FCP_FSM_AN-7.2 Probesfragen, FCP_FSM_AN-7.2 Fragen&Antworten

Machen Sie Sorge um die FCP_FSM_AN-7.2 von Fortinet Prüfung, weil Sie nur noch ein Anfänger sind? Von jetzt an wird It-Pruefung alle Probleme für Sie lösen. Die Lernhilfe von Fortinet FCP_FSM_AN-7.2 Zertifizierung sind umfassend und enthalten unterschiedliche Ziele, daher können sogar die Anfänger sie leicht erfassen. Sie würden den Schlüssel für den Durchlauf der FCP_FSM_AN-7.2 Prüfung haben und Selbstsicherheit gewinnen, wenn Sie solche Lernhilfe haben. Dann warum warten Sie noch?

Fortinet FCP_FSM_AN-7.2 Prüfungsplan:

Thema	Einzelheiten
Thema 1	• Machine learning, UEBA, and ZTNA: This section of the exam measures the skills of Advanced Security Architects and covers the integration of modern security technologies. It involves performing configuration tasks for machine learning models, incorporating UEBA (User and Entity Behavior Analytics) data into rules and dashboards for enhanced threat detection, and understanding how to integrate ZTNA (Zero Trust Network Access) principles into security operations.
Thema 2	• Incidents, notifications, and remediation: This section of the exam measures the skills of Incident Responders and encompasses the entire incident management lifecycle. This includes the skills required to manage and prioritize security incidents, configure policies for alert notifications, and set up automated remediation actions to contain and resolve threats.
Thema 3	• Rules and subpatterns: This section of the exam measures the skills of SOC Engineers and focuses on the construction and implementation of analytics rules. It involves identifying the different components that make up a rule, utilizing advanced features like subpatterns and aggregation, and practically configuring these rules within the FortiSIEM platform to detect security events.
Thema 4	• Analytics: This section of the exam measures the skills of Security Analysts and covers the foundational techniques for building and refining queries. It focuses on creating searches from events, applying grouping and aggregation methods, and performing various lookup operations, including CMDB and nested queries to effectively analyze and correlate data.

