؤسسية.

يقدم البرنامج خبير معتمد دوليا السيرانية.

واستمرارية خبرة متقدمة في إدارة أزمات الأمن السيراني يتمتع بخبرة عملية واستشارية واسعة. يمتلك المدرب المدرب والاتصال أثناء الأزمات والحوكمة الأعمال والتعامل مع برمجيات الفدية وإدارة والاستجابة للحوادث والمخاطر الرقمية يعتمد اختراقات البيانات

الموجهة وتمارين اتخاذ القرار المدرب على دراسات الحالات الواقعية والمحاكاة والامثال التنظيمي والمرونة المؤسسية. مباشرة داخل مؤسساتهم. وتناسب منهجية وورش التنفيذ لضمان قدرة المشاركين على تطبيق التنفيذية والمناقشات ومتخصصي الأمن السيراني وقادة التقنية ومديري التقديم القيادات التنفيذية وممثلي الجهات الحكومية المعرفة المخاطر والمتخصصين القانونيين وفرق الأزمات متعددة

التخصصات.

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