PassQueen
a.k.a dumpsqueen.com

Certified Threat Protection Analyst Exam

Proofpoint PPAN01

Version Demo

Total Demo Questions: 7

Total Premium Questions: 75

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

An analyst plans to add a domain associated with an active phishing campaign to the TAP URL Defense Custom Blocklist. Which two actions help reduce the risk of unnecessary business disruption? (Select two.)

A. Validate the malicious hostname or domain against campaign evidence.

B. Assess legitimate business use before applying a broad domain-level block.

C. Block the parent domain immediately without reviewing its scope.

D. Allow the destination until the next scheduled policy review.

E. Block every newly registered domain as a precaution.

ANSWER: A B

Explanation:

The analyst should validate the malicious hostname or domain against the observed campaign evidence so that the block is tied to the actual threat infrastructure. The analyst should also assess whether the proposed domain is used by legitimate business services before applying a broad domain-level block.

Blocking a parent domain without assessing its use can disrupt legitimate applications, shared hosting, or widely used services. Allowing the destination until the next policy review or blocking all newly registered domains does not provide a precise, evidence-based response.

QUESTION NO: 2

An attacker registers a domain like “great-company.com” to impersonate “greatcompany.com.” What tactic is being used?

A. Domain Hijacking

B. Display Name Spoofing

C. Lookalike Domain

D. Subdomain Takeover

ANSWER: C

Explanation:

Lookalike Domain is correct because the attacker has registered a separate domain name designed to resemble the legitimate organization’s domain closely enough to mislead recipients. Adding a hyphen, omitting or adding characters, substituting visually similar characters, or selecting a deceptive top-level domain are common ways to create such a resemblance. This technique is also commonly described as typosquatting or domain impersonation when the goal is to exploit users’ tendency to recognize a familiar brand name rather than inspect every character of the sender domain.

In a Proofpoint investigation, the key observation is that the sending domain is not the authentic corporate domain, even though it appears similar at a glance. Analysts should examine the exact envelope-sender and visible From-domain spelling, registration history where available, message authentication results, sending infrastructure, and any associated URLs. Lookalike domains are especially relevant to business email compromise and credential-phishing investigations because they allow a threat actor to establish a controlled sending identity that resembles a trusted brand or executive. Proofpoint describes domain spoofing and impersonation techniques in its domain spoofing threat reference; additional context on deceptive domain registration is available from ICANN’s security, stability, and resiliency resources.

QUESTION NO: 3

A legitimate marketing message was quarantined as spam, and the business owner believes it is a false positive. Which two actions should the analyst take before making a broad allow-listing change? (Select two.)

A. Review the Proofpoint message headers, spam details, and applicable policy result.

B. Validate the sender identity and the legitimacy of the business communication.

C. Disable spam filtering for all recipients while the message is reviewed.

D. Automatically release all messages from the same sending domain.

E. Add the sender to an allow list before reviewing the quarantine evidence.

ANSWER: A B

Explanation:

The analyst should review the message headers and Proofpoint spam details to determine the rule, policy, score, and classification evidence that led to quarantine. The analyst should also validate the sender identity, authentication results, content, and expected business relationship before deciding that the message is legitimate.

A broad allow-listing change made without validation can create a gap that attackers can exploit. Disabling spam protection or automatically releasing all similar messages is not an appropriate response to one suspected false positive.

QUESTION NO: 4

What action does Proofpoint Collab Protection take when a malicious URL is detected?

A. Sends an alert to the userâ€™s manager.

B. Encrypts the browser session.

C. Automatically deletes the URL from the system.

D. Redirects the browser to a block page.

ANSWER: D

Explanation:

Proofpoint Collab Protection protects collaboration environments by applying threat detection and remediation controls to content shared through supported platforms. For a URL identified as malicious, redirecting the browser to a block page is the appropriate enforcement action because it stops the user from reaching the harmful destination at the point of access. This is particularly important for phishing and credential-harvesting links, whose risk can change after a message or file has already been posted in a collaboration channel.

The block-page experience provides immediate, understandable feedback that the destination is unsafe while maintaining the protection boundary between the user and the malicious site. It also supports operational response by recording a blocked access attempt, which can help security teams investigate exposure and determine whether further action is needed. This approach aligns with Proofpoint’s time-of-click URL protection model: URLs can be evaluated when a user attempts to open them, allowing enforcement based on the link’s current threat status rather than only its status when originally shared. Proofpoint describes its collaboration protection capabilities at Proofpoint Collaboration Protection and its URL time-of-click protection approach at Proofpoint URL Defense.

QUESTION NO: 5

When filtering for threats on the TAP People page, which two filters have the highest chance of finding compromises? (Select two.)

