expel®

MITRE ATT&CK in Google Cloud Platform (GCP):
A defender's cheat sheet

expel

Bottom line:

Chasing down GCP alerts and combing through audit logs can be tough if you don't know what to look for (or even if you do).

Knowing which API calls are associated with different attack tactics isn't intuitive—which is why we created this handy guide to help while you're investigating incidents in GCP.

Disclaimer: The first iteration of the GCP Mindmap assumes you have visibility of GCP Cloud Audit Logs, including:

- Admin Activity audit logs
- Data Access audit logs
- System Event audit logs
- Policy Denied audit logs

A helpful way to map MITRE ATT&CK tactics to GCP API calls

This guide contains a breakdown of tactics we see attackers use most often during attacks in Google Cloud Platform (GCP).

To give you a jump start on your own GCP environment, we've mapped the GCP services where these tactics often originate (thanks, crafty attackers) along with the API calls they make to execute on these techniques.

As a bonus, we're throwing in some of our own tips and tricks for you to use when investigating an incident in GCP that's related to any of these attack tactics.

How to use this cheat sheet

This cheat sheet is intended as a resource to help inform GCP alert triage, investigations, and incident response. It helps by quickly identifying potential attacks and maps them to MITRE ATT&CK tactics.

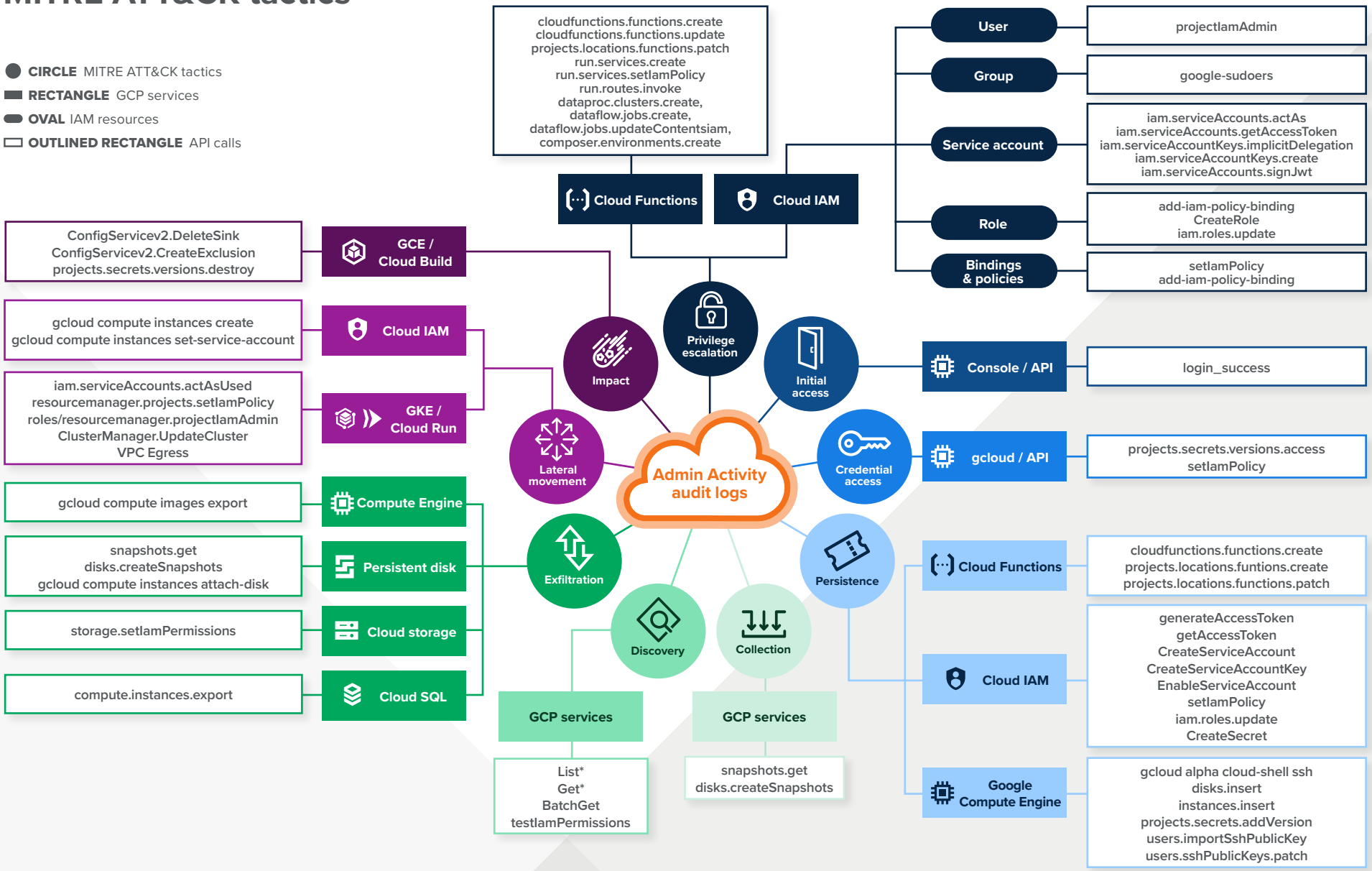
Depending on which phase of an attack you're investigating, you can also use it to identify other potential attack paths and MITRE ATT&CK tactics the attacker might have used. This provides you with a bigger picture perspective and identifies risky activity and behaviors that can indicate compromise and require remediation.

