Fight the CRIME

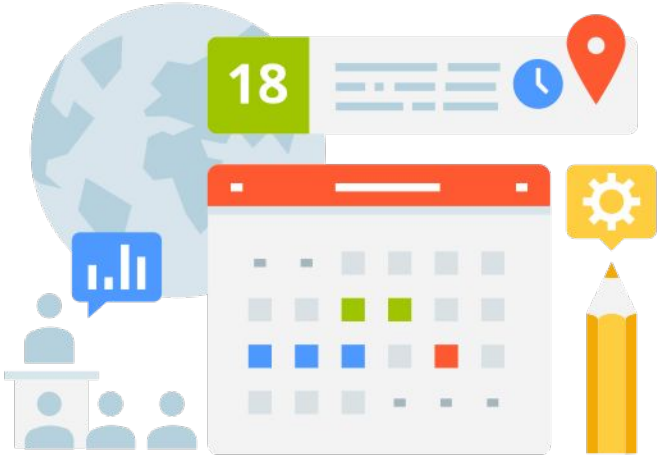
BLUE TEAM

→ SECURITY INCIDENT RESPONSE

Incident Response

Google Cloud Platform

Agenda



- The Mission
- Data exfiltration from cloud storage
- Preparation
- Investigation
- Questions

Mission

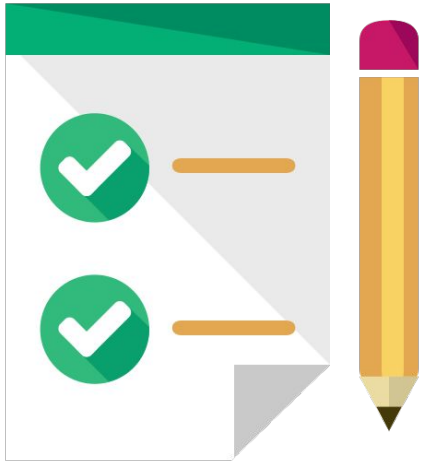
- Attention security analyst, we have a breach in progress! Your mission is to infiltrate the Google Cloud Project and track down the enemy responsible for stealing sensitive data.
- You will need to gather intelligence by analyzing different sources of evidence. Look for unusual activity, such as unauthorized logins, changes to permissions, objects access, and suspicious network traffic.
- Once you've identified the enemy's location, it's time to strike! Use your security tools to contain the breach and prevent further data loss.
- Collect all the evidence you can find to determine the extent of the breach and identify the stolen data. You will need to preserve this evidence for future investigation and legal action.
- Good luck, soldier! The fate of our organization rests in your hands."

Preparation

The Attack

Initial Access 8 techniques	Execution 9 techniques	Persistence 17 techniques	Privilege Escalation 11 techniques	Defense Evasion 25 techniques	Credential Access 15 techniques	Discovery 25 techniques	Lateral Movement 8 techniques	Collection 15 techniques	Command and Control 16 techniques	Exfiltration 9 techniques
Valid Accounts (0/4)	Command and Scripting Interpreter (0/4)	Valid Accounts (0/4)	Valid Accounts (0/4)	Valid Accounts (0/4)	Adversary-in-the-Middle (0/2)	Cloud Storage Object Discovery	Exploitation of Remote Services	Data from Cloud Storage	Application Layer Protocol (0/4)	Exfiltration Over Alternative Protocol (0/3)
Exploit Public-Facing Application	Exploitation for Client Execution	Account Manipulation (0/3)	Abuse Elevation Control Mechanism (0/2)	Abuse Elevation Control Mechanism (0/2)	Brute Force (0/4)	Account Discovery (0/3)	Internal Spearphishing	Adversary-in-the-Middle (0/2)	Communication Through Removable Media	Exfiltration Over Web Service (0/2)
Drive-by Compromise	Inter-Process Communication (0/0)	Boot or Logon Autostart Execution (0/2)	Boot or Logon Autostart Execution (0/2)	Debugger Evasion	Credentials from Password Stores (0/3)	Application Window Discovery	Lateral Tool Transfer	Archive Collected Data (0/3)	Data Encoding (0/2)	Transfer Data to Cloud Account
External Remote Services	Native API	Boot or Logon Initialization Scripts (0/1)	Boot or Logon Initialization Scripts (0/1)	Deobfuscate/Decode Files or Information	Exploitation for Credential Access	Browser Bookmark Discovery	Remote Service Session Hijacking (0/1)	Audio Capture	Data Obfuscation (0/3)	Automated Exfiltration (0/0)
Hardware Additions	Scheduled Task/Job (0/3)	Browser Extensions	Create or Modify System Process (0/1)	Execution Guardrails (0/1)	Forge Web Credentials (0/2)	Cloud Infrastructure Discovery	Remote Services (0/2)	Automated Collection	Dynamic Resolution (0/3)	Data Transfer Size Limits
Phishing (0/3)	Serverless Execution	Compromise Client Software Binary	Escape to Host	Exploitation for Defense Evasion	Input Capture (0/3)	Cloud Service Dashboard	Software Deployment Tools	Clipboard Data	Encrypted Channel (0/2)	Exfiltration Over C2 Channel
Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (0/3)	Event Triggered Execution (0/3)	File and Directory Permissions Modification (0/1)	Modify Authentication Process (0/3)	Cloud Service Discovery	Taint Shared Content	Data from Information Repositories (0/0)	Fallback Channels	Exfiltration Over Other Network Medium (0/1)
Trusted Relationship	System Services (0/0)	Create or Modify System Process (0/1)	Exploitation for Privilege	Hide Artifacts (0/7)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material	Data from Local System	Ingress Tool Transfer	
	User Execution (0/3)			Hijack Execution Flow (0/1)		File and Directory Discovery		Data from Network Shared Drive	Multi-Stage	
				Impair Defenses (0/7)		Network Service Discovery				

Preparation



- Understand Google Cloud Project
- Data Classification Policies
- Communication Templates (External & Internal)
- Cloud storage security guidelines
- Cloud logging / audit policies
- Threat Modeling
- Test your controls
  - Table Tops
  - Playbooks

https://attack.mitre.org/techniques/T1530/

Investigating data breaches due to compromised buckets

Here we go!

- **Built-in audit logs**
- Platform Logs
- Host (VMs) Logs
- App Logs
- **VPC Flow Logs**
- Firewall Logs
- Network Capture
- Load Balancing Logs
- **Google Cloud Storage Logs**
- **Google Cloud Storage Usage Logs**
- GKS logs

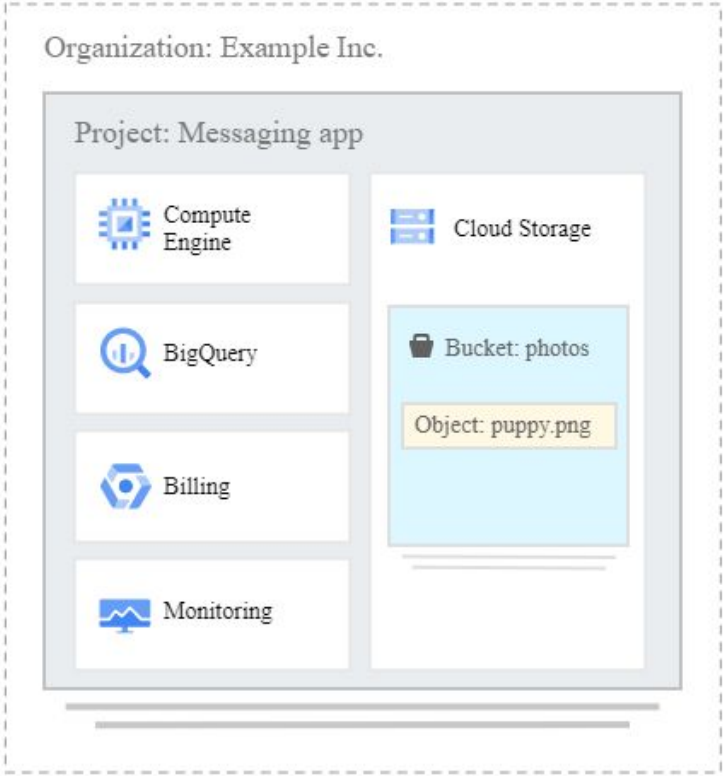
Mission Failed

From: The Boss
To: Cloud Security Engineer
Sent: 2022-11-04T17:28

You lost the mission, you're fired!!!

Investigating data breaches due to compromised buckets

Google Cloud Buckets



Bucket: Each project can contain multiple buckets, which are containers to store your objects. For example, you might create a photos bucket for all the image files your app generates and a separate videos bucket.

