# SecOps-Pro자격증공부자료 - SecOps-Pro최고품질인증시험기출자료

Certificate

SAMPLE

COS PRO

홍길동

생년월일 : ******

자격 종목 및 등급 : C++ 1급

발급일자 : 20**-**-**

자격증번호 : 2*_**_*******

주식회사 와이비엠 대표이사

그 외, DumpTOP SecOps-Pro 시험 문제집 일부가 지금은 무료입니다: https://drive.google.com/open?id=1QFDG1GCzJ9yuf_D-7oCdN96sktIXliCB

근 몇년간IT산업이 전례없이 신속히 발전하여 IT업계에 종사하는 분들이 여느때보다 많습니다. 경쟁이 이와같이 치열한 환경속에서 누구도 대체할수 없는 자기만의 자리를 찾으려면 IT인증자격증취득은 무조건 해야 하는것이 아닌가 싶습니다. Palo Alto Networks인증 SecOps-Pro시험은 IT인증시험중 가장 인기있는 시험입니다. DumpTOP에서는 여러분이Palo Alto Networks인증 SecOps-Pro시험을 한방에 패스하도록 실제시험문제에 대비한Palo Alto Networks인증 SecOps-Pro덤프를 발췌하여 저렴한 가격에 제공해드립니다.시험패스 못할시 덤프비용은 환불처리 해드리기에 고객님께 아무런 페를 끼치지 않을것입니다.

다른 방식으로 같은 목적을 이룰 수 있다는 점 아세요? 여러분께서는 어떤 방식, 어느 길을 선택하시겠습니까? 많은 분들은Palo Alto Networks인증SecOps-Pro시험패스로 자기 일에서 생활에서 한층 업그레이드 되기를 바랍니다. 하지만 모두 다 알고계시는그대로Palo Alto Networks인증SecOps-Pro시험은 간단하게 패스할 수 있는 시험이 아닙니다. 많은 분들이Palo Alto Networks인증SecOps-Pro시험을 위하여 많은 시간과 정신력을 투자하고 있습니다. 하지만 성공하는 분들은 적습니다.

**>> SecOps-Pro자격증공부자료 <<**

## SecOps-Pro최고품질 인증시험 기출자료 - SecOps-Pro Vce

Palo Alto Networks SecOps-Pro 인증시험은 최근 가장 핫한 시험입니다. 인기가 높은 만큼Palo Alto Networks SecOps-Pro시험을 패스하여 취득하게 되는 자격증의 가치가 높습니다. 이렇게 좋은 자격증을 취득하는데 있어서의 필수과목인Palo Alto Networks SecOps-Pro시험을 어떻게 하면 한번에 패스할수 있을가요? 그 비결은 바로DumpTOP의 Palo Alto Networks SecOps-Pro덤프를 주문하여 가장 빠른 시일내에 덤프를 마스터하여 시험을 패스하는것입니다.

## 최신 Security Operations Generalist SecOps-Pro 무료샘플문제 (Q123-Q128):

### 질문 # 123

You are tasked with designing an automated response workflow in Cortex XDR to deal with high-confidence malware detections, specifically targeting ransomware. The workflow should automatically contain the threat, collect forensic data, and enrich the incident for the SOC team. Which of the following combinations of Cortex XDR elements and their functionalities would be critical for building this robust automated response playbook?

- A. Incident Management for case creation; Live Terminal for real-time investigation; and WildFire for dynamic analysis of unknown files.

- B. Exploit Protection for memory-based attacks; Behavioral Threat Protection for process behavior; and 'Host Isolation' triggered manually by a SOC analyst.
- C. Policy Management for global prevention rules; Threat Intelligence Management for IOC feeds; and Device Control to restrict USB usage.
- D. XDR Pro Analytics for root cause analysis; Automated Response (Playbooks) with actions like 'Host Isolation' and 'Forensic Data Acquisition'; and 'Cortex Query Language (XQL)' for post-incident hunting.
- E. Alerts dashboard for incident prioritization; Manual 'File Quarantine' for detected samples; and 'User Activity Monitoring' for suspicious user behavior.

**정답： D**

**설명:**
Option A directly addresses the requirements for an automated response playbook against ransomware. XDR Pro Analytics provides the context for accurate automation. Automated Response (Playbooks) is the core mechanism for triggering actions. 'Host Isolation' is critical for immediate containment, and 'Forensic Data Acquisition' ensures crucial evidence is collected automatically, which is vital for ransomware investigations. XQL, while not directly part of the automated response execution, is essential for defining the conditions that trigger the playbook and for subsequent hunting and validation, making it an integral part of the overall strategy. Options B, C, D, and E either miss the automation aspect, focus on prevention only, or include manual steps instead of fully automated ones.

