SC-200 Bestehen Sie Microsoft Security Operations Analyst! - mit höhere Effizienz und weniger Mühen

P.S. Kostenlose und neue SC-200 Prüfungsfragen sind auf Google Drive freigegeben von ITZert verfügbar: https://drive.google.com/open?id=1SjZCEpINEk2rmX4Orlcx8dardpLFAAcb

Die Microsoft SC-200 Zertifizierungsprüfung ist eine sehr populäre Prüfung. Obwohl es sehr schwierig zu bestehen ist, können Sie diese Prüfung leichter bestehen, wenn Sie die richtige Methode finden. Und Wir ITZert sind Ihre beste Wahl. Mit der 100%-Hitrate Prüfungsunterlagen von ITZert können Sie alle Probleme in der Microsoft SC-200 Zertifizierungsprüfung auslösen. Wenn Sie die Prüfungsfragen und Testantworten ernst lernen, gibt es keine Probleme für Sie. Und nach dem Kauf können Sie einjährigen kostlosen Aktualisierungsservice bekommen. (innerhalb einem Jahr) Sie können über die gewünschten Microsoft SC-200 Schulungsunterlagen beherrschen, wenn Sie auf jeden Fall die neueste Version bekommen. Probieren Sie sofort, bitte.

Die Microsoft SC-200 (Microsoft Security Operations Analyst) Prüfung ist eine Zertifizierungsprüfung, die für Sicherheitsfachleute entwickelt wurde, die Fähigkeiten in Bedrohungsschutz, Informations- und Vorfallreaktion, Schwachstellenmanagement sowie Governance-, Risiko- und Compliance-Management (GRC) besitzen. Diese Prüfung bestätigt das Wissen des Kandidaten, Sicherheitsvorfälle mithilfe verschiedener Sicherheitstools und -techniken zu identifizieren, zu untersuchen und darauf zu reagieren.

Die Microsoft SC-200 Zertifizierung wird in der Branche sehr geschätzt, da sie die Fähigkeiten und Kenntnisse validiert, die für eine effektive Sicherung von Microsoft-Umgebungen erforderlich sind. Sie bietet Sicherheitsfachleuten die Möglichkeit, ihre Expertise unter Beweis zu stellen und sich auf dem Arbeitsmarkt abzuheben. Darüber hinaus kann die Zertifizierung Fachleuten helfen, ihre Karriere voranzutreiben und höhere Gehälter zu verdienen. Insgesamt ist die Microsoft SC-200 Zertifizierung eine ausgezeichnete Investition für Sicherheitsfachleute, die ihre Fähigkeiten und Kenntnisse in Microsoft-Sicherheitstechnologien verbessern möchten.

>> SC-200 Trainingsunterlagen <<

Echte und neueste SC-200 Fragen und Antworten der Microsoft SC-200 Zertifizierungsprüfung

Die Microsoft SC-200 Dumps von ITZert sind die Unterlagen, die von vielen Kadidaten geprüft sind. Und es kann die sehr hohe Durchlaufrate garantieren. Wenn Sie nach der Nutzung der Dumps bei der Microsoft SC-200 Zertifizierung durchgefallen sind, geben wir ITZert Ihnen voll Geld zurück. Oder können Sie auch die kostlosen aktualisierten Dumps bekommen. Mit der Garantie sorgen Sie sich bitte nicht.

Microsoft Security Operations Analyst SC-200 Prüfungsfragen mit Lösungen (Q135-Q140):

135. Frage
You need to configure the Azure Sentinel integration to meet the Azure Sentinel requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Antwort:

Begründung:

Reference:
https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel

136. Frage
You have a Microsoft Sentinel workspace that contains an Azure AD data connector.
You need to associate a bookmark with an Azure AD-related incident.
What should you do? To answer, drag the appropriate blades to the correct tasks. Each blade may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content NOTE: Each correct selection is worth one point.

Antwort:

Begründung:
Explanation:
You can use the Logs blade or incident blade to create a bookmark of an Azure AD-related incident. Once the bookmark is created, you can associate it with the incident by using the incident blade. This allows you to quickly and easily access important information related to the incident in the future.

