



Service Agents

& the Search for

Transitive Access in GCP

Kat Traxler

About Me



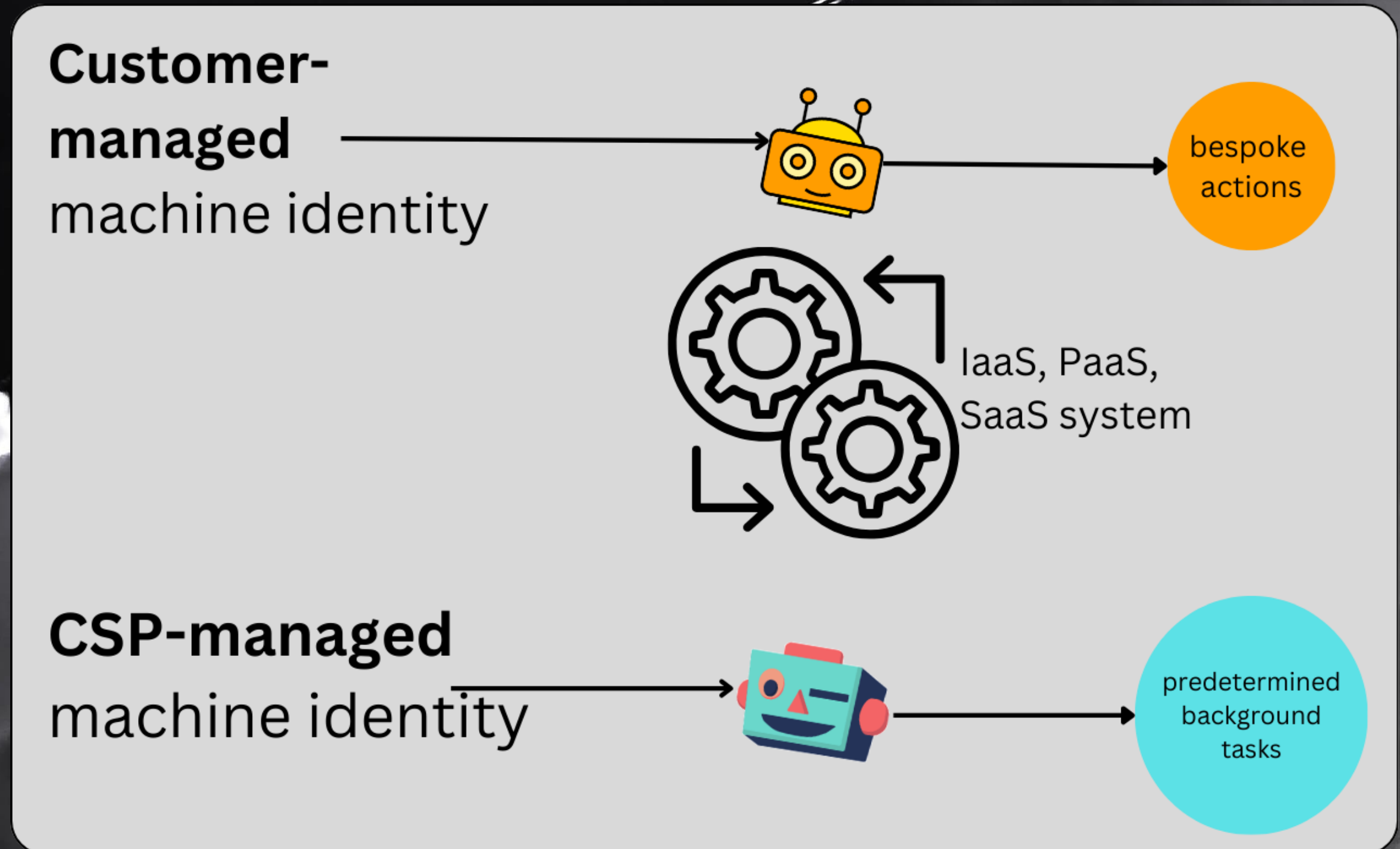
- Security Researcher - Vectra AI
- Google Cloud Security Nerd

Agenda

1. Service Agents, what **are they**?
2. Service Agents, what **can** go wrong?
3. Service Agents, what **did** go wrong?
4. What's next customers

What are Machine Identities?

