



Centralizing Cloud Logs and Events with Microsoft Sentinel

**SANS Webcast - Wednesday May 29th
Eric Johnson & David Hazar**

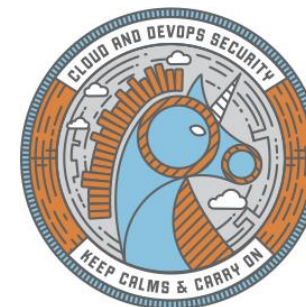
Agenda

- 1 Introductions
- 2 Intra-Cloud Log Aggregation
- 3 Cross-Cloud Data Transfer Patterns
- 4 Microsoft Sentinel
- 5 Conclusions

\$ aws sts get-caller-identity

Eric Johnson

- Principal Security Engineer, Puma Security
 - Coder: cloud infrastructure automation, CI / CD orchestration, cloud architecture, security tool automation
 - Security assessments: cloud, dev/sec/ops, source code, web apps, mobile apps
- Senior Instructor, SANS Institute
 - Contributing author of SEC540, SEC510, SEC549
- Community, Training, Education
 - AWS Community Builder, GPCS, GSSP, GWAPT, AWS Dev, CISSP
 - Iowa State M.S. Information Assurance, B.S. Computer Engineering
- Contact information
 - LinkedIn: <https://www.linkedin.com/in/eric-m-johnson/>
 - Email: ejohnson@pumasecurity.io



<https://graph.microsoft.com/v1.0/me>

David Hazar

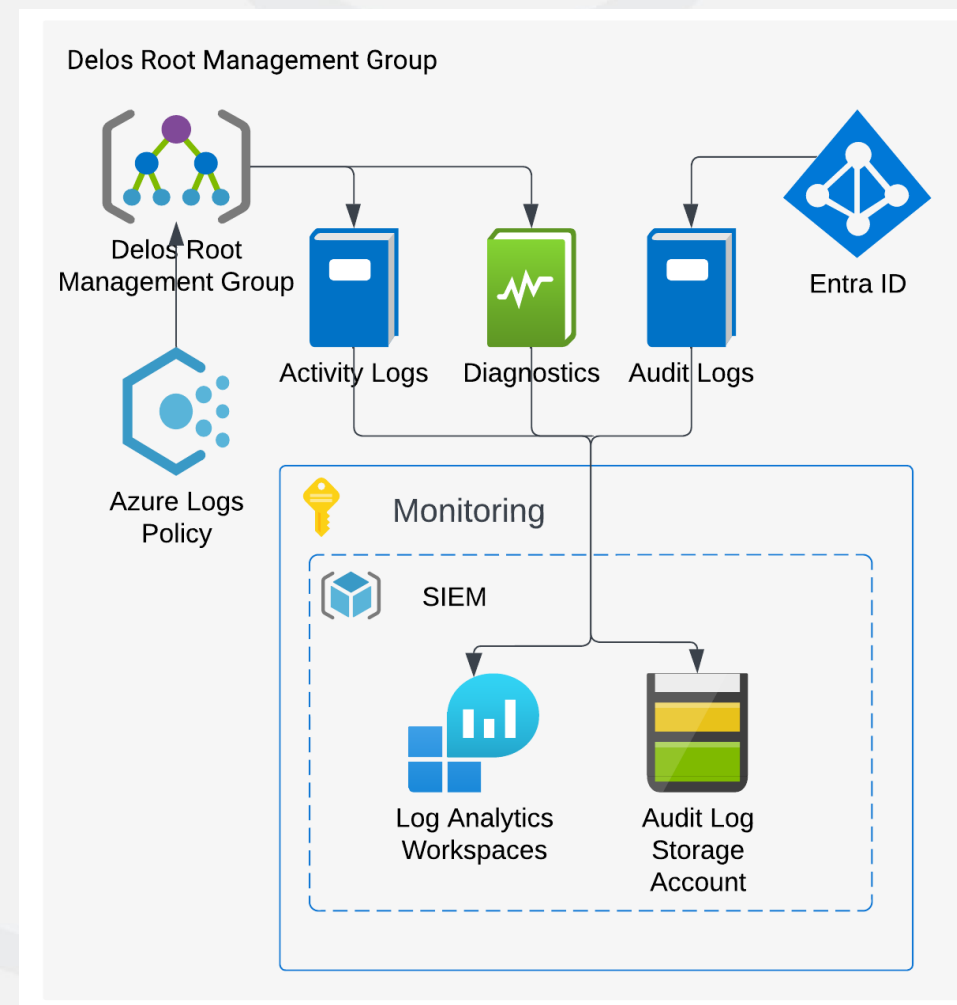
- Owner, HazardSec LLC
 - Cybersecurity consulting
- Co-Founder, CISO, Next Level3
 - Just-in-Time Access and Authorization
- Certified Instructor, SANS Institute
 - Co-author of SEC549: Cloud Security Architecture & MGT516: Building & Leading Vulnerability Management Programs
 - Instructor for SEC540: Cloud Security & DevSecOps Automation
- IANS Faculty Member
- Contact information
 - LinkedIn: <https://www.linkedin.com/in/DavidHazar>
 - Email: david@hazardsec.com



Intra-Cloud Log Aggregation

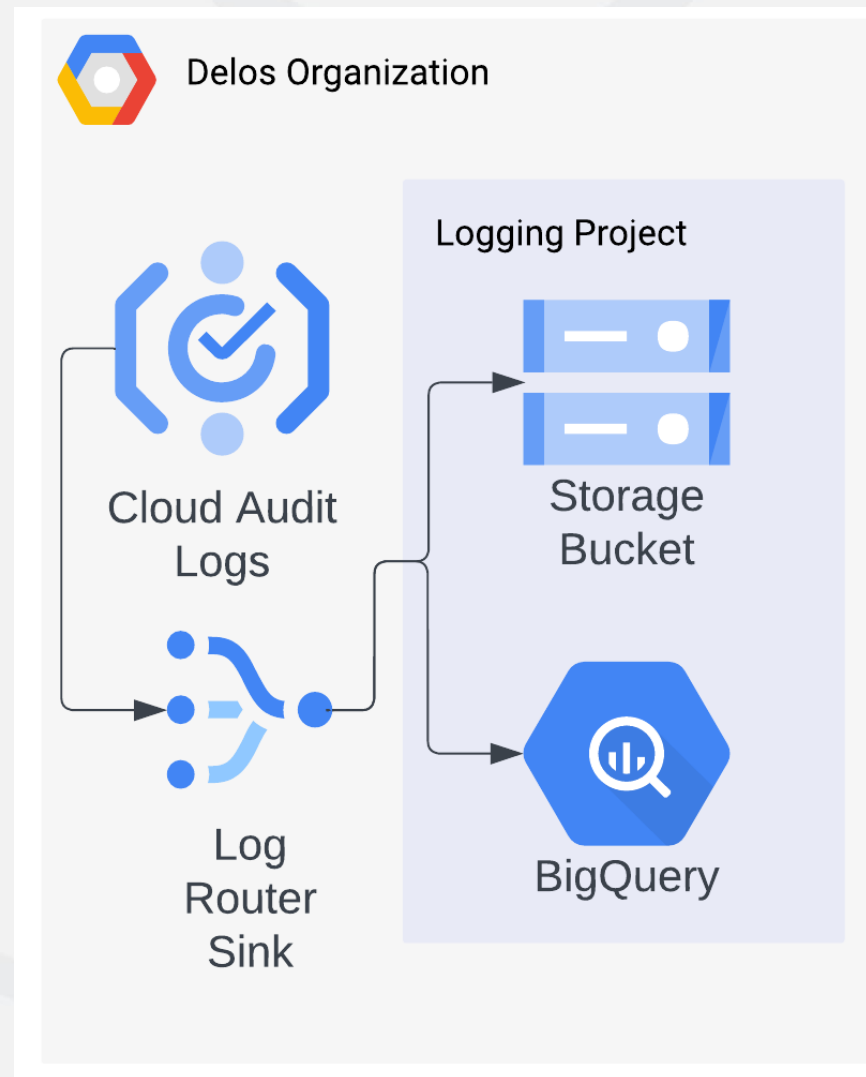
Azure: Centralized Logging Pattern

- Assign audit logging Azure Policy to the root management group:
 - New subscriptions and resources will automatically route log data to the central monitoring storage account / log analytics workspace
 - Existing subscriptions are marked "out of compliance" and fixed using a remediation task
- Create an Entra ID diagnostic setting to send audit and sign in logs to the monitoring subscription



Google Cloud: Centralized Logging Pattern

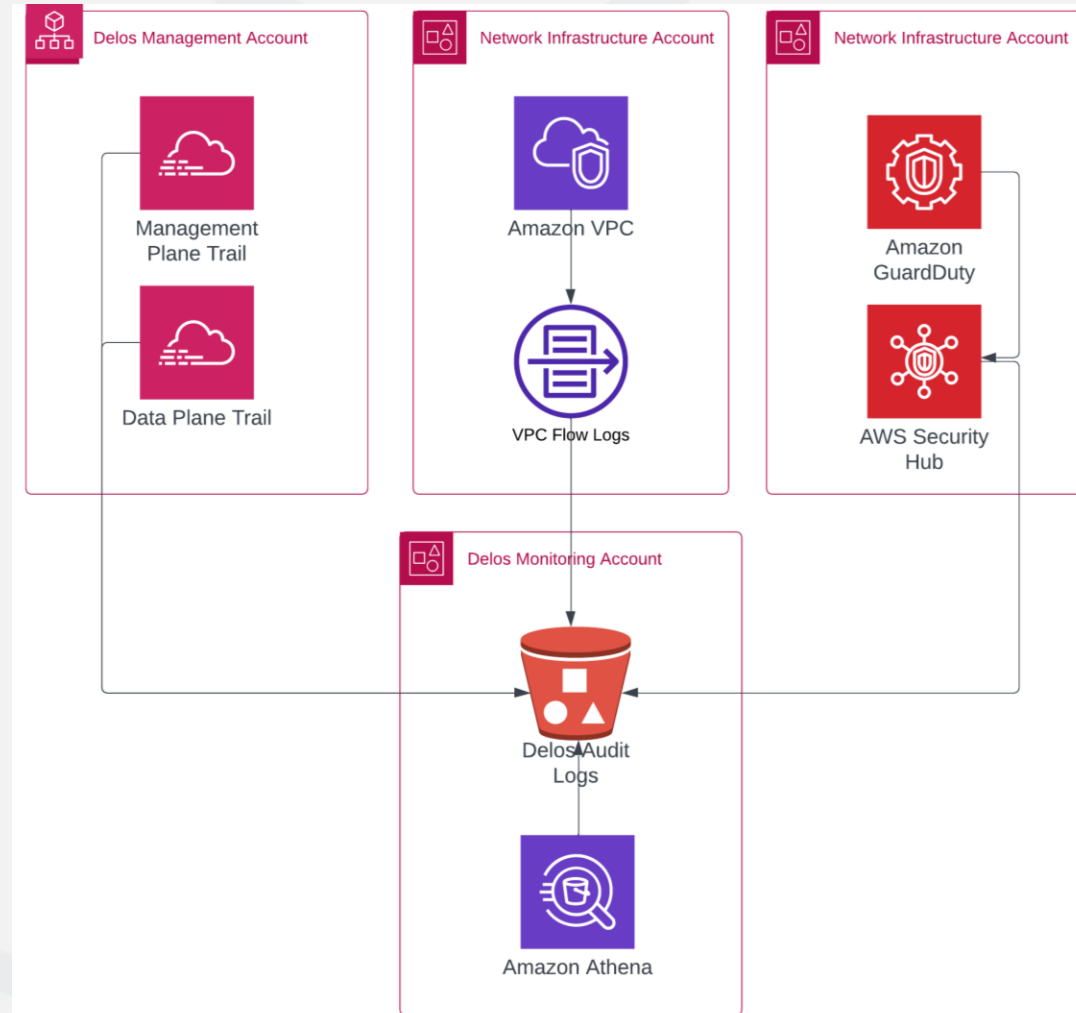
- Cloud audit logging captures admin activity logs by default
- Data plane audit logs are not enabled by default and must be enabled for each service
- Log router sinks can send log data from the organization's logging service to centralized storage, BigQuery, or Pub/Sub topics



AWS: Centralized Logging Pattern

Centralizing log data in AWS is more complicated with cross-account S3 access required for:

- CloudTrail management and data plane trails
- VPC network flow logs
- Delegated Security Hub account findings from compliance, threat intelligence, and third-party scans.
- Delegated GuardDuty / Inspector findings



Demo: Intra-Cloud Data Aggregation

The screenshot displays the Google Cloud Logging interface. At the top, the Google Cloud logo and 'Logging' filter are visible. The search bar contains 'cloud logging'. The main area shows the 'Logs Explorer' with a 'Query' tab selected. The query time range is '1:46:18 PM - 2:46:18 PM'. The interface includes options for 'Log fields' and 'Timeline', both of which are checked. A 'Log fields' sidebar on the left lists resource types: GCS Bucket (71), Audited Resource (64), Cloud Pub/Sub Subscription (12), Google Project (9), Produced API (3), and Service Account (1). The main timeline view shows a horizontal axis with a blue bar representing the query period. Below the timeline, there are 160 results. The results table has columns for SEVERITY, TIME, and SUMMARY. The first three results are audit_log entries from the 'google.pubsub.v1.Subscriber.GetSubscription' method, all with a severity of 'Info' and a principal_email of 'sentinel-connector@logging-177962.iam.gserviceaccount.com'.

