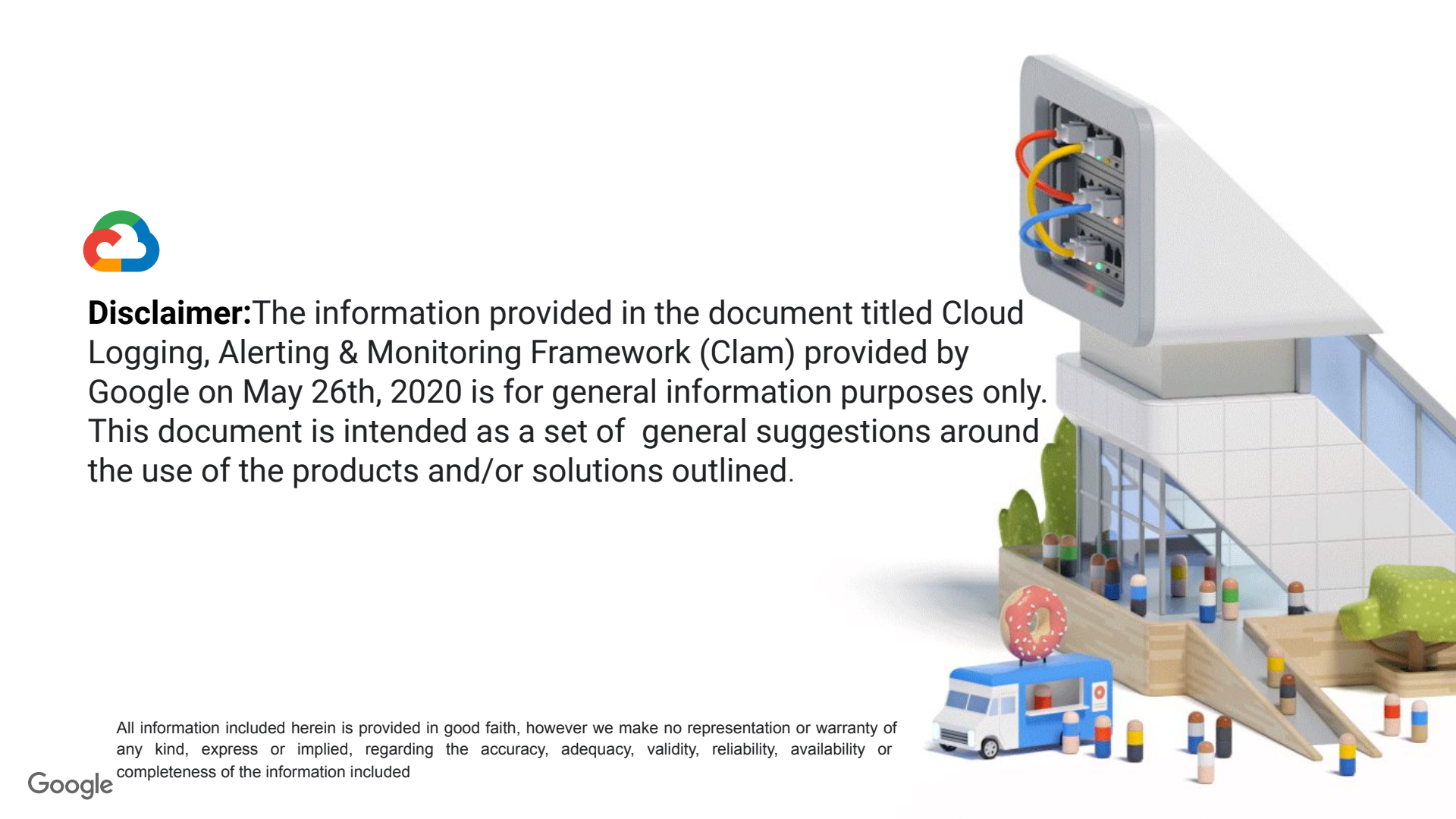
Cloud Logging, Alerting & Monitoring Framework (CLAM Framework)

Elliott Abraham **Jason Bisson**

Security & Compliance, Customer Engineering May 26th 2020



Disclaimer: The information provided in the document titled Cloud Logging, Alerting & Monitoring Framework (Clam) provided by Google on May 26th, 2020 is for general information purposes only. This document is intended as a set of general suggestions around the use of the products and/or solutions outlined.

What is Cloud Logging Alerting and Monitoring (CLAM) Framework?

This Framework focuses on the attack vectors and provides prescriptive guidance to customers on what SHOULD be logged, alerted on, and monitored based on a given attack vector.

What is MITRE ATT&CK Framework?

ATT&CK is a powerful way to classify and study adversary techniques and understand their intent. You can use it to enhance, analyze, and test your threat hunting and detection efforts.

MITRE ATT&CK for GCP

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Exfiltration	Impact
Exploit Public-Facing Application	Account Manipulation	Valid Accounts	Redundant Access	Account Manipulation	Cloud Service Dashboard	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Trusted Relationship	Create Account		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Data from Information Repositories		
Valid Accounts	Implant Container Image		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning	Data from Local System		
	Redundant Access		Valid Accounts		Network Share Discovery	Data Staged		
	Valid Accounts				Remote System Discovery			
					System Information Discovery			
					System Network Connections Discovery			

MITRE ATT&CK for GCP

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Exfiltration	Impact
Exploit Public-Facing Application	Account Manipulation	Valid Accounts	Redundant Access	Account Manipulation	Cloud Service Dashboard	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Trusted Relationship	Create Account		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Data from Information Repositories		
Valid Accounts	Implant Container Image		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning	Data from Local System		
	Redundant Access		Valid Accounts		Network Share Discovery	Data Staged		
	Valid Accounts				Remote System Discovery			
					System Information Discovery			
					System Network Connections Discovery			

Initial Access - Exploit Public-Facing Application

Data Sources

- Cloud Audit Logs, Security Command Center, Web logs, Web application firewall logs, Application logs

Detection

- Use Cloud Armor WAF to monitor improper inputs attempting exploitation, such as SQL injection.
- Use Security Health Analytics (SHA) to identify misconfigurations.
- Monitor application logs for abnormal behavior that may indicate attempted or successful exploitation.

Mitigation

- Use Cloud Armor WAF to block the web's most common attacks.
- Use Cloud Security Scanner to scan externally facing applications for vulnerabilities and establish procedures to patch applications when critical vulnerabilities are discovered.
- Use VPC Service Controls to limit access and protect against data exfiltration.
- Use GKE Sandbox for application isolation.
- Use Identity Aware Proxy (IAP) to control access to cloud applications by verifying user identity and context.
- Use IAM policies to enforce the principle of least-privilege by limiting dashboard visibility to only the resources required.

Initial Access - Trusted Relationship

Data Sources

- Cloud Audit Logs, Admin activity logs, Application logs, Authentication logs, Third-party application logs

Detection

- Use Cloud Audit Logs to establish monitoring for activity conducted by second and third party providers and other trusted entities that may be leveraged as a means to gain access to the network.

Mitigation

- Use VPC Service Controls to isolate infrastructure components that do not require broad network access.
- Perform third-party risk assessments to analyze and control risks presented to your company by parties other than your own company.

Initial Access - Valid Accounts

Data Sources

- Cloud Audit Logs, Authentication logs

Detection

- Use Event Threat Detection (ETD) to monitor Cloud IAM abuse.
- Use Cloud Anomaly Detection (CAD) to monitor service account credentials that are accidentally leaked online or compromised.

Mitigation

- Use Org Policy to limit who can create service account keys.
- Monitor Cloud Anomaly Detection for exposed keys.
- Use VPC Service Controls to protect GCP APIs from arbitrary networks.
- Use 2FA / U2F and require its use.
- Use a tool that prevents password re-use at the company site.
- Install password check up on corp browsers.

