Projekt COMENIANA

KYBERNETICKÁ BEZPEČNOSŤ

MJCH, s.r.o., Projekt COMENIANA

ROBME VECI JEDNODUCHŠIE, LEPŠIE A BEZPEČNEJŠIE

Čo nájdete v tejto brožúre

- Informácie o nás
- Prečo ISO normy
- Informácie o prihlasovaní
- Informácie o skúške a získaní medzinárodného certifikátu
- Krátky prehľad o kurzoch v tejto brožúre
- Kurzy k nasledujúcim normám ISO/IEC 27032, Cloud Security, Pentest Professional, SCADA

Pri každom kurze nájdete tieto informácie:

- pre koho je kurz určený
- obsah kurzu
- ciele kurzu
- priemerný čas potrebný na štúdium
- vedomosti odporúčané pred kurzom
- cena

Názov kurzu	Predpokladaný strávený čas	Certifikát	Cena (s DPH)
ISO/IEC 27032 Foundation	2 dni	skúška	450€
ISO/IEC 27032 Lead Cybersecurity Manager	5 dni	skúška	1250€
Lead Cloud Security Manager	5 dní	skúška	1250€
Lead Pentest Professional	5 dní	skúška	1250€
Lead SCADA Security Manager	5 deň	skúška	1250€

SKÚŠKA A ZÍSKANIE CERTIFIKÁTU

Certifikát môžete získať po úspešnom absolvovaní skúšky.Skúšku je možné absolvovať do 12 mesiacov od zakúpenia kurzu. V prípade, neúspechu prvej skúšky je opravný termín možný najskôr po 15 dňoch a najneskôr do 12 mesiacov od neúspešného pokusu. Absolvovanie kurzu nie podmienkou absolvovania skúšky, okrem kurzov v úrovni Foundation.

Typy skúšok:
Multiple-choice, closed- book – účastníci skúšky nesmú používať žiadne materiály ani svoje poznámky. Tento typ skúšky je zvyčajne v kurzoch Transition a v úrovni Foundaion.
Multiple-choice, open-book - účastníci môžu používať vytlačenú kópiu materiálov z kurzu, tlačenú verziu daného ISO štandardu, osobné poznámky (prístupné cez PECB Exams aplikáciu a/alebo tlačené), tlačený prekladový slovník.

Počas priebehu skúšky kandidát vidí koľko mu zostáva času a koľko otázok už odpovedal. K otázkam sa môže počas skúšky vrátiť a upraviť svoju odpoveď. V prípade, že si nie je istý odpoveďou, danú otázku si môže označiť a vrátiť sa k nej neskôr.

Výsledky online Multiple-choice skúšok má kandidát prakticky okamžite a sú zasielané emailom. Na úspešné zvládnutie skúšky **je potrebné dosiahnuť 75%**.

Získanie certifikátu:
Kandidátom, ktorí skúšku **úspešne absolvovali** bude zaslaná informácia ako požiadať o certifikát.
Tí, ktorí nebudú pri skúške úspešní dostanú emailom informáciu o oblastiach kde mali najnižšiu úspešnosť. Kandidáti, ktorí nesúhlasia s výsledkom skúšky môže podať podnet na examination@pecb.com Kandidátom, ktorí úspešne neabsolvujú ani druhý termín skúšky je odporúčané kurz absolvovať znovu.
Odporúčame aby kurz a skúška boli v rovnakom jazyku (napr. v angličtine).

Platnosť certifikátu:
Vydaný certifikát má platnosť 3 roky. Po troch rokoch je možné certifikát predĺžiť, resp. zvýšiť svoju úroveň preukázaním nadobudnutej praxe v tomto čase.

ISO/IEC 27032 FOUNDATION

Stále väčšie využívanie kybernetického priestoru vedie k väčším kybernetickým hrozbám a vyžaduje si znalosti kybernetickej bezpečnosti. Kurz ISO/IEC 27032 Foundation predstaví hlavné koncepty a požiadavky programu kybernetickej bezpečnosti, vrátane zainteresovaných strán v kybernetickom priestore, mechanizmov útokov a zdieľania a koordinácie informácií.
Po absolvovaní kurzu a certifikačnej skúšky môžu účastníci získať certifikát, ktorý preukáže ich znalosti základných konceptov, princípov a techník kybernetickej bezpečnosti.

