hillel IT school

детальніше про курс

Курс Cybersecurity Manager Online

BASIC LEVEL

20 занять 2 заняття на тиждень

ВИВЧАЄМО ТАКІ ТЕХНОЛОГІЇ

ПРОГРАМА КУРСУ

1. Головні програми комплаєнсу в сфері кібербезпеки

- ISO 27001/27002, 27701, GDPR
- SOC2
- NIS2
- NIST CSF
- Фінансова індустрія: PCI DSS, SOC1, SOX, OSPAR
- Автомотів індустрія: VDA ISA / ENX TISAX, ISO 21434, VW KGAS, ASPICE
- Промислова кібербезпека: ISA 62443
- Українське законодавство та система НД ТЗІ

2. Керування інформаційною безпекою

- Організаційна культура
- Договірні та юридичні вимоги
- Структура організації, ролі та відповідальність
- Розробка стратегії інформаційної безпеки
- SoA та скоуп ISMS

- Внутрішні та зовнішні фактори, цілі безпеки
- Планування ресурсів (люди, інструменти, технології)
- Вимірювання ефективності, метрики
- Покращення
- Внутрішнє та зовнішнє оцінювання та аудити
- Звітність перед керівництвом
- Взаємодія з профільними групами

---

3. Керування ризиками інформаційної безпеки

- Ландшафт ризиків та загроз
- Аналіз та оцінка ризиків
- Обробка ризиків, стратегії реагування
- Володіння ризиками та відповідальність
- Моніторинг ризиків та звітність
- Моделювання загроз

---

4. Управління інцидентами

- Процедура управління інцидентами, ролі та відповідальність
- Стратегії реагування на інциденти
- План реагування
- Класифікація та категорії інцидентів
- Звітність
- Взаємодія з командами швидкого реагування
- Комп’ютерні методи розслідування інцидентів

---

5. Управління інформаційними активами

- Типи активів
- Класифікація даних та активів
- Методи обробки даних в залежності від рівня класифікації
- Видача та повернення активів
- Безпечне видалення інформації
- Життєвий цикл даних
- Захист персональних даних
- Вимоги до захисту даних для хмарних та онпрем активів

- Інтелектуальна власність

---

6. Неперервність бізнесу та відновлення після збоїв

- BIA
- BCP
- DRP
- Аналіз BCP-ризиків
- Симуляція атак та збоїв

---

7. Політики та процедури інформаційної безпеки

- Обов’язкові та рекомендовані документи
- Вимоги та типи документів
- Правила роботи з документами
- Воркфлоу документів — створення, перевірка, погодження
- Ведення історії версій
- Ролі та відповідальність

---

8. Мережева безпека

- Мережева архітектура
- Сегрегація підмереж
- Міжмережеві екрани, WAF
- Логування та моніторинг
- IDS/IPS, DLP, SIEM
- Канали безпечної комунікації

---

9. Управління доступом

- Принцип мінімально необхідних повноважень
- Ревью доступів
- Привілейований доступ (PAM)
- Фізичний та логічний доступ до активів
- Ідентифікація та аутентифікація користувачів та пристроїв
- Моделі контролю доступу
- SSO, MFA

---

10. Управління вразливостями

- Сканування на вразливості — методики та інструментарій
- Зовнішні пентести
- Оцінка ризиків, пріоритети, CVSS
- Вимоги до звітів
- Взаємодія з командою щодо закриття вразливостей
- Прозорість процесу закриття вразливостей для зовнішніх аудиторів
- Повторне тестування та моніторинг

---

11. Операційна безпека

- Управління змінами
- Централізований захист від вірусів та шкідливого ПЗ
- Парольний захист
- Криптографія, FDE, ЕЦП, ключи та сертифікати
- Резервне копіювання
- Управління потужністю та резервуванням

---

12. Безпечний життєвий цикл розробки програмного забезпечення

- Моделі та фреймворки SSDLC
- Вимоги з безпеки на всіх стадіях життєвого циклу розробки ПЗ
- Безпечна архітектура ПЗ та принципи безпечної розробки
- Правила безпечного кодування
- Сегрегація середовищ
- SAST, DAST, SCA
- Управління патчами
- Код ревью
- Аудіт безпеки коду
- Тестування вимог з безпеки
- Управління конфігураціями

---

13. Фізична безпека

- Принцип зонування та вимоги з безпеки до різних зон
- СКУД, охорона, пожежна безпека, відеоспостереження
- Кондиціонування серверних приміщень
- Вимоги з безпеки до пристроїв

- Політика BYOD
- MDM
- Транспортування та утилізація обладнання
- Оновлення та обслуговування обладнання

14. Безпека персоналу

- Онбордінг чекліст
- Вимоги до NDA
- Взаємодія з IT — відкриття та закриття акаунтів, призначення прав доступу, видача активів
- Бекграунд чек
- Офбоардінг чекліст
- Тренінги, навчання
- AUP, дистанційна робота
- Дисциплінарний процес

15. Керування ланцюгом поставок (SCM)

- Класифікація та реєстр постачальників
- Аналіз ризиків постачальників
- Вимоги з кібербезпеки до постачальників
- Критичні функції
- Аудит та моніторинг постачальників

БОНУСИ КУРСУ

Всі студенти курсу пройдуть
тренінг по проходженню
співбесіди та складанню резюме
з нашим HR-фахівцем