

أمان المعلومات والتدقيق ـ كل ما تحتاج إلى معرفته في مجال السيبرانية

المدة: 5 يوم

اللغة: ar

كود الكورس: PI1-120

هدف الكورس

:عند إتمام هذه الدورة، سيكون المشاركون قادرين على

- فهم أهمية الأمن السيبراني داخل المؤسسة.
- استكشاف مزايا الأمن السيبراني الفعّال وتبعات الأمن السيبراني الضعيف.
- مراجعة المواصفات التقنية للأمن السيبراني.
- تنفيذ إدارة أمن المعلومات.
- تحليل بنية الشبكة وأنظمة كشف التسلل.
- إجراء تقييم للمخاطر ووضع خطط لإدارة المخاطر.
- تحديد أساليب تقييم المخاطر.
- الإلمام بمعايير ISO 27001 وCOBITS.
- تقييم النهج المتبع لإدارة الأزمات واستعادة التعافي من الكوارث.
- مراعاة القوانين واللوائح المحلية والإقليمية المتعلقة بالأمن السيبراني.
- مراجعة تكوينات IPv4 وIPv6 والمخاطر المرتبطة بها.

الجمهور

تم تصميم هذه الدورة لأي شخص مسؤول عن الأمن السيبراني وإدارة المخاطر داخل المؤسسة. ستكون مفيدة بشكل خاص لـ:

- مديري المخاطر
- مدققي المخاطر
- مديري المشاريع
- موظفي تقنية المعلومات
- محللي النظم
- مهندسي التكنولوجيا
- مهندسي النظم
- أخصائيي الاتصالات

منهجية التدريب

يستخدم هذا الدورة مجموعة متنوعة من أساليب التعلم للكبار لتعزيز الفهم والاستيعاب الكامل. سيقوم المشاركون بمراجعة أمثلة حقيقية لتدقيق الأمن السيبراني لتسليط الضوء على التفاصيل الرئيسية التي تجعل التدقيق فعالاً.
من خلال الجمع بين العروض التقديمية والمناقشات والعروض العملية، سيطور المشاركون فهماً شاملاً للمفاهيم والمبادئ والمهارات المتعلقة بتدقيق الأمن السيبراني وإدارة المخاطر. سيتم منحهم لاحقاً الفرصة لإنشاء عمليات تدقيق خاصة بهم تتعلق بأدوارهم، وتزويدهم بالمعدات والبرامج المثالية للقيام بذلك.

الملخص

في العصر الحديث، تتطور التكنولوجيا بسرعة هائلة. ومع ذلك، تصاحب التكنولوجيا الجديدة مخاطر جديدة. يجب على أي مؤسسة تستخدم التكنولوجيا بأي شكل أن تكون واعية للأمن السيبراني وأن تمتلك خططاً لإدارة المخاطر لضمان سلامة النظام.

الأمن السيبراني هو عملية حماية المعلومات التنظيمية ويشمل جميع الجوانب الرقمية، بما في ذلك الشؤون المالية ومعلومات العملاء. قد تكون التهديدات السيبرانية طفيفة وفي معظم الأحيان مجرد إزعاج. ومع ذلك، توجد تهديدات كبيرة يمكن أن تعطل وظائف الأعمال بشكل كامل، مما يؤدي إلى خسارة الأصول والعملاء والسمعة. الحفاظ على إدارة مخاطر فعالة يقلل من احتمالية حدوث المخاطر ويسمح للمؤسسة بأن تكون مستعدة بشكل أفضل في حال وقوعها.

لكي يكون الأمن السيبراني فعالاً، يجب إجراء تدقيقات للأمن السيبراني. ستقوم هذه التدقيقات بتفصيل التقنيات نفسها، والتهديدات المحتملة، والإجراءات الوقائية. يمكن استخدام أطر عمل متعددة كإرشادات لهذه التدقيقات لضمان تغطية جميع المجالات الأساسية.

إن وضع خطط لإدارة المخاطر والأزمات بناءً على المعلومات التي تم جمعها في تدقيقات الأمن السيبراني أمر بالغ الأهمية لضمان استمرارية الأعمال بشكل آمن. في منع المخاطر والسيناريوهات التي تحدث فيها المخاطر، يجب أن تركز الخطط على استمرارية الأعمال وطرق استعادة الخسائر بأمان.

محتوى الكورس والمخطط الزمني

Section 1: IT Security Evolution

- Defining cybersecurity.
- Categorising physical and electronic risk within an organisation.
- Understanding the different communication technologies impacted by identified risks.
- Evaluating computer system designs and how cybersecurity fits within them.
- Reviewing laws and regulations that influence cybersecurity.
- Assess current threats and conduct trend analysis.

Section 2: Risk and Crisis Management

- IPv4 to IPv6 configurations in relation to risk.
- Domain Name System Security Extensions (DNSSEC).
- Identifying what must be involved in crisis and risk management.
- Methods of evaluating risk.
- Creating detailed risk and crisis management plans to be clearly understood by all necessary personnel.

- Forensic and Electronic Investigations.
- Focusing on business continuity.

Section 3: Cybersecurity Audit Preparation

- Utilising the NIST Cybersecurity Framework to prioritise risks.
- Establishing policy requirements for when cyber incidents occur.
- Understanding the elements of the COBIT 5 framework.
- Creating audit plans aligned with both NIST and COBIT 5 frameworks.

Section 4: Executing Cybersecurity Audits

- Reviewing the bowtie method.
- Using the bowtie for continuous risk management.
- Conducting cybersecurity audits using AuditXP software.
- Creating audit questionnaires in AuditXP aligned with NIST and COBIT 5 frameworks.
- Maintaining detailed records of completed audits.
- Integrating audit results with known information to update risk management plans.

Section 5: Cybersecurity Management

- Forming a team of competent individuals.
- Evaluating audits and utilising NIST to prioritise risks.
- Communicating with the team and delegating tasks effectively.
- Creating action plans detailing cybersecurity intentions.
- Implementing changes.
- Continuously monitoring cybersecurity and working for system improvement.

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 معتمدة من المجلس البريطاني للتقييم وخدمة اعتماد التطوير المهني (BAC)

ISO 29993.و ISO 21001و ISO 9001 كما أنها معتمدة وفق معايير ،(CPD) المستمر

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

الذكاء الاصطناعي وإدارة البيانات, تطبيقات تكنولوجيا المعلومات والكمبيوتر, التكنولوجيا, المالية والمحاسبة

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/G-48k90DvaM?si=ASUXct8oU0j3Fufi