Pre koho je kurz určený?

- Jednotlivcom zapojeným do kybernetickej bezpečnosti.
- Jednotlivcom, ktorí sa zaujímajú o kybernetickú bezpečnosť.
- Jednotlivcom, ktorí chcú kariérne napredovať v oblasti kybernetickej bezpečnosti.

Obsah kurzu

- Úvod do ISO/IEC 27032 a základných princípov a konceptov kybernetickej bezpečnosti.
- Program kybernetickej bezpečnosť.

Rozsah kurzu

- Účastníci majú k dispozícii viac ako 200 stranový materiál, ktorý obsahuje praktické cvičenia, príklady a testy podobné certifikačnej skúške. Priemerný čas na štúdium je 2 dni.

Odporúčané vedomosti pred kurzom

Pred kurzom nie sú potrebné predchádzajúce školenia alebo vedomosti v tejto oblasti.

Cena

450 EUR s DPH / *Cena zahŕňa: online prístup k študijným materiálom cez platformu PECB, certifikačnú skúšku, opravnú certifikačnú skúšku, certifikát (v prípade úspešného absolvovania skúšky)*

ISO/IEC 27032 LEAD CYBERSECURITY MANAGER

Kurz kybernetickej bezpečnosti SO/IEC 27032 umožní účastníkom získať odborné znalosti a kompetencie potrebné na podporu organizácie pri implementácii a riadení programu kybernetickej bezpečnosti založenom na normách ISO/IEC 27032 a NIST Cybersecurity framework. Počas kurzu získajú komplexné znalosti o kybernetickej bezpečnosti, o vzťahu medzi kybernetickou bezpečnosťou a inými typmi informačnej bezpečnosti a o úlohe zainteresovaných strán v kybernetickej bezpečnosti.

Pre koho je kurz určený?

- Profesionálom v oblasti kybernetickej bezpečnosti.
- Odborníkom na informačnú bezpečnosť.
- Jednotlivcom zodpovedným za vývoj programu kybernetickej bezpečnosti.
- IT špecialistov.
- Odborným poradcov v oblasti IT.
- IT profesionálom, ktorí chcú zlepšiť svoje technické zručnosti a znalosti.

Obsah kurzu

- Úvod do ISO/IEC 27032 a základných princípov a konceptov kybernetickej bezpečnosti.
  - Základné pojmy, program kybernetickej bezpečnosti, analýza organizácie
- Politiky kybernetickej bezpečnosti, riadenie rizík a mechanizmy útokov
- Kontroly kybernetickej bezpečnosti, zdieľanie informácií a koordinácia
- Riadenie incidentov a zlepšovanie
- Riadenie incidentov v kybernetickej bezpečnosti, reakcia na incidenty, testovanie, meranie výkonu

Rozsah kurzu

- Účastníci majú k dispozícii viac ako 450 stranový materiál, ktorý obsahuje praktické cvičenia, príklady a testy podobné certifikačnej skúške. Predpokladaný čas na štúdium je 5 dní.

Odporúčané vedomosti pred kurzom

Základné znalosti ISO/IEC 27032 a podrobná znalosť bezpečnosti informácií.

Cena

1250 EUR s DPH / *Cena zahŕňa: online prístup k študijným materiálom cez platformu PECB, certifikačnú skúšku, opravnú certifikačnú skúšku, certifikát (v prípade úspešného absolvovania skúšky)*

LEAD CLOUD SECURITY MANAGER

Kurz Lead Cloud Security Manager Vám umožní získať kompetencie potrebné na podporu organizácie pri efektívnom plánovaní, implementácii, správe, monitorovaní a udržiavaní cloudového bezpečnostného programu založeného na ISO/IEC 27017 a ISO/IEC 27018. Dozviete sa koncepty a princípy cloud computingu, riadenia bezpečnostných rizík cloud computingu, kontroly špecifické pre cloud, riadenie bezpečnostných incidentov cloudu a testovanie bezpečnosti cloudu.

Pre koho je kurz určený?

