

Microsoft Discussions



**Exam AZ-900 All Questions**

View all questions & answers for the AZ-900 exam

Go to Exam

EXAM AZ-900 TOPIC 1 QUESTION 233 DISCUSSION

Actual exam question from Microsoft's AZ-900

Question #: 233

Topic #: 1

[\[All AZ-900 Questions\]](#)

You have an Azure Sentinel workspace.  
You need to automate responses to threats detected by Azure Sentinel.  
What should you use?

- A. adaptive network hardening in Azure Security Center
- B. Azure Service Health
- C. Azure Monitor workbooks
- D. adaptive application controls in Azure Security Center

Show Suggested Answer

by [Lincoln01](#) at Dec. 31, 2021, 5:21 a.m.

Comments

Type your comment...

Submit

[kwldgseeker](#) **Highly Voted** 2 years, 6 months ago

Either the answer is playbooks (which is not a provided choice) or the question itself is wrong. Workbooks does not provide for automation. It is a visualization / reporting tool. If you still doubt, look up "automate responses to threats detected by Azure Sentinel." in Google and you will find "Playbooks" in the results and nowhere will you find "Workbooks". I really love the spirit and intent of the site and have respect for the small team behind it. At the same time I have to question where these questions came from. There are far too many discrepancies, errors and omissions to justify the asking price (which I regrettably paid as I thought my membership was for all tests, not just the AZ-900!). Clean up the discrepancies, errors and omissions (and include more than just one test) and it will be worth the asking price.

   upvoted 40 times

  **NoursBear** 2 months, 4 weeks ago

I agree or it could be Logic Apps. Question is wrong

   upvoted 2 times

  **[Removed]** 1 year, 8 months ago

What you're saying is just wrong. The following link shows very clear that the given answer is the correct one:




<https://learn.microsoft.com/en-us/training/modules/protect-against-security-threats-azure/3-detect-respond-threats-sentinel?ns-enrollment-type=learningpath&ns-enrollment-id=learn.az-900-%20describe-general-security-network-security-features>

   upvoted 3 times

  **Ni\_yot** 1 year, 8 months ago

I this is value for money. Time and time again pple are passing the exam using this site. you cant have everything handed to you on a plate. There is the option to pay \$20 for 20 questions form MS if desired.

   upvoted 6 times

  **TamHas** Highly Voted  2 years, 9 months ago

This answer is correct, see statement from Microsoft site:

Once you have connected your data sources to Microsoft Sentinel, you can visualize and monitor the data using the Microsoft Sentinel adoption of Azure Monitor Workbooks, which provides versatility in creating custom dashboards. While the Workbooks are displayed differently in Microsoft Sentinel, it may be useful for you to see how to create interactive reports with Azure Monitor Workbooks. Microsoft Sentinel allows you to create custom workbooks across your data, and also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source. <https://docs.microsoft.com/en-us/azure/sentinel/monitor-your-data>

   upvoted 21 times

  **NoursBear** 1 week, 6 days ago

no Workbooks do not use automatic response to threats, Playbooks do

   upvoted 2 times

  **PN60** Most Recent  20 hours, 16 minutes ago

Is there a moderator that can provide evidence of the correct answer?

   upvoted 1 times

  **JUMP56** 4 months ago

<https://learn.microsoft.com/en-us/azure/sentinel/automate-incident-handling-with-automation-rules?tabs=onboarded>

   upvoted 1 times

  **Payu1994** 6 months, 3 weeks ago



To automate responses to threats detected by Azure Sentinel, you should use option D: adaptive application controls in Azure Security Center.

Azure Security Center provides adaptive application controls, which allow you to automatically respond to threats detected by Azure Sentinel. These controls enable you to define and enforce policies that govern the types of applications allowed to run on your virtual machines (VMs) and servers. By configuring adaptive application controls, you can automatically block or allow applications based on predefined rules and policies, helping to mitigate security risks and protect your environment from potential threats.

   upvoted 2 times

  **SAFM** 1 year ago

This topic is no longer present in the learning syllabus for AZ-900, anybody can confirm?

   upvoted 6 times

  **zellick** 1 year, 9 months ago

Selected Answer: C

C is the answer.

<https://learn.microsoft.com/en-us/azure/sentinel/monitor-your-data>

Once you have connected your data sources to Microsoft Sentinel, you can visualize and monitor the data using the Microsoft Sentinel adoption of Azure Monitor Workbooks, which provides versatility in creating custom dashboards. While the Workbooks are displayed differently in Microsoft Sentinel, it may be useful for you to see how to create interactive reports with Azure Monitor Workbooks. Microsoft Sentinel allows you to create custom workbooks across your data, and also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.

with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.

