Основи кібербезпеки 1.0

Область застосування і зміст

Останнє оновлення 1 червня 2018 р.

Цільова аудиторія

Курс *Основи Кібербезпеки 1.0* призначений для слухачів, які зацікавлені в більш поглибленому вивченні області кібербезпеки. Цей підготовчий курс містить огляд галузі кібербезпеки. Навчальна програма досліджує характеристики і тактику кіберзлочинців. Потім вона заглиблюється в технології, продукти і процедури професіоналів боротьби з кіберзлочинністю. Навчальна програма підходить для слухачів на багатьох рівнях освіти і типах установ, включаючи середні школи, професіональні і технічні училища, коледжі та університети.

Попередня підготовка

Для правильного розвитку навичок учні повинні бути знайомі зі змістом і навичками, які описані в попередньому курсі:

- Вступ до кібербезпеки 2.0

Цільові сертифікації

Для цього курсу немає цільових сертифікацій

Опис навчального плану

Курс має багато можливостей, щоб допомогти слухачам зрозуміти наступні поняття:

- багатий мультимедійний контент, включаючи інтерактивні дії, відеоролики, ігри та тести, охоплює безліч стилів навчання і допомагає стимулювати навчання і зміцнити знання;
- практичні заняття і навчальні заходи на основі симулятора Packet Tracer допомагають учням розвивати навички критичного мислення і навички вирішення складних проблем;
- інноваційні методи оцінювання забезпечують негайний зворотний зв'язок для оцінки набутих знань і навичок;
- технічні поняття пояснюються з використанням мови, яка є зрозумілою для учнів на всіх рівнях, а вбудовані інтерактивні дії переривають читання вмісту курсу і допомагають зміцнити знання;
- навчальна програма заохочує слухачів до розгляду можливості отримання додаткової освіти в області IT, але також акцентує увагу на прикладних навичках та практичному досвіді.

Активності Cisco Packet Tracer призначені для використання з Packet Tracer версії 6.3 або вище.

Цілі навчальної програми

Курс *Основи кібербезпеки 1.0* охоплює основні знання і навички у всіх областях безпеки в кіберпросторі - інформаційна безпека, системна безпека, мережна безпека, мобільна безпека, фізична безпека, етика і закони, пов'язані технології, використання технологій захисту і пом'якшення у захисті бізнесу.

Після закінчення курсу *Основи кібербезпеки 1.0* слухачі зможуть виконувати наступні задачі:

- описати характеристики злочинців і героїв в сфері кібербезпеки;
- описати, як принципи конфіденційності, цілісності і доступності, пов'язані з станом даних і контрзаходами щодо кібербезпеки;
- описати тактику, методи та процедури, які використовуються кіберзлочинцями;
- описати, як технології, продукти і процедури використовуються для захисту конфіденційності та для забезпечення цілісності і високої доступності;
- пояснити, як професіонали кібербезпеки використовують технології, процеси та процедури для захисту всіх компонентів мережі;
- пояснити мету законів, пов'язаних з кібербезпекою.

Мінімальні системні вимоги

Для кращого навчання рекомендується типовий розмір класу від 12 до 15 слухачів і співвідношення у вигляді одного лабораторного ПК на одного учня. У крайньому випадку два слухача можуть ділити один лабораторний ПК для практичних лабораторних робіт. У деяких лабораторних роботах необхідно підключити студентські лабораторні ПК до локальної мережі.

Вимоги до обладнання лабораторного ПК

- Комп'ютер з об'ємом оперативної пам'яті 2 ГБ і 8 ГБ вільного місця на диску
- Доступ в Інтернет для завантаження Oracle VirtualBox і файлу образу віртуальної машини

Огляд навчального плану

Курс *Основи кібербезпеки 1.0* допомагає слухачам:

- розуміти гравців в світі кібербезпеки і мотивацію кіберзлочинців і фахівців з кібербезпеки.
- навчитися визначати атаки та їх ознаки, процеси і контрзаходи безпеки.
- отримати базові знання в різних областях безпеки.
- надбати навички в області керування безпекою, контролю, захисту та технологією мінімізації наслідків.
- вивчити закони безпеки, етику і способи розробки політик безпеки.
- дізнатися о функціях спеціалістів в області кібербезпеки і кар'єрних можливостях.

