509.4

Google Workspace Forensics and IR

SANS | GIAC CERTIFICATIONS

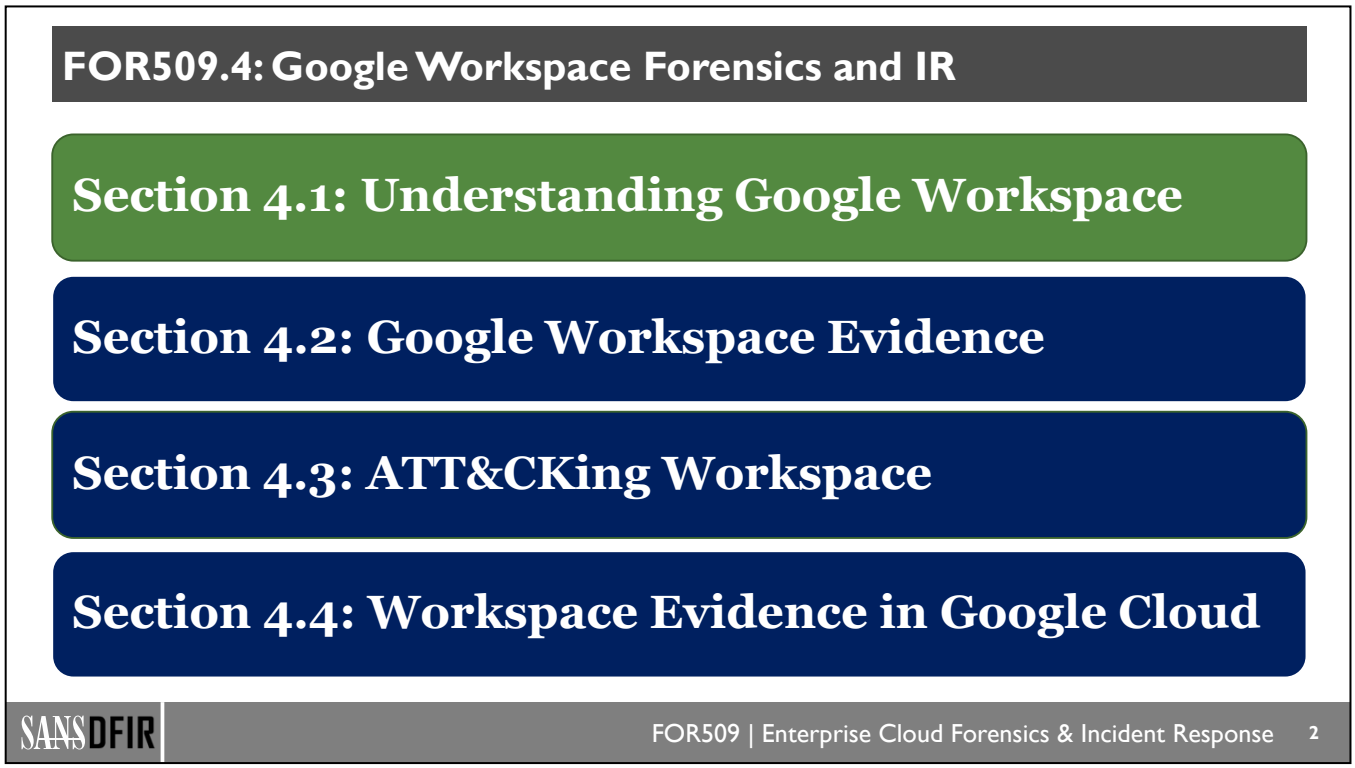
THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

All reference links are operational in the browser-based delivery of the electronic workbook.

FOR509.4 Enterprise Cloud Forensics and Incident Response

Google Workspace Forensics and IR

This page intentionally left blank.



This page intentionally left blank.

Google Workspace Forensics and IR Roadmap

4.1: Understanding Google Workspace

4.2: Google Workspace Evidence

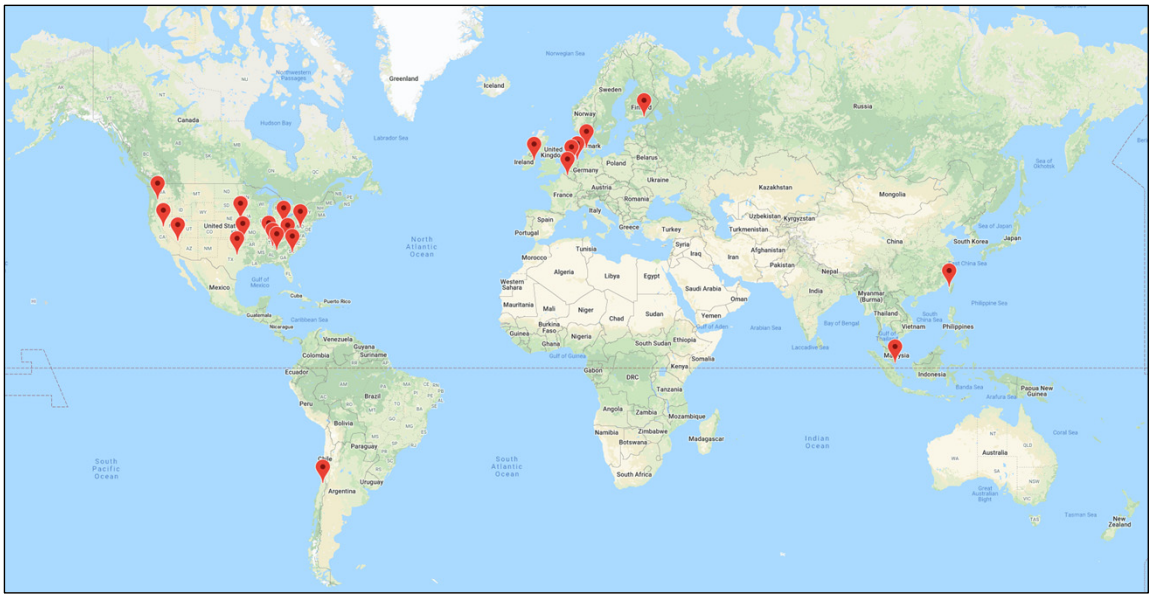
4.3: ATT&CKing Workspace

4.4: Workspace Evidence in Google Cloud

- Google's Footprint and Shared Responsibility
- History of Google Workspace
- Google Workspace Services
- Workspace Editions, Permissions, and Structure
- Google Workspace Groups & Permissions

This page intentionally left blank.

Google's Global Footprint (1)



Google Workspace has data centers distributed around the globe in North America, South America, Europe, and Asia. [1] When you set up a new Google Workspace instance it is defaulted to a global data region. This means the data that you store within Google Workspace could be distributed among any of Google's data centers.

If you require your data for Google Workspace to be held in a specific region you get the choice of either the United States or Europe.[2] You will notice that because of these two options that Google has many data centers concentrated in both regions. Being able to specify which region your Google Workspace data is held within is also dependent on the licensing type that you have for Google Workspace.

Regardless of if you choose Globally Distributed, United States, or Europe for your data to be hosted, there is no functionality difference with the services offered within Google Workspace.[3]

1. https://for509.com/8b7fn (Google Data Centers)
2. https://for509.com/7jyl3 (Data regions: Choose a geographic location for your data)
3. https://for509.com/st2wu (Data regions)

Google's Global Footprint (2)

Google Workspace Regions

- By default, Workspace will store data globally distributed around the world.
- Workspace offers two specific regions if needed:
  - United States
  - Europe
- Using specific regions can cause latency issues for users outside of the region.
- Data extraction for DFIR can be slower when organizations are using specific regions.

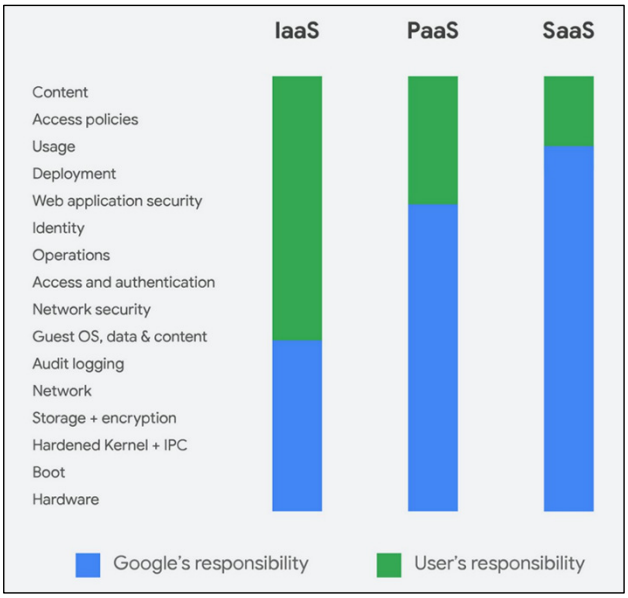
Google Workspace has data centers distributed around the globe in North America, South America, Europe, and Asia. [1] When you set up a new Google Workspace instance it is defaulted to a global data region. This means the data that you store within Google Workspace could be distributed among any of Google's data centers.

If you require your data for Google Workspace to be held in a specific region you get the choice of either the United States or Europe.[2] You will notice that because of these two options that Google has many data centers concentrated in both regions. Being able to specify which region your Google Workspace data is held within is also dependent on the licensing type that you have for Google Workspace.

Regardless of if you choose Globally Distributed, United States, or Europe for your data to be hosted, there is no functionality difference with the services offered within Google Workspace.[3]

1. https://for509.com/8b7fn (Google Data Centers)
2. https://for509.com/7jyl3 (Data regions: Choose a geographic location for your data)
3. https://for509.com/st2wu (Data regions)

Google's Shared Responsibility



Shared Responsibility

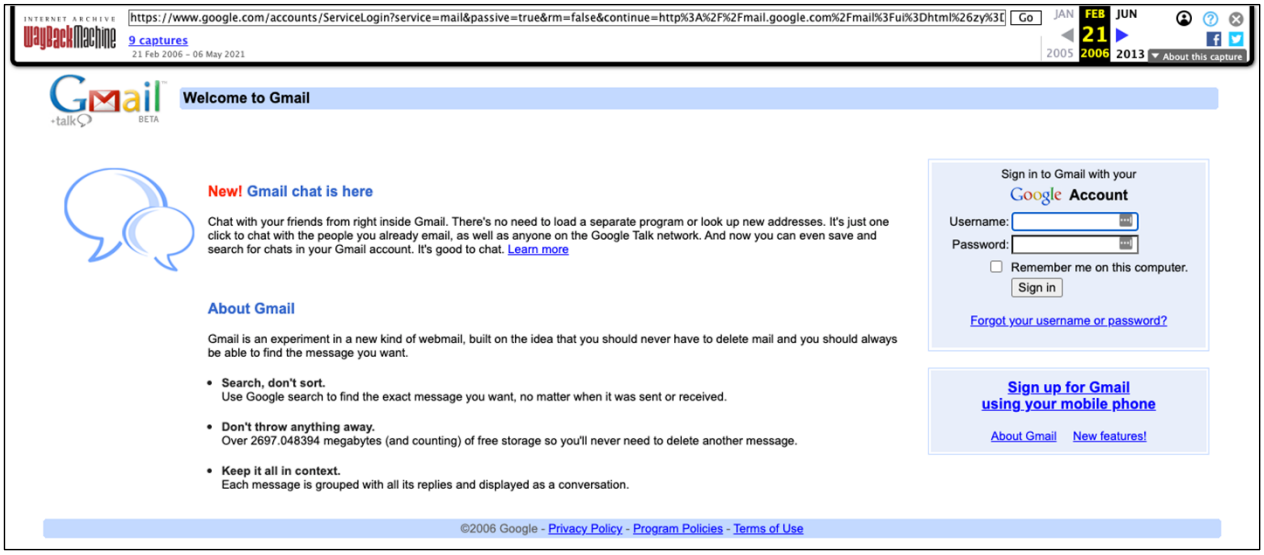
- Google uses a similar shared responsibility model already shown with Microsoft and Amazon
- For DFIR professionals, Google looks after logging as soon as you move to their platform
- Other security services, useful for DFIR, don't become available until you move to PaaS and SaaS

Like the other providers discussed previously in this class, Google also uses the concept of shared responsibility,[1] where the customer takes part of the responsibility of running, operating, and protecting parts of their system, regardless of whether it's IaaS, PaaS, or SaaS.

From a digital forensics perspective, we get the benefit of logging as soon as we move into Google Workspace and Google Cloud, regardless of what type of *aaS we're using. However, more useful security monitoring and protection features become available when we use PaaS and SaaS. While we aren't going into detail of SaaS in this section, we'll look at it further in future editions of this class when Google Workspace is introduced.

1. https://for509.com/knhw6 (Google Workspace data protection implementation guide, December 2020)

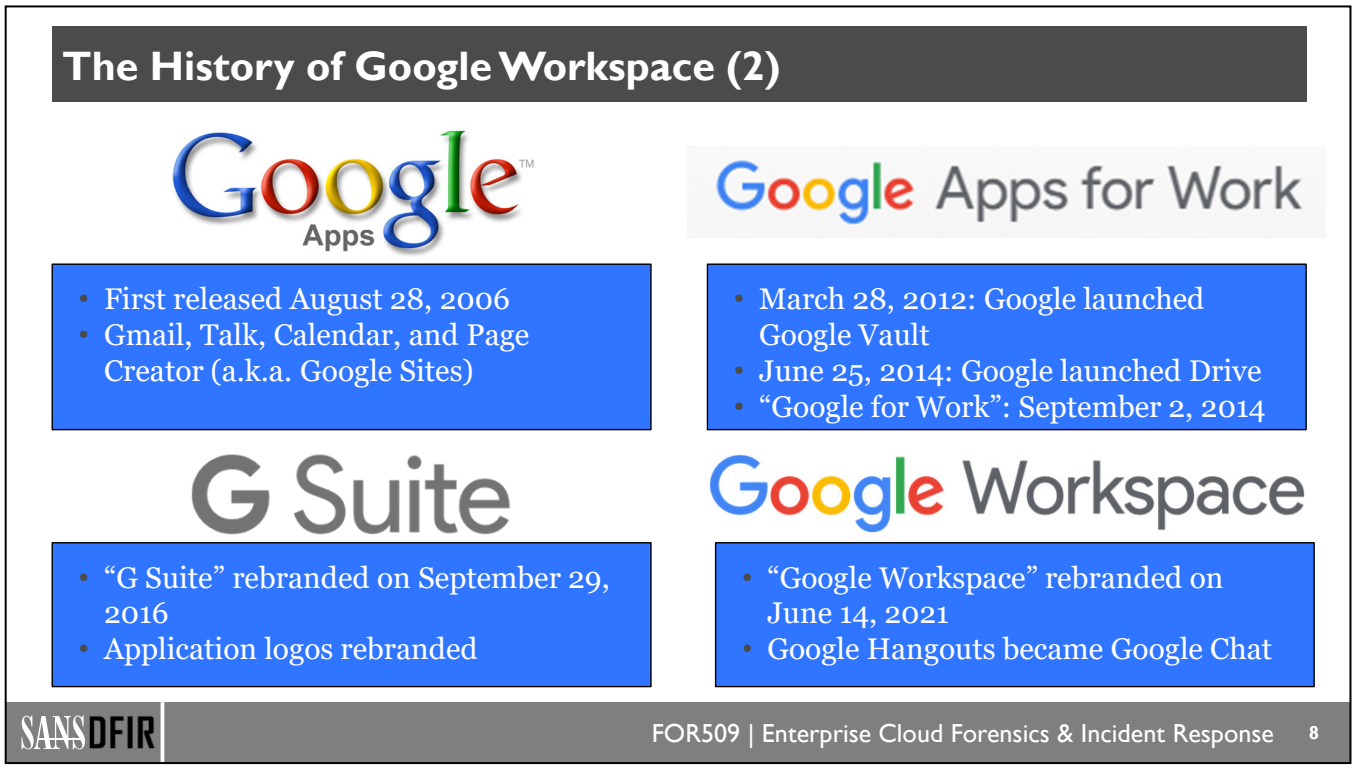
The History of Google Workspace (1)



Google first announced they were offering a commercialized version of their Gmail platform back on February 10, 2006, for students in San José City College where they started testing a hosted version of Google's Gmail platform. This was the first time Google branched out their online offering to a third party to host their corporate email, although in this case it was only student email for college.[1]

The image above[2] shows what Google looked like back on February 21, 2006. Since this time Gmail, and the business services offered by Google, have significantly changed.

1. https://for509.com/frtx0 (Big Mail On Campus)
2. https://for509.com/f6gwk (Internet Archive Wayback Machine)



Following the testing done on a college in San Jose City, Google released their first commercial version of Google Apps[1] in August 2006. At the time Google Apps didn't include anywhere near the level of services offered today, but it did include services such as Gmail, Talk, Calendar, and Page Creator, which later became Google Sites. It was also in 2006 that Google announced an edition specifically for education institutions. The inclusion of an education edition has been something Google has stuck with since their initial creation back in 2006.

In early 2007, Google also announced a premier edition of Google Apps. This was intended as a business-level addition separate to the free offering that was offered in 2006. Not only was it a paid version of Google Apps, but it also included additional storage space and guaranteed SLAs when it came to using Google Apps.

In 2010, Google also introduced the Google apps marketplace that provided third-party business applications to integrate with Google Apps. In the same year they also introduced the government edition of Google Apps, known as "Google Apps for Government".

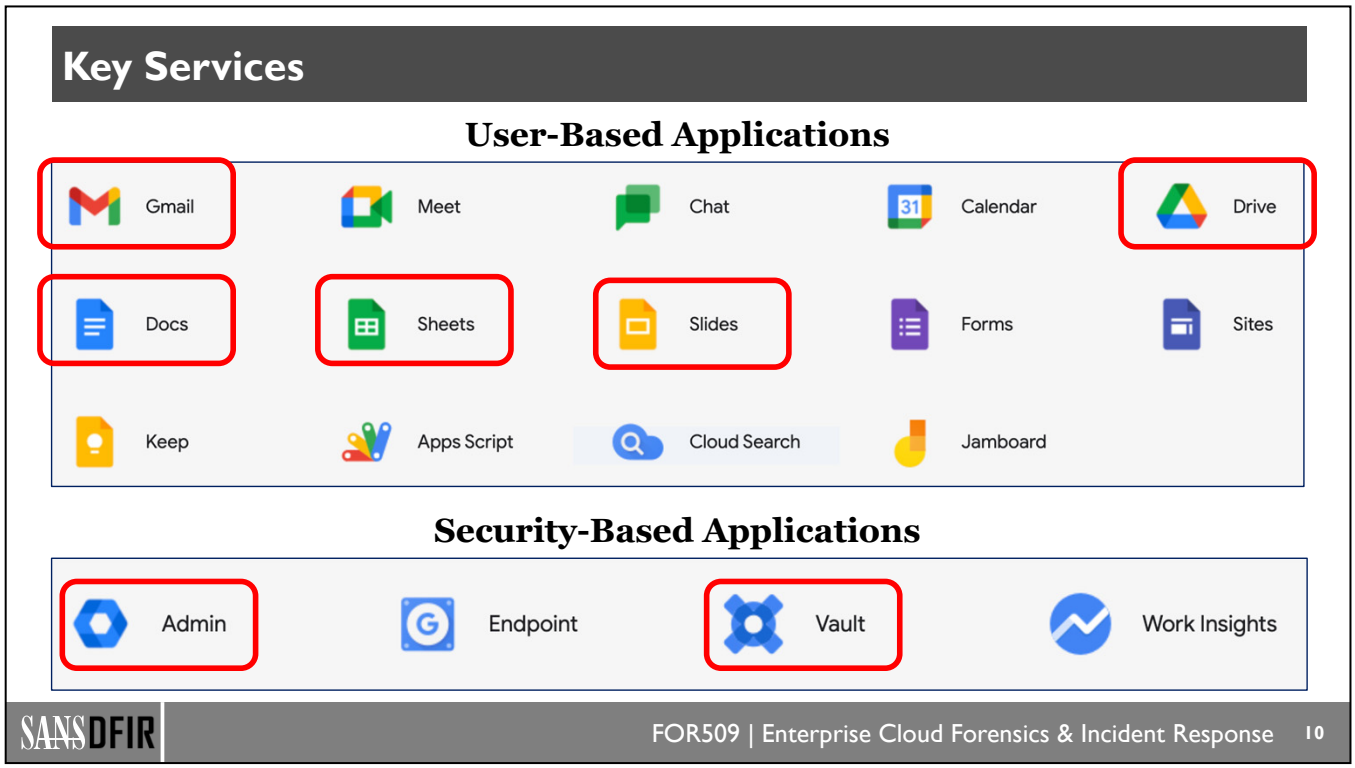
In early 2012, Google launched the first version of Google Vault to provide eDiscovery services for uses of Google Apps. It was later this year that Google also introduced Google Drive to provide online storage.

In late 2014, Google announced a rename of their Google Apps that was being used by Enterprises to now be called Google for Work. Google again rebranded Google Apps to G Suite in late 2016.[2]

In mid 2021, Google also changed the way that a lot of the chat functionality worked, providing a more integrated service for users. This was likely part of their response to providing better services for remote workers during the COVID-19 pandemic. During this time, they also rebranded it again to be Google Workspace.[3]

In early 2022, Google finally announced that their free legacy addition of G Suite will be deprecated. This will see the end to any legacy free Google Workspace accounts after the middle of 2022.

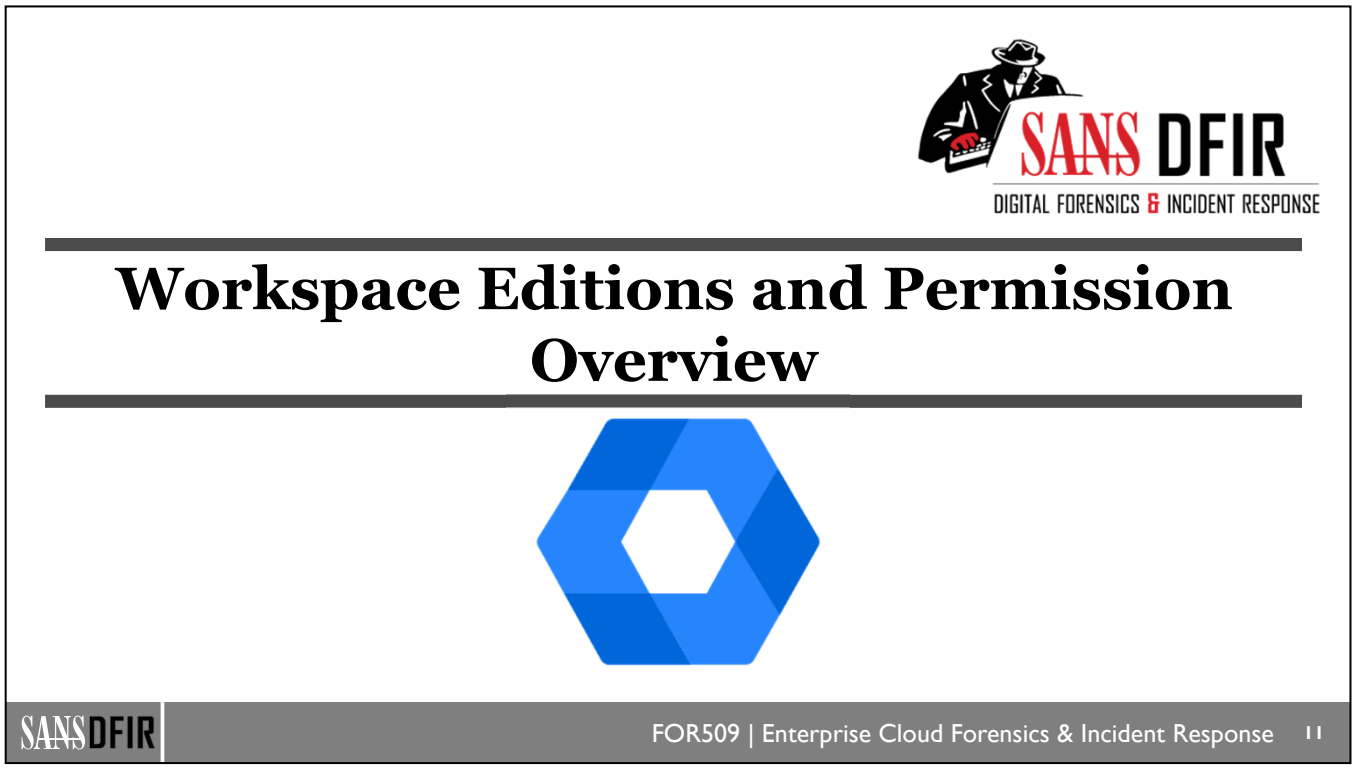
1. https://for509.com/1edim (Wikipedia: Google Workspace)
2. https://for509.com/nbgur (Introducing G Suite)
3. https://for509.com/9weul (Google Workspace Transition)



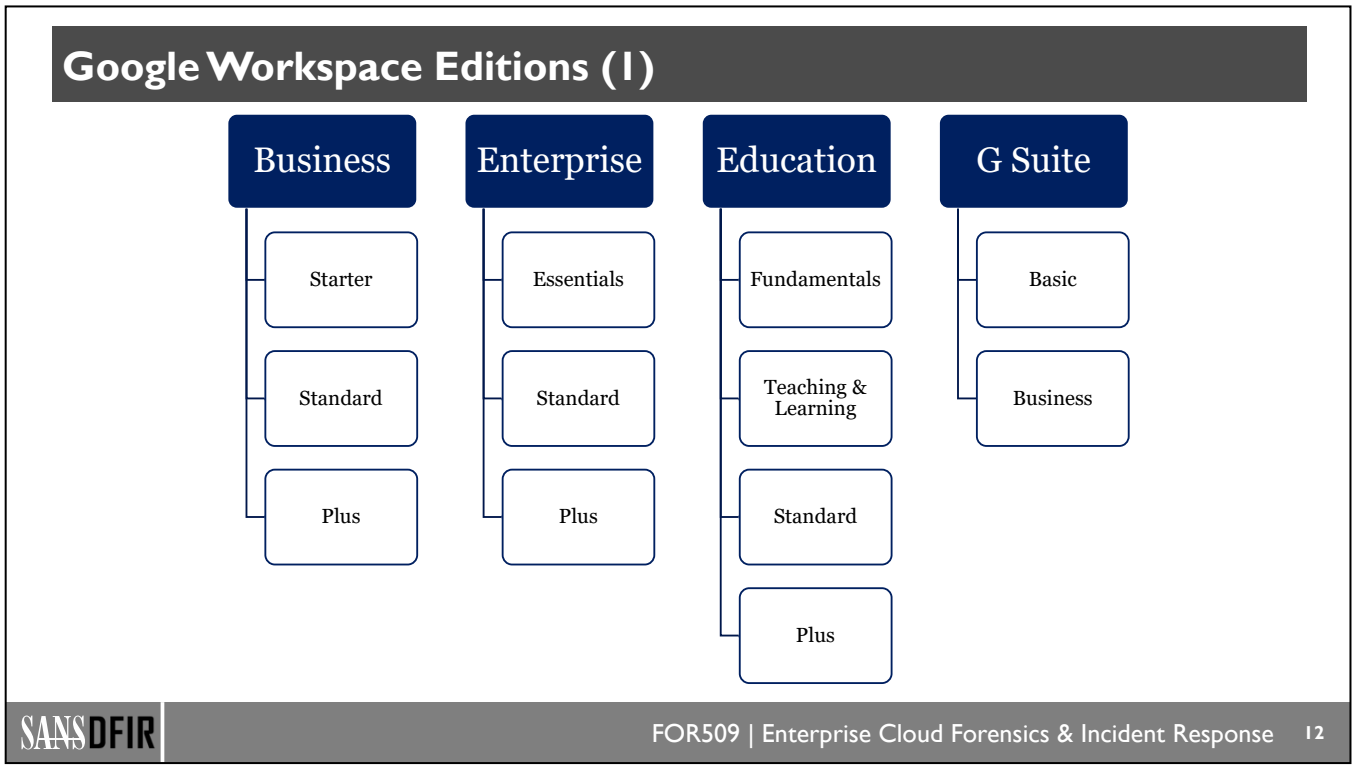
Google Workspace has a growing number of built-in applications. Thankfully, over time Google has also added in security features to assist in protecting these applications or to assist investigators trying to collect evidence from these applications. Throughout this section we will focus on some of the key applications used by most organizations and the key areas within Google Workspace that provide us evidence when conducting investigations. For the most part this will be the security-based applications; however, we will limit the security-based services we look at to those which provide useful information for digital forensics and incident response.

Reference:

https://for509.com/hai6y (Workspace Features)



This page intentionally left blank.



Google Workspace provides a significant amount of flexibility between the base license that you purchase when setting up Google Workspace and add-ons that you can add on top of that base edition. Due to this, there is a significant number of different configurations that can exist for Google Workspace. In this slide we've tried to show you the common editions and the sub-editions that exist within each of the categories offered for Google Workspace. This is by no means an exhaustive list; however, it should prove useful to give you an understanding of how the various editions within Google Workspace are structured.

The different editions that are provided with Google Workspace also come different features. In some cases, this can increase, or decrease, the amount of visibility you might have when it comes to collecting evidence for digital forensics and incident response. Through this section we will focus on the Enterprise edition[1] as it is the most used by organizations. While we will not go into detail about the other editions, understand that the Business edition[2] does not have the same level of visibility that is offered in both the Enterprise and Education[3] editions of Google Workspace.

1. https://for509.com/r5jxl (Compare Enterprise editions)
2. https://for509.com/tfng5 (Compare Google Workspace editions)
3. https://for509.com/lc3pj (Compare Education editions)

Reference:

https://for509.com/tdhq5 (Compare G Suite Basic and Business editions)

Google Workspace Editions (2)

Starter/Essential	Standard	Plus
• Basic • Limited Logging for User and Admin Actions • No Drive Logging • No Audit Reports • Limited Data Protection	• Complete Audit Logging • DLP *(Enterprise Only)*	• Vault • Device Management *(Business Only)* • Increased Security Features • LDAP Features • Increased Size/Users

The above table is intended to give you an understanding of the differences between Starter or Essential, Standard, and Plus which are all sub-editions underneath the primary license types offered by Google Workspace. Of most significance, from an incident response and digital forensics perspective, is that the Starter or Essential editions do not provide very much visibility in the way of logging or capturing evidence from email. It's only when organizations use the Standard edition that they will start to get access to detailed Logging.[1] Visibility increases even further with the Plus addition which gives access to Vault that we will look at later in this section.[2]

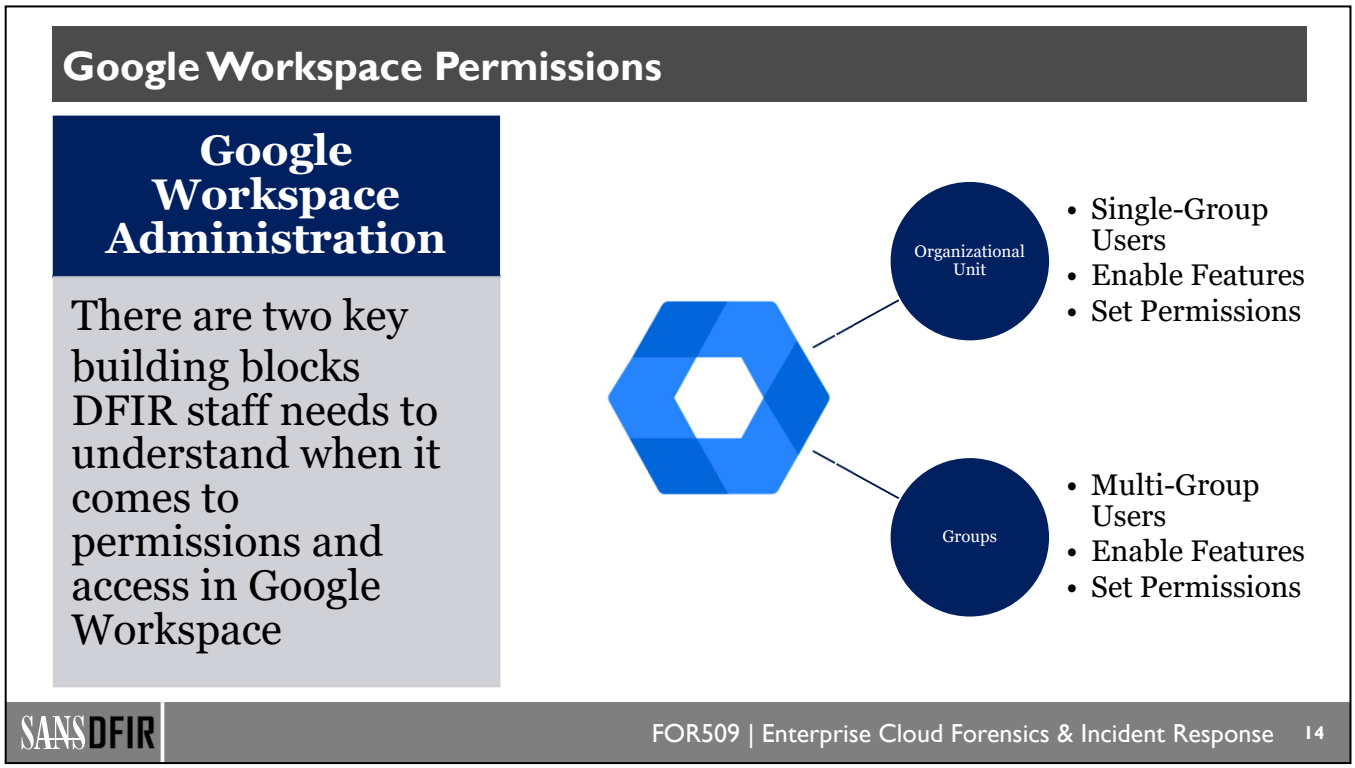
There are also additional security-based features that are included within the Plus edition that are not specifically relevant to incident response ad digital forensics but are useful for protecting an organization and providing automated alerting to try and detect a security incident ahead of time.

The functionality provided within the Education edition licensing has been excluded from the above table as it is vastly different in terms of the functionality provided in all the subcategories for the licensing that accompanies the Education edition license. Without going into specific details for the Education edition, it essentially has more functionality in the lower tiers of the sublicensing compared to the commercial versions of Google Workspace. To understand the features provided within the Education edition of Google Workspace, you can use the link below.[3]

1. https://for509.com/tfng5 (Compare Google Workspace editions)
2. https://for509.com/r5jxl (Compare Enterprise editions)
3. https://for509.com/lc3pj (Compare Education editions)

Reference:

https://for509.com/tdhq5 (Compare G Suite Basic and Business editions)

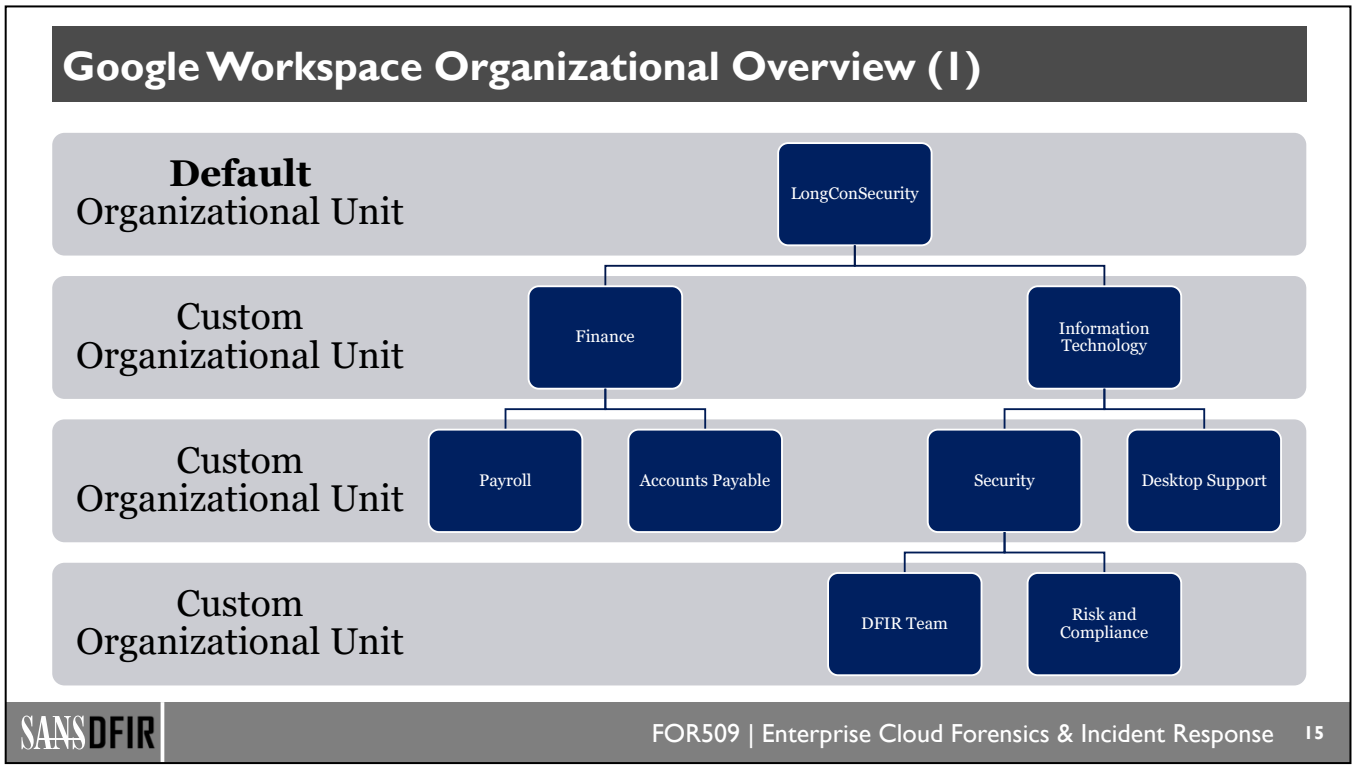


Google Workspace has its own built-in authentication and identity management service; however, when it comes to permissions within Google Workspace there are two fundamental building blocks that we need to understand from a digital forensics and incident response perspective. These are Organizational Units and Groups, both of which provide the ability to add additional permissions to users and to enable or disable features and functionality within Google Workspace. Furthermore, both could be used independently to apply different permissions sets to different users. Understanding how permissions work within Google Workspace is important when it comes to understanding abuse of accounts or investigating accounts that have been compromised.

