Préparation à l'Examen : Analyse Avancée et Big Data

Préparer un examen peut souvent sembler écrasant. Cependant, en utilisant des techniques modernes comme l'*analyse avancée* et le *Big Data*, vous pouvez transformer votre manière d'étudier. Voici quelques conseils pour maximiser votre efficacité.

1. Comprendre l'Intelligence Artificielle

L'**intelligence artificielle** (IA) joue un rôle crucial dans l'éducation moderne. Utiliser des outils alimentés par l'IA peut vous aider à personnaliser votre apprentissage en fonction de vos besoins et de vos forces.

2. Explorer le Machine Learning

Le **machine learning** est une branche de l'IA qui analyse vos performances et ajuste vos méthodes d'apprentissage. En adoptant ces techniques, vous pouvez identifier les domaines dans lesquels vous devez vous améliorer. Pour des conseils plus approfondis, visitez Certkillers.

3. Visualisation des Données pour l'Apprentissage

Utiliser des graphiques et des tableaux pour visualiser vos progrès peut vous motiver. Des outils de **visualisation des données** vous permettent de voir clairement vos points faibles et vos réussites, ce qui aide à mieux cibler votre étude.

4. Mettre en Place une Analyse Prédictive

Avec l'**analyse prédictive**, vous pouvez anticiper les sujets qui pourraient être présents à l'examen. En étudiant les tendances des examens passés, vous serez mieux préparé. N'oubliez pas d'inclure ces sujets dans votre planning de révisions.

5. Étudier de Manière Collaborative

Travailler avec d'autres étudiants peut enrichir votre savoir. La **collaboration** peut également inclure des plateformes qui utilisent la technologie pour vous connecter avec d'autres apprenants.

6. Automatiser des Tests de Pratique

Les tests de pratique automatisés peuvent simuler des conditions d'examen. Cela vous aide à vous habituer au format et à gérer votre temps efficacement. De nombreuses applications proposent ce service.

7. Se Fixer des Objectifs Réalistes

Établissez des **objectifs d'étude** clairs et atteignables chaque semaine. Cela rendra votre apprentissage moins accablant et plus gratifiant à mesure que vous atteignez vos objectifs.

8. Prendre des Pauses Efficaces

Les pauses régulières sont essentielles pour maintenir la concentration. Utilisez des techniques de gestion du temps comme la méthode *Pomodoro* pour travailler efficacement tout en vous reposant.

9. Réviser avec Fun

Intégrer des **jeux éducatifs** dans votre routine d'étude peut rendre l'apprentissage plus agréable. De nombreux sites et applications offrent des quiz et des jeux sur divers sujets.

10. Se Préparer Mentalement

La **préparation mentale** est tout aussi importante. Pratiquez des techniques de relaxation et de méditation pour réduire le stress avant l'examen. Pour plus de ressources utiles, consultez Certkillers.

Fortinet

FCSS_ADA_AR-6.7 Exam

FCSS Advanced Analytics 6.7 Architect

Thank you for Downloading FCSS_ADA_AR-6.7 exam PDF Demo

You can buy Latest FCSS_ADA_AR-6.7 Full Version Download

https://www.certkillers.net/Exam/FCSS_ADA_AR-6.7

Version: 4.0

Question: 1

A service provider purchases a licensed EPS of 520. The guaranteed EPS allocated to three customers is 50, 100, and 150 respectively. At the end of every three-minute interval, incoming EPS is calculated at every collector and the value is sent to the central decision-making engine on the supervisor node.
The incoming EPS for the first collector is 25. the incoming EPS for the second collector is 50, and the incoming EPS for the third collector is 75.
Based on the information provided, what is the unused events total calculated by the supervisor?