Google Cloud Logging interface showing a query for 'cloud logging' with a timeline view and log results.

Log fields: Log fields Timeline

Log fields sidebar:

- RESOURCE TYPE
- GCS Bucket: 71
- Audited Resource: 64
- Cloud Pub/Sub Subscription: 12
- Google Project: 9
- Produced API: 3
- Service Account: 1
- SEVERITY

Timeline view showing results for May 28, 2024, from 1:46 PM to 2:47 PM.

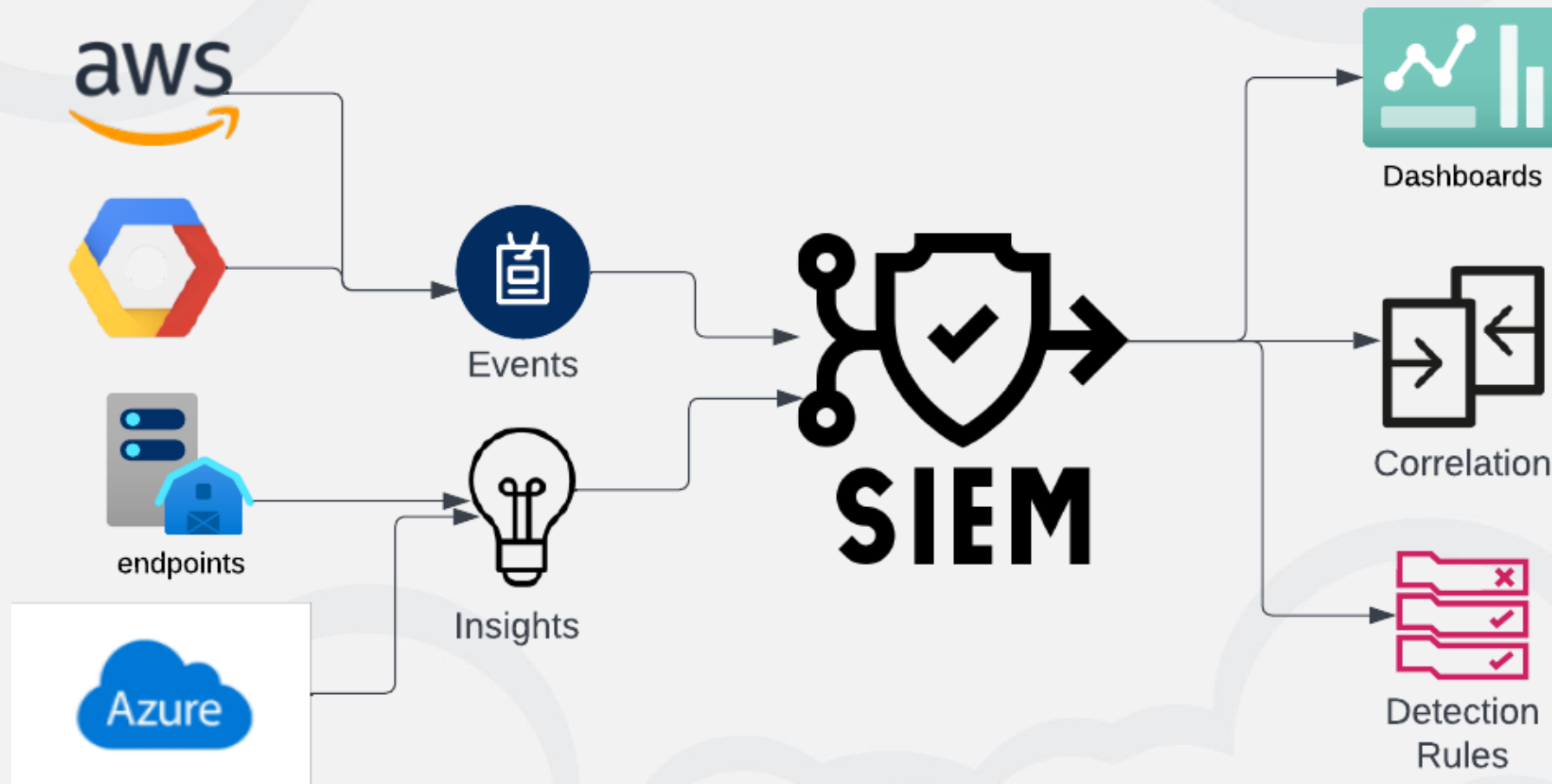
160 results

SEVERITY	TIME	SUMMARY
Info	13:47:35.362	audit_log, method: "google.pubsub.v1.Subscriber.GetSubscription", principal_email: "sentinel-connector@logging-177962.iam.gserviceaccount.com"
Info	13:52:36.287	audit_log, method: "google.pubsub.v1.Subscriber.GetSubscription", principal_email: "sentinel-connector@logging-177962.iam.gserviceaccount.com"
Info	13:57:37.469	audit_log, method: "google.pubsub.v1.Subscriber.GetSubscription", principal_email: "sentinel-connector@logging-177962.iam.gserviceaccount.com"



Cross-Cloud Log Aggregation

Centralizing High Value Cloud Log Sources



Data Transfer Patterns

Two design patterns are often used for migrating cloud data:

Push Architecture

- Supports real-time data streaming and event-driven systems
- Minimizes latency and deliver data is delivered as soon as it is ready
- Requires less noise as the receiver does not need to poll for new data
- Higher complexity managing connections and delivery formats

Pull Architecture

- Supports systems that do not need real-time delivery using periodic updates
- Allows the receiver to control how often data is pulled into the designation
- Increases overhead for the sender and can introduce latency receiving the data
- Lower complexity with a simpler implementation

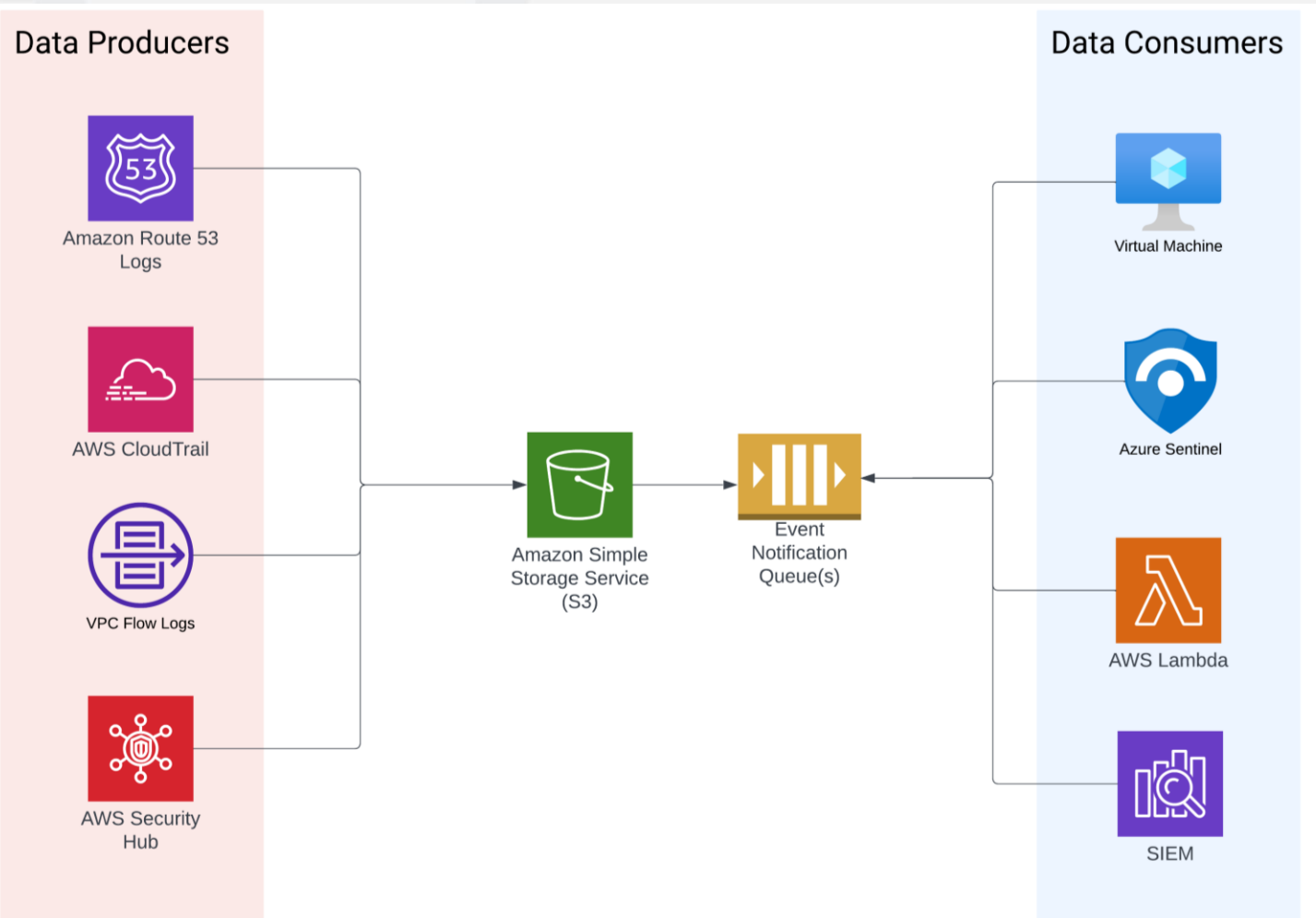


AWS: Kinesis Log Export Pattern



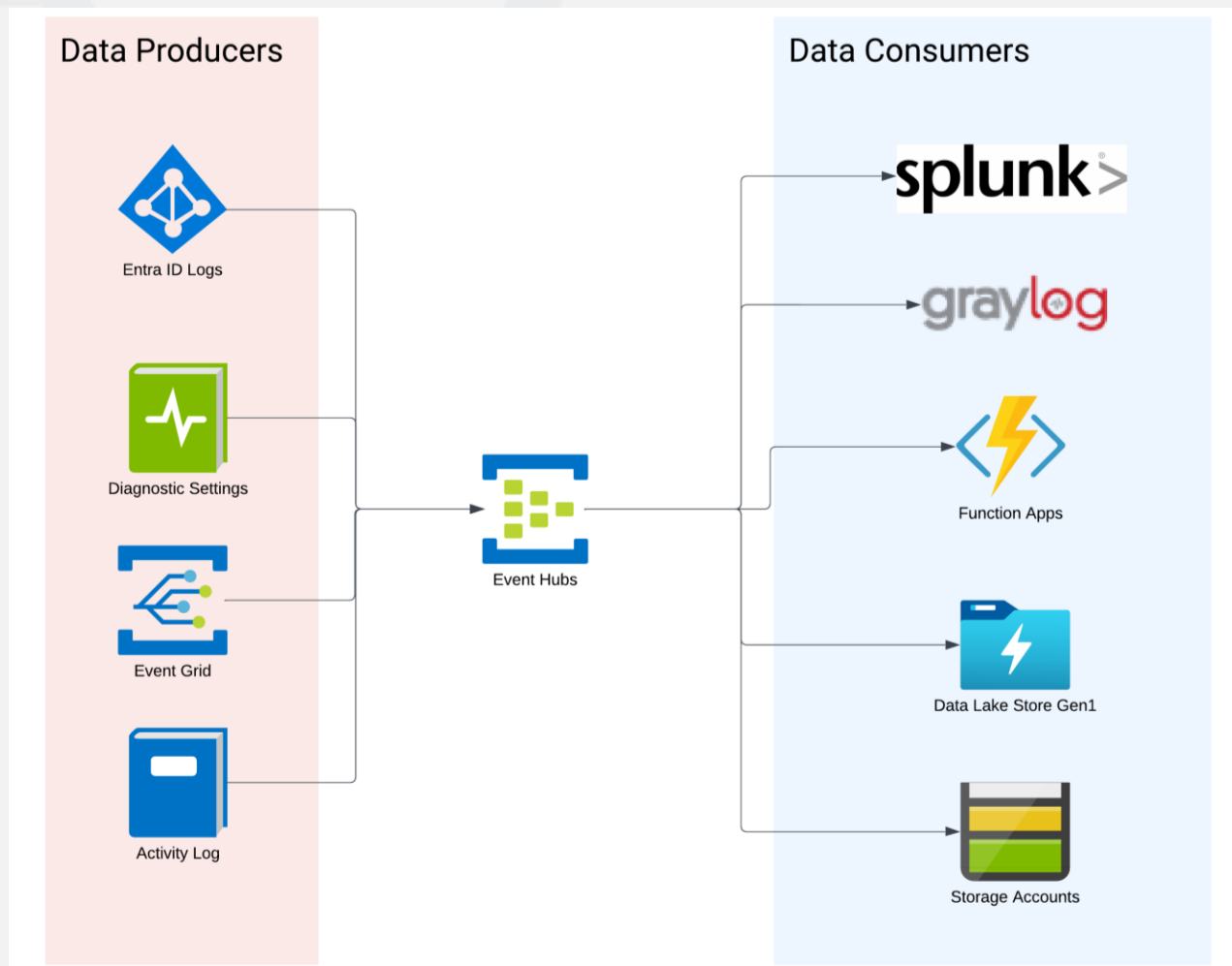
- **Kinesis Firehose** uses a push pattern to stream from data producers to data consumers in near real time.
- **Kinesis Data Streams** stores and shards data and makes available to consumers using a pull pattern.

AWS: S3 / SQS Log Export Pattern



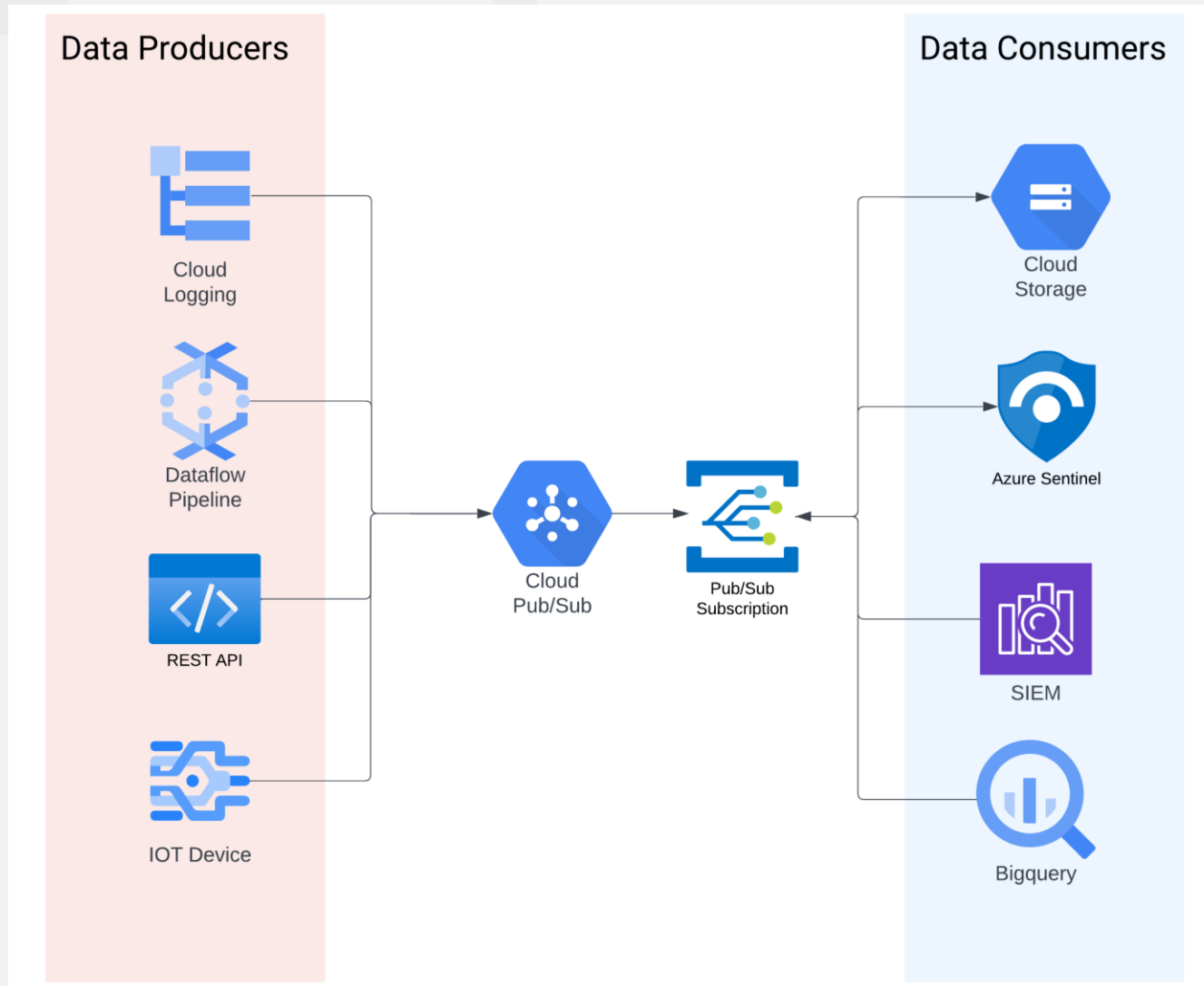
- **Data Producers** write log data into a central S3 bucket with event notifications sending messages to an SQS queue.
- **Data Consumers** poll the queue(s) for new messages and then pull the new log objects from the S3 bucket.

Azure: Event Hub Log Export Pattern



- **Data Producers** inside the root management group send events and log data to the **Azure Event Hub**.
- **Data Consumers** subscribed to the Event Hub **receive** data over the Advanced Message Queuing Protocol (AMQP).

Google Cloud: Pub/Sub Log Export Pattern



- **Data Producers** write data into a Google Cloud Pub/Sub topic.
- **Data Consumers** subscribe to the Pub/Sub topic using either a push or a pull architecture to process messages as they become available.

Demo: Cross-Cloud Data Aggregation

[Option+S]



N. Virginia ▾

AWSReadOnlyAccess/student@delos-international-managem

Event notifications (2)

Edit

Delete

Create event notification

Send a notification when specific events occur in your bucket. [Learn more](#)

<input type="checkbox"/>	Name ▲	Event types	Filters	Destination type	Destination
<input type="checkbox"/>	tf-s3-queue-20240304183305229900000001	All object create events	CloudTrail/AWSLogs/, .json.gz	SQS queue	sentinel-cloudtrail-sqs
<input type="checkbox"/>	tf-s3-queue-20240304183305229900000002	All object create events	VPCFlow/AWSLogs/, .log.gz	SQS queue	sentinel-vpcflowlogs-s



Microsoft Sentinel

Cloud Provider SIEM Services

Cloud providers also offer SIEM platforms for customers:

AWS: Security Lake / Glue/ Lambda / S3

- No one offering that could be called a cloud-native SIEM and SOAR.
- Instead, AWS has taken the microservices approach of providing the various capabilities of a SIEM (data storage, analytics, ingestion).

