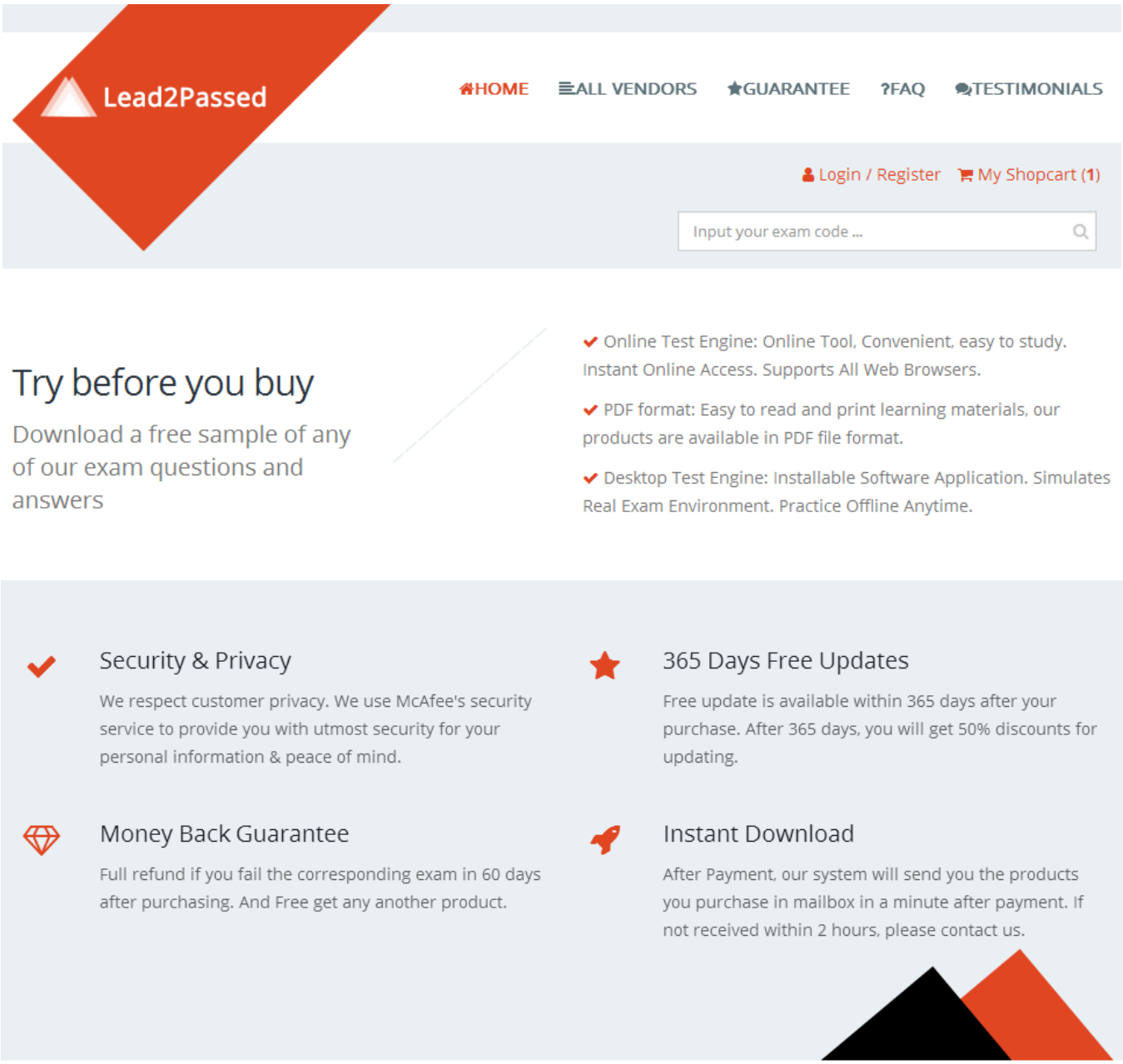
Lead2Passed



http://www.lead2passed.com

Valid Certification Exam Dumps Materials and Study Guide - Lead2Passed

Exam : **GCP-SOE-B**

Title : Security Operations Engineer (Beta)

Vendor : Google

Version : DEMO

NO.1 Your organization uses Google Security Operations (SecOps) for security analysis and investigation. Your organization has decided that all security cases related to Data Loss Prevention (DLP) events must be categorized with a defined root cause specific to one of five DLP event types when the case is closed in Google SecOps. How should you achieve this?

A. Customize the Close Case dialog and add the five DLP event types as root cause options.

B. Customize the Case Name format to include the DLP event type.

C. Create a Google SecOps SOAR playbook that automatically assigns case tags where each tag contains the unique definition of one of the five DLP event types.

D. Create case tags in Google SecOps SOAR where each tag contains a unique definition of each of the five DLP event types, and have analysts assign them to cases manually.

Answer: A

NO.2 You are a SOC manager at an organization that recently implemented Google Security Operations (SecOps). You need to monitor your organization's data ingestion health in Google SecOps. Data is ingested with Bindplane collection agents. You want to configure the following:
- Receive a notification when data sources go silent within 15 minutes.
- Visualize ingestion throughput and parsing errors. What should you do?

A. Configure notifications in Cloud Monitoring when ingestion sources become silent in Bindplane. Monitor and visualize Google SecOps data ingestion metrics using Bindplane Observability Pipeline (OP).

B. Configure silent source notifications for Google SecOps collection agents in Cloud Monitoring. Create a Cloud Monitoring dashboard to visualize data ingestion metrics.

C. Configure silent source alerts based on rule detections for anomalous data ingestion activity in Risk Analytics. Monitor and visualize the alert metrics in the Risk Analytics dashboard.

D. Configure automated scheduled delivery of an ingestion health report in the Data Ingestion and Health dashboard. Monitor and visualize data ingestion metrics in this dashboard.

Answer: B

NO.3 Your organization's Google Security Operations (SecOps) tenant is ingesting a vendor's firewall logs in its default JSON format using the Google-provided parser for that log. The vendor recently released a patch that introduces a new field and renames an existing field in the logs. The parser does not recognize these two fields and they remain available only in the raw logs, while the rest of the log is parsed normally. You need to resolve this logging issue as soon as possible while minimizing the overall change management impact. What should you do?

A. Use the web interface-based custom parser feature in Google SecOps to copy the parser, and modify it to map both fields to UDM.

B. Use the Extract Additional Fields tool in Google SecOps to convert the raw log entries to additional fields.

C. Deploy a third-party data pipeline management tool to ingest the logs, and transform the updated fields into fields supported by the default parser.

D. Write a code snippet, and deploy it in a parser extension to map both fields to UDM.

Answer: B

NO.4 Your organization is a Google Security Operations (SecOps) customer. The compliance team

requires a weekly export of case resolutions and SLA metrics of high and critical severity cases over the past week. The compliance team's post- processing scripts require this data to be formatted as tabular data in CSV files, zipped, and delivered to their email each Monday morning.
What should you do?

A. Use statistics in search, and configure a Google SecOps SOAR job to format and send the report.

B. Build a detection rule with outcomes, and configure a Google SecOps SOAR job to format and send the report.

C. Build an Advanced Report in SOAR Reports, and schedule delivery of the report.

D. Generate a report in SOAR Reports, and schedule delivery of the report.

Answer: A

NO.5 Your organization uses Google Security Operations (SecOps) for security analysis and investigation. Your organization has decided that all security cases related to Data Loss Prevention (DLP) events must be categorized with a defined root cause specific to one of five DLP event types when the case is closed in Google SecOps. How should you achieve this?

A. Customize the Case Name format to include the DLP event type.

B. Create a Google SecOps SOAR playbook that automatically assigns case tags where each tag contains the unique definition of one of the five DLP event types.

C. Customize the Close Case dialog and add the five DLP event types as root cause options.

D. Create case tags in Google SecOps SOAR where each tag contains a unique definition of each of the five DLP event types, and have analysts assign them to cases manually.

Answer: C

NO.6 You are threat hunting for an advanced threat group known for targeted, novel attacks by deploying campaign-specific infrastructure. You want to develop detections based on the threat group's behaviors so you can effectively detect whether the threat group has attacked your organization. What should you do?

A. Identify exposed technologies and products used by your organization, and develop detections to search for signs of exploitation.

B. Find intelligence reports in Google Threat Intelligence that relate to the threat actor, identify their behavior in previous campaigns, and use the past behavior to design detections in Google Security Operations (SecOps).

C. Search for the threat actor in Google Threat Intelligence, export the IOCs associated with the threat actor into a Google Security Operations (SecOps) list, and develop detections that reference this list.

D. Search for the threat actor in Google Threat Intelligence, review the threat actor's tactics, techniques, and procedures (TTPs), and design detections based on the TTPs in Google Security Operations (SecOps).

Answer: D

NO.7 Your organization recently implemented Google Security Operations (SecOps). You need to create a solution that allows the security team to monitor data ingestion into Google SecOps in real time. You also need to configure a solution that automatically sends a notification if one of the data sources stops ingesting dat a. You need to minimize the cost of these configurations.

What should you do?

A. Create Looker dashboards to visualize the data ingestion, and configure an alerting policy in Looker to send a notification in case of failure.

B. Create Looker dashboards to visualize the data ingestion, and configure an alerting policy in Cloud Monitoring to send a notification in case of failure.

C. Use Google SecOps SIEM dashboards to visualize the data ingestion and configure an alerting policy in Cloud Logging to send a notification in case of failure.

D. Use Google SecOps SIEM dashboards to visualize the data ingestion, and configure an alerting policy in Cloud Monitoring to send a notification in case of failure.

Answer: D

NO.8 You are a senior SOC analyst in your organization. You are receiving alerts of traffic to a command and control (C2) IP address. You want to use Google Security Operations (SecOps) to investigate the IP address associated with the C2 IP address. What should you do?

A. Use Google SecOps SOAR Search to run a playbook designed to investigate the suspicious IP address and identify related outbound and inbound traffic.

B. Use Google SecOps SOAR Search to identify the cases where the suspicious IP address exists.

C. Conduct a Google SecOps SIEM Search that uses src.ip and target.ip to identify outbound and inbound traffic associated with the suspicious IP address.

D. Use Google SecOps SIEM Search to query against the grouped ip field, and use the enriched field from the suspicious events to identify related activity.

Answer: C

NO.9 Which approach BEST improves detection of compromised service accounts in Google Cloud?

A. Monitoring VM uptime

B. Alerting on login failures only

C. Baseline service account behavior and alert on deviations

D. Disabling all service accounts You are managing the integration of Security Command Center (SCC) with downstream tooling.

Answer: C