- Odborníkom v oblasti cloudovej bezpečnosti a informačnej bezpečnosti, ktorí chcú spravovať cloudový bezpečnostný program.
- Manažérom a konzultantom, ktorí sa snažia osvojiť si osvedčené postupy zabezpečenia cloudu.
- Jednotlivcom, ktorí sú zodpovední za údržbu a správu cloudového bezpečnostného programu.
- Technickým expertom, ktorí sa snažia zlepšiť svoje znalosti o cloudovom zabezpečení.
- Expertným poradcom cloudovej bezpečnosti.

Obsah kurzu

- Úvod do ISO/IEC 27017 a ISO/IEC 27018 a spustenie programu cloudovej bezpečnosti.
  - Normy a regulačné rámce, základné koncepty cloud computingu, úlohy a zodpovednosti súvisiace s bezpečnosťou informácií, politika informačnej bezpečnosti pre cloud computing.
- Správa bezpečnostných rizík cloud computingu a kontroly špecifické pre cloud.
  - Riadenie bezpečnostných rizík cloud computingu, výber a návrh ovládacích prvkov, implementácia kontrol špecifických pre Cloud.
- Správa bezpečnostných incidentov v cloude, testovanie, monitorovanie a neustále zlepšovanie.

Rozsah kurzu

- Účastníci majú k dispozícii viac ako 450 stranový materiál, ktorý obsahuje praktické cvičenia, príklady a testy podobné certifikačnej skúške. Predpokladaný čas na štúdium je 5 dní.

Odporúčané vedomosti pred kurzom

Základné znalosti noriem ISO/IEC 27017 a ISO/IEC 27018 a všeobecné znalosti o konceptoch cloud computingu.

Cena

1250 EUR s DPH / *Cena zahŕňa: online prístup k študijným materiálom cez platformu PECB, certifikačnú skúšku, opravnú certifikačnú skúšku, certifikát (v prípade úspešného absolvovania skúšky)*

LEAD PENTEST PROFESSIONAL

Na kurze Lead Pentest Professional účastníci získajú potrebné odborné znalosti na vedenie profesionálneho penetračného testu pomocou kombinácie praktických techník a manažérskych zručností.
Kurz je zameraný špeciálne na vedomosti a zručnosti, ktoré potrebujú profesionáli, ktorí chcú viesť alebo sa zúčastniť penetračného testu. Zaoberá sa najnovšími technickými poznatkami, nástrojmi a technikami v kľúčových oblastiach vrátane infraštruktúry, bezpečnosti webových aplikácií, mobilnej bezpečnosti a sociálneho inžinierstva. Okrem toho sa tento kurz sústreďuje na to, ako prakticky aplikovať to, čo sme sa naučili, na súčasné každodenné penetračné testovanie a nerozširuje nesúvisiace, zastarané alebo zbytočné teoretické koncepty.

Pre koho je kurz určený?

- IT profesionálom, ktorí chcú zlepšiť svoje technické znalosti.
- Audítorom, ktorí chcú pochopiť procesy penetračného testovania.
- IT a rizikovým manažérom, ktorí sa snažia podrobnejšie pochopiť vhodné použitie penetračných testov.
- Penetračným testerov.
- Odborníkom v oblasti kybernetickej bezpečnosti.

Obsah kurzu

- Úvod do penetračného testovania, etiky, plánovania a rozsahu.
  - Princípy penetračného testovania, právne a etické otázky, základné princípy informačnej bezpečnosti a riadenie rizík, fázy penetračného testovania.
- Technické základy, znalosti a techniky (s praktickými cvičeniami vo všetkých oblastiach).
- Vykonanie penetračného testu (pomocou nástrojov a techník) a preskúmanie testovacích oblastí.
- Analýza výsledkov testovania, reportovania a sledovania.
  - Dokumentácia kontroly, akčné plány a následné opatrenia.

Rozsah kurzu

- Účastníci majú k dispozícii viac ako 450 stranový materiál, ktorý obsahuje praktické cvičenia, príklady a testy podobné certifikačnej skúške. Predpokladaný čas na štúdium je 5 dní.

Odporúčané znalosti pred kurzom

- Základné znalosti penetračného testovania a komplexná znalosť kybernetickej bezpečnosti.