- AWS Service Linked Roles
- GCP Service Agents
- Azure System-Assigned Managed Identities



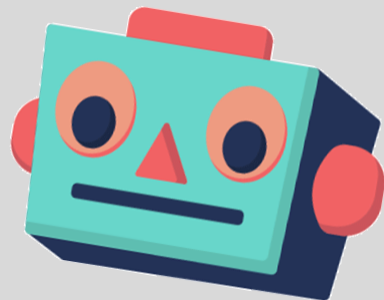
Service Accounts

➔ Google-Managed Service Accounts

➔ Service Agents (P4SAs)

Service Accounts

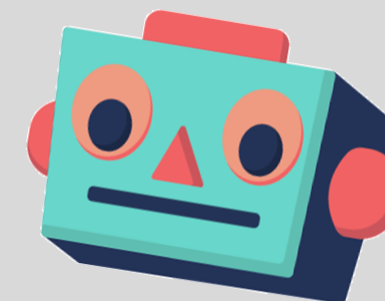
*Customer-Managed Service
Accounts*



project

*Google-managed
Service Accounts*

service agents



project

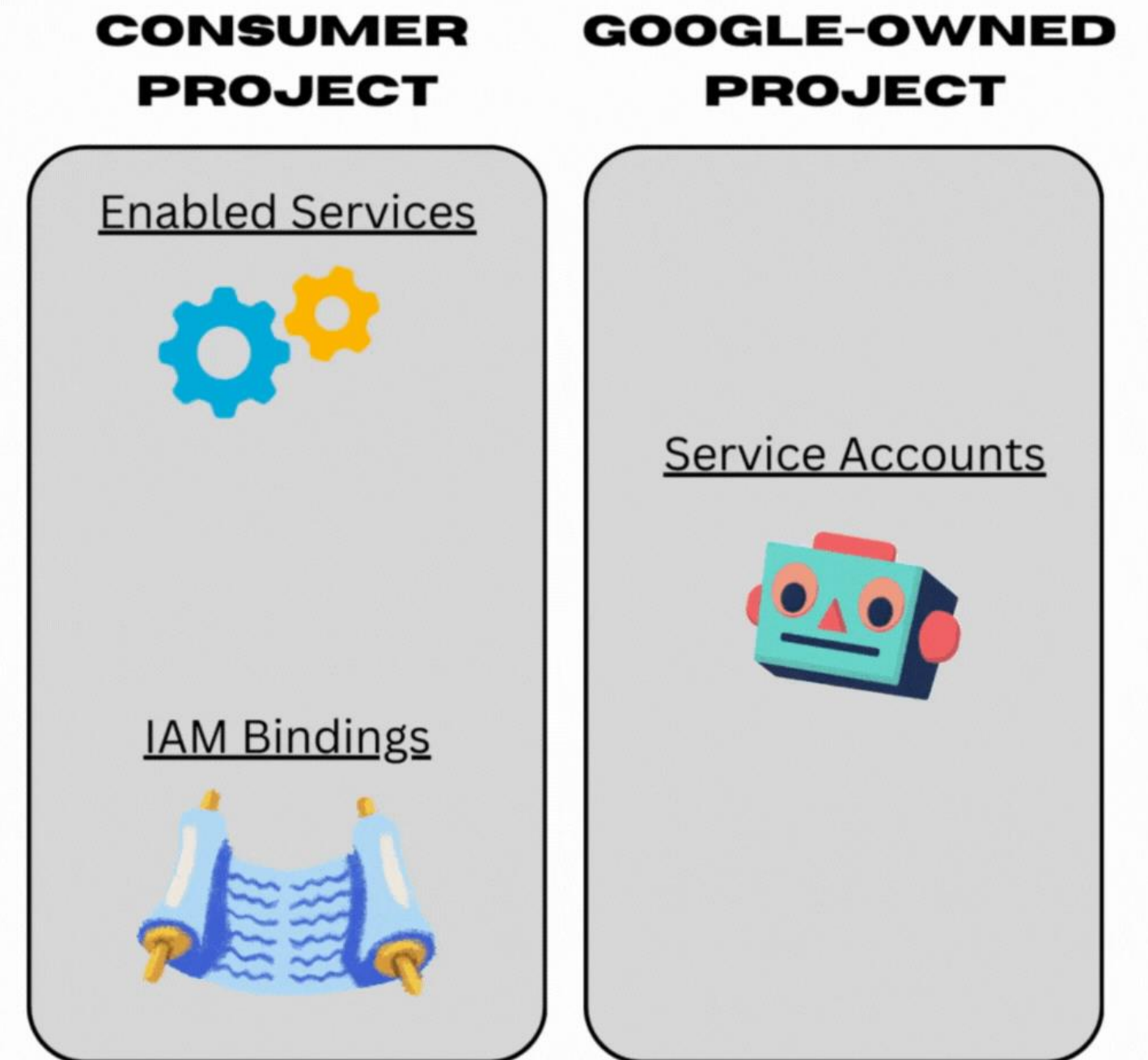
project

*one-to-one
relationship*

Per Product Per Project (P4SAs)

