



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.passapply.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 type of policy should an administrator utilize to prevent the spread of malware through cloud applications?

- A. Access monitoring
- B. File transfer
- C. File sharing
- D. Access enforcement

Correct Answer: A

QUESTION 2

How does the Detect module get data?

- A. Firewalls and proxies
- B. CloudSOC gateway and cloud application APIs
- C. Firewalls and proxies, and CloudSOC gateway
- D. Cloud application APIs

Correct Answer: C

QUESTION 3

Refer to the exhibit from the Investigate module. What type of policy should an administrator utilize to prevent users from accessing files using an unmanaged device?



DETAILS

Browser	Internet Explorer
Activity Type	Policy Alert
Longitude	73.866699
Latitude	18.533300
Source Location	Pune (India)
Request URI	https://docs.google.com/spreadsheets/u/0/d/1FAhdy1J9i0MyIRLFr1u-BBhNW-hWt...
Referrer URI	https://drive.google.com/drive/my-drive
Policy Type	File Transfer via Gatelets
File Size	14.4KB
Actions Taken	Block,
User Agent	Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko
Request Size	1570
Device	Windows 10.0
Country	India
City	Pune
Time Zone	Asia/Kolkata
Region	16
Anonymous Proxy	false
Account Type	Internal
Device Management Sta..	Unmanaged

- A. Access enforcement
- B. File sharing
- C. File transfer
- D. Device enforcement

Correct Answer: C

QUESTION 4

Where should an administrator locate unshared content within the Securlet module that contains risky information?

- A. Exposed content
- B. Activities
- C. Other Risks
- D. Apps

Correct Answer: B

QUESTION 5

What Rule Type in ContentIQ do movies, presentations, raster images, spreadsheets, word processors, and vector graphics belong to?

- A. Content format



- B. Content types
- C. Custom categories
- D. File format

Correct Answer: A

QUESTION 6

What is the objective of the Data Exposure policy?

- A. To notify an administrator when activities, such as objects being modified, are performed in a cloud application.
- B. To block users from logging into cloud applications if their ThreatScore is higher than a certain level.
- C. To restrict the direct sharing of documents from cloud applications based both on their content and the characteristics of the user.
- D. To notify the administrator, file owner or acting user and/or to prevent users from sharing documents, either publicly, externally, or internally.

Correct Answer: D

QUESTION 7

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 8

How does the Securlet module get data?

- A. Firewall and proxies
- B. CloudSOC gateway
- C. Cloud application APIs
- D. CloudSOC gateway and cloud application APIs

Correct Answer: D

QUESTION 9

What type of log upload should an administrator use during production?

- A. FTP
- B. Web upload
- C. SCP/SFTP
- D. APIs

Correct Answer: C

QUESTION 10

Where should an administrator locate the level of exposure in files in the Securlet module?

- A. Exposure level
- B. Exposed files
- C. Exposed content
- D. Exposure summary

Correct Answer: A

QUESTION 11

What module should an administrator utilize to view all the activities in cloud applications and conduct analysis?

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



Correct Answer: A

QUESTION 12

What Rule Type in ContentIQ profiles do FERPA, GLBA, HIPAA, PCI AND PII belong to?

- A. Regular expressions
- B. Content types
- C. Risk types
- D. Keywords

Correct Answer: B

Reference: <https://www.symantec.com/content/dam/symantec/docs/data-sheets/cloudsoc-security-forsaas-en.pdf>

QUESTION 13

What CloudSOC module should an administrator use to identify and understand how information is used within cloud applications?

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

Correct Answer: C

QUESTION 14

Which CloudSOC module is similar to an Intrusion Protection System (IPS)/Intrusion Detection System (IDS)?









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

Correct Answer: A

QUESTION 15



Refer to the exhibit. What modules are used in the use case "Protect information from accidental and intentional exposure 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					
	1.2) Determine optimal cloud application adoption based on business risk and cost of ownership.					
 2) Data Security	2.2) Identify and understand how information is used within cloud applications					
	2.3) Protect information from accidental and intentional exposure within cloud applications					
 3) Threat Protection	3.1) Identify and remediate malicious behaviour within cloud applications					

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

Correct Answer: A

[250-437 PDF Dumps](#)

[250-437 Exam Questions](#)

[250-437 Braindumps](#)