For example, if you see suspected credential access, you can investigate by checking how that identity authenticated to GCP, if they've assumed any other roles, and if there are other suspicious API calls indicating the presence of an attacker. Other tactics that an attacker may execute prior to credential access include discovery, persistence, and privilege escalation.

GCP mind map for investigations and incidents

MITRE ATT&CK tactics

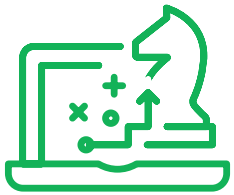
- **CIRCLE** MITRE ATT&CK tactics
- **RECTANGLE** GCP services
- **OVAL** IAM resources
- **OUTLINED RECTANGLE** API calls



* represents a wildcard that can be substituted for several AWS APIs

www.expel.com

A closer look at tactics, techniques and API calls

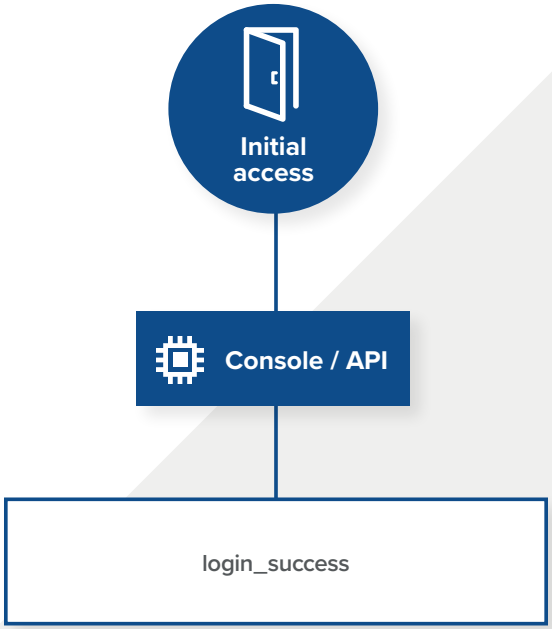


To help you get a better sense of how we think about our investigations in GCP, let's take a closer look at the tactics, techniques and associated API calls attackers might use.

MITRE ATT&CK tactic:

Initial access

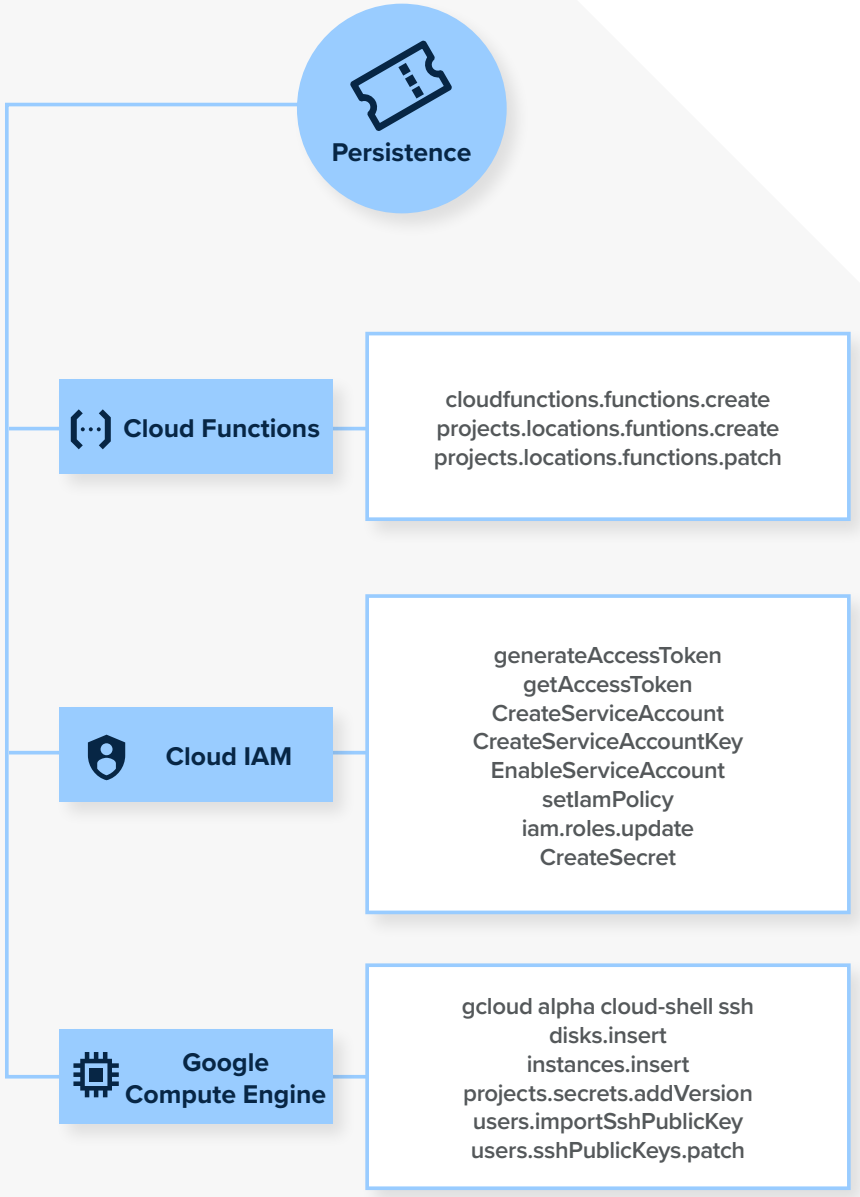
- **Why attackers do it:** To gain access to your GCP environment.
- **How attackers execute it:** GCP console or command-line interface.
- **Look in Google Workspace Audit Logs for event name:**: login_success
- **Investigation tips and tricks:** Review the source of authentication, user-agent strings and the credentials used to access the GCP environment. Investigate the authenticating principal, geo-impossible authentications, suspicious IP addresses, and anomalous authentication behavior. Check for new or suspicious OAuth token usage. Review storage options where secrets containing credentials or access keys may be exposed publicly.
- **Disclaimer:** *In order to have visibility of user login activity, you must enable Google Workspace data sharing within Google Cloud.*



