Prüfungsnummer:SC-200-deutsch

Prüfungsname:(deutsche Version und englische Version) Microsoft Security Operations Analyst

Version:demo

Achtung: Aktuelle englische Version zu SC-200 bei uns ist gratis!!

1.Sie sind als Cloudadministrator für das Unternehmen it-pruefungen.de tätig. Das Unternehmen hat ein Microsoft 365-Abonnement, das Azure Defender verwendet.

Sie haben 100 virtuelle Maschinen in einer Ressourcengruppe mit dem Namen RG1.

Sie weisen einem neuen Benutzer mit dem Namen SecAdmin1 die Rolle Sicherheitsadministrator zu.

Sie müssen sicherstellen, dass SecAdmin1 mithilfe von Azure Defender Korrekturoptionen auf die virtuellen Computer anwenden kann. Die Lösung muss das Prinzip der Vergabe geringstmöglicher Berechtigungen verwenden.

Welche Rolle sollten Sie SecAdmin1 zuweisen?

A.Die Rolle Sicherheitsleseberechtigter für das Abonnement
B.Die Rolle Mitwirkender für das Abonnement
C.Die Rolle Mitwirkender für RG1
D.Die Besitzerrolle für RG1

Korrekte Antwort: C

Erläuterungen:

Azure Security Center-Empfehlungen enthalten Vorschläge dazu, wie Sie Ihre Ressourcen besser schützen können. Sie implementieren eine Empfehlung, indem Sie die in der Empfehlung beschriebenen Schritte zur Bereinigung ausführen. Um die Behebung zu vereinfachen und die Sicherheit Ihrer Umgebung zu verbessern (und Ihre Sicherheitsbewertung zu erhöhen), enthalten viele Empfehlungen eine Korrektur-Option. Die Korrektur hilft Ihnen, eine Empfehlung für mehrere Ressourcen schnell zu korrigieren.

Die Rolle des Sicherheitsadministrators gewährt SecAdmin1 vollen Zugriff auf das Azure Security Center. SecAdmin1 benötigt jedoch zusätzlich Berechtigungen, um die Konfigurationsänderungen auf die virtuellen Computer anzuwenden.

Die Rolle Mitwirkender gewährt Vollzugriff zum Verwalten aller Ressourcen innerhalb des Gültigkeitsbereichs, allerdings nicht zum Zuweisen von Rollen in Azure RBAC oder zum Verwalten von Zuweisungen in Azure Blueprints.

Der folgende Microsoft Docs-Artikel enthält weitere Informationen zum Thema:

Umsetzen von Empfehlungen in Azure Security Center

2.Sie stellen einen virtuellen Linux Computer in einem neuen Azure Abonnement bereit.

Sie aktivieren Azure Defender und integrieren den virtuellen Computer in Azure Defender.

Sie müssen überprüfen, ob ein Angriff auf den virtuellen Computer eine Warnung in Azure Defender auslöst.

Welche zwei Bash-Befehle sollten Sie auf der virtuellen Maschine ausführen?

(Jede korrekte Antwort stellt einen Teil der Lösung dar. Wählen Sie zwei Antworten.)

A.cp /bin/echo ./asc_alerttest_662jfi039n
B../alerttest testing eicar pipe
C.cp /bin/echo ./alerttest
D../asc_alerttest_662jfi039n testing eicar pipe

Korrekte Antwort: A, D

Erläuterungen:

Wenn Sie die neuen Vorschaufunktionen für Warnungen verwenden, die unter Verwalten von und Reagieren auf Sicherheitswarnungen in Azure Security Center beschrieben werden, können Sie Beispielwarnungen erstellen. Dafür sind nur einige wenige Klicks im Azure-Portal auf der Seite „Sicherheitswarnungen“ erforderlich.

Verwenden Sie Beispielwarnungen für Folgendes:

Evaluieren des Werts und der Möglichkeiten von Azure Defender
Überprüfen von Konfigurationen, die Sie für Ihre Sicherheitswarnungen vorgenommen haben (z. B. SIEM-Integrationen, Workflowautomatisierung und E-Mail-Benachrichtigungen)
Simulieren von Warnungen auf Ihren Azure-VMs (Linux)

Nach der Installation des Security Center-Agents auf Ihrem Computer führen Sie auf dem Computer, auf dem sich die angegriffene Ressource für die Warnung befinden soll, die folgenden Schritte aus:

Kopieren Sie eine ausführbare Datei an einem geeigneten Speicherort, und benennen Sie sie in ./asc_alerttest_662jfi039n um. Beispiel:

cp /bin/echo ./asc_alerttest_662jfi039n

Öffnen Sie die Eingabeaufforderung, und führen Sie diese Datei aus:

./asc_alerttest_662jfi039n testing eicar pipe

Warten Sie fünf bis zehn Minuten, und öffnen Sie die Security Center-Warnungen. Eine Warnung sollte angezeigt werden.