P4SA Creation Workflow

1. Enable a GCP Service: Required is the *serviceusage.services.enable* permission
2. Service Account Created: As a result of the enablement, a Service Account is created in a Google-Owned Project
3. Role Assigned: A 'Service Agent' Role is assigned to the new Service Account at the project-level of the consumer project



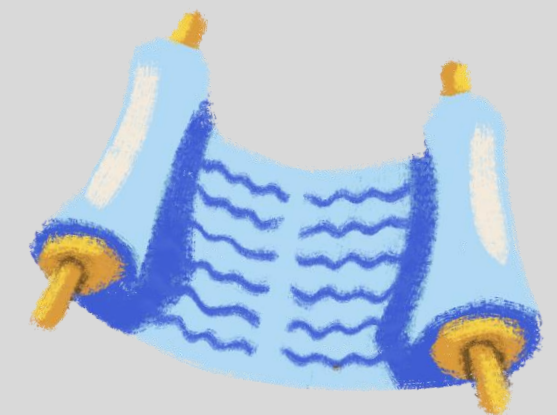
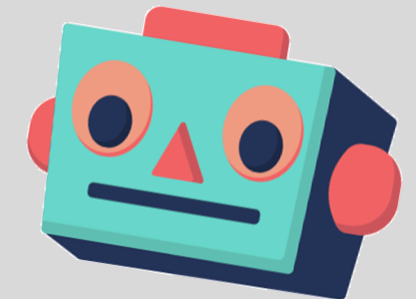
Threat Modeling Service Agents

What CAN'T go wrong (generally*)

Spoofing

- The **permissions** to Spoof (impersonate) a Service Agent are managed in the **Google-owned Project**
- Spoofing (impersonation) threats are managed by the CSP