Object: An individual file, such as an image called puppy.png.

https://cloud.google.com/storage/docs/introduction

Google Cloud Buckets

- **Name your bucket**

Pick a **globally unique**, permanent name. Naming guidelines

media-0666

Tip: Don't include any sensitive information

Labels (optional)

Labels are key:value pairs that allow you to group related buckets together or with other Cloud Platform resources. Learn more

Key 1: tlp

Value 1: red

+ ADD LABEL

TRAFFIC LIGHT PROTOCOL
https://www.first.org/tlp/

Google Cloud Buckets

Bucket details

customers-2494

Location	Storage class	Public access	Protection
us (multiple regions in United States)	Standard	Subject to object ACLs	None

OBJECTS | CONFIGURATION | PERMISSIONS | PROTECTION | LIFECYCLE | OBSERVAI

Overview	
Created	November 1, 2022 at 1:37:03 PM GMT+1
Updated	November 1, 2022 at 1:37:03 PM GMT+1
Location type	Multi-region
Location	us (multiple regions in United States)
Replication	Default
Default storage class	Standard
Requester Pays	OFF
Tags	None
Labels	tlp : amber
Cloud Console URL	https://console.cloud.google.com/storage/browser/customers-2494
gsutil URI	gs://customers-2494
Permissions	
Access control	Fine-grained
Public access prevention	Not enabled by org policy or bucket setting

Edit access control

Choose how to control object access in this bucket.

- ○ Uniform
  Ensure uniform access to all objects in the bucket by using only bucket-level permissions (IAM). This option becomes permanent after 90 days. Learn more
- ◉ Fine-grained
  Specify access to individual objects by using object-level permissions (ACLs) in addition to your bucket-level permissions (IAM). Learn more

Google Cloud Buckets

Edit access

Object name: terraform.tar.gz

If you don't rely on individual object-level access, you can start managing all access uniformly at the bucket-level. Go to the bucket's Permissions tab to get started. Learn more

Entity	Name	Access
Entity 1 * Project	Name 1 owners-71741976249	Access 1 * Owner
Entity 2 * Project	Name 2 editors-71741976249	Access 2 * Owner
Entity 3 * Project	Name 3 viewers-71741976249	Access 3 * Reader
Entity 4 * User	Name 4 drodriguez	Access 4 * Owner

Edit access control

Choose how to control object access in this bucket.

- (●) **Uniform**
  Ensure uniform access to all objects in the bucket by using only bucket-level permissions (IAM). This option becomes permanent after 90 days. Learn more
- ( ) **Fine-grained**
  Specify access to individual objects by using object-level permissions (ACLs) in addition to your bucket-level permissions (IAM). Learn more

⚠ Uniform access control removes object ACLs from this bucket. This will revoke object access for users who rely solely on ACLs for access unless you add their permissions to the bucket's IAM policy. Learn more

Google Cloud Buckets

Bucket details

customers-2494

Location	Storage class	Public access	Protection
us (multiple regions in United States)	Standard	Subject to object ACLs	None

OBJECTS | CONFIGURATION | PERMISSIONS | PROTECTION | LIFECYCLE | OBSERVAI

Overview	
Created	November 1, 2022 at 1:37:03 PM GMT+1
Updated	November 1, 2022 at 1:37:03 PM GMT+1
Location type	Multi-region
Location	us (multiple regions in United States)
Replication	Default
Default storage class	Standard
Requester Pays	OFF
Tags	None
Labels	tlp : amber
Cloud Console URL	https://console.cloud.google.com/storage/browser/customers-2494
gsutil URI	gs://customers-2494
Permissions	
Access control	Fine-grained
Public access prevention	Not enabled by org policy or bucket setting

Public access prevention may be enforced through an org policy or bucket-level setting:

- **Enabled via org policy inheritance** means public access is restricted by an org policy
- **Enabled via bucket setting** means public access is only restricted at the bucket level
- **Not enabled by org policy or bucket setting** means public access is not restricted
- **Not enabled via bucket setting; org policy status unavailable** means that public access is not restricted at the bucket level but could be inherited at the org, folder, or project level

Google Cloud Buckets

IAM & Admin

- IAM
- Identity & Organization
- Policy Troubleshooter
- Policy Analyzer NEW
- Organization Policies
- Service Accounts

Organization policies + CUSTOM CONSTRAINT

- Enforce FIPS-compliant machine types
- Enforce Public Access Prevention
- Enforce uniform bucket-level access
- Google Cloud Platform - Detailed Audit Logging Mode
- Google Cloud Platform - Resource Location Restriction
- Require Enabled Services Allow List for Cross-Organization Move
- Require Firestore Service Agent for import/export
- Require OS Login

Enforce Public Access Prevention

Secure your Cloud Storage data from public exposure by enforcing public access prevention. This governance policy prevents existing and future resources from being accessed via the public internet by disabling and blocking ACLs and IAM permissions that grant access to `allUsers` and `allAuthenticatedUsers`. Enforce this policy on the entire organization (recommended), specific projects, or specific folders to ensure no data is publicly exposed.

