

250-437^{Q&As}

Administration of Symantec CloudSOC - version 1

Pass Symantec 250-437 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/250-437.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Symantec
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1

How does the Audit module get data?

- A. Firewalls and proxies
- B. Cloud application APIs
- C. CloudSOC gateway
- D. Manual uploads

Correct Answer: A

QUESTION 2









What module should an administrator use to create policies with one click, and send them to the Protect Module?

- A. Detect
- B. Investigate
- C. Audit
- D. Securlet

Correct Answer: D

QUESTION 3

Refer to the exhibit. Which module(s) are utilized in the use case "Identify and understand how information is used within cloud applications"?

USE CASES		 Audit	 Detect	 Protect	 Investigate	 Securlets
 1) Cloud Visibility	1.1) Identify and determine business risk of cloud applications being used within the organization					
 2) Data Security	1.2) Determine optimal cloud application adoption based on business risk and cost of ownership.					
	2.2) Identify and understand how information is used within cloud applications					
 3) Threat Protection	2.3) Protect information from accidental and intentional exposure within cloud applications					
	3.1) Identify and remediate malicious behaviour within cloud applications					

- A. Investigate
- B. Securlets
- C. Protect, Investigate, and Securlets

D. Detect, Protect, and Investigate

Correct Answer: C

QUESTION 4

Which CloudSOC module should an administrator use to identify and determine business risk of cloud applications within an organization?

- A. Investigate
- B. Protect
- C. Audit
- D. Detect

Correct Answer: D

QUESTION 5

Refer to the exhibit. What action should an administrator take if this incident was found in the Investigate module?

Source Location	Sunnyvale (Unites States)
Name	vb_macro.xls
Referrer URI	https://drive.google.com/drive/my-drive
Request URI	https://doc-0c-ag-docs.googleusercontent.com/docs/securesc/0rm1j5aml20ffeu8...
Account Type	Internal
File Size	62.5KB
Risks	VBA Macros
Device	Mac OS X
Anonymous Proxy	false
City	Sunnyvale
Country	United States
Region	CA
Time Zone	America/Los_Angeles
User Agent	Mozilla/5.0.(Macintosh;Intel Mac OS X 10.12; rv 56.0) Gecko/20100101 Firefox/56.0
Transaction ID	8541da4a-9c30-414f-8c8a-75b54bdd19b1
Threat Prevention	VBA MACROS Matched Expressions (Suspicious-keywords) (Module1.bas::ActiveWorkbook.SaveAs (May save the current workbook)

- A. Create an access enforcement policy and block access to the file
- B. Create a file transfer policy and block the download of the file
- C. Create a file sharing policy and block the sharing of the file
- D. Create an access monitoring policy and monitor the usage of the file

Correct Answer: D

[250-437 PDF Dumps](#)

[250-437 Exam Questions](#)

[250-437 Braindumps](#)