**질문 # 124**
A custom application running on a Linux server is suspected of being compromised. The threat actor is believed to be leveraging a zero-day vulnerability in the application to execute arbitrary code and establish a reverse shell. Cortex XDR agents are deployed on this Linux server. You, as a SOC analyst, need to identify the exact process that initiated the reverse shell, its parent process, and any outbound network connections to suspicious external IPs. Which XDR Query Language (XQL) query against Cortex Data Lake would be most effective for this specific investigation, assuming the reverse shell typically connects to port 443 on an unprivileged user's behalf from an unusual location?

- A. □
- B. □
- C. □
- D. □
- E. □

**정답： B**

**설명:**
To identify the reverse shell's process, its parent, and outbound connections, we need to correlate network connection events with process execution events. Option B starts by filtering for relevant network connections (outbound on port 443), then joins this with process execution data using the process ID. This allows for identifying the process responsible for the network connection and its parent , process_events.actor_process_command_line'), and the destination IP. Option A has an incorrect join condition; it tries to filter for bash/sh first and then join based on process_id, which might miss other reverse shell binaries. Options C, D, and E are irrelevant to the specific goal of tracing a reverse shell's process and network activity.

**질문 # 125**
A Security Operations Center (SOC) analyst is investigating a critical alert in Cortex XDR related to a suspicious PowerShell script execution detected on a Windows endpoint. The alert indicates 'Exploit Attempt - Malicious Script'. Upon initial review, the analyst observes that the script attempted to establish an outbound connection to a known malicious IP address and download a secondary payload. The SOC needs to quickly contain the threat, gather forensic data, and understand the full scope of the attack. Which of the following Cortex XDR elements and actions would be most effective in addressing this incident, considering both detection and response capabilities?

- A. Send a 'File Quarantine' command for the detected PowerShell script and then perform a 'Full Disk Scan' on the affected endpoint to find other potential threats.
- B. Review the 'Incidents' dashboard for related alerts and immediately create a new 'Custom Alert' rule based on the observed malicious IP address.
- C. Utilize 'XDR Pro Analytics' to identify similar behaviors across the environment and then trigger an 'Endpoint Response' action to delete the malicious script.
- D. Isolate the endpoint using Host Isolation, then leverage Live Terminal to examine the process tree and retrieve the

suspicious script for analysis.

- E. Execute an 'IOC Scan' across all endpoints using the malicious IP address and file hash, and then immediately block the IP address in the network firewall.

**정답： D**

**설명:**
Option A is the most effective immediate response. Host Isolation prevents further lateral movement and C2 communication. Live Terminal allows for immediate forensic investigation, including inspecting the process tree, viewing script contents, and gathering additional artifacts directly from the compromised host, which is crucial for understanding the attack's scope. While other options have merit, they are either less immediate, more reactive, or lack the combined containment and investigative capabilities for this specific scenario.

**질문 # 126**
A forensic team requires an XSOAR automation that, once triggered by a critical incident, performs the following actions: 1. Collects a forensic image from an endpoint via EDR. 2. Uploads the image to a secure cloud storage (e.g., S3). 3. Initiates an external cloud-based forensic analysis service, passing the S3 link. 4. Monitors the analysis service for completion (can take hours). 5. Downloads the analysis report and attaches it to the incident. Which of the following XSOAR design patterns (involving Scripts and/or Jobs) would be most suitable to handle the long-running, asynchronous nature of steps 3 and 4, ensuring the incident doesn't remain 'stuck' waiting for completion?

- A. Steps 1 and 2 are handled by a playbook. A separate long-running Job is continuously active, polling for new S3 images, then performs steps 3-5 independently and updates XSOAR incidents externally.
- B. The initial playbook initiates steps 1-3. For step 4, the playbook transitions the incident to a 'Pending Analysis' status and sends a message to an external message queue. A separate microservice consumes the message, performs steps 4 & 5, and then updates the XSOAR incident via API.
- C. The initial playbook initiates steps 1-3. For step 4, the playbook uses a 'Wait for condition' task and a custom command (backed by a Python Script) that polls the analysis service until completion. The playbook remains active during this wait.
- D. A single Python Script executed within the playbook that sequentially performs all 5 steps, using
- E. The initial playbook initiates steps 1-3. For step 4, a new XSOAR Job is created dynamically by the playbook, scheduled to run periodically and check the analysis service status. Upon completion, this Job triggers another playbook or updates the original incident for step 5.

