Fortinet

NSE6_NDR_AN-26

Fortinet NSE 6 - FortiNDR Cloud 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 SOC engineer wants a custom internal application to programmatically pull FortiNDR Cloud detection and event data on a schedule, without an analyst clicking through the portal.
Which mechanism is designed for this programmatic data exchange?

A. Triggering host isolation through the FortiEDR integration to gather the detection data directly from the endpoints
B. Downloading a packet capture for each session so the external application can parse the raw traffic itself
C. Tuning the detectors so their output is automatically formatted for the external application to read
D. The FortiNDR Cloud API functions, which allow another tool to exchange data with the platform programmatically

Answer: D

Question: 2

FortiNDR Cloud raises a high-confidence detection of command-and-control beaconing from an internal host. The analyst confirms the activity through the timeline and enrichment, and the threat appears active and likely to spread.
What is the BEST way to use the integrated toolset to contain the endpoint while preserving network evidence?

A. Trigger host isolation through the FortiEDR integration to contain the endpoint while FortiNDR Cloud retains network-wide visibility and evidence
B. Delete the detection and rely on future IOC-based alerts to catch any recurrence of the same activity later
C. Use an IQL query to block the host's outbound traffic directly at the network sensor itself
D. Tune the detector to lower its severity so it stops re-alerting on the compromised host for the entire remainder of the active incident response window

Answer: A

Question: 3

An analyst is investigating a detection in FortiNDR Cloud and wants to add external threat context before deciding on a disposition.
Which two actions enrich the investigation with external context?

(Choose two.)

A. Raise the detection's severity to force an escalation.
B. Use OSINT to research an external domain or IP for its reputation and ownership.
C. Delete the detection's metadata from the investigation.
D. Check a suspicious file hash against VirusTotal for its known-malware reputation.
E. Isolate the endpoint host to stop the observed activity.
F. Increase the sensor's capture throughput so more traffic is recorded during the investigation.

Answer: B,D

Question: 4

An analyst has determined that a detection reflects benign activity and is choosing a resolution for it. The platform also offers a choice about how broadly that resolution should apply.
What does the scoping choice determine when a resolution is applied?

A. It determines which sensors are permitted to forward their captured metadata to the cloud back-end for this specific entity's traffic.
B. It determines the severity value that the platform will assign to any future detections produced by the same detector.
C. It determines the enrichment sources, such as OSINT and VirusTotal, that will be consulted the next time this entity comes up for investigation.
D. It determines how broadly the resolution applies, for example only to this specific entity or instance versus to matching activity more widely.

Answer: D

Question: 5

While working a detection, an analyst notices a suspicious external domain referenced within it and decides to investigate that indicator further before deciding on a disposition.
Which two actions are consistent with an IOC investigation carried out within a detection?
(Choose two.)

A. Immediately isolate every host in the environment before determining whether the indicator is actually malicious or benign.
B. Reduce the detector's confidence value so the indicator stops appearing in the detection results the analyst is reviewing.
C. Search other event metadata for the same indicator to find which additional entities also communicated with it.
D. Rely solely on the single detection event and avoid correlating the indicator against any other observed activity.

E. Check the indicator against external enrichment such as OSINT and VirusTotal to assess whether it is already known to be malicious.

Answer: C,E

Question: 6

An analyst is tracking a detection's progress through triage over time.
What does the investigation stage represent?

A. It tracks where the detection sits in the analyst's workflow — for example, not started, in progress, or resolved.
B. It sets the confidence level that the detector will apply to the finding the next time that detector happens to fire.
C. It is the MITRE ATT&CK technique identifier the platform assigns to categorize the detection.
D. It measures the network throughput of the sensor that produced the detection over the capture window.

Answer: A

Question: 7

An analyst is building a quick reference that pairs each protocol's metadata with the threat behavior it most strongly reveals.
Which three pairings are correct?
(Choose three.)

A. Flow metadata most strongly reveals the plaintext contents of web requests.
B. SSL metadata most strongly reveals suspicious or anomalous certificates in encrypted sessions.
C. DCE/RPC metadata most strongly reveals the certificate details of encrypted sessions.
D. DNS metadata most strongly reveals covert command-and-control and data exfiltration that abuse name resolution.
E. SMB metadata most strongly reveals lateral movement through Windows file-share access.

Answer: B,D,E

Question: 8

During onboarding, a colleague assumes that every packet crossing the network is captured and stored in full by FortiNDR Cloud.
Which statement best describes what the sensors primarily send to the cloud back-end?

A. They capture and forward every packet in full for all monitored traffic, acting as a continuous full-packet recorder that stores the entire environment's payloads.
B. They primarily extract and forward rich per-event metadata, together with selective packet data, rather than continuous full packet capture of all traffic.
C. They forward only aggregate byte counters and totals, with no per-connection or per-protocol detail retained.
D. They forward endpoint process telemetry gathered from host agents installed across the fleet.

Answer: B

Question: 9

After the back-end matches detections, the FortiNDR Cloud pipeline relates individual signals to one another before the resulting events are retained for later search.
Which pipeline stage performs this relating of separate signals?

A. Intelligence correlation, which relates separate signals to one another after detection matching and before data storage.
B. Enrichment, which adds external threat-intelligence context to extracted entities early in the pipeline, before detection matching runs.
C. Data storage, which retains the finished events and metadata so analysts can query them long after correlation runs.
D. Entity information extraction, which identifies hosts, domains, and similar entities from the incoming metadata.

Answer: A

Question: 10

A colleague argues that FortiNDR Cloud's SaaS architecture is essentially the same as a traditional on-premises analytics deployment.
Which two statements correctly distinguish FortiNDR Cloud's SaaS NDR architecture from an on-prem analytics stack?
(Choose two.)

A. Analysts must maintain a local on-prem cluster to store and correlate all detections.
B. The heavy detection and analysis processing is hosted in the vendor's cloud back-end rather than on a customer-run analytics stack.
C. All analysis is performed offline on exported packet files, with no cloud component involved.
D. Customer-deployed sensors are responsible for observing traffic and producing metadata, not for running the analytics themselves.
E. Each sensor must be licensed and deployed as a standalone endpoint agent on every host.

Answer: B,D

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/