Der folgende Microsoft Docs-Artikel enthält weitere Informationen zum Thema:

Generieren von Azure Defender-Beispielwarnungen

3.Sie konfigurieren Azure Sentinel. Sie müssen eine Microsoft Teams-Nachricht an einen Kanal senden, wenn eine Anmeldung von einer verdächtigen IP-Adresse erkannt wird.

Welche beiden Aktionen sollten Sie in Azure Sentinel ausführen?

(Jede korrekte Antwort stellt einen Teil der Lösung dar. Wählen Sie zwei Antworten.)

A.Erstellen Sie ein Playbook.
B.Verknüpfen Sie ein Playbook mit einem Incident.
C.Aktivieren Sie das Entity Behavior Analytics-Feature von Azure Sentinel.
D.Erstellen Sie eine Arbeitsmappe.
E.Aktivieren Sie die Regel vom Typ Fusion.

Korrekte Antwort: A, B

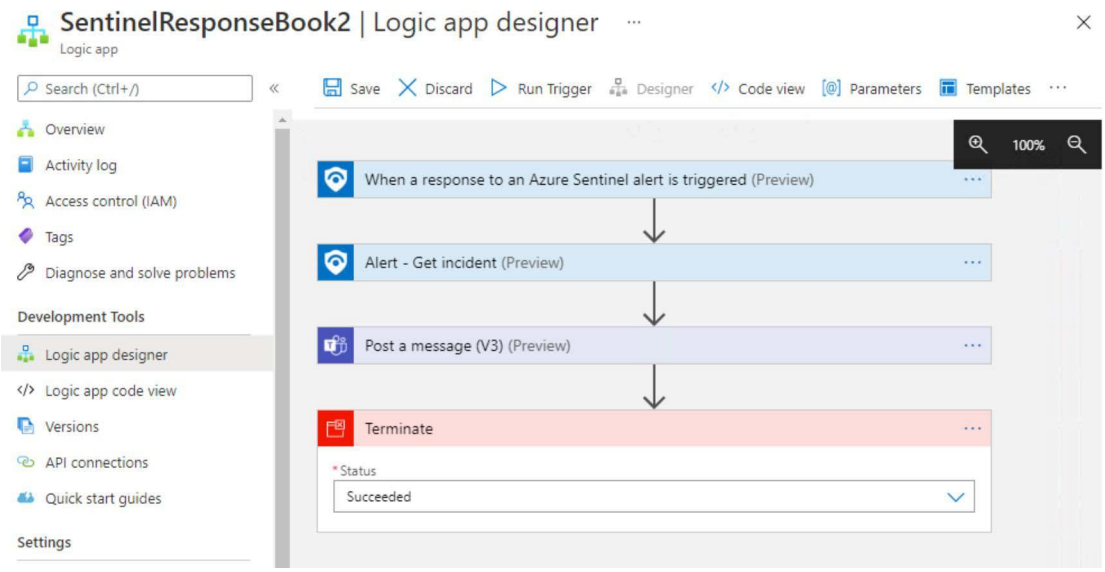
Erläuterungen:

Automatisierungsregeln helfen bei der Selektierung von Vorfällen in Azure Sentinel. Hiermit können Sie Vorfälle automatisch den richtigen Mitarbeitern zuweisen, überflüssige Vorfälle oder bekannte False Positives schließen, den Schweregrad ändern und Tags hinzufügen. Außerdem sind sie der Mechanismus, mit dem Playbooks als Reaktion auf Vorfälle ausgeführt werden können.