A user account can only exist with a single **Organizational Unit**. From the investigation perspective, once you have identified the Organizational Unit that a user exists within, you would not have to look for user account within any other Organizational Units. As you will see in the upcoming content, Organizational Units can be embedded underneath each other. A user can exist only once in an Organizational Unit; however, they could exist anywhere from the top, middle, or bottom of an embedded Organizational Unit.[1]

A user account can exist within multiple **Groups**. To further complicate things with groups, a group can exist with inside another group as well. Groups, inside of Google Workspace, are commonly used as a streamlined way of applying permissions to a group of user accounts. This is similar to how Security Groups are used within Microsoft Active Directory. Because a user can exist within multiple groups and groups can be also be embedded within each other, a user account can easily mistakenly end up with permissions that were not intended by the administrator of Google Workspace.[2]

1. https://for509.com/h8uf9 (Add an organizational unit)
2. https://for509.com/x4idb (Create a group & choose group settings)



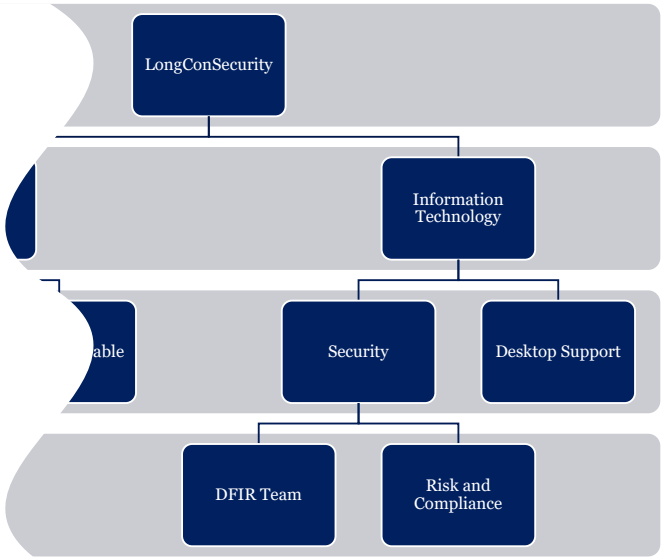
Google Workspace has a default Organizational Unit that every new user is put into by default. A Google Workspace account does not require more than a single default Organizational Unit. However, Organizational Units can be particularly helpful in grouping common uses together for better management or policy enforcement. They can also be grouped together in hierarchy similar to what is shown on this page.

Reference:
https://for509.com/501z2 (How the organizational structure works)

Google Workspace Organizational Overview (2)

Organizational Structure

- All users or devices are put into a single Organizational Unit.
  - If you don't define any they are put into the default Organizational Unit.
- Organizational Units can be embedded under each other.
- Features, or permissions, can be enabled/disabled for each Organizational Unit.
- Child Organizational Units inherit settings. Custom settings to child Organizational Units are not affected by parent settings changes.
- Organizational Units are different to groups.

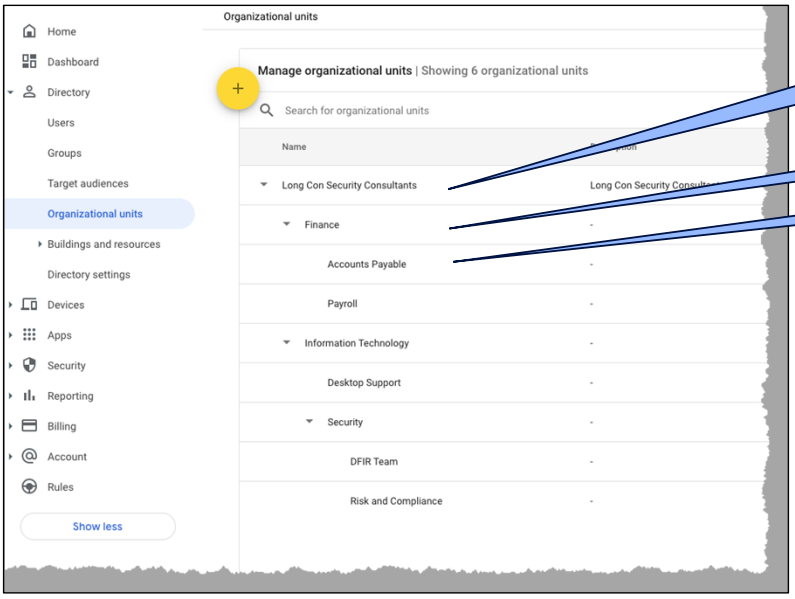


In addition to grouping common user groups together, organizational units can be used to enable or disable features within Google Workspace. This is often used by organizations when they want to provide additional features or to limit features for a specific user group. For example, an organization may choose to limit a user account's ability to be used as a YouTube account or disable the use of Photos in Google Workspace. Limiting features for users is also common practice when a user account is used by a third-party contractor that may not need access to all the features for services provided to full-time employees of an organization.

When Organizational Units are embedded underneath of each other, a unit lower down the embedded tree will inherit from units above it within the inheritance tree. This is important to remember when permissions are applied to Organizational Units.

Reference:
https://for509.com/501z2 (How the organizational structure works)

Google Workspace Organizational Overview (3)



Default Organizational Unit

Custom Organizational Unit

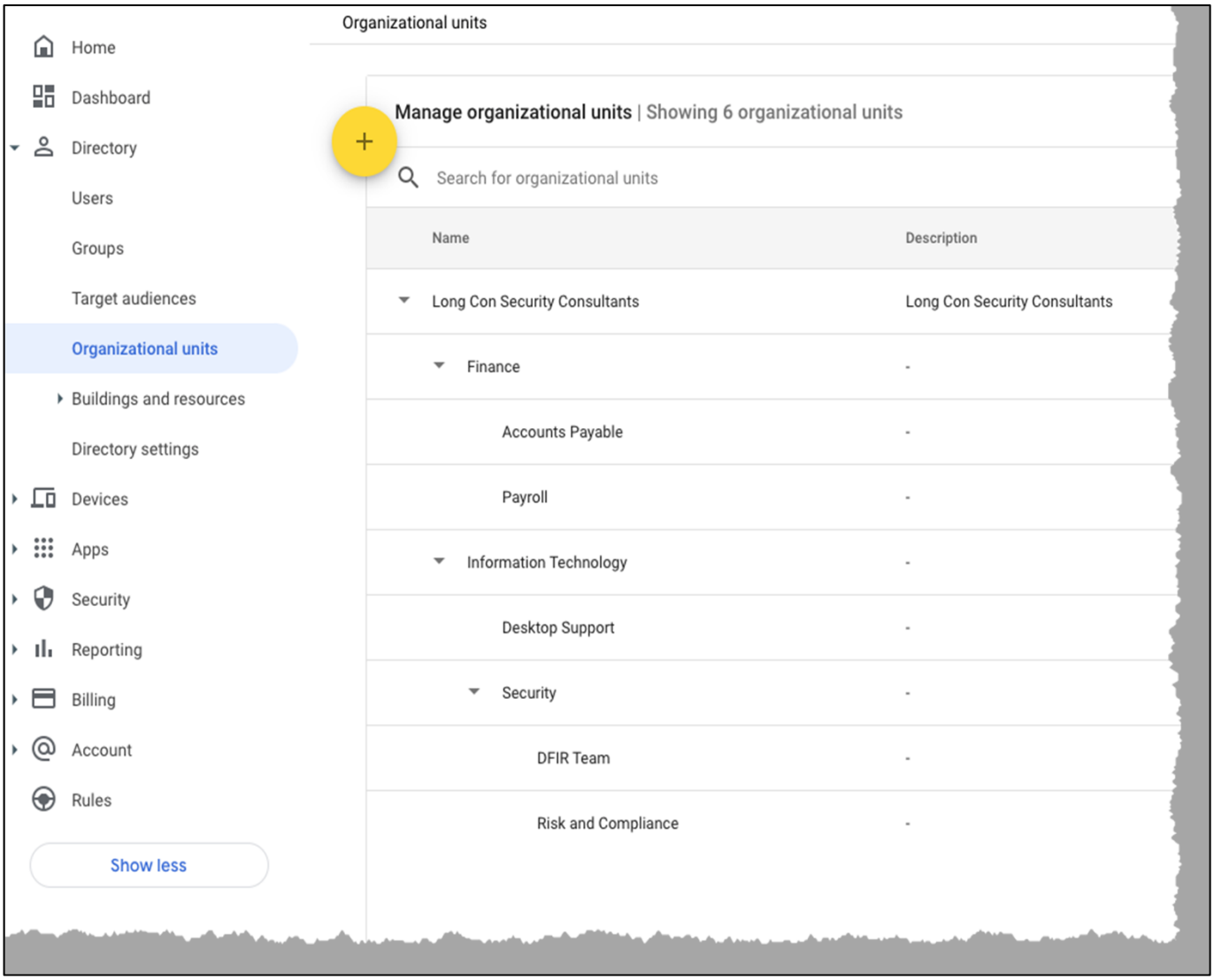
Child Custom Organizational Unit

Organizations

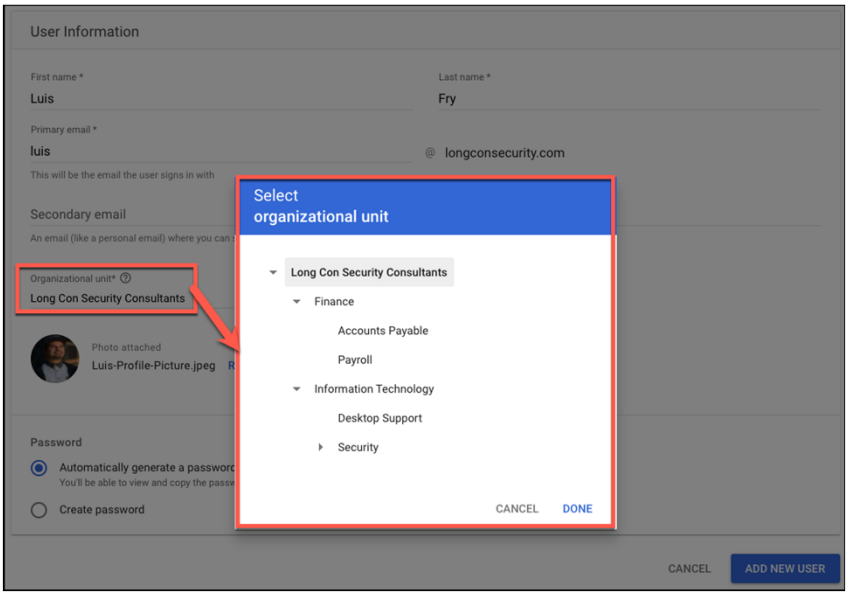
- All changes are made within the **Admin Console**
- Organizational Units are accessed under **Directory**

To determine the organization structure that has been set up inside of Google Workspace, you will need to first access the **Admin Console**. From here you can navigate the **Directory** menu and the **Organizational Units** subdirectory item. Within the **Manage organizational units** section you will find the default Organizational Unit at the top and all the custom and child organizational units listed underneath it. This area inside of Google Workspace will not tell you which users are in each Organizational Unit, but it will give you an understanding of the child and parent hierarchy within Google Workspace.

Reference:
https://for509.com/501z2 (How the organizational structure works)



Google Workspace Organizational Overview (4)

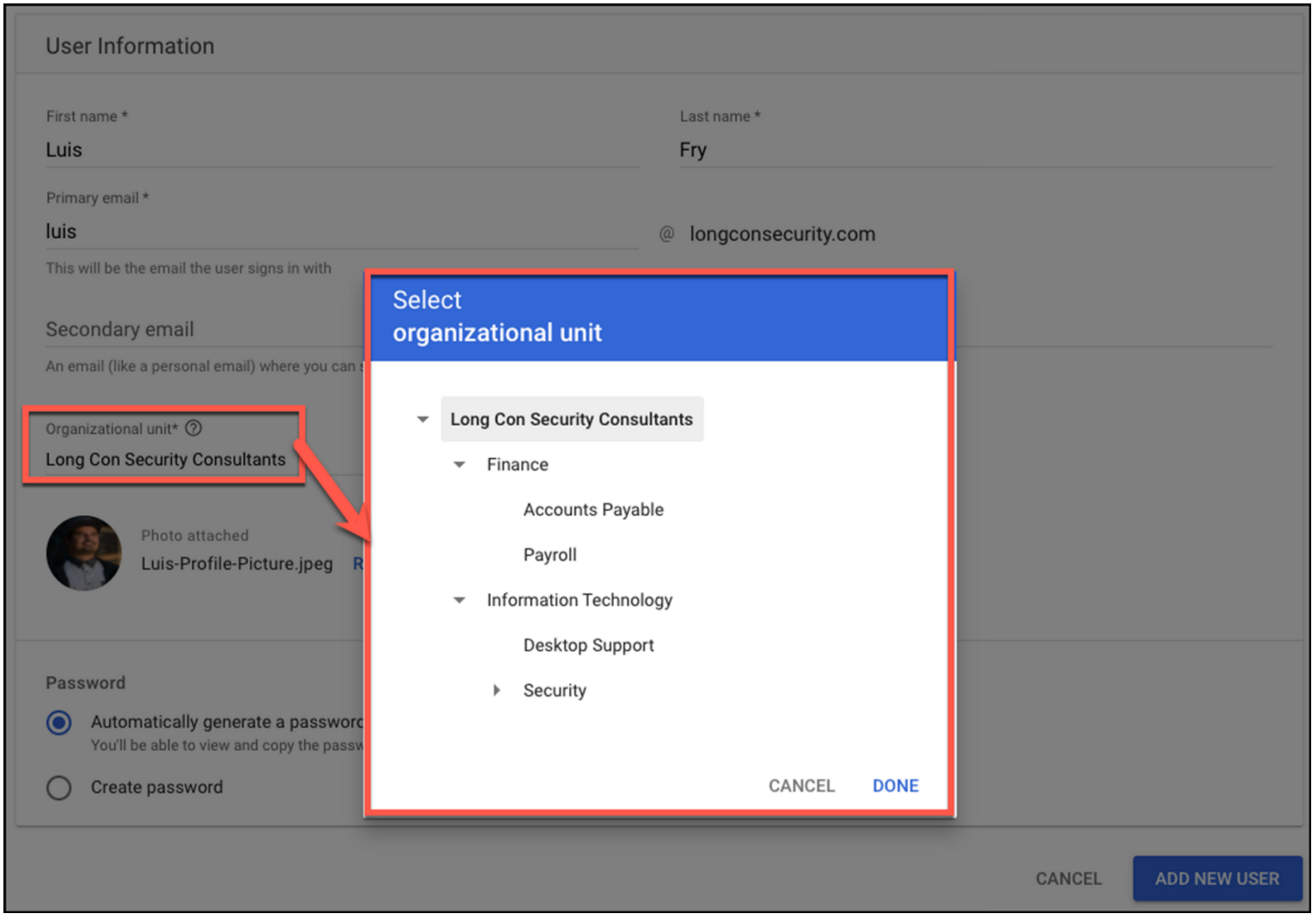


Organizational Units

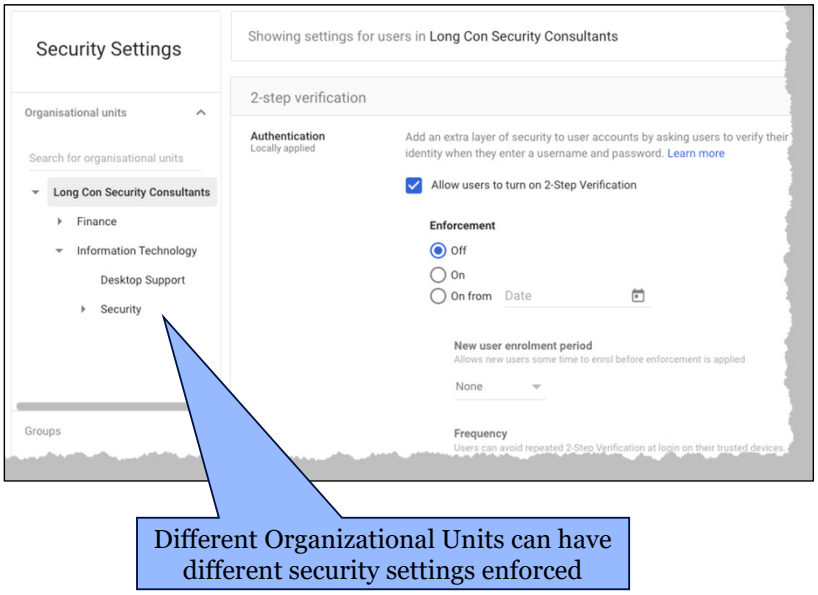
- Users can only exist in one Organizational Unit.
- Organizational Units are added when users are created.
- Organizational Units can be changed at any time.
- The Organizational Unit will default to the highest parent unless changed.

To find out which Organizational Unit that has been assigned to a user account, you would need to look at the user account details inside the Admin Console for Google Workspace. From here, you can also alter the Organizational Unit for the user if you are an organization admin. Generally, when a user account is created you must assign it to an Organizational Unit. If you choose not to, it will be assigned to the default Organizational Unit for the Workspace.

Reference:
https://for509.com/501z2 (How the organizational structure works)



Google Workspace Organizational Overview (5)

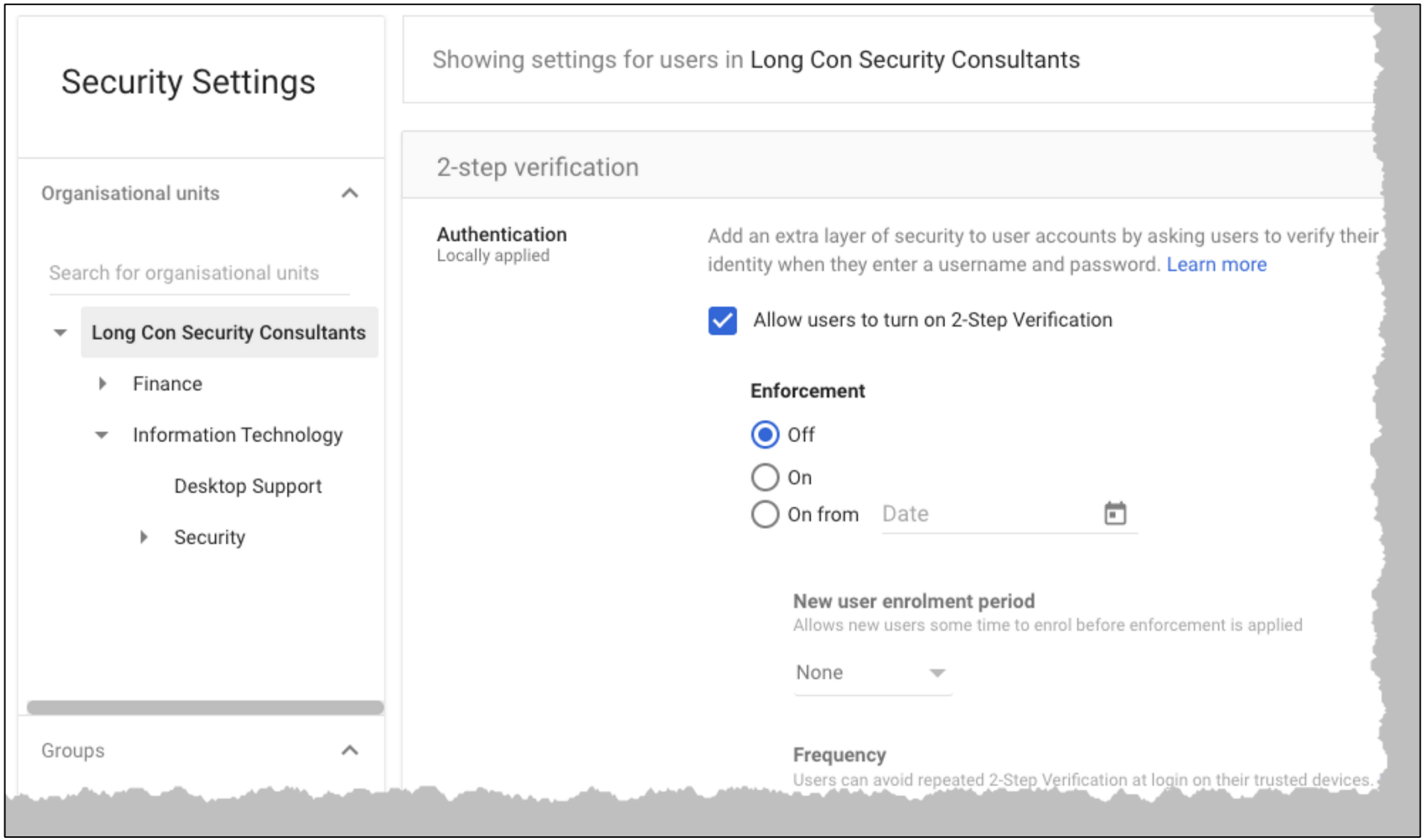


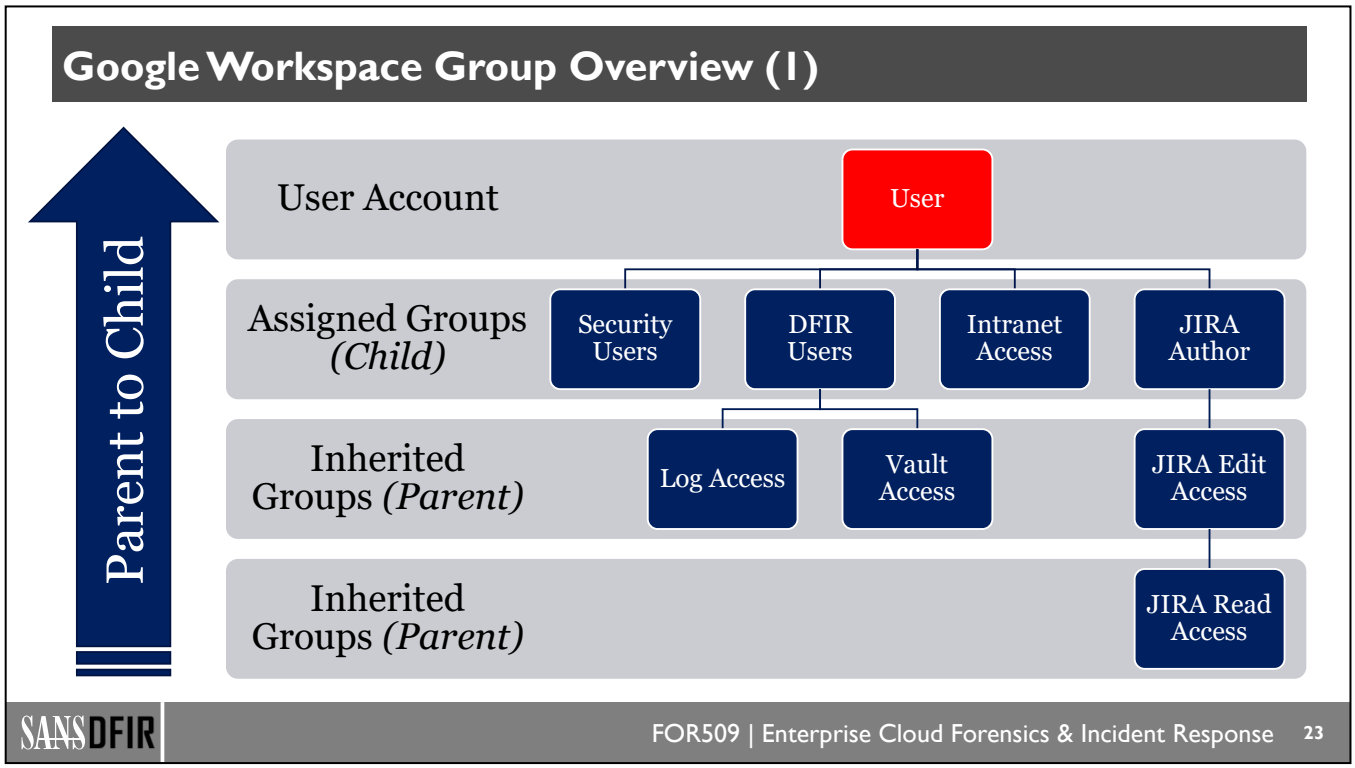
Organizational Units

- Settings within the Workspace Admin console can be applied to different Organizational Units.
- This means users in different Units may have different settings enabled.
- When investigating user accounts check what settings are applied to the Organizational Unit they are within.
- These settings changes are captured in the Admin Log Events.

Within the Google Workspace Admin Console, specific settings can be enforced or relaxed per Organizational Unit. This allows different Units to have slightly different permissions and features. In the above screenshot is the Security Settings area within the Admin Console. You can see that different Units can be selected and have their own Authentication permissions applied. Remember that permissions are inherited from top to bottom, so any changes made at a high Unit will apply to child Units. Although, you can override inherited permissions on child Units.

When investigating a compromised user account, ensure you identify which Organizational Unit the account is within, then, you should check permission or setting changes to their Unit, or simply the permissions that they are granted. Any changes to settings against Organizational Units are logged within the Admin Log Events log, which we'll cover later.





Unlike an organizational unit you can have multiple groups assigned to a single user account. In the example above four user groups have been assigned to a single user account; however, you'll notice that two of those groups also have inherited groups assigned to them.

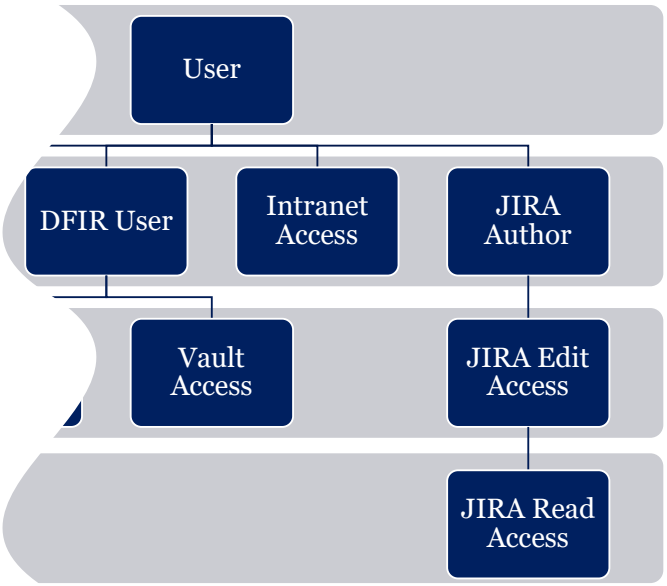
Inherited groups occur when another group is also a member of a group. In the example on this page, the "DFIR Users" group is a member in both the "Log Access" group and the "Vault Access" group. This will result in members within the "DFIR Users" group also inheriting the same permissions that are assigned to the "Log Access" group and the "Vault Access" group. Additionally, you could also have multiple inherited groups, as is the example with the "JIRA" groups shown on this page.

Reference:
https://for509.com/fp2zd (Get started managing groups for an organization)

Google Workspace Group Overview (2)

User Group Structure

- Groups are not mandatory, but they make permissions a lot easier.
- A User can be in many Groups.
- Groups can be embedded under each other.
- Permissions, or features, can be enabled/disabled for each group.
- Child Groups inherit settings from all embedded Parent Groups. Permissions on embedded Groups will flow down from all the Groups embedded above it.
- Groups are different to Organizations.



Groups can be used to assign specific permissions or features or be used as mailing groups. These are very similar to how security groups and mailing groups work inside of Microsoft Active Directory. Unlike an Organizational Unit, groups are not mandatory, and users are not required to be assigned to any groups. The use of groups within large organizations reduces the burden of administration when it comes to new users and quickly assigning permissions to them based on existing groups.

From a digital forensics and incident response perspective, groups can result in users being overprovisioned access by mistake when there are a significant number of inherited groups that get assigned to a single user account. You will see on the next page that this can also be further complicated when ownership of groups is assigned to one administrator user.

Using groups to configure permissions and features for users can have its advantage for digital forensics and incident response staff. Consider that you could have three groups set up that provide different levels of sharing access for Google Drive. These could be set up so that one group may only allow for internal sharing of documents on Google Drive, another may allow for sharing to only trusted domains, and the third could be set up to allow sharing with anyone outside the Organization. Using groups this way can make it quicker and easier to alter which user groups are allowed to share documents inside a Google Drive and could help get a data exfiltration incident under control quickly. This doesn't only apply to Google Drive; it can apply to all the features available in Google Workspace.

Reference:
https://for509.com/fp2zd (Get started managing groups for an organization)

Google Workspace Groups: Permission Model

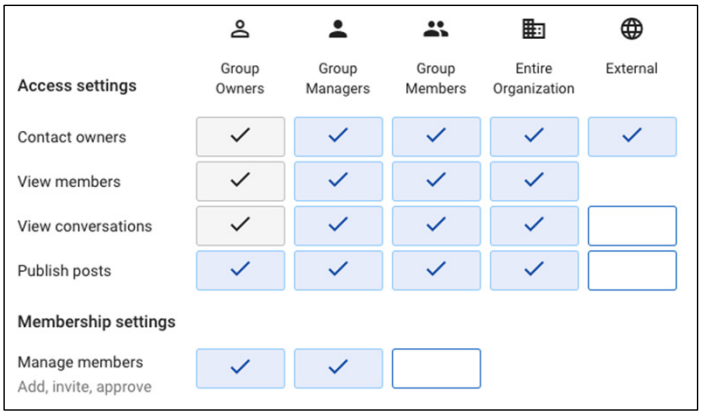
Google Workspace Groups allow for fine grain control over permissions. It also allows Users to set/change/add permissions.

User Types

- Group Owners
- Group Managers
- Group Members
- Whole Organization
- External to Organization

Permissions

- Contact Owners
- View Members
- View Conversations
- Make Posts
- Add New Members



Above is an example of a Public Group's default permissions.

Groups inside of Google Workspace have three primary types of members: an Owner, a Manager, and a Member. All of these member types can have multiple users assigned to them. These primary member types define who has control over a group. This often involves who can add members to the group or approve new member requests. It is important to understand that it's not always an organization administrator who is assigned an owner of a group. It's not uncommon to find group owners are leaders that represent the user group for the users inside of that group. Often this means that new members can be added to the group quickly and easily by someone that is a trusted person that's part of that group. As an investigator this is something that you need to be aware of, especially when it comes to groups that allow for high-level permissions to be assigned.

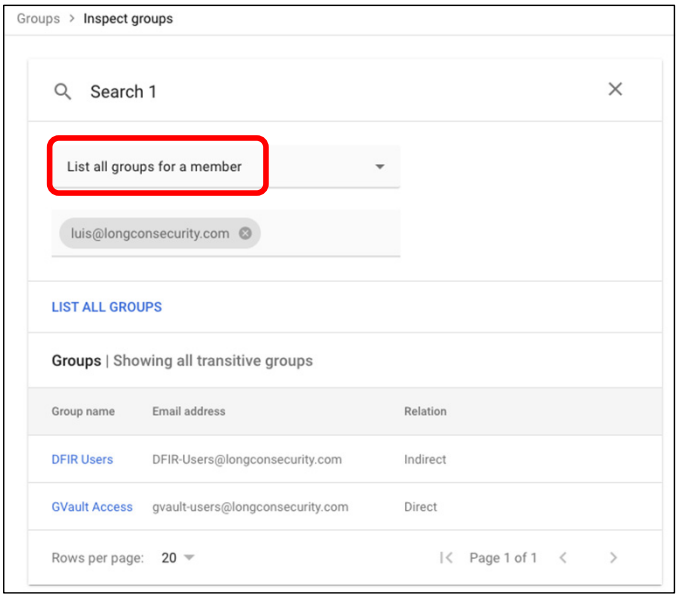
You can also define how anyone outside of the group, but still part of organization, can view or access details of the group, along with anyone outside of the Google Workspace Organization and how they can interact with the group as well. Google Workspace also provides the ability to set up dynamic groups, which allows for users to be automatically assigned to a group based on details within the user account in the admin console. Details on how dynamic groups work are provided below in the references section.

References:

https://for509.com/3jc76 (Assign roles to a group's members)

https://for509.com/hpkmg (Customize service settings with configuration groups)

Google Workspace Groups: Inspecting Groups (1)



Inspect Groups

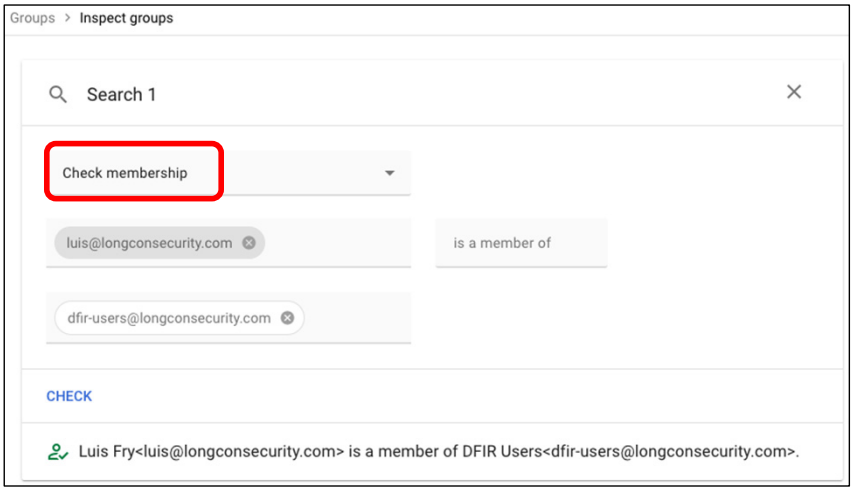
- Workspace Admin allows you to check **what Groups a User is in**.
- This is useful for checking multi-inheritance for embedded groups.
- "Indirect" shows a Group the user is within, based on another Group that inherits the "Indirect" Group.
- This is taken from the example shown previously.

Within the Google Admin Console there is the ability to inspect users and groups assigned to them, or the users that have been assigned to a group.[1] This can make it much quicker to understand if a user account has been misused permissions and groups that user account is a part of. Additionally, the Inspect Groups function will also tell you if a group has been inherited or if the user was directly assigned to the group.

In the example provided on this page, we can see that the Luis user account was directly assigned the "Vault Access" group and that the "DFIR Users" group was indirectly assigned to the user account as well, as it would have been inherited via another group.

1. https://for509.com/t93bw (Track group information in the Groups list)

Google Workspace Groups: Inspecting Groups (2)

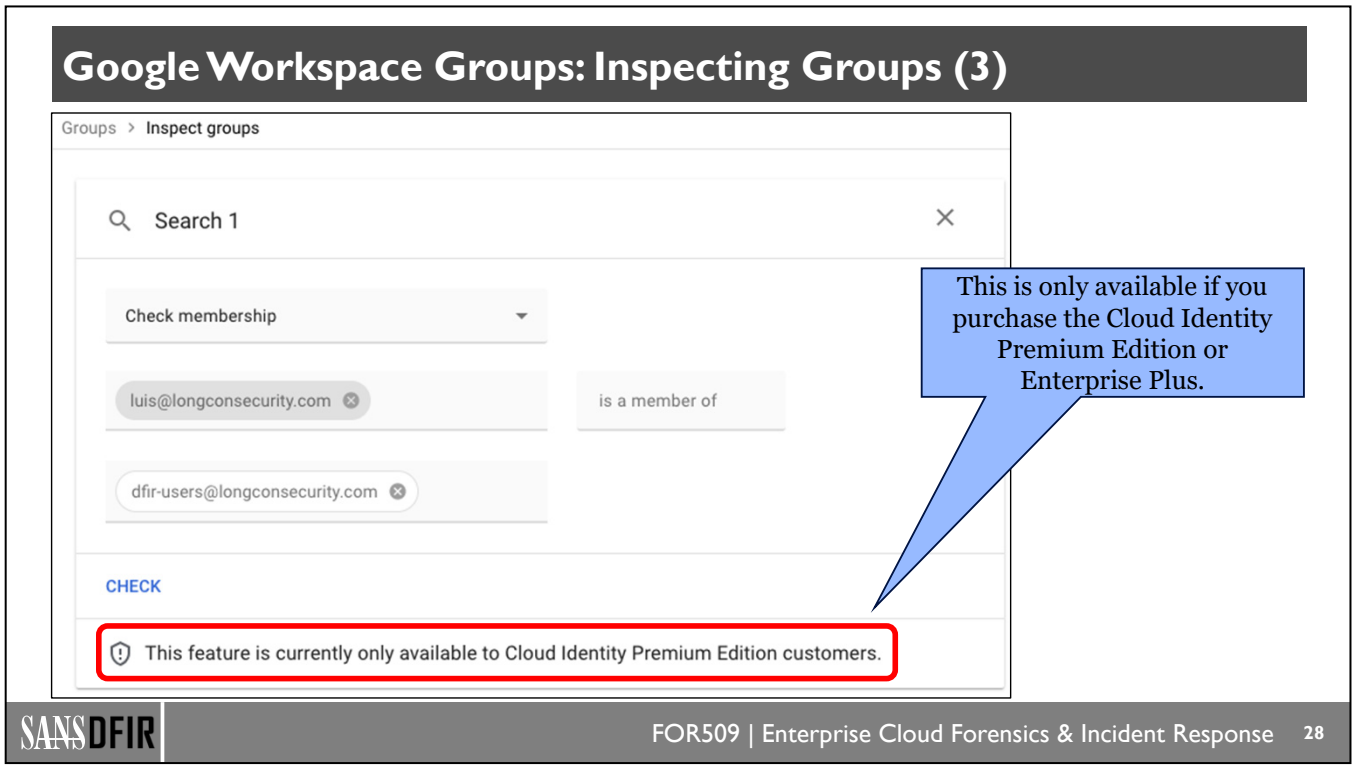


Groups

- Workspace Admin allows you to check Users within Groups.
- This is useful for verify if a user has Group permissions based on inheritance for embedded groups.
- This is only available if you purchase the Cloud Identity Premium Edition.

