# *Questões do Exame SC – 200*

# *Parte 1*

1. Você precisa receber um alerta de segurança quando um usuário tenta entrar de um local que nunca foi usado pelos outros usuários em sua organização para entrar.
Qual política de detecção de anomalias você deve usar?
A. Impossible travel
B. Activity from anonymous IP addresses
**C. Activity from infrequent country**
D. Malware detection

2. Sua empresa tem um único escritório em Istambul e uma assinatura do Microsoft 365.
A empresa planeja usar políticas de acesso condicional para impor a autenticação multifator (MFA). Você precisa aplicar o MFA para todos os usuários que trabalham remotamente.
O que você deve incluir na solução?

A. a fraud alert
B. a user risk policy
**C. a named location**
D. a sign-in user policy

3. Você tem uma assinatura do Microsoft 365 que contém 1.000 dispositivos Windows 10. Os dispositivos possuem o Microsoft Office 365 instalado.
Você precisa atenuar as seguintes ameaças de dispositivo:
- Macros do Microsoft Excel que baixam scripts de sites não confiáveis
- Usuários que abrem anexos executáveis no Microsoft Outlook
- Explorações de regras e formulários do Outlook

O que você deve usar?

A. Microsoft Defender Antivirus
**B. attack surface reduction rules in Microsoft Defender for Endpoint**
C. Windows Defender Firewall
D. adaptive application control in Azure Defender

4. Sua empresa implanta os seguintes serviços:
- Microsoft Defender para Identidade
- Microsoft Defender para ponto de extremidade
- Microsoft Defender para Office 365

Você precisa fornecer a um analista de segurança a capacidade de usar a Central de Segurança do Microsoft 365. O analista deve ser capaz de aprovar e

rejeitar ações pendentes geradas pelo Microsoft Defender para Endpoint. A solução deve usar o princípio do menor privilégio. Which two roles should assign to the analyst? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. the Compliance Data Administrator in Azure Active Directory (Azure AD)
**B. the Active remediation actions role in Microsoft Defender for Endpoint**
C. the Security Administrator role in Azure Active Directory (Azure AD)
**D. the Security Reader role in Azure Active Directory (Azure AD)**

5.Você tem um locatário do Microsoft 365 que usa o Microsoft Exchange Online e o Microsoft Defender para Office 365. O que você deve usar para identificar se a limpeza automática de zero hora (ZAP) moveu uma mensagem de email da caixa de correio de um usuário?

**A. the Threat Protection Status report in Microsoft Defender for Office 365 Most**
B. the mailbox audit log in Exchange
C. the Safe Attachments file types report in Microsoft Defender for Office 365
D. the mail flow report in Exchange

6. Você tem uma assinatura do Microsoft 365 E5 que usa o Microsoft SharePoint Online.
Você exclui usuários da assinatura. Você precisa ser notificado se os usuários excluídos baixaram vários documentos de sites do SharePoint Online durante o mês anterior à exclusão de suas contas. O que você deve usar?

A. a file policy in Microsoft Defender for Cloud Apps
B. an access review policy
C. an alert policy in Microsoft Defender for Office 365
**D. an insider risk policy**

7. Você tem uma assinatura do Microsoft 365 que tenha o Microsoft 365 Defender habilitado.
Você precisa identificar todas as alterações feitas nos rótulos de sensibilidade durante os últimos sete dias. O que você deve usar?

A. the Incidents blade of the Microsoft 365 Defender portal
B. the Alerts settings on the Data Loss Prevention blade of the Microsoft 365 compliance center
**C. Activity explorer in the Microsoft 365 compliance center**
D. the Explorer settings on the Email & collaboration blade of the Microsoft 365 Defender portal

8. Você tem uma assinatura do Microsoft 365 E5 que está vinculada a um locatário híbrido do Azure AD.

Você precisa identificar todas as alterações feitas no grupo Administradores de Domínio nos últimos 30 dias. O que você deve usar?