MITRE ATT&CK for GCP

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Exfiltration	Impact
Exploit Public-Facing Application	Account Manipulation	Valid Accounts	Redundant Access	Account Manipulation	Cloud Service Dashboard	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Trusted Relationship	Create Account		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Data from Information Repositories		
Valid Accounts	Implant Container Image		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning	Data from Local System		
	Redundant Access		Valid Accounts		Network Share Discovery	Data Staged		
	Valid Accounts				Remote System Discovery			
					System Information Discovery			
					System Network Connections Discovery			

Persistence - Account Manipulation

Data Sources

- Cloud Audit Logs, Admin activity, API monitoring, Windows event logs, Packet capture

Detection

- Use Event Threat Detection (ETD) to monitor Cloud IAM abuse.
- Use Cloud Anomaly Detection (CAD) to monitor service account credentials that are accidentally leaked online or compromised.

Mitigation

- Use Org Policy to limit who can create service accounts.
- Use 2FA / U2F and require its use.

Persistence - Create Account

Data Sources

- Cloud Audit Logs, G Suite, Cloud Identity audit logs, Process monitoring, Process command-line parameters, Windows event logs

Detection

- Use Event Threat Detection (ETD) to monitor Cloud IAM abuse.
- Use Cloud Audit Logs to perform regular audits of user and service accounts to detect suspicious accounts that may have been created by an adversary.

Mitigation

- Use Org Policy to limit who can create service accounts.
- Use Org Policy to restrict the creation of accounts that are outside of the domain.
- Use 2FA / U2F and require its use.

Persistence - Implant Container Image

Detection

- Use Cloud Audit Logs to monitor calls that have been made to the Kubernetes API server.

Mitigation

- Use Container-Optimized OS (COS), which is Hardened, purpose-built minimal host OS image based on Chromium OS.
- Use Binary Authorization for verification of provenance and block deployments that do not meet the requirements.
- Use Container Registry Vulnerability Scanning to scan images and packages for known CVEs.

Persistence - Redundant Access

Data Sources

- Cloud Audit Logs, Packet capture, Network protocol analysis, File monitoring, Authentication logs

Detection

- Use Event Threat Detection (ETD) to monitor connections to malicious IPs/Domains.
- Use Packet Mirroring to monitor suspicious network traffic.

Mitigation

- Implement third-party Network Intrusion detection and prevention (IPS/IDS) systems that use network signatures to identify traffic for specific adversary malware.

Persistence - Valid Accounts

Data Sources

- Cloud Audit Logs, Authentication logs

Detection

- Use Event Threat Detection (ETD) to monitor Cloud IAM abuse.
- Use Cloud Anomaly Detection (CAD) to monitor service account credentials that are accidentally leaked online or compromised.

Mitigation

- Use Org Policy to limit who can create service account keys.
- Monitor Cloud Anomaly Detection for exposed keys.
- Use VPC Service Controls to protect GCP APIs from arbitrary networks.
- Use 2FA / U2F and require its use.
- Use a tool that prevents password re-use at the company site.
- Install password check up on corp browsers.

MITRE ATT&CK for GCP

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Exfiltration	Impact
Exploit Public-Facing Application	Account Manipulation	Valid Accounts	Redundant Access	Account Manipulation	Cloud Service Dashboard	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Trusted Relationship	Create Account		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Data from Information Repositories		
Valid Accounts	Implant Container Image		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning	Data from Local System		
	Redundant Access		Valid Accounts		Network Share Discovery	Data Staged		
	Valid Accounts				Remote System Discovery			
					System Information Discovery			
					System Network Connections Discovery			

Privilege Escalation - Valid Accounts

Data Sources

- Cloud Audit Logs, Authentication logs

Detection

- Use Event Threat Detection (ETD) to monitor Cloud IAM abuse.
- Use Cloud Anomaly Detection (CAD) to monitor service account credentials that are accidentally leaked online or compromised.

Mitigation

- Use Org Policy to limit who can create service account keys.
- Monitor Cloud Anomaly Detection for exposed keys.
- Use VPC Service Controls to protect GCP APIs from arbitrary networks.
- Use 2FA / 2SV and require its use.
- Use a tool that prevents password re-use at the company site.
- Install password check up on corp browsers.

