

"كيف تصبح خبيرًا في قيادة أمن المعلومات المتقدمة: الدورة الاحترافية في السيبرانية"

المدة: 5 يوم

اللغة: ar

كود الكورس: PI1 - 132

هدف الكورس

عند إتمام هذه الدورة، سيكون المشاركون قادرين على:

- تطوير فهم عميق لمبادئ الأمن السيبراني وأفضل الممارسات.
- إتقان استراتيجيات إدارة المخاطر والتخفيف منها.
- التعامل مع تعقيدات الامتثال القانوني والتنظيمي.
- تصميم وتنفيذ برامج أمنية شاملة.
- تعزيز قدرات الاستجابة للحوادث والتعافي منها.
- التحضير لامتحان شهادة CISSP.

الجمهور

تستهدف هذه الدورة:

- المتخصصين البارزين في مجال تكنولوجيا المعلومات والأمن السيبراني.
- كبار مسؤولي أمن المعلومات (CISOs).
- استشاريي ومديري أمن تكنولوجيا المعلومات.
- مهندسي أمن الشبكات.
- محللي ضمان المعلومات.

منهجية التدريب

تستخدم هذه الدورة مجموعة متنوعة من أساليب التعلم للكبار لتعزيز الفهم والاستيعاب الكامل، بما في ذلك:

- محاضرات تفاعلية ومناقشات.
- دراسات حالة واقعية وأمثلة.
- مشاريع جماعية وتمارين تعاونية.
- تدريب عملي باستخدام أدوات وأطر عمل الأمن السيبراني.

الملخص

يُزوِّد هذا البرنامج الشامل المشاركين بالخبرات اللازمة لقيادة وإدارة مبادرات الأمن السيبراني داخل المؤسسات. مع التركيز على الجوانب الاستراتيجية والعملية، يغطي البرنامج إدارة المخاطر، والامتثال القانوني والتنظيمي، والاستجابة

للحوادث. من خلال جلسات تفاعلية، ودراسات حالة، وتمارين عملية، سيطور المشاركون المهارات اللازمة لتصميم أطر أمنية قوية، وضمان حماية البيانات، والاستجابة بفعالية للتهديدات السيبرانية.

محتوى الكورس والمخطط الزمني

Section 1: Introduction to Cybersecurity and Leadership

- Overview of the cybersecurity landscape
- Leadership roles in cybersecurity
- Case studies on cybersecurity breaches and responses

Section 2: Risk Management and Governance

- Principles of risk management
- Developing and implementing security policies
- Legal, regulatory, and compliance frameworks

Section 3: Security Architecture and Engineering

- Designing secure systems and networks
- Security models and frameworks
- Secure software development practices

Section 4: Identity and Access Management

- Authentication and authorisation methods
- Identity lifecycle management
- Implementing access control measures

Section 5: Security Operations and Incident Management

- Monitoring and detecting security incidents

- Incident response planning and execution
- Business continuity and disaster recovery

Section 6: Exam Preparation and Review

- Review of key CISSP domains
- Mock exams and practice questions
- Exam strategies and tips

تفاصيل الشهادة

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

شهادات Holistique Training معتمدة من المجلس البريطاني للتقييم (BAC) وخدمة اعتماد التطوير المهني (CPD)، المستمر 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, التكنولوجيا, الاتصالات

مقالات ذات صلة



Top 10 Cybersecurity Courses And Training Programs

In today's digital era, mastering cybersecurity is vital. Courses like CISSP, CEH, and CISM cover security fundamentals, risk management, access control, and software security. They prepare professionals for certifications, incident handling, identity management, compliance, and resilient application development, ensuring robust protection of digital .assets