Inspect groups provides a number of different search options as well as the ability to verify that a member is inside of a group as well.

Reference:
https://for509.com/t93bw (Track group information in the Groups list)



The ability to quickly identify what groups a user is in and what users are within groups is only available within the Enterprise Plus edition or with the Cloud Identity Premium Edition add-on to any of the other base subscriptions. The Cloud Identity Premium Edition add-on provides a number of useful functions within the admin console for digital forensics and incident response staff. For organizations that do not have a need for the Enterprise Plus edition of Google Workspace, using the Cloud Identity Premium Edition add-on is a cheaper way of getting some of the more advance identity and access management, and security features, that are not available in the lower tier editions of Google Workspace.

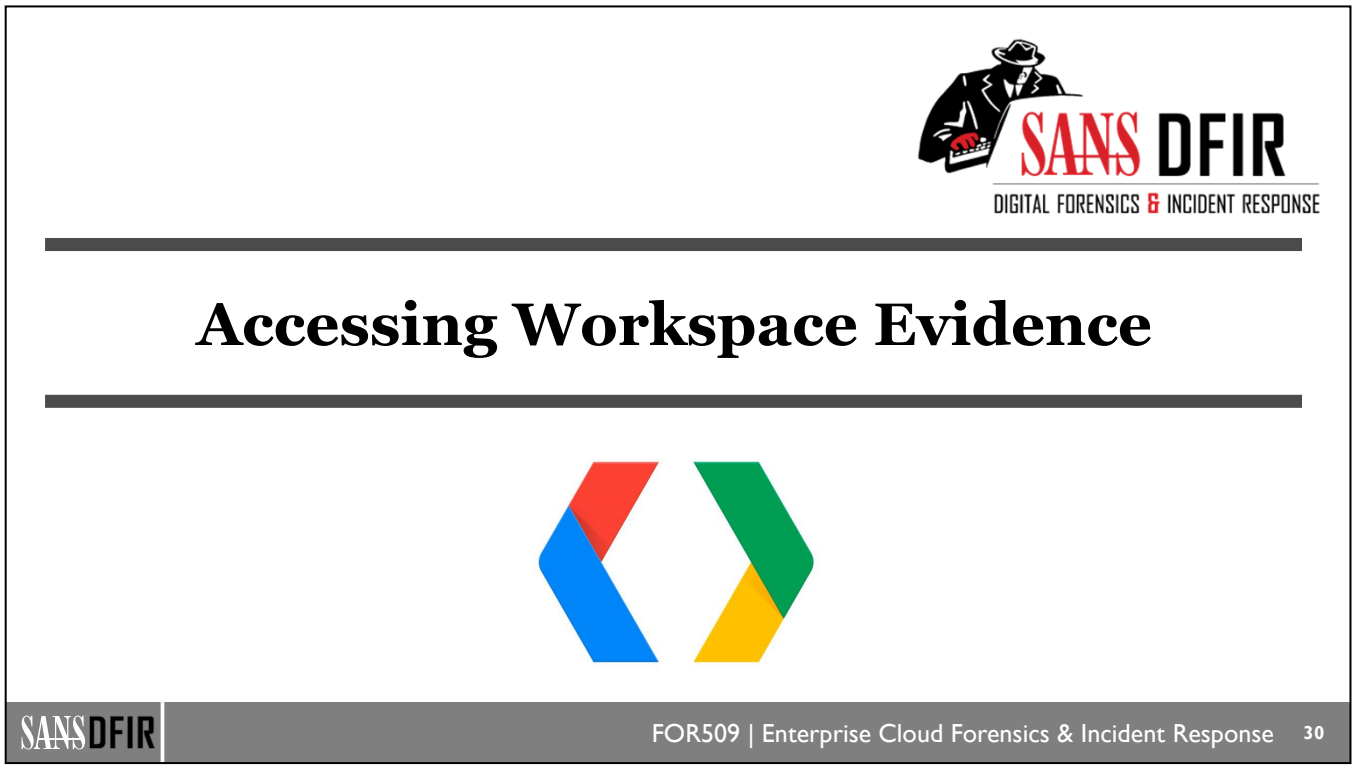
References:
https://for509.com/tdrei (Cloud Identity)
https://for509.com/dz3bn (Compare Cloud Identity features & editions)

Google Workspace Forensics and IR Roadmap

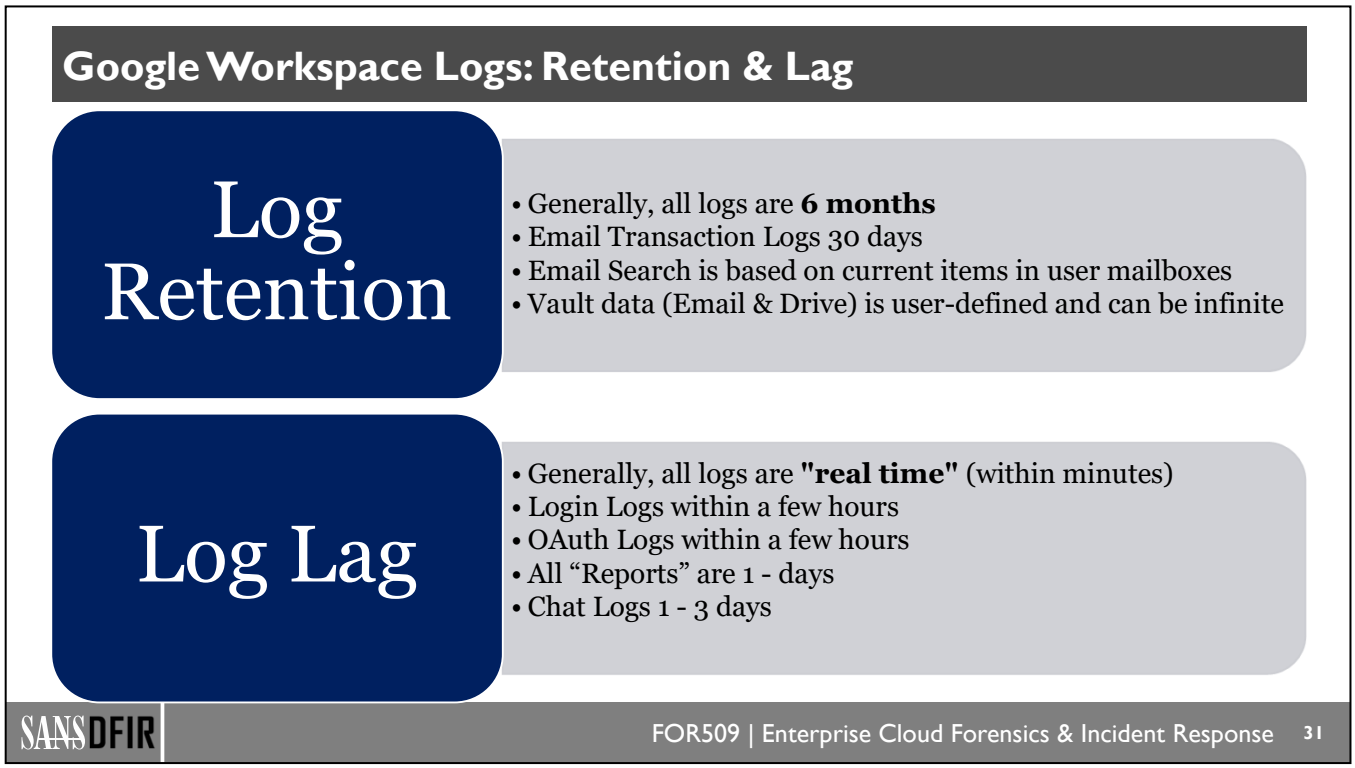
- 4.1: Understanding Google Workspace
- 4.2: Google Workspace Evidence
- 4.3: ATT&CKing Workspace
- 4.4: Workspace Evidence in Google Cloud

- Workspace Admin Logs and SDK
- Collecting Logs from Workspace
- Workspace Admin Audit Logs
- Sending Workspace Logs to Google Cloud
- Setting Up Access for API Log Collection
- Collecting Logs via API

This page intentionally left blank.



This page intentionally left blank.



Google Workspace generally holds all logs for 6 months and usually provides these logs in near real time, which usually means they are available for exporting or searching within a few minutes. There are exceptions to these rules for some specific log times.

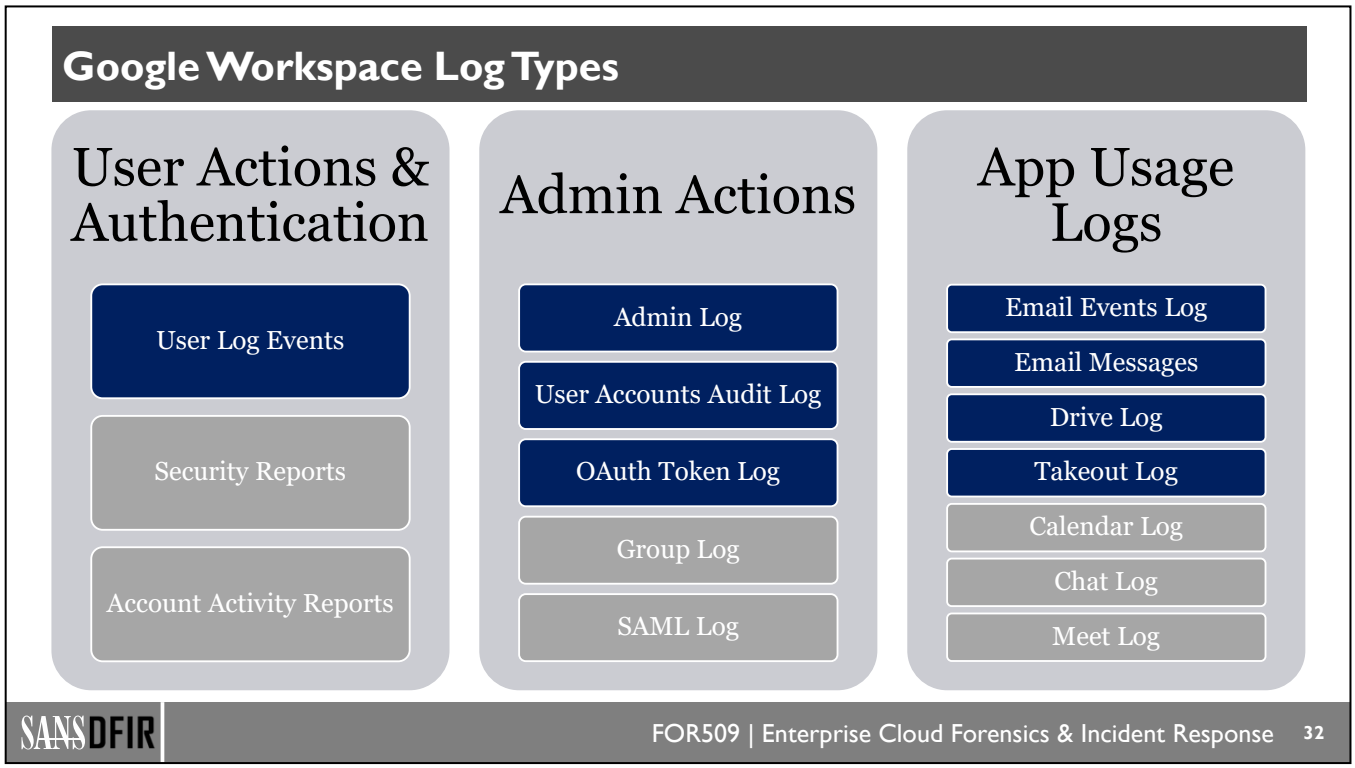
When it comes to Email transaction logs, they are only held for 30 days due to the number of logs generated, however, this information can be obtained from email header information if an email was delivered to a user mailbox. There is also the possibility with Google Vault to retain all emails permanently, or for a user-defined timeframe. More details on email logs are provided in a later section.

The log lag, or delay on when logs are made available is generally real time, however there are exceptions to this. Of significant note to investigations are the Login Logs which could be delayed by a few hours, similar with the OAuth Token Logs. Additionally, any information within the Admin Console that produces a "Report" should be considered delayed by 1-3 days. The Report delay is due to the reports being based on information within a whole Organization, for example, consider that the reports maybe based of data in every users Drive or Email, this can take considerable time to generate. While we don't cover them in this section, the Chat Logs in Workspace are also delayed by 1-3 days.

Within the admin console, there is no way to extend the lifetime of these logs. The only way to extend the lifetime of these logs is to send them into Google Cloud and extend their retention period while they are stored within Google Cloud. Google Cloud has a maximum limit of 10 years for storing logs.

Reference:

https://for509.com/fngm6 (Data Retention and Lag Times)



There are a large number of different log types within Google Workspace which are all documented within their support pages[1]. This slide contains some of the more important log types that DFIR investigators commonly use or need to be aware of. The log available can generally be calorized into;

- User Actions and Authentication that occur with the use of a user account
- Administrative Actions that occur within the Admin Console and with permissions that users have
- Application Usage Logs that show what actions a user has performed while using Google Workspace

Additionally, the log types that are blue above are specifically covered in sections of this course.

Previously, Google merged a log known as the Login Audit Log and the User Accounts Audit Log into a single log now called the User Log Events. There is still some legacy documentation within Google's support pages that will reference these older log names.

Remember that the logs above all have slightly different lag times before they are available for users to search or extract. It is also worth understanding that these lag times should be considered as the minimum time required before you start searching events within the logs. This is because some events within logs can arrive faster than others. Furthermore, Google recently combined the Login Audit Log and the User Accounts Audit Log into the User Log Events, however, there is still a different lag between Login events and User Account events. During our testing of Google Workspace, we observed password resets arriving prior to a login event for the user when we conducted searches shorter than the lag time of log events. For this reason, we recommend that no searches should be relied upon that are run shorter than the lag times.

1. https://for509.com/fngm6 (Data Retention and Lag Times)

Workspace Admin Logs and SDK

Accessing Log Evidence

- DFIR within Workspace primarily consists of event timeline collection and direct evidence collection.
- To create a timeline of Workspace events we are reliant on logging.
- Workspace provides you two keyways to access logs:
  - **Workspace Admin Interface**
  - **API** via the Workspace Admin Console SDK
- There are two types of API data sets we will commonly use for DFIR:
  - **Activity Reports:** for specific Workspace Applications (i.e., Gmail, Drive, etc.)
  - **Usage Reports:** for events related to user accounts

When it comes to collecting evidence for Google Workspace there are two primary data sets that we can access and use as evidence. These are the reports that I provided inside of the Workspace admin interface—all the logs that are made available via the Workspace admin console API.[1] When it comes to using either of these data sets, they both provide the same fundamental information; however, there are a few small differences between the two of them that would impact forensic analysis.

The other significant difference between these two sources of evidence is the speed in which we can collect the evidence in the format that both these evidence sources produce. Although fundamentally these are two different sources of evidence, within both of them there are also subsets of evidence as well.

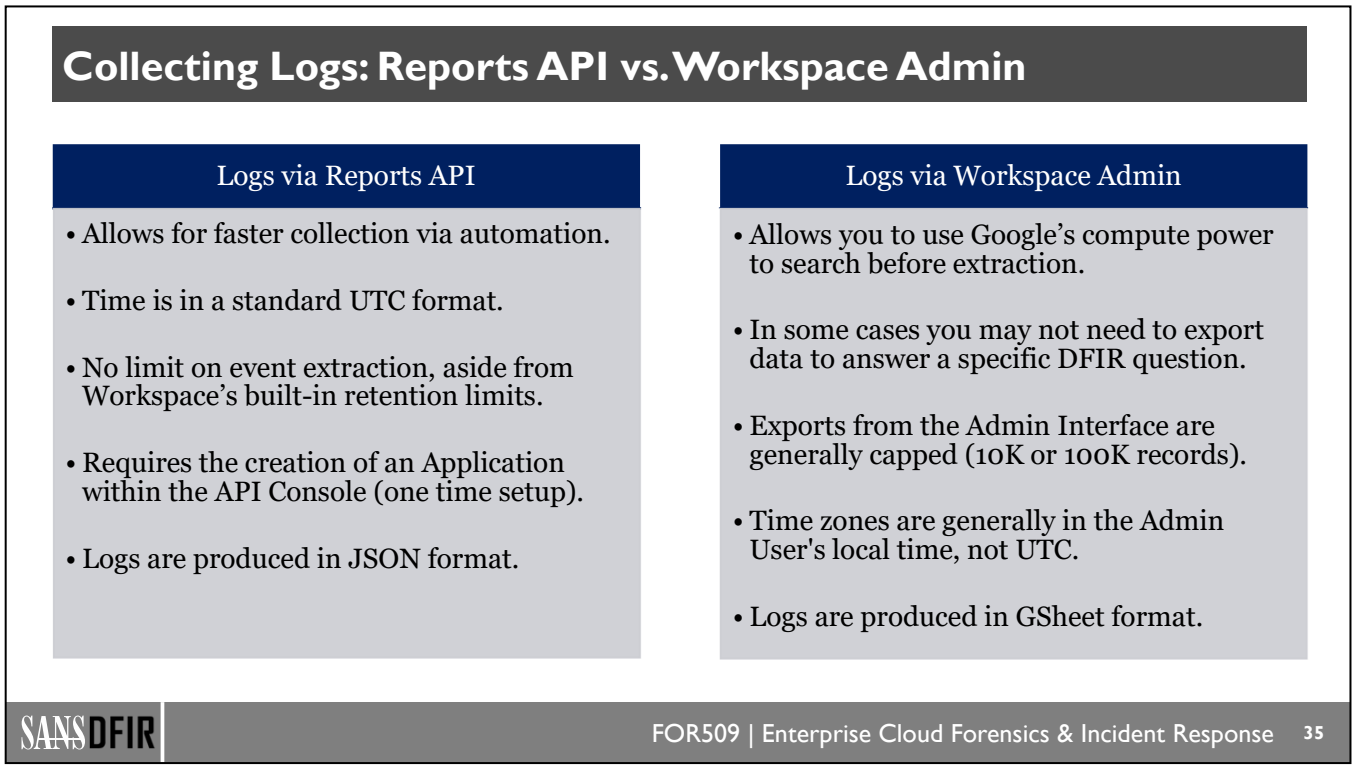
The Workspace admin interface provides an easy and and simple way of visually seeing and navigating the evidence produced by logs. However, all of the subsets of data types within the Workspace admin interface are all separated inside the interface itself. This means to go and collect all of the evidence that may be useful for investigating a Workspace compromise would require you to navigate through multiple screens and click multiple buttons. While this might be useful in cases where you have to visually walk a third party through cutting the evidence, it is by no means the fastest way to go and collect data from Google Workspace.

The Workspace admin console Software Development Kit (SDK) provides the ability to access data in Google Workspace via API calls. This includes being able to retrieve reports in JSON-based output. There are two primary types of reports that we can collect with the Workspace admin console API; they are activity reports and usage reports.

Activity reports provide us with details of activities that have occurred on different services provided inside of Google Workspace. This includes activity on Google Drive, authentication activity, OAuth activity with third-party applications, along with activity that has occurred inside of the admin console. The activity reports provide a good insight to changes or alterations that have been made inside of the different services for Google Workspace.

Usage reports, on the other hand, provide details of events related to user accounts and how user accounts have been used.

1. https://for509.com/ivgzw (Reports API Overview)



There are a few key differences between collecting evidence via the API or from the Workspace admin interface. Of the most important note to begin with the API allows for a much faster and consistent collection of logs. This is purely because collection of logs by API can be scripted so there is consistency each time data is collected. However, setting up the ability to collect logs via API does take some time initially as it requires a Service Account with special workspace permissions before logs can be collected.[1]

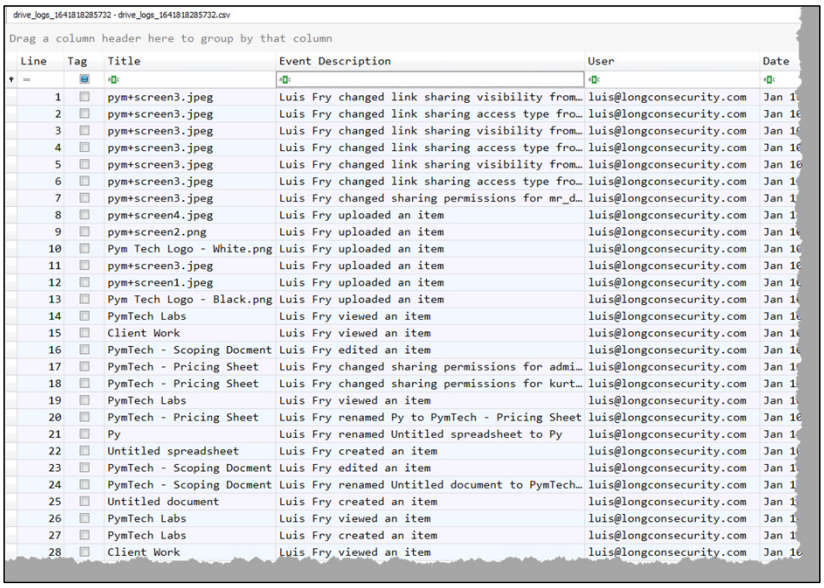
One of the more challenging differences between using either the API logs or Workspace admin logs, is that time displayed in both of these log types is different to each other. The time displayed in logs extracted via the Google Workspace admin interface are all in the local time zone of the user extracting the logs, with the accompanying time zone. Whereas the logs collected via API contain all timestamps in UTC format.

There are also limitations in the Google Workspace Admin interface around how many events are recorded for each log type that is downloaded. Depending on the log type downloaded via the interface, you're either restricted to 10,000 events or 100,000 events inside a single log download. This would mean if you were trying to collect a complete picture of all logs via the interface you would have to break up a search into multiple time ranges ensuring that the logs generated do not exceed 10,000 events. This limitation does not exist when collecting logs via the API.

Lastly, the format that log files are produced when using the interface are only GSheet format (for now), whereas logs via the API can be produced in JSON format. JSON format is far easier to manipulate when it comes to ingesting the logs into a log analysis platform. The GSheet format can also be useful if you don't have a log analysis platform ready to use. At the time of publishing Google Workspace only allows for GSheet exporting of logs from the user interface. Once the logs are exported to GSheet format they can then be saved in CSV format for further manipulation in other tools.

1. https://for509.com/wi15d (Reports API: Prerequisites)

Workspace Admin Audit Logs



drive_logs_1641818285732 - drive_logs_1641818285732.csv

Drag a column header here to group by that column

Line	Tag	Title	Event Description	User	Date
1		pym+screen3.jpeg	Luis Fry changed link sharing visibility from…	luis@longconsecurity.com	Jan 1
2		pym+screen3.jpeg	Luis Fry changed link sharing access type fro…	luis@longconsecurity.com	Jan 1
3		pym+screen3.jpeg	Luis Fry changed link sharing visibility from…	luis@longconsecurity.com	Jan 1
4		pym+screen3.jpeg	Luis Fry changed link sharing access type fro…	luis@longconsecurity.com	Jan 1
5		pym+screen3.jpeg	Luis Fry changed link sharing visibility from…	luis@longconsecurity.com	Jan 1
6		pym+screen3.jpeg	Luis Fry changed link sharing access type fro…	luis@longconsecurity.com	Jan 1
7		pym+screen3.jpeg	Luis Fry changed sharing permissions for mr_d…	luis@longconsecurity.com	Jan 1
8		pym+screen4.jpeg	Luis Fry uploaded an item	luis@longconsecurity.com	Jan 1
9		pym+screen2.png	Luis Fry uploaded an item	luis@longconsecurity.com	Jan 1
10		Pym Tech Logo - White.png	Luis Fry uploaded an item	luis@longconsecurity.com	Jan 1
11		pym+screen3.jpeg	Luis Fry uploaded an item	luis@longconsecurity.com	Jan 1
12		pym+screen1.jpeg	Luis Fry uploaded an item	luis@longconsecurity.com	Jan 1
13		Pym Tech Logo - Black.png	Luis Fry uploaded an item	luis@longconsecurity.com	Jan 1
14		PymTech Labs	Luis Fry viewed an item	luis@longconsecurity.com	Jan 1
15		Client Work	Luis Fry viewed an item	luis@longconsecurity.com	Jan 1
16		PymTech - Scoping Docment	Luis Fry edited an item	luis@longconsecurity.com	Jan 1
17		PymTech - Pricing Sheet	Luis Fry changed sharing permissions for admi…	luis@longconsecurity.com	Jan 1
18		PymTech - Pricing Sheet	Luis Fry changed sharing permissions for kurt…	luis@longconsecurity.com	Jan 1
19		PymTech Labs	Luis Fry viewed an item	luis@longconsecurity.com	Jan 1
20		PymTech - Pricing Sheet	Luis Fry renamed Py to PymTech - Pricing Sheet	luis@longconsecurity.com	Jan 1
21		Py	Luis Fry renamed Untitled spreadsheet to Py	luis@longconsecurity.com	Jan 1
22		Untitled spreadsheet	Luis Fry created an item	luis@longconsecurity.com	Jan 1
23		PymTech - Scoping Docment	Luis Fry edited an item	luis@longconsecurity.com	Jan 1
24		PymTech - Scoping Docment	Luis Fry renamed Untitled document to PymTech…	luis@longconsecurity.com	Jan 1
25		Untitled document	Luis Fry created an item	luis@longconsecurity.com	Jan 1
26		PymTech Labs	Luis Fry viewed an item	luis@longconsecurity.com	Jan 1
27		PymTech Labs	Luis Fry created an item	luis@longconsecurity.com	Jan 1
28		Client Work	Luis Fry viewed an item	luis@longconsecurity.com	Jan 1

Audit Logs with Timeline Explorer

- Workspace Audit Logs are all exported as CSV file formats via GSheet.
- A quick DFIR tool for viewing these logs is Eric Zimmerman's Timeline Explorer.
- Timeline Explorer will allow for faster searching and manipulation of the CSV data than Excel.
- **Remember**: GSheet/CSVs can have their data limited to 10k or 100k rows.

If you decided that collecting logs via the interface and in CSV format was your preferred option, there are still ways to perform analysis on the logs collected. Using tools like Eric Zimmerman's Timeline Explorer[1] will allow you to import CSV data and run searches or filtering across the data to perform analysis.[2]

This can be a particular useful option if trying to set up a Service Account to collect logs via an API is difficult based on the investigation you're performing. One key limitation to remember when it comes to perform in analysis with CSV data and timeline explorer, is that the logs you have collected via the workspace admin interface will be limited to either 10,000 or 100,000 events. This may mean that you are missing data across the log source that you are investigating in Timeline Explorer. The quickest way to check if you maybe missing data is to check the highest line Number you have within Timeline Explorer. If that has been capped at 10,000 or 100,000 advance you know that there will be data missing from the log that you are currently reviewing.

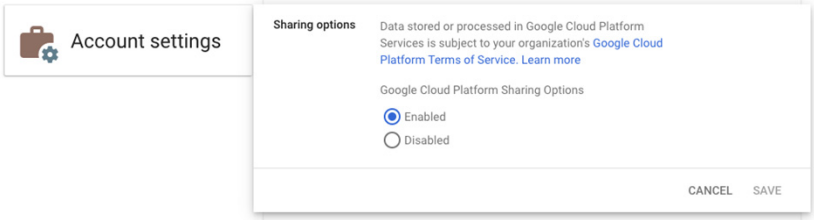
1. https://for509.com/ztools (Eric Zimmerman's Tools)
2. https://for509.com/ra5l6 (Introducing and Using Timeline Explorer)

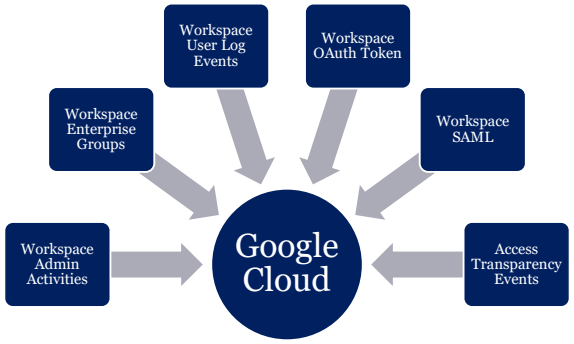
drive_logs_1641818285732 - drive_logs_1641818285732.csv

Drag a column header here to group by that column

Line	Tag	Title	Event Description	User	Date
1		pym+screen3.jpeg	Luis Fry changed link sharing visibility from…	luis@longconsecurity.com	Jan 1
2		pym+screen3.jpeg	Luis Fry changed link sharing access type fro…	luis@longconsecurity.com	Jan 1
3		pym+screen3.jpeg	Luis Fry changed link sharing visibility from…	luis@longconsecurity.com	Jan 1
4		pym+screen3.jpeg	Luis Fry changed link sharing access type fro…	luis@longconsecurity.com	Jan 1
5		pym+screen3.jpeg	Luis Fry changed link sharing visibility from…	luis@longconsecurity.com	Jan 1
6		pym+screen3.jpeg	Luis Fry changed link sharing access type fro…	luis@longconsecurity.com	Jan 1
7		pym+screen3.jpeg	Luis Fry changed sharing permissions for mr_d…	luis@longconsecurity.com	Jan 1
8		pym+screen4.jpeg	Luis Fry uploaded an item	luis@longconsecurity.com	Jan 1
9		pym+screen2.png	Luis Fry uploaded an item	luis@longconsecurity.com	Jan 1
10		Pym Tech Logo - White.png	Luis Fry uploaded an item	luis@longconsecurity.com	Jan 1
11		pym+screen3.jpeg	Luis Fry uploaded an item	luis@longconsecurity.com	Jan 1
12		pym+screen1.jpeg	Luis Fry uploaded an item	luis@longconsecurity.com	Jan 1
13		Pym Tech Logo - Black.png	Luis Fry uploaded an item	luis@longconsecurity.com	Jan 1
14		PymTech Labs	Luis Fry viewed an item	luis@longconsecurity.com	Jan 1
15		Client Work	Luis Fry viewed an item	luis@longconsecurity.com	Jan 1
16		PymTech - Scoping Docment	Luis Fry edited an item	luis@longconsecurity.com	Jan 1
17		PymTech - Pricing Sheet	Luis Fry changed sharing permissions for admi…	luis@longconsecurity.com	Jan 1
18		PymTech - Pricing Sheet	Luis Fry changed sharing permissions for kurt…	luis@longconsecurity.com	Jan 1
19		PymTech Labs	Luis Fry viewed an item	luis@longconsecurity.com	Jan 1
20		PymTech - Pricing Sheet	Luis Fry renamed Py to PymTech - Pricing Sheet	luis@longconsecurity.com	Jan 1
21		Py	Luis Fry renamed Untitled spreadsheet to Py	luis@longconsecurity.com	Jan 1
22		Untitled spreadsheet	Luis Fry created an item	luis@longconsecurity.com	Jan 1
23		PymTech - Scoping Docment	Luis Fry edited an item	luis@longconsecurity.com	Jan 1
24		PymTech - Scoping Docment	Luis Fry renamed Untitled document to PymTech…	luis@longconsecurity.com	Jan 1
25		Untitled document	Luis Fry created an item	luis@longconsecurity.com	Jan 1
26		PymTech Labs	Luis Fry viewed an item	luis@longconsecurity.com	Jan 1
27		PymTech Labs	Luis Fry created an item	luis@longconsecurity.com	Jan 1
28		Client Work	Luis Fry viewed an item	luis@longconsecurity.com	Jan 1

Sending Logs to Google Cloud (1)





Audit Logs in Google Cloud

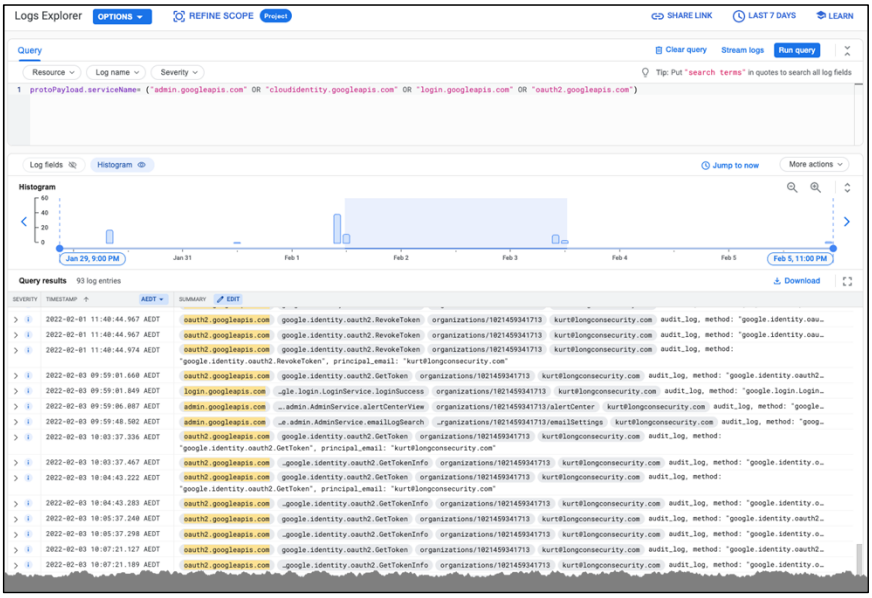
- Has to be turned on; it is off by default.
- Logs retained in Google Cloud are based on your Google Cloud Log Bucket settings.
- Not all Audit Logs are shipped to Google Cloud; they are mainly logs related to authentication and user auditing. They don't include email or resource access.
- Logs are held under the Organization in Google Cloud, not in a Project. We will discuss this more in the Google Cloud DFIR Section.

Another method for also collecting logs out of Google Workspace is sending them directly to the Logging API in Google Cloud.[1] This is a particularly useful way of collecting logs from Google Workspace and holding them for a much longer period of time. The only downside to this method is that not all logs generated by Google Workspace are sent to Google Cloud. Six log types are sent to Google Cloud for Enterprise user licenses, which are the predominant log types that we would be most interested in when it comes to conducting an investigation. For non-Enterprise users they will only receive the Admin Activities, User Log Events, and Enterprise Groups logs. However, these five log types alone may not produce the entire picture you are attempting to look for if an investigation is related to data access or exfiltration that you would otherwise get if you collected all of the logs inside of Google Workspace. You will also notice that logs related to email transit and access are also not included in the log types that are shipped to Google Cloud. Unfortunately, you cannot edit the type of logs that are sent from Google Workspace over to Google Cloud. These are hard set by Google—the only option you get is whether you decide to send logs to Google Cloud or not.

We will look further into how logs are held and shipped inside of Google Cloud in the Google Cloud section of the class.

1. https://for509.com/fmzs7 (Share data with Google Cloud)

Sending Logs to Google Cloud (2)



Service Names

```
admin.googleapis.com
cloudidentity.googleapis.com
login.googleapis.com
oauth2.googleapis.com
```

Audit Logs in Google Cloud

- There are a significant number of useful events sent to Google Cloud.
- The Admin Activities Service and Workspace Login Audit Service contain the most DFIR relevant events.
- Log extractions from Google Cloud is covered in the Google Cloud DFIR Section.

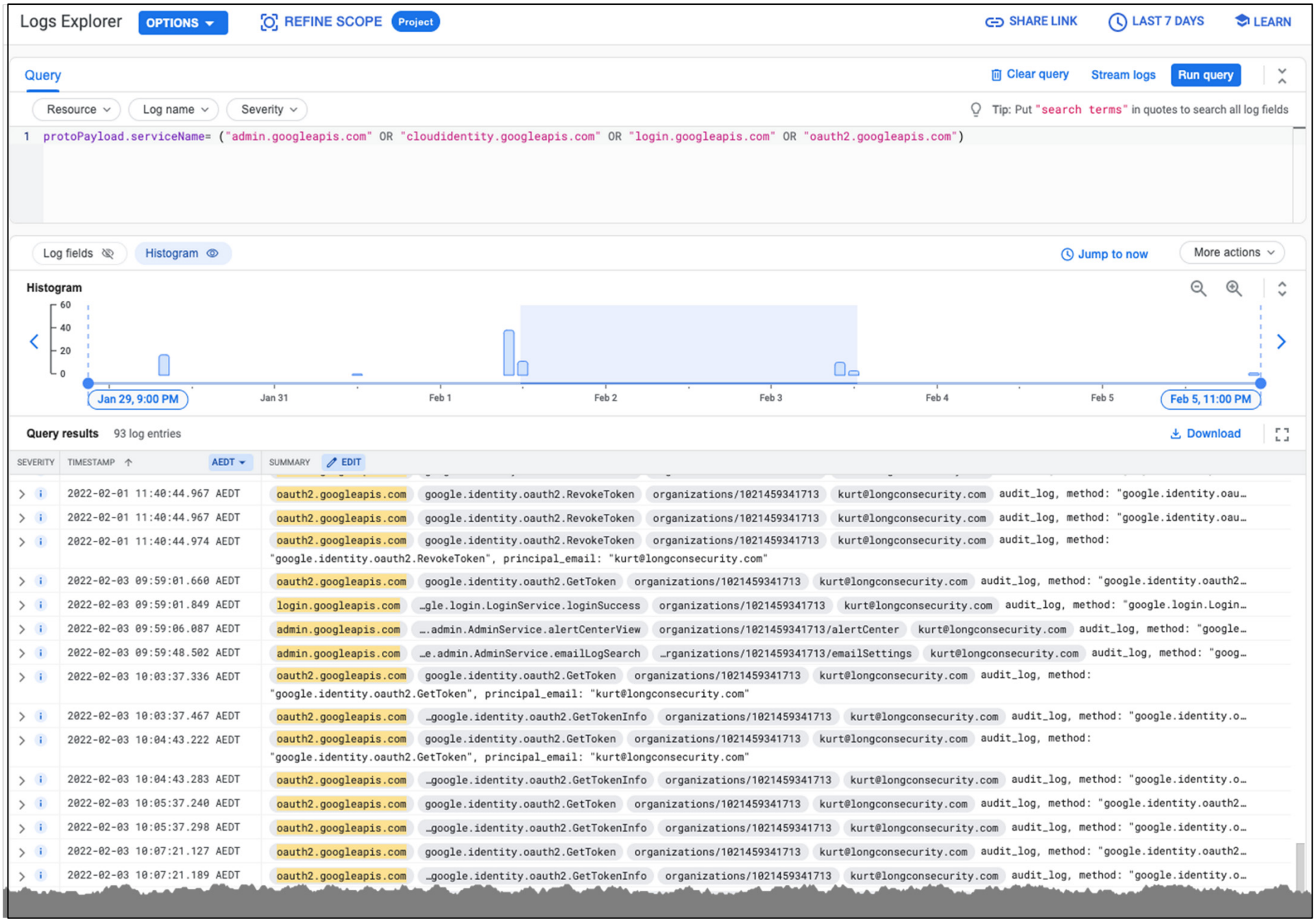
Once logs are inside of Google Cloud you can query the service names relevant to the log types that were sent from Google Workspace.[1] We will look more at the Google Cloud log explorer in the Google Cloud section of the class; however, for now understand that as soon as the logs are sent to Google Cloud you are able to search and query them in a similar way that we will do when extracting the logs via API from Google Workspace and putting them in our own login analysis platform.