MITRE ATT&CK tactic:

Persistence

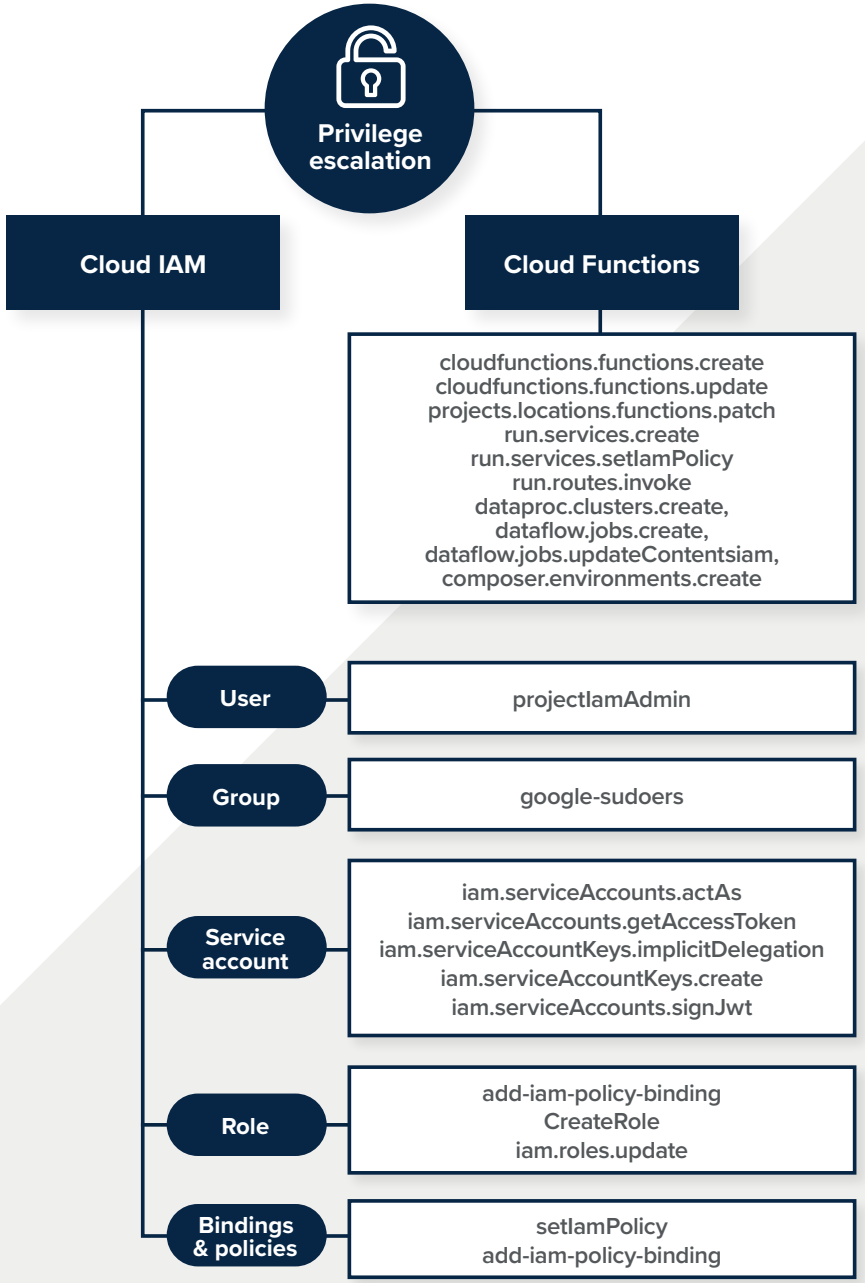
- **Why attackers do it:** To maintain access to your GCP environment across any interruptions.
- **How attackers execute it:** Google Cloud Identity, Google Compute Engine, Cloud Functions and IAM API.
- **Look for these API calls:** iam.servceAccounts.setIamPolicy, CreateServiceAccount, CreateServiceAccountKey, CreateRole, generateAccessToken
- **Investigation tips and tricks:** Look out for new or updated IAM resources, service account creation, role modifications, and permission updates. Persistence in these services is intended to provide the attacker with a means to reenter the GCP environment.