Bei Playbooks handelt es sich um eine Sammlung von Prozeduren, die über Azure Sentinel als Reaktion auf eine Warnung oder einen Vorfall ausgeführt werden können. Ein Playbook kann Ihnen dabei helfen, Ihre Reaktion zu automatisieren und zu orchestrieren, und es kann so festgelegt werden, dass es automatisch ausgeführt wird, wenn bestimmte Warnungen oder Vorfälle generiert werden. Hierzu wird es an eine Analyseregel oder an eine Automatisierungsregel angefügt. Bei Bedarf kann es aber auch manuell ausgeführt werden.

Da Playbooks in Azure Sentinel auf in Azure Logic Apps erstellten Workflows basieren, stehen Ihnen die Leistung, Anpassbarkeit und integrierten Vorlagen zur Verfügung, die Sie von Logic Apps gewohnt sind. Jedes Playbook wird zwar speziell für das Abonnement erstellt, zu dem es gehört, unter Playbooks werden jedoch alle Playbooks angezeigt, die für alle ausgewählten Abonnements verfügbar sind.

Das folgende Playbook postet eine Nachricht in einen definierten Microsoft Teams-Kanal, wenn eine Reaktion auf eine Azure Sentinel-Warnung ausgelöst wird.



Der folgende Microsoft Docs-Artikel enthält weitere Informationen zum Thema:

Tutorial: Verwenden von Playbooks mit Automatisierungsregeln in Azure Sentinel

4.Sie planen, eine benutzerdefinierte Azure Sentinel-Abfrage zu erstellen, die eine visuelle Darstellung der von Azure Security Center generierten Sicherheitswarnungen bereitstellt.

Sie müssen eine Abfrage erstellen, die verwendet wird, um ein Balkendiagramm anzuzeigen.

Was sollten Sie in die Abfrage aufnehmen?

A.extend
B.bin
C.count
D.workspace

Korrekte Antwort: C

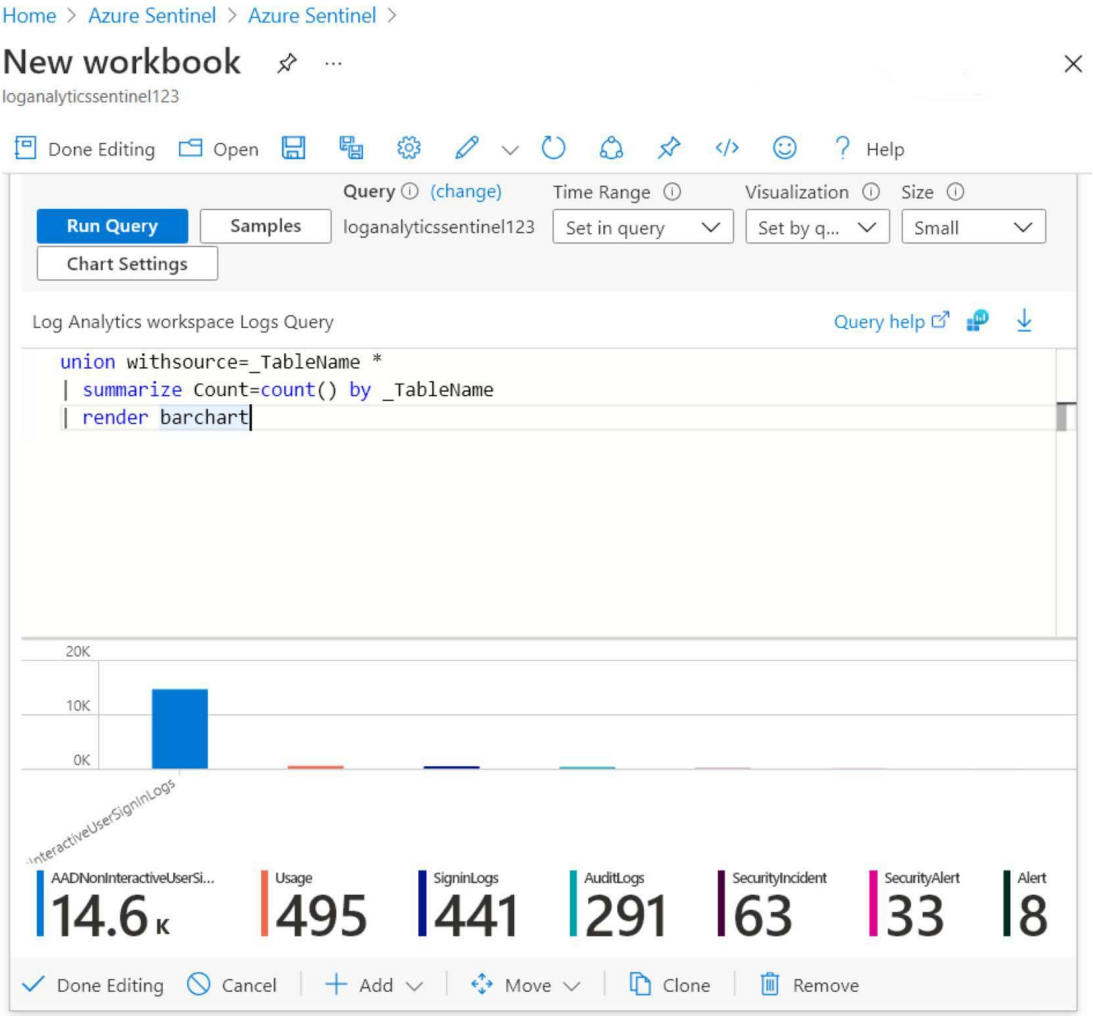
In Arbeitsmappen können Überwachungsdaten in Diagrammen präsentiert werden. Unterstützte Diagrammtypen sind Liniendiagramm, Balkendiagramm, Balkendiagramm (kategorisch), Flächendiagramm, Punktdiagramm, Kreisdiagramm und Zeitdiagramm. Ersteller können u. a. Höhe, Breite, Farbpalette, Legende, Titel und die Meldung „Keine Daten“ für das Diagramm anpassen. Außerdem können über Diagrammeinstellungen Achsentypen und Datenreihenfarben angepasst werden.