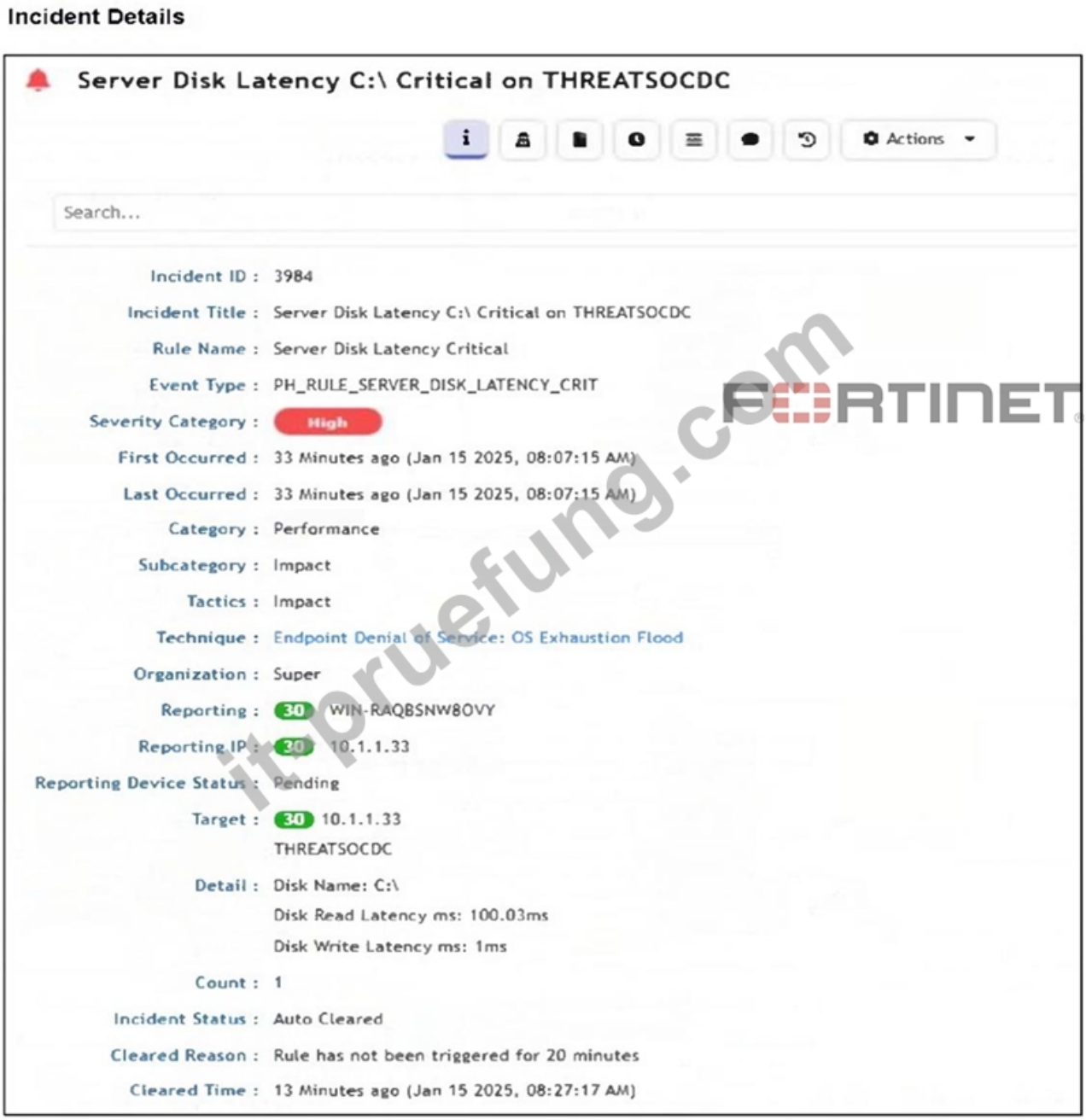
>> FCP_FSM_AN-7.2 Probesfragen <<

FCP_FSM_AN-7.2 Fragen&Antworten, FCP_FSM_AN-7.2 Exam

Wir It-Pruefung bieten Ihnen verschiede Unterlagensversionen, die Ihre Nutzung erleichtern können. Die PDF-Versionen können das Lesen erleichtern und Ihnen die aktuellen Fortinet FCP_FSM_AN-7.2 Prüfungsfragen zeigen, Die Software-Versionen sind die Simulationssoftwaren, die Ihre Vorbereitungssituation auf jeden Fall testen. Wenn Sie wissen wollen, ob Sie sich für Fortinet FCP_FSM_AN-7.2 Prüfung gut bereit sind, können Sie helfen, Ihre Stärke und Schwäche ganz schnell finden, um Ihren nächsten Lernplan zu erstellen.

Fortinet FCP - FortiSIEM 7.2 Analyst FCP_FSM_AN-7.2 Prüfungsfragen mit Lösungen (Q20-Q25):

20. Frage
Refer to the exhibit.



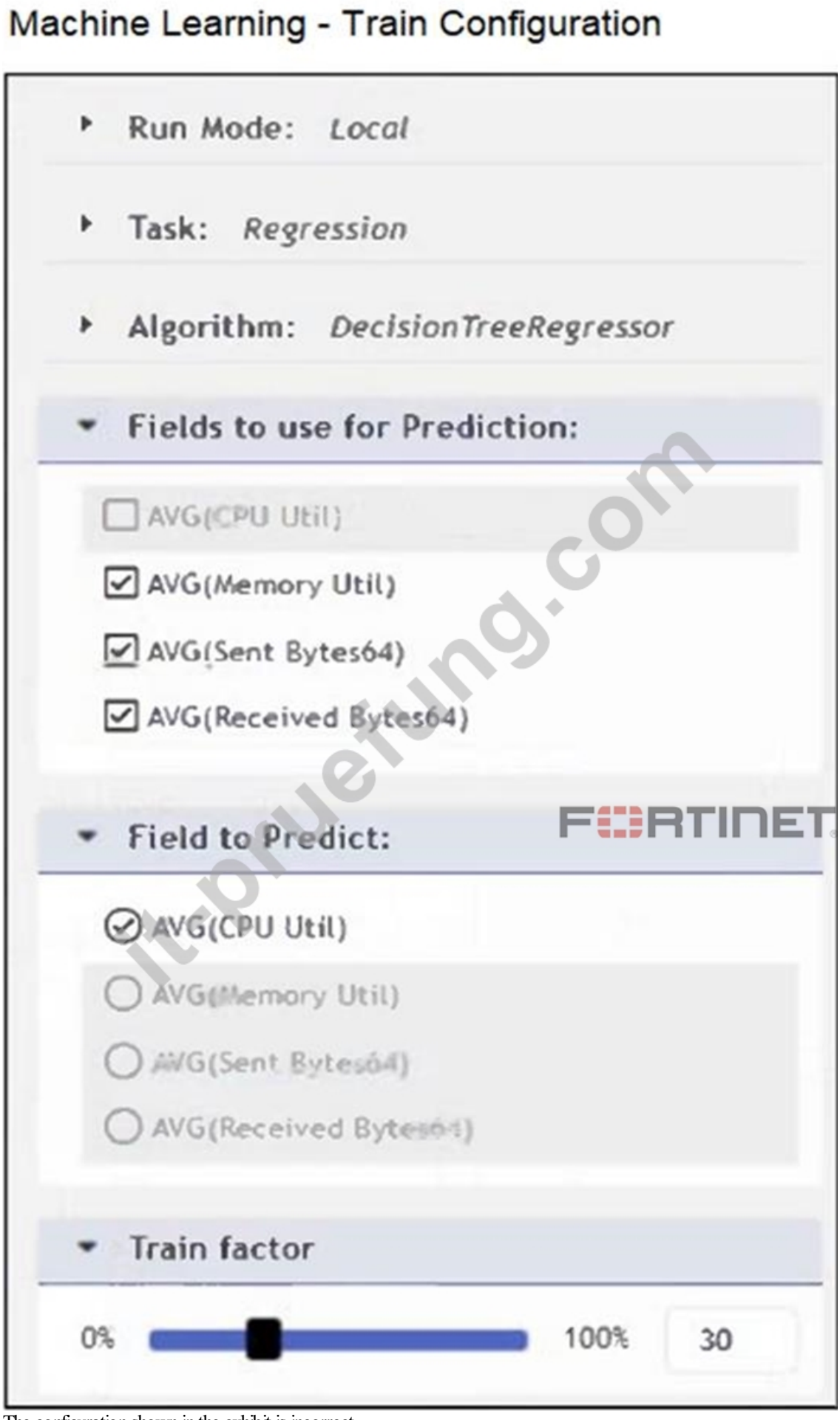
How was this incident cleared?

