ExamsIndex
Practice Materials & Tests

DEMO VERSION

Palo Alto Networks

SecOps-Pro Exam

Palo Alto Networks Security Operations Professional

Exam Latest Version: 6.0

Question 1. (Single Select)

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.

Correct 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.

Question 2. (Multi Select)

Consider an incident categorization and prioritization framework within Palo Alto Networks XSOAR. An analyst identifies an alert indicating a 'Brute Force' attempt (MITRE ATT&CK T 1110) against an administrative service. The asset involved is tagged in XSOAR as having 'PCI-DSS Data' and 'Internet-Facing'. Which of the following XSOAR automation script segments would correctly classify this incident as 'Critical' and categorize it appropriately, adhering to best practices for a compliance-driven environment? (Select all that apply)

A:

```
if 'T1110' in incident.get('mitre_techniques') and 'PCI-DSS Data' in incident.get('asset_tags') and 'Internet-Facing' in incident.get('asset_tags'):
    incident.set('severity', 'Critical');
    incident.set('category', 'Compliance Breach Attempt');
```

B:

```
if 'Brute Force' in incident.get('name') or 'T1110' in incident.get('playbook_tags'):
    if incident.get('affected_asset_type') == 'Admin_Server' and incident.get('network_exposure') == 'External':
        incident.set('severity', 'High');
        incident.set('category', 'Credential Attack');
```

C:

```
# Assume a pre-defined 'CriticalAssets' list in a global XSOAR lookup
if 'T1110' in incident.get('mitre_techniques') and incident.get('affected_asset_id') in demisto.get(CriticalAssets):
    incident.set('severity', 'Critical');
    incident.set('category', 'TopTier Attack');
```

D:

```
incident.set('severity', 'Low');
incident.set('category', 'AlertReview'); # Default categorization, no specific prioritization logic
```

E:

```
incident.addTag('BruteForce');
incident.addTag('PCI_Related');
incident.set('owner', 'Compliance_Team');
```

Correct Answer: A, C

```
if 'T1110' in incident.get('mitre_techniques') and 'PCI-DSS Data' in incident.get('asset_tags') and 'Internet-Facing' in incident.get('asset_tags'):
    incident.set('severity', 'Critical');
    incident.set('category', 'Compliance Breach Attempt');
```

```
# Assume a pre-defined 'CriticalAssets' list in a global XSOAR lookup
if 'T1110' in incident.get('mitre_techniques') and incident.get('affected_asset_id') in demisto.get(CriticalAssets):
    incident.set('severity', 'Critical');
    incident.set('category', 'TopTier Attack');
```

Explanation:

Both A and C are valid approaches for critical categorization. Option A directly checks for the MITRE technique tag and specific asset tags ('PCI-DSS Data', 'Internet-Facing'), which are explicit indicators of high risk in a compliance-driven environment, leading to a 'Critical' severity and a 'Compliance Breach Attempt' category. Option C leverages a pre-defined list of 'CriticalAssets' (which should encompass assets with PCI-DSS data and internet exposure) and the MITRE technique. If the 'CriticalAssets' list is accurately maintained and 'TopTier Attack' is an appropriate category for such a high-impact incident in their schema, this is also a very effective and scalable method. Option B uses less precise attributes and a slightly lower severity. Options D and E fail to address the core prioritization requirement.

Question 3. (Multi Select)

Consider an incident categorization and prioritization framework within Palo Alto Networks XSOAR. An analyst identifies an alert indicating a 'Brute Force' attempt (MITRE ATT&CK T 1110) against an administrative service. The asset involved is tagged in XSOAR as having 'PCI-DSS Data' and 'Internet-Facing'. Which of the following XSOAR automation script segments would correctly classify this incident as 'Critical' and categorize it appropriately, adhering to best practices for a compliance-driven environment? (Select all that apply)

A:

```
if 'T1110' in incident.get('mitre_techniques') and 'PCI-DSS Data' in incident.get('asset_tags') and 'Internet-Facing' in incident.get('asset_tags'):
    incident.set('severity', 'Critical');
    incident.set('category', 'Compliance Breach Attempt');
```

B:

```
if 'Brute Force' in incident.get('name') or 'T1110' in incident.get('playbook_tags'):
    if incident.get('affected_asset_type') == 'Admin_Server' and incident.get('network_exposure') == 'External':
        incident.set('severity', 'High');
        incident.set('category', 'Credential Attack');
```

C:

```
# Assume a pre-defined 'CriticalAssets' list in a global XSOAR lookup
if 'T1110' in incident.get('mitre_techniques') and incident.get('affected_asset_id') in demisto.get(CriticalAssets):
    incident.set('severity', 'Critical');
    incident.set('category', 'TopTier Attack');
```

D:

```
incident.set('severity', 'Low');
incident.set('category', 'AlertReview'); # Default categorization, no specific prioritization logic
```

E:

```
incident.addTag('BruteForce');
incident.addTag('PCI_Related');
incident.set('owner', 'Compliance_Team');
```

Correct Answer: A, C

```
if 'T1110' in incident.get('mitre_techniques') and 'PCI-DSS Data' in incident.get('asset_tags') and 'Internet-Facing' in incident.get('asset_tags'):
    incident.set('severity', 'Critical');
    incident.set('category', 'Compliance Breach Attempt');
```

```
# Assume a pre-defined 'CriticalAssets' list in a global XSOAR lookup
if 'T1110' in incident.get('mitre_techniques') and incident.get('affected_asset_id') in demisto.get(CriticalAssets):
    incident.set('severity', 'Critical');
    incident.set('category', 'TopTier Attack');
```

Explanation:

Both A and C are valid approaches for critical categorization. Option A directly checks for the MITRE technique tag and specific asset tags ('PCI-DSS Data', 'Internet-Facing'), which are explicit indicators of high risk in a compliance-driven environment, leading to a 'Critical' severity and a 'Compliance Breach Attempt' category. Option C leverages a pre-defined list of 'CriticalAssets' (which should encompass assets with PCI-DSS data and internet exposure) and the MITRE technique. If the 'CriticalAssets' list is accurately maintained and 'TopTier Attack' is an appropriate category for such a high-impact incident in their schema, this is also a very effective and scalable method. Option B uses less precise attributes and a slightly lower severity. Options D and E fail to address the core prioritization requirement.

