Вступ до кібербезпеки

Огляд курсу

Цей курс вивчає кібертенденції, кіберзагрози, безпеку в кіберпросторі та захист особистих і корпоративних даних.

Переваги

Сучасний взаємопов'язаний світ робить усіх більш сприйнятливими до кібератак. Навчіть, як захищати особисті дані та конфіденційність в Інтернеті, у соціальних мережах, і чому все більше і більше робочих місць у IT вимагають обізнаності та розуміння кібербезпеки.

Досліджуйте можливості в сфері технологій

- ✓ Формуйте розуміння кібербезпеки для безпечного цифрового життя
- ✓ Дізнайтеся про багато кар'єрних можливостей, для яких потрібні навички з кібербезпеки

Деталі курсу

Цільова аудиторія: Учні середніх шкіл, студенти коледжів, інші слухачі

Орієнтовний час для завершення: 6 годин

Передумови: Немає

Проходження курсу: самостійно або Під керівництвом інструктора

Основні компоненти навчання:

- ✓ 5 розділів та 7 лабораторних робіт
- ✓ Інтерактивні завдання та контрольні роботи
- ✓ 1 фінальний іспит

Визнання курсу: Цифровий бейдж

Рекомендований наступний курс:
Основи мереж (Networking Essentials) чи Основи кібербезпеки (Cybersecurity Essentials)

skillsforall.com | netacad.com

Вимоги

- Приналежність до ACS: Рекомендована
- Підготовка інструктора: Опційна
- Фізичне обладнання: Комп'ютер та Інтернет
- Додаткове необхідне обладнання: Ні

Networking Academy

Вступ до кібербезпеки

Обсяг курсу та послідовність вивчення

Зміст

Цільова аудиторія

Курс «Вступ до кібербезпеки» версії 3.0 призначений для слухачів, які розглядають кар'єру в галузі кібербезпеки. Цей пробний курс надає слухачам початкові знання про кібербезпеку, вивчаючи способи забезпечення безпеки в Інтернеті, різні типи зловмисного програмного забезпечення та атак, заходи, які використовують організації для пом'якшення атак, і досліджує можливості кар'єрного зростання. Онлайн-курс підходить для слухачів на різних рівнях освіти та в різних типах закладів: інститути, середні школи, університети, коледжі, професійно-технічні училища, навчальні заклади курсового навчання та громадські центри.

Передумови

Немає ніяких передумов для вивчення цього курсу.

Узгодження сертифікації

Узгодження сертифікації: цей курс є частиною програми кар'єрного зростання в галузі кібербезпеки, яка узгоджується із сертифікацією CCST з кібербезпеки..

Опис курсу

Вступ до кібербезпеки містить:

- П'ять розділів, що складаються з ключових тем.
- Розділи розвивають критичне мислення, вирішення проблем, співпрацю та практичне застосування навичок.

Завдання на рівні теми призначені для того, щоб оцінити, наскільки слухач володіє навичками курсу, дозволяючи слухачам перевірити розуміння, перш ніж складати контрольну роботу чи іспит. Мова, що описує поняття, створена для легкого розуміння слухачами на всіх рівнях підготовки.

- Оцінювання та практичні завдання, зосереджені на конкретних компетенціях, призначені для підвищення рівня розуміння та забезпечення гнучкості мислення на шляху навчання.
- Мультимедійні засоби навчання містять лабораторні роботи на папері, відео та тести, спрямовані на різноманітні стилі навчання, стимулюють навчання та сприяють засвоєнню знань.
- Лабораторні роботи та вправи в симуляторі Packet Tracer допомагають учням розвивати критичне мислення та навички вирішення складних проблем.
- Інноваційне оцінювання забезпечує миттєвий зворотний зв'язок для підтримки рівня знань і навичок.
- Слухачі вивчають основи безпеки в Інтернеті.
- Слухачі знайомляться з різними типами шкідливих програм і атак, а також з тим, як організації захищаються від цих атак.
- Слухачі досліджують варіанти кар'єри в галузі кібербезпеки.

Мета і завдання курсу

Матеріал курсу допоможе вам розвинути такі навички, зокрема:

- Пояснювати основи безпеки в Інтернеті, зокрема, що таке кібербезпека та її потенційний вплив.
- Пояснювати найпоширеніші кіберзагрози, атаки та вразливості.
- Пояснювати як захищати себе онлайн.
- Пояснювати як організації можуть захистити свою діяльність від атак.
- Отримати доступ до різноманітної інформації та ресурсів, щоб дослідити різні варіанти кар'єри в галузі кібербезпеки.

Вимоги до обладнання

Будь-який пристрій із доступом до Інтернету (смартфони/планшети/ноутбуки/настільні комп'ютери).