**A. the Modifications of sensitive groups report in Microsoft Defender for Identity**
B. the identity security posture assessment in Microsoft Defender for Cloud Apps
C. the Azure Active Directory Provisioning Analysis workbook
D. the Overview settings of Insider risk management

9. Você tem uma assinatura do Microsoft 365 que usa o Microsoft 365 Defender.
Você planeja criar uma consulta de caça do Microsoft Defender. Você precisa criar uma consulta controlada personalizada que será usada para avaliar o status de ameaça da assinatura.  No portal do Microsoft 365 Defender, qual página você deve usar para criar a consulta?

A. Threat analytics
**B. Advanced Hunting**
C. Explorer
D. Policies & rules

10. Você tem uma assinatura do Microsoft 365 que usa o Azure Defender.
Você tem 100 máquinas virtuais em um grupo de recursos chamado RG1.
Você atribui as funções de administrador de segurança a um novo usuário chamado SecAdmin1. Você precisa garantir que o SecAdmin1 possa aplicar correções rápidas às máquinas virtuais usando o Azure Defender. A solução deve usar o princípio do menor privilégio.
Qual função você deve atribuir ao SecAdmin1?

A. the Security Reader role for the subscription
B. the Contributor for the subscription
**C. the Contributor role for RG1**
D. the Owner role for RG1

***Questões do Exame SC – 200***

***Parte 2***

Você tem uma assinatura do Azure que tem o Microsoft Defender para Cloud habilitado. Alertas de atividades de autenticação suspeitas têm aparecido no painel Proteções de carga de trabalho. Você precisa recomendar uma solução para avaliar e corrigir os alertas usando a automação do fluxo de trabalho. A solução deve minimizar o esforço de desenvolvimento. O que você deve incluir na recomendação?

A. Azure Monitor webhooks
B. Azure Event Hubs
C. Azure Functions apps
**D. Azure Logics Apps**

2. Sua empresa tem uma infraestrutura de nuvem híbrida.
A empresa planeja contratar vários funcionários temporários dentro de um breve período. Os funcionários temporários precisarão acessar aplicativos e dados na rede local da empresa.
A política de segurança da empresa impede o uso de dispositivos pessoais para acessar dados e aplicativos da empresa.
Você precisa recomendar uma solução para fornecer ao funcionário temporário acesso aos recursos da empresa. A solução deve ser capaz de ser dimensionada sob demanda.
O que você deve incluir na recomendação?

**A. Deploy Azure Virtual Desktop, Azure Active Directory (Azure AD) Conditional Access, and Microsoft Defender for Cloud Apps.**
B. Redesign the VPN infrastructure by adopting a split tunnel configuration.
C. Deploy Microsoft Endpoint Manager and Azure Active Directory (Azure AD) Conditional Access.
D. Migrate the on-premises applications to cloud-based applications.

3. Sua empresa está se preparando para a adoção da nuvem. Você está projetando a segurança para zonas de aterrissagem do Azure. Quais dois controles preventivos você pode implementar para aumentar a pontuação segura? Cada resposta correta apresenta uma solução completa.
NOTA: Cada seleção correta vale um ponto.

**A. Azure Web Application Firewall (WAF)**
B. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
C. Microsoft Sentinel

**D. Azure Firewall**
E. Microsoft Defender for Cloud alerts

4. Você tem uma assinatura do Azure que tem o Microsoft Defender para Cloud habilitado.
Você precisa aplicar os padrões ISO 27001:2013 para a assinatura. A solução deve garantir que os recursos não compatíveis sejam corrigidos automaticamente.
O que você deve usar?

**A. Azure Policy**
B. Azure Blueprints
C. the regulatory compliance dashboard in Defender for Cloud
D. Azure role-based access control (Azure RBAC)

5. Você tem uma assinatura do Microsoft 365 e uma assinatura do Azure. O Microsoft 365 Defender e o Microsoft Defender para Nuvem estão habilitados. A assinatura do Azure contém 50 máquinas virtuais. Cada máquina virtual executa aplicativos diferentes no Windows Server 2019. Você precisa recomendar uma solução para garantir que somente aplicativos autorizados possam ser executados nas máquinas virtuais. Se um aplicativo não autorizado tentar ser executado ou instalado, o aplicativo deverá ser bloqueado automaticamente até que um administrador autorize o aplicativo.
Qual controle de segurança você deve recomendar?

