

أمن السيبراني وإدارة المخاطر في العالم العربي

المدة: 5 يوم

اللغة: ar

كود الكورس: PI1-103

هدف الكورس

- لتكون قادرًا على تحديد مخاطر أمن السيبرانية في إدارة البيانات
- لتكون قادرًا على تطوير المهارات للتعرف على التهديدات ومكافحتها المتعلقة بأمن السيبرانية
- لتكون قادرًا على تعلم جميع مخاطر السيبرانية والقضايا والتهديدات
- لتكون قادرًا على وضع ضوابط فعالة وحلول لمواجهة التهديدات السيبرانية
- لتكون قادرًا على تطوير سياسات واتصالات تتناول حوكمة المعلومات والامتثال والمعايير وتتناول أيضًا متطلبات القانون والتدقيق
- لتكون واثقًا في توعية الأمان والتدريب الأمني
- لتكون قادرًا على تحسين استراتيجيات أمن السيبرانية الحالية، ومراجعة الأدوات بثقة ومناقشة الأمان والسرية وحلول الأعمال للحد من المخاطر التشغيلية
- لتكون قادرًا على تحسين المعرفة العملية والمعايير الصناعية العالمية وأفضل الممارسات في مجال أمن السيبرانية وإدارة مخاطر المعلومات
- لتكون قادرًا على تطبيق معايير ISO بما في ذلك إدارة السجلات بموجب ISO15489 وإدارة أمن المعلومات بموجب ISO 27001 للحد من التهديدات والمخاطر

الجمهور

- مهندسو التكنولوجيا
- مدير تكنولوجيا المعلومات
- مدير معلومات رئيسي
- مسؤولو مخاطر رئيسيون
- موظفو تطوير التطبيقات
- موظفو أبحاث البيانات
- المحترفون الراغبون في تعلم استراتيجيات الأمن السيبراني، وحكم المعلومات، ومعايير ISO
- أولئك الذين يعملون في إدارة أنظمة تكنولوجيا المعلومات، والقانون، وإدارة المخاطر، وأمن المعلومات، والمشاريع، والموارد البشرية، والمشتريات
- الراغبون في الانتقال إلى الأدوار الإدارية وأمن تكنولوجيا المعلومات

منهجية التدريب

يتم التدريس في مجموعة متنوعة من البيئات، بما في ذلك التعليم المباشر في الفصل الدراسي، لضمان تمكين المشاركين من توسيع معرفتهم بالموضوع وتعزيز مهاراتهم. تُقدم الدورة بطرق متنوعة من قبل مدرس متخصص، وتشمل هذه الطرق عروض باوربوينت، ومراجعة المقالات والمواد ذات الصلة، بالإضافة إلى تمارين ومناقشات جماعية أو فردية. قد يتم تحديد بعض الأعمال المستقلة، وستتطلب الدورة تقديم مقالات لإثبات الفهم واختبار نهاية الدورة. يُشجع على تدوين الملاحظات، ويمكنك استخدام الأجهزة الإلكترونية لهذا الغرض.

سيكون دليل الدورة جزءًا من عملية التعلم، ولكنه سيوفر لك مراجع للمستقبل. يُشجع على طرح الأسئلة، وإذا لزم الأمر، قضاء وقت فردي مع المدرس لمراجعة أي قضايا. خلال وقتك في الفصل، ستتمكن من التواصل مع زملاء في أدوار مماثلة.

الملخص

تستمر العصر الرقمي في التطور بوتيرة مذهلة. وهذا يعني أن جميع المؤسسات الآن تستخدم التكنولوجيا التي تأتي بثمن. هناك زيادة في مخاطر الهجمات السيبرانية التي تسرق المعلومات والحاجة للامتثال للتشريعات القانونية والتدقيقات وقضايا الامتثال الأخرى. إذا كنت تعمل في هذا المجال، سيقدم لك هذا الدورة كل ما تحتاج إلى معرفته حول حماية البيانات وأمن السيبران. سيتم مناقشة طرق لتقليل المخاطر داخل المؤسسة ومناقشة امتثال جميع المعايير العالمية. ستتضمن معلومات حول كيفية حماية خصوصية المستخدم النهائي والعمل ضمن إطارات تنظيم ISO لإدارة أمن المعلومات.