Зміст курсу

У таблиці 1 нижче детально описано розділи та пов'язані з ними компетенції. Кожен розділ є інтегрованою одиницею навчання, яка складається із змісту, завдань та оцінювання, спрямованих на певний набір компетенцій. Розмір розділу залежить від глибини знань і навичок, необхідних для опанування компетенції.

Таблиця 1 – Назва розділу і мета

Назва розділу / Назва теми	Мета
Розділ 1: Вступ до кібербезпеки	
1.0: Вступ до кібербезпеки	Пояснити основи безпеки в Інтернеті, зокрема, що таке кібербезпека та її потенційний вплив.
1.1 Світ кібербезпеки	Пояснити, що таке кібербезпека та її потенційний вплив.
1.2 Корпоративні дані	Визначити типи конфіденційної інформації, яку хакери можуть використати, щоб вторгнутися у ваше приватне життя та/або завдати шкоди вашій репутації, де вони можуть отримати доступ до цієї інформації та чому вона цікавить кіберзлочинців.
1.3 Що було викрадено?	Пояснити, що таке корпоративні дані та чому вони повинні бути захищені.
1.4 Кібер-зловмисники	Описати, хто такі кібер-зловмисники та чого вони хочуть.
1.5 Кібервійни	Пояснити, що таке кібервійна і чому країни та уряди потребують фахівців з кібербезпеки, щоб допомогти захистити своїх громадян та інфраструктуру.
Розділ 2: Атаки, поняття та методи	
2.0: Атаки, поняття та методи	Пояснити найпоширеніші кіберзагрози, атаки та вразливості.
2.1 Аналіз кібератаки	Визначити різні типи зловмисного програмного забезпечення та їх симптоми.

2.2 Методи проникнення	Описати різні методи проникнення.
2.3 Вразливість системи безпеки та експлойти	Пояснити, як знайти вразливі місця безпеки.
2.4 Ландшафт кібербезпеки	Пояснити, як класифікувати вразливості системи безпеки.
Розділ 3: Захист даних і конфіденційність	
3.0 Захист даних і конфіденційність.	Пояснити, як захистити себе в мережі.
3.1 Захист ваших пристроїв та мережі	Визначити способи захисту своїх комп'ютерних пристроїв.
3.2 Обслуговування даних	Пояснити, як захистити та зберегти свої дані.
3.3 Хто володіє вашими даними?	Пояснити, як угоди про надання послуг, наведені в Умовах надання послуг, визначають поводження з персональними даними.
3.4 Захист конфіденційності в Інтернеті	Впровадити методи безпечного зберігання даних.
3.5 Дослідіть ризики своєї поведінки в Інтернеті	Пояснити способи підвищення безпеки онлайн-даних.
Розділ 4: Захист організації	
4.0 Захист організації	Пояснити, як організації можуть захистити свою діяльність від атак.
4.1 Пристрої та технології кібербезпеки	Пояснити застосування різних брандмауерів, пристроїв безпеки та програмного забезпечення, які використовують фахівці з кібербезпеки для захисту мережі, даних і обладнання організації.
4.2 Підхід до кібербезпеки на основі поведінки	Пояснити, як виявити кіберзагрозу за допомогою підходів безпеки, заснованих на поведінці.
4.3 Підхід Cisco до кібербезпеки	Пояснити підхід Cisco до кібербезпеки, включаючи команду CSIRT і Посібник із безпеки.
Розділ 5: Чи готові Ви пов'язати своє майбутнє з кібербезпекою?	
5.0 Чи готові Ви пов'язати своє майбутнє з кібербезпекою?	Отримати доступ до різноманітної інформації та ресурсів, щоб дослідити різні варіанти кар'єри в галузі кібербезпеки.
5.1 Правові та етичні питання	Окреслити деякі особисті та корпоративні правові проблеми, які можуть виникнути під час роботи в сфері кібербезпеки.
5.2 Освіта та кар'єра	Визначити, які професійні сертифікати та наступні кроки потрібно зробити, щоб продовжити кар'єру в кібербезпеці.

Управління загрозами у кібербезпеці

Огляд курсу

Цей курс вивчає управління в кібербезпеці та керування загрозами. Навчіться розробляти політики та гарантувати, що ваша організація дотримується етичних стандартів, правової та нормативної бази.

Переваги

Попит на спеціалістів у галузі безпеки продовжує зростати. Отримайте розширені знання, які ви використовуватимете на робочому місці як фахівець з кібербезпеки.

