WWW.KASOLUTION.COM.BR

Curso Oficial da Microsoft

Microsoft Cybersecurity Architect (SC-100)

Microsoft Cybersecurity Architect (SC-100)

Este curso prepara os alunos com experiência para projetar e avaliar estratégias de segurança cibernética nas seguintes áreas: Zero Trust, Governance Risk Compliance (GRC), operações de segurança (SecOps), dados e aplicativos. Os alunos também aprenderão a projetar e arquitetar soluções usando princípios de confiança zero e especificar requisitos de segurança para infraestrutura em nuvem em diferentes modelos de serviço (SaaS, PaaS, IaaS).

Carga horária: 4 dias / 8 noites.

Módulo 1: Construir uma estratégia e arquitetura geral de segurança

Lições

- Introdução
- Visão geral de Zero Trust
- Desenvolva pontos de integração em uma arquitetura
- Desenvolva requisitos de segurança com base nos objetivos de negócios
- Traduza os requisitos de segurança em recursos técnicos
- Projete a segurança para uma estratégia de resiliência
- Projete uma estratégia de segurança para ambientes híbridos e multilocatários
- Projete estratégias técnicas e de governança para filtragem e segmentação de tráfego
- Entenda a segurança para protocolos
- Exercício: Construir uma estratégia e arquitetura de segurança geral
- Verificação de conhecimento
- Resumo

Após concluir este módulo, os alunos serão capazes de:

- Desenvolver pontos de integração em uma arquitetura
- Desenvolver requisitos de segurança com base nos objetivos de negócios
- Traduzir os requisitos de segurança em recursos técnicos
- Projetar a segurança para uma estratégia de resiliência
- Projetar estratégia de segurança para ambientes híbridos e multilocatários
- Projetar estratégias técnicas e de governança para filtragem e segmentação de tráfego

Módulo 2: Projete uma estratégia de operações de segurança

Lições

- Introdução
- Compreenda estruturas, processos e procedimentos de operações de segurança
- Projete uma estratégia de segurança de registro e auditoria
- Desenvolva operações de segurança para ambientes híbridos e multinuvem
- Projete uma estratégia para gerenciamento de informações e eventos de segurança (SIEM) e orquestração de segurança
- Avalie os fluxos de trabalho de segurança
- Revise as estratégias de segurança para gerenciamento de incidentes
- Avalie a estratégia de operações de segurança para compartilhar inteligência técnica de ameaças
- Monitore as fontes para obter insights sobre ameaças e mitigações

Após concluir este módulo, os alunos serão capazes de:

- Projetar uma estratégia de segurança de registro e auditoria
- Desenvolver operações de segurança para ambientes híbridos e multinuvem
- Projetar uma estratégia para gerenciamento de informações e eventos de segurança (SIEM) e orquestração de segurança
- Avaliar os fluxos de trabalho de segurança
- Revisar as estratégias de segurança para gerenciamento de incidentes
- Avaliar as operações de segurança para obter inteligência técnica contra ameaças
- Monitorar as fontes para obter insights sobre ameaças e mitigações

Módulo 3: Projete uma estratégia de segurança de identidade

Lições

- Introdução
- Acesso seguro aos recursos da nuvem
- Recomende um armazenamento de identidade para segurança
- Recomende estratégias seguras de autenticação e autorização de segurança
- Acesso condicional seguro
- Projete uma estratégia para atribuição e delegação de funções
- Defina governança de identidade para revisões de acesso e gerenciamento de direitos
- Projete uma estratégia de segurança para acesso de função privilegiada à infraestrutura
- Projete uma estratégia de segurança para atividades privilegiadas
- Entenda a segurança para protocolos

Após concluir este módulo, os alunos serão capazes de:

- Recomendar um armazenamento de identidade para segurança
- Recomendar estratégias seguras de autenticação e autorização de segurança
- Realizar acesso condicional seguro
- Projetar uma estratégia para atribuição e delegação de funções
- Definir a governança de identidade para revisões de acesso e gerenciamento de direitos
- Projetar uma estratégia de segurança para acesso de função privilegiada à infraestrutura
- Projetar uma estratégia de segurança para acesso privilegiado

Módulo 4: Avalie uma estratégia de conformidade regulatória

Lições

- Introdução
- Interprete os requisitos de conformidade e seus recursos técnicos
- Avalie a conformidade da infraestrutura usando o Microsoft Defender for Cloud
- Interpretar pontuações de conformidade e recomendar ações para resolver problemas ou melhorar a segurança
- Projete e validar a implementação do Azure Policy
- Design para requisitos de residência de dados
- Traduza os requisitos de privacidade em requisitos para soluções de segurança

Após concluir este módulo, os alunos serão capazes de:

- Interpretar os requisitos de conformidade e seus recursos técnicos
- Avaliar a conformidade da infraestrutura usando o Microsoft Defender for Cloud
- Interpretar pontuações de conformidade e recomendar ações para resolver problemas ou melhorar a segurança
- Projetar e validar a implementação do Azure Policy
- Realizar design para requisitos de residência de dados
- Traduzir os requisitos de privacidade em requisitos para soluções de segurança