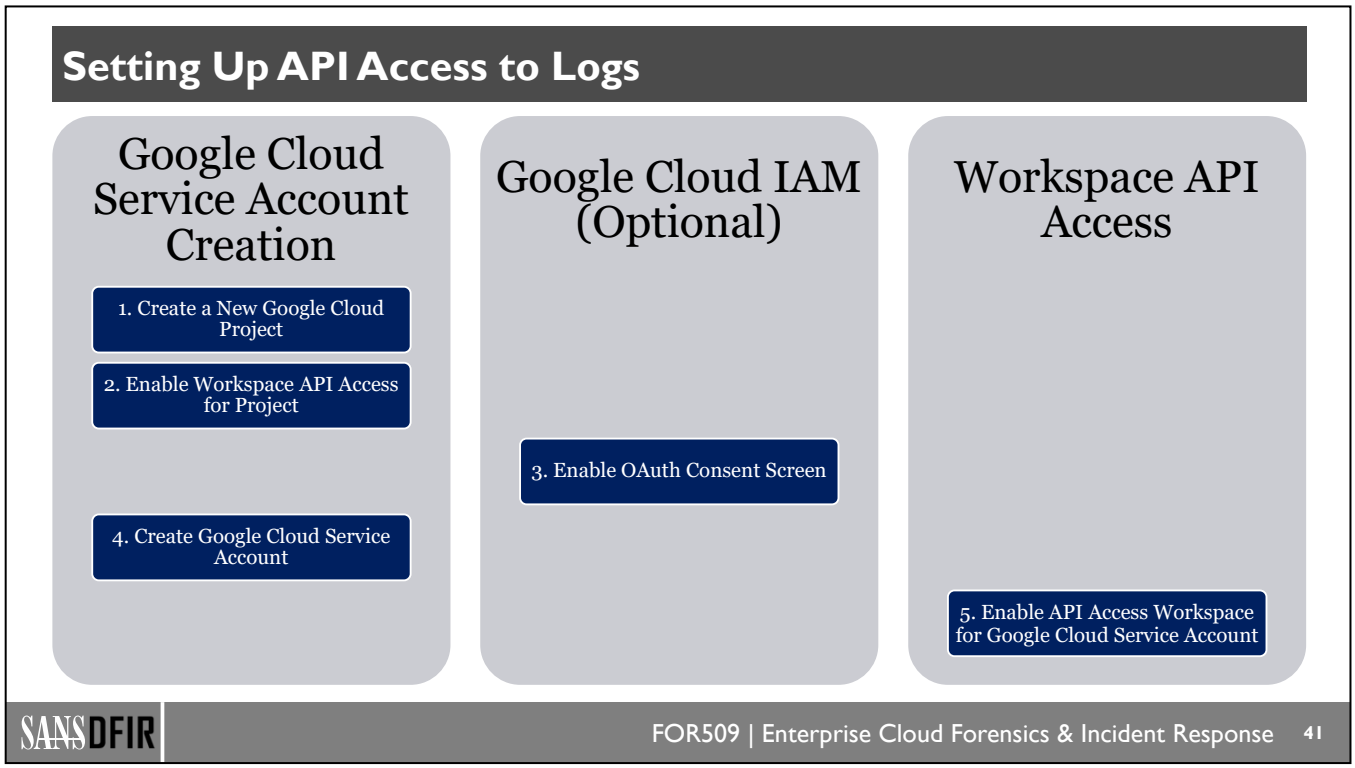
When the logs from Google Workspace arrive in Google Cloud, they will be within four different service names which we have provided above. The below query can also be used to query the logs coming from Google Workspace; however, keep in mind that to view these logs you need to be looking at the root organization in Google Cloud. We will discuss details of the root organization further in the Google Cloud section of the class.

Query:

```
protoPayload.serviceName= ("admin.googleapis.com" OR
"cloudidentity.googleapis.com" OR "login.googleapis.com" OR
"oauth2.googleapis.com")
```

1. https://for509.com/ufiyd (Audit logs for Google Workspace)





When it comes to extracting Google Workspace logs there are a few steps we need to do before we can extract them via API. The start of this process involves creating a Service Account and enabling access for that Service Account to access the Google Workspace API.

1. To create a Service Account to be used with Google Workspace we need to create a new Google Cloud project with the same parent organization used for Google Workspace.

2. Because Google Cloud has a lot of its API locked down by default, we have to enable the Workspace API access for the project that we just created where we intend to create a Service Account that we will use to collect logs.

3. We then need to enable an internal OAuth consent screen which will allow us to authenticate with our Service Account when we attempt to collect the logs from Google Workspace. This is probably a fairly familiar screen that you are used to seeing when you use your Google Workspace account to authenticate to a third-party service.

4. Once we've set up the above three items we can now create a Service Account, inside of the Google Cloud project that we created at step one.

5. After we've created our Service Account we need to then provide permission for that Service Account to access the Google Workspace API. This is done back inside of the Google Workspace admin interface.

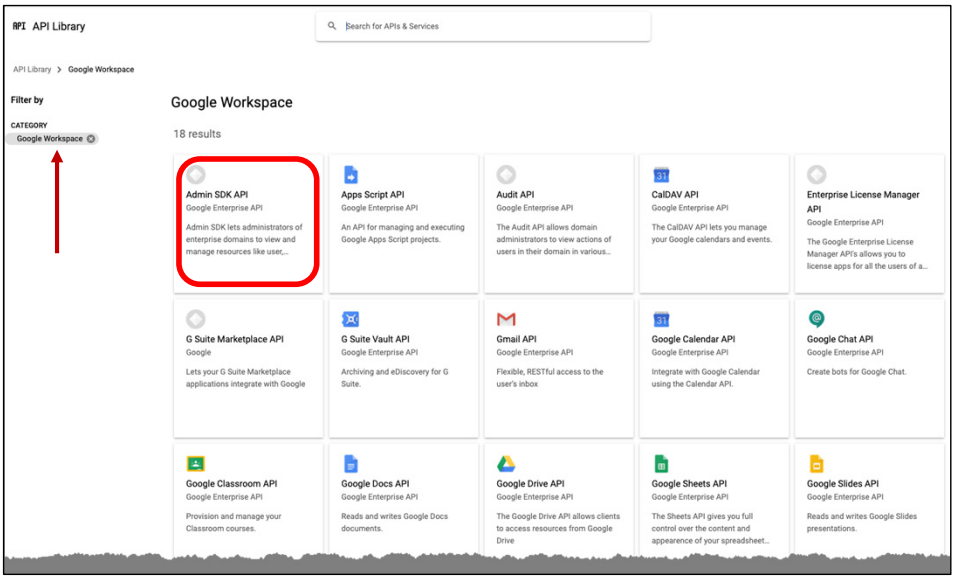
The above process requires you to jump in between both Google Cloud and Google Workspace in terms of setting up a Service Account and providing permissions back inside of Google Workspace.

This process does not require you to be running infrastructure inside of Google Cloud; it simply requires the use of the Service Accounts inside of DCP as the concept of a Service Account does not exist inside of Google Workspace.

Reference:

https://for509.com/2eol7 (Create a service account)

API Access: Setting Up API Permissions



API Library Permissions

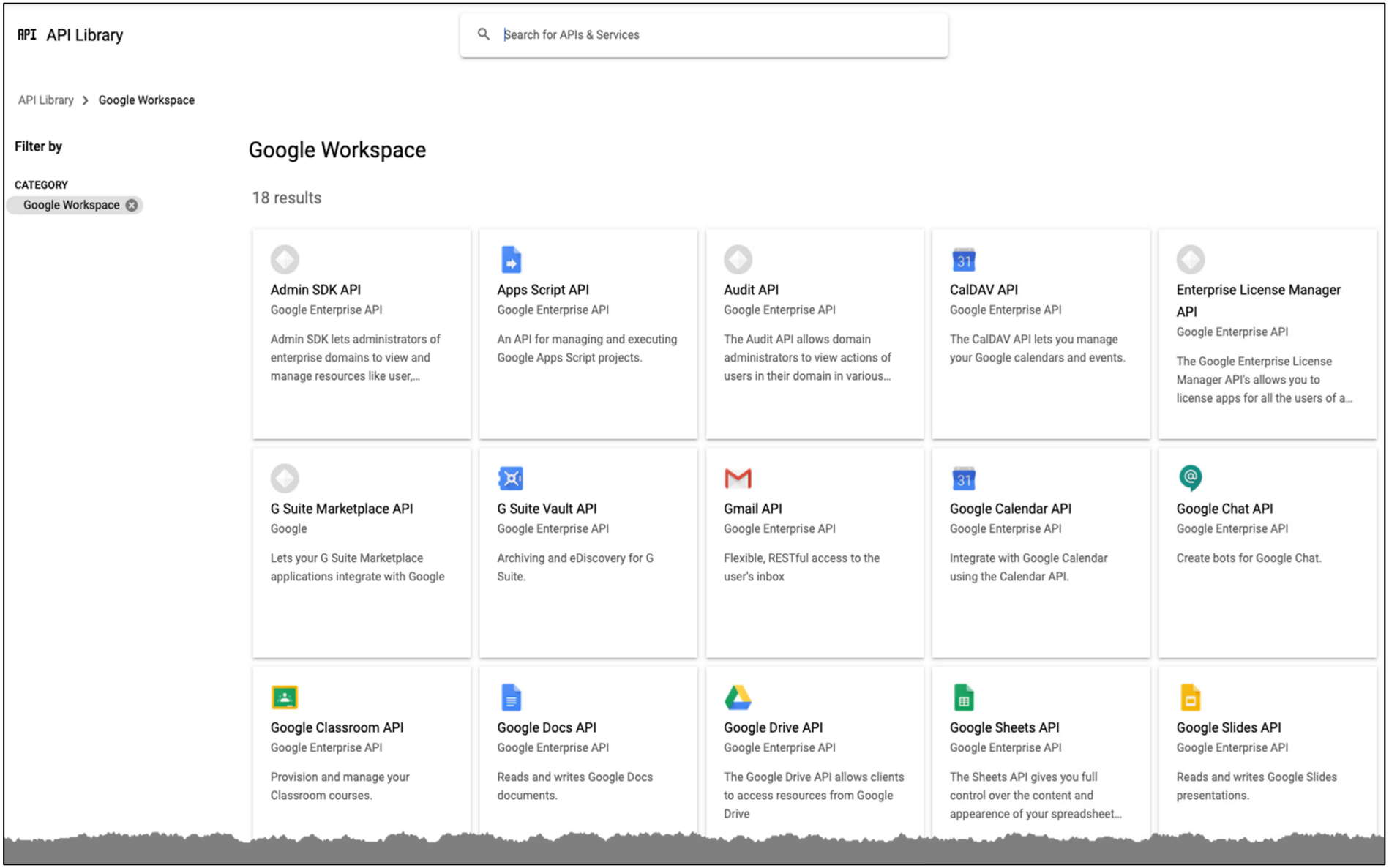
- Based on what is shown in this class you will only need *Admin SDK API* access.
- If you want to also access Vault specific requests, which is outside the scope of this class, you should enable *G Suite Vault API*.

The above screenshot shows the permissions that need to be added to the project where are you create the Service Account that will be used to access the Google Workspace API. You'll notice that you can narrow down the permissions to just those that are using the Google Workspace category on the left-hand side. From here you only need to select the Admin SDK API as the item that the project needs permission to access.

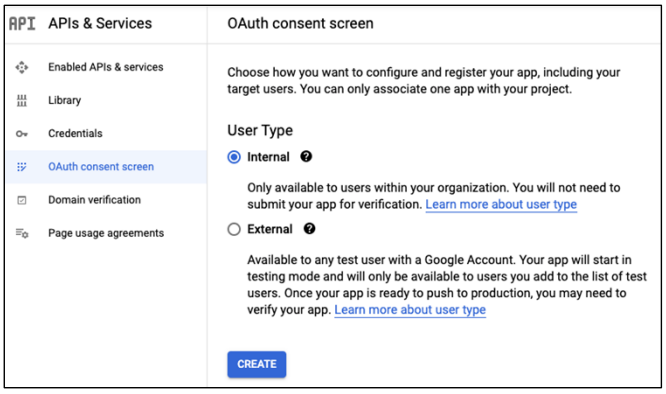
If you also want to use the same Service Account to access other resources inside a Google Workspace, for example, the Vault API, you will also need to add those permissions to this project. Interacting with Vault via Service Account is outside the scope of this class but may be useful if you intend to use the Service Account to perform lookback functions or additional analysis on email across an entire organization.

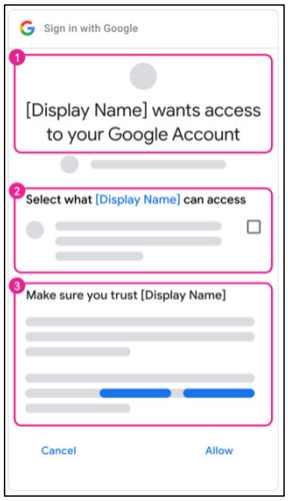
Reference:

https://for509.com/2eol7 (Create a service account)



Enable OAuth Consent Screen





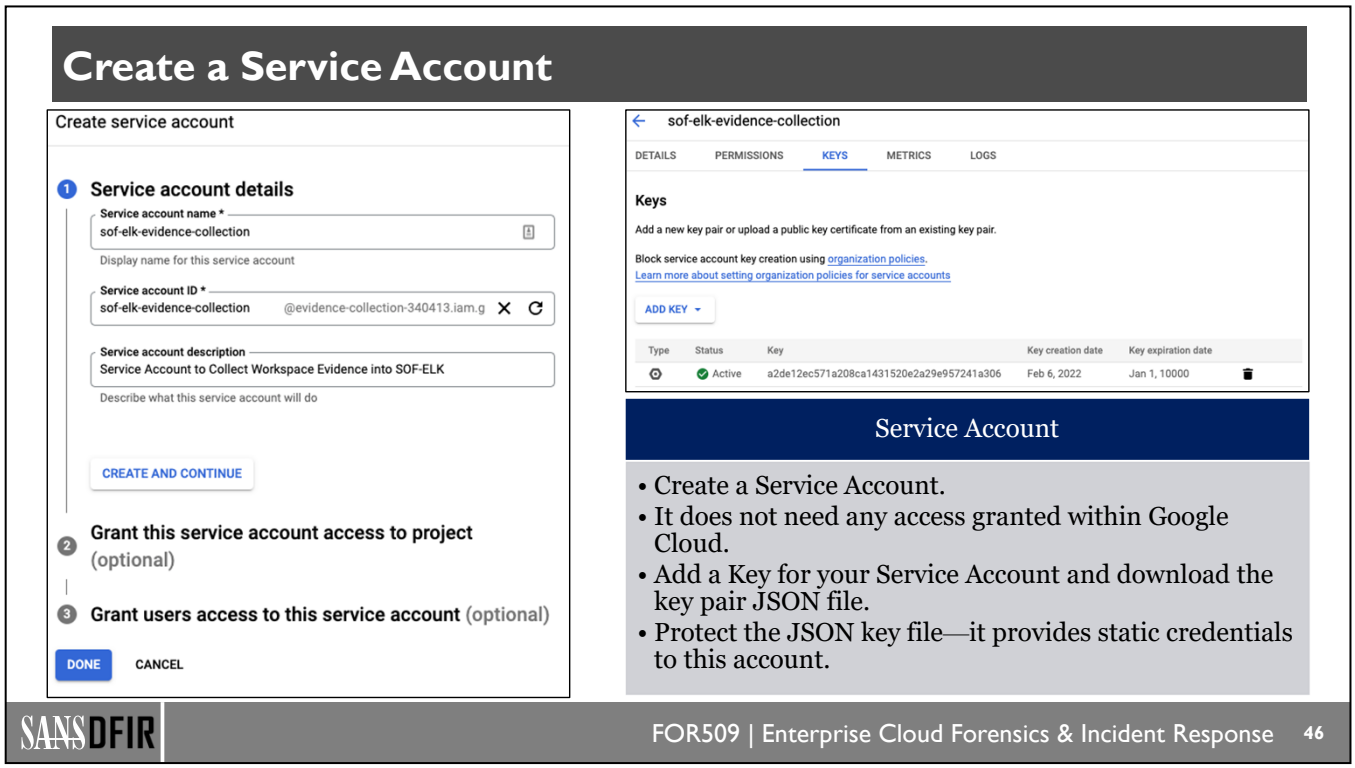
OAuth Consent Screen

- This will link your Service Account access with the Project you just set up.
- This allows your API request to receive authorization via OAuth 2.0.
- Users will be presented with a screen similar to the OAuth App Request shown here.

You will also need to enable OAuth consent on the project where are you have given API access over to Google Workspace. This allows for the authorization screen to be used when requesting access to the APIs in Google Workspace.

Reference:

https://for509.com/2eol7 (Create a service account)

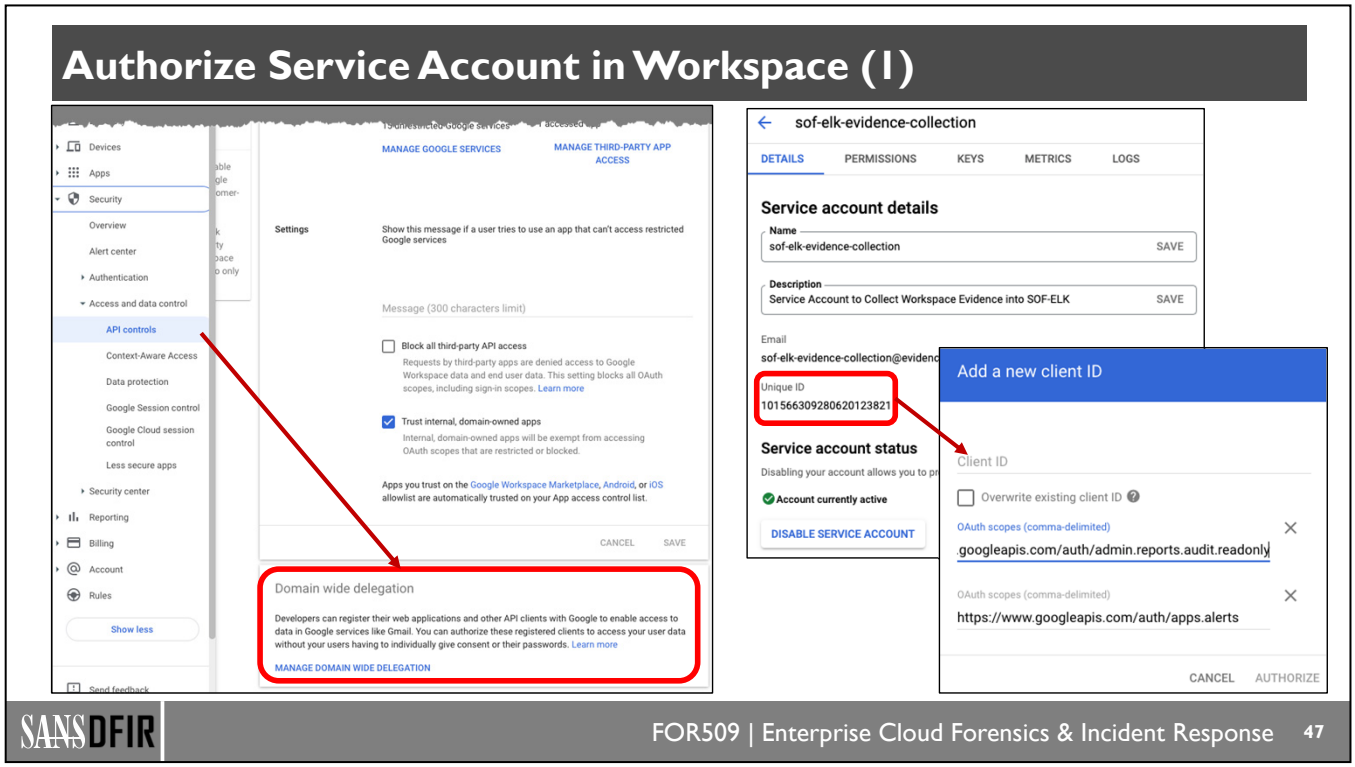


After API permissions and the OAuth consent screen have been set up, it is time to create a service account inside of Google Cloud. This is relatively simple to do; however, as mentioned earlier there is no concept of a service account inside of Google Workspace which is why Google Cloud has to be used for a service account. After the service account is created there are no additional permissions that need to be added at the time of the account creation. Once the account is created you can access the keys for the service account so they can be used in a script to access the Google Workspace API.

You will also need to download the JSON file of the access key that you create against the service account. The JSON file is the equivalent to a static password for the account, so ensure that you protect it appropriately.

Reference:

https://for509.com/2eol7 (Create a service account)

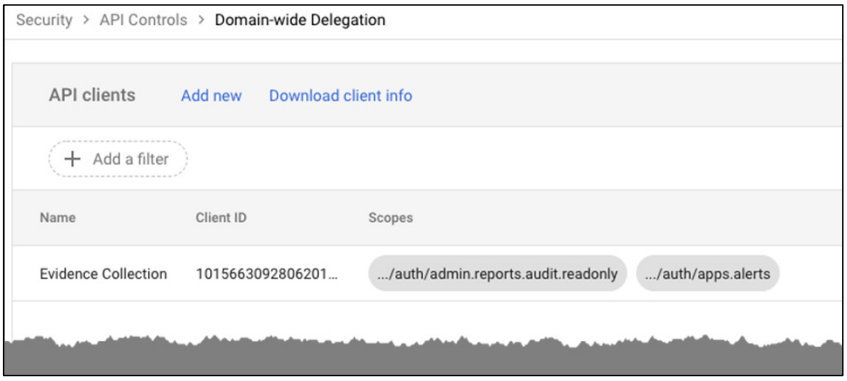


After permissions for the Service Account have been created in Google Cloud, it's time to move back over into the Google Workspace admin interface. Inside the admin interface you will need to give domain wide delegation to the Service Account that you just created. Although giving domain-wide delegation may sound like very broad permissions, we can limit the access against Google Workspace API for the Service Account to only the audit logs and only the ability to read the audit logs.

Reference:

https://for509.com/2eol7 (Create a service account)

Authorize Service Account in Workspace (2)



API Access Scope

- https://www.googleapis.com/auth/admin.reports.audit.readonly
- https://www.googleapis.com/auth/apps.alerts

API Access Scope

- You need to authorize domain-wide access for your Service Account in Google Cloud.
- You should limit your delegation to only the API URLs needed to access logs.
- This will help ensure your Service Account can't make changes to the Workspace.

As part of giving domain-wide delegation to the Service Account we created over in Google Cloud, we can limit the scope of access that the Service Account can use against the Google Workspace API. For the purpose of collecting evidence from an investigation perspective the Service Account really only needs ability to read audit reports and alerts generated by Google Workspace. We can limit the scope of access using the above scope restrictions to prevent our Service Account from having wide ranging access against the entire Google Workspace domain.

Reference:

https://for509.com/2eol7 (Create a service account)

API Access Automation: Installation Process

gws-log-collection.py

- The below commands set up the gws-log-collection.py script on your local system.
- This prepares you for connecting to Google Workspace to pull all available JSON logs.
- You would also need to move the credential .json file you downloaded when creating a Service Account into the below directory.

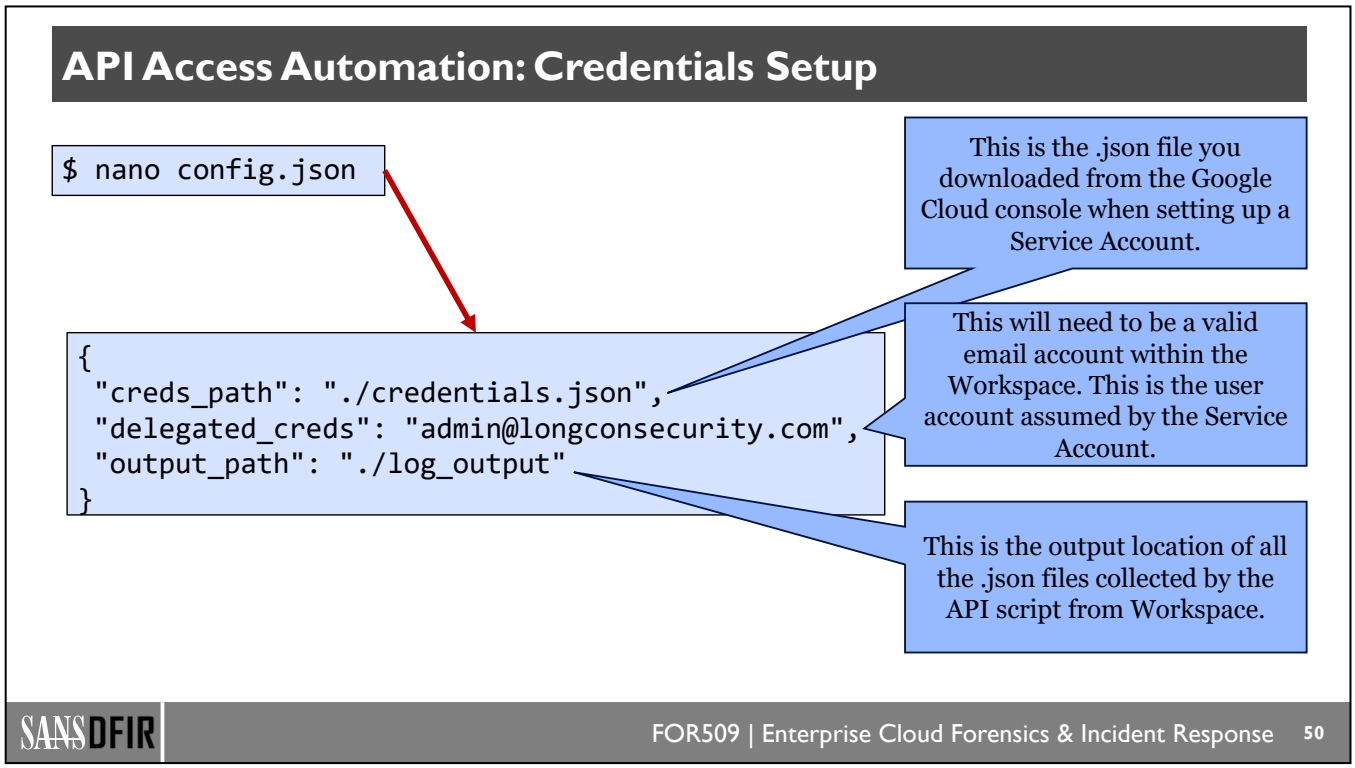
```
$ git clone https://github.com/dlcowen/sansfor509/tree/main/GWS/gws-log-
collection.git

$ cd gws-log-collection

$ mkdir log_output

$ sudo pip3 install -r requirements.txt
```


Now that we have our Service Account and all the permissions set up correctly, we can now access the Google workspace API via third-party tools or a script that we may generate to be able to collect logs. Megan Roddie has developed a Python script[1] that allows us to collect all of the Google Workspace logs using a Service Account and the credentials that we set up previously. All of the labs throughout this section of the class had the logs collected using this technique.

Remember that the script will need access to the credential JSON file that was downloaded when you created an access key for the Service Account in a previous step.

Using Megan's script, we can collect all of the logs available for Google Workspace via the API in JSON format ready to be loaded into a log analysis platform.

1. https://for509.com/l3waf (Megan Roddie's GWS Log Collection Script)



As part of the script developed by Megan,[1] you will need to alter the config.json file and update:

- the location of the JSON file containing the Service Account credentials.
- the principal name for the Service Account.
- the output folder where you would like all of the JSON files written to that will be collected via the script.

1. https://for509.com/l3waf (Megan Roddie's GWS Log Collection Script)

API Access Automation: Downloading JSON Logs

gws-log-collection.py

- Once the configuration file is set up correctly you can run the gws-get-logs.py script to download all the available Workspace logs.
- Currently, the logs collected are; Admin Audit Logs, Calendar Logs, Chat Logs, GDrive Audit Logs, User Log Events, and User Audit Logs.

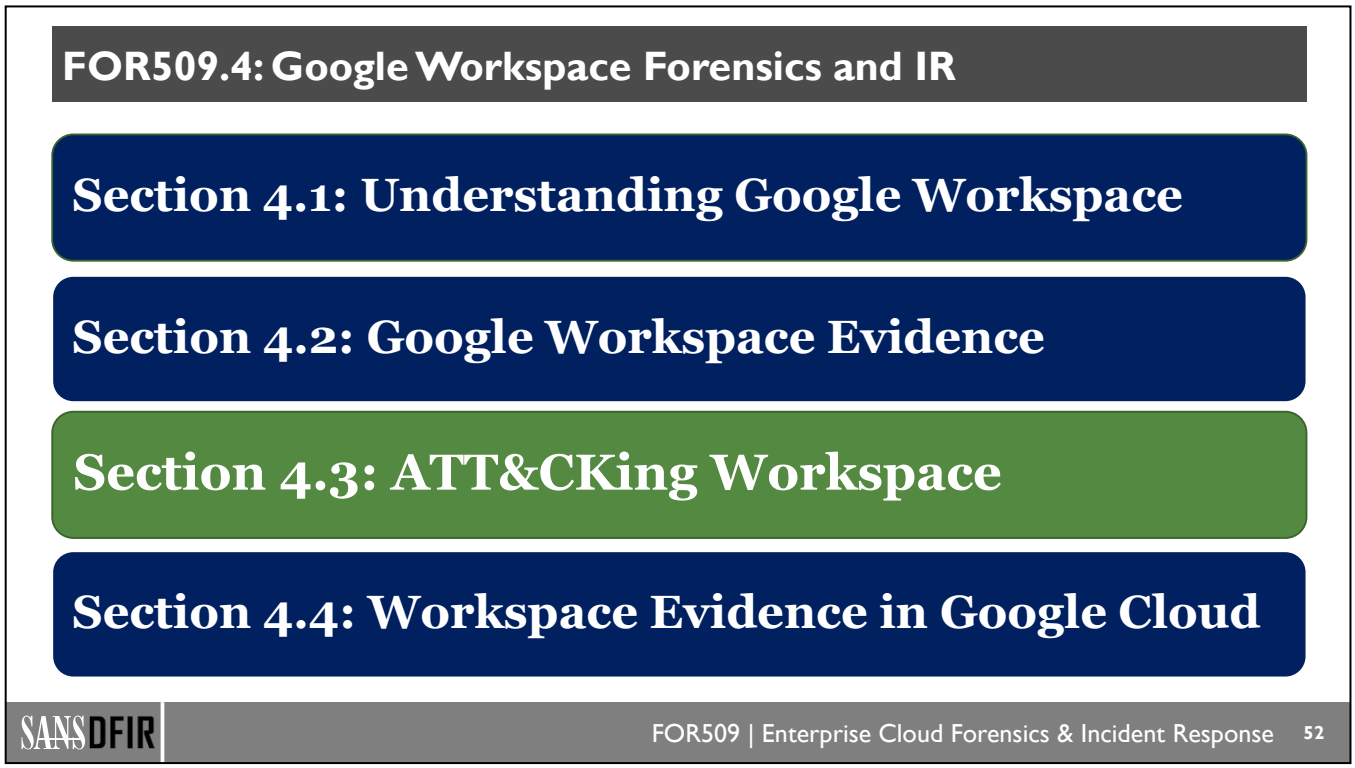
```
$ python3 gws-get-logs.py

$ cd log_output

$ ls
admin_logs.json  calendar_logs.json  chat_logs.json  drive_logs.json
login_logs.json  user_logs.json
```


Once you have run the Google workspace log collection script you can then go and check the output to ensure that the JSON files have all been written to the location you specified in the config.json file.

The above represents the output you should see if all the logs were collected successfully, and all the permissions were applied correctly to the Service Account.

Reference:

https://for509.com/l3waf (Megan Roddie's GWS Log Collection Script)



This page intentionally left blank.

Google Workspace Forensics and IR Roadmap

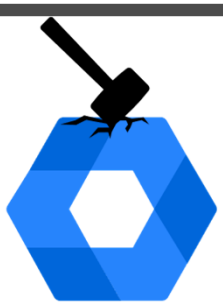
- 4.1: Understanding Google Workspace
- 4.2: Google Workspace Evidence
- 4.3: ATT&CKing Workspace
- 4.4: Workspace Evidence in Google Cloud

- Attacks against Google Workspace
- Workspace Detections & Automated Alerts
- Email Compromise Investigation
- Email Log Analysis
- Google Vault Analysis
- Advanced Phishing & Malware
- **Lab 4.1**: Google Workspace Admin BEC

This page intentionally left blank.

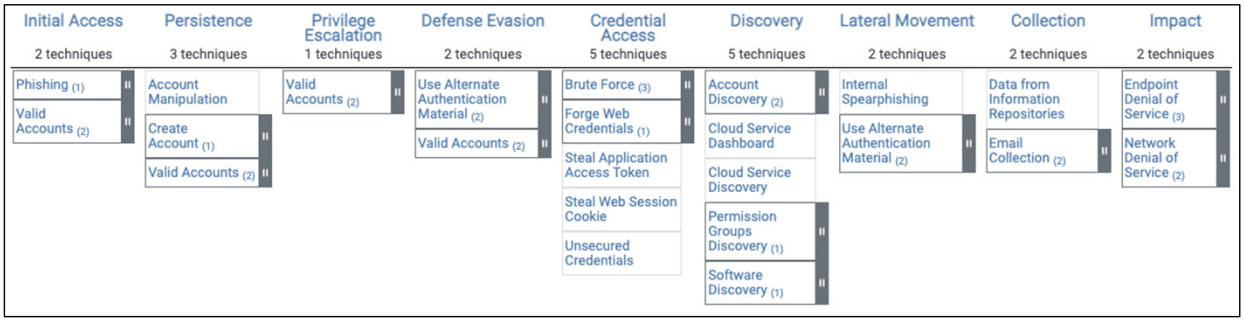
SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

ATT&CKing Workspace



This page intentionally left blank.

