Cybersecurity Essentials 1.1
Âmbito e Sequência

Última atualização a 16 de junho de 2021

Público-Alvo

O curso *Cybersecurity Essentials 1.1* foi concebido para os estudantes interessados em prosseguir estudos mais avançados no campo da cibersegurança. Este curso preparatório fornece uma visão geral do campo de cibersegurança. O currículo explora as características e táticas usadas por cibercriminosos. Neste aprofundam-se as tecnologias, produtos e procedimentos de uso profissional de cibersegurança no combate ao cibercrime. O currículo é adequado para alunos de diversos níveis de escolaridade e de ensino, incluindo ensino básico e secundário, ensino universitário, institutos e escolas profissionais e centros comunitários.

Pré-requisitos

Para a construção de competências adequadas, os estudantes devem estar familiarizados com o conteúdo e competências descritas no curso pré-requisito:

- Introduction to Cybersecurity 2.0

Certificações Alvo

Não há certificações alvo para este curso

Descrição do Currículo

O curso possui muitas características para ajudar os estudantes a compreender estes conceitos:

- Conteúdo rico em multimédia, incluindo atividades interativas, vídeos e questionários, que abrangem uma diversidade de estilos de aprendizagem e ajudam a estimular a aprendizagem e a promover uma maior retenção de conhecimentos.
- Laboratórios práticos (hands-on) e atividades de aprendizagem baseadas em simulação Packet Tracer ajudam os estudantes a desenvolver pensamento crítico e competências de resolução de problemas complexos
- Avaliações inovadoras fornecem um feedback imediato para suportar a avaliação de conhecimentos e competências adquiridas
- Os conceitos técnicos são explicados usando linguagem dirigida aos estudantes de todos os níveis, e as atividades interativas embebidas separam a leitura do conteúdo e ajudam a reforçar a capacidade de compreensão
- O currículo incentiva os estudantes a considerarem formação adicional em TI, mas também enfatiza as competências aplicadas e a experiência prática

As atividades Cisco Packet Tracer estão desenhadas para o uso do Packet Tracer 6.3 ou posterior.

Objetivos Curriculares

Cybersecurity Essentials 1.1 cobre os conhecimentos básicos e competências essenciais em todos os domínios de segurança no mundo cibernético - segurança da informação, segurança de sistemas, segurança de rede, segurança móvel, segurança física, ética e legislação, tecnologias relacionadas, e uso de técnicas de defesa e mitigação protegendo as empresas.

Após a conclusão do curso *Cybersecurity Essentials 1.1*, os estudante serão capazes de realizar as seguintes tarefas:

- Descrever as características dos criminosos e especialistas de cibersegurança.
- Descrever como os princípios de confidencialidade, integridade e disponibilidade se relacionam com os estados dos dados e as contramedidas de cibersegurança.
- Descrever as táticas, técnicas e procedimentos utilizados por cibercriminosos.
- Descrever como as tecnologias, produtos e procedimentos são usados para proteger a confidencialidade.
- Descreva como as tecnologias, produtos e procedimentos são usados para garantir a integridade.
- Descreva como as tecnologias, produtos e procedimentos fornecem alta disponibilidade.
- Explicar como os profissionais de cibersegurança usam as tecnologias, processos e procedimentos para defender todos os componentes da rede.
- Explicar o propósito das leis relacionadas com a cibersegurança.

Requisitos Mínimos

Para obter a melhor experiência de aprendizagem, recomendamos uma turma com um tamanho típico de 12 a 15 estudantes e um rácio de um PC de laboratório por estudante. No máximo, dois alunos podem partilhar um PC do laboratório durante os laboratórios práticos. Algumas atividades laboratoriais exigem que os PCs do laboratório estejam ligados a uma rede local.

Requisitos de Hardware de Laboratório

- Computador com um mínimo de 2 GB de RAM e 8 GB de espaço livre em disco
- Acesso à Internet de alta velocidade para descarregar o Oracle VirtualBox e o ficheiro da imagem da máquina virtual

Descrição geral do currículo

Cybersecurity Essentials 1.1 ajuda os estudantes a:

- Compreender os jogadores no mundo da cibersegurança e a motivação de cibercriminosos e especialistas em cibersegurança.
- Aprender a identificar ataques de segurança, sintomas, processos e contramedidas.
- Aprender conhecimentos fundamentais nos vários domínios da segurança.
- Desenvolver competências em tecnologias de gestão de segurança, controles, proteção e mitigação.
- Aprender as leis de segurança, ética e como desenvolver políticas de segurança.
- Aprender as funções de diferentes profissionais de cibersegurança e as opções de carreira.