Question 4. (Single Select)

An organization is using a bespoke vulnerability management system that integrates with Palo Alto Networks Panorama for firewall rule management and XSOAR for incident orchestration. A new zero-day vulnerability (CVE-2023-XXXX) affecting a critical web application is disclosed. The vulnerability management system flags all instances of this application. For effective incident categorization and prioritization, what dynamic attributes or processes are crucial to incorporate, going beyond mere vulnerability detection?

A: The CVSS score of the CVE and the number of affected instances. While important, these are static at disclosure and don't reflect environmental factors or active exploitation.
B: Leveraging external threat intelligence feeds (e.g., Unit 42, CISA KEV) to confirm active exploitation of CVE-2023-XXXX in the wild, correlating with observed network traffic (e.g., Palo Alto Networks firewall logs for unusual HTTP requests), and assessing the business impact of the specific web application.
C: Assigning all alerts related to CVE-2023-XXXX to the highest priority, irrespective of whether the application is internet-facing or handles sensitive data.
D: Prioritizing remediation based solely on the operating system of the affected server, as OS-level vulnerabilities are always most critical.
E: Ignoring the vulnerability until a patch is released, as immediate action is often disruptive.

Correct Answer: B

Explanation:

Prioritizing a zero-day vulnerability goes far beyond its static CVSS score or the number of affected systems. Option B outlines a comprehensive, dynamic approach: 1) Active Exploitation Confirmation: External threat intelligence (like CISA KEV or Unit 42 reports) indicating active exploitation in the wild immediately elevates the threat. 2) Correlated Network Activity: Analyzing Palo Alto Networks firewall logs or other network telemetry for unusual traffic patterns (e.g., specific HTTP requests, C2 communications) that align with known exploitation attempts for that CVE provides high-fidelity in-house detection. 3) Business Impact Assessment: Understanding the criticality of the specific web application (e.g., public-facing, handles sensitive customer data, critical business function) is paramount. Combining these three dynamic factors allows for truly informed categorization (e.g., 'Active Zero-Day Exploitation on Crown Jewel Asset') and prioritization (e.g., 'Critical - Immediate Containment'). Options A, C, D, and E represent static, overly broad, or negligent approaches.

Question 5. (Single Select)

A global enterprise manages its security incidents using Palo Alto Networks XSOAR. The CEO's laptop, classified as a 'Tier 0' asset, triggers an alert for an 'Unknown Malware Execution' (WildFire verdict: 'Grayware'). Historically, 'Grayware' on endpoints has been deprioritized. However, given the asset's criticality, the SOC needs a dynamic prioritization mechanism. Which set of XSOAR automation steps and corresponding incident attributes should be leveraged to

ensure this incident is elevated appropriately, even with a 'Grayware' verdict?

- Step 1: Set incident category to 'Malware' and severity to 'Low'. Step 2: Manually check asset owner. This is reactive and doesn't dynamically elevate.
- Step 1: Configure an XSOAR pre-processing rule to enrich incidents with asset criticality based on CMDB integration (e.g., 'Tier 0'). Step 2: Implement a conditional XSOAR playbook task: IF 'WildFire_Verdict' == 'Grayware' AND 'Asset_Criticality' == 'Tier 0', THEN set incident 'Severity' to 'High' and 'Category' to 'Executive Compromise Attempt'.
- Step 1: Create a custom XSOAR field 'is_CEO_Laptop'. Step 2: If 'is_CEO_Laptop' is 'true', set severity to 'Critical' regardless of WildFire verdict. This is overly broad and doesn't consider the specific 'Grayware' context.
- Step 1: Block the 'Grayware' hash at the firewall. Step 2: Close the incident automatically. This bypasses proper prioritization and investigation based on asset criticality.
- Step 1: Assign the incident to the endpoint team with 'Informational' priority. Step 2: Await their manual assessment. This fails to address the immediate prioritization need for a critical asset.

A: Option A
B: Option B
C: Option C
D: Option D
E: Option E

Correct Answer: B

Explanation:

Option B provides the most robust and dynamic solution. The key is to integrate asset criticality into the incident enrichment and subsequent prioritization logic. Step 1, using an XSOAR pre-processing rule, automatically enriches the incident data with the 'Tier 0' criticality from the CMDB. This means the incident context always includes the asset's importance. Step 2, the conditional playbook task, is crucial: it explicitly checks for both the 'Grayware' verdict AND the 'Tier 0' asset criticality. When both conditions are met, it overrides the default 'Grayware' low severity and elevates the incident to 'High' severity with a specific category like 'Executive Compromise Attempt', ensuring it receives immediate attention despite the initially 'lower' malware verdict. This demonstrates a sophisticated understanding of context-aware incident prioritization.

ExamsIndex

Demo PDF Complete

Your SecOps-Pro Demo (5 Questions)

Get the Complete Version

Full Questions with Detailed Explanations

Interactive Web-Based Exams Available

To get 50% off, use Coupon Code: OCT50

https://examsindex.com/exam/secops-pro