Arbeitsmappen unterstützen Diagramme für Protokolle und Metrikdatenquellen.

Zeitreihendiagramme wie Bereichs-, Balken-, Linien-, Punkt- und Zeitdiagramme können mithilfe des Steuerelements für Abfragen in Workbooks einfach erstellt werden. Entscheidend ist, über Zeit- und Metrikinformationen im Resultset zu verfügen.

We have to aggregate the security alerts by using the count() function. The desired chart type can be specified by the render keyword.

Wir müssen die count()-Funktion verwenden, um die Sicherheitswarnungen zu aggregieren. Für das Rendern des Ergebnissatzes als Balkendiagramm wird das Schlüsselwort render verwendet.



Der folgende Microsoft-Artikel enthält weitere Informationen zum Thema:

Azure Sentinel Workbooks

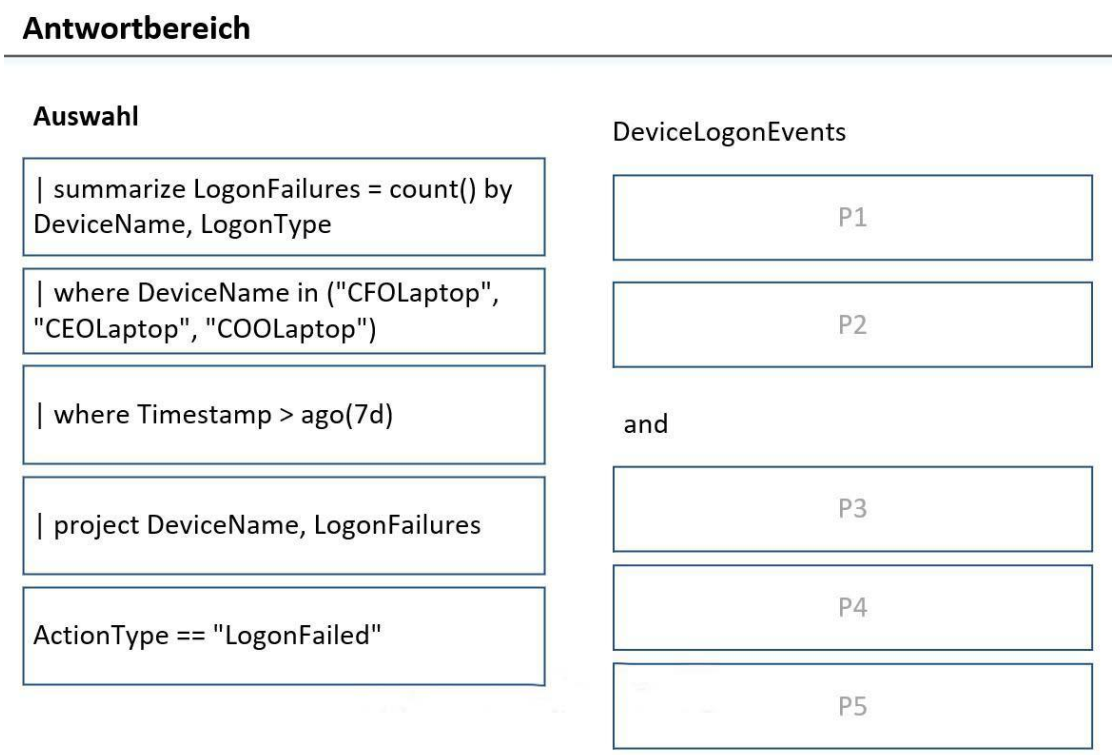
5.Sie sind als Cloudadministrator für das Unternehmen it-pruefungen.de tätig. Sie untersuchen einen Vorfall mithilfe von Microsoft 365 Defender.

