

# ***KillTest***

높은 품질, 더 나은 서비스



## 연습 문제

<https://www.killtest.kr>

1년간 무료 업데이트 제공

**Exam : CloudSec-Pro**

**Title : Palo Alto Networks Cloud  
Security Professional**

**Version : DEMO**

1.Which two actions should be implemented by a SOC manager to improve the efficiency of the team's incident response process? (Choose two.)

- A. Reduce the number of analysts on shift to minimize resource usage.
- B. Establish a clear incident response playbook for common security incidents.
- C. Implement regular training and simulation exercises.
- D. Upgrade the physical security of the facility.

**Answer: BC**

2.A company's SOC team and network security team operate independently but have a directive from the CISO to work more closely together due to issues resulting from a lack of cross-team collaboration. This often delays incident response, as analysts on both teams find themselves unknowingly working on the same alerts.

Which solution will improve security metrics and outcomes while aligning to the directive from the CISO?

- A. Implement network segmentation techniques combined with log analysis and periodic manual threat hunting
- B. Integrate automated threat intelligence
- C. Integrate and consolidate visibility and response capabilities across the company attack surface
- D. Implement a Unified Threat Management (UTM) system

**Answer: C**

3.In which two use cases is the use of SIEM more appropriate than the use of SOAR to investigate a user who logs in with a malicious IP address? (Choose two.)

- A. Using predefined rules and patterns to identify data points
- B. Enriching data and triaging alert information
- C. Continuously monitoring data for pattern recognition
- D. Mapping external threats to SOC incidents

**Answer: AC**

4.Which concept proactively enhances internal processes for incident response and management against known threats?

- A. Threat intelligence
- B. Security Information and Event Management (SIEM)
- C. User and Entity Behavior Analytics (UEBA)
- D. Endpoint detection and response (EDR)

**Answer: A**

5.Which action should be taken to investigate multiple log sources when researching a known threat by using threat intelligence?

- A. Build an XQL query using the Query Builder.
- B. O Identify characteristics used to create a behavioral indicator of compromise (BIOC) or correlation rule.
- C. Select an event of interest and open the Causality View.
- D. Review the sequence of events in the timeline.

**Answer: A**