**A. adaptive application controls in Defender for Cloud**
B. app protection policies in Microsoft Endpoint Manager
C. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps
D. Azure Security Benchmark compliance controls in Defender for Cloud

6. Você tem uma assinatura do Azure que é usada como uma zona de aterrissagem do Azure para um aplicativo.
Você precisa avaliar a postura de segurança de todas as cargas de trabalho na zona de pouso.
O que você deve fazer primeiro?

A. Configure Continuous Integration/Continuous Deployment (CI/CD) vulnerability scanning.
B. Obtain Azure AD Premium Plan 2 licenses.
C. Add Microsoft Sentinel data connectors.
**D. Enable the Defender plan for all resource types in Microsoft Defender for Cloud.**

7. Você tem o Microsoft Defender for Cloud atribuído a grupos de gerenciamento do Azure.
Você tem uma implantação do Microsoft Sentinel.

Durante a triagem de alertas, você precisa de informações adicionais sobre os eventos de segurança, incluindo sugestões de correção.
Quais dois componentes você pode usar para atingir o objetivo? Cada resposta correta apresenta uma solução completa.
NOTA: Cada seleção correta vale um ponto.

**A. Microsoft Sentinel threat intelligence workbooks**
B. Microsoft Sentinel notebooks
**C. threat intelligence reports in Defender for Cloud**
D. workload protections in Defender for Cloud

8. Um cliente está implantando imagens do Docker em 10 recursos do Serviço Kubernetes do Azure (AKS) em quatro assinaturas do Azure. Você está avaliando a postura de segurança do cliente. Você descobre que os recursos do AKS estão excluídos das recomendações de pontuação segura. Você precisa produzir recomendações precisas e atualizar a pontuação segura. Quais duas ações você deve recomendar no Microsoft Defender para Nuvem? Cada resposta correta apresenta parte da solução.
NOTA: Cada seleção correta vale um ponto.

**A. Enable Defender plans.**
**B. Configure auto provisioning.**
C. Add a workflow automation.
D. Assign regulatory compliance policies.
E. Review the inventory.

9. Você tem o Microsoft Defender for Cloud atribuído a grupos de gerenciamento do Azure.
Você tem uma implantação do Microsoft Sentinel.
Durante a triagem de alertas, você precisa de informações adicionais sobre os eventos de segurança, incluindo sugestões de correção.
Quais dois componentes você pode usar para atingir o objetivo? Cada resposta correta apresenta uma solução completa.
NOTA: Cada seleção correta vale um ponto.

**A. Microsoft Sentinel threat intelligence workbooks**
B. Microsoft Sentinel notebooks
C. threat intelligence reports in Defender for Cloud
D. workload protections in Defender for Cloud

10. Sua empresa tem um escritório em Seattle.
A empresa tem dois conjuntos de dimensionamento de máquina virtual do Azure hospedados em redes virtuais diferentes.
A empresa planeja contratar desenvolvedores na Índia.
Você precisa recomendar uma solução que forneça aos desenvolvedores a capacidade de se conectar às máquinas virtuais por SSL a partir do portal do Azure. A solução deve atender aos seguintes requisitos:

☞ Impedir a exposição dos endereços IP públicos das máquinas virtuais.
☞ Forneça a capacidade de se conectar sem usar uma VPN.
☞ Minimize os custos.
Quais duas ações você deve executar? Cada resposta correta apresenta parte da solução.
NOTA: Cada seleção correta vale um ponto.

**A. Create a hub and spoke network by using virtual network peering.**
B. Deploy Azure Bastion to each virtual network.
**C. Deploy Azure Bastion to one virtual network.**
D. Create NAT rules and network rules in Azure Firewall.
E. Enable just-in-time VM access on the virtual machines.