Sie müssen eine erweiterte Suche erstellen, um fehlgeschlagene Anmeldeauthentifizierungen auf drei Geräten mit den Namen CFOLaptop, CEOLaptop und COOLaptop zu erkennen.

Wie vervollständigen Sie die Abfrage?

(Die verfügbaren Abfragesegmente werden in der Abbildung dargestellt. Klicken Sie auf die Schaltfläche Zeichnung und ordnen Sie die Segmente in der richtigen Reihenfolge an.)

Abbildung



A.P1: | project DeviceName, LogonFailures
P2: | where Timestamp > ago(7d) and
P3: | where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop")
P4: | summarize LogonFailures = count() by DeviceName, LogonType
P5: ActionType == "LogonFailed"
B.P1: | where Timestamp > ago(7d)
P2: | where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop") and
P3: ActionType == "LogonFailed"
P4: | summarize LogonFailures = count() by DeviceName, LogonType
P5: | project DeviceName, LogonFailures
C.P1: ActionType == "LogonFailed"
P2: | summarize LogonFailures = count() by DeviceName, LogonType and
P3: | project DeviceName, LogonFailures
P4: | where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop"
P5: | where Timestamp > ago(7d)
D.P1: | where Timestamp > ago(7d)
P2: | summarize LogonFailures = count() by DeviceName, LogonType and
P3: ActionType == "LogonFailed"
P4: | where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop")
P5: | project DeviceName, LogonFailures

Korrekte Antwort: B

Erläuterungen:

Bei der erweiterten Suche handelt es sich um ein abfragebasiertes Tool für die Bedrohungssuche, mit dem Sie Rohdaten von bis zu 30 Tagen erkunden können. Sie können Ereignisse in Ihrem Netzwerk proaktiv überprüfen, um Bedrohungsindikatoren und Entitäten zu finden. Der flexible Zugriff auf Daten ermöglicht eine uneingeschränkte Suche nach bekannten und potenziellen Bedrohungen.

Die DeviceLogonEvents Tabelle im Schema der erweiterten Suche enthält Informationen zu Benutzeranmeldungen und anderen Authentifizierungsereignissen auf Geräten.

Die Abfrage selbst beginnt in der Regel mit einem Tabellennamen gefolgt von mehreren Elementen, die mit einer Pipe beginnen (|).

```
DeviceLogonEvents
| where Timestamp > ago(7d)
| where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop")
and
ActionType == "LogonFailed"
| summarize LogonFailures = count() by DeviceName, LogonType
| project DeviceName, LogonFailures
```

Die folgenden -Artikel enthalten weitere Informationen zum Thema:

Proaktive Suche nach Bedrohungen mit erweiterter Suche

rlernen der Abfragesprache für die erweiterte Suche

DeviceLogonEvents

6.Sie haben ein Microsoft 365 E5-Abonnement. Sie planen, domänenübergreifende Untersuchungen mit Microsoft 365 Defender durchzuführen.