Опис курсу

Таблиця 1. Опис курсу *Основи кібербезпеки 1.0*

Розділ	Цілі та задачі
Розділ 1. Кібербезпека - світ експертів і злочинців	**Описати характеристики експертів і злочинців в галузі кібербезпеки**
1.1 Світ кібербезпеки	Описати загальні характеристики, що складають світ кібербезпеки
1.2 Кіберзлочинці проти фахівців з кібербезпеки	Описати різницю між фахівцями з кібербезпеки і злочинцями
1.3 Типові загрози	Порівняти, як загрози кібербезпеки впливають на окремих осіб, підприємства і організації
1.4 Розповсюдження загроз	Описати фактори, які призводять до поширення і зростання кіберзлочинності
1.5 Підготовка більшої кількості спеціалістів	Описати організації та зусилля, які спрямовані на розширення кібербезпеки
Розділ 2. Куб кібербезпеки	**Описати, як принципи конфіденційності, цілісності і доступності, пов'язані з станом даних, і контрзаходами щодо кібербезпеки**
2.1 Три виміри кібербезпеки	Описати три виміри кубу МакКамбера
2.2 Тріада КЦД	Описати принципи конфіденційності, цілісності та доступності
2.3 Стани даних	Розрізнити три стани даних
2.4 Засоби протидії злочинності	Порівняти типи контрзаходів проти кіберзлочинності
2.5 Структура керування IT-безпекою	Описати модель кібербезпеки ISO
Розділ 3. Кібербезпека - загрози, вразливості та атаки	**Описати тактику, методи та процедури, які використовуються кіберзлочинцями**
3.1 Шкідливе програмне забезпечення та зловмисний код	Розрізнити типи шкідливих програм і зловмисного коду
3.2. Обман	Порівняти різні методи, які використовуються в соціальній інженерії
3.3 Атаки	Порівняти різні типи кібератак
Розділ 4. Мистецтво захисту таємниць	**Описати, як технології, продукти і процедури використовуються для захисту конфіденційності**
4.1 Криптографія	Пояснити, як методи шифрування захищають конфіденційність.
4.2 Контроль доступу	Описати, як методи контролю доступу захищають конфіденційність.
4.3 Приховування даних	Опишіть концепцію приховування даних.

Розділ 5. Мистецтво забезпечення цілісності	**Описати, як технології, продукти і процедури використовуються для забезпечення цілісності**
5.1 Типи засобів контролю цілісності даних	Пояснити процеси, які використовуються для забезпечення цілісності
5.2 Цифрові підписи	Пояснити призначення цифрових підписів
5.3 Сертифікати	Пояснити призначення цифрових сертифікатів
5.4 Забезпечення цілісності бази даних	Поясніть необхідність забезпечення цілісності бази даних
Розділ 6. Концепція п'яти дев'яток	**Описати, як технології, продукти і процедури забезпечують високу доступність**
6.1 Висока доступність	Пояснити концепцію високої доступності
6.2 Заходи для поліпшення доступності	Поясніть, як заходи високої доступності використовуються для покращення доступності
6.3 Реагування на інциденти	Описати, як план реагування на інциденти покращує високу доступність
6.4 Відновлення після катастроф	Описати, як планування аварійного відновлення грає важливу роль в забезпеченні високої доступності
Розділ 7. Захист домену кібербезпеки	**Пояснити, як професіонали кібербезпеки використовують технології, процеси та процедури для захисту всіх компонентів мережі**
7.1 Захист систем та пристроїв	Пояснити, як процеси і процедури захищають системи
7.2 Укріплення захисту серверів	Пояснити, як захистити сервери в мережі
7.3 Укріплення захисту мережі	Пояснити, як реалізувати заходи безпеки для захисту мережевих пристроїв
7.4 Фізична безпека	Пояснити, як застосовуються заходи фізичної безпеки для захисту мережевого обладнання
Розділ 8. Як стати спеціалістом з кібербезпеки	**Пояснити мету законів, які пов'язані з кібербезпекою**
8.1 Домени кібербезпеки	Опишіть, як області кібербезпеки використовуються в тріаді КЦД
8.2 Розуміння етики роботи в кібербезпеці	Пояснити етичні цінності в галузі кібербезпеки і як ними керуватись
8.3 Наступний крок	Пояснити дії, які необхідно виконати в майбутньому щоб стати професіоналом в області кібербезпеки

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**