Technical Exercise for Cortex Partner SA

Objective

The objective of this exercise is to evaluate your ability to integrate and utilize Palo Alto Networks' Cortex XSIAM platform. You will be tasked with pulling alerts from Cortex XSIAM and storing them in a cloud storage bucket. You will then present your approach, the API endpoints used, and any observations about the alert schema or Cortex XSIAM in general.

Exercise Instructions

Prerequisites

1. Access to a Cortex XSIAM instance.
2. Access to a cloud storage service (e.g., AWS S3, Google Cloud Storage, Azure Blob Storage).
3. Basic understanding of RESTful APIs and cloud storage services.
4. Programming environment set up to make API calls (e.g., Curl, Python, Postman).

Task Overview

1. **Authenticate with Cortex XSIAM API**: Obtain the necessary credentials and authenticate with the Cortex XSIAM API.
2. **Pull Alerts from Cortex XSIAM**: Use the appropriate API endpoints to pull alerts from Cortex XSIAM.
3. **Store Alerts in Cloud Storage**: Store the retrieved alerts in a cloud storage bucket.
4. **Presentation**: Prepare a presentation detailing your approach, the API endpoints used, and any observations about the alert schema or Cortex XSIAM in general.

Detailed Steps

Step 1: Authenticate with Cortex XSIAM API

- Obtain the API key or OAuth token required to authenticate with the Cortex XSIAM API.
- Use the authentication endpoint to obtain an access token if necessary.
- Document the authentication process and any challenges faced.

Step 2: Pull Alerts from Cortex XSIAM

- Identify the API endpoint(s) used to retrieve alerts from Cortex XSIAM. Typically, this might be an endpoint like `/alerts`.
- Make API calls to pull alerts data. Ensure you handle pagination if the number of alerts is large.

- Document the API endpoints used, the request parameters, and the response structure.

Step 3: Store Alerts in Cloud Storage

- Choose a cloud storage service (e.g., AWS S3, Google Cloud Storage, Azure Blob Storage).
- Write a script or use a tool to upload the retrieved alerts to the cloud storage bucket.
- Ensure the alerts are stored in a structured format (e.g., JSON, CSV).
- Document the process of storing alerts, including any code snippets or tools used.

Step 4: Presentation

- Prepare a presentation (e.g., PowerPoint, Google Slides) that includes the following:
    - **Introduction**: Brief overview of the task and its objectives.
    - **API Endpoints**: List and describe the API endpoints used.
    - **Alert Schema**: Discuss the structure of the alert data, including any notable fields or observations.
    - **Cloud Storage**: Explain how the alerts were stored in the cloud storage bucket, including any code snippets or tools used.
    - **Challenges and Observations**: Highlight any challenges faced during the exercise and any observations about Cortex XSIAM or the alert schema.

Submission

- Be prepared to present the following during the technical interview:
    - The script or code used to pull alerts and store them in the cloud storage bucket.
    - The presentation detailing your approach and findings.
    - Any additional documentation or notes that support your work.

Evaluation Criteria

- **Technical Accuracy**: Correct use of API endpoints and cloud storage services.
- **Completeness**: All steps of the exercise are completed and documented.
- **Clarity**: Clear and concise presentation of the approach and findings.
- **Problem-Solving**: Ability to handle challenges and provide solutions.
- **Observations**: Insightful observations about the alert schema and Cortex XSIAM.

Good luck, and we look forward to your presentation!