Cena

1250 EUR s DPH / *Cena zahŕňa: online prístup k študijným materiálom cez platformu PECB, certifikačnú skúšku, opravnú certifikačnú skúšku, certifikát (v prípade úspešného absolvovania skúšky)*

LEAD SCADA SECURITY MANAGER

Na kurze Lead SCADA Security Manager účastníci získajú odborné znalosti na plánovanie, navrhovanie a implementáciu efektívneho programu na ochranu SCADA systémov. Okrem toho budú schopní porozumieť bežným hrozbám, zraniteľnostiam, rizikám súvisiacim s priemyselnými riadiacimi systémami (ICS) a technikám používaným na riadenie týchto rizík. Toto školenie sa zameriava na viaceré aspekty bezpečnostného manažmentu a zručnosti súvisiace s bezpečnosťou SCADA/ICS.

Pre koho je kurz určený?

- Bezpečnostným profesionálom, ktorí majú záujem získať zručnosti v oblasti SCADA.
- IT profesionálom, ktorí chcú zlepšiť svoje technické zručnosti a znalosti.
- IT a rizikových manažérom, ktorí chcú podrobnejšie porozumieť systémom ICS a SCADA.
- Vývojárov SCADA systémov.
- SCADA IT profesionálov.

Obsah kurzu

- Úvod do SCADA a ICS.
  - Základné princípy a koncepty SCADA, charakteristiky priemyselných riadiacich systémov (ICS), hrozieb a zraniteľností.
- Návrh bezpečnostného programu a architektúry sieťovej bezpečnosti.
  - Návrh programu, bezpečnostný program SCADA, hodnotenie rizika, architektúra sieťovej bezpečnosti pre systémy SCADA.
- Implementácia bezpečnostných kontrol ICS, správy incidentov a kontinuity podnikania.
  - Vykonávanie bezpečnostných kontrol pre SCADA systémy, riadenie incidentov, monitorovanie, analýza a vyhodnocovanie meraní.
- Bezpečnostné testovanie SCADA systémov.
  - Princípy testovania, právne a etické otázky, prístupy penetračného testovania, testovanie bezpečnosti ICS, vedenie penetračného testu, dokumentácia testu, kontrola kvality a správa, kompetencia a hodnotenie SCADA Security manažérov

Rozsah kurzu

- Účastníci majú k dispozícii viac ako 450 stranový materiál, ktorý obsahuje praktické cvičenia, príklady a testy podobné certifikačnej skúške. Predpokladaný čas na štúdium je 5 dní.

Odporúčané znalosti pred kurzom

- Základné znalosti SCADA Security.

Cena

1250 EUR s DPH / *Cena zahŕňa: online prístup k študijným materiálom cez platformu PECB, certifikačnú skúšku, opravnú certifikačnú skúšku, certifikát (v prípade úspešného absolvovania skúšky)*

Kontaktujte nás na kurzy@comeniana.com alebo na telefónnom čísle +421 917 164 652

ĎALŠIE KURZY V NAŠEJ PONUKE:

Kybernetická bezpečnosť:
ISO/IEC 27032 Kybernetická bezpečnosť
Cloud security
Penetračné testovanie
SCADA

Kontinuita podnikania:
ISO 22301 Kontinuita podnikania
Disaster Recovery

Kvalita a manažment:
ISO 9001 Manažment kvality
ISO/IEC 20000 Manažment služieb
ISO 21502 Projektový manažment
ISO 13485 Medical Devices Quality Management System
ISO/IEC 17025 Laboratory Management System
Six Sigma
ISO 55001 Asset Management System
ISO 28000 Supply Chain Security Management System

Governance, riziká, zhody:
ISO 31000 Risk Management
ISO 37001 Anti-Bribery
ISO 37301 Compliance Management System
ISO/IEC 38500 IT Governance

Súkromie a ochrana osobných údajov:
ISO/IEC 27701 Privacy Information Management System
General Data Protection Regulation (GDPR)

Ďalšie:
ISO 45001 Occupational Health and Safety Management System
ISO 22000 Food Safety Management System
ISO 18788 Security Operations Management System
ISO 50001 Energy Management System
ISO 14001 Environmental Management System
ISO 26000 Social Responsibility Management System

COMENIANA
by MJCH