KA SOLUTION
WWW.KASOLUTION.COM.BR

Curso Oficial da Microsoft

Microsoft Security Operations Analyst (SC-200)

Microsoft Security Operations Analyst (SC-200)

Aprenda como investigar, responder e caçar ameaças usando o Microsoft Azure Sentinel, Azure Defender e Microsoft 365 Defender. Neste curso, você aprenderá como mitigar ameaças cibernéticas usando essas tecnologias. Especificamente, você configurará e usará o Azure Sentinel, bem como utilizará Kusto Query Language (KQL) para realizar detecção, análise e geração de relatórios. O curso foi projetado para pessoas que trabalham em uma função de trabalho de Operações de Segurança e ajuda os alunos a se prepararem para o exame SC-200: Analista de Operações de Segurança da Microsoft.

Carga Horária: 4 dias / 8 noites.

Módulo 1: Mitigar ameaças usando o Microsoft Defender for Endpoint

Implemente a plataforma Microsoft Defender for Endpoint para detectar, investigar e responder a ameaças avançadas. Saiba como o Microsoft Defender for Endpoint pode ajudar sua organização a se manter segura. Aprenda como implantar o ambiente Microsoft Defender for Endpoint, incluindo dispositivos integrados e configuração de segurança. Aprenda a investigar incidentes e alertas usando o Microsoft Defender for Endpoints. Execute caça avançada e consulte especialistas em ameaças. Você também aprenderá a configurar a automação no Microsoft Defender for Endpoint gerenciando as configurações ambientais. Por último, você aprenderá sobre os pontos fracos do seu ambiente usando o Gerenciamento de Ameaças e Vulnerabilidades no Microsoft Defender for Endpoint.

Lições

- Proteja-se contra ameaças com o Microsoft Defender for Endpoint.
- Implantar o ambiente Microsoft Defender para Endpoint.
- Implementar aprimoramentos de segurança do Windows 10 com o Microsoft Defender for Endpoint.
- Gerenciar alertas e incidentes no Microsoft Defender for Endpoint.
- Realize investigações de dispositivos no Microsoft Defender for Endpoint.
- Executar ações em um dispositivo usando o Microsoft Defender for Endpoint.
- Realizar investigações de evidências e entidades usando o Microsoft Defender for Endpoint.
- Configure e gerencie a automação usando o Microsoft Defender for Endpoint.
- Configure para alertas e detecções no Microsoft Defender for Endpoint.
- Utilize o gerenciamento de ameaças e vulnerabilidades no Microsoft Defender for Endpoint.

Depois de concluir este módulo, você será capaz de:

- Definir os recursos do Microsoft Defender para Endpoint.
- Definir as configurações de ambiente do Microsoft Defender para Endpoint.
- Configurar regras de redução da superfície de ataque em dispositivos Windows 10.
- Investigar alertas no Microsoft Defender for Endpoint.
- Descrever as informações forenses do dispositivo coletadas pelo Microsoft Defender for Endpoint.
- Conduzir a coleta de dados forenses usando o Microsoft Defender for Endpoint.
- Investigar contas de usuário no Microsoft Defender for Endpoint.
- Gerenciar configurações de automação no Microsoft Defender for Endpoint.
- Gerenciar indicadores no Microsoft Defender for Endpoint.
- Descrever o gerenciamento de ameaças e vulnerabilidades no Microsoft Defender for Endpoint.

Módulo 2: Mitigar ameaças usando o Microsoft 365 Defender

Análise dados de ameaças entre domínios e corrija ameaças rapidamente com orquestração e automação integradas no Microsoft 365 Defender. Saiba mais sobre as ameaças à segurança cibernética e como as novas ferramentas de proteção contra ameaças da Microsoft protegem os usuários, dispositivos e dados da sua organização. Use a detecção e remediação avançadas de ameaças baseadas em identidade para proteger suas identidades e aplicativos do Azure Active Directory contra o comprometimento.

Lições

- Introdução à proteção contra ameaças com Microsoft 365.
- Mitigar incidentes usando o Microsoft 365 Defender.
- Proteja suas identidades com o Azure AD Identity Protection.
- Corrija os riscos com o Microsoft Defender for Office 365.
- Proteja seu ambiente com o Microsoft Defender for Identity.
- Proteja seus aplicativos e serviços em nuvem com o Microsoft Cloud App Security.
- Responda a alertas de prevenção de perda de dados usando o Microsoft 365.
- Gerenciar riscos internos no Microsoft 365.

Depois de concluir este módulo, você será capaz de:

- Explicar como o cenário de ameaças está evoluindo.
- Gerenciar incidentes no Microsoft 365 Defender.
- Conduzir caça avançada no Microsoft 365 Defender.
- Descrever os recursos de investigação e correção do Azure Active Directory Identity Protection.
- Definir os recursos do Microsoft Defender para Endpoint.
- Explicar como o Microsoft Defender for Endpoint pode remediar os riscos em seu ambiente.
- Definir a estrutura do Cloud App Security.
- Explicar como o Cloud Discovery ajuda você a ver o que está acontecendo em sua organização.