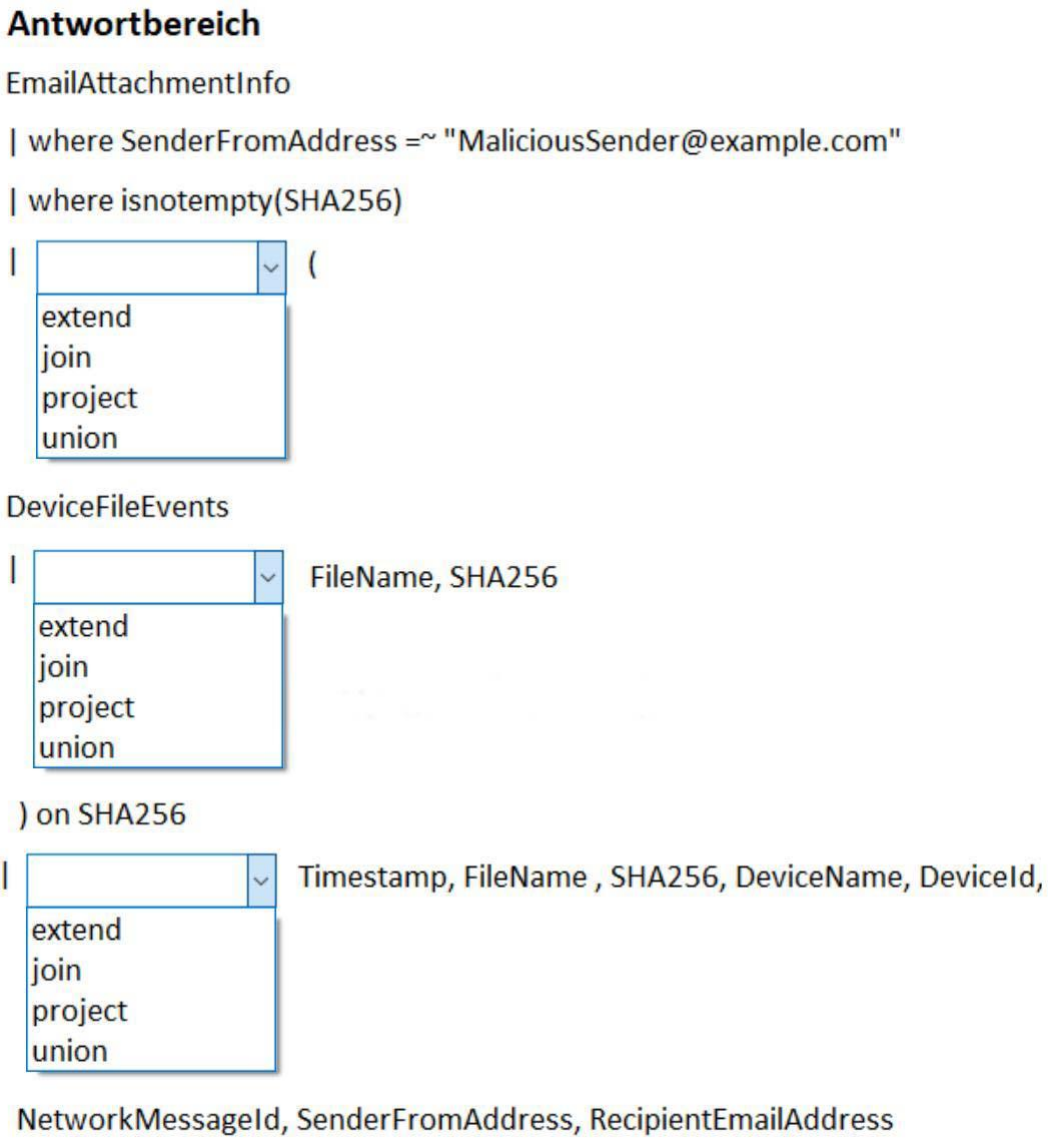
Sie müssen eine erweiterte Suche erstellen, um Geräte zu identifizieren, die von einem schädlichen E-Mail-Anhang betroffen sind.

Wie vervollständigen Sie die gezeigte Abfrage?

(Wählen Sie zum Beantworten der Frage die entsprechenden Optionen im Antwortbereich aus. Für jede richtige Auswahl erhalten Sie einen Punkt.)

Abbildung

Antwortbereich



A.P1: union
P2: join
P3: project
B.P1: join
P2: extend
P3: project
C.P1: union
P2: project
P3: extend
D.P1: join
P2: project
P3: project

Korrekte Antwort: D

Erläuterungen:

Wenn Sie von einer E-Mail-Adresse wissen, die schädliche Dateien (MaliciousSender@example.com) sendet, können Sie diese Abfrage ausführen, um zu ermitteln, ob Dateien von diesem Absender auf Ihren Geräten vorhanden sind.Sie können diese Abfrage beispielsweise verwenden, um Geräte zu identifizieren, die von einer Schadsoftwareverteilungskampagne betroffen sind.

