hillel IT school

подробнее о курсе

Курс **Cybersecurity Engineering** Online

BASIC LEVEL

24 занятия 2 занятия в неделю

ПРОГРАММА КУРСА

1. Introduction to Cybersecurity

Направления кибербезопасности, роли специалистов, типы угроз, CIA Triad.

2. Networking Fundamentals

TCP/IP, DNS, HTTP/HTTPS, порты, маршрутизация.

3. Operating Systems Security

Основы Windows и Linux, пользователи, права доступа.

4. Security Fundamentals

Аутентификация, авторизация, MFA, принцип наименьших привилегий.
Практика: анализ сетевой конфигурации, создание пользователей и настройка прав доступа в тестовой системе.

5. Linux Administration

Файловая система, терминал, процессы, службы.

6. Linux Security

Права доступа, SSH, журналы событий, обновления.

7. Network Security

Firewall, сегментация сетей, VPN, сетевые политики.

8. Network Monitoring

Wireshark, анализ сетевых пакетов, выявление аномалий.
Практика: настройка тестовой Linux-системы и анализ сетевого трафика учебной среды.

9. Introduction to SOC

Функции SOC, L1/L2/L3, процессы мониторинга.

10. Log Management

Системные журналы, типы событий, сбор и хранение логов.

11. SIEM Fundamentals

Архитектура SIEM, корреляция событий, правила мониторинга.

12. Incident Detection

Анализ оповещений, приоритизация и классификация инцидентов.
Практика: работа с учебными логами, создание простых правил выявления подозрительных событий.

13. Web Security Fundamentals

HTTP, cookies, sessions, authentication.

14. OWASP Top 10

Основные категории уязвимостей веб-приложений.

15. Secure Coding

Безопасная обработка данных, валидация, управление секретами.

16. Security Testing

Методология проверки безопасности собственного тестового приложения.
Практика: анализ специально подготовленного уязвимого учебного приложения и подготовка рекомендаций по устранению проблем.

17. Cloud Security Fundamentals

Облачная инфраструктура, модели ответственности.

18. Identity & Access Management

IAM, роли, политики доступа.

19. Infrastructure Monitoring

Мониторинг ресурсов, журналы и оповещения.

20. Security Best Practices

Backup, patch management, vulnerability management.
Практика: аудит конфигурации тестовой облачной среды и формирование рекомендаций.

---

21. Incident Response

Жизненный цикл реагирования на инциденты.

---

22. Digital Forensics Fundamentals

Сохранение доказательств, работа с копиями журналов, базовый анализ.

---

23. Final Project Workshop

Работа над финальным проектом.

---

24. Final Project Defense

Презентация и защита результатов.
Финальный проект: Security Monitoring Lab. Студент создает учебную среду для мониторинга безопасности IT-инфраструктуры.
Результат:

- Настроенная тестовая инфраструктура.
- Сбор и анализ системных журналов.
- Набор правил выявления событий.
- Сценарий реагирования на учебный инцидент.
- Документация и презентация проекта.

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

В конце курса выполняется дипломный проект.

© 2026 Компьютерная школа Hillel • ТОВ "Едмейк" • Код ЄДРПОУ 44790295