KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **SecOps-Pro**

Title : Palo Alto Networks Security Operations Professional

Version : DEMO

1.A Security Operations Center (SOC) using Palo Alto Networks XSOAR for incident management receives a high volume of alerts daily. An analyst is tasked with prioritizing incidents related to potential data exfiltration.
Which of the following incident categorization criteria, when combined, would MOST effectively facilitate accurate prioritization for data exfiltration incidents, considering both technical indicators and business impact?
A. Source IP Geolocation and Destination Port. While useful, these alone may not capture the full context of data exfiltration.
B. Threat Intelligence Feed Match (e.g., C2 IP from Unit 42) and Affected Asset Criticality (e.g., Crown Jewel Asset). This combines technical indicators with business impact for effective prioritization.
C. Time of Day and User Department. These are primarily contextual and less indicative of immediate threat severity.
D. Alert Volume from a specific sensor and Protocol Used. Alert volume can be misleading, and protocol alone might not signify exfiltration.
E. File Hash Reputation (WildFire) and Endpoint OS Version. File hash is good for malware, but OS version isn't a primary exfiltration indicator.
Answer: B
Explanation:
Effective incident prioritization for data exfiltration requires a combination of strong technical indicators and an understanding of the business impact. Matching an IP to a known Command and Control (C2) server from a reputable threat intelligence source like Unit 42 (Palo Alto Networks' threat research team) provides a high-fidelity technical indicator of a potential breach. Coupling this with the criticality of the affected asset (e.g., a server hosting sensitive customer data, classified as a 'Crown Jewel') directly informs the business risk, enabling accurate prioritization. Other options either lack sufficient technical specificity for exfiltration or don't adequately account for business impact.

2.A large enterprise is implementing a new incident response playbooks within Palo Alto Networks Cortex XSOAR. They need to define a comprehensive incident categorization schema that supports dynamic prioritization based on the MITRE ATT&CK framework and internal asset criticality ratings.
Which of the following XSOAR automation snippets, when integrated, best demonstrates an approach to dynamically categorize and prioritize an incident based on the detection of a 'Lateral Movement' technique (T 1021 – Remote Services) and the involved asset's 'Crown Jewel' status?
A)
```
incident.set('category', 'Lateral Movement');
incident.set('priority', 'Medium');
```
This is too static and doesn't account for dynamic prioritization based on asset criticality.
B)
```
if 'T1021' in incident.tags and 'CrownJewel' in incident.assets.get('criticality'):
    incident.set('category', 'Advanced Persistent Threat');
    incident.set('severity', 'Critical');
elif 'T1021' in incident.tags:
    incident.set('category', 'Internal Network Compromise');
    incident.set('severity', 'High');
```
This snippet correctly uses ATT&CK tags and asset criticality to dynamically categorize and assign

severity, which directly influences prioritization.

C)

```
incident.set('incidentName', 'T1021 Detected');
incident.set('owner', 'SOC_Team_A');
```

This snippet is for incident naming and assignment, not categorization or prioritization logic.

D)

```
incident.addTag('MITRE_T1021');
incident.addTag('Affected_Server');
```

This snippet only adds tags, which can be used for categorization later, but doesn't implement the prioritization logic itself.

E)

```
incident.set('status', 'Open');
incident.set('playbook', 'LateralMovementPlaybook');
```

This snippet sets status and assigns a playbook, not directly addressing categorization or dynamic prioritization.

A. Option A

B. Option B

C. Option C

D. Option D

Answer: B

Explanation:

Option B best demonstrates dynamic categorization and prioritization. It checks for the presence of the MITRE ATT&CK technique ID (T1021) in the incident's tags (assuming these tags are applied by initial detection mechanisms or XSOAR ingestion). Crucially, it then checks the criticality of the involved assets. If both 'Tl 021' and 'CrownJewel' criticality are present, it elevates the category to 'Advanced Persistent Threat' and sets the severity to 'Critical', indicating a high-priority incident. If only 'T 1021' is present, it assigns a 'High' severity, still acknowledging the threat but indicating a potentially lower business impact. This logic directly maps to a robust categorization and prioritization scheme.

3.During a post-incident review of a successful ransomware attack, the incident response team identifies that initial alerts were generated but deprioritized due to an 'Information' severity classification. Analysis reveals the alerts, while individually low-fidelity, collectively pointed to a reconnaissance phase followed by credential access on a critical server.

What adjustment to the incident categorization and prioritization framework would be most effective in preventing similar oversights?