👍 ↩ 🚩 upvoted 2 times

🗨️ 👤 **AnitaArab** 1 year, 11 months ago

Yup, it says it right here - Azure Monitor Workbooks

"The company will also use Azure Monitor Workbooks to automate responses to threats."

<https://docs.microsoft.com/en-us/learn/modules/protect-against-security-threats-azure/3-detect-respond-threats-sentinel?ns-enrollment-type=learningpath&ns-enrollment-id=learn.az-900-describe-general-security-network-security-features>

👍 ↩ 🚩 upvoted 4 times

🗨️ 👤 **NoursBear** 1 week, 6 days ago

no your link is not taking you anywhere useful today, the documentation clearly explains the differences between the two

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **HHHo** 2 years, 6 months ago

Got this in exam on 2022.04.18

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **Tin\_Nguyen** 2 years, 6 months ago

C for me

"The company will also use Azure Monitor Workbooks to automate responses to threats."

<https://docs.microsoft.com/en-us/learn/modules/protect-against-security-threats-azure/3-detect-respond-threats-sentinel?ns-enrollment-type=learningpath&ns-enrollment-id=learn.az-900-describe-general-security-network-security-features>

👍 ↩ 🚩 upvoted 7 times

🗨️ 👤 **Contactforinitish** 2 years, 7 months ago

Odd one out but I would disagree with answer. Workbooks are just dashboard and takes no action themselves.

Sentinel uses playbook against known situations but playbook uses two things among others Adaptive network hardening (to reduce attack surface) and Adaptive Application Control (to have a known safe application list & block application on suspicious behavior). Since the Application control needs advance work, I would say surface reduction would be first choice in case of any attack. Hence A

👍 ↩ 🚩 upvoted 2 times

🗨️ 👤 **forestwood** 2 years, 8 months ago

Workbook does not provide automation. So i do not agree with the answer

👍 ↩ 🚩 upvoted 5 times

🗨️ 👤 **blobstorage** 2 years, 8 months ago

I think it should be Playbooks,

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

👍 ↩ 🚩 upvoted 6 times

🗨️ 👤 **nsp24** 2 years, 9 months ago

I think answer is correct

<https://docs.microsoft.com/en-us/azure/sentinel/monitor-your-data>

👍 ↩ 🚩 upvoted 2 times

🗨️ 👤 **TheKraemer** 2 years, 9 months ago

The explanation is missing here! I don't spend money for this!!

👍 ↩ 🚩 upvoted 13 times

🗨️ 👤 **johnny1001** 2 years, 7 months ago

oh yes you do

👍 ↩ 🚩 upvoted 18 times

🗨️ 👤 **Borbala** 2 years, 9 months ago

I agree - it should be Azure Logic Apps.

"Automate your common tasks and simplify security orchestration with playbooks that integrate with Azure services and your existing tools.

Built on the foundation of Azure Logic Apps..."

<https://docs.microsoft.com/en-us/azure/sentinel/overview>

👍 ↩ 🚩 upvoted 4 times

🗨️ 👤 **nimblealliance** 2 years, 6 months ago

Yes , I too think it should be Azure logic Apps :-

<https://www.xenonstack.com/blog/azure-sentinel-and-its-components#:~:text=Azure%20Sentinel%20is%20a%20SIEM,proactive%20hunting%2C%20and%20threat%20response.>

Playbooks: A Playbook is a collection of procedures to execute in response to an alert trigger by Azure Sentinel. They leverage Azure Logic Apps. So, the user can use flexibility, capability, customizability, and built-in templates of Logic Apps. To automate and orchestrate tasks/workflows that can be ready to configure to run manually or execute automatically when specific alerts are triggered.

But it isn't available in the options lol

   upvoted 1 times

  **Lincoln01** 2 years, 9 months ago

I think these should be playbook but not seen in the options

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

   upvoted 2 times

  **ajl22** 2 years, 9 months ago

Azure Monitor workbooks vs. Azure Sentinel playbooks is confusing, yes!

   upvoted 1 times

**Start Learning for free**



### Social Media

[Facebook](#) , [Twitter](#)

[YouTube](#) , [Reddit](#)

[Pinterest](#)



We are the biggest and most updated IT certification exam material website.

Using our own resources, we strive to strengthen the IT professionals community for free.



© 2024 ExamTopics

ExamTopics doesn't offer Real Microsoft Exam Questions. ExamTopics doesn't offer Real Amazon Exam Questions. ExamTopics Materials do not contain actual questions and answers from Cisco's Certification Exams.

CFA Institute does not endorse, promote or warrant the accuracy or quality of ExamTopics. CFA® and Chartered Financial Analyst® are registered trademarks owned by CFA Institute.