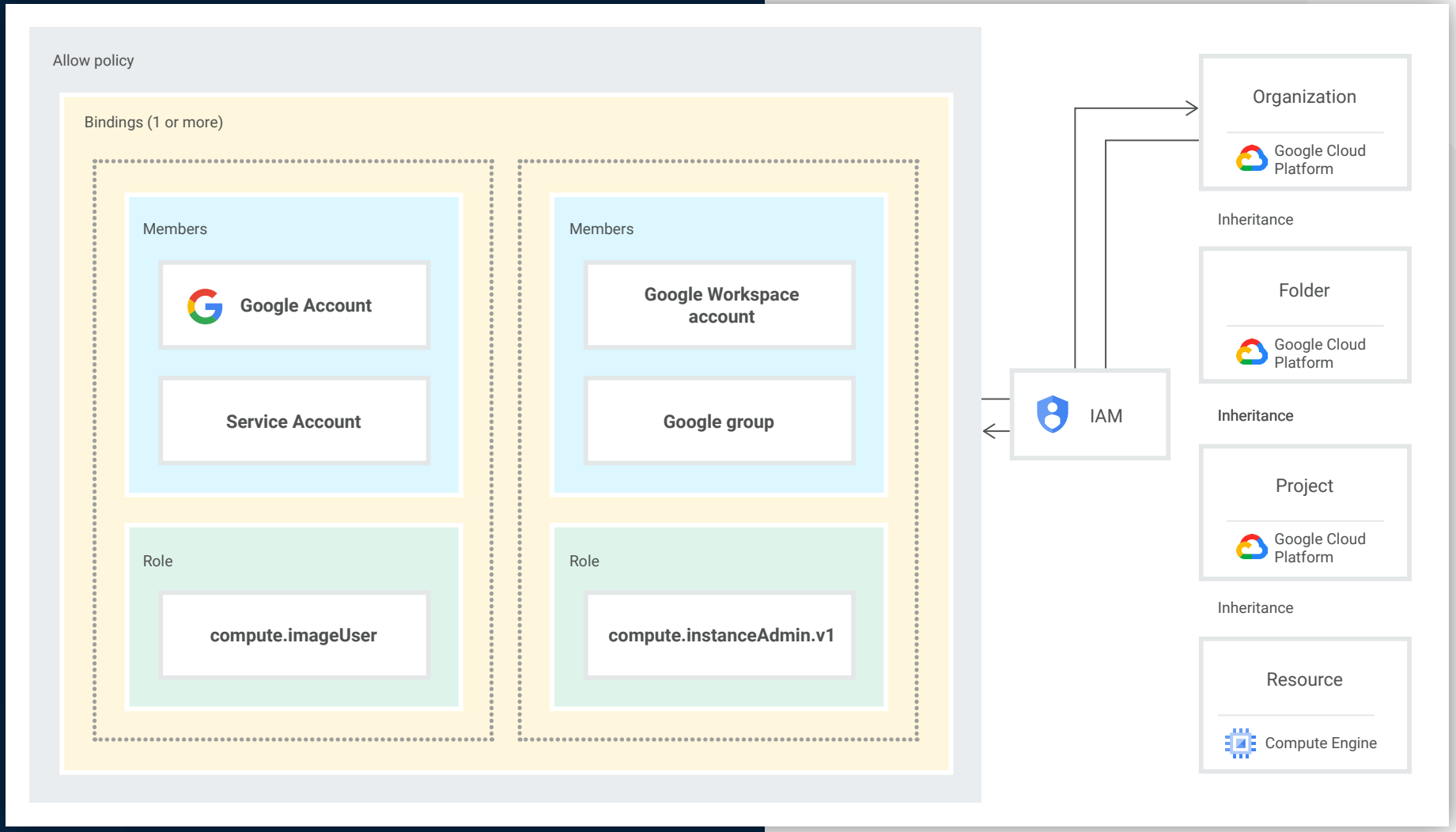


MITRE ATT&CK tactic:

Privilege escalation

- **Why attackers do it:** To gain higher-level permissions within your GCP environment and complete their objective(s). Elevated permissions are typically required to establish persistence, access credentials, and perform collection and exfiltration.
- **How attackers execute it:** GCP IAM and Cloud Functions.
- **Look for these API calls:** iam.servceAccounts.actAs, iam.servceAccounts.getAccessToken, dataproc.clusters.create, dataflow.jobs.create, dataflow.jobs.updateContentsiam, composer.environments.create, add-iam-policy-binding, CreateRole, iam.role.update, setIamPolicy, add-iam-policy-binding
- **Investigation tips and tricks:** Look out for new or updated IAM resources, service account creation, role modifications, and permission updates. Persistence in these services is intended to provide the attacker with a means to reenter the GCP environment.



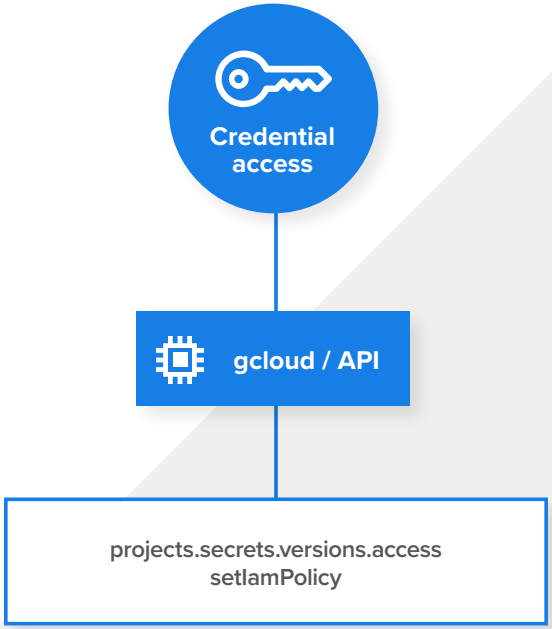


GCP tiers of access hierarchy and inherited permissions (source: Google Cloud)

MITRE ATT&CK tactic:

Credential access

- **Why attackers do it:** To access and acquire credentials in the GCP environment. Stolen credentials allow attackers to gain access to GCP resources, settings, and permissions.
- **How attackers usually execute it:** GCP IAM and Secret Manager.
- **Look for these API calls:** projects.secrets.versions.access, SetIamPolicy
- **Investigation tips and tricks:** Review the principal authentication details, source of activity, and other API calls performed by the principal to see if this behavior is abnormal. It's likely the attacker performed a series of other events before trying to access credentials.



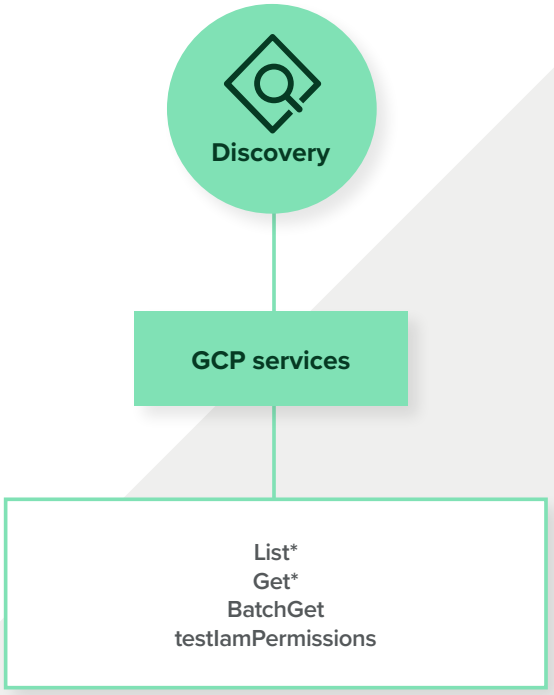
- `~/.config/gcloud/credentials.db`
- `~/.config/gcloud/legacy_credentials/[ACCOUNT]/adc.json`
- `~/.config/gcloud/legacy_credentials/[ACCOUNT]/.boto`
- `~/.credentials.json`

Locations of secrets stored in plain text that require root access to view.

MITRE ATT&CK tactic:

Discovery

- **Why attackers do it:** To discover and enumerate sensitive information about the GCP environment.
- **How attackers usually execute it:** GCP IAM.
- **Look for these API calls:** List*, Get*, BatchGet, testIamPermissions, iam service-accounts list, projects get-iam-policy
- **Investigation tips and tricks:** Automated reconnaissance typically occurs in bursts and can be noisy in audit logs. Investigate the principal to see if these API calls are in line with expected behavior. A time series of API calls can be helpful when determining if these API calls are expected.



