Fortinet

NSE6_CNP_AN-26

Fortinet NSE 6 - FortiCNAPP 26 Analyst

For More Information – Visit link below:

https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 6.0

Question: 1

A shift-left program must cover three distinct concerns: flaws in first-party source, known-vulnerable third-party libraries, and credentials committed into the repository.
Which three capabilities map to those three concerns respectively?
(Choose three.)

A. SCA for known-vulnerable third-party dependencies.
B. DAST for all three, since it exercises the whole application.
C. SAST for insecure patterns in first-party source code.
D. Hard-coded secrets detection for committed credentials.
E. Network segmentation for all three, enforced at the firewall.

Answer: A,C,D

Question: 2

A benign internal administration tool is newly deployed and repeatedly triggers anomaly alerts because its binary is unfamiliar to the baseline. Analysts are spending time dismissing these as false positives.
Which action reduces the false positives while preserving detection of genuine threats?

A. Tune the detection policy to account for the known-good behavior.
B. Remove the threat engine's correlation so only single events are reported.
C. Raise every alert to critical severity so none is overlooked.
D. Disable behavioral analytics so the anomaly alerts stop firing.

Answer: A

Question: 3

FortiCNAPP's real-time behavioral analytics establishes a baseline of normal activity for users, machines, and workloads.
How does this BEST differ from static signature-based detection?

A. It depends on a continuously updated signature feed to recognize any anomaly.
B. It matches activity only against a fixed list of previously known malicious indicators.
C. It learns normal behavior and flags deviations, catching threats with no signature.
D. It compares configuration files against published compliance benchmarks.

Answer: C

Question: 4

Two misconfiguration findings share the same nominal severity, yet FortiCNAPP ranks one much higher for remediation.
Which contextual factors would justify prioritizing one finding over the other despite equal severity? (Choose two.)

A. One finding lies on an attack path to a sensitive asset through an over-privileged identity
B. One finding's severity label is displayed in a different color in the console
C. One resource is reachable from the internet while the other is isolated on an internal network
D. One finding belongs to a compliance framework with more total controls
E. One finding was reported more recently than the other

Answer: A,C

Question: 5

An analyst wants FortiCNAPP to continuously flag cloud resources that drift from configuration best practice, such as a storage bucket exposed to the public internet.
Which capability continuously assesses cloud configuration and surfaces these misconfiguration findings?

A. CSPM
B. CIEM
C. CWPP
D. SAST

Answer: A

Question: 6

FortiCNAPP assigns an identity risk score to cloud identities as part of its CIEM analysis.
Why does a CNAPP treat identity as a first-class risk dimension alongside posture and workload risk?

A. Because behavioral analytics cannot run unless every identity has a risk score
B. Because identities are the only assets that compliance frameworks require monitoring
C. Because identity scoring replaces the need to assess cloud configuration
D. Because excess, unused entitlements are a primary attacker route

Answer: D

Question: 7

A workload suddenly spawns an unfamiliar process and opens an unusual outbound connection while it is running.
Which capability is designed to detect this?

A. Compliance reporting, which maps resources to framework controls.
B. CIEM entitlement analysis, which evaluates identity permissions.
C. CWPP real-time behavioral analytics, which flags deviations from baselined behavior.
D. CSPM configuration assessment, which checks resource settings against best practice.

Answer: C

Question: 8

An organization wants broad coverage of cloud configuration, posture, and identity data across many accounts, with no software installed on hosts.
Which deployment model fits this requirement?

A. Agentless, but limited to runtime process anomaly detection.
B. Agentless, connecting via cloud APIs to assess configuration and posture.
C. Agent-based, because only an agent can read cloud identity and permission data.
D. Agent-based, deploying a runtime agent to every host and container.

Answer: B

Question: 9

One governance team wants to measure the environment against a widely recognized industry baseline, while another team wants to enforce a rule unique to their own organization.
How do a compliance framework and a custom policy differ in FortiCNAPP?

A. A framework is a standardized baseline, while a custom policy is an organization-specific rule.
B. They are identical; a compliance framework is just another name for a custom policy.
C. Both apply only to runtime workloads and never to configuration posture.
D. A compliance framework enforces organization-specific rules; a custom policy is a fixed industry baseline.

Answer: A

Question: 10

A colleague mentions that FortiCNAPP shares its detection heritage with a platform Fortinet acquired, which is why the docs still use an older product name.
Which platform is FortiCNAPP based on?

A. The FortiSOAR orchestration and automation platform.
B. The FortiGate next-generation firewall platform.
C. The former Lacework platform, now rebranded.
D. The FortiSIEM security analytics platform.

Answer: C

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/