137. Frage
You have 50 on-premises servers.
You have an Azure subscription that uses Microsoft Defender for Cloud. The Defender for Cloud deployment has Microsoft Defender for Servers and automatic provisioning enabled.
You need to configure Defender for Cloud to support the on-premises servers. The solution must meet the following requirements:
* Provide threat and vulnerability management.
* Support data collection rules.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Antwort:

Begründung:
Explanation:
To integrate on-premises servers into Microsoft Defender for Cloud and support features such as Threat and Vulnerability Management (TVM) and data collection rules, the servers must first be connected to Azure Arc. Azure Arc allows non-Azure servers to be managed as Azure resources and enables Defender for Cloud capabilities such as endpoint protection, vulnerability management, and compliance assessment.
The correct sequence of steps is:
1## Generate the installation script:
In the Azure portal, navigate to Azure Arc # Servers # Add. From there, select the appropriate subscription and resource group, then generate the Azure Arc onboarding script. This script includes registration commands and configuration for the machine to connect to Azure.
2## Install the Azure Connected Machine agent:
On each on-premises server, run the generated script. This installs the Azure Connected Machine agent (Azure Arc agent), which establishes communication between the on-premises server and Azure. After installation, the server appears as an Arc-enabled machine in the Azure portal.
3## Create an Azure Arc Data Controller (if data services are required):
Once the machines are connected, you can configure data services or additional Defender for Cloud features (such as data collection and TVM). The Azure Arc Data Controller provides hybrid data capabilities for managing and monitoring on-premises workloads.
This sequence aligns with Microsoft's Defender for Cloud documentation and Arc onboarding best practices, ensuring minimal administrative overhead while enabling full SecOps visibility across hybrid environments.

138. Frage
You need to create a query for a workbook. The query must meet the following requirements:
* List all incidents by incident number.
* Only include the most recent log for each incident.
How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Antwort:

Begründung:
Explanation:
Reference:
https://www.drware.com/whats-new-soc-operational-metrics-now-available-in-sentinel/

139. Frage
You have a Microsoft 365 subscription that uses Microsoft Defender XDR.
You discover that when Microsoft Defender for Endpoint generates alerts for a commonly used executable file, it causes alert fatigue. You need to tune the alerts.
Which two actions can an alert tuning rule perform for the alerts?
Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

- A. hide
- B. merge
- C. resolve
- D. assign
- E. delete

Antwort: A,C

Begründung:
Microsoft's alert-tuning capability (previously called suppression) in Microsoft Defender is intentionally focused on reducing alert noise by changing the handling of alerts that match defined conditions. When you open the Tune alert pane for an alert you can define conditions and then choose an action. The product documentation and the Tune alert UI show two supported actions: Hide alert (prevents the alert from surfacing in the default alert queue / UI) and Resolve alert (automatically close/resolve the alert so it no longer requires manual triage). Those two actions are the built-in tuning outcomes designed to reduce fatigue from frequent false positives. Other operations listed in the question-such as deleting alerts, merging alerts, or assigning ownership-are not offered as actions inside the alert-tuning rule itself (assigning or other workflow actions are available elsewhere in the product or via automation), so the only valid tuning rule actions are hide and resolve. This behavior is documented in the Microsoft Defender (XDR) "investigate and tune alerts" guidance and in the alert-tuning (suppression) documentation.

140. Frage
.....

- SC-200 Prüfungsfragen □ SC-200 Prüfungsfragen □ SC-200 Zertifizierungsfragen ⤴ URL kopieren { www.echtefrage.top } Öffnen und suchen Sie ☀ SC-200 □☀□ Kostenloser Download □SC-200 Antworten
- SC-200 Fragenkatalog □ SC-200 Zertifizierungsfragen □ SC-200 Fragenpool □ Suchen Sie auf 【 www.itzert.com 】 nach kostenlosem Download von 《 SC-200 》 □SC-200 Buch
- SC-200 Übungsmaterialien □ SC-200 Zertifizierungsfragen □ SC-200 Dumps □ Öffnen Sie die Website ▸ www.echtefrage.top ◂ Suchen Sie （ SC-200 ） Kostenloser Download □SC-200 Zertifizierungsfragen
- SC-200 Deutsche Prüfungsfragen □ SC-200 Lernhilfe □ SC-200 Testing Engine □ Erhalten Sie den kostenlosen Download von 【 SC-200 】 mühelos über ▸ www.itzert.com ◂ □SC-200 Prüfungsfragen
- SC-200 Testing Engine □ SC-200 Kostenlos Downloden □ SC-200 Fragenpool □ URL kopieren ➥ www.pruefungfrage.de □ Öffnen und suchen Sie ▹ SC-200 ◃ Kostenloser Download □SC-200 Quizfragen Und Antworten
- www.stes.tyc.edu.tw, portal.mathtutorofflorida.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, academy.gti.com.ng, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes

2026 Die neuesten ITZert SC-200 PDF-Versionen Prüfungsfragen und SC-200 Fragen und Antworten sind kostenlos verfügbar: https://drive.google.com/open?id=1SjZCEpINEk2rmX4Orlcx8dardpLFAAcb