KATALÓG SLUŽIEB 2024

NAKIB

ŠKOLENIA

NÁRODNÁ AKADÉMIA PRE KYBERNETICKÚ
A INFORMAČNÚ BEZPEČNOSŤ

NAKIB.SK

NAKIB

ŠKOLENIA

Manažér kyber bezpečnosti (MKB)

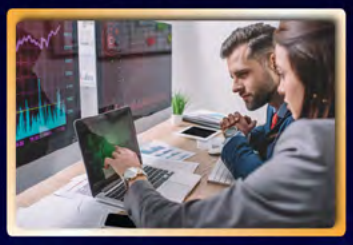
Audítor kyber bezpečnosti (AKB)

Manažér pre kyber bezpečnosť MKB podľa NIS2

TISAX® Manažér pre informačnú bezpečnosť v automotív

Nová norma ISO 27001:2022

Vykonávanie analýzy rizík



Manažér pre riadenie kontinuity činností

Znalosti Zákona o ITVS 95/2019

Požiadavky v oblasti ochrany osobných údajov v zmysle GDPR

Základy hackingu

DORA

Zákon o utajovaných skutočnostiach 215/2004 Z. z.

AI - Umelá inteligencia

Kybernetická bezpečnosť v OT prostredí

NAKIB.SK

NAKIB

ŠKOLENIA

Manažér kyber bezpečnosti (MKB)

PRÍPRAVA NA CERTIFIKAČNÚ SKÚŠKU A VÝKON ROLE MANAŽÉRA KYBERNETICKEJ BEZPEČNOSTI, PODĽA POŽIADAVIEK UVEDENÝCH VO VYHLÁŠKE ZOKB Č. 492_2022

Čo je?

Školenie Manažér kybernetickej bezpečnosti je komplexný program, ktorý rozvíja znalosti a zručnosti potrebné na efektívne riadenie kybernetickej bezpečnosti v organizácii. Školenie sa zameriava na rôzne aspekty kybernetickej bezpečnosti, ako napríklad: Riadenie rizík: Identifikácia, analýza a hodnotenie rizík kybernetických útokov. Ochrana dát: Implementácia a dodržiavanie bezpečnostných opatrení na ochranu dát. Reagovanie na incidenty: Vytvorenie a implementácia plánu reakcie na kybernetické incidenty. Dodržiavanie predpisov: Pochopenie a dodržiavanie relevantných legislatívnych požiadaviek v oblasti kybernetickej bezpečnosti. Leadership: Vedenie tímu kybernetickej bezpečnosti a budovanie povedomia o kybernetickej bezpečnosti v celej organizácii.

Prečo?

Absolvovanie školenia Manažér kybernetickej bezpečnosti prináša viacero benefitov:
Zvýšenie kybernetickej bezpečnosti: Získanie znalostí a zručností potrebných na efektívne riadenie kybernetickej bezpečnosti a zníženie rizika kybernetických útokov. Zníženie finančných strát: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadov šetrí finančné prostriedky. Posilnenie dôvery a reputácie: Demonštrovanie záväzku k kybernetickej bezpečnosti posilňuje dôveru zákazníkov, partnerov a regulačných orgánov v organizáciu. Zlepšenie súladu s regulačnými požiadavkami: Mnoho regulačných predpisov vyžaduje od organizácií implementáciu a dodržiavanie bezpečnostných opatrení.
Zvýšenie produktivity: Zníženie výpadkov a porúch súvisiacich s kybernetickými útokmi.

Pre koho?

Školenie Manažér kybernetickej bezpečnosti je určené pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za riadenie kybernetickej bezpečnosti v organizácii. IT profesionálov: Ktorí sa chcú špecializovať na oblasť kybernetickej bezpečnosti. Osoby zodpovedné za ochranu dát: V rámci organizácie. Audítorov informačných systémov: Ktorí sa chcú zamerať na audity kybernetickej bezpečnosti. Každý, kto sa chce dozvedieť viac o riadení kybernetickej bezpečnosti.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o kybernetickej bezpečnosti: Školenie pokrýva širokú škálu tém relevantných pre riadenie kybernetickej bezpečnosti. Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty riadenia kybernetickej bezpečnosti a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi. Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti a zručnosti v oblasti kybernetickej bezpečnosti. Networking: Školenie umožňuje účastníkom nadviazať kontakty s ostatnými profesionálmi v oblasti kybernetickej bezpečnosti.

NAKIB

ŠKOLENIA

Audítor kyber bezpečnosti (AKB)

PRÍPRAVA NA CERTIFIKAČNÚ SKÚŠKU A VÝKON ROLE AUDÍTOR KYBERNETICKEJ BEZPEČNOSTI, PODĽA POŽIADAVIEK UVEDENÝCH VO VYHLÁŠKE ZOKB Č. 492_2022

Čo je?

Školenie Audítor kybernetickej bezpečnosti je komplexný program, ktorý rozvíja znalosti a zručnosti potrebné na vykonávanie auditov kybernetickej bezpečnosti v organizáciách. Školenie sa zameriava na rôzne aspekty auditu kybernetickej bezpečnosti, ako napríklad: Metodika auditu: Získanie znalostí o rôznych typoch auditov a osvedčených postupoch v tejto oblasti. Hodnotenie rizík: Identifikácia, analýza a hodnotenie rizík kybernetických útokov v rámci auditu. Technické aspekty: Pochopenie bežných zraniteľností a technických kontrolných mechanizmov. Právne a regulačné požiadavky: Znalosť relevantných legislatívnych požiadaviek v oblasti kybernetickej bezpečnosti. Komunikačné a prezentačné zručnosti: Efektivita komunikácie s manažmentom a ostatnými zainteresovanými stranami o výsledkoch auditu.

Prečo?