This policy overrides existing public permissions. Public access will be revoked for existing buckets and objects after this policy is enabled.

Applies to

Organization "85 bits

- (●) Inherit parent's policy
- ( ) Google-managed default
- ( ) Customize

SAVE CANCEL

Google Cloud Buckets

Choose how to protect object data

Your data is always protected with Cloud Storage but you can also choose from these additional data protection options to prevent data loss. Note that object versioning and retention policies cannot be used together.

Protection tools

- (●) None
- ( ) Object versioning (best for data recovery)
  For restoring deleted or overwritten objects. To minimize the cost of storing versions, we recommend limiting the number of noncurrent versions per object and scheduling them to expire after a number of days. Learn more
- ( ) Retention policy (best for compliance)
  For preventing the deletion or modification of the bucket's objects for a specified minimum duration of time after being uploaded. Learn more

Data encryption

- (●) Google-managed encryption key
  No configuration required
- ( ) Customer-managed encryption key (CMEK)
  Manage via Google Cloud Key Management Service

Google Cloud Storage Logs

Disabled by Default!

Google Cloud | DFIR | Search (/) for resources, docs, products, and more | Search

IAM & Admin

- IAM
- Identity & Organization
- Policy Troubleshooter
- Policy Analyzer NEW
- Organization Policies
- Service Accounts
- Workload Identity Federat...
- Labels
- Tags
- Settings
- Privacy & Security
- Identity-Aware Proxy
- Roles
- Audit Logs
- Manage Resources

Audit Logs | SET DEFAULT CONFIGURATION | HELP ASSISTANT | HIDE INFO PANEL | LEARN

Default configuration	Admin Read:	Data Read:	Data Write:
0 exempted principals	Disabled	Disabled	Disabled

Data Access audit logs configuration

The effective data access configuration below combines the configuration for the currently selected resource and the data access configurations set on all parent resources.

Filter: Google Cloud Storage
Enter property name or value

Service	Admin Read	Data Read	Data Write
Google Cloud Storage	–	–	–

Google Cloud Storage

LOG TYPES | EXEMPTED PRINCIPALS

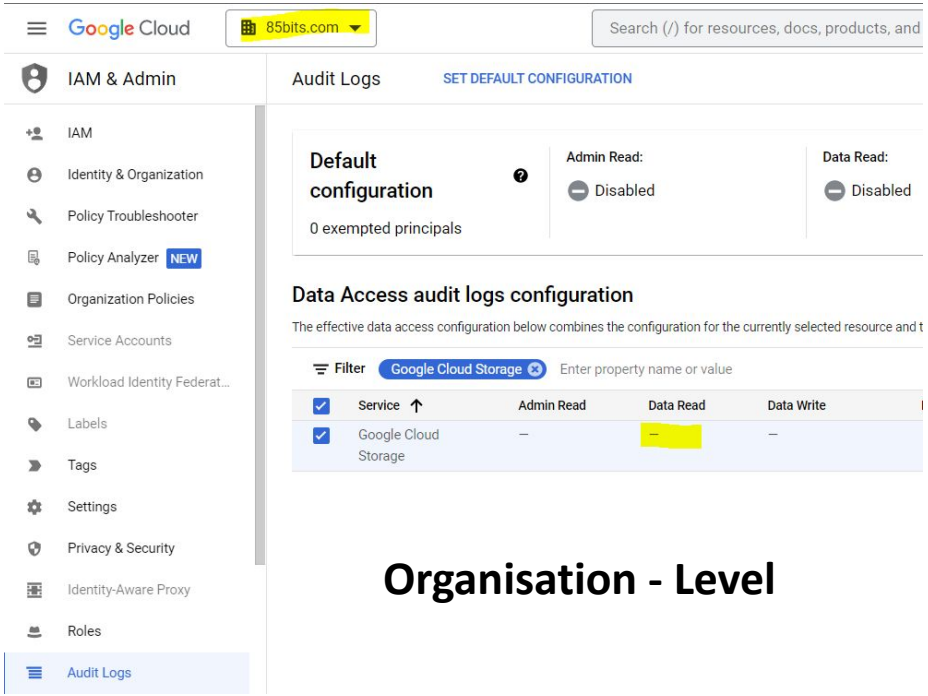
You can configure what types of operations are recorded in your Data Access audit logs for the selected services. There are several subtypes of Data Access audit logs:

Enabling audit logging for Google Cloud Storage disallows authenticated browser downloads for non-public objects. Learn more

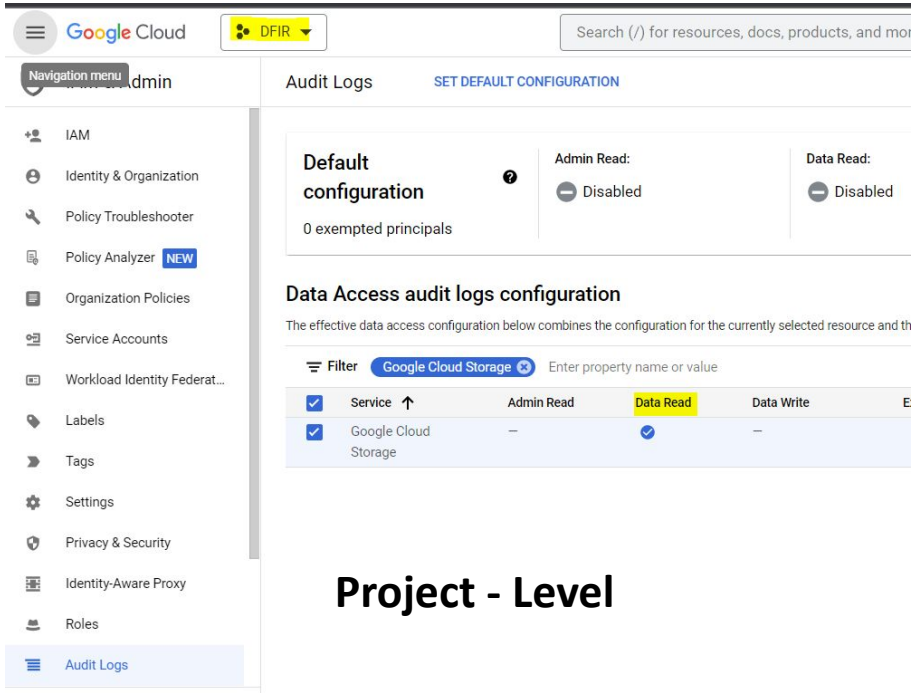
- [ ] Admin Read
  Records operations that read metadata or configuration information.
- [ ] Data Read
  Records operations that read user-provided data.
- [ ] Data Write
  Records operations that write user-provided data.

SAVE

Google Cloud Storage Logs



Organisation - Level



Project - Level

Google Cloud Storage Logs

Google Cloud | DFIR | logs explorer

Logs Explorer | REFINE SCOPE | Project

Query | Recent (6) | Saved (0) | Suggested (

Last 1 hour | Search all fields

```
1 resource.type="gcs_bucket"
2 protoPayload.methodName="storage.objects.get"
```

Google Cloud | DFIR | logs explorer

Logs Explorer | REFINE SCOPE | Project

Query | Recent (9) | Saved (0) | Suggested (0)

Last 1 hour | Search all fields

```
1 resource.type="gcs_bucket"
2 protoPayload.methodName="storage.objects.list"
3
```

Log fields | Histogram

Google Cloud Storage Logs

```
# Bucket creation
gsutil mb gs://bucket-logs4dfir
```

```
# Grant permissions group:role
gsutil iam ch group:cloud-storage-analytics@google.com:legacyBucketWriter
gs://bucket-logs4dfir
```

```
# Enable logging
gsutil logging set on -b gs://bucket-logs4dfir gs://customers-249
```

https://cloud.google.com/storage/docs/access-logs#delivery

```
┌──(dvirus㉿gondor)-[~]
└─$ whoami
```

Daniel Rodriguez
Security Consultant
Incident Response / Digital Forensics
Twitter @dvirus
Website: https://dvirus.training/

FOOCAFÉ
Learn · Create · Share · Grow

2600 MALMÖ

BLUE TEAM