MITRE ATT&CK for GCP

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Exfiltration	Impact
Exploit Public-Facing Application	Account Manipulation	Valid Accounts	Redundant Access	Account Manipulation	Cloud Service Dashboard	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Trusted Relationship	Create Account		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Data from Information Repositories		
Valid Accounts	Implant Container Image		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning	Data from Local System		
	Redundant Access		Valid Accounts		Network Share Discovery	Data Staged		
	Valid Accounts				Remote System Discovery			
					System Information Discovery			
					System Network Connections Discovery			

Defense Evasion - Redundant Access

Data Sources

- Cloud Audit Logs, Packet capture, Network protocol analysis, File monitoring, Authentication logs

Detection

- Use Event Threat Detection (ETD) to monitor connections to malicious IPs/Domains

Mitigation

- Implement Network Intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware.

Defense Evasion - Revert Cloud Instance

Data Sources

- Cloud Audit Logs

Detection

- Use Cloud Audit Logs to monitor resource API calls.

Mitigation

- Use Org Policy to limit who can use compute and storage resources
- Use IAM policies to enforce the principle of least-privilege by limiting dashboard visibility to only the resources required.

Defense Evasion - Unused/Unsupported Cloud Regions

Data Sources

- Cloud Audit Logs

Detection

- Use Cloud Audit Logs to monitor system logs to review activities occurring across all cloud environments and regions. Configure alerting to notify of activity in normally unused regions or if the number of instances active in a region goes above a certain threshold.
- Use CSCC Asset Inventory to monitor all the resources at the organization level

Mitigation

- Use tools like Forseti and Chef Inspec to ensuring consistent standards are enforced in every environment, at every stage of development.
- Use Org Policies to restrict resource location.

Defense Evasion - Valid Accounts

Data Sources

- Cloud Audit Logs, Authentication logs

Detection

- Use Event Threat Detection (ETD) to monitor Cloud IAM abuse.
- Use Cloud Anomaly Detection (CAD) to monitor service account credentials that are accidentally leaked online or compromised.

Mitigation

- Use Org Policy to limit who can create service account keys.
- Monitor Cloud Anomaly Detection for exposed keys.
- Use VPC Service Controls to protect GCP APIs from arbitrary networks.
- Use 2FA / U2F and require its use.
- Use a tool that prevents password re-use at the company site.
- Install password check up on corp browsers.

MITRE ATT&CK for GCP

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Exfiltration	Impact
Exploit Public-Facing Application	Account Manipulation	Valid Accounts	Redundant Access	Account Manipulation	Cloud Service Dashboard	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Trusted Relationship	Create Account		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Data from Information Repositories		
Valid Accounts	Implant Container Image		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning	Data from Local System		
	Redundant Access		Valid Accounts		Network Share Discovery	Data Staged		
	Valid Accounts				Remote System Discovery			
					System Information Discovery			
					System Network Connections Discovery			

Credential Access - Account Manipulation

Data Sources

- Cloud Audit Logs, Authentication logs

Detection

- Use Event Threat Detection (ETD) to monitor Cloud IAM abuse.
- Use Cloud Anomaly Detection (CAD) to monitor service account credentials that are accidentally leaked online or compromised.

Mitigation

- Use Org Policy to limit who can create service account keys.
- Monitor Cloud Anomaly Detection for exposed keys.
- Use VPC Service Controls to protect GCP APIs from arbitrary networks.
- Use 2FA / U2F and require its use.
- Use a tool that prevents password re-use at the company site.
- Install password check up on corp browsers.

Credential Access - Cloud Instance Metadata API

Data Sources

- Cloud Audit Logs, Authentication logs, CLI commands, Powershell, syslogs

Detection

- Monitor access to the Instance Metadata API and look for anomalous queries.
- It may be possible to detect adversary use of credentials they have obtained. See Valid Accounts for more information.

Mitigation

- A properly configured Web Application Firewall (WAF) may help prevent external adversaries from exploiting Server-side Request Forgery (SSRF) attacks that allow access to the Cloud Instance Metadata API.

