Fortinet

NSE5_FAS_AD-26

Fortinet NSE 5 - FortiAppSec Cloud 26 Administrator

Latest Version: 6.0

Question: 1

Beyond matching request content against its signature database, the FortiAppSec Cloud WAF parses SQL statements and compiles HTML and JavaScript taken from the request.
What does this syntax-based analysis achieve?

A. It rewrites the request so that the dangerous syntax is neutralized before the origin receives it
B. It replaces the signature database for the SQL Injection and Cross Site Scripting categories entirely
C. It cuts false positives by judging whether the content is genuinely executable syntax
D. It builds a behavioral model of each parameter's values

Answer: C

Question: 2

An analyst reviewing an incident needs the individual request-level records that the incident was built from, rather than the correlated summary.
Where are those records found?

A. In the Gateways section
B. In the attack logs
C. In the Insights section
D. In the Threat Analytics dashboard

Answer: B

Question: 3

How does FortiAppSec Cloud Client-Side Protection obtain visibility into what happens in a visitor's browser?

A. It replays each response through a headless browser inside the platform and records the result
B. It requires the development team to embed a software development kit in the application's front-end code
C. It injects a lightweight JavaScript collector into eligible HTTP responses
D. It installs a browser extension that visitors are prompted to accept on their first visit

Answer: C

Question: 4

An administrator sets a security rule's action to Deny with no log to keep the attack logs clean. A month later the security team cannot reconstruct what that rule stopped, and no incident was ever raised for it. What should the action have been, and why?

A. Alert, because the requests would then be recorded and the team would retain full visibility of the activity
B. Alert and Deny, because analytics can only correlate events that were logged in the first place
C. Deny with no log is correct, and the logging should be enabled separately in the Threat Analytics settings
D. Period Block, because blocking a source for a duration produces an incident

Answer: B

Question: 5

What does the Threat Analytics service do with the attack events observed across an organization's applications?

A. It uses machine learning to identify attack patterns across the whole application estate, aggregates them into security incidents and assigns a severity
B. It scores each event from 0 to 100 and blocks the source once a configured score is exceeded
C. It forwards each observed event to the configured external log collector and retains its own copy of each one for the period the contract provides
D. It matches each event against the signature database, raising an alert where a signature is recognized

Answer: A

Question: 6

A regulated organization must retain application attack evidence well beyond the platform's own storage, and correlate it with logs from its firewalls and endpoints.
Which two destinations does FortiAppSec Cloud support for collecting attack logs?
(Choose two.)

A. FortiFlex
B. FortiDAST
C. FortiADC
D. FortiAnalyzer
E. FortiSIEM

Answer: D,E

Question: 7

Two GSLB virtual server pools are configured with the Weight method. Pool A carries a weight of 3 and pool B a weight of 1. How is traffic divided?

A. Pool A receives three requests and then pool B receives every request until the counts even out
B. Pool A receives 30 percent of requests and pool B receives 10 percent, with the rest spread by proximity
C. Pool A receives three times as many requests as pool B
D. Pool A receives all requests until it reaches three times pool B's connection limit, then B takes over

Answer: C

Question: 8

Client-Side Protection has been enabled on a retail site for three weeks. It is reporting several high-risk third-party domains, but the security team notices that the scripts from those domains are still executing in visitors' browsers.
What is the most likely explanation?

A. High-risk findings need Threat Analytics confirmation first
B. The collector cannot block scripts served over HTTPS, so those domains are outside its enforcement reach
C. The scripts are allowlisted by the application's own Content Security Policy header, which overrides the module
D. The module is running in observation mode, which collects telemetry without blocking anything

Answer: D

Question: 9

An analyst is asked to determine whether a series of probes against three applications over four days is one coordinated campaign or unrelated noise.
Which Threat Analytics concept is the right unit of investigation, and why?

A. The incident, because it is where related events across assets and over time are already correlated into one object with a severity
B. The application, because a campaign is defined by the asset it targets
C. The individual attack log entry, because only the raw record preserves the detail needed to compare the probes

D. The gateway, because grouping by the inspecting gateway shows which probes shared an inspection path

Answer: A

Question: 10

In the FortiAppSec Cloud Client-Side Protection architecture, where is the risk of a script or domain actually assessed?

A. In the WAF gateway, which scores third-party scripts as they pass through the response path
B. In the injected collector itself, which scores each script before allowing it to execute
C. In the visitor's browser using the site's Content Security Policy report endpoint
D. In the platform's backend components, which analyze script and domain risk using AI

Answer: D

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer