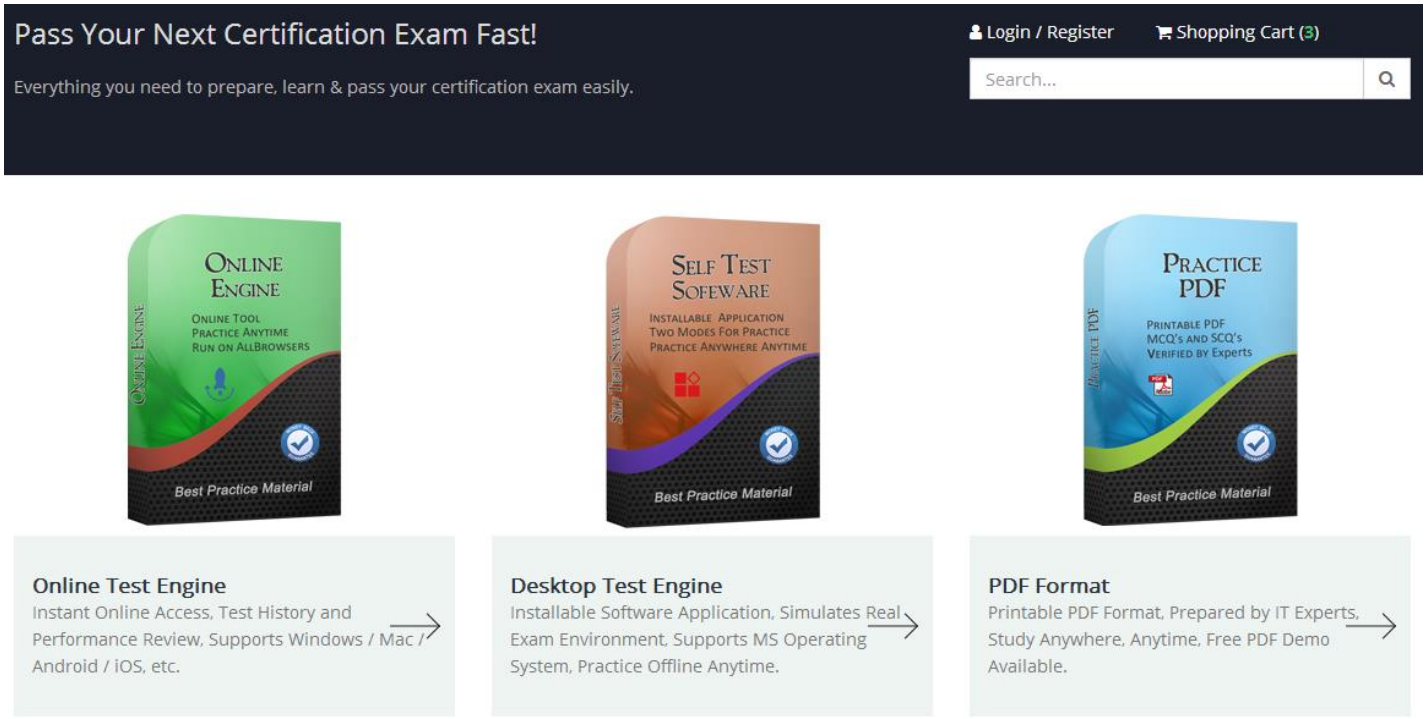
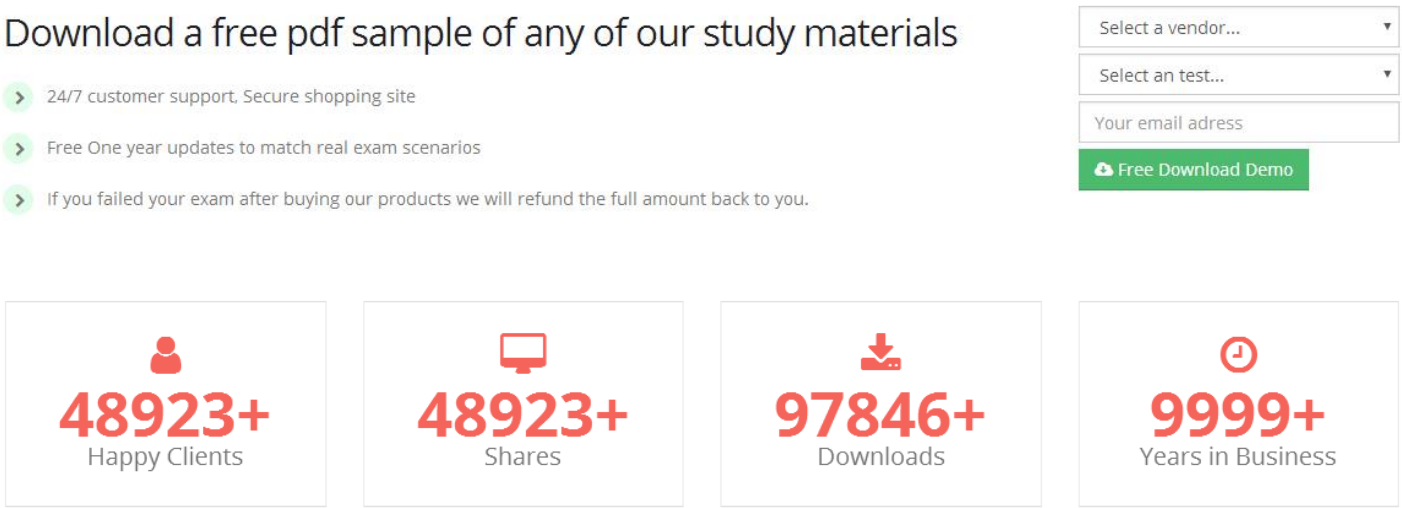
ExamcollectionPass





http://www.examcollectionpass.com/

Everything you need to prepare, learn & pass your certification exam easily.

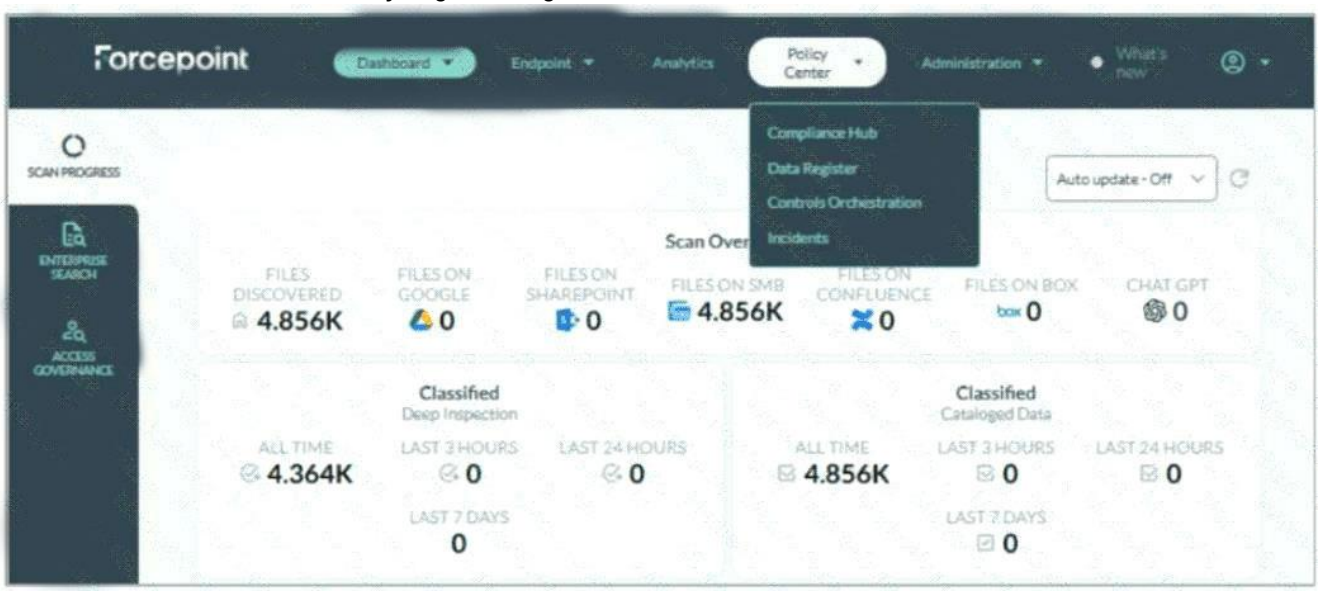
Exam : **DSPM-Deploy-and-Administer**

Title : Certified Forcepoint DSPM - Professional: Deploy and Administer Exam

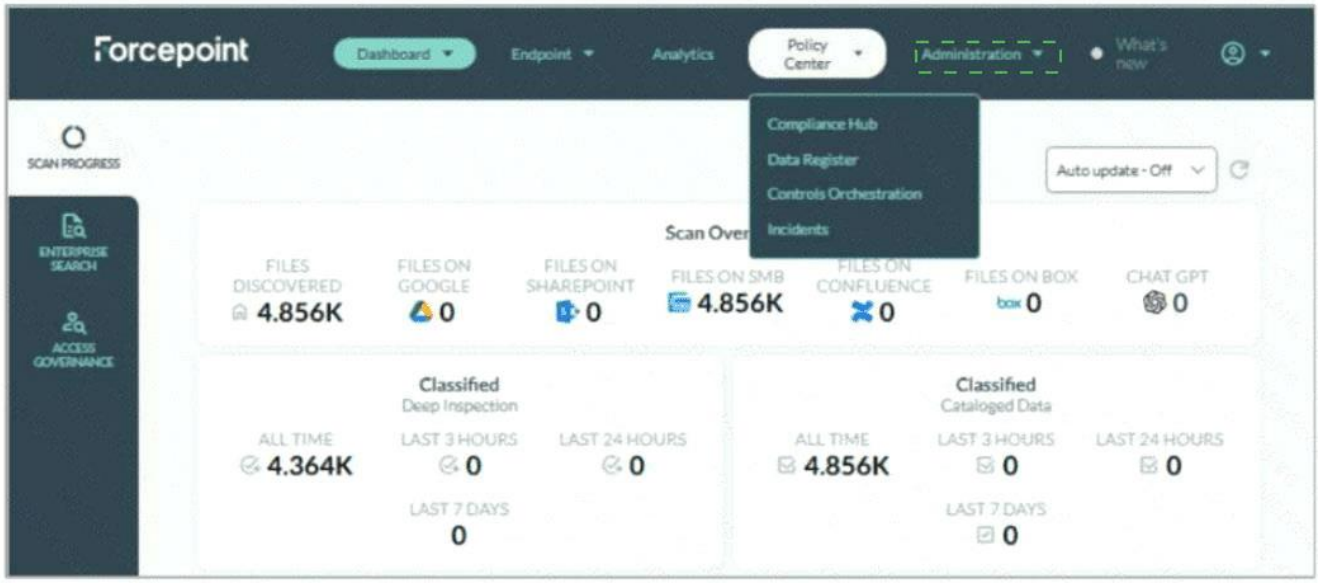
Vendor : Forcepoint

Version : DEMO

NO.1 Adam needs to update the taxonomy tags in Forcepoint DSPM to match his company's policies. Where on the UI are taxonomy tags managed?



Answer:



Explanation:
Administration > Taxonomy
Taxonomy tags are managed from the Administration menu, specifically under Administration > Taxonomy . In the screenshot, Adam should not select Policy Center ; the currently open menu shows Compliance Hub, Data Register, Controls Orchestration, and Incidents, but taxonomy management is not located there. The correct UI action is to open the Administration drop-down on the top navigation bar and select Taxonomy .
Forcepoint's DSPM documentation states that the Taxonomy page displays predefined AI Mesh tags, which cannot be removed, and also allows administrators to add custom tags for pattern matching and detection rules. It further explains that taxonomy mapping can connect AI Mesh tags with data-source taxonomies so mapped tags can be written back as the organization's own labels.
This location is important because taxonomy governs the classification language DSPM applies to scanned data. By updating taxonomy tags, Adam aligns DSPM classification output with the company's internal handling policies, sensitivity labels, and compliance terminology. Forcepoint also

notes that new taxonomy tags are created from the Taxonomy tab under the Administration section, and that applied tags are visible in the Data Asset Inventory. References/topics: Administration, Taxonomy, AI Mesh Tags, Classification Tags, Pattern Matching, Detection Rules .