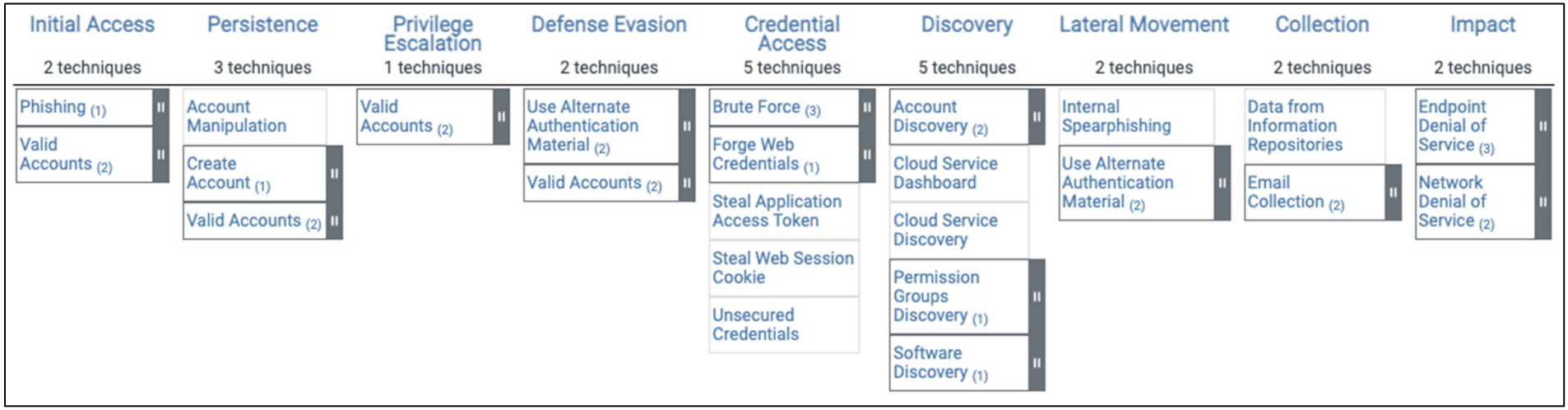
MITRE ATT&CK for Google Workspace

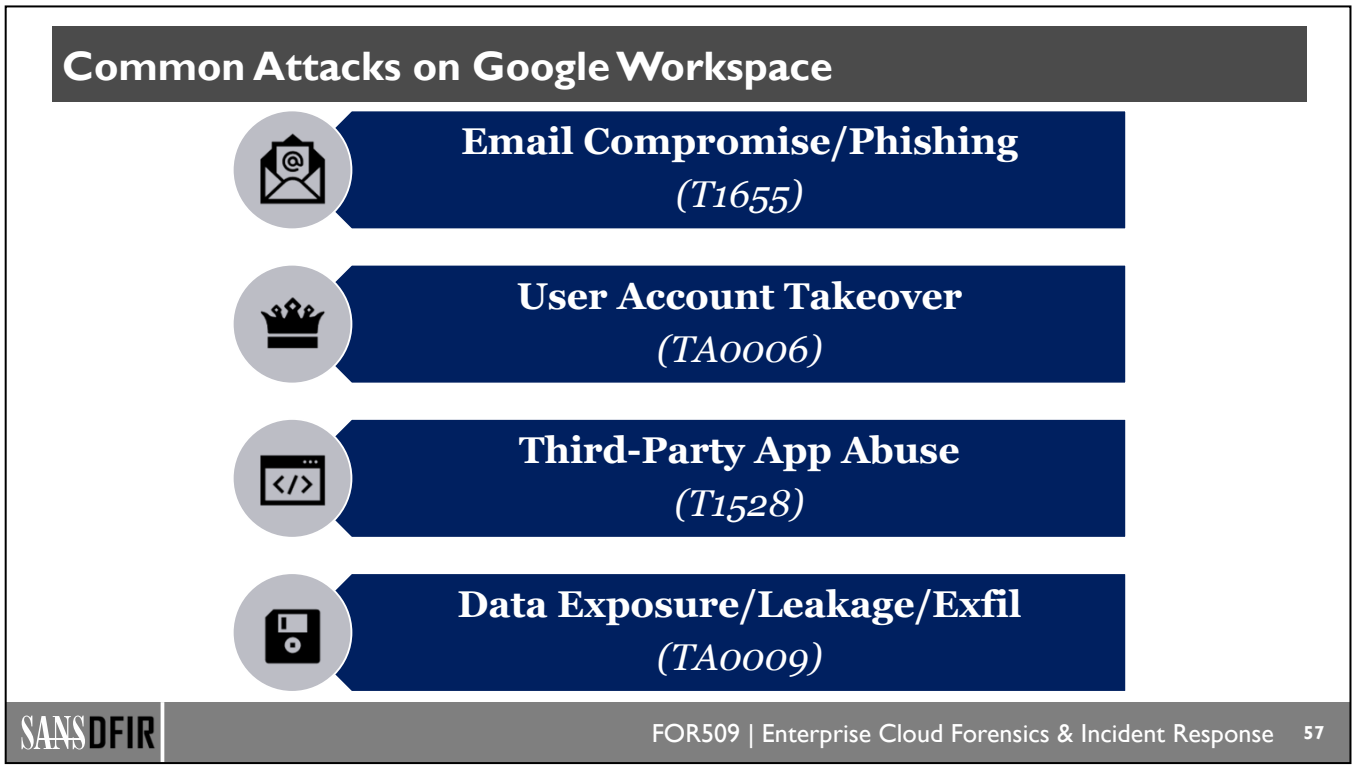


Understanding how a threat actor performs attacks against Google Workspace is a key piece of knowledge when it comes to understanding how to better investigate an incident that occurs inside of Google Workspace. MITRE has pull together a matrix of tactics and techniques that have been observed in the wild against Google Workspace.[1] We can use this information to better understand how threat actors abuse Google Workspace. It is worth understanding that the Google Workspace matrix is a continually evolving matrix and may not include all attacks possible against Google Workspace.

When using the MITRE ATT&CK matrix for Google Workspace, it is worth keeping in mind that the techniques provided in the matrix are generic in nature to ensure that they are lying to other matrixes that MITRE has produced. For example, the technique "Steal Application Access Tokens" provides general information on abusing OAuth; it does not provide specifics of how OAuth may be abused in Google Workspace.

1. https://for509.com/t1i6x (MITRE Google Workspace ATT&CK)





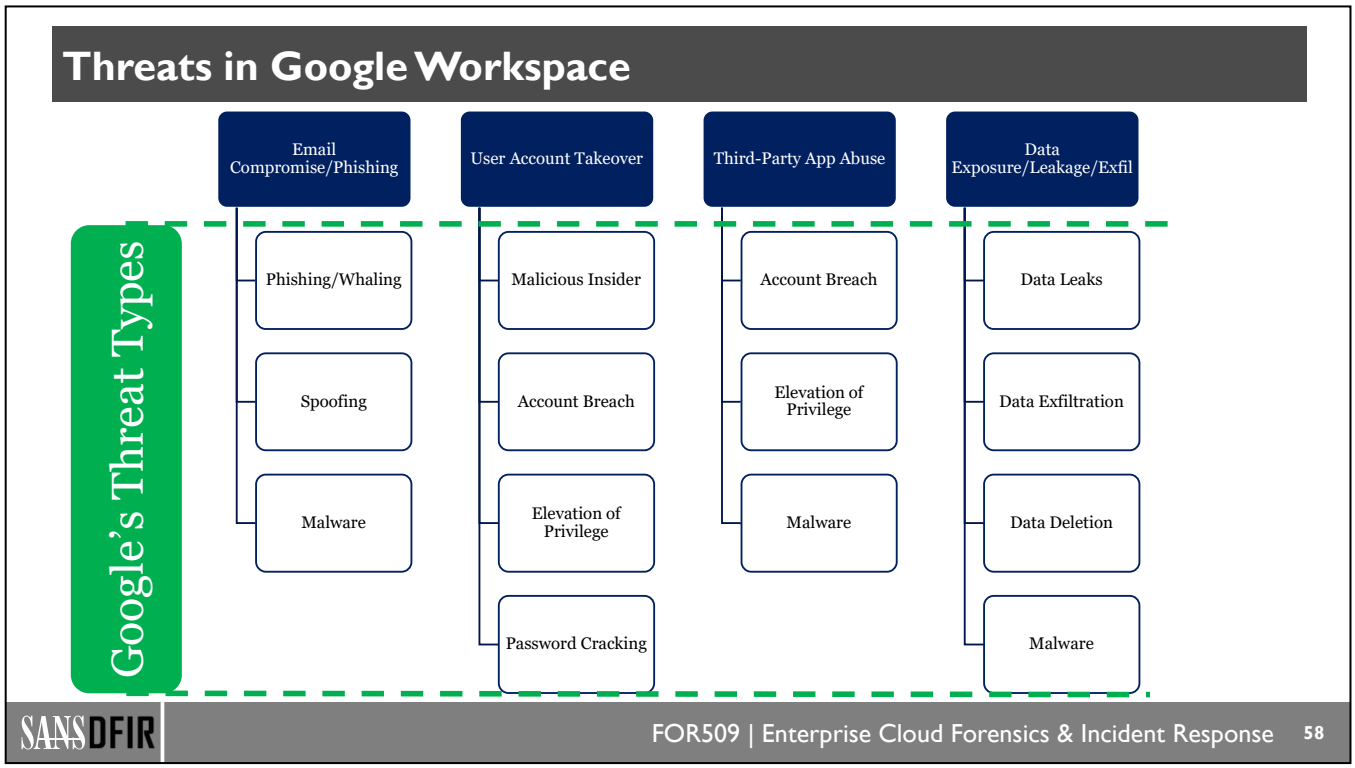
For the remainder of the Google Workspace section of the class, we have decided to focus on four common attack scenarios that we regularly see inside of Google Workspace.

One of the most common attacks scenarios that we see, not only in Google Workspace but across most SaaS platforms, is email phishing and/or compromise. This is an attack that is not only used by organized crime groups but also by state-sponsored threat actors.

The takeover of an administrator account is probably one of the more devastating attacks that can occur inside of Google Workspace. When a threat actor has control over an administrator account there are no limits to what actions they may be able to perform inside of a Google Workspace instance.

We will also look at third-party abuse, what is more technically known as OAuth abuse. These types of attacks are starting to become more common and can quickly be used to propagate in combination with phishing email. Furthermore, this type of attack often goes undetected for much longer than the other types of attacks we will be looking at in Google Workspace.

Lastly will also be looking at some of the common data exposure and data exfiltration techniques that are abused in Google Workspace. While we will not be looking at every possible type of data exfiltration, we will look at the concepts required to be able to investigate a data exposure or exfiltration incident that would apply to the majority of different techniques available to exfiltration data out of Google Workspace.



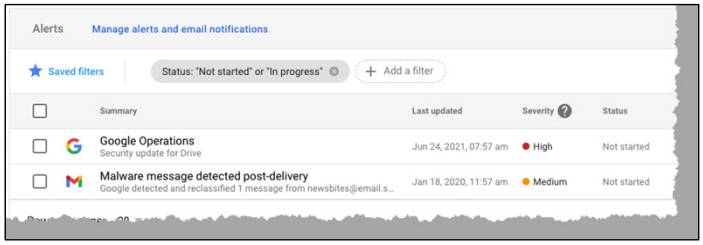
Google provides a number of predefined threat types that are used in a lot of Google Workspace's reports.[1] In the above slide we have taken the four common attack techniques that we will be looking at in this section and matched them up to the threat types that Google use for Google Workspace. Google Workspace provides a dedicated security health page in its administration interface; however, not all the above threat types will be visible depending on the type of license that you have for Google Workspace.

The above matrix is to assist investigators with understanding the types of reporting that may be available in the security health page to help investigate for common types of attacks that we will be looking at in Google Workspace.

1. https://for509.com/lf752 (Google Workspace Threat Types)

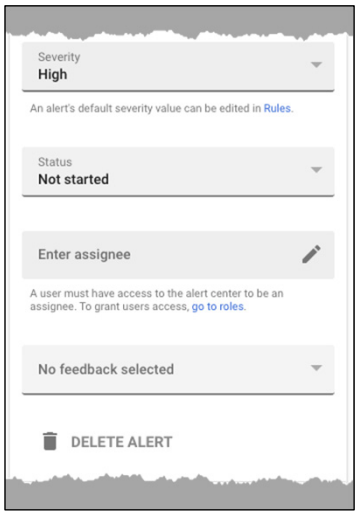
Workspace Detection and Automated Alerts

FOR509 is not a detection class; there are resources in the notes section.



Workspace Alerts and Detections

- Workspace has automated alerts based on license types within the Security Dashboard.
- Admins can created their own alert types from Audit logs within Workspace.
- Google provides some alerting for detected APT attacks.



While this class is specifically dedicated to investigating an incident after it has occurred and collecting evidence to support the investigation, it is worth noting that Google Workspace provides several detection and automated alerting tools. We will not be focusing on these tools in the class, but it is worth you understanding that they exist and may help in determining how an initial compromise occurred inside of a Google Workspace.

Of most relevance is the security dashboard that provides notifications from Google directly along with alerts related to email that have been reclassified or notifications that a state -attack may have targeted one of your users.

As shown previously, we looked at how logs could be collected directly from the administration interface. There is also the ability to set alerts for each of the audit reports in the admin interface. This can allow you to set up your own alerts to notify you of anomalous activity inside of Google Workspace. A number of references have been provided below if you need further information on how to set up simple detection inside of Google Workspace. Be aware that some of these features may not be available in some of the lower-tiered licenses for Google Workspace.

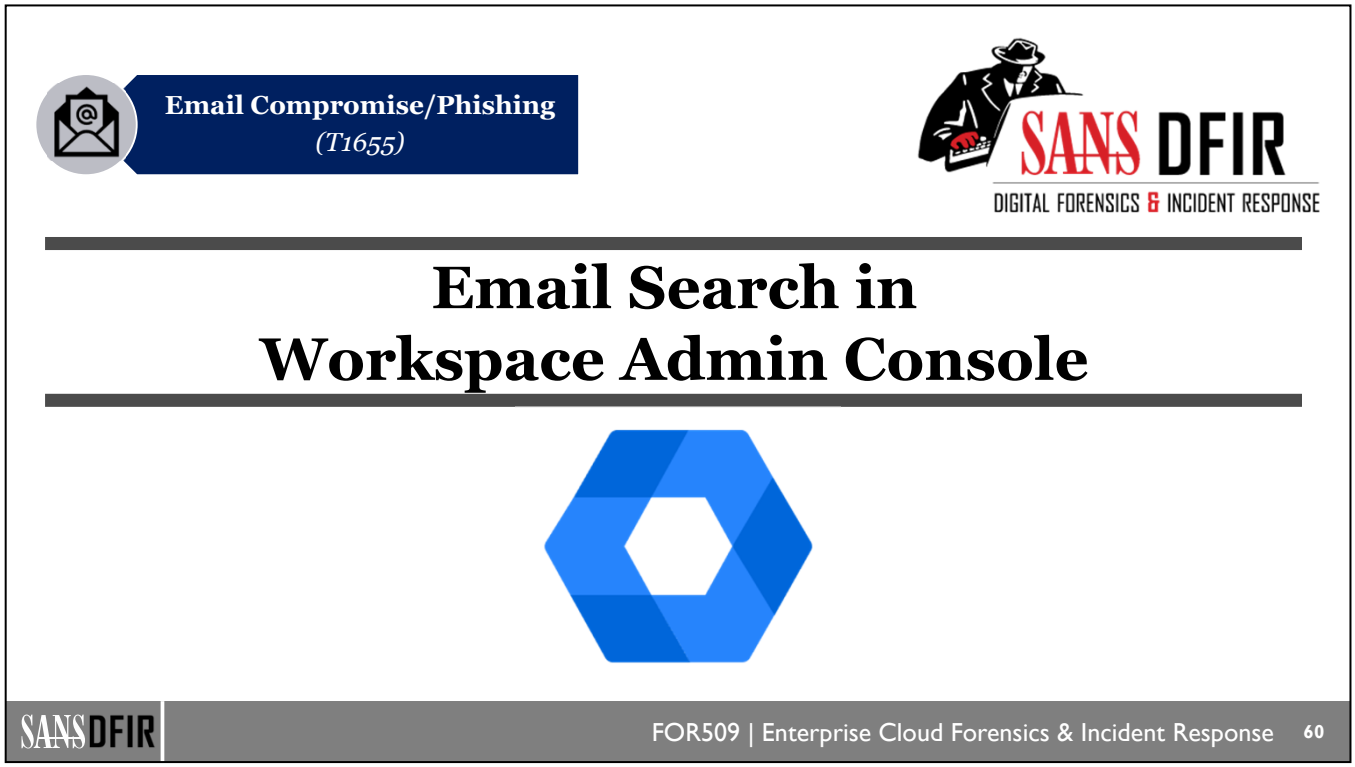
References:

https://for509.com/o25n8 (Use the security dashboard)

https://for509.com/z83m6 (Admin email alerts & system-defined rules)

https://for509.com/rgjw0 (Admin alerts for suspicious login activity)

https://for509.com/mgdho (Government-backed attack alerts)



This page intentionally left blank.

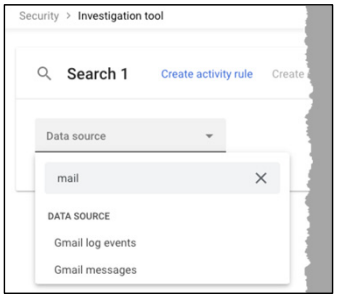
Workspace Email Logs and Data Sources Available

Gmail Log Events

- Transaction logs based on inbound and outbound email flows
- Search based on header information (i.e. DKIM, SPF, etc.)
- Search based on attachment hash
- Contains full message headers and body contents
- Shows threaded messages in email chain
- Search limits on 30 days (see next section)
- Export limits apply

Gmail Messages

- Limited to only emails currently in Mailbox
- Limited fields to search on (standard Gmail search)
- Contains full message headers and body contents
- Shows threaded messages in email chain
- No time limit on search history
- Export limits apply



Google Workspace introduced the security investigation tool in 2022 to the Admin Console that now allows administrators to search both email transaction logs and emails currently within a user's mailbox. Previously, to search emails in a user's mailbox, an organization needed to use Google Vault, however, that is no longer the case.

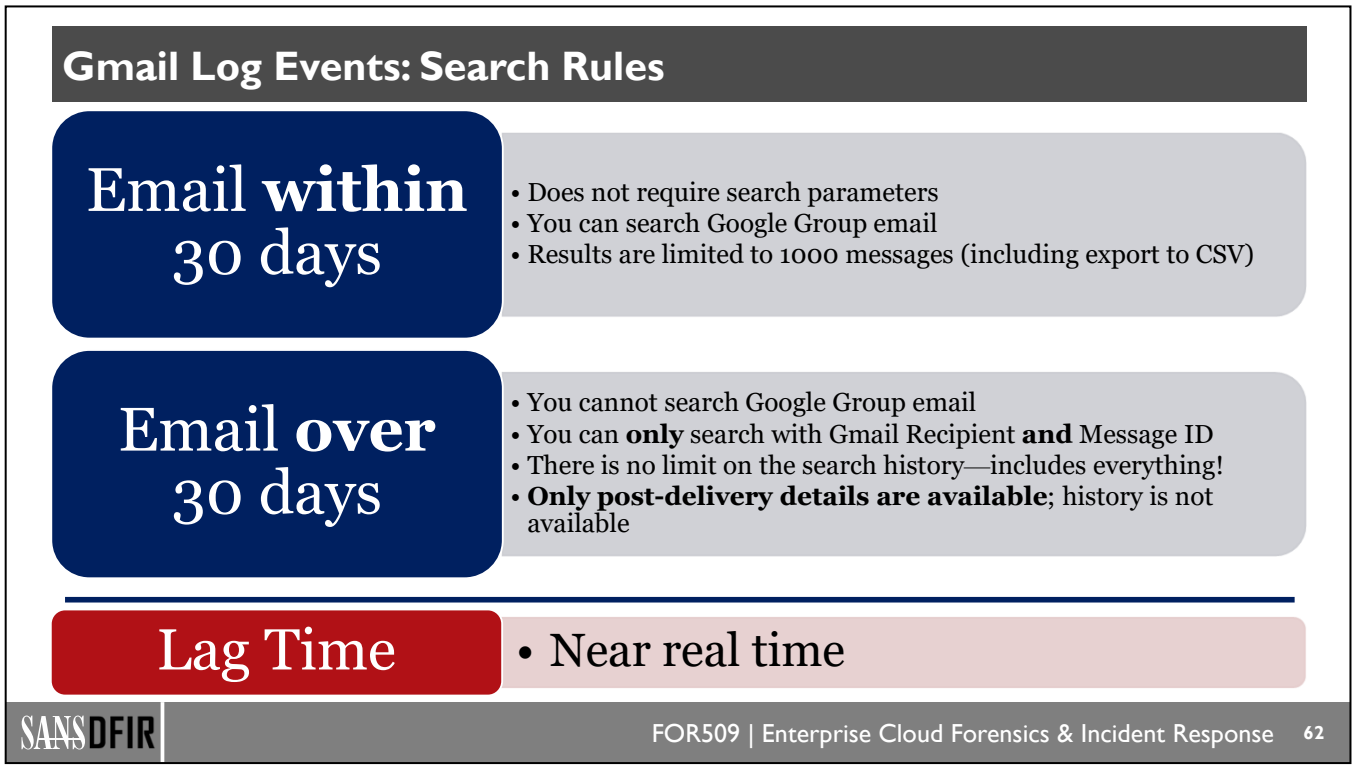
The Gmail Log Events are similar to email transaction logs. However, the new investigation tool provides a significant increase in the fields that are available to be searched. This is probably the most valuable log source for investigating phishing emails delivered or sent in the last 30 days. Using this log source, you get a wide range of header fields that previously weren't searchable, for example, being able to search on header From fields, SPF domain information, DKIM domain information, or even the malware family type and email attachment hash, will significantly help DFIR investigators. The only obvious limitation to this log source is the 30 days search limit, which we discuss later in this section.

The Gmail Messages log allows searching across users' mailboxes for any email currently within their mailbox. Unlike the Gmail Log Events, this log source does not limit how far back in time you can search, the only limit is based on what email is currently in a user's mailbox. If a user has deleted an email, then it has aged out of their Bin folder, you will not be able to see it within this log source. There are other ways of obtaining emails that have aged out of a mailbox Bin folder, which we'll look at later in this section. The limitation on the Gmail Messages log source is that the fields you can use for searching are significantly limited compared to the Gmail Log Events; that's not to say it is not helpful, only that the field types are limited to those fields a standard user could search if they were searching their own Gmail mailbox.

References:

https://for509.com/9d6yw (Gmail messages)

https://for509.com/2b0aw (Gmail log events)



When investigating a compromise mailbox or phishing email, the Google admin console provides you with the ability to search email transaction logs. These logs provide you the ability to see what email messages have been received inbound to your Google Workspace instance and what email messages have left your organization. Email transaction logs are searchable in near real time, or within a couple of minutes, depending on how large your organization is and whether your organization has been set up in a dedicated region. In most of the research that was performed for this course, email logs could lag by up to 24 hours; however, in most scenarios they only took minutes.

Google Workspace also stores the logs differently depending on if they are within the last 30 days or if they occurred over 30 days ago. Email transaction logs that occurred within 30 days do not require specific search parameters and can be displayed on the screen inside of the admin console. When you are viewing logs in this manner, they are also limited to only 1000 messages, which also applies to the export of the logs to CSV or a GSheet.

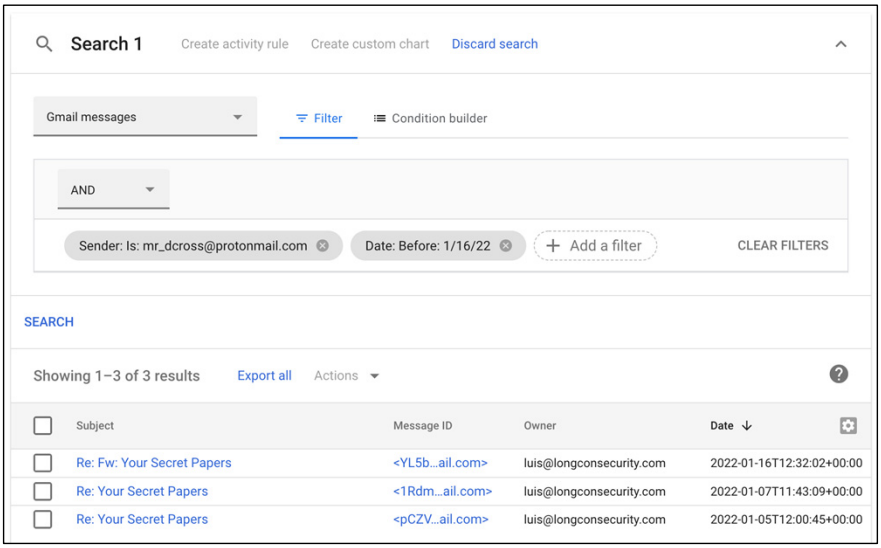
Email transaction logs that you wish to search for which may have occurred over 30 days ago can only be searched based on the recipient or message ID. The search history for anything over 30 days has no limit on it—this will include all email received by any user in your Google Workspace account. Additionally, you are also limited to only searching mailboxes owned by users; you cannot search for email transaction logs that occurred with Google Groups.

References:

https://for509.com/gi4t1 (Track message delivery with Email Log Search)

https://for509.com/ka3bn (Data Retention and Lag Times)

Gmail Messages Search (1)



Gmail Messages Log

- This recently moved to the Investigation Tool and provides more fine-grained searching of email data.
- For large organizations searches can take a while; use Message ID to speed up searching.

Within the Google Workspace admin console is the ability to perform searches against email transaction logs. The search interface was recently upgraded to include more fine-grained searching functionality, it is now included within the investigation tool within the Admin Console. Users are able to find email messages that are of interest based on sender or recipient or IP address information. When using the search functionality, it is fastest to search based on the message ID, if that is already known.

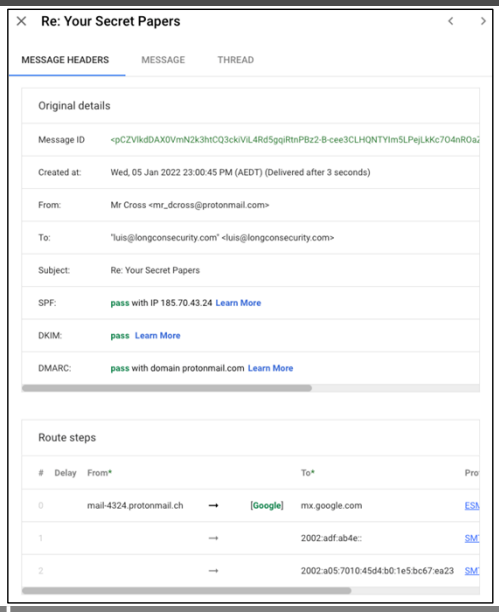
Remember that if you are searching for email transactions that occurred over 30 days ago you are restricted to being able to search only based on the message ID. Additionally, you are also restricted to only 1000 results per search, so ensure that your searches are specific so there are no results missing from your search that has run.

Using the email log search to look for email inside of a user's mailbox can be useful when a user has reported a phishing email and you need to determine how many other uses may have received the same phishing email. Furthermore, this can be useful when looking for a sender IP if the initial sender has used a different email address as part of the phishing campaign, but they have all originated from the same SMTP server. The only downside to using this method to search for phishing email is that you are limited to only the last 30 days of logs.

Reference:

https://for509.com/sh1iu (Track message delivery with Email Log Search)

Gmail Messages Search (2)



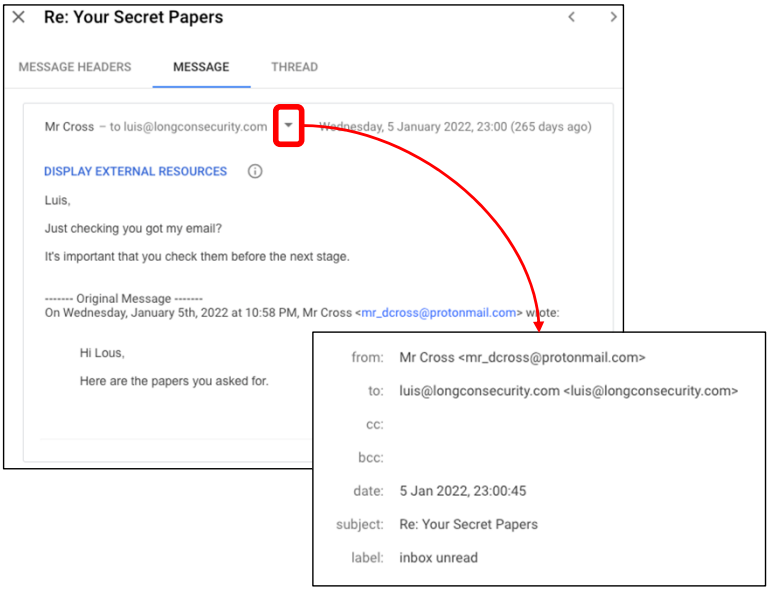
Message Detail

Once you click on an email from the previous screen header information can be extracted.

Once you have identified an email transaction from the email log search, you can then look at details about that email transaction showing your information related to the SMTP path that is transited to arrive at its final location. In the message headers section, it will show you details on if the email was fully delivered to the the user's mailbox.

it will also show you the current status of this email in a user's mailbox. This is helpful to understand whether users who have received an email have opened it or whether it is still in an unopened state inside a user's mailbox. This can allow you to decide whether you should remove an email, such as a phishing email, manually from a user's mailbox before they get the chance to open a malicious email.

Gmail Messages Search (3)



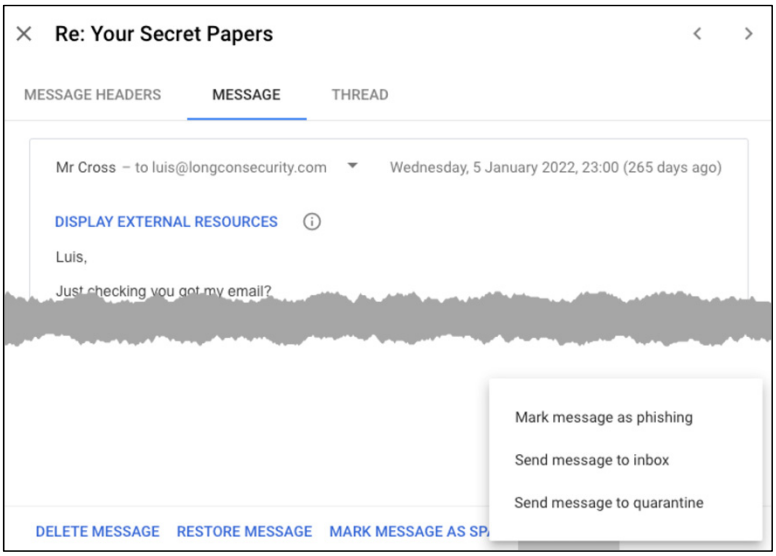
Message Detail

- The Message section provides full message content (body).
- From the dropdown arrow, details of the email status can be determined.

Within the Message section, an investigator will be promoted as to why they wish to see the full body contents of the email they are looking at, this detail is logged for auditing. Once the Message contents are visible, any external resources, for example images, are not loaded by default. This can give an investigator a better view of what the email may have looked like to the end user that received it.

Additionally, there is a dropdown arrow at the top of the Message section, this will show you the current status of this email in a user's mailbox. This is helpful in understanding whether users who have received an email have opened it or whether it is still in an unopened state inside a user's mailbox. This can allow you to decide whether you should remove an email, such as a phishing email, manually from a user's mailbox before they get the chance to open a malicious email.

Gmail Messages Search (4)



Message Actions

- Within the Investigator Tool admins can perform actions on emails after they are delivered.
- This can range from;
  - Delete/Restore
  - Un/Mark as Spam
  - Un/Mark as Phishing
  - Send to Admin Quarantine

Within the Investigator Tool it is now possible to perform actions on some search results. In the case of emails, if we find an email that should really be removed from a user's mailbox, that action can be taken all from within the Admin Console. The actions are fairly simple in their ability, very similar to what a user would have the options within their own mailbox, with only one exception, quarantine.

Marking an email as Spam or Phishing has the same effect from a user's perspective, the email is sent to the Junk folder. The only difference is what information is sent to Google about the email you've identified. You can also remove an email from the Junk folder by using the Send Message to Inbox option.

For messages that should be removed, as they may contain sensitive data, you can use the Delete Message option, which will remove it from the user's mailbox. You can also restore messages with the Restore Message option.

For emails that are malicious in nature and need to be removed from a user's inbox to protect the organization, and the user, you should Send Message to Quarantine. This is the only additional option that an admin can perform, that a user cannot. This will remove the email from the user's mailbox and put it in the Workspace Quarantine, however, if the email is older than the retention policy for emails it will be immediately deleted from your Workspace. More details on retention policies are provided in an upcoming section.

Reference:

https://for509.com/jfl07 (Take action based on search results)

Gmail Log Events Search

Gmail Log Events

- Email that gets quarantined, or rejected in transit, will only appear in Gmail Log Events.
- This is because the email would have never made it to the end user.
- Emails, like this example, will only be searchable for 30 days, unless you record the Message ID.

The Gmail log events search can also be useful to see emails that may have been quarantined by Google. It's possible for inbound emails, sent to users, to automatically get quarantined by Google without any notification to the user or the administrators of Google Workspace. Additionally, the sender does not receive a notification when Google quarantines an email this way.

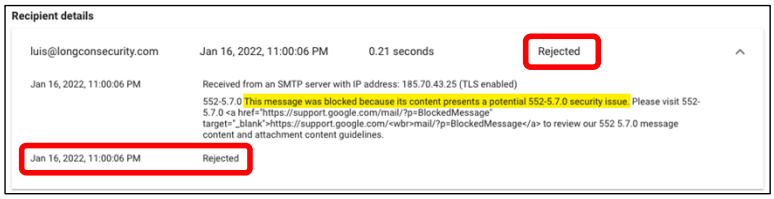
The above is an example of one such email that has been quarantined due to the rules that Google has in place around receiving attachments. The above inbound email had an attachment with an executable file inside of a zip file. This file type is blocked by Gmail by default[1] and is automatically quarantined, as shown above.

1. https://for509.com/q4fsa (File types blocked in Gmail)

Gmail: Advanced Phishing & Malware (1)

Blocked Attachment Types

- Gmail will automatically block a number of file types and prevent delivery, even if they are in compressed files including some password-protected files.
- Attachments with malicious macros are also blocked by the same Gmail service.
- There is no way to access these email messages when they are blocked by Gmail.
- Evidence of these are only shown in the Email Log Search log when you expand the "Recipient details" section.
- These blocked email messages are not shown in Vault or in the Quarantine.



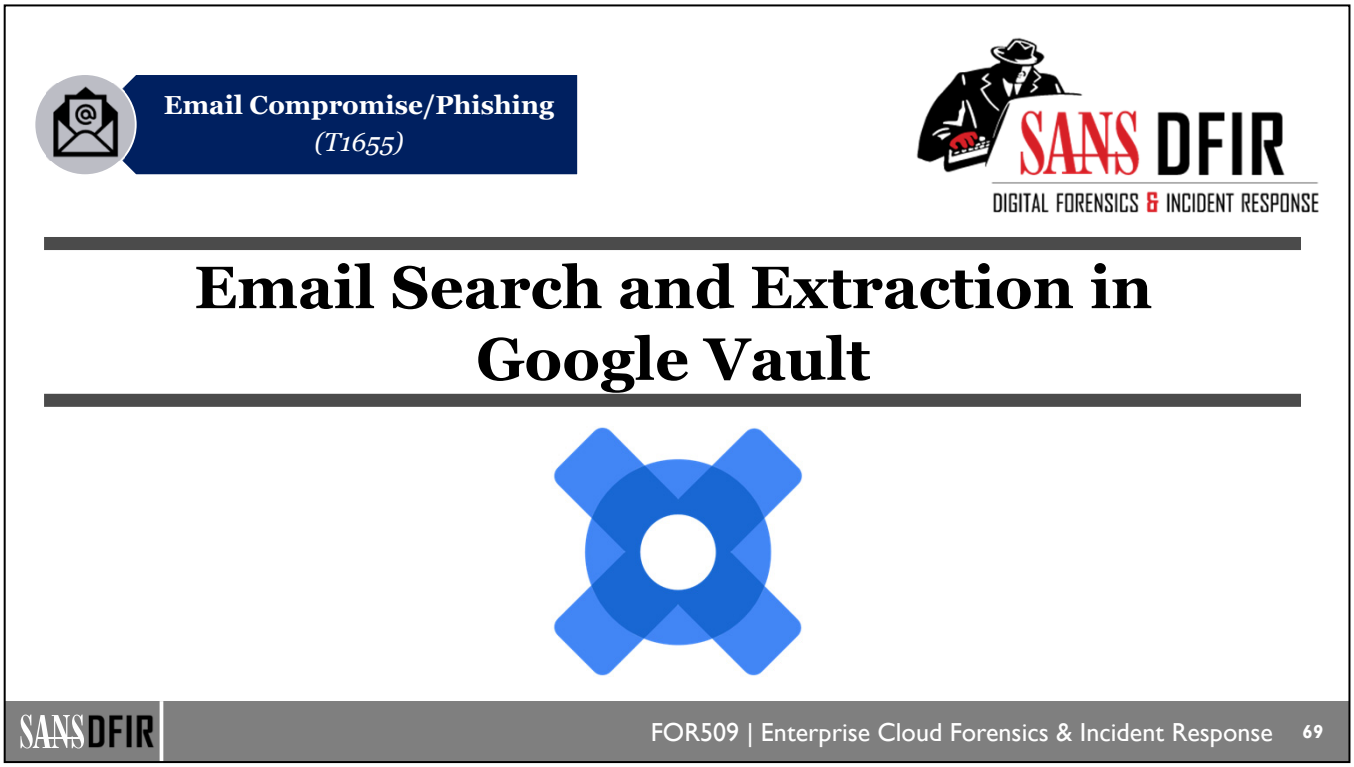

```
.ade, .adp, .apk, .appx, .appxbundle,
.bat, .cab, .chm, .cmd, .com, .cpl,
.dll, .dmg, .ex, .ex_, .exe, .hta,
.ins, .isp, .iso, .jar, .js, .jse,
.lib, .lnk, .mde, .msc, .msi, .msix,
.msixbundle, .msp, .mst, .nsh, .pif,
.ps1, .scr, .sct, .shb, .sys, .vb,
.vbe, .vbs, .vxd, .wsc, .wsf, .wsh
```


Gmail has a number of automatic blocking filters enabled based on attachment type for inbound email. Above is a list of the attachment types that are prohibited for inbound email. These are automatically blocked and rejected, as shown previously. This will also include any of the above attachment types inside of a zip or compressed file with no password. Gmail will also attempt to brute force password-protected compressed files with common password names—for example, “infected”.