Absolvovanie školenia Audítor kybernetickej bezpečnosti prináša viacero benefitov:
Zvýšenie kybernetickej bezpečnosti: Získanie znalostí a zručností potrebných na identifikáciu a riešenie slabín v kybernetickej bezpečnosti organizácie. Zníženie rizika kybernetických útokov: Včasná identifikácia a náprava zraniteľností znižuje riziko úspešných kybernetických útokov. Zlepšenie súladu s regulačnými požiadavkami: Audity kybernetickej bezpečnosti pomáhajú organizáciám splniť regulačné požiadavky v tejto oblasti. Zvýšenie dôvery a reputácie: Demonštrovanie záväzku k kybernetickej bezpečnosti posilňuje dôveru zákazníkov, partnerov a regulačných orgánov v organizáciu. Zlepšenie riadenia kybernetickej bezpečnosti: Audity kybernetickej bezpečnosti pomáhajú organizáciám identifikovať oblasti, v ktorých je potrebné zlepšiť riadenie kybernetickej bezpečnosti.

Pre koho?

Školenie Audítor kybernetickej bezpečnosti je určené pre:
IT profesionálov: Ktorí sa chcú špecializovať na oblasť auditovania kybernetickej bezpečnosti.
Audítorov informačných systémov: Ktorí sa chcú zamerať na audity kybernetickej bezpečnosti.
Zamestnancov v oblasti kybernetickej bezpečnosti: Ktorí chcú rozšíriť svoje znalosti a zručnosti v oblasti auditovania. Manažérov a vedúcich pracovníkov: Zodpovedných za riadenie kybernetickej bezpečnosti v organizácii. Každý, kto sa chce dozvedieť viac o auditovaní kybernetickej bezpečnosti.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o auditovaní kybernetickej bezpečnosti: Školenie pokrýva širokú škálu tém relevantných pre auditovanie kybernetickej bezpečnosti. Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty auditovania kybernetickej bezpečnosti a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi. Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti a zručnosti v oblasti auditovania kybernetickej bezpečnosti. Networking: Školenie umožňuje účastníkom nadviazať kontakty s ostatnými profesionálmi v oblasti kybernetickej bezpečnosti.

NAKIB

ŠKOLENIA

Manažér pre kyber podľa NIS2 (MKB)

VÝROBNÉ SPOLOČNOSTI VRÁTANE PRODUCENTOV POTRAVÍN BUDÚ MUSIEŤ ZAVIESŤ SYSTÉMY INFORMAČNEJ A KYBERNETICKEJ BEZPEČNOSTI

Čo je?

Školenie Manažér pre kybernetickú bezpečnosť MKB podľa NIS2 je komplexný program, ktorý rozvíja znalosti a zručnosti potrebné na efektívne riadenie kybernetickej bezpečnosti v organizáciách v súlade s smernicou NIS2 (Smernica o opatreniach pre vysokú úroveň kybernetickej bezpečnosti). Školenie sa zameriava na rôzne aspekty kybernetickej bezpečnosti s dôrazom na požiadavky NIS2, ako napríklad: Riadenie rizík: Identifikácia, analýza a hodnotenie rizík kybernetických útokov v kontexte NIS2. Ochrana dát: Implementácia a dodržiavanie bezpečnostných opatrení na ochranu dát v súlade s NIS2. Reagovanie na incidenty: Vytvorenie a implementácia plánu reakcie na kybernetické incidenty v súlade s NIS2. Dodržiavanie predpisov: Pochopenie a dodržiavanie požiadaviek NIS2 a relevantných legislatívnych predpisov v oblasti kybernetickej bezpečnosti. Leadership: Vedenie tímu kybernetickej bezpečnosti a budovanie povedomia o kybernetickej bezpečnosti v celej organizácii s ohľadom na NIS2.

Prečo?

Absolvovanie školenia Manažér pre kybernetickú bezpečnosť MKB podľa NIS2 prináša viacero benefitov:
Zvýšenie kybernetickej bezpečnosti: Získanie znalostí a zručností potrebných na efektívne riadenie kybernetickej bezpečnosti a zníženie rizika kybernetických útokov v súlade s NIS2. Zníženie finančných strát: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadov šetrí finančné prostriedky. Posilnenie dôvery a reputácie: Demonštrovanie záväzku k kybernetickej bezpečnosti a k dodržiavaniu požiadaviek NIS2 posilňuje dôveru zákazníkov, partnerov a regulačných orgánov v organizáciu. Zlepšenie súladu s regulačnými požiadavkami: Školenie sa zameriava na splnenie požiadaviek NIS2 a relevantných legislatívnych predpisov v oblasti kybernetickej bezpečnosti. Zvýšenie produktivity: Zníženie výpadkov a porúch súvisiacich s kybernetickými útokmi.

Pre koho?

Školenie Manažér pre kybernetickú bezpečnosť MKB podľa NIS2 je určené pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za riadenie kybernetickej bezpečnosti v organizácii, s dôrazom na splnenie požiadaviek NIS2. IT profesionálov: Ktorí sa chcú špecializovať na oblasť kybernetickej bezpečnosti a implementáciu NIS2. Osoby zodpovedné za ochranu dát: V rámci organizácie s ohľadom na požiadavky NIS2. Audítorov informačných systémov: Ktorí sa chcú zamerať na audity kybernetickej bezpečnosti s ohľadom na NIS2. Každý, kto sa chce dozvedieť viac o riadení kybernetickej bezpečnosti v súlade s NIS2.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o kybernetickej bezpečnosti v kontexte NIS2: Školenie pokrýva širokú škálu tém relevantných pre riadenie kybernetickej bezpečnosti s ohľadom na požiadavky NIS2. Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty riadenia kybernetickej bezpečnosti a implementácie NIS2 a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi. Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti a zručnosti

ŠTANDARD PRE VÝROBCOV AUTOMOBILOV A ICH DODÁVATEĽOV ZALOŽENÝ NA ŠTANDARDE ISO 27001

Čo je?

Školenie TISAX Manažér pre informačnú bezpečnosť v automobilovom priemysle je komplexný program, ktorý rozvíja znalosti a zručnosti potrebné na efektívne riadenie informačnej bezpečnosti v súlade s požiadavkami TISAX (Trusted Information Security Assessment Exchange). TISAX je rámec pre hodnotenie informačnej bezpečnosti v automobilovom priemysle, ktorý definuje požiadavky na ochranu informácií a dát v dodávateľskom reťazci.

Prečo?