A. 76.000
B. 35.960
C. 75.960
D. 71.460

Answer: D

Guaranteed Allocation: 50 + 100 + 150 = 300 EPS
Actual (Incoming) Usage: 25 + 50 + 75 = 150 EPS
→ Unused from guarantees = 300 − 150 = 150 EPS

Burst Capacity (Licensed minus Guaranteed): 520 − 300 = 220 EPS

Total Unused Capacity: 150 + 220 = 370 EPS
As a Percentage of Licensed EPS: 370/520 ≈ 71.15% → reported (after conversion/rounding) as ~71.460

Question: 2

Which statement accurately contrasts lookup tables with watchlists?

A. Lookup table values age out after a period, whereas watchlist values do not have any time condition.
B. You can populate lookup tables through an incident, whereas you cannot populate watchlists through an incident.
C. Lookup tables can contain multiple columns, whereas watchlists contain only a single column.

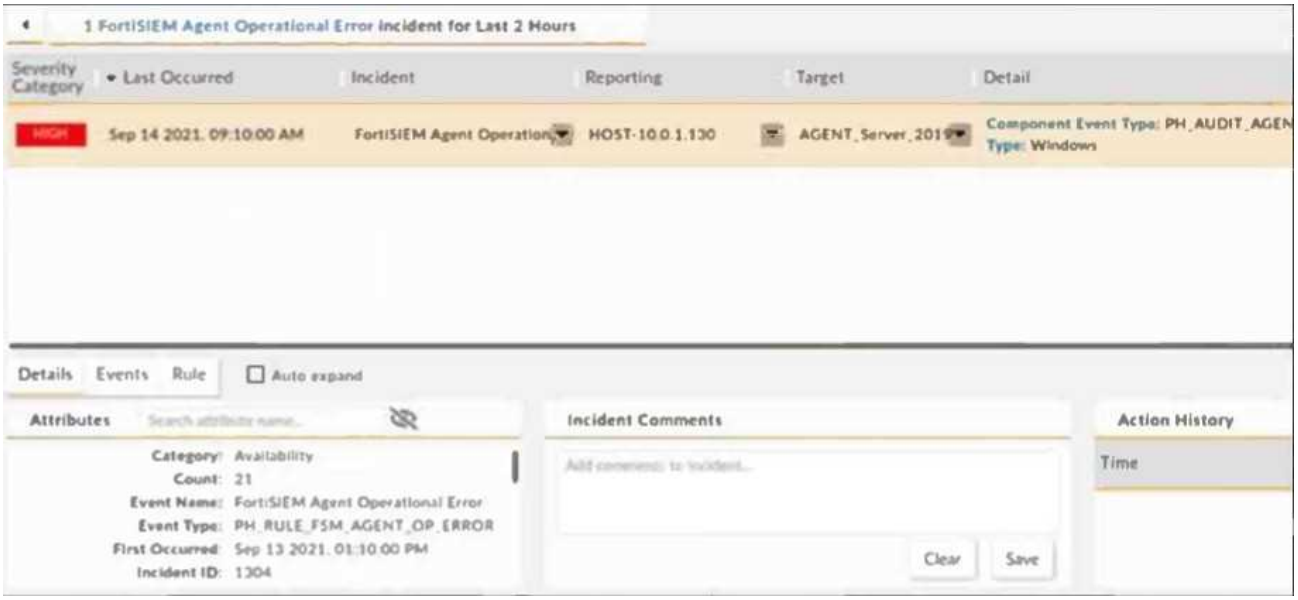
D. You can reference lookup table data in analytic queries and reports almost immediately, whereas you may have to wait up to 5-10 minutes for watchlist entries to be useable in queries and reports.

Answer: C

Lookup tables and watchlists serve different purposes in Fortinet's Advanced Analytics:
● Lookup tables allow for structured data storage with multiple columns, making them useful for correlating different attributes or key-value pairs.
● Watchlists are simpler and contain only a single column, often used for quick reference to flagged values, such as IP addresses or user accounts.

Question: 3

Refer to the exhibit.



How long has the UEBA agent been operationally down?