Azure: Sentinel

- Cloud-Native SIEM and SOAR
- Direct Competitor to Google Cloud Chronicle
- Natively stream security alerts from Microsoft Defender for Cloud into Microsoft Sentinel

GCP: Chronicle

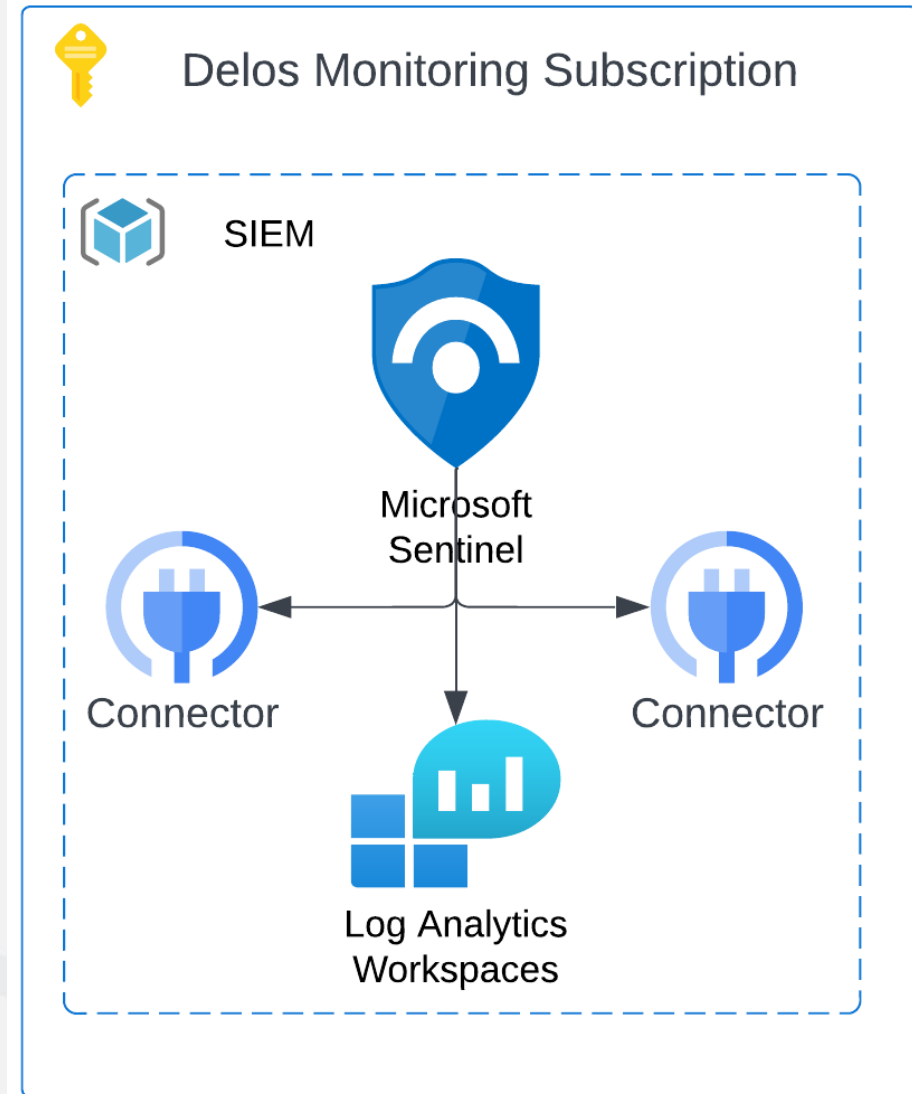
- Cloud-Native SIEM and SOAR
- Native analytics tools such as Looker
- Direct competitor to Azure Sentinel



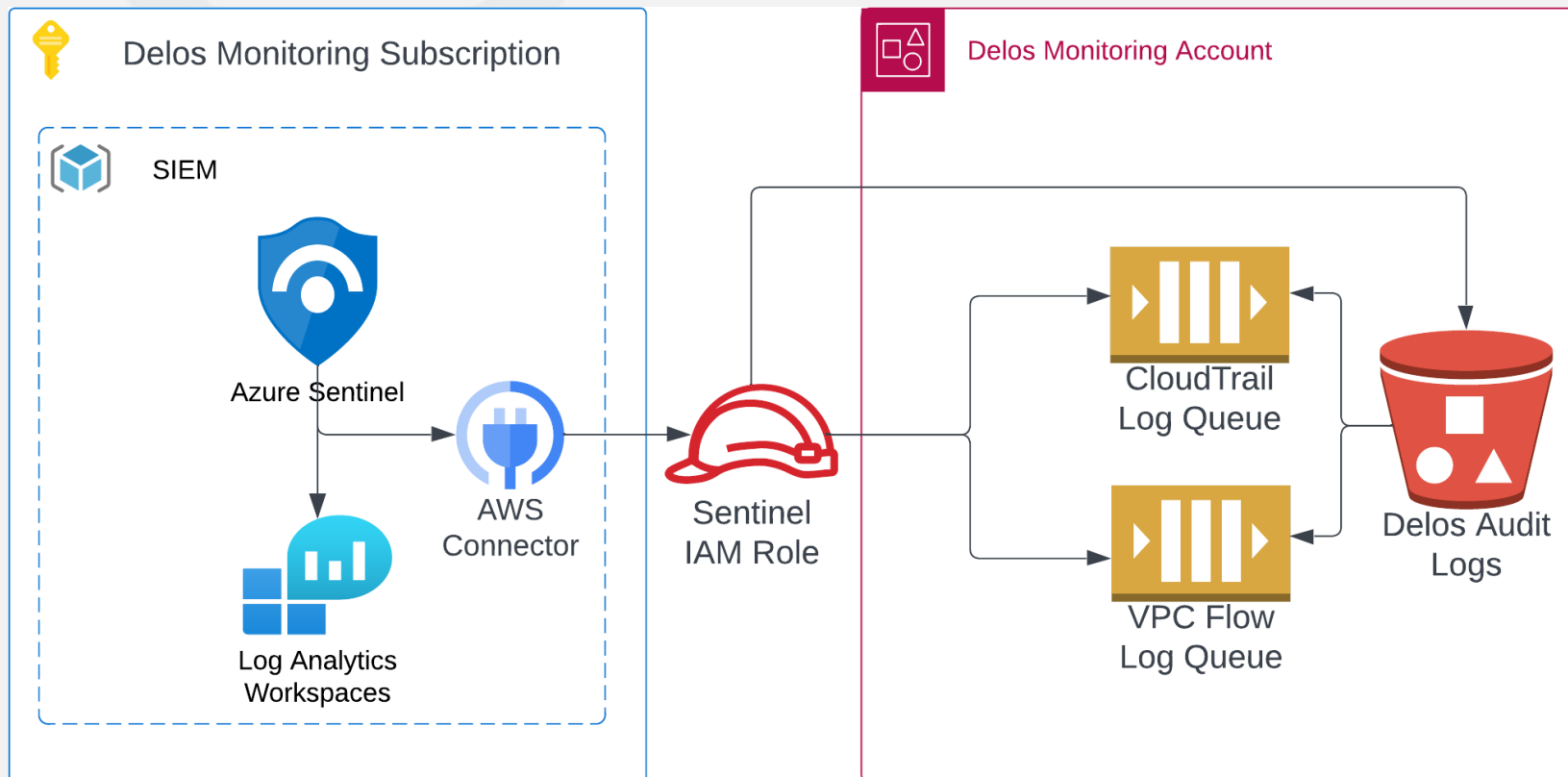
Microsoft Sentinel SIEM / SOAR Platform

Microsoft Sentinel provides a managed platform for cross-cloud and hybrid security analytics and threat intelligence:

- Extends the capabilities of the centralized log analytics workspace
- Data connectors ingest data from various sources (Entra ID, Defender for Cloud, AWS, Google Cloud, etc.)
- Discovers threats using behavior analysis, threat intelligence feeds, and predefined / custom queries
- Manages incident lifecycle for alerts, triage, response, and resolution



Microsoft Sentinel: Ingesting AWS Logs with SQS and S3



- **AWS monitoring account resources:**

- Create a queue for each log type
- Configure an S3 event notification per log type prefix
- Create an IAM Role that trusts the Sentinel tenant and workspace id

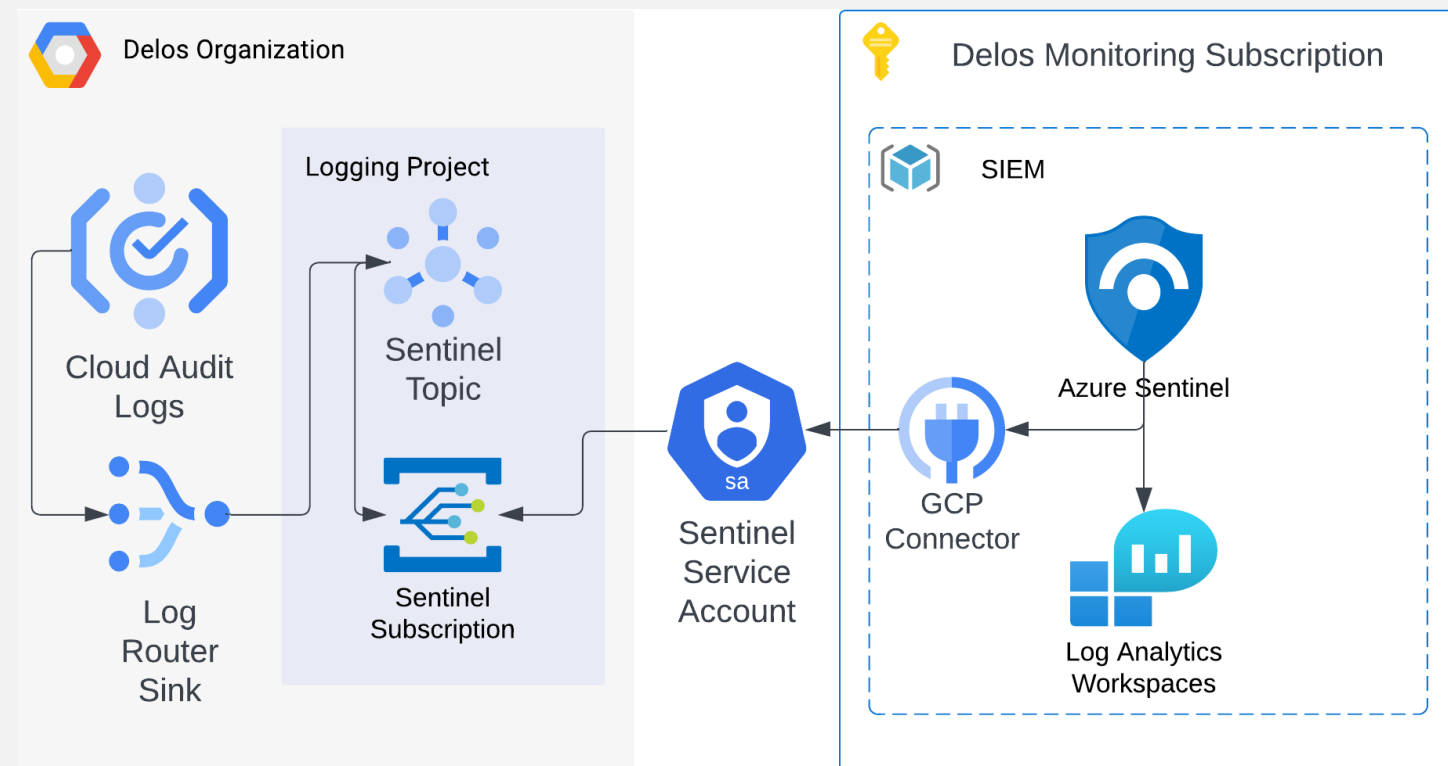
- **Sentinel workspace resources:**

- Data connector for each log type assumes the IAM role and checks the queue
- Pulls new objects from the audit log bucket into the Sentinel workspace