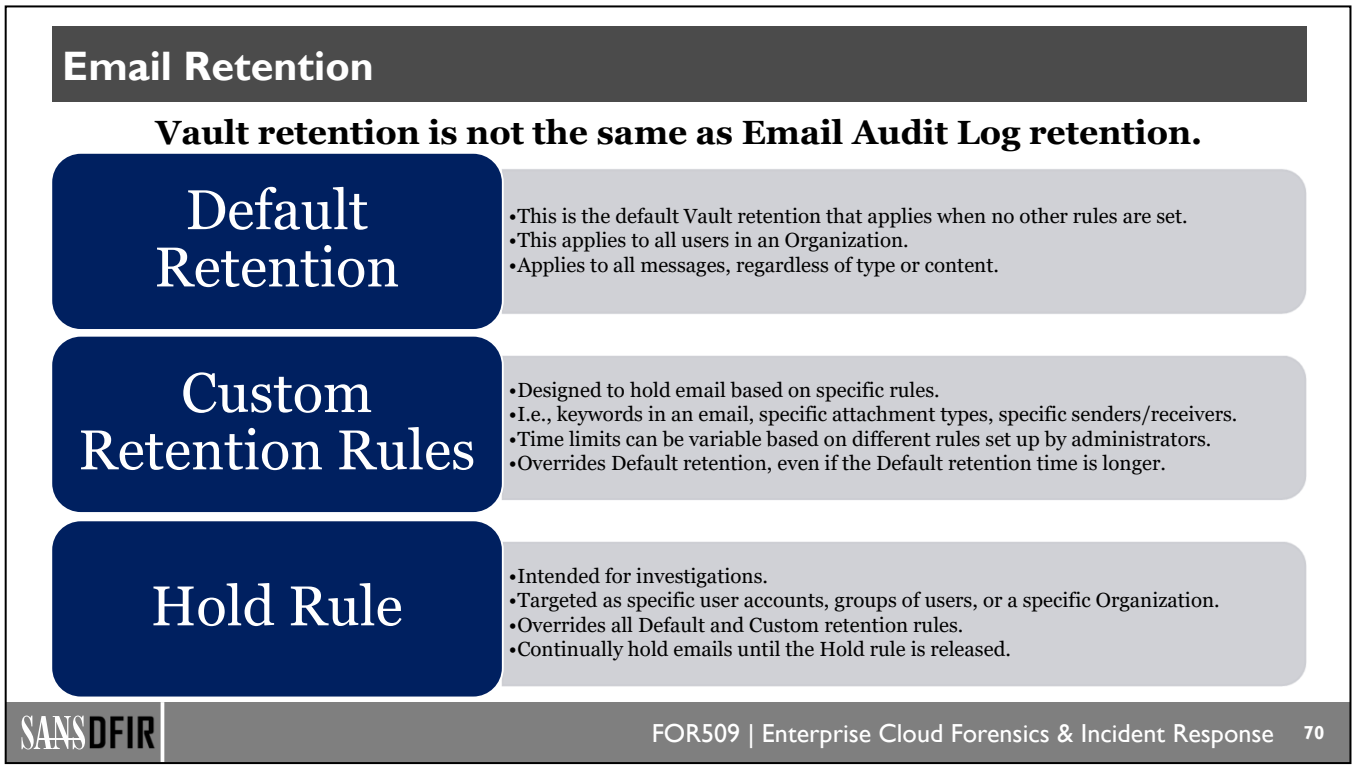
Email that gets blocked in this manner only ever appear in the email log search section of Google Workspace; they will not appear in Vault or in Quarantine inside of the admin console. This is because they are blocked by Google’s Gmail gateway which assesses email before it even arrives into a Google Workspace organization's data store. This means there is no possible way to retrieve email that you identified as rejected or blocked because they include one of the attachments above.

Reference:

https://for509.com/n41a2 (File types blocked in Gmail)



This page intentionally left blank.



Performing an email-based investigation is always dependent on how long the data is retained inside of Google Workspace. Understanding how email is retained is a key component to being able to perform email-based investigations. Unfortunately, this is not as simple as giving a certain number of how many days an email is retained for as there are a number of exemptions that can apply to email based on settings with inside of Google Workspace.

To start with, understand email is retained in the user's mailbox for as long as they leave it outside of the Trash folder. This means that if users never delete email in the mailbox, the email itself is retained permanently until the mailbox is either removed or until the user deletes an email.

Once a user deletes an email in the mailbox, it's moved into the trash folder. Email stays in a useless trash folder for up to 30 days by default. Once 30 days has reached the email is then deleted from the user's trash folder and is no longer visible to the user. Once this has occurred, a number of different scenarios may occur depending on what happens with the email that has now been removed from the user's mailbox.

Before we talk about specific retention rules, inside of Google Workspace, it's important to understand that, again, once an email has been removed from the user's trash folder the email is then held for 30 days by Google by default. This means that the email would be searchable inside of Google Vault and would still appear in other log analysis tools and investigation tools inside of the Google admin console.

Default Retention Rules

In the Google Workspace licenses that include Vault there is the ability to set a default retention rule for Gmail, Drive, Groups, Chat, Meet, and Sites. For a brand-new Google Workspace there are no default retention rules set so these will have to be manually enabled. This means that by default on a brand-new Google Workspace instance that had the Google Vault feature enabled the default 30-day retention by Google is all that would be applied to email after they fall out of a user's mailboxes trash folder. The Google Vault default retention rules can be sets from and definitely down to one day.

Additionally, the retention rules can be used to not only purge messages that are considered expired (email messages that have been sitting in trash for 30 days), but they can also permanently delete messages after they have been sent or received. This is only used inside of organizations that are extremely sensitive to holding data inside of mailboxes and ensuring that the messages are removed within a certain time frame after they have been read or sent. This latter option is rarely used.

Custom Retention Rules

The default retention rules applies to all mailboxes across the entire Google Workspace organization; however, you may want to create custom retention rules based on specific users or keywords inside of an email or documents. To do this you would create a custom retention rule. Custom retention rules override default retention rules regardless of if the custom retention rule is shorter than the default retention rule. This means it could be possible to have email messages removed earlier than what the default retention rule is set to.

Hold Rules

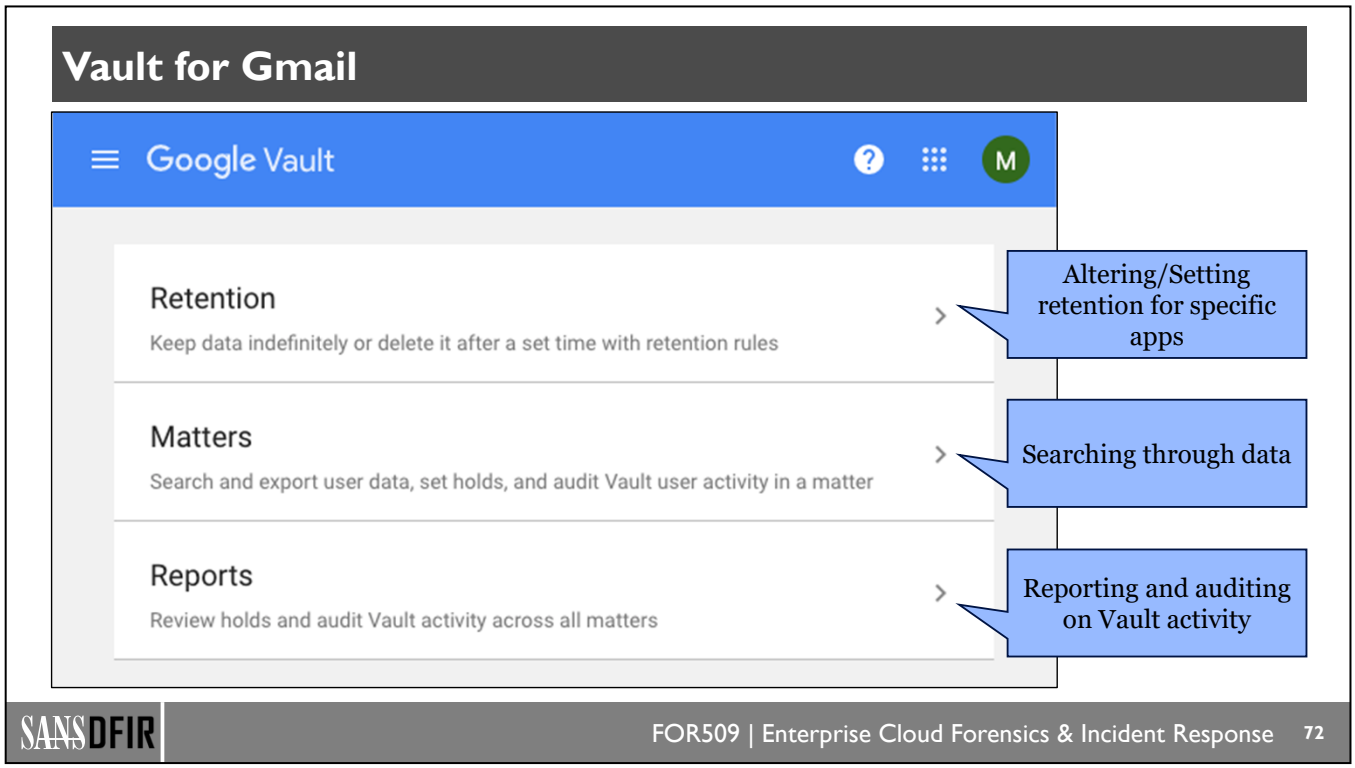
As with a lot of investigations there are often times where we might be investigating a user's mailbox, or specific types of email that have been sent and received inside an organization, and we want to maintain that evidence without any retention rule taking over and removing email. This may also apply to Google is built-in 30-day retention after an email has been removed from a user’s trash folder. To enable this, we can use hold rules inside of Google Vault—this allows us to ensure that no email or documents related to investigation are purged so that we can maintain evidence and continue to perform analysis. Hold rules will also apply for new email or documents that are generated that meet the rule requirements. This process is also sometimes referred to as a legal hold when you need to ensure that a user cannot remove evidence that may be required for legal reasons.

References:

https://for509.com/sr9ok (How Retention Works)

https://for509.com/zup3t (Retain Gmail Messages with Vault)

https://for509.com/y1v0u (Data retention and lag times)

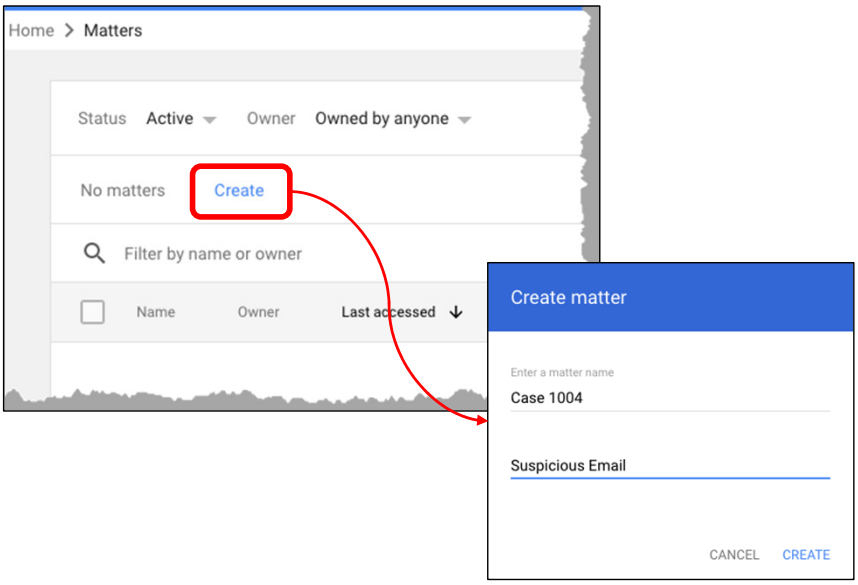


Above is an example of what Google looks like when you first initially access the Vault. You're given the option to set up retention rules, create a new matter—this is where we would perform searches through mailboxes or Google Drive documents—and auto generate reports, which is useful when we need to understand when a hold or search was run against a user's mailbox or Google Drive documents.

Reference:

https://for509.com/xj31n (What is Google Vault?)

Vault: Creating a Matter



Create Matter

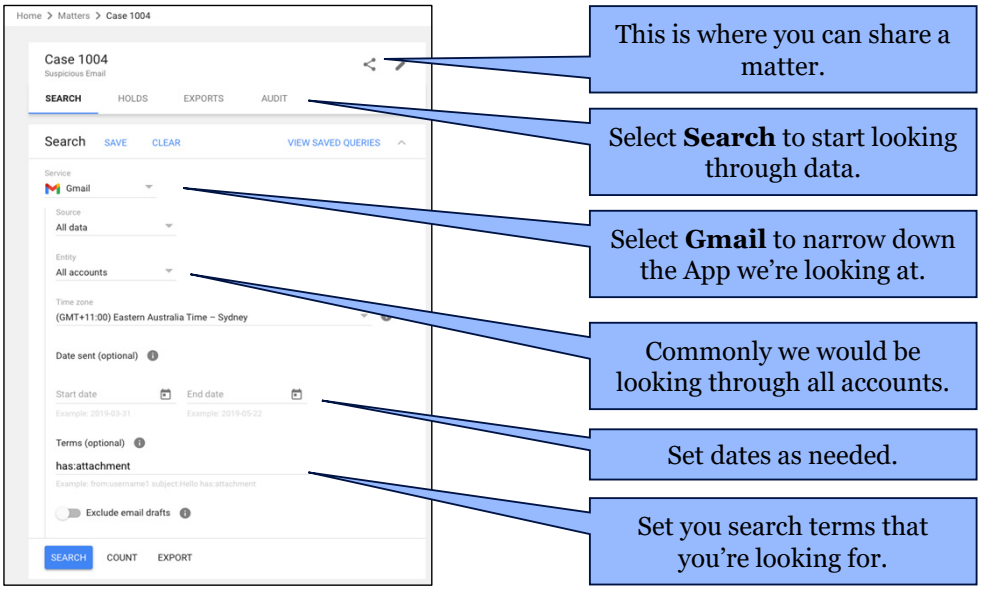
- To be able to search in Vault, you first need to create a "matter".
- This will hold all your search activities.
- You can also collaborate with others inside a matter.

To perform an email-based search against all the users' mailboxes, we would need to create a new matter.[1] A matter is used to hold the searches that we would perform based on a specific type of investigation that we may be doing. Often during investigations, you would set up a new matter for the case that you are working on. If you had several cases that you were investigating, typically you would have a separate matter for each of those cases as a way of compartmentalizing investigations you're performing and data you are obtaining for that investigation.

Multiple investigators can also work together on one matter. Once you have set up a new matter you can share access to that matter with other users you also have access to in Google Vault inside your Workspace.[2] This can allow you to more easily collaborate on larger investigations.

1. https://for509.com/9ghop (Create and manage matters)
2. https://for509.com/954gu (Share matters with other Vault users)

Vault for Gmail: Search



Once you have set up a matter inside of Google Vault you can then determine which service you want to start searching. For an email investigation, you would select Gmail as the service type and then start to fill in the search parameters required for your investigation. The Google search inside of Vault has a small number of preset fields that you can use to run a search. This search allows you to specify a particular user account or search all the accounts across the entire Workspace organization. There is also the "Terms (optional)" search at the bottom which allows you to run more complex searches across all users' mailboxes.

Reference:

https://for509.com/ze603 (Use Vault to search Gmail and classic Hangouts)

Vault for Gmail: Searching Rules & Terms

- Vault can search for English words and numbers; it does not search punctuation.
- Use "**-**" or "**NOT**" to exclude a search term.
- You can use "**field:value**" to search a field for a specific value.
- Vault assumes "**AND**" when there are spaces between search terms.
- Valid search operators include:
  - **AND**
  - **OR**
  - **NOT**
  - *****
  - **AROUND**

```
to:
from:
cc:
replyto:
in:inbox
in:spam
label:ProjectX/parts
is:read
is:unread
larger:1M
larger:20K
filename:secrets.zip
filename_exect:SeCrEts.zip
has:attachment
```

```
to:luis@longconsecurity.com AND from:*@protonmail.com AND
has:attachment AND (larger:20K AND smaller:100k) AND ("urgent"
OR "secret" OR open AROUND 15 attachment)
```

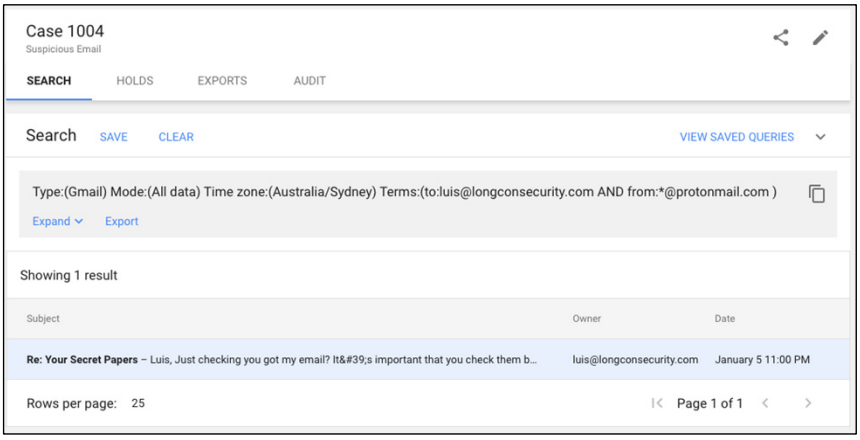
SANS DFIR FOR509 | Enterprise Cloud Forensics & Incident Response 75

Using the "Terms (optional)" field within Vault search for Gmail allows you to run more complex searches similar to what you can run in the search field inside of Gmail. This can allow you to run searches with complex operators and fields along with excluding field information as well. There is a large number of fields and operators that can be used inside of Vault;[1] what is provided above are just the more common search terms used for investigation. The below reference contains a complete list of all fields in terms that can be used.

There are some limitations when it comes to performing a search with Vault. You can only search English-based words, which means the characters from other character sets cannot be searched. Additionally, Vault only allows for searching of letters and numbers—it does not search based on punctuation. This also means it's not possible to search for a href link inside of HTML in an email, which could be extremely important when looking for phishing email with embedded links.

1. https://for509.com/v5wgh (Use operators to refine a search in Vault)

Vault: Searching Gmail (1)



Search Results

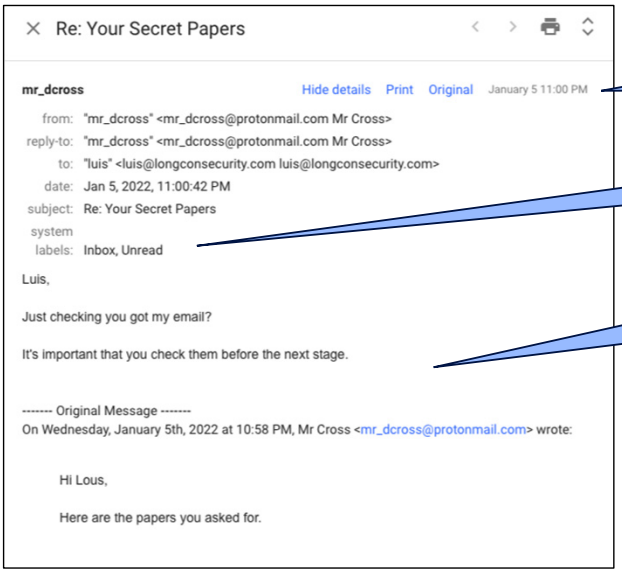
- Results are group based on email thread, similar to how they are grouped within a Gmail inbox.
- You may not see all the email across all your user accounts until you click on the email thread shown.

Once you've run a search, which can sometimes take a number of minutes depending on how large organization is, the results are displayed back to you in a threaded list. This is similar to how email would appear inside of a user's inbox; however, in this scenario you are looking at a threaded email across the entire organization. This means that the one row shown above may contain multiple email messages that you would not see you until you have clicked on this row.

Reference:

https://for509.com/0cbpg (Use Vault to search Gmail and classic Hangouts)

Vault: Searching Gmail (2)



Expand "Details" to see all header information.

System labels will tell you the emails current state in the user's mailbox.

You will have full body content, including any previous content included in the body.

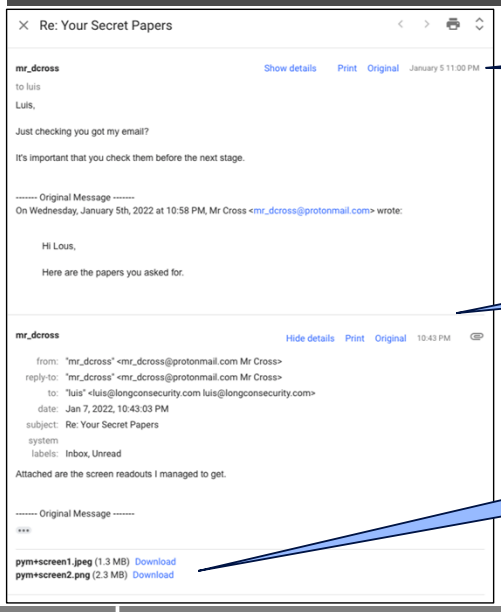
Search Tip

You can use the message content to also exclude email messages that don't match your intended search.

Once you click on the results you will then get to see metadata details about the email, along with the email body and details on the current state of the email inside of users' mailboxes. As described earlier, understanding the state that an email is currently in inside of users' mailboxes can be helpful in assessing if a user has viewed the email or not, which could help determine if a user is likely within scope for your investigation of malicious email.

If this is the first search that you have run inside of Google Vault, you may also find your results are returning email messages that are not relevant to your investigation. Remember that you can use information from the email messages that are not relevant and exclude them by refunding your search further with the minus or "NOT" parameter.

Vault: Searching Gmail (3)



The time you see in here is the time zone of the local system you're using your web browser from.

Where there are multiple messages in a thread, they are grouped together when you view their detail in Vault.

Attachments on email are directly downloadable from the message detail screen.

When viewing email inside of Google Vault, it's important to remember that the time that you are seen displayed to you on screen is based on your browser's local system time. At the time of publishing this content you are not shown UTC information to be able to determine this yourself quickly.

You will also be able to see attachments and download them while viewing an email from your search results. Be cautious when downloading attachments as they are downloaded in their original form with no protection. This can sometimes cause issues if your local system's antivirus detects the download is malicious and removes it from your system. Attachments are not shown in the browser, so there is a little risk of an attachment auto opening and exploiting your browser—they are instead forced as a file download.

Re: Your Secret Papers

mr_dcross Show details Print Original January 5 11:00 PM

to luis

Luis,

Just checking you got my email?

It's important that you check them before the next stage.

------- Original Message -------
On Wednesday, January 5th, 2022 at 10:58 PM, Mr Cross <mr_dcross@protonmail.com> wrote:

> Hi Lous,
>
> Here are the papers you asked for.

mr_dcross Hide details Print Original 10:43 PM

from: "mr_dcross" <mr_dcross@protonmail.com Mr Cross>
reply-to: "mr_dcross" <mr_dcross@protonmail.com Mr Cross>
to: "luis" <luis@longconsecurity.com luis@longconsecurity.com>
date: Jan 7, 2022, 10:43:03 PM
subject: Re: Your Secret Papers
system labels: Inbox, Unread

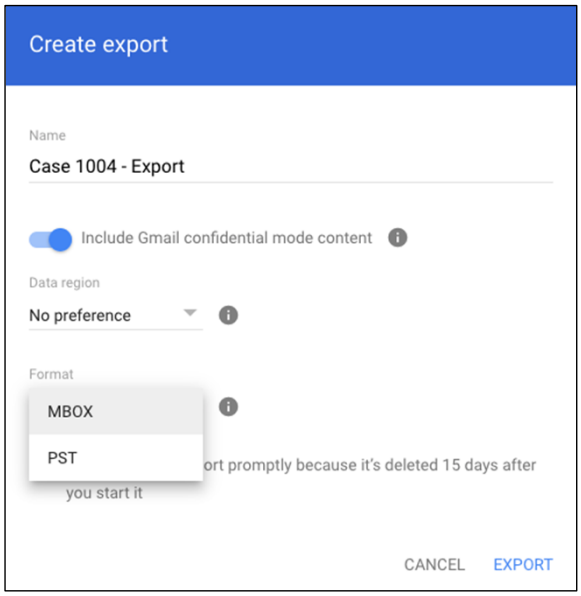
Attached are the screen readouts I managed to get.

------- Original Message -------

•••

pym+screen1.jpeg (1.3 MB) Download
pym+screen2.png (2.3 MB) Download

Vault: Gmail Export (1)



Search Results

- To retain search results as evidence in a case you must export the results.
- MBOX is the most versatile format for exporting and analyzing data.
- Vault can also be used to export and search email created with Gmail's Confidential Mode.

Once you have created a search that matches the email you are looking for as part of your investigation, you can then export the email and data associated with the investigation to hold as evidence for your case.

Depending on the size of your organization and the quantity of results you are trying to export, it can take several minutes or hours to export results from Google Vault. This means that you will have to give your export a name that is relevant to your case so you can find it once all the results have been collated and are ready for download. You also need to decide at this point whether you want the export made available to you in MBOX format or PST format. Most incident responders choose MBOX as it is the most versatile and easiest to consume once it has been downloaded.

You can also limit your export to be in a specific data region if you have requirements around the data not leaving Europe or the United States. Outside of these two regions the only option is "no preference".

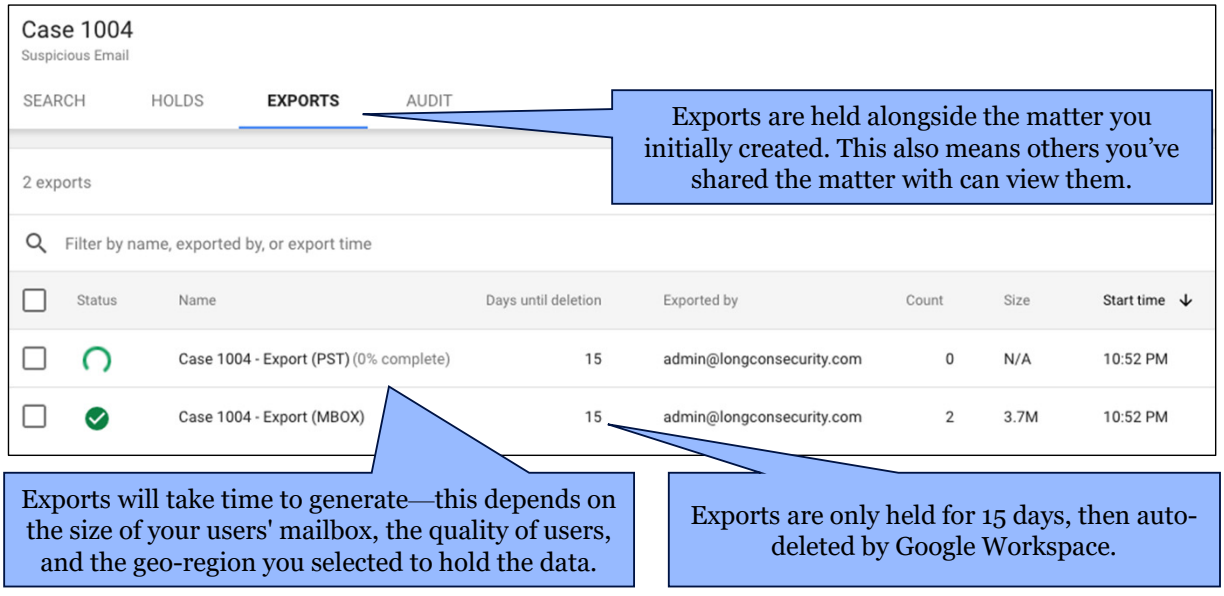
You will also notice an option around including Gmail content that was created in confidential mode. Google Vault will allow searching and exporting of Gmail email messages even if they were created in confidential mode.

References:

https://for509.com/t158g (Export data from Vault)

https://for509.com/iw6sz (Choose a location for your Vault export data)

Vault: Gmail Export (2)

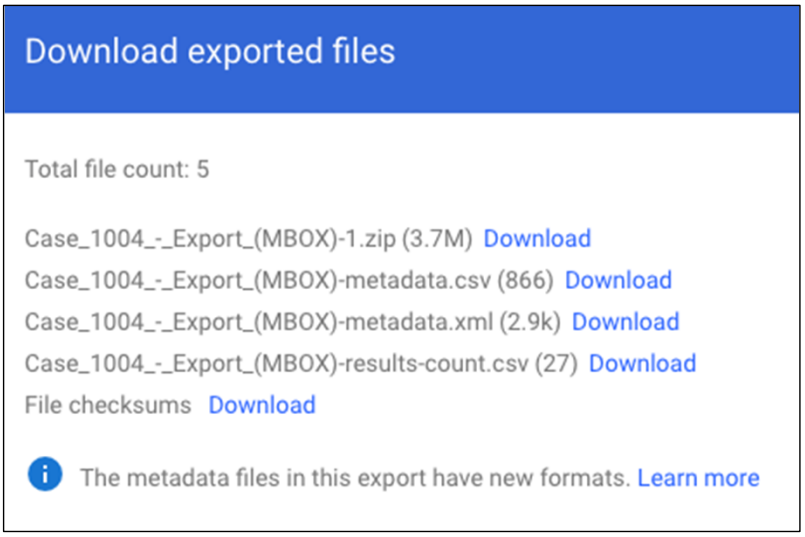


An export's search results can take minutes to hours to complete depending on the size of your organization and the quantity of results you're attempting to export. Exports from Vault are never instantaneous, regardless of how small an organization is. You can find the results of your exports under the Exports tab inside of the matter that you initially created for your search. You can also produce a number of exports based on different searches you may have run for a single investigation. You will have up to 15 days to download the results of your export before they are automatically deleted by Google Workspace; however, there is no limit on how many times you can download the export within the 15-day limit. Keep in mind that anyone that you have shared the matter with will also be able to download these results.

Reference:

https://for509.com/tak0w (Download an export from Vault)

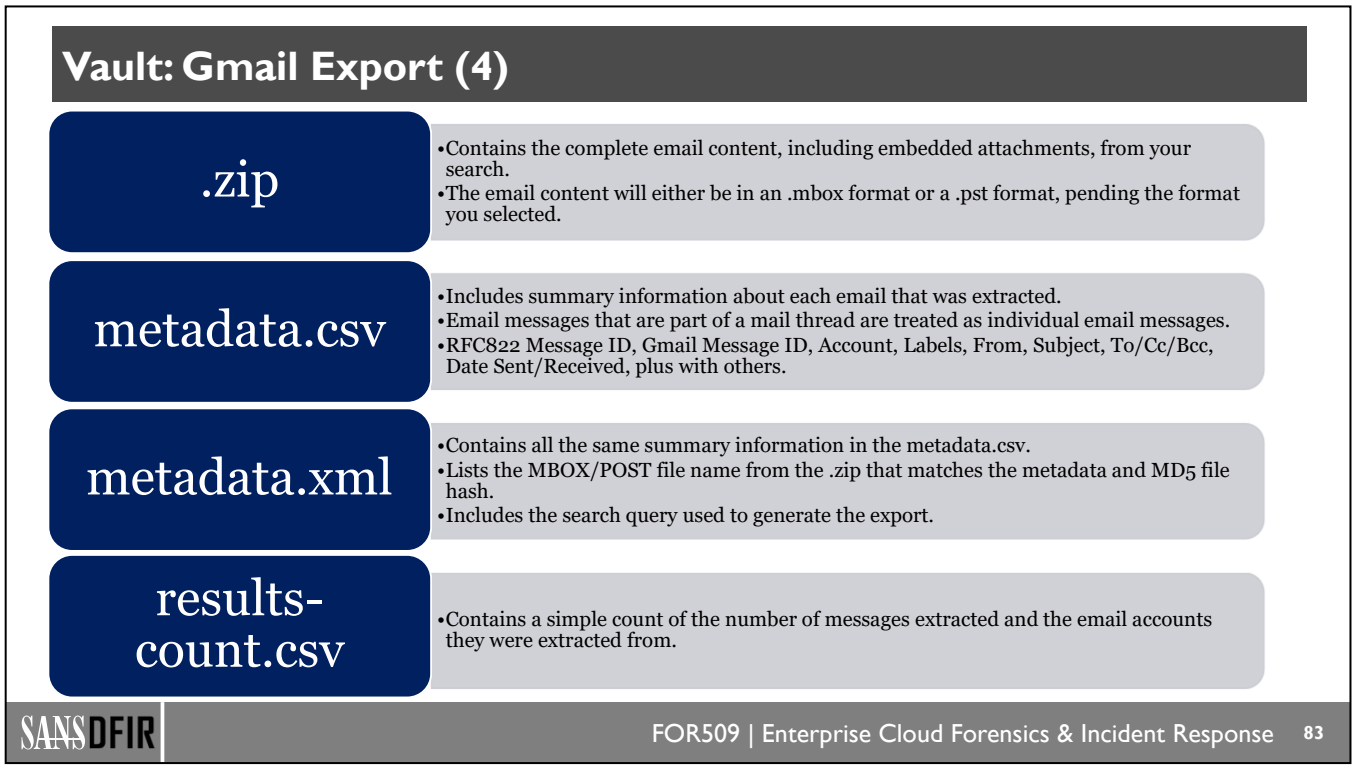
Vault: Gmail Export (3)



Download Files

- When you download results from an export you are presented with multiple files to download.
- From a DFIR perspective you need to download all five of the files.

Once you click on one of the exports it will present you with five file types to download. You should download all five of these file types as they all contain different information which is useful to hold as evidence for a case.



Within the files that you are presented to download is a .zip file that contains all of the email contents in either the MBOX format or PST format that you selected at the time of the export. This .zip file also includes attachments to any of the email messages as well, so be aware that if you have antivirus running on the system where you are downloading this file it may identify the file as malicious and quarantine it.

The metadata.csv file contains metadata information about the email messages that is extracted based on your search along with summary information about the email messages as well.

The .XML file is similar to the metadata.csv file in that the contents it contains are related to the email messages from your search; however, it also includes the search query that you used to generate the export.

The results-count.csv file contains a very simple count on the number of messages that are extracted and the number of email accounts that they originated from.

The checksum file that can also be downloaded as part of the export results contains a checksum for all of the other files to ensure that you have downloaded the complete file and no data has been lost or manipulated in transit.

Reference:

https://for509.com/42v7m (Vault export contents)

Vault: Gmail Export: metadata.xml (1)

```
<Documents><Document DocID='ACD7onoeJjHxuZ1yEiZkNyBZTJak[SNIP]>
<Tags>
<Tag TagName='#From' TagDataType='Text' TagValue='mr_dcross@protonmail.com Mr Cross'/>
<Tag TagName='#To' TagDataType='Text' TagValue='luis@longconsecurity.com
luis@longconsecurity.com'/>
<Tag TagName='#CC' TagDataType='Text' TagValue=''/>
<Tag TagName='#BCC' TagDataType='Text' TagValue=''/>
<Tag TagName='#Subject' TagDataType='Text' TagValue='Re: Your Secret Papers'/>
<Tag TagName='Labels' TagDataType='Text' TagValue='^INBOX,^UNREAD'/>
<Tag TagName='#DateSent' TagDataType='DateTime' TagValue='2022-01-05T04:00:42.000-
08:00'/>
<Tag TagName='#DateReceived' TagDataType='DateTime' TagValue='2022-01-05T04:00:45.181-
08:00'/>
</Tags>
<Files> <File FileType='Native'>
<ExternalFile FileName='1721115916690188496-40e42373-e652-498d-a2b4-a83f54d53ab4.mbox'
FileSize='6907' Hash='9175288aea8ca5c22bd269dfca82148d'/>
</File></Files></Document>
```


The above XML data, from the metadata file of a Google vault export, is a sample record of one of the email messages from a vault export. The metadata file itself contains multiple entries that represent all the email extracted as part of a vault export. For brevity, we have condensed the XML data in the above slide; however, it would be formatted correctly in the actual metadata file.

There are a few interesting elements contained in the metadata XML file. To start with, the Date Sent and the Date Received timestamps do not match the time zone of where the email originated from or where the mailbox for the user is located; it also does not match the location of where the Google Workspace admin was located when the Google Vault export was produced. It is likely that the timestamp contained in the XML is the location of the MTA SMTP server that last processed the email before it arrived in the user's mailbox.

While the BCC field is included in the metadata file, this field would only be relevant if the email originated from inside the Google Workspace organization of where it was exported. Even if this was an inbound email with multiple recipients in the BCC field, there would still be individual email messages inside the metadata XML file with the recipients in the To field.

Reference:

https://for509.com/42v7m (Vault export contents)

Vault: Gmail Export: metadata.xml (2)

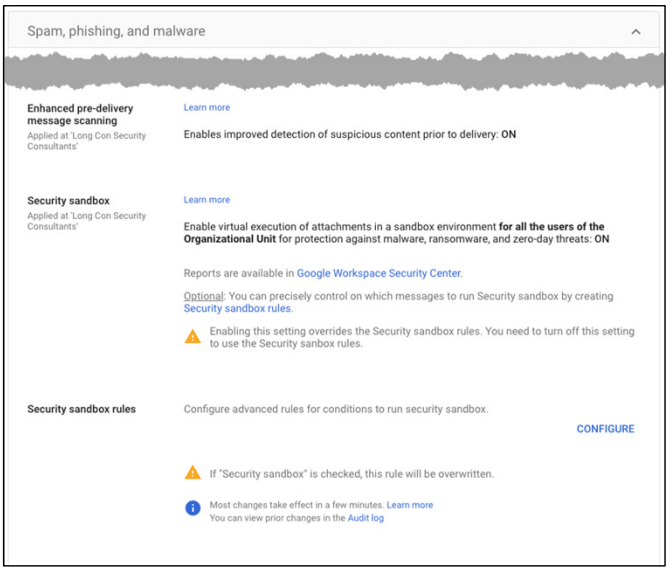
```
[SNIP]
<CustomBatchInfo>
    <Query>
        <UserQuery>( to:luis@longconsecurity.com AND from:*@protonmail.com  )
        </UserQuery>
        <TimeZone>GMT+10:00</TimeZone>
        <Custodians></Custodians>
    </Query>
</CustomBatchInfo>
[SNIP]
```

Within the Query tags you will also have the TimeZone field that shows the time zone used for time-based searches to produce the export.

Within the UserQuery tags in the XML you will have the full search query that was used to generate the export. Keep this for your case notes.

At the base of the metadata XML file is the query used to generate the results for the Vault export, along with the time zone of the operator that generated the Vault export. Again, the above XML data has been condensed for brevity so that it fits within the page.

Gmail: Advanced Phishing & Malware (2)



Phishing & Malware Detection

- Gmail provide two key phishing and malware detection tools useful for DFIR.
- **Enhanced pre-delivery message scanning**, on by default, checks mail for phishing email. If detected, email messages are moved to a user's **spam** folder.
- **Security sandbox**, off by default, will send attachments to a sandbox in an attempt to identify malicious content. If detected, email messages are moved to the user's **spam** folder.
- **Security sandbox** detections are in the Workspace security center.

Google Workspace contains a number of advanced phishing and anti-malware detection and defensive measures. Two of the key tools used by Gmail are the enhanced predelivery message scanning, which is on by default. This feature checks email to determine whether they may be considered spam, in which case they are moved to the user's spam folder.

The second feature, which is off by default, is the security sandbox. This allows you to send email with attachments to a sandbox that attempts to categorize any malicious content in the email or its attachment. In the event that an attachment is detected as malicious, it is moved into the spam folder of the user's mailbox. In addition to this, any malicious detection from the security sandbox is also recorded inside the security center within the admin console.