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
//Get emails with attachments identified by a SHA-256
| where isnotempty(SHA256)
| join (
//Check devices for any activity involving the attachments
DeviceFileEvents
| project FileName, SHA256
) on SHA256
| project Timestamp, FileName , SHA256, DeviceName, DeviceId,    NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Der folgende Microsoft Docs-Artikel enthält weitere Informationen zum Thema:

Gefahrensuche über Geräte, E-Mails, Apps und Identitäten hinweg

7.Sie sind als Cloudadministrator für das Unternehmen it-pruefungen.de tätig. Das Unternehmen hat ein Azure Abonnement. Azure Defender ist für alle unterstützten Ressourcentypen aktiviert.

Sie erstellen eine Azure Logik-App mit dem Namen LA1.

Sie planen, LA1 zu verwenden, um in Azure Security Center erkannte Sicherheitsrisiken automatisch zu korrigieren.

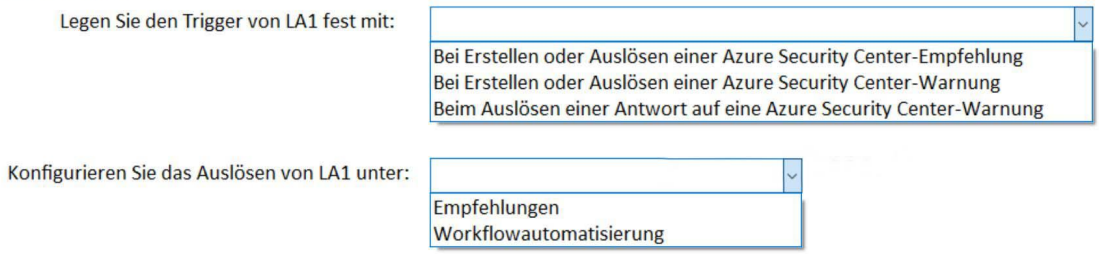
Sie müssen LA1 im Security Center testen.

Wie gehen Sie vor?

(Wählen Sie zum Beantworten der Frage die entsprechenden Optionen im Antwortbereich aus. Für jede richtige Auswahl erhalten Sie einen Punkt.)