A. Exposure > Permitted Clicks

B. Users > Locations

C. Exposure > Delivered with Accessible Threat

D. Threats > False Positives Only

E. Users > VIP

ANSWER: A C

Explanation:

Exposure > Permitted Clicks and **Exposure > Delivered with Accessible Threat** are the most useful filters for prioritizing people who may have been compromised. A permitted click records an actual user interaction with a URL that was allowed at click time. This provides a high-value behavioral signal because the user reached the destination rather than merely receiving a suspicious message. Analysts can use the associated click details and timeline to investigate the destination, determine whether credentials may have been entered, and correlate the activity with identity, endpoint, or network events.

Delivered with an accessible threat identifies users who received a message containing a threat that remained available to them. This is an important exposure condition: the malicious payload or URL was not only detected, but was present in the user's mailbox or message experience where interaction could occur. Combining accessible-threat exposure with user-centric investigation helps analysts identify recipients requiring rapid validation and remediation. Proofpoint Threat Protection is designed to provide visibility into malicious email and user interaction, while TAP adds post-delivery threat intelligence and click-related context for investigation. See Proofpoint Targeted Attack Protection and Proofpoint Email Protection.

QUESTION NO: 6

Refer to Exhibit:

X-Proofpoint-Banner-Trigger: inbound

MIM-version: 1.0

Content-Type: multipart/mixed; boundary="boundary-1698346305"

X-CLX-Shades: MLX

X-Proofpoint-Virus-Version: vendor=baseguard

engine=ICAP:2.0.272,Aquarius:18.0.987,Hydra:6.0.619,FMLib:17.11.176.26 definitions=2023-10-26_22,2023-10-26_01,2023-05-22_02

X-Proofpoint-Spam-Details: rule=spam policy=default score=89 bulkscore=0 phishscore=0 mlxlogscore=-91 suspectscore=0 malwarescore=0 adultscore=0 spamscore=89 classifier=spam adjust=0 reason=mlx scancount=l engine=8.12.0-2310240000 definitions=main-2310260209

In the process of reviewing a false positive, you see the following email header. What was the reason the message was quarantined by the Proofpoint Protection Server?

A. A custom spam rule caused the message to be quarantined.

B. An anti-virus rule forced the message to be quarantined.

C. The recipient's personal block list forced quarantine of the message.

D. A content policy rule (DLP/compliance) forced quarantine of the message.

ANSWER: A

Explanation:

A custom spam rule caused the message to be quarantined. The dispositive evidence is the `X-Proofpoint-Spam-Details` header, which identifies `rule=spam` and `policy=default`. This records that the message was processed under

the spam rule path of the applicable Proofpoint policy. The spam evaluation also reports `score=89` and `spamscore=89`, showing that the message accumulated a high spam score sufficient for the configured spam action, including quarantine. The `classifier=spam` value further confirms the classification category used for the decision.

The `reason=mlx` field identifies MLX as the classification reason associated with that spam verdict. MLX is Proofpoint's machine-learning-based detection technology, and the accompanying `X-CLX-Shades: MLX` header is consistent with MLX involvement in the message assessment. For false-positive analysis, these fields direct the analyst to review the spam-policy threshold and spam-classification behavior that applied to the recipient and message flow. The virus-version header only establishes that antivirus engines and definitions were present for scanning; the spam-details header provides the actual rule family and scoring evidence for this quarantine decision. See Proofpoint's Threat Reference and Proofpoint Help Center for product documentation and threat-classification guidance.

QUESTION NO: 7

You would like to view the total number of uncleared threats or false positives that have been interacted with by users over the past 2 weeks. How can this be accomplished on the TAP Dashboard?

A. On the Threats page, select Last 14 days and click on the "Intended" column header.

B. On the Threats page, select Last 14 days and click on the "At Risk" column header.

C. On the Threats page, select Last 14 days and click on the "Impacted" column header.

D. On the Threats page, select Last 14 days and click on the "Highlighted" column header.

ANSWER: C

Explanation:

On the Threats page, select Last 14 days and click on the "Impacted" column header. This view aligns directly with the requirement to identify items that users have interacted with, because the Impacted measure represents the population affected by detected threats. Applying the Last 14 days time range constrains the dashboard data to the requested two-week reporting period, while selecting the Impacted column focuses the analyst on the relevant interaction-based count. This is useful for triage because an interaction can indicate a higher-priority event requiring investigation, such as a recipient clicking a malicious URL or otherwise engaging with a message-associated threat. The Threats dashboard is intended to give security analysts a consolidated view of threat activity and enable them to prioritize investigations using the available threat and user-impact context. Reviewing the Impacted value over the selected time range therefore provides the appropriate operational view for uncleared threats or false positives that have reached and involved users. Proofpoint describes TAP as providing visibility into people targeted by threats and the associated attack activity; see Proofpoint Targeted Attack Protection and Proofpoint Threat Reference.