**정답： B,C**

**설명:**
This scenario highlights asynchronous operations. Options C and E are both viable depending on the scale and existing infrastructure: Option C (Wait for Condition + Script): This is the most common and often preferred XSOAR native pattern for handling long-running external processes within a single playbook execution. The playbook 'pauses' at the 'Wait for condition' task, which periodically executes a script to check the status of the external service. The playbook remains active but doesn't consume excessive resources while waiting, and resumes automatically when the condition is met. This keeps the entire workflow contained within one playbook execution and incident context. Option E (External Microservice + Message Queue): For extremely long-running tasks (hours to days), or scenarios requiring complex external processing, offloading to an external microservice via a message queue (e.g., SQS, Kafka) is highly scalable. XSOAR initiates the external process, then lets the microservice handle the long wait. The microservice then updates XSOAR via API when done. This decouples the XSOAR playbook from the long-running wait. Option A is extremely inefficient and will tie up XSOAR resources. Option B introduces unnecessary complexity by dynamically creating Jobs, and a Job for polling is generally less integrated into the incident's direct workflow than a playbook's 'Wait for condition'. Option D is too decoupled and doesn't directly manage the specific incident's state for steps 3-5 effectively from an XSOAR perspective. Therefore, both C and E offer valid, robust solutions, representing different architectural choices for managing asynchronous operations. C is a direct XSOAR feature for this, while E is a broader system design pattern often integrated with XSOAR.

**질문 # 127**
An advanced persistent threat (APT) group has successfully breached a large organization's network, and the SOC is in the 'eradication' phase. They have identified several compromised endpoints and a C2 server that the attackers were using. The APT group is known for using custom malware variants and sophisticated evasion techniques. Which of the following set of actions and Palo Alto Networks tools, when combined, offers the most robust and proactive approach to eradicating the threat, preventing re-infection, and improving future detection capabilities?

- A. Performing a full re-imaging of all compromised endpoints, and updating antivirus signatures on the NGFW.
- B. Disabling all suspicious user accounts, and conducting a vulnerability scan across the entire network.
- C. Deploying Cortex XDR agents to all endpoints for real-time protection, and blocking all C2 IP addresses at the NGFW.
- D. Blocking all outbound traffic from the internal network to prevent data exfiltration, and enforcing multifactor authentication (MFA) for all user accounts.
- E. Implementing network segmentation with micro-segmentation policies via NSX integration (or similar) on the NGFW, leveraging WildFire to generate custom threat intelligence for newly discovered malware, and pushing these IOCs to all security controls (NGFW, XDR, SIEM) via MineMeld or a custom integration. Simultaneously, perform an XQL hunt in Cortex XDR for similar attack patterns across the entire environment.

**정답： E**

**설명:**
This question requires a multi-faceted approach to address an APT in the eradication phase, focusing on preventing re-infection and improving future detection.
1. Network Segmentation/Micro-segmentation: Crucial for preventing lateral movement and containing future breaches. By segmenting the network, even if one segment is compromised, the blast radius is limited. While NSX is mentioned, the core concept is micro-segmentation, which Palo Alto NGFWs can also enforce.
2. WildFire for Custom Threat Intelligence: Since the APT uses custom malware, WildFire is essential for analyzing these unique samples, generating new signatures and IOCs.
3. Pushing IOCs to all Security Controls (MineMeld/Custom Integration): This is paramount for proactive defense. Newly generated IOCs from WildFire must be immediately pushed to the NGFW (for blocking at the perimeter/internal segments), Cortex XDR (for endpoint detection and prevention), and the SIEM (for correlation and alerting). MineMeld is a Palo Alto Networks tool for sharing and consuming threat intelligence.
4. XQL Hunt in Cortex XDR: An APT attack implies a persistent, broader compromise. An XQL hunt across the entire environment is essential to find any other instances of the attack, un-identified compromised systems, or remnants of the APT activity. This moves beyond simple eradication to ensuring full scope and preventing re-infection from overlooked components.
Let's evaluate other options:
A: While good, simply deploying XDR and blocking IPs is insufficient for an APT that uses evasive custom malware and potentially dynamic C2s.
B: Re-imaging is part of eradication, but updating AV signatures alone won't protect against custom, zero-day malware.
D: Blocking all outbound traffic is too disruptive and not sustainable. MFA is crucial but a preventative measure, not an eradication strategy for an active APT.
E: Disabling accounts and vulnerability scans are important steps but not comprehensive enough for eradicating a sophisticated APT and building future resilience.

