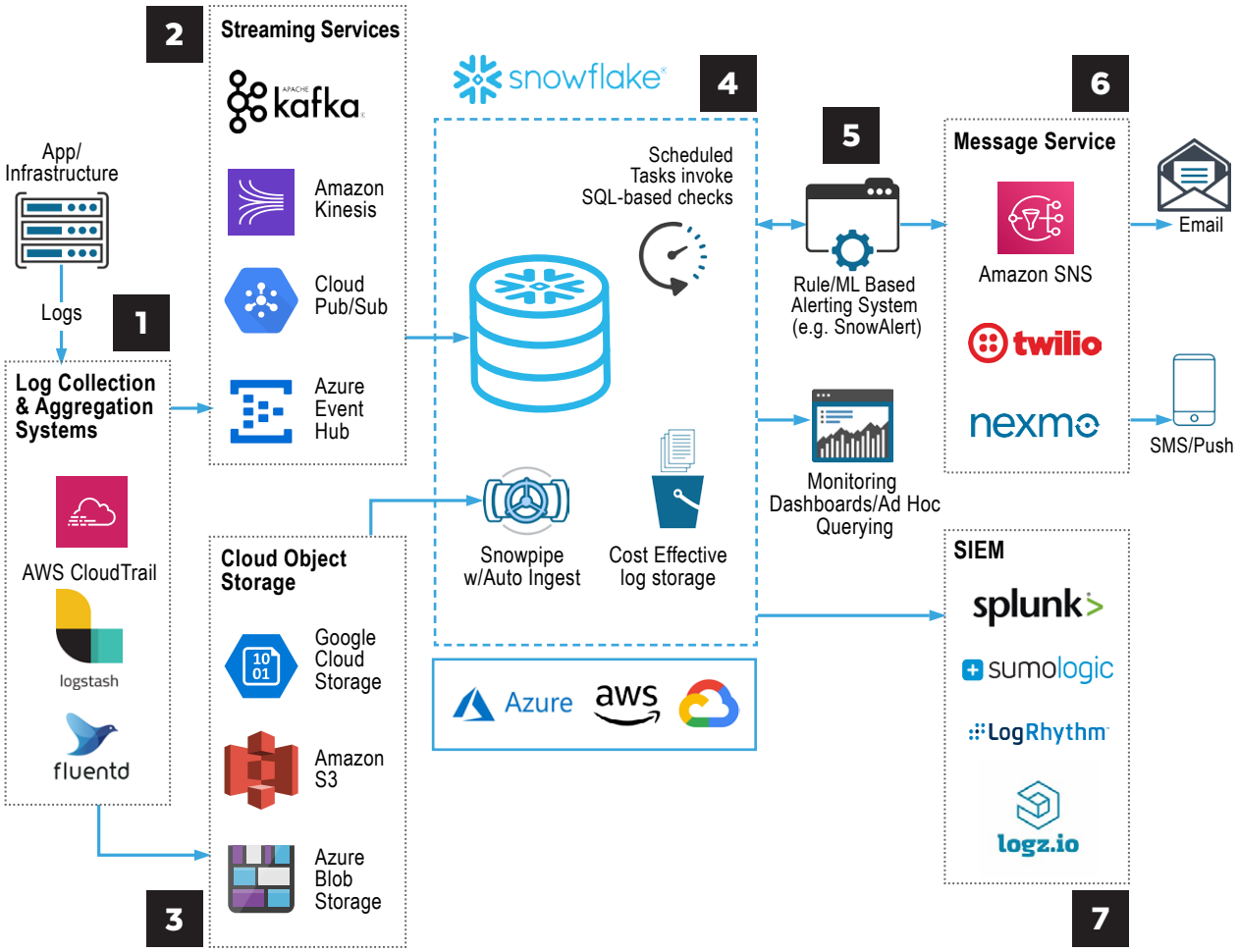
APPLICATION HEALTH AND SECURITY ANALYTICS REFERENCE ARCHITECTURE

APPLICATION HEALTH AND SECURITY ANALYTICS



OBJECTIVE

Analyze large volumes of log data to identify security threats and monitor application health.

DESCRIPTION

1. The application and its infrastructure log large volumes of event data that can be used to monitor application health and detect malicious behavior. Log collection and aggregation systems centralize log data from multiple sources and deliver it to a streaming service (2) or to cloud object storage (3).
2. The streaming service buffers log data to ensure reliable and continuous ingestion.
3. Depending on which log collector and aggregation system is used, data can be staged in cloud object storage without the need for a streaming service.
4. Snowflake stores and analyzes the log data, which can be saved for long periods at commodity storage prices. Snowpipe with Auto-Ingest automates the ingestion from cloud object storage. Scheduled tasks invoke SQL-based queries to detect suspicious behavior or application health concerns.
5. External rule-based alerting systems, such as SnowAlert, can detect suspicious activity or health concerns. Operations teams can monitor the application via dashboards or ad hoc queries.
6. A messaging service uses email, SMS, or push notifications to notify operations teams of events that require attention.
7. SIEM systems can leverage data in Snowflake for advanced searching and alerting capabilities.