*Google-Owned
Project*

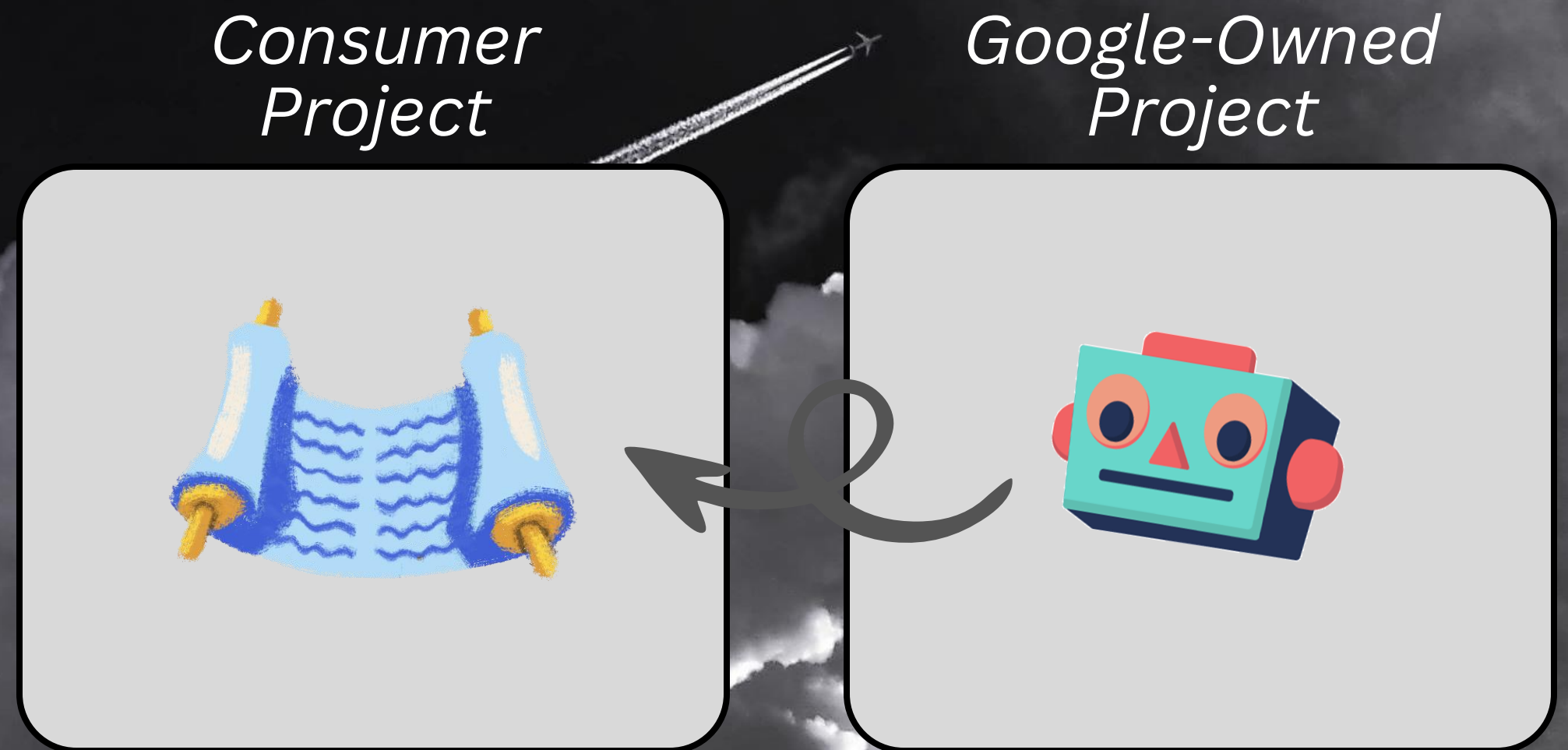


Threat Modeling Service Agents

What CAN go wrong

Privilege Escalation

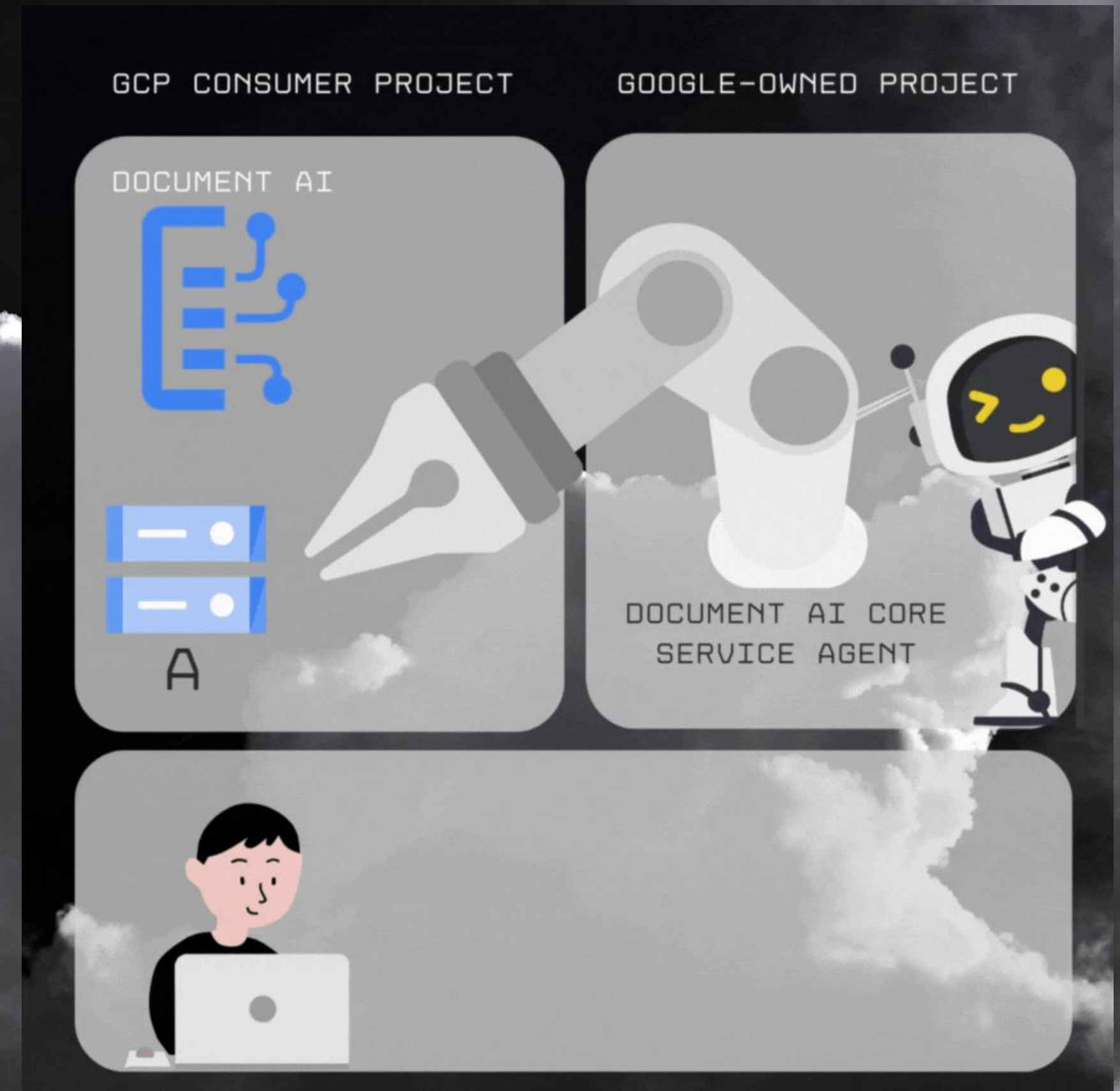
- The **permissions** needed to use a service agent are managed in the consumer-project
- Privilege Escalation threats can be exposed by service functionality