Absolvovanie školenia TISAX Manažér pre informačnú bezpečnosť prináša viacero benefitov:
Zvýšenie informačnej bezpečnosti: Získanie znalostí a zručností potrebných na efektívne riadenie informačnej bezpečnosti a zníženie rizika kybernetických útokov v súlade s požiadavkami TISAX.
Zníženie finančných strát: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadov šetrí finančné prostriedky. Posilnenie dôvery a reputácie: Demonštrovanie záväzku k informačnej bezpečnosti a k dodržiavaniu požiadaviek TISAX posilňuje dôveru zákazníkov, partnerov a regulačných orgánov v organizáciu.
Zlepšenie súladu s regulačnými požiadavkami: Školenie sa zameriava na splnenie požiadaviek TISAX a relevantných legislatívnych predpisov v oblasti informačnej bezpečnosti. Zvýšenie produktivity: Zníženie výpadkov a porúch súvisiacich s kybernetickými útokmi.

Pre koho?

Školenie TISAX Manažér pre informačnú bezpečnosť v automobilovom priemysle je určené pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za riadenie informačnej bezpečnosti v organizácii, s dôrazom na splnenie požiadaviek TISAX. IT profesionálov: Ktorí sa chcú špecializovať na oblasť informačnej bezpečnosti a implementáciu TISAX. Osoby zodpovedné za ochranu dát: V rámci organizácie s ohľadom na požiadavky TISAX.
Audítorov informačných systémov: Ktorí sa chcú zamerať na audity informačnej bezpečnosti s ohľadom na TISAX. Každý, kto sa chce dozvedieť viac o riadení informačnej bezpečnosti v súlade s TISAX.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o informačnej bezpečnosti v kontexte TISAX: Školenie pokrýva širokú škálu tém relevantných pre riadenie informačnej bezpečnosti s ohľadom na požiadavky TISAX.
Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty riadenia informačnej bezpečnosti a implementácie TISAX a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi.
Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti a zručnosti v oblasti riadenia informačnej bezpečnosti v súlade s TISAX. Networking: Školenie umožňuje účastníkom nadviazať kontakty s ostatnými profesionálmi v oblasti informačnej bezpečnosti v automobilovom priemysle.

ŠKOLENIE NOVÁ NORMA ISO 27001:2022 PRINÁŠA REVOLUČNÚ ZMENU V RIADENÍ INFORMAČNEJ BEZPEČNOSTI

Čo je?

Školenie Nová norma ISO 27001:2022 je komplexný program, ktorý rozvíja znalosti a zručnosti relevantné pre implementáciu a údržbu systému riadenia informačnej bezpečnosti podľa novej verzie normy ISO 27001:2022. Školenie sa zameriava na rôzne aspekty normy, ako napríklad: Požiadavky normy: Podrobné pochopenie požiadaviek novej verzie normy ISO 27001:2022. Implementácia systému: Praktické kroky a nástroje na implementáciu systému riadenia informačnej bezpečnosti. Riadenie rizík: Identifikácia, analýza a hodnotenie rizík informačnej bezpečnosti v súlade s normou. Ochrana dát: Implementácia a dodržiavanie bezpečnostných opatrení na ochranu dát v súlade s normou. Audity a hodnotenia: Pochopenie procesov auditovania a hodnotenia systému riadenia informačnej bezpečnosti.

Prečo?

Absolvovanie školenia Nová norma ISO 27001:2022 prináša viacero benefitov:
Zvýšenie informačnej bezpečnosti: Získanie znalostí a zručností potrebných na efektívne riadenie informačnej bezpečnosti a zníženie rizika kybernetických útokov. Zníženie finančných strát: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadov šetrí finančné prostriedky. Posilnenie dôvery a reputácie: Demonštrovanie záväzku k informačnej bezpečnosti a k dodržiavaniu medzinárodne uznávanej normy posilňuje dôveru zákazníkov, partnerov a regulačných orgánov v organizáciu. Zlepšenie súladu s regulačnými požiadavkami: Norma ISO 27001:2022 je v súlade s mnohými regulačnými požiadavkami v oblasti informačnej bezpečnosti. Zvýšenie produktivity: Zníženie výpadkov a porúch súvisiacich s kybernetickými útokmi.

Pre koho?

Školenie Nová norma ISO 27001:2022 je určené pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za riadenie informačnej bezpečnosti v organizácii.
IT profesionálov: Ktorí sa chcú špecializovať na oblasť informačnej bezpečnosti a implementáciu normy ISO 27001:2022.
Osoby zodpovedné za ochranu dát: V rámci organizácie. Audítorov informačných systémov: Ktorí sa chcú zamerať na audity informačnej bezpečnosti s ohľadom na normu ISO 27001:2022.
Každý, kto sa chce dozvedieť viac o riadení informačnej bezpečnosti podľa normy ISO 27001:2022.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o norme ISO 27001:2022: Školenie pokrýva širokú škálu tém relevantných pre implementáciu a údržbu systému riadenia informačnej bezpečnosti podľa novej verzie normy.
Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty implementácie a údržby systému riadenia informačnej bezpečnosti a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi.
Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti a zručnosti v oblasti riadenia informačnej bezpečnosti podľa normy ISO 27001:2022. Networking: Školenie umožňuje účastníkom nadviazať kontakty s ostatnými profesionálmi v oblasti informačnej bezpečnosti.

NAKIB

ŠKOLENIA

Vykonávanie analýzy rizík

VYKONANIE ANALÝZY RIZÍK Z POHĽADU ICT PRE POTREBY INFORMAČNEJ ALEBO KYBER BEZPEČNOSTI, PRIVACY PRE VÝKON DPIA PODĽA GDPR ALEBO PROTIKORUPČNÉHO SYSTÉMU.

Čo je?

Školenie Vykonávanie analýzy rizík je komplexný program, ktorý rozvíja znalosti a zručnosti potrebné na efektívne identifikovanie, hodnotenie a riadenie rizík v rôznych kontextoch. Školenie sa zameriava na rôzne aspekty analýzy rizík, ako napríklad: Metódy analýzy: Pochopenie a používanie rôznych metód analýzy rizík, ako napríklad FMEA, HAZOP a SWOT. Identifikácia rizík: Systematická identifikácia potenciálnych rizík v rôznych oblastiach, ako napríklad v oblasti informačnej bezpečnosti, projektového manažmentu alebo v prevádzke.Hodnotenie rizík: Kvantifikácia a kvalifikácia rizík na základe ich pravdepodobnosti a dopadu. Riadenie rizík: Implementácia a monitorovanie stratégie riadenia rizík pre zníženie ich dopadu. Komunikácia o rizikách: Efektivna komunikácia o rizikách s manažmentom a ostatnými zainteresovanými stranami.