Credential Access - Credentials in Files

Data Sources

- CSCC, DLP, Data access logs

Detection

- Use Cloud Security Command Center (CSCC) to monitor Data Loss Prevention (DLP) alerts.

Mitigation

- Use DLP API to preemptively search for files containing passwords and take actions to reduce the exposure risk when found.
- Conduct user training to ensure that developers and system administrators are aware of the risk associated with having plaintext passwords in software configuration files that may be left on endpoint systems or servers.
- Use GCP Secrets Manager to encrypt, store, manage, and audit infrastructure and application-level secrets.

MITRE ATT&CK for GCP

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Exfiltration	Impact
Exploit Public-Facing Application	Account Manipulation	Valid Accounts	Redundant Access	Account Manipulation	Cloud Service Dashboard	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Trusted Relationship	Create Account		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Data from Information Repositories		
Valid Accounts	Implant Container Image		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning	Data from Local System		
	Redundant Access		Valid Accounts		Network Share Discovery	Data Staged		
	Valid Accounts				Remote System Discovery			
					System Information Discovery			
					System Network Connections Discovery			

Discover - Cloud Service Dashboard

Data Sources

- Cloud Audit Logs

Detection

- Use Cloud Audit Logs to monitor account activity logs to see actions performed and activity associated with the cloud service management console.

Mitigation

- Use 2FA / U2F and require its use.
- Use IAM policies to enforce the principle of least-privilege by limiting dashboard visibility to only the resources required

Discover - Cloud Service Discovery

Data Sources

- Cloud Audit Logs

Detection

- Use Cloud Audit Logs to monitor API call made to cloud services for anomalous behavior that may indicate adversarial presence within the environment.

Mitigation

- Use IAM policies to enforce the principle of least-privilege by limiting dashboard visibility to only the resources required.
- Use VPC Service Controls to protect GCP APIs from unauthorized access.

Discover - Network Service Scanning

Data Sources

- VPC flow logs, Netflow, Network protocol analysis, Packet capture, Process command-line parameters, Process use of network

Detection

- Use network intrusion detection/prevention systems (partner solutions) to identify scanning activity. Monitor for process use of the networks and inspect intra-network flows to detect port scans.

Mitigation

- Implement CIS system hardening benchmark standards to ensure that unnecessary ports and services are closed to prevent risk of discovery and potential exploitation.
- Use GCP VPC networks to implement proper network segmentation.
- Use network intrusion detection/prevention systems to detect and prevent remote service scans.
- Use VPC Service Controls to protect GCP APIs from arbitrary networks.

Discover - Network Share Discovery

Data Sources

- VPC flow logs, Netflow, Network protocol analysis, Packet capture, Process command-line parameters, Process use of network

Detection

- Use Cloud Audit Logs and data access logs to monitor anomalous access.

Mitigation

- Use VPC Service Controls to protect GCP APIs from arbitrary networks.

Discover - Remote System Discovery

Data Sources

- Cloud Audit Logs, CLI commands, Powershell, syslogs

Detection

- Monitor processes and command-line arguments for actions that could be taken to gather system and network information.

Mitigation

- This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

Discover - System Information Discovery

Data Sources

- Cloud Audit Logs, Process monitoring, Process command-line parameters

Detection

- Cloud Audit Logs can be used to identify access to certain APIs and dashboards that may contain system information. Depending on how the environment is used, that data alone may not be useful due to benign use during normal operations.

Mitigation

- Use IAM policies to enforce the principle of least-privilege by limiting dashboard visibility to only the resources required.

Discover - System Network Connections Discovery

Data Sources

- Process command-line parameters (Windows and Linux)

Detection

- Monitor processes and command-line arguments (e.g. netstat, lsof) for actions that could be taken to gather system and network information.