Módulo 5: Avalie a postura de segurança e recomende estratégias técnicas para gerenciar riscos

Lições

- Introdução
- Avalie as posturas de segurança usando benchmarks
- Avalie as posturas de segurança usando o Microsoft Defender for Cloud
- Avalie as posturas de segurança usando Secure Scores
- Avalie a higiene de segurança das cargas de trabalho na nuvem
- Segurança de design para uma zona de aterrissagem do Azure
- Interprete inteligência técnica de ameaças e recomendar mitigações de risco
- Recomende recursos ou controles de segurança para mitigar os riscos identificados

Após concluir este módulo, os alunos serão capazes de:

- Avaliar as posturas de segurança usando benchmarks
- Avaliar as posturas de segurança usando o Microsoft Defender for Cloud
- Avaliar as posturas de segurança usando Secure Scores
- Avaliar a higiene de segurança das cargas de trabalho na nuvem
- Segurança de design para uma zona de aterrissagem do Azure
- Interpretar inteligência técnica de ameaças e recomendar mitigações de risco
- Recomendar recursos ou controles de segurança para mitigar os riscos identificados

Módulo 6: Entenda as práticas recomendadas de arquitetura e como elas estão mudando com a nuvem

Lições

- Introdução
- Planeje e implemente uma estratégia de segurança entre as equipes
- Estabeleça uma estratégia e um processo para a evolução proativa e contínua de uma estratégia de segurança
- Entenda os protocolos de rede e as práticas recomendadas para segmentação de rede e filtragem de tráfego

Após concluir este módulo, os alunos serão capazes de:

- Descrever as práticas recomendadas para segmentação de rede e filtragem de tráfego
- Planejar e implementar uma estratégia de segurança entre as equipes
- Estabelecer uma estratégia e um processo para avaliação proativa e contínua da estratégia de segurança

Módulo 7: Projete uma estratégia para proteger os endpoints do servidor e do cliente

Lições

- Introdução
- Especifique linhas de base de segurança para endpoints de servidor e cliente
- Especifique requisitos de segurança para servidores
- Especifique requisitos de segurança para dispositivos móveis e clientes
- Especifique requisitos para proteger os Serviços de Domínio Active Directory
- Projete uma estratégia para gerenciar segredos, chaves e certificados
- Projete uma estratégia para acesso remoto seguro
- Compreenda estruturas, processos e procedimentos de operações de segurança
- Entenda os procedimentos forenses profundos por tipo de recurso

Após concluir este módulo, os alunos serão capazes de:

- Especificar linhas de base de segurança para endpoints de servidor e cliente
- Especificar requisitos de segurança para servidores
- Especificar requisitos de segurança para dispositivos móveis e clientes
- Especificar requisitos para proteger os serviços de domínio Active Directory
- Projetar uma estratégia para gerenciar segredos, chaves e certificados
- Projetar uma estratégia para acesso remoto seguro
- Compreender estruturas, processos e procedimentos de operações de segurança
- Entender os procedimentos forenses profundos por tipo de recurso

Módulo 8: Projete uma estratégia para proteger serviços PaaS, IaaS e SaaS

Lições

- Introdução
- Especifique linhas de base de segurança para serviços PaaS
- Especifique linhas de base de segurança para serviços IaaS
- Especifique linhas de base de segurança para serviços SaaS
- Especifique requisitos de segurança para cargas de trabalho de IoT
- Especifique requisitos de segurança para cargas de trabalho de dados
- Especifique requisitos de segurança para cargas de trabalho da Web
- Especifique requisitos de segurança para cargas de trabalho de armazenamento
- Especifique requisitos de segurança para contêineres
- Especifique requisitos de segurança para orquestração de contêiner

Após concluir este módulo, os alunos serão capazes de:

- Especificar linhas de base de segurança para serviços PaaS, SaaS e IaaS
- Especificar os requisitos de segurança para IoT, dados, armazenamento e cargas de trabalho da Web
- Especificar requisitos de segurança para contêineres e orquestração de contêineres

Módulo 9: Especificar requisitos de segurança para aplicativos

Lições

- Introdução
- Entenda a modelagem de ameaças de aplicativos
- Especifique prioridades para mitigar ameaças a aplicativos
- Especifique um padrão de segurança para integrar um novo aplicativo
- Especifique uma estratégia de segurança para aplicativos e APIs

Após concluir este módulo, os alunos serão capazes de:

- Especificar prioridades para mitigar ameaças a aplicativos
- Especificar um padrão de segurança para integrar um novo aplicativo
- Especificar uma estratégia de segurança para aplicativos e APIs

Módulo 10: Projete uma estratégia para proteger os dados

Lições

- Introdução
- Priorize a mitigação de ameaças aos dados
- Projete uma estratégia para identificar e proteger dados confidenciais
- Especifique um padrão de criptografia para dados em repouso e em movimento

Após concluir este módulo, os alunos serão capazes de:

- Priorizar a mitigação de ameaças aos dados
- Projetar uma estratégia para identificar e proteger dados confidenciais
- Especificar um padrão de criptografia para dados em repouso e em movimento