***Questões do Exame SC – 200***

***Parte 3***

1. You have a third-party security information and event management (SIEM) solution.

You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign-events in near real time.

What should you do to route events to the SIEM solution?

A. Create an Azure Sentinel workspace that has a Security Events connector.

**B. Configure the Diagnostics settings in Azure AD to stream to an event hub.**

C. Create an Azure Sentinel workspace that has an Azure Active Directory connector.

D. Configure the Diagnostics settings in Azure AD to archive to a storage account.

2. You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually.

You deploy Azure Sentinel.

You need to use the existing logic app as a playbook in Azure Sentinel.

What should you do first?

A. And a new scheduled query rule.

B. Add a data connector to Azure Sentinel.

C. Configure a custom Threat Intelligence connector in Azure Sentinel.

**D. Modify the trigger in the logic app.**

3. Your company uses Azure Sentinel to manage alerts from more than 10,000 IoT devices.

A security manager at the company reports that tracking security threats is increasingly difficult due to the large number of incidents.

You need to recommend a solution to provide a custom visualization to simplify the investigation of threats and to infer threats by using machine learning.

What should you include in the recommendation?

A. built-in queries

B. livestream

**C. notebooks**

D. bookmarks

4. You have an Azure Sentinel workspace.

You need to test a playbook manually in the Azure portal.

From where can you run the test in Azure Sentinel?

A. Playbooks

B. Analytics

C. Threat intelligence

**D. Incidents**

4. You have a custom analytics rule to detect threats in Azure Sentinel.

You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED.

What is a possible cause of the issue?

A. There are connectivity issues between the data sources and Log Analytics.

B. The number of alerts exceeded 10,000 within two minutes.

C. The rule query takes too long to run and times out.

**D. Permissions to one of the data sources of the rule query were modified.**

5. Your company uses Azure Sentinel.

A new security analyst reports that she cannot assign and resolve incidents in Azure Sentinel.

You need to ensure that the analyst can assign and resolve incidents. The solution must use the principle of least privilege.

Which role should you assign to the analyst?

**A. Azure Sentinel Responder**

B. Logic App Contributor

C. Azure Sentinel Contributor

D. Azure Sentinel Reader

6. You recently deployed Azure Sentinel.

You discover that the default Fusion rule does not generate any alerts. You verify that the rule is enabled.

You need to ensure that the Fusion rule can generate alerts.

What should you do?

A. Disable, and then enable the rule.

**B. Add data connectors**

C. Create a new machine learning analytics rule.

D. Add a hunting bookmark.

A company uses Azure Sentinel.

7. You need to create an automated threat response.

What should you use?

A. a data connector

**B. a playbook**

C. a workbook

D. a Microsoft incident creation rule

8. You have an Azure Sentinel deployment in the East US Azure region.

You create a Log Analytics workspace named LogsWest in the West US Azure region.

You need to ensure that you can use scheduled analytics rules in the existing Azure Sentinel deployment to generate alerts based on queries to LogsWest.

What should you do first?

A. Deploy Azure Data Catalog to the West US Azure region.

B. Modify the workspace settings of the existing Azure Sentinel deployment.

**C. Add Azure Sentinel to a workspace.**

D. Create a data connector in Azure Sentinel.

9. You create a custom analytics rule to detect threats in Azure Sentinel.

You discover that the rule fails intermittently.

What are two possible causes of the failures? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

**A. The rule query takes too long to run and times out.**

B. The target workspace was deleted.

C. Permissions to the data sources of the rule query were modified.

**D. There are connectivity issues between the data sources and Log Analytics**

You need to visualize Azure Sentinel data and enrich the data by using third-party data sources to identify indicators of compromise (IoC).

What should you use?

**A. notebooks in Azure Sentinel**

B. Microsoft Cloud App Security

C. Azure Monitor

D. hunting queries in Azure Sentinel