Mitigation

- This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

MITRE ATT&CK for GCP

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Exfiltration	Impact
Exploit Public-Facing Application	Account Manipulation	Valid Accounts	Redundant Access	Account Manipulation	Cloud Service Dashboard	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Trusted Relationship	Create Account		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Data from Information Repositories		
Valid Accounts	Implant Container Image		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning	Data from Local System		
	Redundant Access		Valid Accounts		Network Share Discovery	Data Staged		
	Valid Accounts				Remote System Discovery			
					System Information Discovery			
					System Network Connections Discovery			

Collection - Data from Cloud Storage Object

Data Sources

- Cloud Audit Logs, CSCC SHA

Detection

- Use Security Health Analytics (SHA) to identify misconfigurations, such as publically accessible storage buckets
- Use Cloud Audit Logs to monitor data access logs for unusual activity.
- Use DLP API to identify files with sensitive information in storage buckets

Mitigation

- Use continues compliance tools like Forseti to enforce security policy on storage buckets.
- Use VPC service controls to further protect APIs with sensitive data.
- Use IAM policies to limit user account to the least privileges required.
- Use Bucket Policy Only to prevent individual ACLs.
- Use org policy to disallow the creation of public buckets

Collection - Data from Information Repositories

Data Sources

- Cloud Audit Logs, OAuth audit logs, Application logs, Authentication logs, Data loss prevention, Third-party application logs

Detection

- Monitor and alert on users that are retrieving and viewing a large number of documents and pages; this behavior may be indicative of programmatic means being used to retrieve all data within the repository.

Mitigation

- Consider periodic review of accounts and privileges for critical and sensitive repositories.
- Use DLP API to preemptively search for files containing passwords and take actions to reduce the exposure risk when found.

Collection - Data from Local System

Data Sources

- File monitoring, Process monitoring, Process command-line parameters.

Detection

- Monitor processes and command-line arguments for actions that could be taken to collect files from a system.

Mitigation

- Use hardened OS like COS to limit number of services that can be exploited.
- Enforce Data classification policy to limit storing of sensitive data on local systems.
- Use OS login to manage SSH access to Linux instances.

Collection - Data Staged

Data Sources

- File monitoring, Process monitoring, Process command-line parameters

Detection

- Monitor processes and command-line arguments for actions that could be taken to collect and combine files.

Mitigation

- This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

MITRE ATT&CK for GCP

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Exfiltration	Impact
Exploit Public-Facing Application	Account Manipulation	Valid Accounts	Redundant Access	Account Manipulation	Cloud Service Dashboard	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Trusted Relationship	Create Account		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Data from Information Repositories		
Valid Accounts	Implant Container Image		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning	Data from Local System		
	Redundant Access		Valid Accounts		Network Share Discovery	Data Staged		
	Valid Accounts				Remote System Discovery			
					System Information Discovery			
					System Network Connections Discovery			

Exfiltration - Transfer Data to Cloud Account

Data Sources

- Cloud Audit Logs, Data Access logs, Authentication logs

Detection

- Use Cloud Audit Logs to monitor data access logs for unusual activity, monitor for anomalous file transfer activity between accounts and to untrusted VPCs.
- Use DLP API to identify files with sensitive information like service accounts keys and application passwords.

Mitigation

- Use DLP API to preemptively search for files containing passwords and take actions to reduce the exposure risk when found.
- Use VPC service controls to further protect APIs with sensitive data.
- Use IAM policies to limit user account to the least privileges required.

MITRE ATT&CK for GCP

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Exfiltration	Impact
Exploit Public-Facing Application	Account Manipulation	Valid Accounts	Redundant Access	Account Manipulation	Cloud Service Dashboard	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Trusted Relationship	Create Account		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Data from Information Repositories		
Valid Accounts	Implant Container Image		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning	Data from Local System		
	Redundant Access		Valid Accounts		Network Share Discovery	Data Staged		
	Valid Accounts				Remote System Discovery			
					System Information Discovery			
					System Network Connections Discovery			

Impact - Resource Hijacking

Data Sources

- Cloud Audit Logs, Process use of network, Process monitoring, Network protocol analysis, Network device logs

Detection

- Use Event Threat Detection (ETD) to monitor crypto hijacking.
- Use Cloud Anomaly Detection (CAD) to monitor abuse of cloud resources.

Mitigation

- Use Cloud Functions to auto-remediate affected resources.