Unfortunately, not a lot of logging is currently available for either the enhanced pre-delivery message scanning or the security sandbox, outside of detections from the sandbox that are recorded in the security center.

In addition to these two security features to detect suspicious or malicious content, there is also the ability to set up compliance-based rules to block or quarantine email based on the words, phrases, or patterns within the body of an email. It is also possible to set up compliance-based rules based on common attachment types where text-based information can be extracted. This can be used to prevent sensitive information from leaving an environment. For an investigator, this feature can also be useful if you are attempting to monitor a threat actor but also wish to prevent sensitive information from leaving an environment.

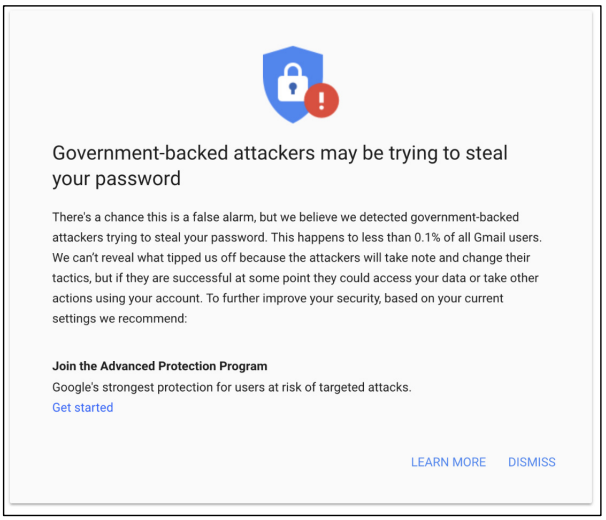
References:

https://for509.com/hufjn (Help prevent phishing with pre-delivery message scanning)

https://for509.com/1bm93 (Set up rules to detect harmful attachments)

https://for509.com/sgfc3 (Set up rules for advanced email content filtering)

Gmail: APT Attack Notifications



Government-Backed Attacks

- Google protect all accounts with government-backed attack detection.
- An alert (left) is given to users when a detection occurs.
- Workspace admins are notified in the **security alert center**. This alert will provide details of detections, the user impacted, and suggested actions.
- These events will not impact any other logs produced by Workspace. If an APT sent an email, the email will still be in **Vault** and the **Email Log**.

Google also monitors all of the Gmail accounts for nine attacks by government-backed actors. Details about this program and the detections used are often kept secret so that government-backed threat actors can't find new ways to evade these detections. When an email or attachment is detected as a potentially targeted attack by a government-backed threat factor, users will be alerted with the above message and Workspace admins are notified within the security alert center.

Email messages or attachments that are detected as a government-backed attack will still appear in all of the common email logs and within Vault. There may also be times when Google does not provide a lot of detail around the email or attachment that is detected as being government backed—they may simply provide details that one of your users have been targeted.

When users within your organization are targeted by government-backed threat actors, Google will often recommend that your users join the advanced phishing and malware protection program. This program is intended to provide stronger security measures to Gmail account users. In fact, this program requires you to enable all security settings provided to the Gmail service. If you opt to disable any of the security features, you are automatically removed from the advanced phishing and malware protection program.

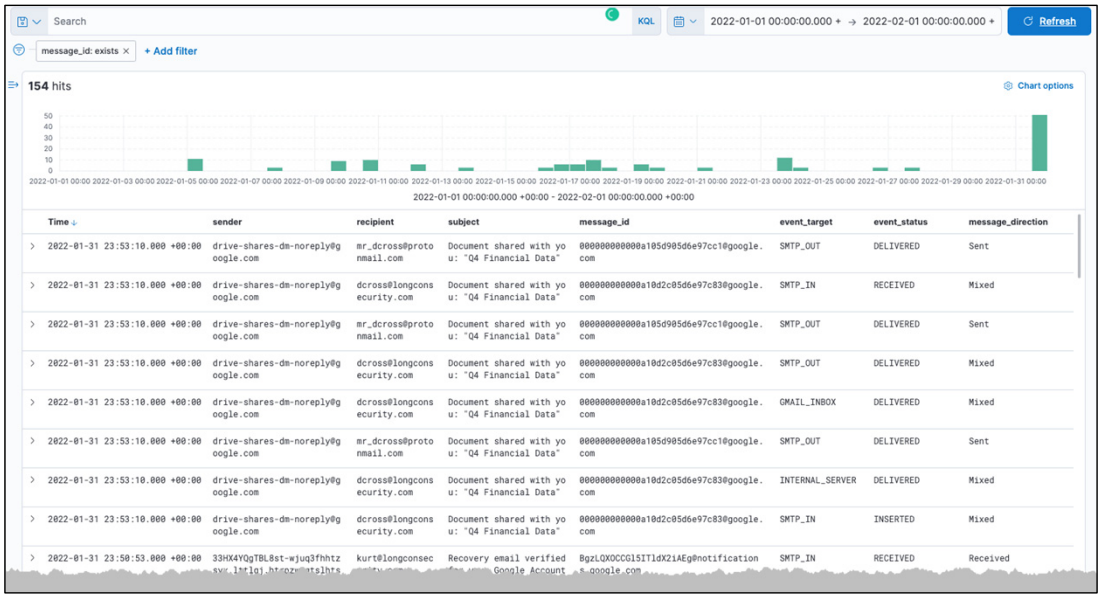
References:

https://for509.com/wtxku (Reassuring our users about government-backed attack warnings)

https://for509.com/5n3e6 (A reminder about government-backed phishing)

https://for509.com/6gz9p (Advanced phishing and malware protection)

Lab 4.1: Google Workspace Admin BEC

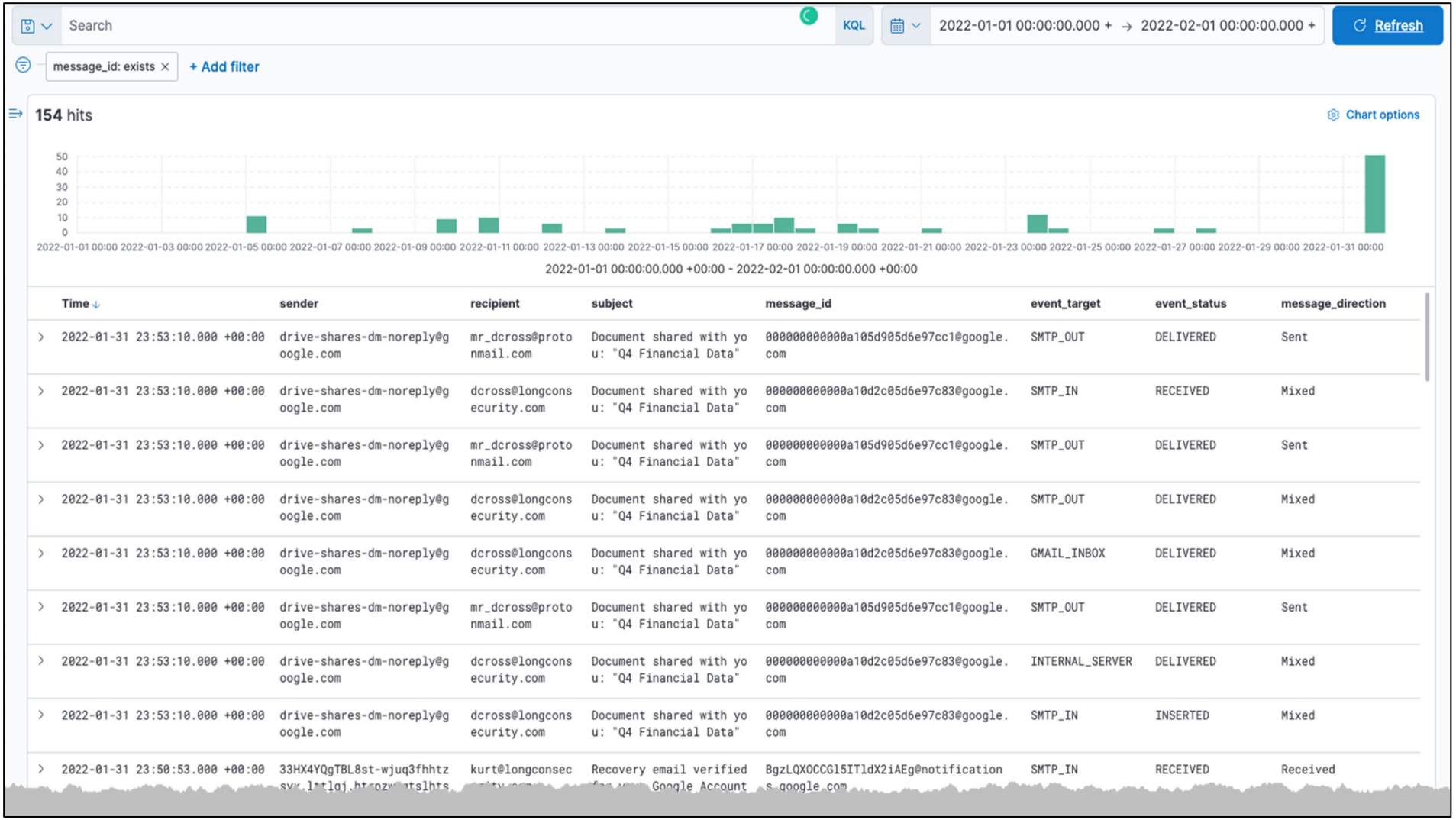


This example shows you the Gmail logs extracted via API from Google Workspace in JSON format and loaded into SOF-ELK. In the upcoming lab, your data set will have a combination of Gmail logs and other data mixed in, so it will be important to get familiar with the filtering functionality in SOF-ELK.

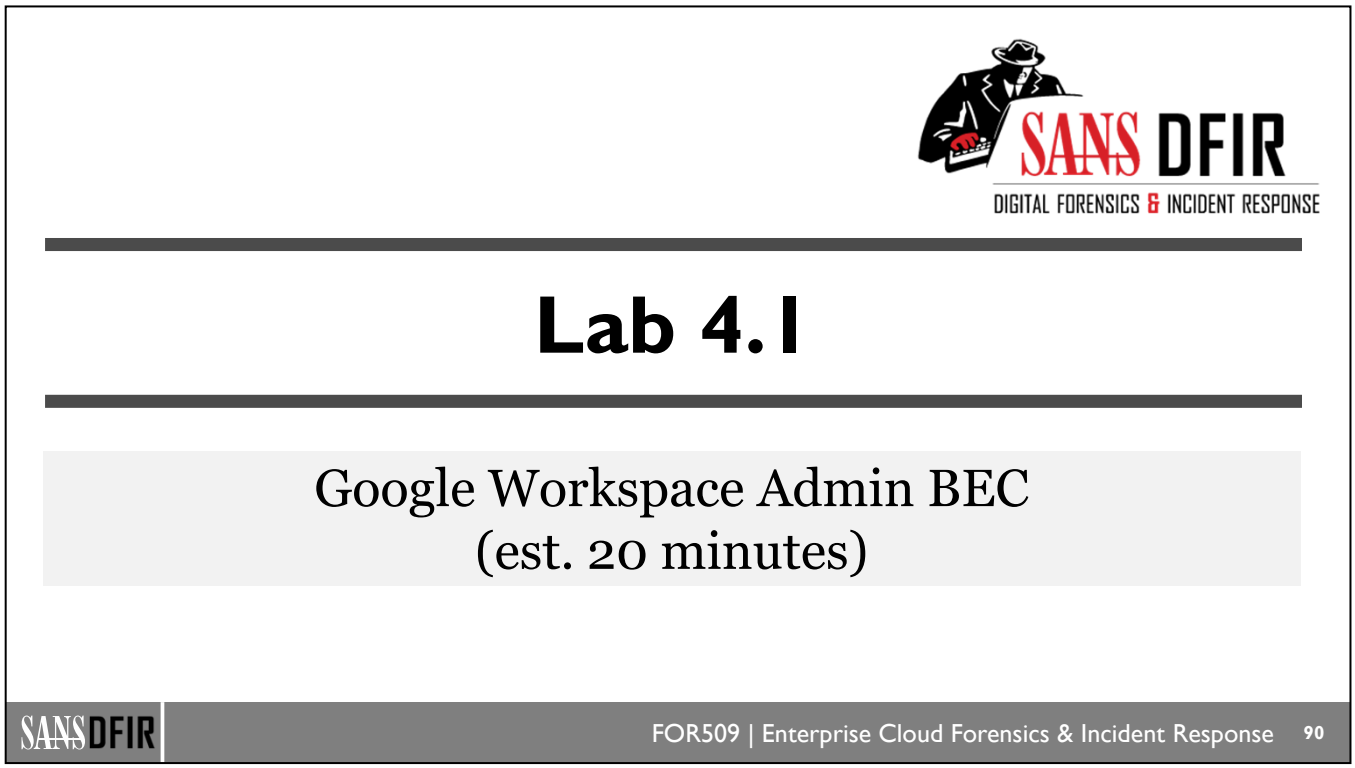
The data set under the "gws-*" index will hold all the Google Workspace data, except for Flow Logs. When you're viewing this index, you will see all Google Workspace data loaded in SOF-ELK. Using the **Add filter** button below the search bar, create a new filter that uses the **message_id** field and **exists**. This will limit your data to only Gmail logs. When you're reviewing email, this filter is simply the starting point. However, when you're looking at malicious email activity, you will also need to pivot to other logs to determine actions that may have been taken by a threat actor.

The filter function at the top can be enabled and disabled by simply clicking on it. Set it to **Temporarily disable** if you want to see all Google Workspace data related to your search in the search bar at the top.

In addition to using the filter, you may also want to add specific fields to see summary values for the log entries. For Gmail log events, the common fields that are useful are @time, sender, recipient, subject, message_id, event_target, event_status, and message_direction. These will provide you with a summary view of each log entry to better understand what is occurring in the logs.



Time	sender	recipient	subject	message_id	event_target	event_status	message_direction
2022-01-31 23:53:10.000 +00:00	drive-shares-dm-noreply@google.com	mr_dcross@protonmail.com	Document shared with you: "Q4 Financial Data"	000000000000a105d905d6e97cc1@google.com	SMTP_OUT	DELIVERED	Sent
2022-01-31 23:53:10.000 +00:00	drive-shares-dm-noreply@google.com	dcross@longconsecurity.com	Document shared with you: "Q4 Financial Data"	000000000000a10d2c05d6e97c83@google.com	SMTP_IN	RECEIVED	Mixed
2022-01-31 23:53:10.000 +00:00	drive-shares-dm-noreply@google.com	mr_dcross@protonmail.com	Document shared with you: "Q4 Financial Data"	000000000000a105d905d6e97cc1@google.com	SMTP_OUT	DELIVERED	Sent
2022-01-31 23:53:10.000 +00:00	drive-shares-dm-noreply@google.com	dcross@longconsecurity.com	Document shared with you: "Q4 Financial Data"	000000000000a10d2c05d6e97c83@google.com	SMTP_OUT	DELIVERED	Mixed
2022-01-31 23:53:10.000 +00:00	drive-shares-dm-noreply@google.com	dcross@longconsecurity.com	Document shared with you: "Q4 Financial Data"	000000000000a10d2c05d6e97c83@google.com	GMAIL_INBOX	DELIVERED	Mixed
2022-01-31 23:53:10.000 +00:00	drive-shares-dm-noreply@google.com	mr_dcross@protonmail.com	Document shared with you: "Q4 Financial Data"	000000000000a105d905d6e97cc1@google.com	SMTP_OUT	DELIVERED	Sent
2022-01-31 23:53:10.000 +00:00	drive-shares-dm-noreply@google.com	dcross@longconsecurity.com	Document shared with you: "Q4 Financial Data"	000000000000a10d2c05d6e97c83@google.com	INTERNAL_SERVER	DELIVERED	Mixed
2022-01-31 23:53:10.000 +00:00	drive-shares-dm-noreply@google.com	dcross@longconsecurity.com	Document shared with you: "Q4 Financial Data"	000000000000a10d2c05d6e97c83@google.com	SMTP_IN	INSERTED	Mixed
2022-01-31 23:50:53.000 +00:00	33HX4YQgTBL8st-wjuq3fhhtz	kurt@longconsec	Recovery email verified	BgzLQXOCCGl5ITldX2iAEg@notification	SMTP_IN	RECEIVED	Received



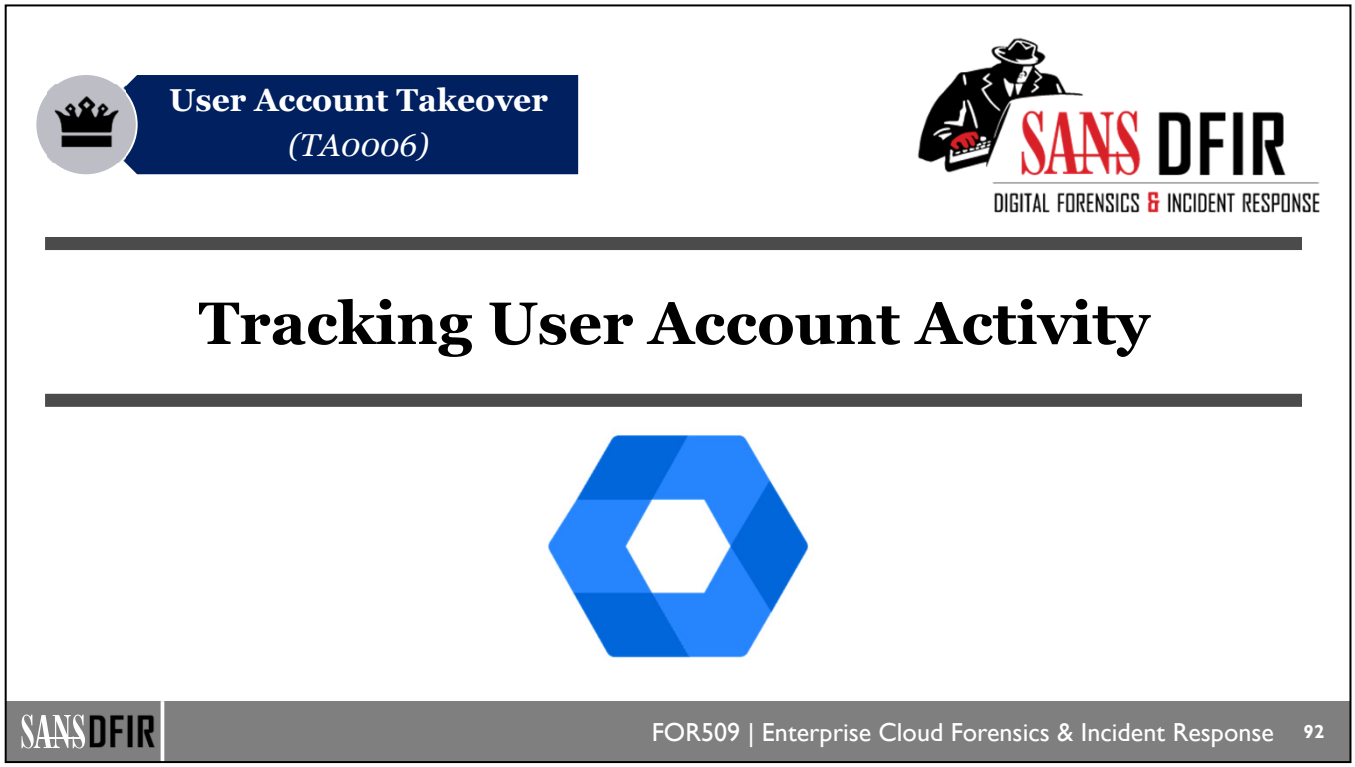
This page intentionally left blank.

Google Workspace Forensics and IR Roadmap

- 4.1: Understanding Google Workspace
- 4.2: Google Workspace Evidence
- 4.3: ATT&CKing Workspace
- 4.4: Workspace Evidence in Google Cloud

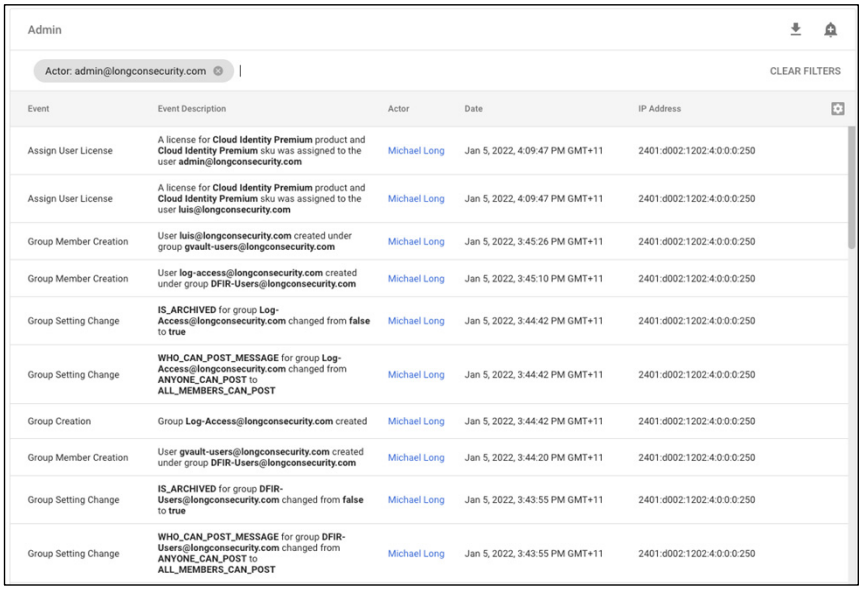
- Workspace Audit Log Rules and Retention
- Login and User Audit Log Analysis
- What is OAuth?
- OAuth Abuse with Third Party-Apps
- Workspace Token Logging and Containment
- **Lab 4.2**: OAuth Abuse with Third-Party Apps

This page intentionally left blank.



This page intentionally left blank.

Admin Audit Logs



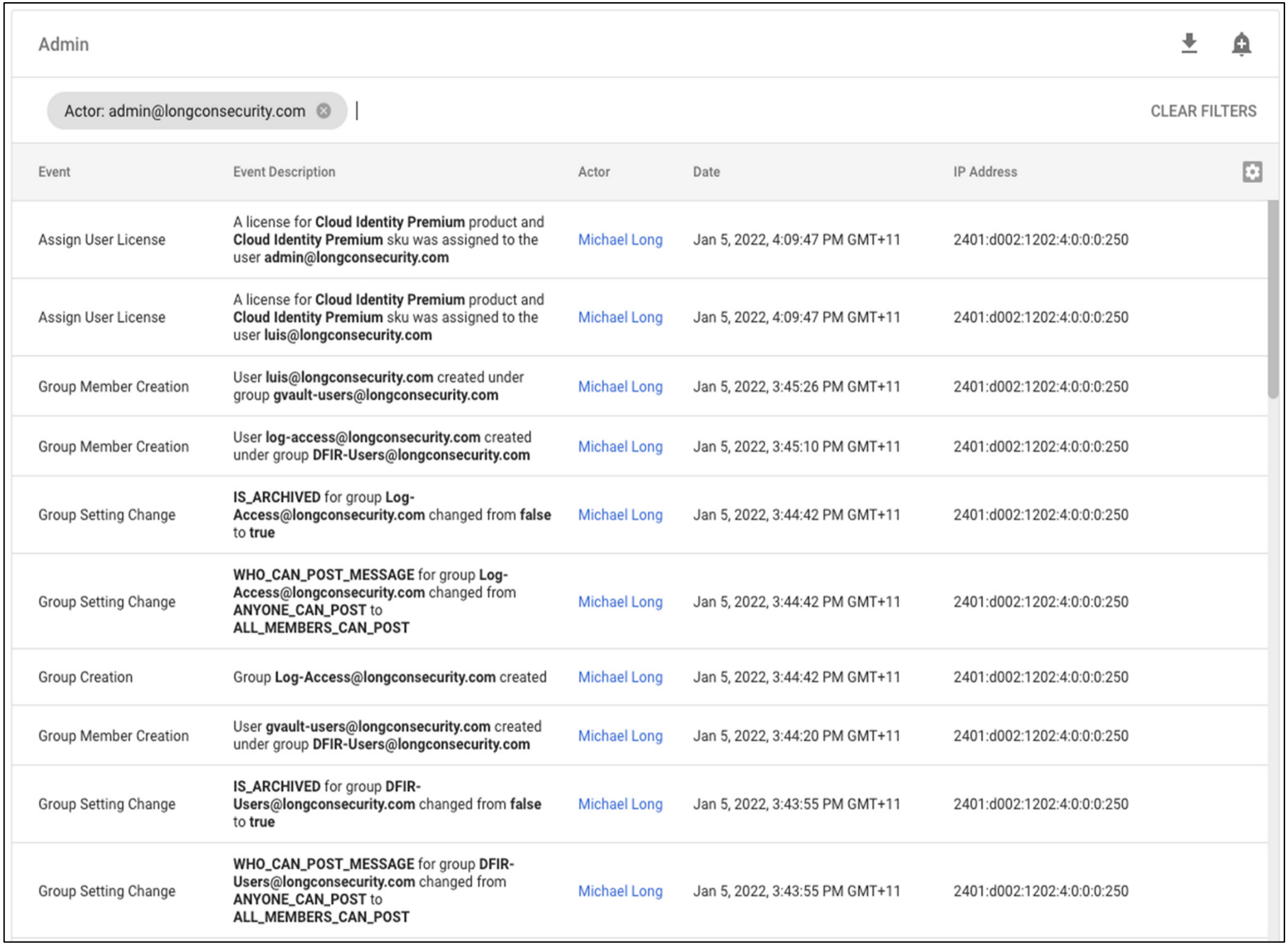
Admin Log

- Admin Audit Logs show events that have occurred within the Google Admin Console.
- These are useful for tracking changes to permissions, services, groups, or settings.
- This log is your "go to" when an Admin Account is compromised

The Admin Audit Log contains events for any change that has occurred within the Google Admin Console. This log tracks all admin tasks and changes to the overall organization. If you suspect an admin account has been compromised, the Admin Audit Log is the primary location you should check first to determine what changes administrator accounts have made to your organization.

Reference:

https://for509.com/lm07z (Admin audit log)



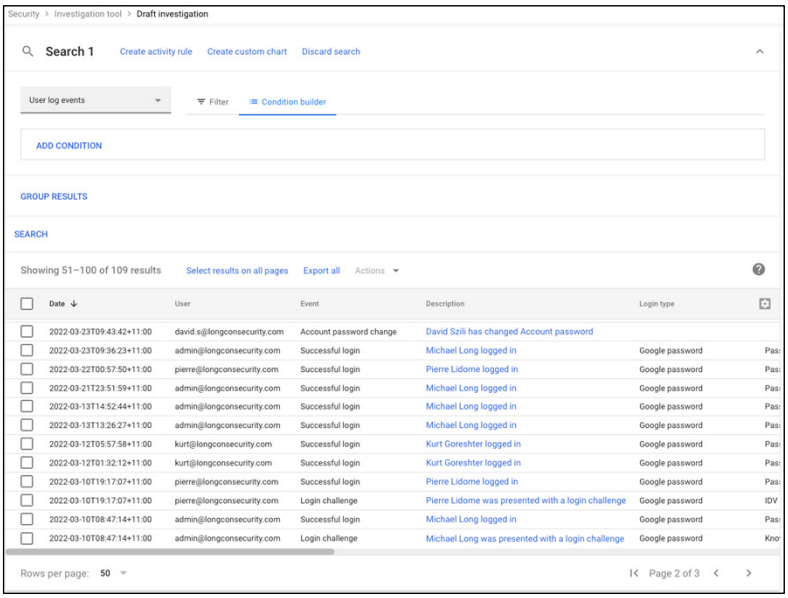
Admin

Actor: admin@longconsecurity.com

CLEAR FILTERS

Event	Event Description	Actor	Date	IP Address
Assign User License	A license for **Cloud Identity Premium** product and **Cloud Identity Premium** sku was assigned to the user **admin@longconsecurity.com**	Michael Long	Jan 5, 2022, 4:09:47 PM GMT+11	2401:d002:1202:4:0:0:0:250
Assign User License	A license for **Cloud Identity Premium** product and **Cloud Identity Premium** sku was assigned to the user **luis@longconsecurity.com**	Michael Long	Jan 5, 2022, 4:09:47 PM GMT+11	2401:d002:1202:4:0:0:0:250
Group Member Creation	User **luis@longconsecurity.com** created under group **gvault-users@longconsecurity.com**	Michael Long	Jan 5, 2022, 3:45:26 PM GMT+11	2401:d002:1202:4:0:0:0:250
Group Member Creation	User **log-access@longconsecurity.com** created under group **DFIR-Users@longconsecurity.com**	Michael Long	Jan 5, 2022, 3:45:10 PM GMT+11	2401:d002:1202:4:0:0:0:250
Group Setting Change	**IS_ARCHIVED** for group **Log-Access@longconsecurity.com** changed from **false** to **true**	Michael Long	Jan 5, 2022, 3:44:42 PM GMT+11	2401:d002:1202:4:0:0:0:250
Group Setting Change	**WHO_CAN_POST_MESSAGE** for group **Log-Access@longconsecurity.com** changed from **ANYONE_CAN_POST** to **ALL_MEMBERS_CAN_POST**	Michael Long	Jan 5, 2022, 3:44:42 PM GMT+11	2401:d002:1202:4:0:0:0:250
Group Creation	Group **Log-Access@longconsecurity.com** created	Michael Long	Jan 5, 2022, 3:44:42 PM GMT+11	2401:d002:1202:4:0:0:0:250
Group Member Creation	User **gvault-users@longconsecurity.com** created under group **DFIR-Users@longconsecurity.com**	Michael Long	Jan 5, 2022, 3:44:20 PM GMT+11	2401:d002:1202:4:0:0:0:250
Group Setting Change	**IS_ARCHIVED** for group **DFIR-Users@longconsecurity.com** changed from **false** to **true**	Michael Long	Jan 5, 2022, 3:43:55 PM GMT+11	2401:d002:1202:4:0:0:0:250
Group Setting Change	**WHO_CAN_POST_MESSAGE** for group **DFIR-Users@longconsecurity.com** changed from **ANYONE_CAN_POST** to **ALL_MEMBERS_CAN_POST**	Michael Long	Jan 5, 2022, 3:43:55 PM GMT+11	2401:d002:1202:4:0:0:0:250

User Log Events (1)



Login Log

- The User Log Events will show use of Google Workspace credentials across any service that uses them for authentication.
- This log will also show changes to an account, related to authentication; for example, MFA changes.
- For DFIR cases, this log contains everything authentication related.

The User Log Events contain all information related to authentication with user accounts inside of your Workspace organization. In addition to tracking authentication and authentication challenges, i.e., a user needs to re-authenticate, it will also show you the changes to an account that relate to authentication, such as multi-factor authentication changes.

Reference:

https://for509.com/82m3d (User Log Events)

Search 1

Create activity rule | Create custom chart | Discard search

User log events

Filter | Condition builder

ADD CONDITION

GROUP RESULTS

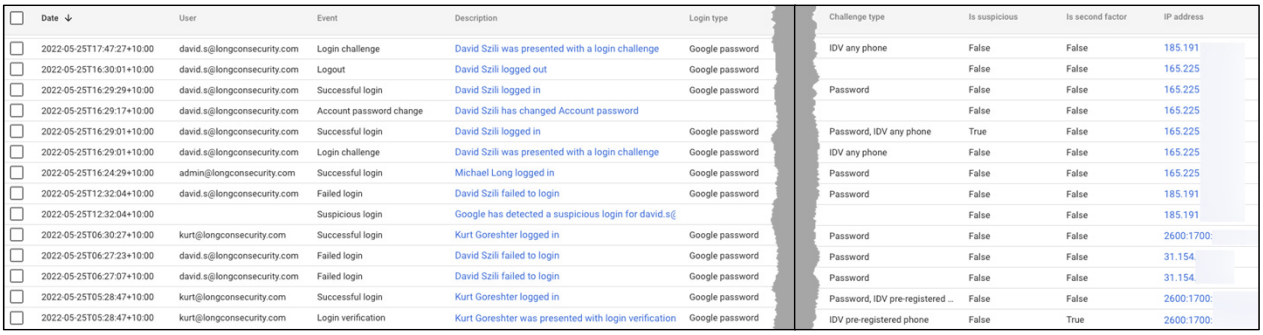
SEARCH

Showing 51–100 of 109 results | Select results on all pages | Export all | Actions

Date	User	Event	Description	Login type	
2022-03-23T09:43:42+11:00	david.s@longconsecurity.com	Account password change	David Szili has changed Account password		
2022-03-23T09:36:23+11:00	admin@longconsecurity.com	Successful login	Michael Long logged in	Google password	Pas
2022-03-22T00:57:50+11:00	pierre@longconsecurity.com	Successful login	Pierre Lidome logged in	Google password	Pas
2022-03-21T23:51:59+11:00	admin@longconsecurity.com	Successful login	Michael Long logged in	Google password	Pas
2022-03-13T14:52:44+11:00	admin@longconsecurity.com	Successful login	Michael Long logged in	Google password	Pas
2022-03-13T13:26:27+11:00	admin@longconsecurity.com	Successful login	Michael Long logged in	Google password	Pas
2022-03-12T05:57:58+11:00	kurt@longconsecurity.com	Successful login	Kurt Goreshter logged in	Google password	Pas
2022-03-12T01:32:12+11:00	kurt@longconsecurity.com	Successful login	Kurt Goreshter logged in	Google password	Pas
2022-03-10T19:17:07+11:00	pierre@longconsecurity.com	Successful login	Pierre Lidome logged in	Google password	Pas
2022-03-10T19:17:07+11:00	pierre@longconsecurity.com	Login challenge	Pierre Lidome was presented with a login challenge	Google password	IDV
2022-03-10T08:47:14+11:00	admin@longconsecurity.com	Successful login	Michael Long logged in	Google password	Pas
2022-03-10T08:47:14+11:00	admin@longconsecurity.com	Login challenge	Michael Long was presented with a login challenge	Google password	Kno

Rows per page: 50 | Page 2 of 3

User Log Events (2)



Date	User	Event	Description	Login type	Challenge type	Is suspicious	Is second factor	IP address
2022-05-25T17:47:27+10:00	david.s@longconsecurity.com	Login challenge	David Szili was presented with a login challenge	Google password	IDV any phone	False	False	185.191
2022-05-25T16:30:01+10:00	david.s@longconsecurity.com	Logout	David Szili logged out	Google password		False	False	165.225
2022-05-25T16:29:29+10:00	david.s@longconsecurity.com	Successful login	David Szili logged in	Google password	Password	False	False	165.225
2022-05-25T16:29:17+10:00	david.s@longconsecurity.com	Account password change	David Szili has changed Account password			False	False	165.225
2022-05-25T16:29:01+10:00	david.s@longconsecurity.com	Successful login	David Szili logged in	Google password	Password, IDV any phone	True	False	165.225
2022-05-25T16:29:01+10:00	david.s@longconsecurity.com	Login challenge	David Szili was presented with a login challenge	Google password	IDV any phone	False	False	165.225
2022-05-25T16:24:29+10:00	admin@longconsecurity.com	Successful login	Michael Long logged in	Google password	Password	False	False	165.225
2022-05-25T12:32:04+10:00	david.s@longconsecurity.com	Failed login	David Szili failed to login	Google password	Password	False	False	185.191
2022-05-25T12:32:04+10:00		Suspicious login	Google has detected a suspicious login for david.s@			False	False	185.191
2022-05-25T06:30:27+10:00	kurt@longconsecurity.com	Successful login	Kurt Goreshter logged in	Google password	Password	False	False	2600:1700:
2022-05-25T06:27:23+10:00	david.s@longconsecurity.com	Failed login	David Szili failed to login	Google password	Password	False	False	31.154.
2022-05-25T06:27:07+10:00	david.s@longconsecurity.com	Failed login	David Szili failed to login	Google password	Password	False	False	31.154.
2022-05-25T05:28:47+10:00	kurt@longconsecurity.com	Successful login	Kurt Goreshter logged in	Google password	Password, IDV pre-registered ...	False	False	2600:1700:
2022-05-25T05:28:47+10:00	kurt@longconsecurity.com	Login verification	Kurt Goreshter was presented with login verification	Google password	IDV pre-registered phone	False	True	2600:1700:

User Accounts Log

- The User Log Events also shows high risk actions performed by a user accounts.
- The User Log Events will include both normal user behavior, along with high-risk activity that occurred on an account, which can provide a much quicker view of malicious changes to accounts when conducting an investigation.

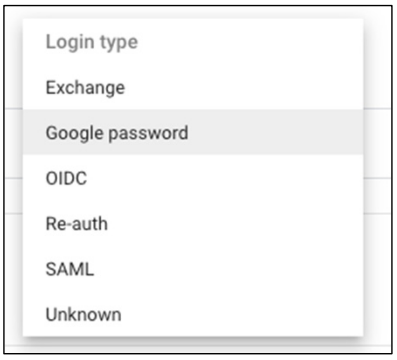
The User Log Events also contains information related to changes to a user account or other high-risk events that may have been performed by user accounts. This allows you to see high-risk events together with normal user activity. This can allow you to narrow down to a single user account and get a better picture of all the activity related to that user account, especially if there is suspicious activity mixed in with normal user behavior.

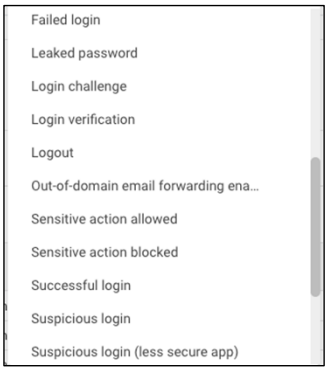
Reference:

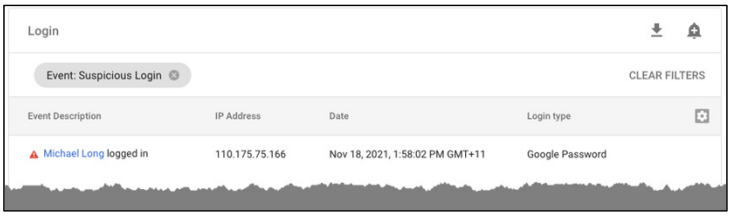
https://for509.com/v4ot8 (User accounts audit log)

User Log Events (3)

Login Type	Details
Exchange	The user account authenticated via OAuth login, or an existing session, with existing authentication token, was merged into on session.
Google Password	The user performed a login with a Google password prompt.
OIDC	Authentication with an OpenID Connect (OIDC) single sign-in event.
Re-Auth	The user was prompted to re-authenticate by Workspace.
SAML	The user authenticated with a SAML single sign-on.
Unknown	The user account signed in with an unknown method to Google.