Abbildung

Antwortbereich

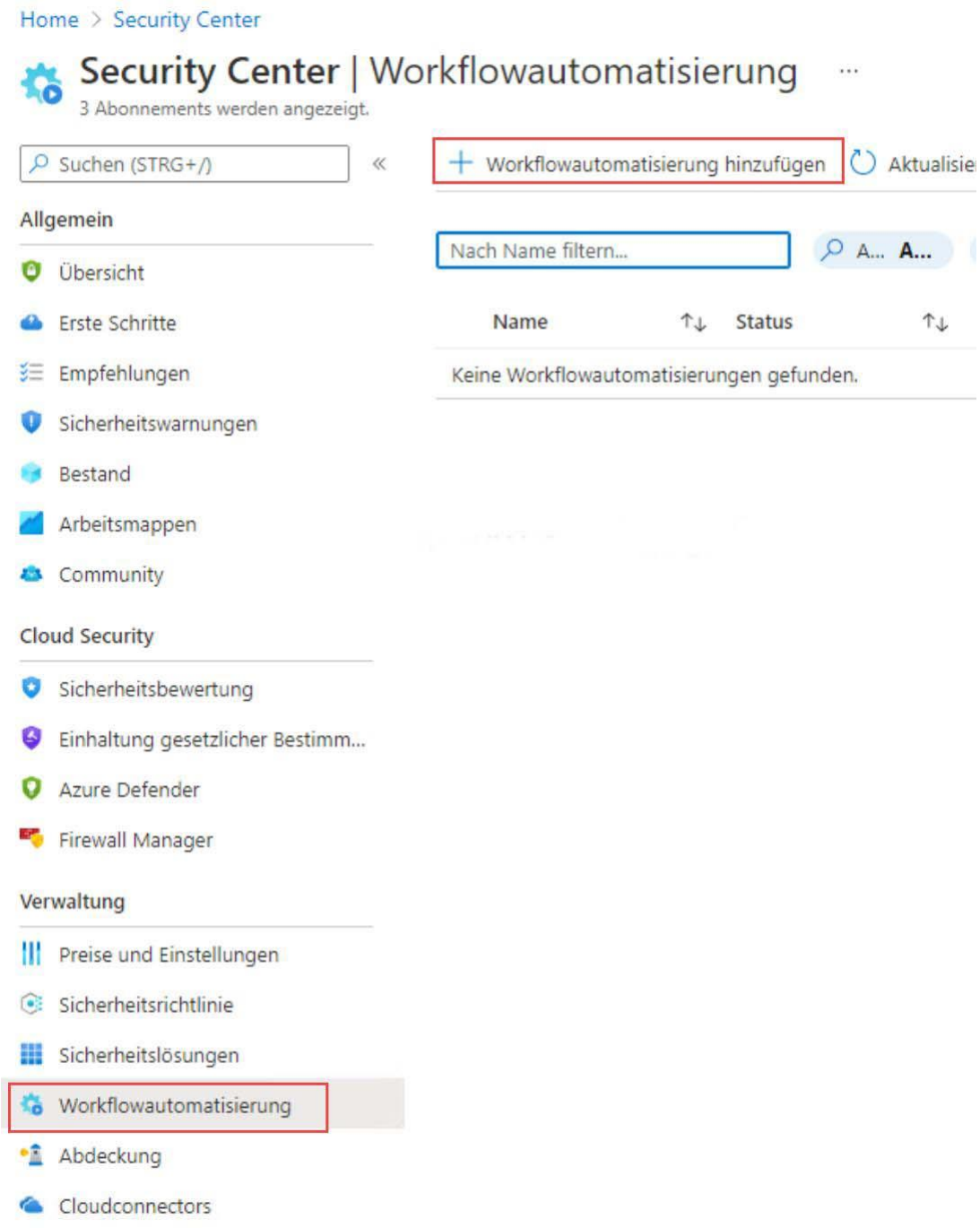


A.Legen Sie den Trigger von LA1 fest mit: Bei Erstellen oder Auslösen einer Azure Security Center-Empfehlung
Konfigurieren Sie das Auslösen von LA1 unter: Empfehlungen
B.Legen Sie den Trigger von LA1 fest mit: Bei Erstellen oder Auslösen einer Azure Security Center-Empfehlung
Konfigurieren Sie das Auslösen von LA1 unter: Workflowautomatisierung
C.Legen Sie den Trigger von LA1 fest mit: Bei Erstellen oder Auslösen einer Azure Security Center-Warnung
Konfigurieren Sie das Auslösen von LA1 unter: Empfehlungen
D.Legen Sie den Trigger von LA1 fest mit: Bei Erstellen oder Auslösen einer Azure Security Center-Warnung
Konfigurieren Sie das Auslösen von LA1 unter: Workflowautomatisierung
E.Legen Sie den Trigger von LA1 fest mit: Beim Auslösen einer Antwort auf eine Azure Security Center-Warnung
Konfigurieren Sie das Auslösen von LA1 unter: Empfehlungen
F.Legen Sie den Trigger von LA1 fest mit: Beim Auslösen einer Antwort auf eine Azure Security Center-Warnung
Konfigurieren Sie das Auslösen von LA1 unter: Workflowautomatisierung

Korrekte Antwort: B

Erläuterungen:

Die Automatisierung des Workflows wird im Security Center unter "Workflowautoamtisierung" gestartet:



Der Logik-App-Designer unterstützt diese Security Center-Trigger:

Bei Erstellen oder Auslösen einer Azure Security Center-Empfehlung: Wenn Ihre Logik-App auf einer Empfehlung basiert, die veraltet ist oder ersetzt wird, funktioniert die Automatisierung nicht mehr, und Sie müssen den Trigger aktualisieren.

Bei Erstellen oder Auslösen einer Azure Security Center-Warnung: Sie können den Trigger so anpassen, dass er sich nur auf Warnungen mit den für sie interessanten Schweregraden bezieht.

Wenn eine Bewertung der Einhaltung gesetzlicher Vorschriften durch das Security Center erstellt oder ausgelöst wird: Auslösen von Automatisierungen basierend auf Aktualisierungen von Bewertungen der Einhaltung gesetzlicher Vorschriften.

Der folgende Microsoft Docs-Artikel enthält weitere Informationen zum Thema:

utomatisieren der Reaktionen auf Security Center-Trigger