Prečo?

Absolvovanie školenia Vykonávanie analýzy rizík prináša viacero benefitov:
Zníženie rizík: Získanie znalostí a zručností potrebných na efektívnu identifikáciu a riadenie rizík, čím sa znižuje ich dopad na organizáciu. Zlepšenie rozhodovania: Analýza rizík umožňuje informovanejšie a efektívnejšie rozhodovanie v rôznych oblastiach. Zvýšenie efektivity: Riadenie rizík pomáha predchádzať problémom a zbytočným stratám. Zlepšenie súladu s regulačnými požiadavkami: Mnoho regulačných požiadaviek vyžaduje od organizácií implementáciu systému riadenia rizík. Zvýšenie konkurencieschopnosti: Schopnosť efektívne riadiť riziká je dôležitou súčasťou konkurencieschopnosti v dnešnom dynamickom prostredí.

Pre koho?

Školenie Vykonávanie analýzy rizík je určené pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za riadenie rizík v organizácii.
Projektových manažérov: Ktorí potrebujú efektívne riadiť riziká v projektoch.
IT profesionálov: Ktorí sa chcú špecializovať na oblasť riadenia rizík.
Audítorov: Ktorí sa chcú zamerať na audity riadenia rizík.
Každý, kto sa chce dozvedieť viac o analýze a riadení rizík.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o analýze a riadení rizík: Školenie pokrýva širokú škálu tém relevantných pre efektívne riadenie rizík. Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty analýzy a riadenia rizík a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi. Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti a zručnosti v oblasti analýzy a riadenia rizík. Networking: Školenie umožňuje účastníkom nadviazať kontakty s ostatnými profesionálmi v oblasti riadenia rizík.

NAKIB

ŠKOLENIA

Manažér pre riadenie kontinuity činností

RIADENIE BCM PODĽA ISO 22301 A ISO 22313. VYKONANIE ANALÝZY OBCHODNÉHO DOPADU PODĽA ISO 22317, PRÍPRAVA A TESTOVANIE PLÁNOV OBNOVY

Čo je?

Školenie Manažér pre riadenie kontinuity činností je komplexný program, ktorý rozvíja znalosti a zručnosti potrebné na efektívne riadenie kontinuity činností v organizácii. Školenie sa zameriava na rôzne aspekty riadenia kontinuity činností, ako napríklad: Identifikácia rizík: Rozpoznanie a analýza rizík, ktoré by mohli narušiť chod organizácie. Plánovanie kontinuity: Vytváranie a implementácia plánu kontinuity činností, ktorý zaistí fungovanie organizácie aj v prípade neočakávaných udalostí. Testovanie a cvičenie plánu: Pravidelné testovanie a cvičenie plánu kontinuity činností pre zaistenie jeho efektívnosti. Komunikácia a koordinácia: Zaistenie efektívnej komunikácie a koordinácie medzi rôznymi oddeleniami a zainteresovanými stranami v rámci riadenia kontinuity činností. Udržiavanie a aktualizácia plánu: Pravidelné aktualizácie plánu kontinuity činností v súlade s aktuálnymi podmienkami a potrebami organizácie.

Prečo?

Absolvovanie školenia Manažér pre riadenie kontinuity činností prináša viacero benefitov:
Zvýšenie odolnosti organizácie: Získanie znalostí a zručností potrebných na efektívne riadenie kontinuity činností a zaistenie fungovania organizácie aj v prípade neočakávaných udalostí. Zníženie finančných strát: Predchádzanie a minimalizácia dopadov výpadkov a narušení chodu organizácie. Posilnenie dôvery a reputácie: Demonštrovanie záväzku k kontinuite činností posilňuje dôveru zákazníkov, partnerov a regulačných orgánov v organizáciu. Zlepšenie súladu s regulačnými požiadavkami: Mnoho regulačných požiadaviek vyžaduje od organizácií implementáciu systému riadenia kontinuity činností. Zvýšenie produktivity: Zníženie prestojov a rýchle obnovenie chodu organizácie po neočakávaných udalostiach.

Pre koho?

Školenie Manažér pre riadenie kontinuity činností je určené pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za riadenie kontinuity činností v organizácii. IT profesionálov: Ktorí sa chcú špecializovať na oblasť riadenia kontinuity činností. Osoby zodpovedné za krízové manažment: V rámci organizácie. Audítorov: Ktorí sa chcú zamerať na audity riadenia kontinuity činností. Každý, kto sa chce dozvedieť viac o riadení kontinuity činností.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o riadení kontinuity činností: Školenie pokrýva širokú škálu tém relevantných pre efektívne riadenie kontinuity činností. Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty riadenia kontinuity činností a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi. Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti a zručnosti v oblasti riadenia kontinuity činností. Networking: Školenie umožňuje účastníkom nadviazať kontakty s ostatnými profesionálmi v oblasti riadenia kontinuity činností.

APLIKOVANIE ZÁKONA O ITVS, BEZPEČNOSTNÝ PROJEKT, ZÁKLADY SDLC, VYKONANIE ANALÝZY RIZÍK

Čo je?

Školenie Znalosti Zákona o informačných technológiách vo verejnej správe 95/2019 je komplexný program, ktorý rozvíja znalosti a zručnosti relevantné pre pochopenie a dodržiavanie Zákona o informačných technológiách vo verejnej správe (ZITVS) č. 95/2019 Z. z. Školenie sa zameriava na rôzne aspekty ZITVS, ako napríklad: Povinnosti a práva: Pochopenie povinností a práv verejných subjektov v súvislosti s informačnými technológiami. Informačné systémy: Kategorizácia a riadenie informačných systémov vo verejnej správe. Kybernetická bezpečnosť: Implementácia a dodržiavanie bezpečnostných opatrení v súlade s ZITVS. Ochrana osobných údajov: Pochopenie a dodržiavanie GDPR v kontexte ZITVS. Elektronické služby: Poskytovanie elektronických služieb verejnej správy v súlade s ZITVS. Zadávanie zákaziek: Pochopenie procesov zadávania zákaziek na informačné technológie vo verejnej správe.