Módulo 3: Mitigar ameaças usando o Azure Defender

Use o Azure Defender integrado com a Central de Segurança do Azure, para Azure, nuvem híbrida e proteção e segurança de carga de trabalho local. Aprenda a finalidade do Azure Defender, a relação do Azure Defender com a Central de Segurança do Azure e como habilitar o Azure Defender. Você também aprenderá sobre as proteções e detecções fornecidas pelo Azure Defender para cada carga de trabalho na nuvem. Saiba como você pode adicionar recursos do Azure Defender ao seu ambiente híbrido.

Lições

- Planeje proteções de carga de trabalho na nuvem usando o Azure Defender.
- Explicar as proteções de carga de trabalho em nuvem no Azure Defender.
- Conecte os ativos do Azure ao Azure Defender.
- Conecte recursos não-Azure ao Azure Defender.
- Corrija alertas de segurança usando o Azure Defender.

Depois de concluir este módulo, você será capaz de:

- Descrever os recursos do Azure Defender.
- Explicar os recursos da Central de Segurança do Azure.
- Explicar quais cargas de trabalho são protegidas pelo Azure Defender.
- Explicar como funcionam as proteções do Azure Defender.
- Configurar o provisionamento automático no Azure Defender.
- Descrever o provisionamento manual no Azure Defender.
- Conectar máquinas não-Azure ao Azure Defender.
- Descrever alertas no Azure Defender.
- Corrigir alertas no Azure Defender.
- Automatizar respostas no Azure Defender.

Módulo 4: Criar consultas para o Azure Sentinel usando Kusto Query Language (KQL)

Grave instruções Kusto Query Language (KQL) para consultar dados de log para realizar detecções, análises e relatórios no Azure Sentinel. Este módulo enfocará os operadores mais usados. As instruções KQL de exemplo mostrarão consultas de tabela relacionadas à segurança. KQL é a linguagem de consulta usada para realizar análises de dados para criar análises, pastas de trabalho e realizar buscas no Azure Sentinel. Aprenda como a estrutura básica da instrução KQL fornece a base para construir instruções mais complexas. Aprenda como resumir e visualizar dados com uma instrução KQL fornece a base para criar detecções no Azure Sentinel. Aprenda a usar a Kusto Query Language (KQL) para manipular dados de string ingeridos de fontes de log.

Lições

- Construir instruções KQL para o Azure Sentinel.
- Analise os resultados da consulta usando KQL.
- Crie instruções de várias tabelas usando KQL.
- Trabalhe com dados no Azure Sentinel usando Kusto Query Language.

Depois de concluir este módulo, você será capaz de:

- Construir declarações KQL.
- Pesquisar arquivos de registro para eventos de segurança usando KQL.
- Filtrar as pesquisas com base na hora do evento, gravidade, domínio e outros dados relevantes usando KQL.
- Resumir os dados usando instruções KQL.
- Renderizar visualizações usando instruções KQL.
- Extrair dados de campos de string não estruturados usando KQL.
- Extrair dados de dados de string estruturada usando KQL.
- Criar funções usando KQL.

Módulo 5: Configurar seu ambiente Azure Sentinel

Comece com o Azure Sentinel configurando corretamente o espaço de trabalho do Azure Sentinel. Os sistemas tradicionais de gerenciamento de eventos e informações de segurança (SIEM) normalmente levam muito tempo para instalar e configurar. Eles também não são necessariamente projetados com cargas de trabalho em nuvem em mente. O Azure Sentinel permite que você comece a obter insights de segurança valiosos de sua nuvem e dados locais rapidamente. Este módulo ajuda você a começar. Saiba mais sobre a arquitetura dos espaços de trabalho do Azure Sentinel para garantir que você configure seu sistema para atender aos requisitos de operações de segurança da sua organização. Como analista de operações de segurança, você deve entender as tabelas, campos e dados ingeridos em seu espaço de trabalho. Aprenda a consultar as tabelas de dados mais usadas no Azure Sentinel.

Lições

- Introdução ao Azure Sentinel.
- Criar e gerenciar espaços de trabalho do Azure Sentinel.
- Consultar logs no Azure Sentinel.
- Use listas de observação no Azure Sentinel.
- Utilize inteligência de ameaças no Azure Sentinel.