Підготовка до кар'єри

- ✓ Формує основи кібербезпеки
- ✓ Досліджує безліч можливостей із працевлаштування у галузі кібербезпеки
- ✓ Розвиває навички для управління загрозами, наприклад, як оцінювати мережу на наявність вразливостей, керувати ризиками та реагувати на інциденти з безпеки

SkillsForAll.com

Деталі курсу

Цільова аудиторія: учні середніх шкіл, студенти коледжів та професійно-технічних училищ; Перепрофілювання для роботи у галузі кібербезпеки.

Орієнтовний час для завершення: 20 годин

Передумови: Вступ до кібербезпеки, Основи мереж, Безпека кінцевих вузлів та Захист мережі

Проходження курсу: Під керівництвом інструктора чи самостійно

Основні компоненти навчання:
- ✓ 6 розділів
- ✓ 16 лабораторних робіт та завдань у Cisco Packet Tracer
- ✓ 28+ інтерактивних завдань та контрольних робіт
- ✓ 1 фінальний іспит

Визнання курсу: Цифровий бейдж

Узгодження сертифікації: Цей курс є частиною Кар'єрного шляху з кібербезпеки, який узгоджується з сертифікацією CCST Cybersecurity.

Вимоги

- Потрібна приналежність до ASC: Ні
- Потрібна підготовка інструктора: Ні
- Потрібне фізичне обладнання: Ні

Управління загрозами у кібербезпеці

Обсяг курсу та послідовність вивчення

Зміст

Цільова аудиторія

Курс «Управління загрозами у кібербезпеці» підходить для учнів із середнім рівнем навичок читання, базовою комп’ютерною грамотністю та зацікавлених у пошуку роботи початкового рівня у галузі кібербезпеки.

Передумови

Курс не передбачає виконання якихось попередніх умов, а до слухачів висуваються такі основні вимоги:

- Базові навички користування операційною системою ПК
- Розуміння мереж TCP/IP, зокрема мережних протоколів, сервісів та процесів

Хоча це і необов’язково, проте учням рекомендовано пройти такі курси в рамках навчання з кібербезпеки:

- Вступ до кібербезпеки
- Основи мереж
- Безпека кінцевих вузлів
- Захист мережі

Узгодження сертифікації

Узгодження сертифікації: цей курс є частиною програми кар’єрного зростання в галузі кібербезпеки, яка узгоджується із сертифікацією CCST з кібербезпеки.

Опис курсу

Управління загрозами у кібербезпеці має багато функцій, які допомагають учням зрозуміти концепції безпеки. Матеріали курсу включають:

- Шість розділів, що складаються з ключових тем.
- Розділи розвивають критичне мислення, вирішення проблем, співпрацю та практичне застосування навичок.
- Кожен розділ містить практичні завдання та оцінювання, як-от завдання для самоперевірки, лабораторні роботи або завдання у програмі з моделювання мереж Cisco® Packet Tracer.
- Завдання на рівні теми призначені для того, щоб оцінити, наскільки слухач володіє навичками курсу, дозволяючи слухачам перевірити розуміння, перш ніж складати контрольну роботу чи іспит.
- Формулювання, що описують поняття, створені для легкого розуміння слухачами на всіх рівнях підготовки.
- Оцінювання та практичні завдання, зосереджені на конкретних компетенціях, призначені для підвищення рівня розуміння та забезпечення гнучкості мислення на шляху навчання.
- Мультимедійні засоби навчання містять лабораторні роботи на папері, відео та тести, спрямовані на різноманітні стилі навчання, стимулюють навчання та сприяють засвоєнню знань.
- Лабораторні роботи та вправи в симуляторі Packet Tracer допомагають учням розвивати критичне мислення та навички вирішення складних проблем.
- Інноваційне оцінювання забезпечує миттєвий зворотний зв'язок для підтримки рівня знань і навичок.
- Технічні поняття пояснюються доступною мовою базового рівня.

- Вбудовані інтерактивні завдання урізноманітнюють читання великих блоків тексту та покращують сприйняття матеріалу.
- Цей курс робить основний акцент на прикладних навичках та практичному досвіді, водночас заохочуючи слухачів до подальшого здобування освіти у галузі інформаційних технологій (IT).

Мета і завдання курсу

Управління загрозами у кібербезпеці представляє важливі фундаментальні концепції кібербезпеки, такі як етика та управління, тестування безпеки мережі, розвідувальні дані про загрози, оцінка вразливостей кінцевої точки, управління ризиками та реагування після інцидентів. До кінця курсу слухачі будуть підготовлені до участі в широкому спектрі заходів з управління загрозами та реагування на інциденти як член операційної групи з кібербезпеки.

