You are reviewing the IP address associated to an alert generated by Microsoft Defender for Endpoint.
You need to identify the number of managed devices that successfully connected to the IP address during the previous 30 days.
Which section can you use to identify the device?
Select only one answer.
IP details Alerts Observed in organization Prevalence

You plan to submit several files for deep file analysis in Microsoft Defender for Endpoint.
Which two file types can you submit? Each correct answer is a complete solution.
Select all answers that apply.
.ps1 .com .exe .dll .cmd

You are reviewing the profile page for a user named User1 in the Microsoft 365 Defender portal.
You need to identify the device that the user signed in from the most often.
What should you use to identify the device?
Select only one answer.
On the User summary pane On the Overview tab On the Alerts tab On the Observed in organization tab

You manage Microsoft 365 Defender incidents.
You need to configure determination for an incident from the Microsoft 365 Defender portal.
What should you configure first?
Select only one answer.
Classification Status Assign to Incident name

You need to assign a built-in Azure Active Directory role to a user named Admin1.
Admin1 must be able to configure incident email notifications in Microsoft 365 Defender. The solution must satisfy the principle of least privilege.
Which role should you use?
Select only one answer.
Global Administrator Security Operator Security Administrator Security Reader

You manage Microsoft 365 Defender incidents.
You need to reduce the number of false positive incidents.
What should you do?
Select only one answer.

Set the classification for false positive incidents to **false**. Set the classification for false positive incidents to **true**. Configure the determination for false positive incidents. Create a custom indicator allow list.

You plan to create custom detection rule for your advanced hunting queries against Microsoft 365 Defender data.
What is the maximum number of alerts that will be generated by the rule?
Select only one answer.
10 100 1000 Unlimited

You manage Microsoft 365 Defender in an Active Directory Domain Services (AD DS) environment.
You plan to run advanced hunting queries against Microsoft 365 Defender data.
You need to identify the schema table that contains the system events from the Active Directory Domain Services (AD DS) domain controllers.
Which schema table should you identify?
Select only one answer.
IdentityDirectoryEvents IdentityInfo IdentityLogonEvents IdentityQueryEvents

You received a Microsoft Defender for Cloud for Resource Manager alert that details the provisioning of an Azure resource by a suspicious Azure Active Directory (Azure AD) user.
You need to review the list of all resource changes by a specific Azure AD user.
What should you use?
Select only one answer.
Azure AD sign-in logs Azure AD audit logs Azure Security Center alerts Azure Activity logs

You review a Microsoft Defender for Cloud alert that details an attempt to retrieve a secret from an Azure key vault by a suspicious user. You notice the following details:
- Azure key vault firewall is enabled
- Attempt originated from a resource in your Azure subscription.
You need to mitigate the issue.
What should you do?
Select only one answer.
Modify the vault's access policy Modify the vault's firewall settings Delete the secret from the key vault Delete the key vault

You need to automate the response to a Microsoft Defender for Cloud security alert.
Which Azure resource should you use?
Select only one answer.
◉ Logic app ○ Automation runbook ○ Function app ○ Security Center workbook

Your company has an Azure subscription that hosts resources in multiple Azure regions in different countries.
What are two primary drawbacks of implementing single-tenant with regional workspaces Microsoft Sentinel in your environment as compared to the single-tenant single workspace option? Each correct answer presents part of the solution.
Select all answers that apply.
☐ Limited support for querying data across workspaces ☑ Increased cost of network bandwidth ☐ Lack of a single pane of glass ☑ Increased cost of compute services ☐ Increased deployment complexity

You need to ensure that a user has the required RBAC role to create and run Microsoft Sentinel playbooks. The solution must use the principle of least privilege.
Which two roles should you use? Each correct answer presents part of the solution.
Select all answers that apply.
☑ Microsoft Sentinel Responder ☐ Contributor ☐ Azure Log Analytics Contributor
☑ Microsoft Sentinel Contributor ☐ Azure Logic App Contributor

Your company's security policy has several data retention requirements.
You need to identify whether Microsoft Sentinel satisfies the data retention requirements.
What is the maximum data retention period of an Microsoft Sentinel workspace?
Select only one answer.
◉ 90 days ○ 365 days ○ 730 days ○ 5 years

You need to collect logs in Common Event Format (CEF) from a
Linux server by using Microsoft Sentinel.
What should you do on the Linux server?
Select only one answer.
○ Install the Connected Machine agent. ◉ Install the Log Analytics Agent. ○ Allow inbound TCP port 514. ○ Allow inbound UDP port 514.

You plan to implement Microsoft Sentinel.
You need to identify the Azure service required to implement Microsoft Sentinel.
Which Azure service should you identify?
Select only one answer.
○ Microsoft Defender for Cloud ○ Azure Storage ◉ Azure Log Analytics ○ Azure SQL database

You plan to implement Microsoft Sentinel.
You need to identify a Microsoft Sentinel connector to an external solution through API.
What connector should you identify?
Select only one answer.
○ Microsoft Defender for Cloud Apps ○ Amazon Web Services CloudTrail ○ Azure Web Application Firewall ◉ Barracuda Web Application Firewall

You need to create custom expressions in Microsoft Sentinel scheduled alert rules.
Which language should you use?
Select only one answer.
○ T-SQL ◉ KQL ○ C# ○ JavaScript

You plan to perform an activity that will trigger an alert for an existing active Microsoft Sentinel analytics rule.
You need to prevent the alert. The solution must minimize administrative effort.
What action should you perform on the rule?
Select only one answer.
○ Duplicate ○ Delete ○ Edit ◉ Disable

You are creating a Microsoft Sentinel rule that is based on a Microsoft security template.
What rule setting is read-only?
Select only one answer.
○ Status ◉ Microsoft Security Service ○ Trigger of the automated response ○ Conditions of the automated response

You plan to close a Microsoft Sentinel incident.
You need to specify that the incident was suspicious, but the incident was expected.
What value should you specify for the incident?
Select only one answer.
○ Undetermined ◉ Benign Positive ○ False Positive ○ True Positive

You need to identify the Microsoft Sentinel alerts associated to a specific user in your organization and the computer used by that user.
The solution must minimize administrative effort.
What should you use?
Select only one answer.
◉ an entity ○ a workbook ○ a notebook ○ a playbook

What is the refresh frequency of Microsoft Sentinel Livestream queries?
Select only one answer.
1 second 30 seconds 5 minutes 10 minutes

You perform threat hunting in Microsoft Sentinel.
You need to retain a query that was run, as well as the query results. The solution must minimize administrative effort.
What should you create?
Select only one answer.
Configure a favorite. Create a bookmark. Modify a workbook. Create a notebook.

75%