A. Implement an automated system to escalate any 'Information' level alert to 'Low' severity after 24 hours, regardless of context.

B. Mandate manual review of all 'Information' severity alerts by a Tier 1 SOC analyst within 1 hour of generation.

C. Develop correlation rules in the SIEM (e.g., Splunk, QRadar) or SOAR (e.g., XSOAR) to elevate incident severity based on sequences of related low-severity events targeting high-value assets.

D. Increase the threshold for all network-based alerts by 50% to reduce false positives and focus only on high-severity alerts.

E. Categorize all alerts related to critical servers as 'High' severity by default, irrespective of the initial

detection's confidence level.
Answer: C
Explanation:
The core issue described is the failure to recognize a low-and-slow attack chain composed of individually low-fidelity events. Implementing correlation rules (Option C) in the SIEM or SOAR is the most effective solution. This allows the system to analyze multiple seemingly innocuous events in sequence, identify patterns indicative of an attack (e.g., reconnaissance followed by credential access on a critical asset), and then automatically elevate the aggregated incident's severity and priority.
Options A and B are inefficient or reactive.
Option D risks missing legitimate threats.
Option E would lead to significant alert fatigue and false positives, overwhelming analysts.

4.A threat intelligence team produces a report on a new APT group known for targeting specific industry sectors using novel obfuscation techniques. This report includes IOCs (Indicators of Compromise) and TTPs (Tactics, Techniques, and Procedures).
How should this intelligence be integrated into an organization's incident categorization and prioritization process to maximize its impact?
A. The IOCs should be immediately blocked at the firewall, and the TTPs added to a static incident classification matrix.
B. The IOCs should be used to create new detection rules with a 'Critical' severity, and the TTPs should inform playbooks and analyst training for identifying related behavioral anomalies and dynamically assigning higher priority to incidents matching these TTPs.
C. The report should be circulated to all IT staff for awareness, and any alerts matching the IOCs should be manually reviewed daily.
D. Only the IOCs should be ingested into the SIEM as watchlists, and TTPs should be ignored as they are too abstract for direct prioritization.
E. The intelligence should primarily be used for retrospective hunting exercises and not directly integrated into real-time categorization.
Answer: B
Explanation:
Integrating threat intelligence effectively means leveraging both IOCs and TTPs. IOCs (like hashes, IPs, domains) are excellent for creating specific, high-fidelity detection rules (Option B), which can be automatically assigned a high severity due to the known threat actor. TTPs, being behavioral patterns, are crucial for informing and refining incident categorization and prioritization beyond just IOC matches. By understanding the APT group's TTPs, security teams can:
1) Create more sophisticated detection logic in the SIEM/EDR, 2) Develop or modify XSOAR playbooks to look for combinations of events that align with these TTPs, and 3) Train analysts to recognize these behaviors, allowing them to dynamically assign higher priority to incidents exhibiting these characteristics, even if no explicit IOCs are present. This holistic approach significantly improves detection and response capabilities.

5.An organization is migrating its security operations to a cloud-native environment, leveraging Palo Alto Networks Prisma Cloud for security posture management and cloud workload protection. Incident response requires adapting existing on-premise prioritization schemes.

Which of the following factors becomes SIGNIFICANTLY more impactful for incident prioritization in a cloud-native context compared to traditional on-premise environments?
A. The physical location of the server hosting the affected application. This is less relevant in cloud as physical location is abstracted.
B. The organizational unit responsible for the application. While important, this is a consistent factor.
C. The specific cloud service (e.g., S3 bucket, Lambda function, Kubernetes pod) involved and its configured IAM permissions. Misconfigurations or compromises of these can have rapid, widespread impact.
D. The brand of the underlying hardware vendor. Cloud abstracts hardware, making this irrelevant.
E. The patching cycle of the operating system. While important, patching is often automated or managed differently in cloud, and other cloud-specific factors take precedence.
Answer: C
Explanation:
In a cloud-native environment, the specific cloud service and its IAM (Identity and Access Management) permissions are paramount for incident prioritization. A misconfigured S3 bucket with public access, a compromised Lambda function with excessive permissions, or a vulnerable Kubernetes pod could lead to rapid data exposure, privilege escalation, or resource abuse, often with broader and faster impact than traditional on-premise incidents. The blast radius and potential for lateral movement are heavily influenced by cloud service configurations and IAM. This makes understanding and prioritizing based on these factors critical.