**질문 # 128**

......

# 시험패스 가능한 SecOps-Pro자격증공부자료 덤프 샘플문제 다운받기

Palo Alto Networks SecOps-Pro인증시험패스하기는 너무 힘들기 때문입니다, DumpTOP의Palo Alto Networks SecOps-Pro덤프는 레알시험의 모든 유형을 포함하고 있습니다.객관식은 물론 드래그앤드랍,시뮬문제등 실제시험문제의 모든 유형을 포함하고 있습니다.

SecOps-Pro시험은 it인증 인기자격증을 취득하는 필수과목입니다, 가격이 착한데 비해 너무나 훌륭한 덤프품질과 높은 적중율은 저희 사이트가 아닌 다른곳에서 찾아볼수 없는 혜택입니다.

- 100% 합격보장 가능한 SecOps-Pro자격증공부자료 인증시험덤프 □ ✔ SecOps-Pro □✔□를 무료로 다운로드하려면▹ www.koreadumps.com ◃웹사이트를 입력하세요SecOps-Pro최신 인증시험 기출문제
- SecOps-Pro인증시험 인기덤프 □ SecOps-Pro인증공부문제 □ SecOps-Pro퍼펙트 최신 덤프모음집 □ 무료 다운로드를 위해✔ SecOps-Pro □✔□를 검색하려면□ www.itdumpskr.com □을(를) 입력하십시오SecOps-Pro시험대비 덤프 최신 데모
- 100% 유효한 SecOps-Pro자격증공부자료 공부자료 □ ▸ www.itdumpskr.com ◂을(를) 열고{ SecOps-Pro }를 입력하고 무료 다운로드를 받으십시오SecOps-Pro시험난이도
- 100% 합격보장 가능한 SecOps-Pro자격증공부자료 인증시험덤프 □ 【 www.itdumpskr.com 】을 통해 쉽게□ SecOps-Pro □무료 다운로드 받기SecOps-Pro유효한 덤프공부
- SecOps-Pro시험난이도 □ SecOps-Pro인증공부문제 □ SecOps-Pro시험정보 □ ➡ kr.fast2test.com □□□에서⇛ SecOps-Pro ⇚를 검색하고 무료 다운로드 받기SecOps-Pro유효한 시험대비자료
- 100% 합격보장 가능한 SecOps-Pro자격증공부자료 인증시험덤프 □ 무료 다운로드를 위해 지금□ www.itdumpskr.com □에서□ SecOps-Pro □검색SecOps-Pro인증시험 인기덤프
- SecOps-Pro시험정보 □ SecOps-Pro덤프샘플문제 체험 □ SecOps-Pro시험대비 덤프 최신 데모 □ 무료 다운로드를 위해➠ SecOps-Pro □를 검색하려면□ www.koreadumps.com □을(를) 입력하십시오SecOps-Pro인증공부문제
- 100% 합격보장 가능한 SecOps-Pro자격증공부자료 인증시험덤프 □ 무료로 다운로드하려면□ www.itdumpskr.com □로 이동하여➠ SecOps-Pro □를 검색하십시오SecOps-Pro유효한 덤프공부
- 100% 합격보장 가능한 SecOps-Pro자격증공부자료 인증시험덤프 □ 무료 다운로드를 위해「 SecOps-Pro 」를 검색하려면“ www.dumptop.com ”을(를) 입력하십시오SecOps-Pro시험대비 덤프공부
- SecOps-Pro자격증공부자료 최신 덤프데모 □ 오픈 웹 사이트“ www.itdumpskr.com ”검색▹ SecOps-Pro ◃무료 다운로드SecOps-Pro시험대비 덤프공부
- 100% 유효한 SecOps-Pro자격증공부자료 공부자료 □ 【 www.dumptop.com 】웹사이트에서□ SecOps-Pro □를 열고 검색하여 무료 다운로드SecOps-Pro시험대비 덤프공부
- masteringbusinessonline.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.flirtic.com, www.stes.tyc.edu.tw, github.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.dibiz.com, www.stes.tyc.edu.tw, Disposable vapes

그 외, DumpTOP SecOps-Pro 시험 문제집 일부가 지금은 무료입니다: https://drive.google.com/open?id=1QFDG1GCzJ9yuf_D-7oCdN96sktIXliCB