Prečo?

Absolvovanie školenia Znalosti Zákona o informačných technológiách vo verejnej správe 95/2019 prináša viacero benefitov: Zvýšenie informovanosti: Získanie komplexného prehľadu o požiadavkách ZITVS a relevantných legislatívnych predpisov. Zníženie rizík: Predchádzanie sankciám a pokutám za nedodržiavanie ZITVS. Zvýšenie efektivity: Zlepšenie riadenia informačných technológií vo verejnej správe.Zvýšenie kybernetickej bezpečnosti: Posilnenie ochrany informačných systémov a dát pred kybernetickými hrozbami. Zlepšenie kvality elektronických služieb: Poskytovanie kvalitných a dostupných elektronických služieb pre občanov.

Pre koho?

Školenie Znalosti Zákona o informačných technológiách vo verejnej správe 95/2019 je určené pre: Zamestnancov verejnej správy: Ktorí sa podieľajú na riadení informačných technológií, kybernetickej bezpečnosti, ochrane osobných údajov, či poskytovaní elektronických služieb. Vedúcich pracovníkov: Zodpovedných za dodržiavanie ZITVS v rámci svojej organizačnej jednotky. IT profesionálov: Ktorí sa chcú špecializovať na oblasť informačných technológií vo verejnej správe. Právnikov: Ktorí sa venujú právnym aspektom informačných technológií a verejnej správy. Každý, kto sa chce dozvedieť viac o ZITVS a jeho dopade na verejnú správu.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy: Získanie komplexného prehľadu o ZITVS: Školenie pokrýva širokú škálu tém relevantných pre pochopenie a dodržiavanie ZITVS. Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty implementácie ZITVS a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi. Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti o ZITVS. Networking: Školenie umožňuje účastníkom nadviazať kontakty s ostatnými profesionálmi v oblasti informačných technológií vo verejnej správe.

NAKIB

ŠKOLENIA

Požiadavky v oblasti ochrany OÚ GDPR

POŽIADAVKY EU REGULÁCIE PRE OCHRANU OSOBNÝCH ÚDAJOV PODĽA GDPR NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679

Čo je?

Školenie Požiadavky v oblasti ochrany osobných údajov v zmysle požiadaviek nariadenia GDPR je komplexný program, ktorý rozvíja znalosti a zručnosti relevantné pre pochopenie a dodržiavanie GDPR (General Data Protection Regulation). Školenie sa zameriava na rôzne aspekty GDPR, ako napríklad: Základné pojmy: Definícia a pochopenie kľúčových pojmov GDPR ako sú osobné údaje, dotknutá osoba, prevádzkovateľ, sprostredkovateľ, súhlas a podobne.Povinnosti prevádzkovateľa: Pochopenie a implementácia povinností prevádzkovateľa v súvislosti so spracovaním osobných údajov, ako sú princípy spracovania, práva dotknutej osoby, technické a organizačné opatrenia a podobne. Práva dotknutej osoby: Pochopenie a implementácia práv dotknutej osoby, ako je právo na prístup k informáciám, právo na opravu, právo na vymazanie a podobne. Spracovanie osobných údajov: Praktické aspekty spracovania osobných údajov v rôznych kontextoch, ako je napríklad spracovanie osobných údajov v marketingu, v e-shope, v kamerovom systéme a podobne. Dokumentačné povinnosti: Pochopenie a implementácia dokumentačných povinností prevádzkovateľa, ako je vedenie záznamov o spracovateľských činnostiach, posudzovanie vplyvu na ochranu osobných údajov a podobne. Sankcie: Pochopenie a prevencia sankcií za porušenie GDPR.

Prečo?

Absolvovanie školenia Požiadavky v oblasti ochrany osobných údajov v zmysle požiadaviek nariadenia GDPR prináša viacero benefitov: Zvýšenie informovanosti: Získanie komplexného prehľadu o požiadavkach GDPR a relevantných legislatívnych predpisov. Zníženie rizík: Predchádzanie sankciám a pokutám za nedodržiavanie GDPR. Posilnenie dôvery: Demonštrovanie záväzku k ochrane osobných údajov a budovanie dôvery klientov, partnerov a regulačných orgánov. Zlepšenie reputácie: Prezentácia organizácie ako zodpovednej a transparentnej v oblasti ochrany osobných údajov. Zvýšenie efektivity: Zlepšenie procesov spracovania osobných údajov a minimalizácia administratívnej záťaže.

Pre koho?

Školenie Požiadavky v oblasti ochrany osobných údajov v zmysle požiadaviek nariadenia GDPR je určené pre: Zamestnancov: Ktorí sa podieľajú na spracovaní osobných údajov v rôznych oddeleniach, ako napríklad v marketingu, v HR, v IT, v obchodnom oddelení a podobne. Vedúcich pracovníkov: Zodpovedných za dodržiavanie GDPR v rámci svojej organizačnej jednotky.Manažérov: Ktorí potrebujú strategický prehľad o GDPR a jeho dopade na fungovanie organizácie. IT profesionálov: Ktorí sa chcú špecializovať na oblasť ochrany osobných údajov. Právnikov: Ktorí sa venujú právnym aspektom ochrany osobných údajov. Každý, kto sa chce dozvedieť viac o GDPR a jeho dopade na jednotlivcov a organizácie.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o GDPR: Školenie pokrýva širokú škálu tém relevantných pre pochopenie a dodržiavanie GDPR. Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty implementácie GDPR a umožňuje účastníkom aplikovať nadobudnuté znalosti.

ZÁKLADNÉ TECHNIKY HACKERSKÝCH ÚTOKOV

Čo je?