Descrição do curso

Tabela 1. Programa do curso Essentials 1.1 Cybersecurity

Capítulo/Seção	Objetivos/Objetivos
Capítulo 1. Cibersegurança - Um Mundo de Especialistas e Criminosos	**Descrever as características dos criminosos e especialistas de cibersegurança.**
1.1 O mundo da Cibersegurança	Descrever as características comuns que compreendem o mundo da cibersegurança
1.2 Cibercriminosos versus Especialistas em Cibersegurança	Diferenciar as características dos cibercriminosos e especialistas.
1.3 Ameaças Comuns	Comparar como as ameaças à cibersegurança afetam os indivíduos, as empresas e as organizações.
1.4 Espalhando Ameaças à Cibersegurança	Descrever os fatores que levam à disseminação e ao crescimento do cibercrime.
1.5 Criando Mais Especialistas	Descrever as organizações e os esforços comprometidos com a expansão da força de trabalho de cibersegurança.
Capítulo 2. O Cubo de Cibersegurança	**Descrever como os princípios de confidencialidade, integridade e disponibilidade se relacionam com os estados dos dados e as contramedidas de cibersegurança.**
2.1 As Três Dimensões do Cubo de Cibersegurança	Descrever as três dimensões do cubo McCumber.
2.2 Tríade CID	Descrever os princípios da confidencialidade, integridade e disponibilidade
2.3 Estados dos Dados	Diferenciar os três estados dos dados.
2.4 Contramedidas de Cibersegurança	Comparar os tipos de contramedidas de cibersegurança.
2.5 Estrutura de Gestão de Segurança de TI	Descrever o modelo ISO de cibersegurança
Capítulo 3. Ameaças, Vulnerabilidades e Ataques à Cibersegurança	**Descrever as táticas, técnicas e procedimentos utilizados por cibercriminosos.**
3.1 Malware e Código Malicioso	Diferenciar os tipos de malware e código malicioso.
3.2 Fraude	Comparar os diferentes métodos utilizados em engenharia social.
3.3 Ataques	Comparar os diferentes tipos de ciberataques.
Capítulo 4. A Arte de Proteger Segredos	**Descrever como as tecnologias, produtos e procedimentos são usados para proteger a confidencialidade.**
4.1 Criptografia	Explicar como as técnicas de criptografia protegem a confidencialidade.
4.2 Controlos de Acesso	Descrever como as técnicas de controle de acesso protegem a confidencialidade.
4.3 Obscurecendo dados	Descrever o conceito de obscurecimento de dados.

Capítulo 5. A Arte de Garantir a Integridade	**Descrever como as tecnologias, produtos e procedimentos são usados para garantir a integridade.**
5.1 Tipos de controlos de integridade de Dados	Explicar os processos usados para garantir a integridade.
5.2 Assinaturas Digitais	Explicar a finalidade das assinaturas digitais.
5.3 Certificados	Explicar o propósito dos certificados digitais.
5.4 Imposição da Integridade de Bases de Dados	Explicar a necessidade de aplicação da integridade de base de dados.
Capítulo 6. O Conceito dos Cinco Noves	**Descrever como as tecnologias, produtos e procedimentos fornecem alta disponibilidade.**
6.1 Alta Disponibilidade	Explicar o conceito de alta disponibilidade.
6.2 Medidas para melhorar a Disponibilidade	Explicar como as medidas de alta disponibilidade são usadas para melhorar a disponibilidade.
6.3 Resposta a Incidentes	Descrever como um plano de resposta a incidentes melhora a alta disponibilidade.
6.4 Recuperação de Desastres	Descrever como o planeamento de recuperação de desastres desempenha um papel importante na implementação de alta disponibilidade.
Capítulo 7. Proteção de um Domínio de Cibersegurança	**Explicar como os profissionais de cibersegurança usam as tecnologias, processos e procedimentos para defender todos os componentes da rede.**
7.1 Defesa de Sistemas e Dispositivos	Explicar como processos e procedimentos protegem os sistemas.
7.2 Blindagem do Servidor	Explicar como proteger os servidores numa rede.
7.3 Blindagem da Rede	Explicar como implementar medidas de segurança para proteger dispositivos de rede.
7.4 Segurança Física e Ambiental	Explicar como as medidas de segurança física são implementadas para proteger o equipamento de rede.
Capítulo 8. Tornando-se um Especialista de Cibersegurança	**Explicar o propósito das leis relacionadas com a cibersegurança.**
8.1 Domínios de Cibersegurança	Descrever como os domínios de cibersegurança são usados dentro da tríade CIA.
8.2 Compreender a Ética do Trabalho em Cibersegurança	Explicar como a ética fornece orientação.
8.3 Próximo Passo	Explicar como dar o próximo passo no sentido de se tornar um profissional de cibersegurança

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.