

Knowledge check

1 minute

Choose the best response for each of the questions below. Then select **Check your answers**.

Check your knowledge

1. As the lead admin, it's important to convince your team to start using Microsoft Sentinel. You've put together a presentation. What are the four security operation areas of Microsoft Sentinel that cover this area?

☐ Collect, Detect, Investigate, and Redirect.

☒ Collect, Detect, Investigate, and Respond.

✓ That's correct. A SIEM/SOAR solution uses collect, detect, investigate, and respond to identify and protect your organization's network perimeter. .

☐ Collect, Detect, Investigate, and Repair.

2. Your estate has many different data sources where data is stored. Which tool should be used with Microsoft Sentinel to quickly gain insights across your data as soon as a data source is connected?

☒ Azure Monitor Workbooks.

✓ That's correct. Using the Microsoft Sentinel integration with Azure Monitor Workbooks allows you to monitor

data and provides versatility in creating custom workbooks.

- ☐ Playbooks.
- ☐ Microsoft 365 Defender.

Next unit: Summary and resources

[Continue >](#)