NO.2 When Control Orchestration rules are triggered where can you find the events?

A. Default dashboards

B. Overviews

C. Incidents

D. Analytics

Answer: C

Explanation:

Triggered Controls Orchestration rule events are found under Incidents . In Forcepoint DSPM, Controls Orchestration rules are designed to identify data that requires attention by evaluating selected datasets, such as files, trustees, or agent activities, against rule conditions. When a rule condition is met, the result is operationalized as an incident so the security or governance team can review the matched data and determine the appropriate response.

Forcepoint's documentation states that each Controls Orchestration rule is "automatically added as a card in the Incidents tab," and selecting an incident card takes the administrator back to the related rule. It also explains that the Incidents section provides a top-down view of all orchestration rules and available match results. The documented navigation path is Policy Center > Incidents .

The other options are not the correct location for triggered orchestration events. Default dashboards and overviews provide summary visibility, but they are not the dedicated rule-event review workspace. Analytics supports broader investigation and reporting, but Controls Orchestration match results are reviewed through the Incidents workflow. References/topics: Policy Center, Controls Orchestration, Incidents, Rule Match Results, Enterprise Search Review .

NO.3 Which of the following are actions that can be performed from the Enterprise Search page? Select three.

A. Revoking user permissions.

B. Exporting reports.

C. Moving risky files to a private folder.

D. Manually changing the assigned risk.

E. Manually verifying ML classification.

Answer: A B E

Explanation:

The correct selections are Revoking user permissions , Exporting reports , and Manually verifying ML classification . The Enterprise Search page is the primary file-level investigation view in Forcepoint DSPM.

It lists scanned and cataloged files, allows filtering through standard filters or GQL, and provides operational actions against the returned results. Forcepoint states that Enterprise Search allows users to filter file data, save frequently used filters, customize columns, and generate meaningful reports. It also provides an EXPORT button that creates a CSV or JSON download of the filtered data.

Revoking permissions is also supported as a data-governance action. Forcepoint documents that administrators can view or modify file permissions and access rights from the file Actions menu, and supporting documentation identifies required permissions for revoke operations in Microsoft

repositories.
Manual classification validation is explicitly available from the Enterprise Search hamburger menu. Forcepoint states that to adjust a file's machine-learning classification, the user selects Manually verify classification , modifies the ML-suggested classification, and saves the change.
The incorrect choices are outside this specific Enterprise Search action set. Moving risky files to a private folder is not the standard named Enterprise Search action in this workflow, and assigned risk is not manually changed from the page. References/topics: Enterprise Search, Exporting Data, Permissions & Access Rights, Manual ML Classification Verification .

NO.4 Which of the following describes a use case for Forcepoint DSPM pattern matching?

A. Identifying personally identifiable information in Outlook and Gmail emails.

B. Identifying and redacting personally identifiable information on OneDrive.

C. Identifying personally identifiable information on SharePoint.

D. Identifying and encrypting personally identifiable information on Google Drive.

Answer: C

Explanation:
Forcepoint DSPM pattern matching is used to identify defined pieces of information inside scanned content by applying regular expressions. The documented function is discovery and classification: pattern matching identifies particular information in a document by using RegEx that attempts to match file content. This makes identifying personally identifiable information on SharePoint the correct use case. SharePoint is a supported Microsoft data source for scanning, and Forcepoint specifically documents SharePoint Online as a connector used to scan SharePoint accounts and apply classification tags to files containing sensitive data stored in SharePoint.
The key distinction is that pattern matching does not perform remediation actions such as redaction or encryption. Options B and D therefore overstate the capability: Forcepoint DSPM may discover and classify sensitive data that later informs controls, but the pattern itself is not a redaction or encryption engine. Option A is less precise in this context because the question is testing the canonical pattern-matching use case against scanned documents and repositories, while the strongest documented repository example among the choices is SharePoint. Pattern configuration can also assign classification, compliance, and distribution tags when a RegEx is detected, such as GDPR/PII tagging for identifiers. References/topics: Pattern Matching, RegEx, Compliance Tags, SharePoint Scanning, Sensitive Data Classification .