

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

What policy should an administrator utilize to prevent users from downloading files from Box.com when they are outside the corporate IP range?

- A. File transfer
- B. File sharing
- C. Data exposure
- D. Access enforcement

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

An administrator discovers that an employee has been sending confidential documents to a competitor.

What type of policy should the administrator use to block the transmission of files to that domain?

- A. Access monitoring
- B. Data Exposure
- C. File transfer
- D. Access enforcement

Correct Answer: B

QUESTION 4

What Business Readiness Rating (BRR) category does the subcategory "Password Quality Rules" belong to?

- A. Data
- B. Compliance
- C. Business
- D. Access

Correct Answer: D

QUESTION 5

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 6

What policy should an administrator utilize to prevent users from internally sharing files with a group of high risk users?

- A. Access Monitoring
- B. File transfer
- C. Threatscore based
- D. Data exposure

Correct Answer: C

QUESTION 7

What should an administrator use to identify document types specified by the user?

- A. Custom dictionaries
- B. Training profiles
- C. Risk types
- D. Content types

Correct Answer: D

QUESTION 8

Which CloudSOC module(s) use cloud application APIs as data sources?

- A. Detect, Protect, Investigate, and Securllets
- B. Audit
- C. Detect, Protect, and Investigate
- D. Investigate and Securllets

Correct Answer: D

QUESTION 9

What CloudSOC module should an administrator use to prevent the accidental and intentional exposure of information within cloud applications?

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

Correct Answer: C

QUESTION 10

What module can an administrator use to connect certain cloud applications to CloudSOC via APIs, and have complete visibility into the content being shared in those cloud applications?

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

Correct Answer: D

QUESTION 11





What modules are used in the use case "Identify and remediate malicious behavior within cloud applications"?

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

Correct Answer: D

QUESTION 12

Refer to the exhibit. Which CloudSOC module(s) use firewalls and proxies as data sources?

Data sources	 Audit	 Detect	 Protect	 Investigate	 Securlets
Firewalls and proxies					
CloudSOC gateway					
Cloud application API					

- A. Detect, Protect, and Investigate
- B. Detect, Protect, Investigate, and Securlets
- C. Audit and Investigate
- D. Audit

Correct Answer: C

Reference: https://www.niwis.com/downloads/Symantec/Symantec_CloudSOC.pdf

QUESTION 13

What module should an administrator utilize to identify inherent risk in cloud applications?

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

D. Protect

Correct Answer: A

QUESTION 14

Which are three (3) levels of data exposure?

- A. Public, external, and internal
- B. Public, confidential, and company confidential
- C. Public, semi-private, and private
- D. Public, confidential, and private

Correct Answer: A

QUESTION 15

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

[Latest 250-437 Dumps](#)

[250-437 Practice Test](#)

[250-437 Braindumps](#)