

DECEMBER 9-10 BRIEFINGS

# Permission Mining in GCP

**Colin Estep Netskope Threat Labs** 276 . 224





#### Agenda

- IAM Exposure
- IAM in GCP
- A Real Example from GCP
- Permission Mining Solution
- Results and Remediation





## IAM Exposure





#### **IAM Exposure**

- What can your users do?
- Could a compromised credential result in administrator access?
- CodeSpaces was put out of business







#### Why is IAM challenging?

- Too many privileges may be given in a time crunch
- Confusion about the capability of granted permissions
- It is difficult to audit indirect permissions at scale







#### IAM in GCP





#### **Identities in GCP**

There are 4 different types of identities in GCP, which are called Members:

- User
- Group
- Domain
- Service Account

All of these are assigned permissions in the same way





#### **GCP Terminology**

- **Permission**: Allows a specific API call
- **Role**: A collection of permissions

Permiss	ions	
	compute.instances.delete	compute.instances.get
	compute.instances. setMachineType	compute.instances.start







#### **GCP Terminology**

- **Binding**: When a role is assigned to a member
- **Policies**: A collection of bindings

The different types of Roles:

- Basic not recommended
- Predefined
- Custom





#### **GCP Hierarchy**







Members	Members	
G Google Account	Google Workspace domain account	
Service account	Google group	
+	+	
Role	Role	
compute.imageUser	compute.instanceAdmin.v1	







## Service Accounts: Identities and Resources













#### **Binding at a Service Account**







#### **Binding at a Project**







#### **Binding at a Project**







## **Real Example in GCP**















"Owner" Permission Granted





#### Owner

0	Owner	+ EDIT ROLE	CREATE FROM ROLE
÷ <b>e</b>	ID	roles/ov	vner
Θ	Role launch stage	General	Availability
عر	Description		
e,	Full access to all r	esources.	
	3488 assigr	ned permiss	ions









#### **Editor**

θ	Editor	+ EDIT ROLE	CREATE FROM ROLE
÷ <u>•</u>	ID	roles/e	ditor
Θ	Role launch stag	<b>e</b> Genera	l Availability
ع	Descriptior	n	
Ę	Edit access to all	resources.	
	3197 assig	ned permiss	ions













# Why is this a problem?





0	Service accounts	CREATE SERVICE A		ELETE				
• •	Service accounts for proje A service account represents a Google service accounts. Organization policies can be used to se accounts entirely. Learn more about se	ect "siftsec-gcp-o Cloud service identity, s ecure service accounts a ervice account organizat	dev" such as code running o and block risky service tion policies.	on Compute Engine VM account features, suc	As, App Engine apps, or systems running outside Google. <u>L</u> ch as automatic IAM Grants, key creation/upload, or the cre	earn more	about ervice	To assign a project role to page. Edit or delete permissions b "Add Member" to grant new Show inherited pe
۲		8 Filter table			×	0		- Filter tree
ü	🗹 Email	Status	Name 个	Description	Key ID	Ke	Actions	Role / Member
연고	colin-permissions- testing@siftsec-gcp-	0	colin- permissions-	For testing GCP	2e3d5a838e2cf55e71a9faa4067254800304c13b	Ma	:	Cloud Build Service Ag
	dev.iam.gserviceaccount	t.com	testing	permissions				Cloud Dataflow Service
								Cloud Functions Service
\$								Cloud ML Service Ager
0								Compute Engine Service
-								Dataproc Service Agen
								Editor (6)
<b>a</b>								Firebase Service Mana
≡								Kubernetes Engine Ser
<u> </u>								Owner (8)
-								Security Reviewer (5)
21								Service Account Admir
En								Service Account Token
								Service Account User (
D								Viewer (5)



	HIDE INFO PANI	EL
a service ac	count, use the IAM	
elow or	+ ADD MEMBER	
rmissions		
		0
	Inheritance	
ent (1)		
e Agent (1)		
e Agent (1)		
nt (1)		
ce Agent (1)		
t (1)		
gement Servi	ice Agent (1)	
vice Agent (1	)	
n (1)		
Creator (2)		
(4)		



## **Permission Mining Solution**





#### What does it do?

- Can continually monitor the environment
- Uses a graph to find privilege escalation potential
- Provides a report containing direct and indirect permissions
- Users can monitor and mitigate risk