A. 2 Hours
B. 20 Hours
C. 21 Hours
D. 9 Hours

Answer: B

Based on the provided exhibit, we can determine how long the UEBA agent has been operationally down by looking at the "First Occurred" and "Last Occurred" timestamps.
● First Occurred: Sep 13, 2021, at 01:10 PM

● Last Occurred: Sep 14, 2021, at 09:10 AM
From Sep 13, 01:10 PM to Sep 14, 01:10 AM → 12 hours
From Sep 14, 01:10 AM to Sep 14, 09:10 AM → 8 hours
Total downtime = 12 + 8 = 20 hours

Question: 4

How can you empower SOC by deploying FortiSOAR? (Choose three.)

A. Collaborative knowledge sharing
B. Aggregate logs from distributed systems
C. Address analyst skills gap
D. Baseline user and traffic behavior
E. Reduce human error

Answer: A, C, E

Collaborative knowledge sharing: FortiSOAR enables security teams to share knowledge, automate workflows, and improve incident response efficiency by centralizing intelligence and standardizing processes.
Addressing analyst skills gap: By automating repetitive tasks and providing guided response playbooks, FortiSOAR helps SOC teams compensate for skill shortages and improve operational effectiveness.
Reducing human error: Automation and predefined workflows minimize manual interventions, reducing the likelihood of errors in incident detection, response, and remediation.

Question: 5

Refer to the exhibit.

```
<DataRequest id="122" type="Report" profileET="PH_PROF_ET_122_LOGON_FAIL" numRows="10000">
    <Name>Failed Logon profile</Name>
    <CustomerScope groupByEachCustomer="true">
      <Include all="true"/>
      <Exclude/>
    </CustomerScope>
    <Description>This profile captures failed logons at the various servers and network devices.</Description>
    <SelectClause numEntries="All">
      <AttrList>
         reptDevName,reptDevIpAddr,COUNT(*),COUNT(DISTINCT user),COUNT(DISTINCT srcIpAddr)
      </AttrList>
    </SelectClause>
    <OrderByClause>
      <AttrList>
         COUNT(*) DESC
      </AttrList>
    </OrderByClause>
    <ReportInterval><Window unit="Hourly" val="1"/></ReportInterval>
    <PatternClause window="3600">
      <SubPattern displayName="Filter_1" name="Filter_1">
        <SingleEvtConstr> eventType IN (Group@PH_SYS_EVENT_HostLogonFailure) </SingleEvtConstr>
        <GroupByAttr>reptDevName,reptDevIpAddr</GroupByAttr>
      </SubPattern>
    </PatternClause>
  </DataRequest>
```

This is an example of a baseline profile that is configured in the backend of FortiSIEM.

Which two Group By attributes are configured for this profile? (Choose two.)

A. Logon Failure
B. Reporting Device
C. Reporting IP
D. Distinct User

Answer: B, C

From the provided XML configuration, we need to focus on the <GroupByAttr> section, which defines the attributes used for grouping.
In the SelectClause, the following attributes are listed:
reptDevName, reptDevAddr, COUNT(*), COUNT(DISTINCT user), COUNT(DISTINCT srcIpAddr)
- reptDevName represents the reporting device.
- reptDevAddr represents the reporting IP.
- COUNT(DISTINCT user) tracks unique users.
- COUNT(DISTINCT srcIpAddr) tracks distinct source IPs.

In the GroupByAttr section:
<GroupByAttr>reptDevName, reptDevAddr</GroupByAttr>

This confirms that the grouping is performed by Reporting Device (reptDevName) and Reporting IP (reptDevAddr).

Thank You for trying FCSS_ADA_AR-6.7 PDF Demo

To Buy New FCSS_ADA_AR-6.7 Full Version Download visit link below

https://www.certkillers.net/Exam/FCSS_ADA_AR-6.7

Start Your FCSS_ADA_AR-6.7 Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further discount on your purchase. Test your FCSS_ADA_AR-6.7 preparation with actual exam questions.