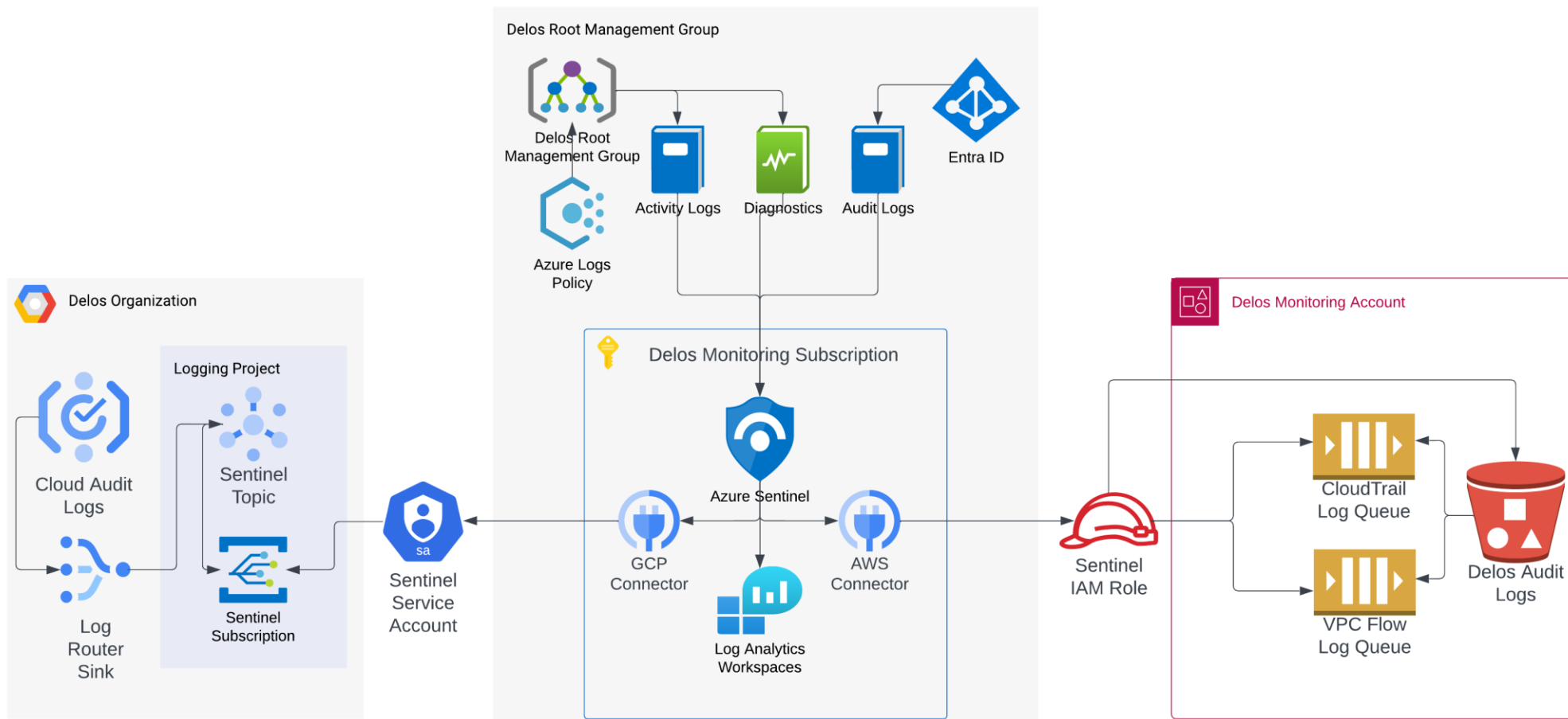


Microsoft Sentinel: Ingesting Google Cloud Logs

- **Google Cloud monitoring project account resources:**
 - Create a cloud logging sink for audit logs to stream to a Pub/Sub topic
 - Create a Pub/Sub pull subscription for the Sentinel workspace
 - Create a service account that trusts the Sentinel tenant and workspace with permission to get subscription messages
- **Sentinel workspace resources:**
 - Data connector for cloud audit logs impersonates the service account
 - Reads messages from the Pub/Sub topic's subscription



Microsoft Sentinel Centralized SIEM Architecture



Demo: Microsoft Sentinel

The screenshot displays the Microsoft Sentinel Logs interface. At the top, it shows the workspace name 'delos-central-analytics-workspace' and a query editor with the query 'GCPAuditLogs | take 5'. The time range is set to 'Last 24 hours'. Below the query editor, there are navigation options for 'Tables', 'Queries', and 'Functions'. A search bar and filter options are also visible. The main area shows a table of results with columns for 'TimeGenerated [UTC]', 'ServiceName', 'MethodName', and 'GCPResource'. The results list several log entries from May 28, 2024, involving Google Cloud Pub/Sub and Asset Service.

Microsoft Sentinel | Logs ...
Selected workspace: 'delos-central-analytics-workspace'

New Query 1* x + Feedback Queries

delos-central-analytics-workspace Run Time range: Last 24 hours Save Share New alert rule Export

Tables Queries Functions ... <<

Search

Filter Group by: Solution

Collapse all

Favorites

You can add favorites by clicking on the ☆ icon

- LogManagement
- Microsoft Sentinel
 - Anomalies
 - AWSCloudTrail
 - AWSVPCFlow
 - GCPAuditLogs
 - SecurityAlert
- Microsoft Sentinel UEBA
 - BehaviorAnalytics

Results Chart Add bookmark

<input type="checkbox"/>	TimeGenerated [UTC] ↑↓	ServiceName	MethodName	GCPResource
<input type="checkbox"/>	> 5/28/2024, 8:07:37.111 PM	pubsub.googleapis.com	google.pubsub.v1.Subscriber.GetSubscription	projects/log
<input type="checkbox"/>	> 5/28/2024, 8:02:33.015 PM	pubsub.googleapis.com	google.pubsub.v1.Subscriber.GetSubscription	projects/log
<input type="checkbox"/>	> 5/28/2024, 6:42:32.775 PM	pubsub.googleapis.com	google.pubsub.v1.Subscriber.GetSubscription	projects/log
<input type="checkbox"/>	> 5/28/2024, 6:22:36.700 PM	pubsub.googleapis.com	google.pubsub.v1.Subscriber.GetSubscription	projects/log
<input type="checkbox"/>	> 5/28/2024, 6:20:37.211 PM	cloudasset.googleapis.com	google.cloud.asset.v1.AssetService.ExportAssets	organizatio



Conclusions

Closing Remarks

Ingesting cross-cloud events can be complex. And expensive!

Centralize audit log data into a data lake per cloud to save on egress data transfer charges

Identify high value events for exporting to a centralized SIEM for monitoring and alerting

Read your SIEM's integration support for each cloud provider to find supported export patterns

Avoid using long-lived credentials for cross-cloud connections. Workload identity is better!





SANS

Hands-On Workshops

AVIATA CLOUD

SOLO FLIGHT CHALLENGE

Around the World 2x

<https://sans.org/ace135>



SANS CLOUD SECURITY

CURRICULUM ROADMAP

Baseline

SEC 388 **Introduction to Cloud Computing and Security**
Ground school for cloud security

Foundational Security Techniques

SEC 488 **Cloud Security Essentials** | GCLD
License to learn cloud security.



Leadership

LDR 520 **Cloud Security for Leaders**
Strategically maximize your cloud investment.

Core

SEC 510 **Cloud Security Controls & Mitigations** | GPCS
Prevent real attacks with controls that matter.

SEC 540 **Cloud Security and DevSecOps Automation** | GCSA
The cloud moves fast. Automate to keep up.

SEC 541 **Cloud Security Threat Detection** | GCTD
Attackers can run but not hide. Our radar sees all threats.

SEC 549 **Cloud Security Architecture**
Design it right from the start.





Specialization

SEC 522 **Application Security: Securing Web Apps, APIs, and Microservices** | GWEB
Not a matter of "if" but "when." Be prepared for a web attack. We'll teach you how.

SEC 588 **Cloud Penetration Testing** | GCPN
Aim your arrows to the sky and penetrate the cloud.

FOR 509 **Enterprise Cloud Forensics and Incident Response** | GCFR
Find the storm in the cloud.