Školenie Základy hackingu je komplexný program, ktorý rozvíja znalosti a zručnosti relevantné pre pochopenie a simuláciu techník používaných hackermi. Školenie sa zameriava na rôzne aspekty hackingu, ako napríklad: Typy hackerov: Úvod do rôznych typov hackerov a ich motívov. Metódy hackovania: Pochopenie a simulácia rôznych metód hackovania, ako sú phishing, social engineering, SQL injection, XSS a podobne. Sieťová bezpečnosť: Základy sieťovej bezpečnosti a zraniteľnosti, ako napríklad sniffing, spoofing, denial-of-service attacks a podobne. Penetračné testovanie: Úvod do penetračného testovania a jeho využitia pri identifikácii a zmierňovaní zraniteľností. Bezpečnosť webu: Zraniteľnosti webových aplikácií a metódy ich zneužitia. Kryptografia: Základy kryptografie a jej využitie pri ochrane dát. Etika hackingu: Dôležitosť etického prístupu k hackingu a zodpovedného používania získaných znalostí.

Prečo?

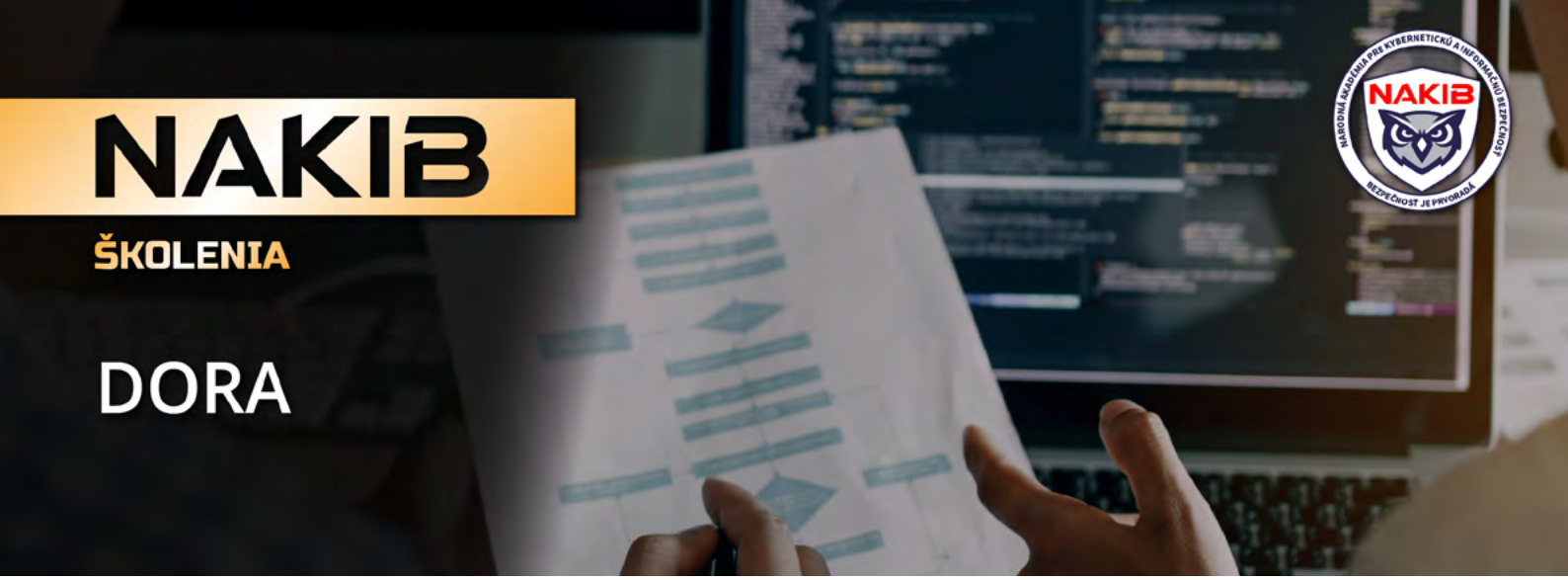
Absolvovanie školenia Základy hackingu prináša viacero benefitov:
Zvýšenie povedomia o kybernetických hrozbách: Získanie komplexného prehľadu o rôznych technikách hackovania a metódach ochrany pred nimi. Zlepšenie kybernetickej bezpečnosti: Posilnenie obranyschopnosti organizácie voči kybernetickým útokom. Rozvoj analytických a logických zručností: Tréning v identifikácii a riešení bezpečnostných zraniteľností. Zvýšenie kariérnych príležitostí: Získanie znalostí a zručností relevantných pre rôzne profesie v oblasti kybernetickej bezpečnosti. Posilnenie pocitu kontroly: Získanie nástrojov a techník na ochranu osobných dát a zariadení pred hackermi.

Pre koho?

Školenie Základy hackingu je určené pre:
IT profesionálov: Ktorí sa chcú špecializovať na oblasť kybernetickej bezpečnosti.
Začínajúcich hackerov: Ktorí sa chcú eticky naučiť techniky používané hackermi.
Študentov informatiky: Ktorí sa chcú dozvedieť viac o kybernetických hrozbách a ich riešení.
Manažérov a vedúcich pracovníkov: Zodpovedných za kybernetickú bezpečnosť v organizácii.
Každý, kto sa chce dozvedieť viac o hackingu a ochrane pred ním.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o hackingu: Školenie pokrýva širokú škálu tém relevantných pre pochopenie rôznych techník hackovania. Rozvoj praktických zručností: Školenie sa zameriava na simuláciu techník hackovania v bezpečnom prostredí a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi.
Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti o hackingu. Networking: Školenie umožňuje účastníkom nadviazať kontakty s ostatnými profesionálmi v oblasti kybernetickej bezpečnosti.



PORADENSTVO V OBLASTI PRÍPRAVY NA MEDZINÁRODNÉHO ŠTANDARDU DORA PRE FINANČNÉ SLUŽBY

Čo je?