تتبع الدورة أحدث الممارسات الجيدة وتعرض لك جميع المهارات المطلوبة لإدارة المعلومات، وضمان التزام التشريعات

القانونية والمعايير وتنفيذ ضوابط التدقيق. ستتعلم أيضًا كيفية البقاء آمنًا عند العمل عبر الإنترنت وكيف يمكنك حماية معلوماتك الشخصية والحساسة. هذا أمر ضروري لأولئك المسؤولين عن التخفيف من مخاطر الجرائم السيبرانية ويساعدك على فهم التأثيرات الكارثية للفشل في حماية مؤسستك بشكل صحيح. جميع الشركات التي تعتمد على البيانات بحاجة على الأقل إلى خبير واحد في فريقها. تغطي الدورة جميع عناصر دورة حياة البيانات وتساعدك في تحديد تهديدات أمن السيبران. بدوره، ستتعلم كيفية إحداث ضوابط ستساعد في تقليل هذا الخطر والخطر على شكل سياسات واستراتيجيات وأنظمة. بالإضافة إلى ذلك، يجب عليك أن تكون على علم بمتطلبات معايير ISO للامتثال والتدقيق القانوني. تغطي الدورة أيضًا التقنيات الجديدة مثل الذكاء الاصطناعي، والإنترنت من الأشياء، والحوسبة السحابية والبلوكتشين حيث من الضروري أن تفهم كل من الفوائد والمخاطر.

محتوى الكورس والمخطط الزمني

القسم 1: مقدمة في الأمن السيبراني وأمن المعلومات

- مقدمة في الأمن السيبراني
- ما هي التهديدات والمخاطر والقضايا عبر الإنترنت؟
- استمرارية الأعمال، الاحتيال وإدارة الكوارث
- المعيار ISO27001 والمعايير ذات الصلة
- حوكمة البيانات والمعلومات والسجلات
- تحديد الأدوار والمسؤوليات لحوكمة المعلومات

القسم 2: متطلبات التدقيق، الجوانب القانونية، الوعي بالمخاطر وISO

- فهم وتصنيف المخاطر المادية والإلكترونية
- إدارة الامتثال: مخاطر التدقيق والقانونية
- إدارة الامتثال: الوثائق والسجلات
- مراجعة إدارة السجلات ISO15489
- كيفية تطبيق ضوابط أمن المعلومات ISO27001
- كيفية تطوير السياسات والإجراءات والمعايير
- نظرة على تحليل التهديدات والاتجاهات الحالية

القسم 3: التنفيذ والتدريب على التقنيات الجديدة

- ما هو مؤشر المخاطر الرئيسي (KRI)
- خطط تنفيذ المشاريع والضوابط
- تطوير خطط إدارة المخاطر والقضايا
- تطوير خطة استمرارية الأعمال
- إدارة حوادث الأمن السيبراني

- إدارة الأزمات السيبرانية

القسم 4: تطبيقات تكنولوجيا المعلومات: الأمن والسلامة

- بروتوكولات الشبكة/الاتصالات/الوصول
- أمن الجدار الناري/التطبيقات/الشبكة
- إدارة المستخدمين، بما في ذلك ضوابط الوصول المعتمدة على الأدوار
- تقنيات ومعايير التشفير
- أمن البريد الإلكتروني/الويب
- أنظمة الأمن السيبراني

القسم 5: السحابة، إنترنت الأشياء والبلوك تشين: الاتجاهات الجديدة في الأمن السيبراني

- الحوسبة السحابية، بما في ذلك العامة والخاصة والهجينة
- تقنية البلوك تشين
- ما هو الاختراق
- الرياضيات في الاختراق
- الثغرات في الأنظمة: التتبع والوقاية

تفاصيل الشهادة

عند إتمام هذه الدورة التدريبية بنجاح، سيحصل المشاركون على شهادة إتمام التدريب من Holistique Training. وبالنسبة للذين يحضرون ويكملون الدورة التدريبية عبر الإنترنت، سيتم تزويدهم بشهادة إلكترونية (e-Certificate) من Holistique Training.

شهادات Holistique Training وخدمة اعتماد التطوير المهني (BAC) معتمدة من المجلس البريطاني للتقييم المستمر (CPD)، كما أنها معتمدة وفق معايير ISO 9001 وISO 21001 وISO 29993.

لهذه الدورة من خلال شهاداتنا، وستظهر هذه النقاط على شهادة إتمام (CPD) يتم منح نقاط التطوير المهني المستمر واحدة عن كل ساعة CPD يتم منح نقطة، CPD ووفقًا لمعايير خدمة اعتماد Holistique Training. التدريب من لأي دورة واحدة نقدمها حاليًا CPD حضور في الدورة. ويمكن المطالبة بحد أقصى قدره 50 نقطة.

التصنيفات

تطبيقات تكنولوجيا المعلومات والكمبيوتر, الذكاء الاصطناعي وإدارة البيانات, التكنولوجيا

مقالات ذات صلة



Navigating Cyber Threats: A Full Guide to Risk Management

In the digital era, cybersecurity risk management is paramount. This blog post delves into the process of identifying, assessing, and mitigating cyber risks. Learn about AI-driven .solutions, UK laws, and how to integrate risk management with your business objectives

YouTube Video

https://www.youtube.com/embed/RCd9Q42fT3E?si=hC7KTNVVH6wrri1u