* represents a wildcard that can be substituted for several GCP APIs

MITRE ATT&CK tactic:

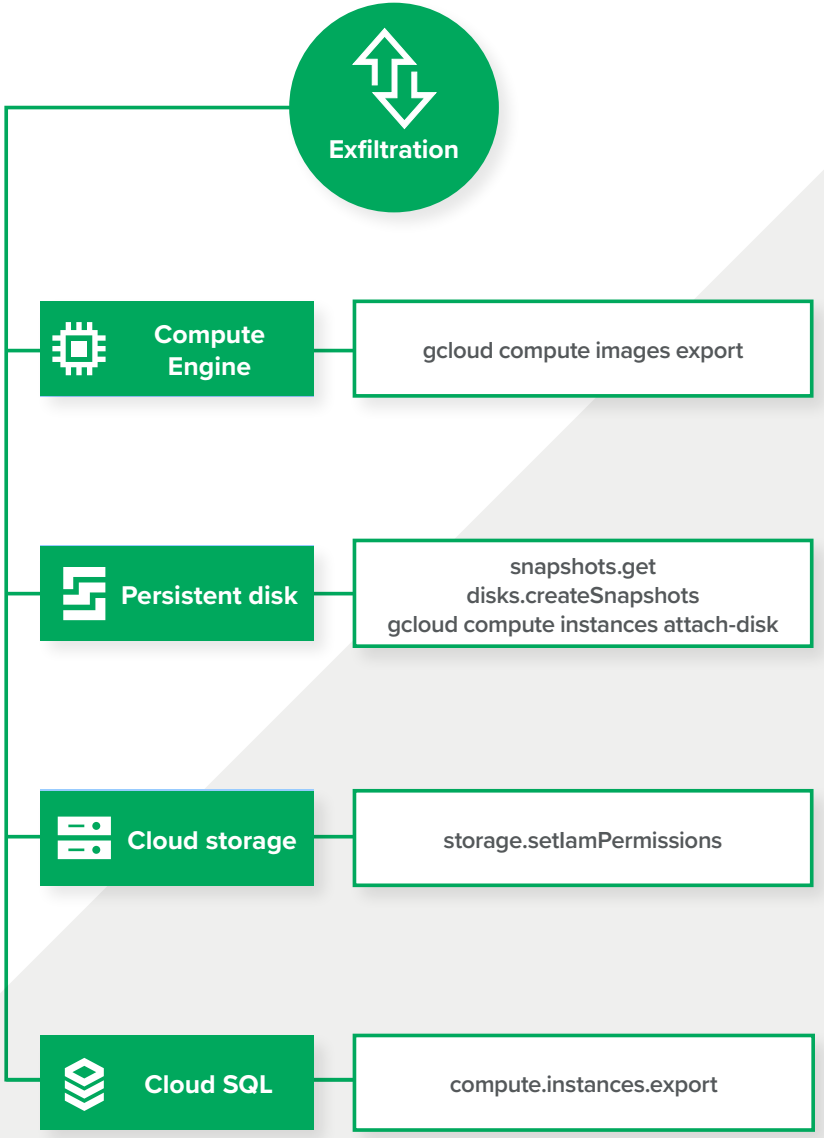
Collection

- **Why attackers do it:** To collect sensitive data from GCP resources and services. Attackers typically exfiltrate collected data to their own infrastructure.
- **How attackers usually execute it:** GCP services.
- **Look for these API calls:** snapshots.get, disk.createSnapshots
- **Investigation tips and tricks:** Look out for any data collection from disk snapshots. Investigate the principal to see where it authenticated from and if it typically interacts with these GCP services to collect sensitive information. A review of historical audit logs for these resources and API calls can also provide insight into whether or not this is expected activity.

MITRE ATT&CK tactic:

Exfiltration

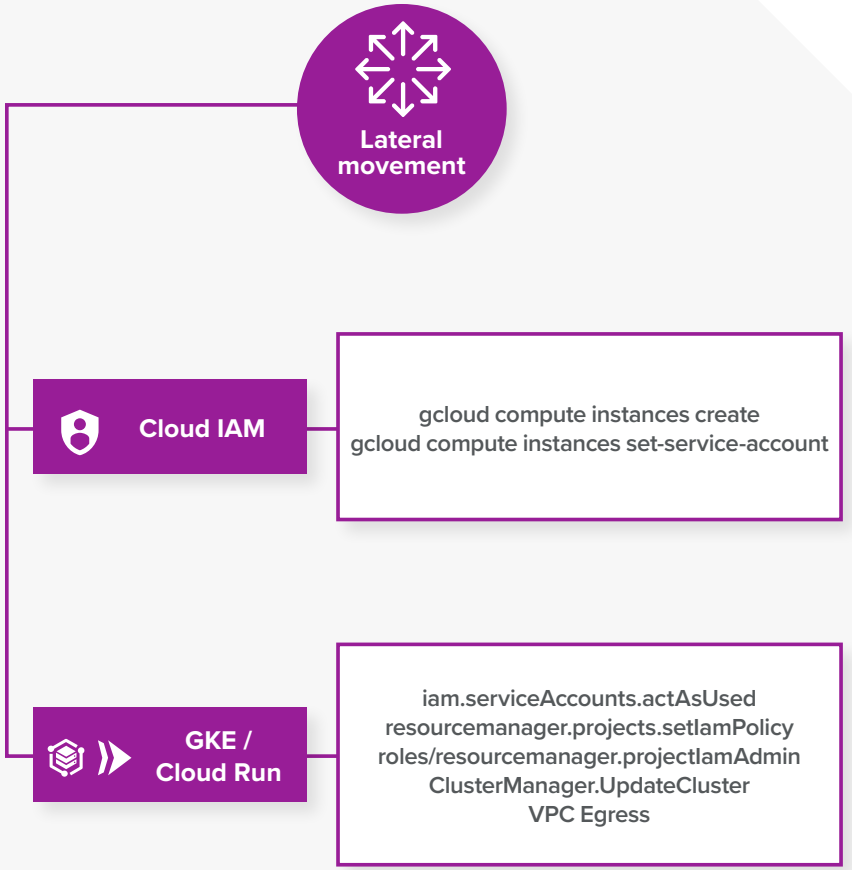
- **Why attackers do it:** To remove sensitive information and data from the GCP environment to attacker-controlled infrastructure.
- **How attackers usually execute it:** Compute Engine, persistent disk, cloud storage and cloud SQL.
- **Look for these API calls:** gcloud compute images export, snapshots.get, disk.createSnapshots, gcloud compute instances attach-disk, storage.setIamPermissions, compute.instances.export
- **Investigation tips and tricks:** Look out for abnormal changes to IAM, image snapshots, and gcloud computer services that would allow the attacker to copy, move, or make the resources publicly available—especially if there isn't a known business need. If you spot suspected exfiltration, investigate the principal's previous API calls, source and method of authentication, along with user-agent string to see if this is in line with normal behavior.



MITRE ATT&CK tactic:

Lateral Movement

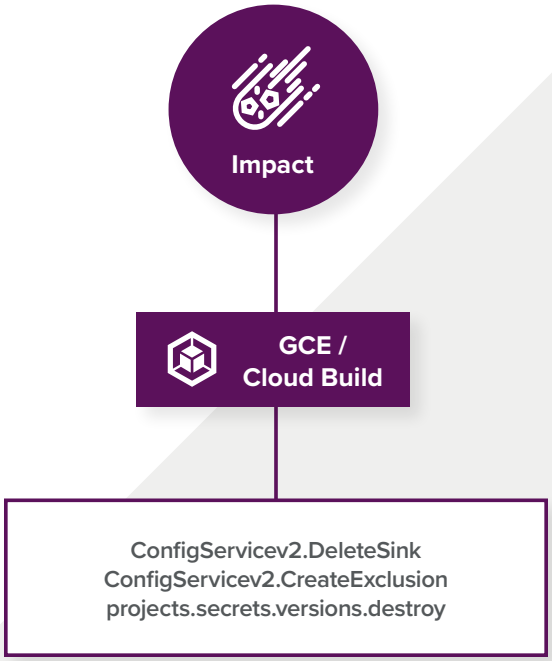
- **Why attackers do it:** To traverse a GCP environment, broaden their attack surface, and expand their reach.
- **How attackers usually execute it:** IAM, Resource Manager and firewall/VPC.
- **Look for these API calls:** iam.servceAccounts.actAsUsed, resourcemanager.projects.setIamPolicy, roles/resourcemanager.projectIamAdmin, ClusterManager.UpdateClustergcp, VPC Ingress
- **Investigation tips and tricks:** Watch for abnormal changes to IAM, policy modifications, and firewall or VPC modifications that can allow the attacker to access additional resources in your environment. If you spot evidence indicative of lateral movement, investigate the principal's previous API calls, source and method of authentication, along with user-agent string, to see if this is in line with normal behavior.



MITRE ATT&CK tactic:

Impact

- **Why attackers do it:** To cause harm, interrupt, or destroy resources in a GCP environment.
- **How attackers usually execute it:** Service Configurations and Cloud CLI.
- **Look for these API calls:** ConfigServicev2.DeleteSink, ConfigServicev2.CreateExclusion, projects.secrets.versions.destroy
- **Investigation tips and tricks:** Look for evidence of data destruction or impairment to configuration services. If you spot evidence of data destruction or suspicious configurations, investigate the principal's prior activity in your environment. Impact occurs late in the attack lifecycle; understanding what actions the suspect principal performed is vital to containment and remediation efforts.



