"المحترف المعتمد في أمن نظم المعلومات (CISSP):
دورة تدريبية شاملة ومعتمدة"

المدة: 5 يوم

اللغة: ar

كود الكورس: PI1 - 134

هدف الكورس

:Upon completion of this course, participants will be able to

- Provide a comprehensive understanding of the eight CISSP CBK domains.
- Develop skills in identifying and mitigating security risks.
- Equip participants with knowledge of best practices in information security management.
- Prepare participants for the CISSP certification exam.
- Enhance participants' ability to design, implement, and manage secure information systems.

الجمهور

هذه الدورة مثالية للمتخصصين في تكنولوجيا المعلومات والممارسين في مجال الأمن المسؤولين عن إدارة وحماية نظم المعلومات في المؤسسات. وهي مفيدة بشكل خاص لـ:

- محللي أمن المعلومات
- مهندسي أمن الشبكات
- مستشاري الأمن
- مديري تكنولوجيا المعلومات
- مسؤولي الأنظمة
- مدققي ومهندسي الأمن
- المحترفين الذين يسعون لتطوير مسيرتهم المهنية في مجال الأمن السيبراني

منهجية التدريب

تتبنى دورة تدريب CISSP نهج التعلم المدمج لضمان قدرة المشاركين على تطبيق المعرفة النظرية والعملية. تتضمن الدورة محاضرات ودراسات حالة وسيناريوهات واقعية ومعامل تطبيقية. يتم دمج المناقشات التفاعلية والأنشطة الجماعية في كل جلسة لتشجيع التعلم التعاوني وتبادل المعرفة بين المشاركين. توفر التمارين والمحاكاة في مجال الأمن السيبراني للمشاركين خبرة عملية في إدارة الحوادث الأمنية وتنفيذ التدابير الوقائية.

يمكن للمشاركين أيضًا الوصول إلى موارد عبر الإنترنت، بما في ذلك أسئلة نموذجية وأدلة دراسية وامتحانات تجريبية لدعم التعلم الذاتي وإعداد الامتحانات.

الملخص

هي برنامج شامل يهدف إلى تزويد محترفي تكنولوجيا (CISSP) دورة تدريبية لشهادة محترف أمن نظم المعلومات المعتمد واحدة من أكثر الشهادات اعترافًا وقيمة على مستوى CISSP المعلومات بمهارات متقدمة في الأمن السيبراني. تُعتبر شهادة العالم، وهي ضرورية للمحترفين الذين يطمحون لبناء وتطوير مسيرتهم المهنية في مجال أمن المعلومات. تغطي الدورة مجموعة متنوعة من الممارسات والسياسات والإجراءات الأمنية لحماية نظم معلومات المؤسسة، بما في ذلك التحكم في .الوصول، التشفير، استعادة البيانات بعد الكوارث، وإدارة الأمن

والتي تُعتبر أساسية ،CISSP تم تصميم هذا التدريب لتقديم فهم شامل للمجالات الثمانية في الجسم المعرفي المشترك لشهادة

للحصول على الشهادة. يتعمق كل مجال في مواضيع حيوية مثل أمن تطوير البرمجيات، إدارة المخاطر، وأمن الشبكات لضمان استعداد المشاركين لمواجهة تحديات الأمن الواقعية.

تجمع هذه الدورة بين المعرفة النظرية والرؤى العملية، وهي مصممة لأولئك الذين يطمحون ليكونوا مستشارين أمنيين، مديري تكنولوجيا المعلومات، أو مدققين أمنيين. من خلال دراسات الحالة، والمحاكاة، والتمارين العملية، سيكتسب المشاركون خبرة في تقييم المخاطر وتخفيفها، وتنفيذ ضوابط الأمن، وفهم الأطر القانونية والتنظيمية التي تحكم أمن المعلومات.

مما يضعهم في موقع الريادة في CISSP، في نهاية الدورة، سيكون لدى المشاركين الأدوات اللازمة لاجتياز امتحان شهادة آفاقهم المهنية وتضمن قدرتهم على حماية مؤسساتهم من CISSP مجال الأمن السيبراني المتطور باستمرار. تعزز شهادة التهديدات الأمنية الحديثة.

محتوى الكورس والمخطط الزمني

Section 1: Introduction to CISSP and Cybersecurity Fundamentals

- Overview of CISSP certification and its importance
- The role of cybersecurity in today’s IT environment
- Introduction to the eight domains of the CISSP CBK

Section 2: Security and Risk Management

- Security governance principles
- Compliance and legal issues in cybersecurity
- Risk management frameworks and methodologies
- Business continuity and disaster recovery planning

Section 3: Asset Security and Security Architecture

- Classification and protection of assets
- Security models and frameworks
- Designing and implementing secure architectures

Section 4: Communication and Network Security

- Network protocols and services
- Securing network infrastructure
- Virtual private networks (VPNs) and firewalls
- Intrusion detection and prevention systems

Section 5: Identity and Access Management (IAM)

- Access control models and methods
- Authentication and authorisation techniques
- Identity as a service (IDaaS)
- Managing user lifecycle and privileges

Section 6: Security Assessment and Testing

- Types of security assessments
- Vulnerability management
- Penetration testing methodologies
- Incident response and forensic investigation

Section 7: Security Operations

- Security operations management
- Logging and monitoring activities
- Security event management systems
- Incident management and disaster recovery

Section 8: Software Development Security

- Secure coding practices
- Software development life cycle (SDLC) and security
- Application security threats and mitigations
- Testing and auditing software for vulnerabilities

تفاصيل الشهادة

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

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

تطبيقات تكنولوجيا المعلومات والكمبيوتر, التكنولوجيا

مقالات ذات صلة

ما هي تكنولوجيا المعلومات؟ دليل شامل لفهم التقنية الحديثة وتطبيقاته

تلعب تكنولوجيا المعلومات دورًا حاسمًا في عالمنا المعاصر، حيث أصبحت جزءًا لا يتجزأ من حياتنا اليومية وعمل الشركات والمؤسسات. سواءً كنا نتحدث عن الحوسبة السحابية، الأمن السيبراني، أو الذكاء الاصطناعي، فإن تكنولوجيا المعلومات تشكل البنية التحتية الرقمية التي تربط العالم وتُسهم في تطوير الصناعات المختلفة. في هذا الدليل المتكامل، سنقدم