#### **Hierarchy Inventory**





## Compile Direct Bindings



Member	Project	
colin-testing@appspot.gserviceacc	ount.com siftsec-gcp-dev	
Role Browser 💌	Condition Add condition	ŧ
Access to browse GCP resources.		
Role	Condition	-
Viewer		





#### **Find Impersonators**

- Owner
- Editor
- Service Account Token Creator
- Service Account Key Admin
- Service Account User

0	Service Account	User	+ EDIT ROLE	Ē
+ <u>e</u>	ID	roles/i	am.serviceAccountUser	
Θ	Role launch stage	Genera	al Availability	
٩	Description			
Ę	Run operations as the s	ervice acco	unt.	
	5 assigned peri	nission	S	
	iam.serviceAccounts.act/	٨s		
	iam.serviceAccounts.list resourcemanager.projects	s.get		
۹	resourcemanager.projects	s.list		



#### CREATE FROM ROLE





			7
t Y		۵	Shared Infrastructure
E	Team	в	
			$\supset$
duct 1		۵	Product 2
			7
st GCP jject		Û	Production GCP Project
it GCP ject		lÎII	Production GCP Project
t GCP ect			Production GCP Project



#### **Find Potential Privilege Escalation**

- Traverse the graph for each member
- Find the Service Accounts in scope
- Compile all of the permissions assigned to Service Accounts
- Apply the extended bindings to the member



**@BLACKHATEVENTS #BHEU** 



## **Our Results**





#### **Member Report**

#### Report for cestep

**Direct Bindings** 

Project bindings 'siftsec-gcp-dev': ['roles/editor']

#### **Extended Bindings**

Organization bindings 'siftsec.com': ['roles/iam.securityReviewer', 'roles/owner', 'roles/pubsub.editor', 'roles/browser']



# aditor' 'roles/browser'l



#### **Graph Layout**

#### Legend:

- Blue => Organization
- Green => Member
- Light Pink => Project
- Dark Pink => Service Account



























#### Remediation

- Bringing service account bindings down the hierarchy
- Changing out basic roles for more granular roles
- Removing bindings that are not needed

We want to proactively reduce risk in the environment without waiting for a compromise.





## **Future Enhancements**





#### **Compute Engine**





#### **Cloud Functions**

θ	Cloud Functions Developer + EDIT R			
+ <u>e</u>	ID roles/cloudfunctions.develope			
Θ	Role launch stage	General Availa	bility	
٩	Description			
Ę	Read and write access	to all functions-relat	ted resources.	
	16 assigned pe	rmissions		
	cloudfunctions.functions	.call		
	cloudfunctions.functions cloudfunctions.functions	.delete .get		
۹	cloudfunctions.functions cloudfunctions.functions	.invoke .list		
\$	cloudfunctions.functions cloudfunctions.functions cloudfunctions.functions	.sourceCodeGet .sourceCodeSet .update		
0	cloudfunctions.locations cloudfunctions.operation	list s.get		
<b>=</b>	cloudfunctions.operation resourcemanager.project	s.list s.get		
	serviceusage.services.ge serviceusage.services.lis	t t		

Member 个	Name
siftsec-gcp-dev@appspot.gserviceaccount.com	App Engine default serv

	Role	Analyzed permissions (excess/total)		
/ice account	Editor	······································	•	
	$\bigcirc$			



#### **Organization Policies**

θ	Organization policies		
+ <u>•</u>	Organization policies for project "siftsec-gcp-dev"		
θ	Cloud Organization Policies let you constrain access to resources at and below this organization, folder or project. You can edit restrictions on the policy detail page.		
2	- Service Account C Filter by policy pame or ID		
Ę	Name 1	ID	Inheritanc
	Disable Automatic IAM Grants for Default Service Accounts	constraints/iam.automaticlamGrantsForDefaultServiceAccounts	Inherited
	Disable service account creation	constraints/iam.disableServiceAccountCreation	Inherited
<u>아</u> 코	Disable service account key creation	constraints/iam.disableServiceAccountKeyCreation	Inherited
•	Disable Service Account Key Upload	constraints/iam.disableServiceAccountKeyUpload	Inherited
\$			







#### **Thank you!**

Colin Estep

@colinestep https://www.linkedin.com/in/colinestep/

Project URL: github.com/netskopeoss/iaas\_permission\_mining

**THREAT LABS** 

