Passcert

Higher Quality, better service!

Q&A

Http://www.passcert.com

We offer free update service for one year.

Exam : **NSE6_CNP_AN-26**

Title : Fortinet NSE 6 - FortiCNAPP 26 Analyst

Version : DEMO

1.Which deployment model in FortiCNAPP requires installing software directly on the workload to provide real-time behavioral analytics and intercept malicious processes?
A. Agentless deployment via Cloud APIs
B. Kubernetes Security Posture Management (KSPM)
C. Agent-based deployment
D. Cloud Infrastructure Entitlement Management (CIEM)
Answer: C
Explanation:
The agent-based deployment model involves installing a lightweight agent directly on the host or container. This is necessary to monitor system calls and provide real-time threat detection and behavioral analytics. Agentless models rely on API integrations and point-in-time snapshots, which cannot provide real-time process blocking.

2.A development team wants to ensure that container images and source code are scanned for vulnerabilities before they are deployed into the production environment.
Which FortiCNAPP concept best describes this practice?
A. Real-time behavioral analytics
B. Cloud Security Posture Management (CSPM)
C. Dynamic Application Security Testing (DAST)
D. Shift-left security
Answer: D
Explanation:
Shift-left security involves integrating security checks (such as image scanning, SAST, and SCA) early in the software development lifecycle (e.g., in the IDE or CI/CD pipeline) rather than waiting until the application is deployed in production.

3.A security administrator is configuring FortiCNAPP to automatically isolate a compromised AWS EC2 instance when a critical threat is detected.
Which Fortinet Security Fabric product should FortiCNAPP integrate with to orchestrate and execute this automated response action?
A. FortiSOAR
B. FortiSIEM
C. FortiGate
D. FortiMail
Answer: A
Explanation:
FortiSOAR provides Security Orchestration, Automation, and Response capabilities. By integrating with FortiCNAPP, FortiSOAR can receive alerts and automatically execute playbooks, such as invoking AWS APIs to quarantine an infected EC2 instance. FortiSIEM is primarily used for event correlation and log management.

4.Which FortiCNAPP feature allows security teams to visualize how multiple distinct risks, such as a vulnerable internet-facing service and an over-privileged IAM role, could be combined by an attacker to compromise sensitive data?

A. SmartFix
B. Compliance Reporting
C. Attack paths
D. Audit Trails
Answer: C
Explanation:
Attack paths visually map out how various misconfigurations, vulnerabilities, and identity risks can be chained together. This visualization helps analysts understand the exploitability of their environment and prioritize remediation efforts based on the actual route an attacker might take.

5.During a code repository analysis, FortiCNAPP alerts the security team about a critical risk in a recent developer pull request. The alert specifies that a file contains an AWS Access Key ID and Secret Access Key in plain text.
Which specific risk did FortiCNAPP detect?
A. Insecure Infrastructure-as-Code (IaC) configuration
B. Hard-coded secrets
C. Software Composition Analysis (SCA) vulnerability
D. Over-privileged container deployment
Answer: B
Explanation:
Hard-coded secrets refer to sensitive information like API keys, passwords, or access tokens embedded directly into the source code. FortiCNAPP integrates with code repositories to scan for and detect these exposed secrets before they are merged into the main codebase.