Матеріал курсу допоможе вам розвинути наступні навички:

- Створення документів і політик, пов'язаних з управлінням кібербезпекою та відповідністю.
- Використання інструментів для перевірки безпеки мережі.
- Оцінка джерела розвідувальних даних про загрози.
- Пояснення, як виконується оцінка та керування вразливостями кінцевих точок.
- Вибір засобів контролю безпеки на основі результатів оцінки ризиків.
- Використання моделі реагування на інциденти та експертні методи для розслідування інцидентів з безпеки.

Вимоги до обладнання

Практичні лабораторні роботи з управління загрозами у кібербезпеці вимагають обладнання, яке є в більшості домашніх мереж. Будь-яка лабораторна робота, яка вимагає складнішого мережного середовища, використовує Packet Tracer, інструмент симуляції мережі.

Програмне забезпечення

- Oracle Virtual Box
- Файли лабораторних робіт для віртуальної машини OVA
- Packet Tracer версії 8.0.1 або вище

Додаткове лабораторне обладнання

- Вузол з ОС Microsoft Windows

Зміст курсу

У таблиці 1 нижче детально описано розділи та пов'язані з ними компетенції. Кожен розділ є інтегрованою одиницею навчання, яка складається із змісту, завдань та оцінювання, спрямована на певний набір компетенцій. Розмір розділу залежить від глибини знань і навичок, необхідних для опанування компетенції.

Таблиця 1: Назва розділу і мета

Назва розділу / Назва теми	Мета

Розділ 1: Управління та відповідність	
1.0 Управління та відповідність	Створення документів та політик щодо управління кібербезпекою та відповідності.
1.1 Управління	Створення політик з кібербезпеки.
1.2 Етика кібербезпеки	Створення особистого кодексу етичної поведінки.
1.3 Структура концепції управління IT-безпекою	Оцінювання засобів контролю безпеки.
Розділ 2: Тестування безпеки мережі	
2.0 Тестування безпеки мережі	Використання інструментів для перевірки безпеки мережі.
2.1 Оцінки безпеки	Використання команд для збирання інформації про мережу та діагностики проблем з підключенням.
2.2 Методи тестування безпеки мережі	Опис методів, які використовуються для тестування безпеки мережі.
2.3 Інструменти тестування безпеки мережі	Опис інструментів, які використовуються для тестування безпеки мережі.
2.4 Тестування на проникнення	Опис процесу використання організацією тестування на проникнення для оцінки безпеки системи.
Розділ 3: Аналіз кіберзагроз	
3.0 Аналіз кіберзагроз	Оцінювання джерел розвідувальних даних про загрози.
3.1 Інформаційні джерела	Оцінювання інформаційних джерел, які використовуються для поширення даних про нові загрози мережній безпеці.
3.2 Засоби аналізу кіберзагроз	Опис різних служб розвідувальних даних про загрози.
Розділ 4: Оцінка вразливостей кінцевого пристрою	
4.0 Оцінка вразливостей кінцевого пристрою	Пояснення, як виконується оцінка та керування вразливостями кінцевих точок.
4.1 Профілювання мережі та сервера	Пояснення значення профілювання мережі та сервера.
4.2 Загальна система оцінки вразливостей (CVSS)	Пояснення, як використовуються звіти загальної системи оцінки вразливостей (CVSS) для опису вразливостей безпеки.
4.3 Безпечне управління пристроями	Пояснення, як методи безпечного керування пристроями використовуються для захисту даних і ресурсів.
Розділ 5: Управління ризиками та контроль безпеки	
5.0 Управління ризиками та контроль безпеки	Вибір заходів контролю безпеки на основі результатів оцінки ризиків.
5.1 Управління ризиками	Пояснення управління ризиками.
5.2 Оцінка ризиків	Пояснення, як розраховують ризики.

5.3 Контроль безпеки	Оцінювання засобів контролю безпеки відповідно до характеристик організації.
Розділ 6: Цифрова експертиза, аналіз інцидентів і реагування	
6.0 Цифрова експертиза, аналіз інцидентів і реагування	Використання моделей реагування на інциденти та експертних методів для розслідування інцидентів з безпеки.
6.1 Робота з доказами та визначення причетних до атаки	Пояснення значення процесів цифрової експертизи.
6.2 Модель Cyber Kill Chain	Ідентифікація кроків в моделі Cyber Kill Chain.
6.3 Ромбоподібна модель аналізу вторгнення	Використання ромбоподібної моделі аналізу вторгнень для класифікації подій вторгнення.
6.4 Реагування на інциденти	Застосування процедур обробки інцидентів NIST 800-61r2 до наданого сценарію інцидентів.
6.5 Аварійне відновлення	Використання команд для резервного копіювання файлів та відновлення мережних операцій.