محترف أمن المعلومات: دوره وأهميته في العصر الرقمي

Duration: 5 Days

Language: ar

Course Code: PI1-127

Objective

عند إتمام هذه الدورة، سيكون المشاركون قادرين على:

- فهم أساسيات الأمن، تقييم المخاطر، التحكم في الوصول، تأمين تطوير البرمجيات، والمفاهيم ذات الصلة.
- مما يمنح المشاركين الفهم والثقة اللازمة للتفوق في سعيهم للحصول CISSP، الاستعداد بشكل كافٍ لاختبار شهادة على الشهادة.
- إتقان صياغة أطر أمنية قوية، التعامل مع الحوادث الأمنية، والتعافي من الاختراقات مع الالتزام بالمعايير القانونية والتنظيمية.
- تطوير الخبرة في إدارة الهوية والوصول، ضمان التحقق والتفويض الآمن، وإدارة الهويات طوال دورة حياتها.
- اكتساب الكفاءات في عمليات الأمن، بما في ذلك المراقبة، الاستجابة للحوادث، وضمان الامتثال، بالإضافة إلى فهم المنهجيات الآمنة لتطوير البرمجيات لبناء تطبيقات قوية.

Audience

تم تصميم هذه الدورة لأي شخص مسؤول عن تقليل المخاطر الأمنية في المؤسسة. ستكون ذات فائدة كبيرة لـ:

- أخصائيو تكنولوجيا المعلومات
- مديرو تكنولوجيا المعلومات
- مديرو المخاطر
- مديرو التوعية الأمنية
- أصحاب الأعمال

- مديرو الأقسام
- مديرو العمليات
- مديرو الأنظمة
- المطورون

Training Methodology

يعتمد هذا الدورة على مجموعة متنوعة من أساليب التعلم للكبار لتعزيز الفهم والاستيعاب الكامل. سيشاهد المشاركون مقاطع فيديو لتسليط الضوء على أهمية تنفيذ عمليات الأمن السيبراني، ولفهم ما قد يحدث في حال عدم أخذ الأمن السيبراني بجدية، وذلك من خلال دراسات حالة واقعية.

بعد ذلك، سيقوم المشاركون بأنشطة جماعية ومناقشات لفهم مدى قوة الأمن السيبراني في مؤسستهم وتطوير خطط لزيادة أمان أنظمتهم وبياناتهم.

Summary

دور محترفي الأمن السيبراني حيوي في حماية الأصول الرقمية والبنية التحتية والمعلومات الحساسة للمنظمة من التهديدات السيبرانية. يُكلف هؤلاء المحترفون بتحديد نقاط الضعف، وتنفيذ التدابير الوقائية، والاستجابة للحوادث الأمنية لتقليل المخاطر بفعالية. مع تزايد وتيرة وتعقيد الهجمات السيبرانية، أصبح دور محترفي الأمن السيبراني لا غنى عنه لضمان استمرارية ونجاح المنظمات في المستقبل. هم أساسيون في الحفاظ على ثقة العملاء، وحماية الملكية الفكرية، وضمان الامتثال التنظيمي، والحفاظ على سمعة المنظمة. مع استمرار تطور التكنولوجيا وتطور التهديدات السيبرانية، سيزداد الطلب على محترفي الأمن السيبراني المهرة. دورهم ضروري لتأمين مستقبل أي منظمة في عالم رقمي متزايد.

Course Content & Outline

Section 1: CISSP & Other Security Concepts

- Introduction to CISSP (Certified Information Systems Security Professional).
- Fundamentals of cybersecurity.
- Network security principles.

- Cryptography essentials.
- Access control mechanisms.
- Security architecture and design.
- Software development security.
- Security operations and incident response.
- Risk management concepts.
- Legal, regulatory, and ethical considerations in security.
- Security testing and assessment techniques.
- Emerging technologies in cybersecurity.
- Integration of security concepts into organisational practices.

Section 2: The Importance of Cybersecurity

- Understanding the significance of cybersecurity in modern society.
- Identifying cyber threats and their potential impacts.
- Exploring cybersecurity best practices for individuals and organisations.
- Recognising the role of cybersecurity in protecting personal and sensitive information.
- Examining the economic and reputational consequences of cyber attacks.
- Discussing legal and regulatory frameworks relevant to cybersecurity.
- Highlighting the importance of cybersecurity in safeguarding critical infrastructure.
- Addressing the challenges and opportunities in the cybersecurity landscape.
- Promoting cybersecurity awareness and education initiatives.
- Emphasising the need for proactive cybersecurity measures in an interconnected world.

Section 3: Asset Security Management

- Asset identification and classification methodologies.
- Risk assessment and management for assets.
- Implementing access controls to safeguard assets.
- Physical security measures for protecting assets.
- Data encryption and protection techniques.
- Asset lifecycle management strategies.
- Security awareness and training for asset management.
- Incident response and recovery procedures for asset security breaches.
- Compliance with asset security regulations and standards.

Section 4: Network Security & Communication Strategies

- Network access control mechanisms and strategies.
- Intrusion detection and prevention systems.
- Secure configuration and management of network devices.
- Virtual private network (VPN) technologies and implementation.
- Wireless network security considerations.
- Network security monitoring and incident response procedures.
- Security best practices for cloud-based networks.
- Role of encryption in securing network communications.

Section 5: Identity & Access Management (IAM)

- Role-based access control (RBAC) implementation.
- Single sign-on (SSO) solutions and federated identity management.
- Identity lifecycle management strategies.
- Multi-factor authentication (MFA) techniques.
- Identity governance and compliance considerations.
- Privileged access management (PAM) principles.
- Identity theft prevention measures.
- Emerging trends and challenges in IAM.

Section 6: Penetration Testing & Software Development

- Understanding software development lifecycle (SDLC).
- Integrating security into each phase of SDLC.
- Identifying vulnerabilities in software applications.
- Penetration testing tools and techniques.
- Conducting code reviews for security vulnerabilities.
- Secure coding best practices.
- Automated and manual penetration testing approaches.
- Reporting and remediation of security findings.
- Continuous integration and deployment security.
- DevSecOps principles and practices.

Section 7: Security Operations Best Practices

- Incident detection and response strategies.
- Security information and event management (SIEM) implementation.
- Security incident management processes.
- Threat intelligence gathering and analysis.

- Security orchestration, automation, and response (SOAR).
- Vulnerability management techniques.
- Log management and monitoring practices.
- Incident response planning and exercises.

Certificate Description

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.

Categories

تطبيقات تكنولوجيا المعلومات والكمبيوتر, التكنولوجيا

Related Articles

الأمن السيبراني: أهميته وفوائده

تعمل سياسة الأمن السيبراني القوية والبنية التحتية معًا لتأمين أنظمة الكمبيوتر والشبكات من أي هجوم أو وصول غير مصرح به. تستثمر الشركات والأفراد والحكومات بكثافة لجني فوائد الأمن السيبراني في حماية أصولهم وبياناتهم ضد المتسللين. لكي تتمكن أي شركة من البقاء في عالم اليوم التنافسي، فإنها تتطلب الأدوات المناسبة واستراتيجية

YouTube Video

https://www.youtube.com/embed/I_fLHTwrcnE?si=-xI7TiYT3wNj4eOG