Depois de concluir este módulo, você será capaz de:

- Identificar os vários componentes e funcionalidades do Azure Sentinel.
- Identificar os casos de uso em que o Azure Sentinel seria uma boa solução.
- Descrever a arquitetura do espaço de trabalho do Azure Sentinel.
- Instalar o espaço de trabalho do Azure Sentinel.
- Gerenciar um espaço de trabalho do Azure Sentinel.
- Criar uma lista de observação no Azure Sentinel.
- Usar KQL para acessar a lista de observação no Azure Sentinel.
- Gerenciar indicadores de ameaça no Azure Sentinel.
- Usar KQL para acessar indicadores de ameaça no Azure Sentinel.

Módulo 6: conectar logs ao Azure Sentinel

Conecte dados em escala de nuvem em todos os usuários, dispositivos, aplicativos e infraestrutura, tanto no local quanto em várias nuvens, para o Azure Sentinel. A abordagem principal para conectar dados de log é usar os conectores de dados fornecidos pelo Azure Sentinel. Este módulo fornece uma visão geral dos conectores de dados disponíveis. Você aprenderá sobre as opções de configuração e os dados fornecidos pelos conectores do Azure Sentinel para o Microsoft 365 Defender.

Lições

- Conecte dados ao Azure Sentinel usando conectores de dados.
- Conecte os serviços da Microsoft ao Azure Sentinel.
- Conecte o Microsoft 365 Defender ao Azure Sentinel.
- Conecte hosts do Windows ao Azure Sentinel.
- Conecte os logs do Common Event Format ao Azure Sentinel.
- Conecte fontes de dados syslog ao Azure Sentinel.
- Conecte os indicadores de ameaça ao Azure Sentine.

Depois de concluir este módulo, você será capaz de:

- Explicar o uso de conectores de dados no Azure Sentinel.
- Explicar o Formato de Evento Comum e as diferenças do conector Syslog no Azure Sentinel.
- Conectar os conectores de serviço da Microsoft.
- Explicar como os conectores criam incidentes automaticamente no Azure Sentinel.
- Ativar o conector do Microsoft 365 Defender no Azure Sentinel.
- Conectar as máquinas virtuais do Windows do Azure ao Azure Sentinel.
- Conectar hosts Windows que não sejam do Azure ao Azure Sentinel.
- Configurar o agente Log Analytics para coletar eventos Sysmon.
- Explicar as opções de implantação do conector Common Event Format no Azure Sentinel.
- Configurar o conector TAXII no Azure Sentinel.
- Ver indicadores de ameaça no Azure Sentinel.

Módulo 7: Criar detecções e realizar investigações usando o Azure Sentinel

Detecte ameaças previamente descobertas e as corrija rapidamente com orquestração e automação integradas no Azure Sentinel. Você aprenderá como criar manuais do Azure Sentinel para responder às ameaças à segurança. Você investigará o gerenciamento de incidentes do Azure Sentinel, aprenderá sobre eventos e entidades do Azure Sentinel e descobrirá maneiras de resolver incidentes. Você também aprenderá como consultar, visualizar e monitorar dados no Azure Sentinel.

Lições

- Detecção de ameaças com análises do Azure Sentinel.
- Resposta a ameaças com manuais do Azure Sentinel.
- Gerenciamento de incidentes de segurança no Azure Sentinel.
- Use a análise de comportamento de entidade no Azure Sentinel.
- Consultar, visualizar e monitorar dados no Azure Sentinel.

Depois de concluir este módulo, você será capaz de:

- Explicar a importância do Azure Sentinel Analytics.
- Criar regras a partir de modelos.
- Gerenciar regras com modificações.
- Explicar os recursos do Azure Sentinel SOAR.
- Criar um manual para automatizar uma resposta a incidentes.
- Investigar e gerenciar a resolução de incidentes.
- Explicar Análise de Comportamento de Usuário e Entidade no Azure Sentinel.
- Explorar entidades no Azure Sentinel.
- Visualizar os dados de segurança usando as pastas de trabalho do Azure Sentinel.

Módulo 8: Execute a busca de ameaças no Azure Sentinel

Neste módulo, você aprenderá a identificar proativamente os comportamentos de ameaça usando as consultas do Azure Sentinel. Você também aprenderá a usar favoritos e transmissão ao vivo para caçar ameaças. Você também aprenderá a usar blocos de anotações no Azure Sentinel para caça avançada.

Lições

- Caça a ameaças com o Azure Sentinel.
- Procure ameaças usando notebooks no Azure Sentinel.

Depois de concluir este módulo, você será capaz de:

- Descrever os conceitos de caça a ameaças para uso com o Azure Sentinel.
- Definir uma hipótese de caça a ameaças para uso no Azure Sentinel.
- Usar consultas para caçar ameaças.
- Observar as ameaças ao longo do tempo com a transm issão ao vivo.
- Explorar bibliotecas de API para caça avançada de ameaças no Azure Sentinel.
- Criar e usar blocos de anotações no Azure Sentinel.