(this is the last page)

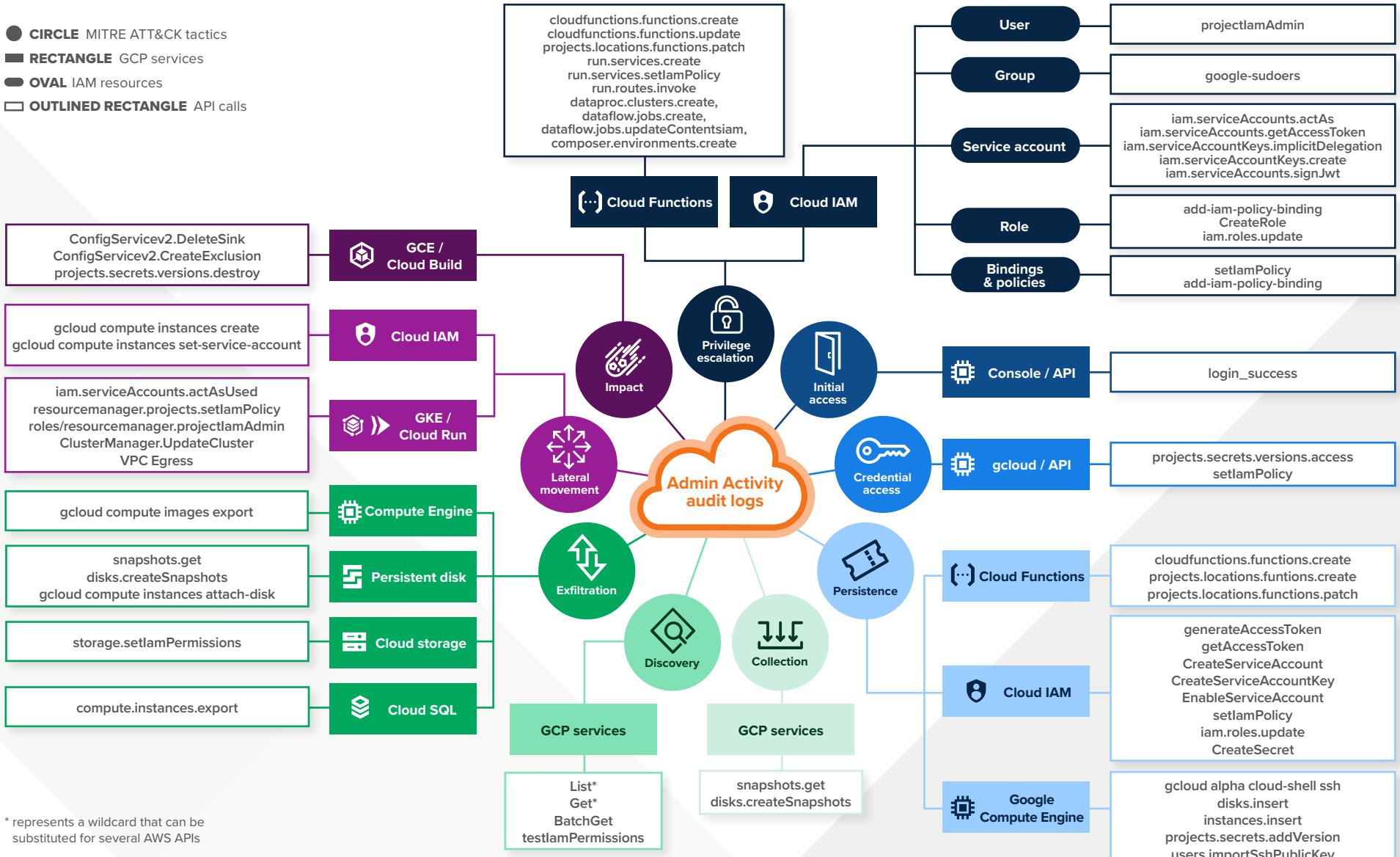
Expel helps companies of all shapes and sizes minimize business risk. Our technology and people work together to make sense of security signals—with your business in mind—to detect, understand, and fix issues fast. Expel offers managed detection and response (MDR), remediation, phishing, and threat hunting. For more information, visit our website, check out our blog, or follow us on LinkedIn or Twitter.

GCP mind map for investigations and incidents

MITRE ATT&CK tactics

expel

CIRCLE MITRE ATT&CK tactics
RECTANGLE GCP services
OVAL IAM resources
OUTLINED RECTANGLE API calls



* represents a wildcard that can be substituted for several AWS APIs

www.expel.com

Create your own GCP mind map

MITRE ATT&CK tactics