

"المدير الأمني للمعلومات ـ دور الرئيس التنفيذي للأمانة في المعلومات"

المدة: 5 يوم

اللغة: ar

كود الكورس: MG2 - 214

هدف الكورس

سيتمكن المشاركون في هذه الدورة من:

- فهم المسؤوليات المتطورة والأهمية الاستراتيجية لدور مدير أمن المعلومات.
- تأسيس وقيادة أطر عمل الأمن السيبراني للمؤسسات.
- تحليل التهديدات الناشئة وتنفيذ استراتيجيات دفاع قوية.

- تصميم وقيادة خطط الاستجابة للحوادث وإدارة الأزمات.
- ضمان الامتثال التنظيمي للمعايير العالمية (مثل GDPR، NIS2، ISO/IEC 27001).
- التفاعل والتواصل بفعالية مع الفرق التنفيذية والجهات التنظيمية ومجلس الإدارة.
- دمج استراتيجية الأمن السيبراني مع أهداف استمرارية الأعمال والتحول الرقمي.

الجمهور

هذه الدورة مثالية لـ:

- كبار مسؤولي أمن المعلومات الحاليين والطامحين (CISOs).
- مديري ومديرات أمن المعلومات.
- المديرين التنفيذيين لحوكمة تكنولوجيا المعلومات وإدارة المخاطر.
- كبار مسؤولي التكنولوجيا (CTOs).
- رؤساء الامتثال والشؤون التنظيمية.
- مستشاري وخبراء الأمن السيبراني.
- أعضاء مجلس الإدارة والمديرين التنفيذيين الكبار المشاركين في الإشراف على الأمن.

منهجية التدريب

تستخدم هذه الدورة مزيجًا من المحاضرات التفاعلية، ودراسات الحالة الواقعية، ومحاكاة حوادث الأمن السيبراني، والمناقشات الجماعية، وتمارين التخطيط الاستراتيجي. يتم تقديمها باستخدام مبادئ تعليم الكبار التي تعزز الفهم والتطبيق والاحتفاظ بمفاهيم القيادة الأمنية المتقدمة. كما سيحصل المشاركون على قوالب وسجلات مخاطر وأطر عمل قابلة للتطبيق في البيئات التنظيمية الواقعية.

الملخص

تم تصميم هذه الدورة التدريبية المتقدمة للمديرين التنفيذيين لأمن المعلومات الحاليين والطموحين الذين يتحملون مسؤولية إنشاء وإدارة وتوسيع أطر الأمن السيبراني للمؤسسات. تستكشف الدورة مشهد التهديدات المتطور، والامتثال التنظيمي، وتخطيط الاستجابة للحوادث، وحوكمة المخاطر، والدور الاستراتيجي للمدير التنفيذي لأمن المعلومات في مواءمة الأمن

السيبراني مع الأهداف التجارية. سيكتسب المشاركون المهارات اللازمة لقيادة عمليات الأمن السيبراني مع تعزيز ثقافة الأمان في جميع أنحاء المنظمة.

بحلول نهاية الدورة، سيكون المشاركون مزودين بالمعرفة والأدوات اللازمة لحماية أصول المؤسسة، وقيادة المبادرات الأمنية متعددة الوظائف، وتقديم المشورة بثقة لمجالس الإدارة وأصحاب المصلحة التنفيذيين بشأن المخاطر السيبرانية والمرونة.

محتوى الكورس والمخطط الزمني

Section 1: The Evolving Role of the CISO

- .Defining the CISO’s mandate and reporting structure
- .Cybersecurity trends and executive-level responsibilities
- .Building a strategic cybersecurity vision aligned with business goals
- .Maturity models and the CISO’s journey: reactive to proactive
- .CISO vs CIO vs CTO roles – coordination and boundary setting

Section 2: Enterprise Security Frameworks & Risk Governance

- .(Designing an enterprise cybersecurity framework (NIST, ISO, COBIT
- .Risk identification, quantification, and control mapping
- .Third-party and supply chain risk management
- .Building a cyber risk register and board-level dashboards
- .Cyber insurance: coverage, limitations, and evaluation

Section 3: Threat Intelligence, Detection & Defence

- .Understanding modern threats: APTs, ransomware, insider threats
- .Threat intelligence lifecycle and threat hunting techniques
- .SOC maturity and incident detection capabilities
- .Endpoint and network protection strategies
- .Zero trust architecture and segmentation

Section 4: Crisis Management & Compliance Leadership

- Building and testing incident response and disaster recovery plans.
- Regulatory frameworks: GDPR, HIPAA, NIS2, PCI DSS, ISO 27001.
- Conducting cyber drills, tabletop exercises, and breach simulations.
- Developing a compliance and audit readiness framework.
- Managing communication and stakeholder trust during breaches.

Section 5: Strategic Alignment, Culture, and Reporting

- Developing a cybersecurity culture: training and awareness strategies.
- Aligning cyber strategy with digital transformation and resilience.
- Board reporting: translating cyber risk into business language.
- KPIs, KRIs, and ROI of cybersecurity programs.
- Final Simulation: Leading a cybersecurity crisis from boardroom to SOC.

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 (BAC) وخدمة اعتماد التطوير المهني 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

القيادة والإدارة, التكنولوجيا, تطبيقات تكنولوجيا المعلومات والكمبيوتر

مقالات ذات صلة



أمن المعلومات:أنواعه وأهميته في حماية البيانات والأنظمة

أمن المعلومات أصبح أحد العناصر الأساسية في العصر الرقمي الذي نعيشه اليوم. مع تزايد الاعتماد على التكنولوجيا في جميع جوانب الحياة اليومية، من الأعمال التجارية إلى الخدمات الحكومية وحتى حياتنا الشخصية، تصبح حماية المعلومات من التهديدات الإلكترونية أكثر أهمية من أي وقت مضى. يشمل أمن المعلومات مجموعة واسعة من السياسات