- A. The incident was cleared automatically by the rule.
- B. The endpoint was rebooted and sent an all-clear signal to FortiSIEM.
- C. FortiSIEM cleared the incident automatically after 24 hours.
- D. The analyst manually cleared the incident from the incident table.

Antwort: A

Begründung:
The Incident Status shows "Auto Cleared", and the Cleared Reason states: "Rule has not been triggered for 20 minutes." This indicates that the incident was automatically cleared by the rule logic after a defined period of inactivity.

21. Frage
Refer to the exhibit.



The configuration shown in the exhibit is incorrect.

What must you change to allow this configuration to be successfully applied to FortiSIEM?

- A. Only one AVG type field must be selected under Fields to use for Prediction.
- B. The selection in Fields to use for Prediction and Field to Predict must match.
- C. The Train factor must be 70% or greater.
- D. Run Mode must be set to ML.

Antwort: D

Begründung:
The Run Mode is set to Local, which is not valid for training machine learning models in FortiSIEM. To apply this configuration correctly, the Run Mode must be set to ML, which enables proper model training and prediction using selected fields.

22. Frage
Which statement about thresholds is true?

- A. FortiSIEM uses global and per device thresholds for performance metrics.
- B. FortiSIEM uses fixed, hardcoded global and device thresholds for all performance metrics.
- C. FortiSIEM uses only global thresholds for performance metrics.
- D. FortiSIEM uses only device thresholds for security metrics.

Antwort: A

Begründung:
FortiSIEM evaluates performance metrics against both global thresholds, which apply system-wide, and per-device thresholds, which can be customized for individual devices. This dual approach allows flexibility in monitoring while ensuring consistent baseline alerting.

23. Frage
How does FortiSIEM update the incident table if a performance rule triggers repeatedly?

- A. FortiSIEM changes the incident status to Repeated, and updates the Last Seen timestamp.
- B. FortiSIEM generates a new incident each time the rule triggers, and updates the First Seen and Last Seen timestamps.
- C. FortiSIEM updates the Incident Count value and Last Seen timestamp.
- D. FortiSIEM generates a new incident based on the Rule Frequency value, and updates the First Seen and Last Seen timestamps.

Antwort: C

Begründung:
When a performance rule triggers repeatedly, FortiSIEM updates the existing incident by incrementing the Incident Count and refreshing the Last Seen timestamp. This avoids flooding the incident table with duplicates while still tracking repeated occurrences.

24. Frage
Refer to the exhibit.

An analyst is trying to identify an issue using an expression based on the Expression Builder settings shown in the exhibit; however, the error message shown in the exhibit indicates that the expression is invalid.
What is the correct syntax to create an expression that generates a total count of matched events?

- A. Matched Events (COUNT)
- B. COUNT(Matched Events)
- C. (COUNT) Matched Events
- D. Matched Events COUNT()

Antwort: B

Begründung:
The correct syntax is COUNT(Matched Events) - with proper capitalization and spacing - to generate a total count of matched events. The error in the exhibit likely stems from a formatting issue (e.g., lowercase count() or incorrect spacing), not the logical structure of the expression.

25. Frage
.....

Probieren Sie vor dem Kauf! Wir It-Pruefung sind verantwortlich für jeder Kunde. Wir bieten Ihnen kostenfreie Demos der Fortinet FCP_FSM_AN-7.2, somit können Sie nach der Probe unbesorgt kaufen. Außerdem können wir Ihnen garantieren, dass Sie keine Reue empfinden werden, nachdem Sie unsere Fortinet FCP_FSM_AN-7.2 Prüfungssoftware gekauft haben. Denn Sie können durch die Benutzung ihre Zuverlässigkeit empfinden. Dadurch bekommen Sie mehr Konfidenz angesichts der Fortinet FCP_FSM_AN-7.2 Prüfung.

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, gratianne2045.blogspot.com, Disposable vapes