Školenie DORA (Digital Operational Resilience Act) je komplexný program, ktorý rozvíja znalosti a zručnosti relevantné pre implementáciu a dodržiavanie nariadenia DORA o digitálnej prevádzkovej odolnosti. Školenie sa zameriava na rôzne aspekty DORA, ako napríklad: Požiadavky nariadenia: Podrobné pochopenie požiadaviek nariadenia DORA, vrátane definície kľúčových pojmov, identifikovaných rizík a povinností regulovaných subjektov. Riadenie rizík ICT: Implementácia a udržiavanie efektívneho systému riadenia rizík v oblasti informačných a komunikačných technológií (ICT) v súlade s DORA. Incident manažment: Pochopenie a implementácia procesov riadenia incidentov ICT v súlade s požiadavkami DORA. Testovanie odolnosti: Plánovanie a realizácia testovania odolnosti ICT infraštruktúry a systémov v súlade s DORA. Dohľad a reporting: Pochopenie a dodržiavanie požiadaviek na dohľad a reporting v súvislosti s DORA. Technické aspekty: Praktické znalosti o technických riešeniach relevantných pre implementáciu DORA, ako napríklad cloudové technológie.

Prečo?

Absolvovanie školenia DORA prináša viacero benefitov:
Zvýšenie odolnosti voči ICT hrozbám: Získanie znalostí a zručností potrebných na efektívne riadenie rizík a budovanie odolnosti voči ICT hrozbám v súlade s DORA. Zníženie rizika sankcií: Predchádzanie sankciám za nedodržiavanie nariadenia DORA. Posilnenie dôvery a reputácie: Demonštrovanie záväzku k digitálnej prevádzkovej odolnosti a budovanie dôvery klientov, partnerov a regulačných orgánov. Zlepšenie súladu s regulačnými požiadavkami: DORA nadväzuje na existujúce regulačné požiadavky v oblasti ICT a jej implementácia prispieva k celkovému súladu. Zvýšenie efektivity a produktivity: Zníženie prestojov a výpadkov ICT systémov a zlepšenie celkovej efektivity prevádzky.

Pre koho?

Školenie DORA je určené pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za implementáciu a dodržiavanie DORA v rámci svojej organizačnej jednotky. IT profesionálov: Ktorí sa podieľajú na riadení ICT rizík, incidente manažmente, testovaní odolnosti a dodržiavaní požiadaviek DORA. Audítorov: Ktorí sa chcú zamerať na audity DORA a digitálnej prevádzkovej odolnosti. Právnikov: Ktorí sa venujú právnym aspektom DORA a regulácie ICT. Každý, kto sa chce dozvedieť viac o DORA a jej dopade na rôzne sektory.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o DORA: Školenie pokrýva širokú škálu tém relevantných pre pochopenie a implementáciu nariadenia DORA. Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty implementácie DORA a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi. Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti o DORA. Networking: Školenie umožňuje účastníkom nadviazať kontakty s ostatnými profesionálmi v oblasti digitálnej prevádzkovej odolnosti.

ŠKOLENIE O APLIKOVANÍ ZÁKONA O UTAJOVANÝCH SKUTOČNOSTIACH 215/2004

Čo je?

Školenie Zákon o utajovaných skutočnostiach 215/2004 Z. z.
Čo to znamená: Školenie Zákon o utajovaných skutočnostiach 215/2004 Z. z. (ZUOS) je komplexný program, ktorý rozvíja znalosti a zručnosti relevantné pre pochopenie a dodržiavanie ZUOS. Školenie sa zameriava na rôzne aspekty ZUOS, ako napríklad: Definícia utajovanej skutočnosti: Pochopenie a identifikácia informácií a vecí, ktoré sa považujú za utajované v súlade s ZUOS. Stupne utajenia: Rozlišovanie medzi rôznymi stupňami utajenia (prísne tajné, tajné, chránené) a ich dopad na manipuláciu s utajovanými skutočnosťami. Povinnosti a práva: Pochopenie a dodržiavanie povinností a práv subjektov, ktoré prichádzajú do styku s utajovanými skutočnosťami. Manipulácia s utajovanými skutočnosťami: Praktické aspekty nakladania s utajovanými informáciami a materiálmi, ako napríklad ich spracovanie, uchovávanie, prenos a likvidácia. Ochrana utajovaných skutočností: Implementácia bezpečnostných opatrení na ochranu utajovaných skutočností pred neoprávneným zneužitím, vyzradením alebo poškodením. Dohľad a sankcie: Pochopenie systému dohľadu nad dodržiavaním ZUOS a sankcií za jeho porušenie.

Prečo?

Absolvovanie školenia Zákon o utajovaných skutočnostiach 215/2004 Z. z. prináša viacero benefitov:
Zvýšenie informovanosti: Získanie komplexného prehľadu o požiadavkách ZUOS a relevantných legislatívnych predpisov. Zníženie rizík: Predchádzanie sankciám a pokutám za nedodržiavanie ZUOS. Ochrana citlivých informácií: Zabezpečenie ochrany utajovaných informácií a materiálov pred neoprávneným prístupom. Posilnenie dôvery a reputácie: Demonštrovanie záväzku k ochrane utajovaných informácií a budovanie dôvery klientov, partnerov a regulačných orgánov. Zvýšenie efektivity: Zlepšenie procesov manipulácie s utajovanými informáciami a minimalizácia administratívnej záťaže.

Pre koho?

Školenie Zákon o utajovaných skutočnostiach 215/2004 Z. z. je určené pre:
Zamestnancov: Ktorí prichádzajú do styku s utajovanými informáciami a materiálmi v rôznych oddeleniach, ako napríklad v štátnej správe, v armáde, v bezpečnostných zložkách, v strategických podnikoch a podobne. Vedúcich pracovníkov: Zodpovedných za dodržiavanie ZUOS v rámci svojej organizačnej jednotky. Manažérov informačnej bezpečnosti: Ktorí sa podieľajú na implementácii a udržiavaní systému ochrany utajovaných informácií. Právnikov: Ktorí sa venujú právnym aspektom ochrany utajovaných informácií. Každý, kto sa chce dozvedieť viac o ZUOS a jeho dopade na rôzne sektory.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o ZUOS: Školenie pokrýva širokú škálu tém relevantných pre pochopenie a dodržiavanie ZUOS. Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty implementácie ZUOS a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi. Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti o ZUOS. Networking: Školenie umožňuje účastníkom nadviazať kontakt s ostatnými profesionálmi z rôznych oblastí.

ŠKOLENIE O VYUŽÍVANÍ AI – UMELEJ INTELIGENCIE V PRAXI

Čo je?