Document AI Service (and its P4SA)

What DID go wrong

- Service processes text (input) and writes result (output)
- Inputs and Outputs can be GCS bucket locations which are end-user controlled



Retrieving Objects without Storage Permissions

The image is a screenshot of a web browser displaying the Google Cloud console. The browser's address bar shows the URL: console.cloud.google.com/workflows/workflow/us-central1/document-ai-batchProcess-data/executions?project=kats-lolz-yolo-project. The console interface includes a top navigation bar with the Google Cloud logo, the project name 'kats-lolz-yolo-project', and a search bar. On the left, there is a sidebar with navigation links for 'Workflows', 'Workflows' (with a sub-link 'Workflows'), and 'Dashboard'. The main content area is titled 'Workflow details' and shows the workflow name 'document-ai-batchProcess-data'. Below this, there are tabs for 'METRICS', 'EXECUTIONS', 'LOGS', 'DETAILS', 'TRIGGERS', 'SOURCE', and 'PERMISSIONS'. The 'EXECUTIONS' tab is active, displaying a table of workflow executions. The table has columns for 'State', 'Execution ID', 'Workflow revision', 'Create time', 'Start time', 'End time', 'Duration', and 'Actions'. One execution is listed with a 'return' state, 'Succeeded' status, and a duration of 46.181 seconds. A notification banner at the bottom of the console states 'Created execution 7e1ac120-8c11-4703-bb8c-8846b1dcc4cf'. The browser's taskbar at the bottom shows various application icons, including the Apple logo, Safari, Calendar (showing SEP 12), Chrome, and several other utility and productivity apps.

Transitive Access via Service Agents

```
▼ protocoload: {  
  @type: "type.googleapis.com/google.cloud.audit.AuditLog"  
  ▼ authenticationInfo: {  
    principalEmail: "service-697769455569@gcp-sa-prod-dai-core.iam.gserviceaccount.com"  
  }  
  ▼ authorizationInfo: [  
    ▼ 0: {  
      granted: true  
      permission: "storage.objects.get" Get Object  
      resource: "projects/_/buckets/document-ai-source-dndw/objects/multi_document.pdf"  
      ▼ resourceAttributes: {  
      }  
    }  
    ▼ 1: {  
      permission: "storage.objects.getIamPolicy"  
      resource: "projects/_/buckets/document-ai-source-dndw/objects/multi_document.pdf"  
      ▼ resourceAttributes: {  
      }  
    }  
  ]  
}
```

Document AI Service Agent

Get Object

Reporting Timeline

Missed Opportunities.....



- **Highlights**

- April 4th: Initial Report
- May 7th: No bounty to be issued as the issue is a result of ‘insufficient documentation’.
- June 22nd: Status Changed to ‘Fixed’ (issue not fixed)
- August 21st: Issue re-open and internal team determining if the issue is ‘working as intended’ or not.
- September 10th: Bounty issued in the amount of \$3,133.70 and categorized as a “bypass of significant security controls”

What's next for the cloud consumer?

Cool its broken, now what?

- “Least Privilege” never had your back
- Think about architecting for an IAM Blast Radius and detecting when things go off the rails

In Conclusion.....

DOCUMENTATION

$$A + B = C$$

VS

REALITY

$$A + B = D$$

$$E + B = D$$

$$E + B = G$$

Questions?

