hillel IT school

Курс **Cybersecurity Engineering** Online

BASIC LEVEL

24 заняття 2 заняття на тиждень

детальніше про курс

ПРОГРАМА КУРСУ

1. Introduction to Cybersecurity

Напрямки кібербезпеки, ролі спеціалістів, типи загроз, CIA Triad.

2. Networking Fundamentals

TCP/IP, DNS, HTTP/HTTPS, порти, маршрутизація.

3. Operating Systems Security

Основи Windows і Linux, користувачі, права доступу.

4. Security Fundamentals

Аутентифікація, авторизація, MFA, принцип найменших привілеїв.
Практика: аналіз мережевої конфігурації, створення користувачів і налаштування прав доступу в тестовій системі.

5. Linux Administration

Файлова система, термінал, процеси, служби.

6. Linux Security

Права доступу, SSH, журнали подій, оновлення.

7. Network Security

Firewall, сегментація мереж, VPN, мережеві політики.

8. Network Monitoring

Wireshark, аналіз мережевих пакетів, виявлення аномалій.
Практика: налаштування тестової Linux-системи й аналіз мережевого трафіку навчального середовища.

9. Introduction to SOC

Функції SOC, L1/L2/L3, процеси моніторингу.

10. Log Management

Системні журнали, типи подій, збір і зберігання логів.

11. SIEM Fundamentals

Архітектура SIEM, кореляція подій, правила моніторингу.

12. Incident Detection

Аналіз сповіщень, пріоритизація і класифікація інцидентів.
Практика: робота з навчальними логами, створення простих правил виявлення підозрілих подій.

13. Web Security Fundamentals

HTTP, cookies, sessions, authentication.

14. OWASP Top 10

Основні категорії вразливостей вебзастосунків.

15. Secure Coding

Безпечна обробка даних, валідація, керування секретами.

16. Security Testing

Методологія перевірки безпеки власного тестового застосунку.
Практика: аналіз спеціально підготовленого вразливого навчального застосунку й підготовка рекомендацій щодо усунення проблем.

17. Cloud Security Fundamentals

Хмарна інфраструктура, моделі відповідальності.

18. Identity & Access Management

IAM, ролі, політики доступу.

19. Infrastructure Monitoring

Моніторинг ресурсів, журнали та сповіщення.

20. Security Best Practices

Backup, patch management, vulnerability management.
Практика: аудит конфігурації тестового хмарного середовища й формування рекомендацій.

---

21. Incident Response

Життєвий цикл реагування на інциденти.

---

22. Digital Forensics Fundamentals

Збереження доказів, робота з копіями журналів, базовий аналіз.

---

23. Final Project Workshop

Робота над фінальним проєктом.

---

24. Final Project Defense

Презентація і захист результатів.
Фінальний проєкт: Security Monitoring Lab. Студент створює навчальне середовище для моніторингу безпеки IT-інфраструктури.
Результат:

- Налаштована тестова інфраструктура.
- Збір та аналіз системних журналів.
- Набір правил виявлення подій.
- Сценарій реагування на навчальний інцидент.
- Документація і презентація проєкту.

Інструменти: Linux, Wireshark, Wazuh, SIEM, Docker, Git.

В кінці курсу виконується дипломний проєкт.

© 2026 Комп'ютерна школа Hillel • ТОВ "Едмейк" • Код ЄДРПОУ 44790295