Školenie AI - Umelá inteligencia je komplexný program, ktorý rozvíja znalosti a zručnosti relevantné pre pochopenie a využitie umelej inteligencie (AI) v rôznych oblastiach. Školenie sa zameriava na rôzne aspekty AI, ako napríklad: Základné pojmy: Definícia a pochopenie kľúčových pojmov AI, ako sú strojové učenie, hlboké učenie, neurónové siete, algoritmy a podobne. Typy AI: Rozdelenie AI na rôzne typy (reaktívna, limitovaná pamäťou, teória mysle), ich vlastnosti a príklady využitia. Využitie AI: Praktické aplikácie AI v rôznych sektoroch, ako napríklad v medicíne, financiách, marketingu, výrobe, doprave a podobne. Etické aspekty: Dôležitosť etického prístupu k AI a zodpovedného používania jej technológií. Budúcnosť AI: Trendy a očakávaný vývoj v oblasti AI v najbližších rokoch.

Prečo?

Absolvovanie školenia AI - Umelá inteligencia prináša viacero benefitov:
Zvýšenie informovanosti: Získanie komplexného prehľadu o rôznych aspektoch AI a jej potenciáli. Zlepšenie konkurencieschopnosti: Získanie znalostí a zručností potrebných pre implementáciu a využitie AI v rôznych oblastiach a posilnenie konkurencieschopnosti na trhu. Zvýšenie efektivity: Automatizácia a optimalizácia procesov pomocou AI a zníženie administratívnej záťaže. Inovácia: Podpora inovatívnych riešení a produktov s využitím AI. Zlepšenie rozhodovania: Využitie AI pre analýzu dát a podporu informovaného a strategického rozhodovania.

Pre koho?

Školenie AI - Umelá inteligencia je určené pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za strategické plánovanie a implementáciu AI v rámci svojej organizačnej jednotky. IT profesionálov: Ktorí sa chcú špecializovať na oblasť AI a strojového učenia. Podnikateľov: Ktorí chcú využiť AI pre rast a inováciu svojho podnikania. Študentov informatiky: Ktorí sa chcú dozvedieť viac o AI a jej potenciálnom využití v praxi. Každý, kto sa chce dozvedieť viac o AI a jej dopade na rôzne sektory.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o AI: Školenie pokrýva širokú škálu tém relevantných pre pochopenie rôznych aspektov AI. Rozvoj praktických zručností: Školenie sa zameriava na praktické aplikácie AI a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi. Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti o AI. Networking: Školenie umožňuje účastníkom nadviazať kontakty s ostatnými profesionálmi v oblasti AI.

ŠPECIFICKÝ PRÍSTUP RIADENIA INFORMAČNEJ A KYBERNETICKEJ BEZPEČNOSTI VO VÝROBNÝCH SPOLOČNOSTIACH

Čo je?

Školenie Kybernetická bezpečnosť v OT prostredí je komplexný program, ktorý rozvíja znalosti a zručnosti relevantné pre ochranu operačných technológií (OT) pred kybernetickými hrozbami. Školenie sa zameriava na rôzne aspekty kybernetickej bezpečnosti v OT prostredí, ako napríklad: Základné pojmy: Definícia a pochopenie kľúčových pojmov kybernetickej bezpečnosti v OT prostredí, ako sú SCADA systémy, ICS systémy, hrozby, zraniteľnosti a riziká. Typy kybernetických hrozieb: Rozdelenie kybernetických hrozieb relevantných pre OT prostredie (malware, phishing, DDoS útoky, zero-day útoky) a ich dopad na OT systémy. Ochrana OT infraštruktúry: Implementácia a udržiavanie bezpečnostných opatrení pre OT infraštruktúru, ako napríklad sieťová segmentácia, firewally, autentifikácia a autorizácia. Riadenie rizík: Identifikácia, analýza a riadenie rizík kybernetickej bezpečnosti v OT prostredí. Incident manažment: Pochopenie a implementácia procesov riadenia incidentov kybernetickej bezpečnosti v OT prostredí. Dodržiavanie regulácií: Pochopenie a dodržiavanie regulačných požiadaviek na kybernetickú bezpečnosť v OT prostredí.

Prečo?

Absolvovanie školenia Kybernetická bezpečnosť v OT prostredí prináša viacero benefitov:
Zvýšenie informovanosti: Získanie komplexného prehľadu o kybernetických hrozbách a rizikách v OT prostredí.
Zníženie rizík: Predchádzanie kybernetickým útokom a minimalizácia ich dopadu na OT systémy a prevádzku. Zvýšenie odolnosti: Posilnenie odolnosti OT infraštruktúry voči kybernetickým hrozbám. Zabezpečenie kontinuity prevádzky: Zníženie prestojov a výpadkov OT systémov v dôsledku kybernetických útokov. Dodržiavanie regulácií: Zabezpečenie súladu s regulačnými požiadavkami na kybernetickú bezpečnosť v OT prostredí.

Pre koho?

Školenie Kybernetická bezpečnosť v OT prostredí je určené pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za kybernetickú bezpečnosť v OT prostredí.
IT profesionálov: Ktorí sa podieľajú na správe a zabezpečení OT infraštruktúry.
Prevádzkových inžinierov: Ktorí pracujú s OT systémami a zariadeniami.
Audítorov: Ktorí sa venujú auditu kybernetickej bezpečnosti v OT prostredí.
Každý, kto sa chce dozvedieť viac o kybernetickej bezpečnosti v OT prostredí.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Získanie komplexného prehľadu o kybernetickej bezpečnosti v OT prostredí: Školenie pokrýva širokú škálu tém relevantných pre pochopenie a riešenie kybernetických hrozieb v OT prostredí.
Rozvoj praktických zručností: Školenie sa zameriava na praktické aspekty kybernetickej bezpečnosti v OT prostredí a umožňuje účastníkom aplikovať nadobudnuté znalosti v praxi. Získanie certifikátu: Po úspešnom absolvovaní školenia účastníci získajú certifikát, ktorý dokazuje ich znalosti o kybernetickej bezpečnosti v OT prostredí. Networking: Školenie umožňuje účastníkom nadviazať kontakty s ostatnými profesionálmi v oblasti kybernetickej bezpečnosti v OT prostredí.