OBJEDNÁVKA

Strana: 1 / 3

Ev. číslo dokladu: **4823**

Datum vystavení: 14.03.2023

Odběratel

Moravskoslezské datové centrum, příspěvková organizace
Na Jízdárně 2824/2
702 00 Ostrava
Česká republika

IČ: 06839517

Kontaktní údaje

Vyřizuje: **Lenka Vaňková**
E-mail: lenka.vankova@msdc.cz
Telefon: 603 112 427
Fax:
Web: www.msdc.cz

Ostatní údaje

Forma úhrady: Převodem
Způsob dopravy: Online dodání produktu
Termín vyřízení: 30.04.2023

Dodavatel

MILOSLAV URBIŠ
Třebovická 5144 / 52
722 00 Ostrava - Třebovice - Třebovice

IČ: 71770810 DIČ: CZ6908105556

E-mail:
Telefon:
Fax:

Objednáváme u Vás

školení ARCHITEKT KYBERNETICKÉ BEZPEČNOSTI pro zaměstnance MSDC (5-10 osob).
V termínech: 17.3.2023, 31.3.2023, 14.4.2023, 28.4.2023

Kurz je zaměřen na návrh, implementaci a rozvoj informační architektury v rámci organizační bezpečnosti. Obsahem kurzu je navrhovat a zavádět bezpečnostní opatření v rámci zajišťování architektury bezpečnosti organizace s vazbou na zákon o kybernetické bezpečnosti č. 181/2014 Sb. a vyhlášky č. 82/2018 Sb.
Toto školení je primárně určeno pro roli Architekta kybernetické bezpečnosti (AKB). Tato role (AKB) navrhuje bezpečnostní architektury informačních systémů, jejich jednotlivé komponenty, vzájemné vazby a dohlíží na soulad implementace architektury informačních systémů se systémem řízení bezpečnosti informací. Navrhuje případně způsoby dalšího rozvoje řízení informační bezpečnosti jako podklad pro rozhodování managementu organizace a jejich vlastníků.

Úvod do ZoKB a managementu rizik
1. Požadavky zákona na KII
2. Zákony, směrnice a normy pro KII
3. Role architekta
4. Zavádění ISMS a ISO 27001 v organizaci s KII
5. Kritická infrastruktura a významné informační systémy
6. Fyzická bezpečnost objektů v KII
7. Analýza rizik a zvládání rizik v KII
8. Návaznost opatření analýzu rizik
9. Správa a management aktiv KII
10. Řízení dodavatelů

Identity a kontrola přístupu
1. Používání identit ve Windows a Active Directory
2. Používání identit v Linuxu
3. Řízení identity uživatelů pomocí centralizovaných IDM
4. Řízení přístupu a bezpečné chování uživatelů
5. Řízení přístupu ke zdrojům operačního systému
6. Řízení přístupu k databázím
7. Správa Hesel

8. Implementace 2FA
9. Zranitelnosti 2FA

Zabezpečení klientů
1. Antivirus a AntiMalware
2. Next Generation antiviry
3. Data Lost Prevention systémy
4. Správa certifikátů na klientech
5. Šifrování disků a USB - Bitlocker a EFS
6. Zabezpečení e-mailové a webové komunikace

Logování a audit
1. Logování ve Windows
2. Logování v Linuxu
3. Logování v aplikacích
4. Typické logovací mechanismy
5. Definice požadavku na zaznamenávání činnosti dle ZKB
6. Požadavky na přesný čas
7. Logování přístupu a práce se síťovými prvky
8. Logování na úrovni operačních systémů a na úrovni aplikací
9. Centrální nástroje pro sběr logů a vyhodnocování událostí
10. Popis základní funkcionality SIEM

Bezpečnost vývoje a aplikací
1. Srovnání různých architektur aplikací
2. Zranitelnost aplikací
3. Akvizice, vývoj a údržba
4. Principy bezpečného vývoje softwaru
5. System Development Life Cycle
6. Testování vyvíjených aplikací
7. Využívání jednotných šablon pro automatizaci a správu

Architektura sítě
1. Next Generation Firewally
2. Next Generation Intrusion Prevention Systemy
3. DDoS - podstata útoku a způsoby ochrany
4. Principy L2 a L3 segmentace sítě
5. Principy vytváření DMZ
6. Slučování a určování aplikaci do VLAN
7. Implementace VPN a detekce KBU / KBI
8. Síťový a aplikační pohled

Síťová bezpečnost
1. Základní pravidla pro L2 a L3 design sítě
2. Principy L2 útoků
3. Útoky MitM využívající ARP
4. Útoky na SPT (Spanning Tree)
5. Útoky na VLAN
6. Útoky na směrovací protokoly L3
7. Doporučení pro konfiguraci přepínačů - řízení přístupu

Detekce a monitoring narušení
1. Požadavky na nepřetržité vyhodnocování KBU
2. Behaviorální analýza síťového provozu
3. Implementace a nasazení SIEM
4. Analýza zjištěných KBU
5. Vyhodnocování a reakce na KBU

Zajišťování vysoké dostupnosti

Ev. číslo dokladu: **4823**

Datum vystavení: 14.03.2023

1. Metody analýzy pro business kontinuitu
2. Požadavky na návrh vysoce dostupných systémů
3. Vysoká dostupnost v praxi
4. Vysoká dostupnost pro systémy řízení a systémy pracující v reálném čase
5. Návaznosti na analýzy business kontinuity
6. Support / Servis
7. SLA pro zajištěný vysoké dostupnosti
8. Náhradní díly

Cena za souhrnné č denní školení činí 70.000,- bez DPH.

-Uvedená cena je nevyšší přípustná-
Objednávka schválena a zkontrolována:
Správce rozpočtu: Mgr. Zuzana Konečná
Datum:
Podpis: 14. 03. 2023 [redacted]

Celkem k úhradě: **84 700,00 Kč**

Příkazce operace: Ing. RNDr. Alois Slovák
Datum:
Podpis: 14. 03. 2023 [redacted]

Na Jízdárně 2824/2
Moravská Ostrava
702 00 Ostrava
IČ: 06839517
www.msdc.cz

Razítko a podpis