The User Log Events contain a wealth of information related to how users have authenticated, and any type of events related to authentication that may be informational or suspicious. Login type provides information as to how a user authenticated and why the event appears in the User Log Events. A reference table of the login types is included above.

Additionally, User Log Events that contain a warning icon are often the result of an unusual or suspicious login. These are categorized as part of the event types that can occur in the User Log Events. Hunting for some of the more unusual login events with the event type can be useful for finding suspicious or malicious logins with user accounts. The example above provides a search showing a suspicious login from Michael Long.

Reference:

https://for509.com/nmvak (User Log Events)

User Log Events: Event Types

Event Type	Details
2-step verification disable	Occurs when a user disables MFA from their account.
Account password change	Occurs each time a user changes their password; excludes an admin forcing a password change at next login.
Failed login	Occurs each time a user fails the login prompt. To see **details of why you need to use the logs from the API,** this isn't visible in the Admin Console.
Government-backed attack	Shows that a known threat actor attempted to access a user account.
Leaked password	Google has detected the user's password is within a known credential dump.
Login challenge	Additional security challenge shown to the user following a suspicious login.
Login verification	Additional security challenge shown when non-suspicious login occurred.
Logout	Occurs each time a user logs out.
Out of domain email forwarding enabled	Occurs when a user enables forwarding of an email outside the organization.
Successful login	Occurs each time a user logs in.
Suspicious login	Occurs when a user logs in with unusual characteristic; for example, a new IP address.
User suspended (*)	Occurs when Google suspends a user account; this can be due to spam or suspicious activity.

There are a large number of different event types that can occur within the User Log Events. The table above is a small sample of common event types that are generally of interest to investigators. At the time of publication, Google had not updated the Event Type definitions since moving to their new Investigation Tool, however, these definitions have been included from the old Login Audit Log events, which closely match up.

A more comprehensive list of all the Event Types from the Login Audit Log events is provided on the following page. You will notice that based on the event types above that the User Log Events don't simply contain authentication events, they also contain events surrounding authentication.

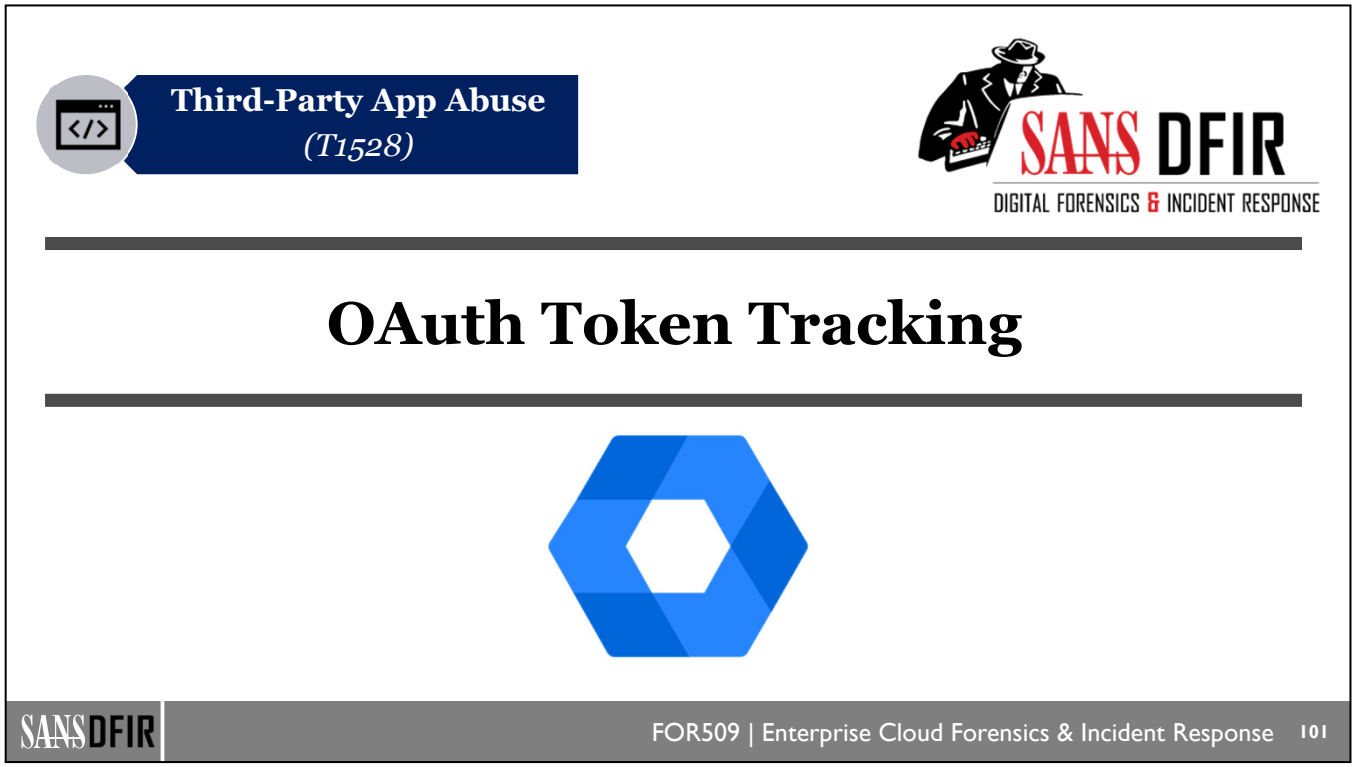
As Google updates their documentation for Event Types, we will endeavor to update the reference links provided in this Book.

Reference:

https://for509.com/pd7wh (User Log Events)

Event name	Description
2-step verification disable	Each time a user disables 2-step verification
2-step verification enroll	Each time a user enrolls in 2-step verification
Account password change	Each time a user changes an account password Note: This refers to users changing passwords at myaccount.google.com. It doesn't include password changes when the admin forces users to change their password at the next sign-in.
Account recovery email change	Each time a user changes a recovery email address
Account recovery phone change	Each time a user changes an account recovery phone number
Account recovery secret question/answer change	Each time a user changes an account recovery secret question and answer
Advanced Protection enroll	Each time a user enrolls in the Advanced Protection Program
Advanced Protection unenroll	Each time a user unenrolls in the Advanced Protection Program
Failed login	Each time a user fails to sign in. You can use the Reports API to view the cause of the failure. For example, the user entered an incorrect password, didn't have access to the service, or their account was suspended.
Government-backed attack	Each time government-backed attackers might have tried to compromise a user account or computer
Leaked password	When a password reset is required because Google detects compromised credentials
Login challenge	User asked an extra security question due to a suspicious sign-in attempt
Login verification	User asked an extra security question when Google did not detect a suspicious sign-in attempt
Logout	Each time a user logs out Note: Even if the user signed in with login types other than Google Password, (such as Exchange, ReAuth, SAML, or Unknown), the Login type for Logout events is displayed as Google Password.
Out of domain email forwarding enabled	Each time a user enables the forwarding of email outside of the domain
Successful login	Each time a user logged in
Suspicious login	Each time a user logged in and the login had some unusual characteristics. For example, if the user logged in from an unfamiliar IP address. Suspicious login events are shown with a red warning icon.
Suspicious login blocked	Each time a suspicious login was blocked
Suspicious login from less secure app blocked	Each time a suspicious login from a less secure app was blocked
Suspicious programmatic login blocked	Each time a suspicious login with programmatic elements was blocked
User suspended	Each time a user was suspended
User suspended (spam through relay)	Each time a user was suspended due to spam relay
User suspended (spam)	Each time a user was suspended due to spam
User suspended (suspicious activity)	Each time a user was suspended due to suspicious activity

Reference:
https://support.google.com/a/answer/4580120 (User Log Events)

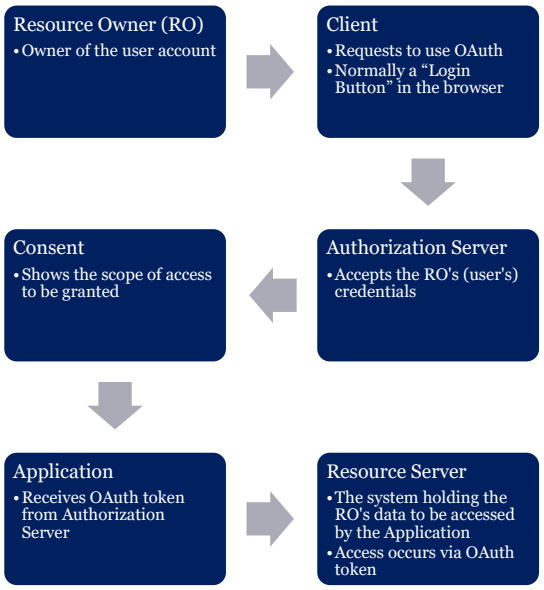


This page intentionally left blank.

What Is OAuth?

tl;dr on OAuth

- OAuth allows applications to access an API with authorization from a user.
- OAuth prevents users or applications having to authenticate each time they want to access an API resource.
- Generally, OAuth tokens can be limited in scope to only be authorized to access specific resources (i.e., Contacts, Drive files, etc.).
- OAuth provides a **token** to prove an application is authorized to the system it's requesting resources from.



OAuth is the process of allowing a user to authorize an application to access user content on their behalf via an API request. This process is in no way specific to only Google Workspace—it exists across many platforms. However, it has been a more recent targeted attack surface against Google Workspace and Google Workspace user accounts.

OAuth is an authorization process that allows the owner of a user account to authorize a third-party service to access information belonging to the user account. Inside of Google Workspace this is typically presented as a login button in the browser when the third-party application requests access to resources owned by the user account. To enable this process to work, the Google Workspace Admin Console needs to enable users to authorize OAuth for their accounts, which is enabled by default.

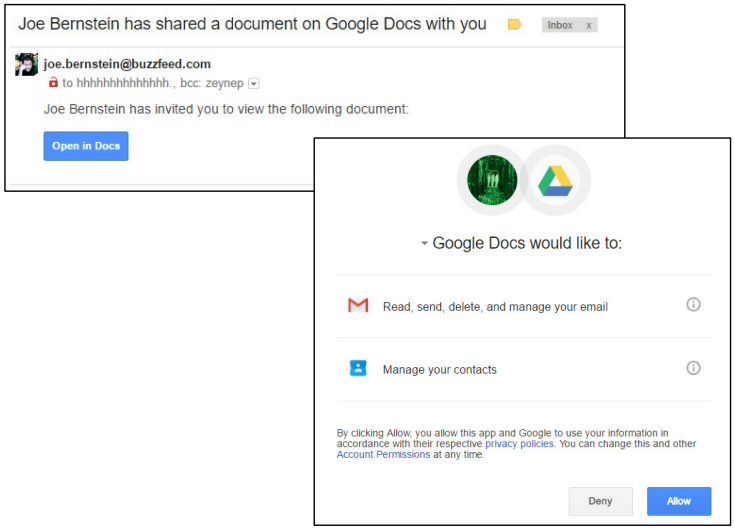
After a user account owner has had their access checked against Google Workspace to ensure OAuth is authorized for their account, they are then provided a list of permissions, referred to as the scope, the third-party application is requesting to access. The owner of the user account needs to approve this access before an OAuth token is generated. It is this scope of access that the OAuth token is limited to when it is generated.

Once the OAuth token is generated. the third-party application can then use the token to request access to resources held within Google Workspace that are owned or controlled by the user accounts.

Reference:

https://for509.com/ntgeb (OAuth Working Group Specifications)

OAuth Abuse with Third-Party Apps: History (1)



The Attack Chain

- One of your contacts sends you a "GDoc" to open.
- You open it and it asks for permissions to your email and contacts.
- All your contacts are spammed with the same attack, from you.

Back in May 2017, a threat actor had managed to turn the abuse of OAuth into almost worm-like functionality with Gmail account users. Victims would receive an email from a sender that they had previously communicated with that contained a link to open a Google Doc. When the victim clicked on this link it prompted the victim to authorize an application called "Google Docs" to access the user's email and contacts. Victims that authorized this access were essentially authorizing a malicious third-party application called "Google Docs", not a legitimate application written by Google. This provided the threat actor with OAuth authorization to access the user's email account and all of their contacts stored in Google.

After the threat actor had obtained access via OAuth, they would then send the same type of phishing email out to all of the contacts they had saved within Google Contacts. This ended up producing a worm-like behavior among Gmail user accounts. Due to the disruption that this attack caused on Gmail user accounts, Google forcefully stepped in and banned the malicious third-party application and revoked all OAuth tokens.

While Google stepped in to contain and eradicate this incident, it goes to show how quickly access can be obtained when using OAuth authorization to a user account's resources.

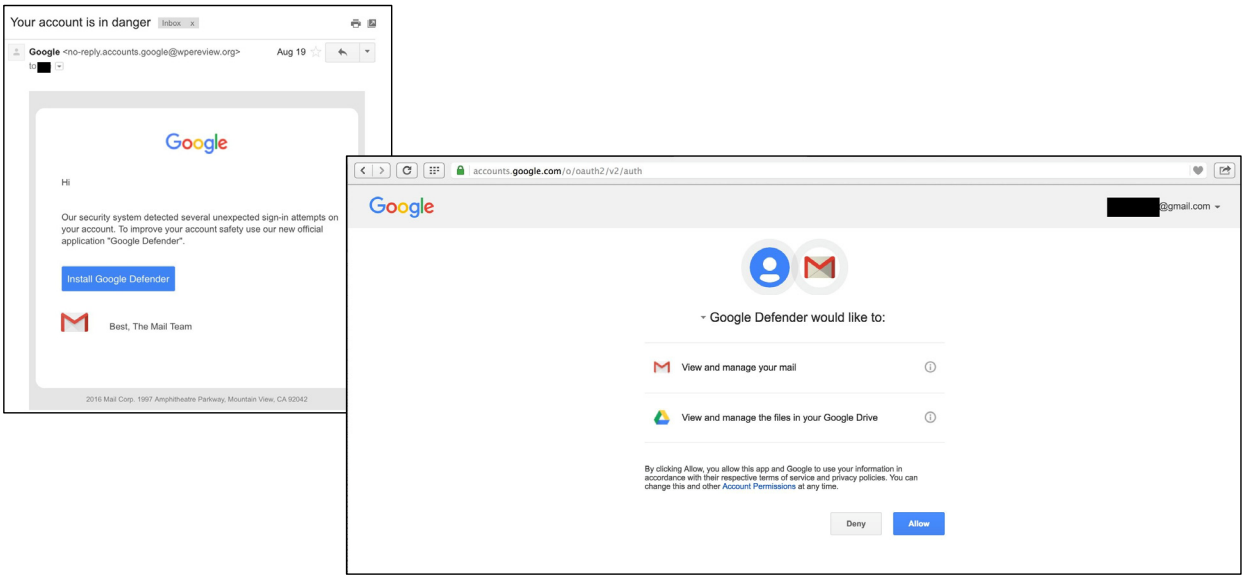
References:

https://for509.com/a1mbu (ISC Diary Entry on GDoc OAuth Attack)

https://for509.com/yjzlw (ZDNet: Fake Google Doc Phishing)

https://for509.com/y1c3o (Twitter Example of OAuth Phishing Doc)

OAuth Abuse with Third-Party Apps: History (2)



Between 2015 and 2016 the threat actor group known as “Fancy Bear” (a.k.a. APT 28) conducted a spear phishing attack against political parties that were using Google workspace. The initial phishing lure told victims that a security system detected unexpected sign-in attempts to their account, and they needed to improve their security with an official “Google Defender” application. This spear phishing attack involved the use of a third-party application called “Google Defender” that requested OAuth authorization to access the victim's Gmail account and their entire GDrive. Victims that allowed authorization for the third-party application would have given the threat actor full access to all email and all documents, including shared documents, that the victim had access to.

This style of attack is preferred by threat actors as it provides a relatively simple way of accessing information owned by the victim. A lot of the time we teach users to not enter their credentials into unknown login prompts; however, this style of attack doesn’t require any username or password from the victim.

Reference:

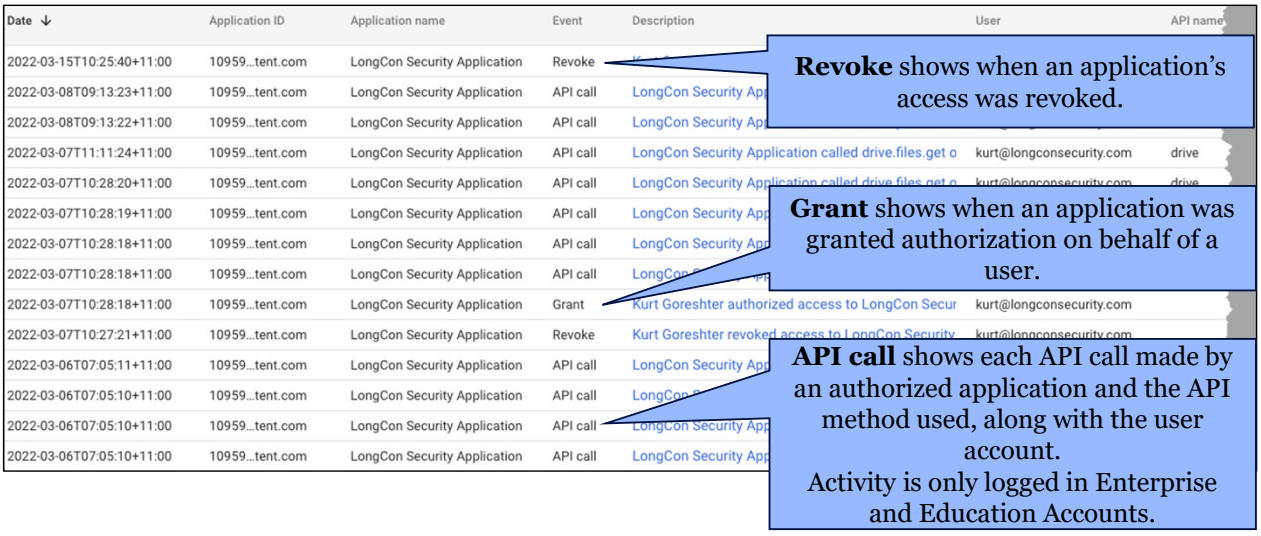
https://for509.com/vr6zg (Pawn Storm Abuses OAuth In Social Engineering Attacks)

For OAuth attacks to be successful they require a threat actor to create a malicious application that requires an OAuth authorization request. The threat actor then requires a victim to authorize the third-party application, generally via a phishing email; however, they can use any tactic that will drive the victim to a consent screen.

When the victim arrives at the OAuth consent screen, they are required to either already be authenticated, or authenticate into Google Workspace. Once the victim grants consent an OAuth token is generated and then made available to the malicious application. From this point, the threat actor now has the permissions and access granted from the consent to screen by the victim. This then allows the threat actor to perform actions on objectives with the OAuth token for authorization to resources the user would normally access to.

It's important to understand that this type of OAuth abuse with a third-party application does not provide any form of privilege escalation or enhanced access that the user/victim would not normally have.

Workspace: OAuth Log Events (1)



Date ↓	Application ID	Application name	Event	Description	User	API name
2022-03-15T10:25:40+11:00	10959...tent.com	LongCon Security Application	Revoke			
2022-03-08T09:13:23+11:00	10959...tent.com	LongCon Security Application	API call	LongCon Security Ap		
2022-03-08T09:13:22+11:00	10959...tent.com	LongCon Security Application	API call	LongCon Security Ap		
2022-03-07T11:11:24+11:00	10959...tent.com	LongCon Security Application	API call	LongCon Security Application called drive.files.get o	kurt@longconsecurity.com	drive
2022-03-07T10:28:20+11:00	10959...tent.com	LongCon Security Application	API call	LongCon Security Application called drive.files.get o	kurt@longconsecurity.com	drive
2022-03-07T10:28:19+11:00	10959...tent.com	LongCon Security Application	API call	LongCon Security Ap		
2022-03-07T10:28:18+11:00	10959...tent.com	LongCon Security Application	API call	LongCon Security Ap		
2022-03-07T10:28:18+11:00	10959...tent.com	LongCon Security Application	API call	LongCon Se		
2022-03-07T10:28:18+11:00	10959...tent.com	LongCon Security Application	Grant	Kurt Goreshter authorized access to LongCon Secur	kurt@longconsecurity.com	
2022-03-07T10:27:21+11:00	10959...tent.com	LongCon Security Application	Revoke	Kurt Goreshter revoked access to LongCon Security	kurt@longconsecurity.com	
2022-03-06T07:05:11+11:00	10959...tent.com	LongCon Security Application	API call	LongCon Security Ap		
2022-03-06T07:05:10+11:00	10959...tent.com	LongCon Security Application	API call	LongCon Se		
2022-03-06T07:05:10+11:00	10959...tent.com	LongCon Security Application	API call	LongCon Security Ap		
2022-03-06T07:05:10+11:00	10959...tent.com	LongCon Security Application	API call	LongCon Security Ap		

Revoke shows when an application's access was revoked.

Grant shows when an application was granted authorization on behalf of a user.

API call shows each API call made by an authorized application and the API method used, along with the user account.
Activity is only logged in Enterprise and Education Accounts.

To track OAuth token authorization and activity, Google Workspace provides an OAuth Log Events. This log will provide information regarding the user accounts that have authorized access along with the application ID that is being used and the activities and KPI requests that have been made by the application. This will not only show you users that have authorized new applications but will also give you the ability to historically see what actions applications may have performed in the context of the user.

Reference:

https://for509.com/x71zk (OAuth Log Events)

Workspace: OAuth Log Events (2)

Date ↓	Application name	Event	API name	API method	Number of response bytes	IP address	Product
2022-03-15T10:25:40+11:00	LongCon Security Application	Revoke			0		Drive Gmail
2022-03-08T09:13:23+11:00	LongCon Security Application	API call	drive	drive.files.get	143	99.129.	Drive
2022-03-08T09:13:22+11:00	LongCon Security Application	API call	drive	drive.permissions.create	116	99.129.	Drive
2022-03-07T11:11:24+11:00	LongCon Security Application	API call	drive	drive.files.get	0	99.129.	Drive
2022-03-07T10:28:20+11:00	LongCon Security Application	API call	drive	drive.files.get	142	99.129.	Drive
2022-03-07T10:28:19+11:00	LongCon Security Application	API call	drive	drive.permissions.create	116	99.129.	Drive
2022-03-07T10:28:18+11:00	LongCon Security Application	API call	drive	drive.files.list	571	99.129.	Drive
2022-03-07T10:28:18+11:00	LongCon Security Application	API call	gmail	gmail.users.messages.send	65	99.129.	Gmail
2022-03-07T10:28:18+11:00	LongCon Security Application	Grant			0	99.129.	Drive Gmail
2022-03-07T10:27:21+11:00	LongCon Security Application	Revoke			0	99.129.	Drive Gmail
2022-03-06T07:05:11+11:00	LongCon Security Application	API call	drive	drive.files.get	142	99.129.	Drive
2022-03-06T07:05:10+11:00	LongCon Security Application	API call	drive	drive.permissions.create	116	99.129.	Drive
2022-03-06T07:05:10+11:00	LongCon Security Application	API call	drive	drive.files.list	571	99.129.	Drive
2022-03-06T07:05:10+11:00	LongCon Security Application	API call	gmail	gmail.users.messages.send	65	99.129.	Gmail

OAuth API Tracking

When we cut some of the less relevant columns out, we get a triage view of the **API call** actions and what API methods were used.

The OAuth Log Events also provide you with information related to the actions features, or services, used by the application with an OAuth token for the user account. Within the Admin Investigator Tool, you can see exactly which API method was called, along with how much data (bytes) were returned as a result of the call to the API method. This will give investigators a better idea of what functionality is being used by the application, along with where it's being used, and how much data was collected by the application. While you cannot get details on exactly what elements within a feature were called, this is a good summary or triage view of OAuth activity.

Reference:

https://for509.com/x71zk (OAuth Log Events)

Workspace: OAuth Log Events via API


```
{"kind": "admin#reports#activity",
  "id": {
    "time": "2022-03-05T20:04:30.683Z",
    "uniqueQualifier": "-7101808226882379960",
    "applicationName": "token",
    "customerId": "C02mvk4dm"},
  "etag": "\"UMvHtdUQGju4SaKTK2kLjj-ZwxshlPj9bXaU2gd <SNIP> "",
  "actor": {
    "email": "kurt@longconsecurity.com",
    "profileId": "112036045880884988161"},
  "ipAddress": "99.129.99.206",
  "events": [
    {"type": "auth",
      "name": "activity",
      "parameters": [
        {"name": "api_name", "value": "drive"},
        {"name": "method_name", "value": "drive.files.list"},
        {"name": "client_id",
          "value": "109590116 <SNIP> lb7t5.apps.googleusercontent.com"},
        {"name": "num_response_bytes", "intValue": "572"},
        {"name": "product_bucket", "value": "DRIVE"},
        {"name": "app_name", "value": "LongCon Security Application"},
        {"name": "client_type", "value": "WEB"}
      ]}]}
```


Token Audit Activity Events

- Collecting the OAuth logs via API provides a more detailed look at activity that occurred with OAuth tokens.
- Additional fields include
  - **client_type** to show source
  - **scope** to show what was authorised initially
  - **num_response_bytes** to indicate how much data was returned in the API request
  - **product_bucket** to indicate the Workspace application accessed

Using the API to retrieve OAuth Log Events provides significantly more information compared to what is provided inside of the Admin console. The OAuth Log Events collected via API provide details relating to the source that was used for the activity, details related to the scope of the initial authorization, information related to how much data was returned in the API request, and details related to which application inside of Workspace was accessed.

Details related to client type and product bucket are provided on the following page for reference.

Reference:

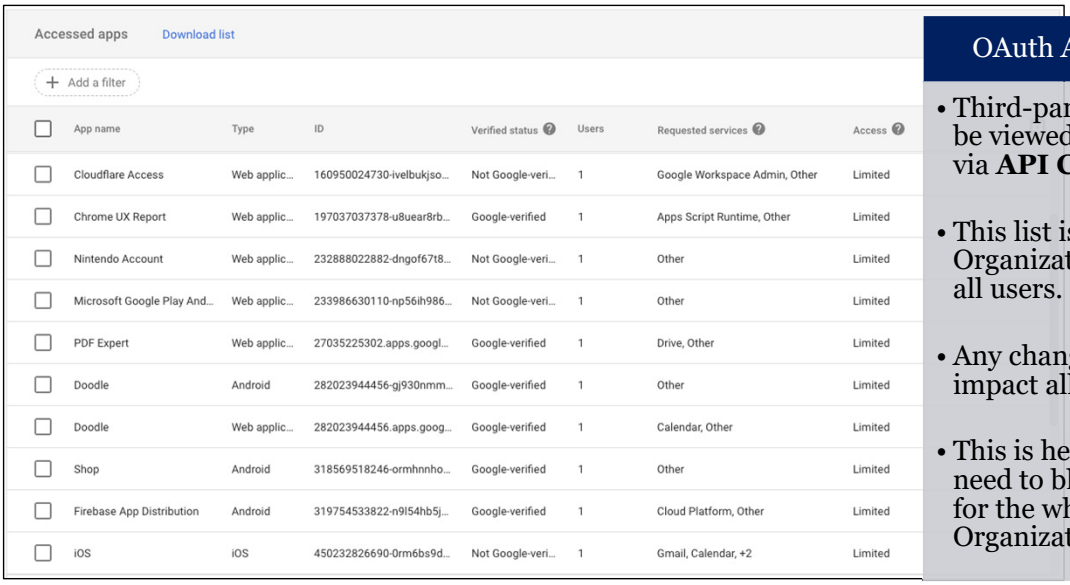
https://for509.com/fy0x8 (OAuth Token Audit Activity Events)

Client Type	Description
CONNECTED_DEVICE	A connected device client.
NATIVE_ANDROID	An Android application.
NATIVE_APPLICATION	A native application.
NATIVE_CHROME_EXTENSION	A Chrome application.
NATIVE_DEVICE	A native device application.
NATIVE_IOS	An iOS application.
NATIVE_SONY	A native Sony application.
TYPE_UNSPECIFIED	An unspecified client type.
WEB	A web application.

Product Bucket	Description
APPS_SCRIPT_API	The Apps Script API product bucket.
APPS_SCRIPT_RUNTIME	The Apps Script runtime product bucket.
CALENDAR	The Calendar product bucket.
CLASSROOM	The Classroom product bucket.
CLOUD_SEARCH	The Cloud Search product bucket.
COMMUNICATIONS	The Communications product bucket.
CONTACTS	The Contacts product bucket.
DRIVE	The Drive product bucket.
GMAIL	The Gmail product bucket.
GPLUS	The G+ product bucket.
GROUPS	The Groups product bucket.
GSUITE_ADMIN	The Google Workspace Admin product bucket.
IDENTITY	The Identity product bucket.
OTHER	A product bucket for applications that don't fall into the other buckets.
TASKS	The Tasks product bucket.
VAULT	The Vault product bucket.

Reference:
https://developers.google.com/admin-sdk/reports/v1/appendix/activity/token (OAuth Token Audit Activity Events)

Revoking OAuth Tokens (1)



OAuth App Review

- Third-party apps can be viewed for all users via **API Controls**.
- This list is Organization-wide for all users.
- Any changes here will impact all users.
- This is helpful if you need to block an app for the whole Organization.

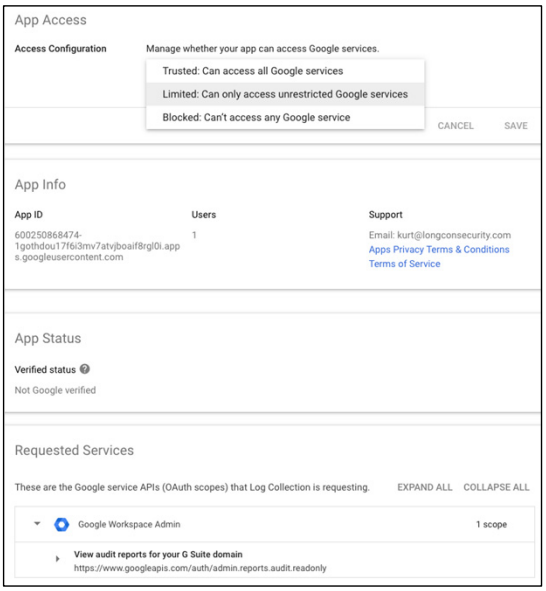
Within the Workspace Admin Console, you can also review all third-party applications API requests and authorizations. This can be helpful to understand all of the applications that are using OAuth to perform API requests against your Google Workspace organization. The applications listed within this section of the Admin Console are for all users across the entire organization. If there is a suspicious or malicious application with access to your organization, it can be relatively quick to find that application in this list by searching the requested resources that the application has access to.

References:

https://for509.com/z631q (Control which third-party & internal apps access Google Workspace data)

https://for509.com/i975q (Automatic OAuth 2.0 token revocation upon password change)

Revoking OAuth Tokens (2)



Token Access Removal

- OAuth tokens are revoked when a user changes their password.
  - IMAP access can take up to 1 hour to age out.
- Viewing an app will let you review who is using the app and the permissions it has.
- This example is a non-verified app that has not been submitted to Google for review.

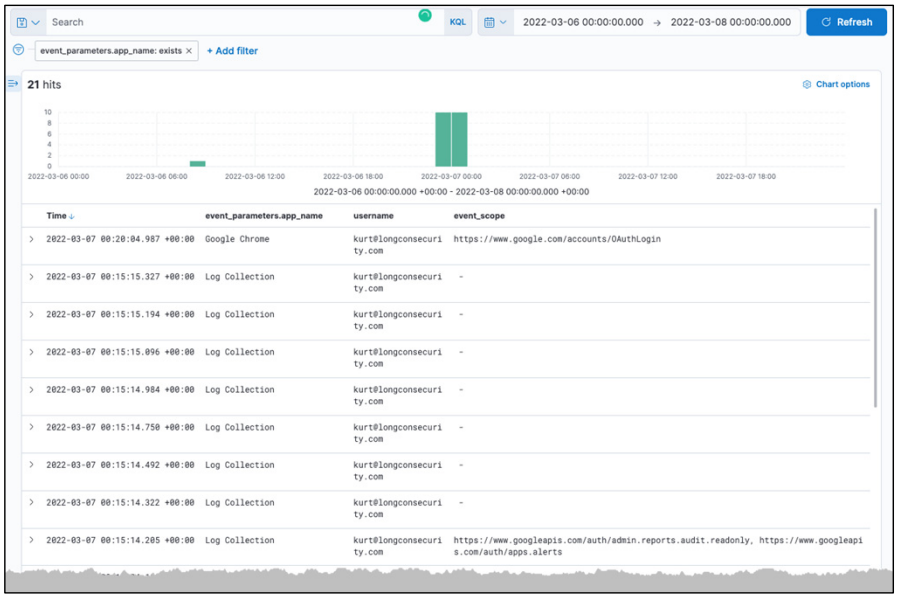
Once you have identified an application that you want to review or revoke access for, you then can restrict the application further or block it entirely for your Google Workspace. Additionally, you will be able to see the user accounts that have authorized the application to the perform API requests using OAuth tokens on their behalf.

References:

https://for509.com/r5git (Control which third-party & internal apps access Google Workspace data)

https://for509.com/vhild (What is a verified third-party app?)

Lab 4.2: OAuth Abuse with Third-Party Apps

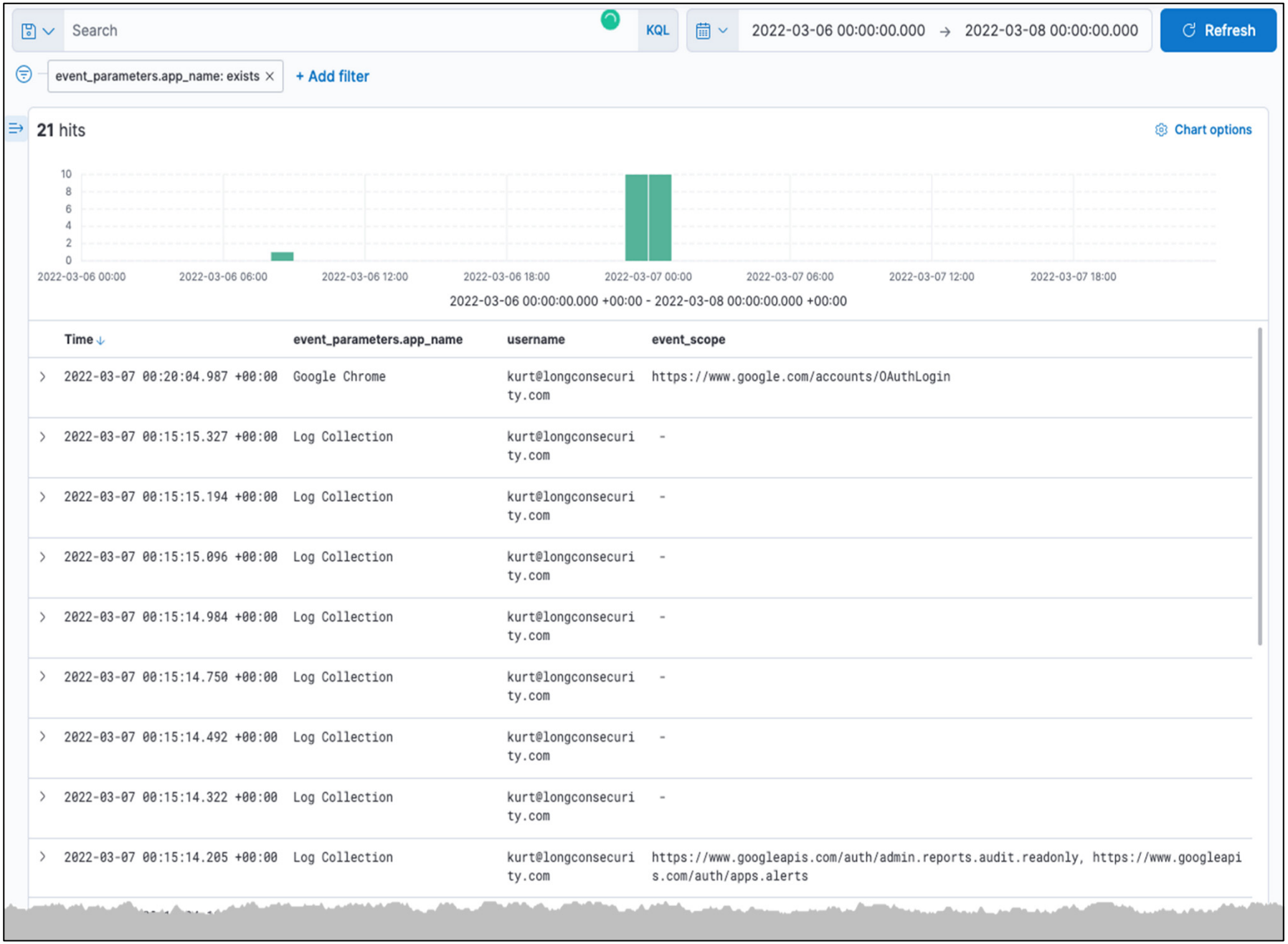


The example above shows you SOF-ELK with the OAuth logs extracted from Google Workspace in JSON format via an API request and loaded into SOF-ELK. In the upcoming lab, you will need to limit your data set if you have loaded other data into SOF-ELK already.

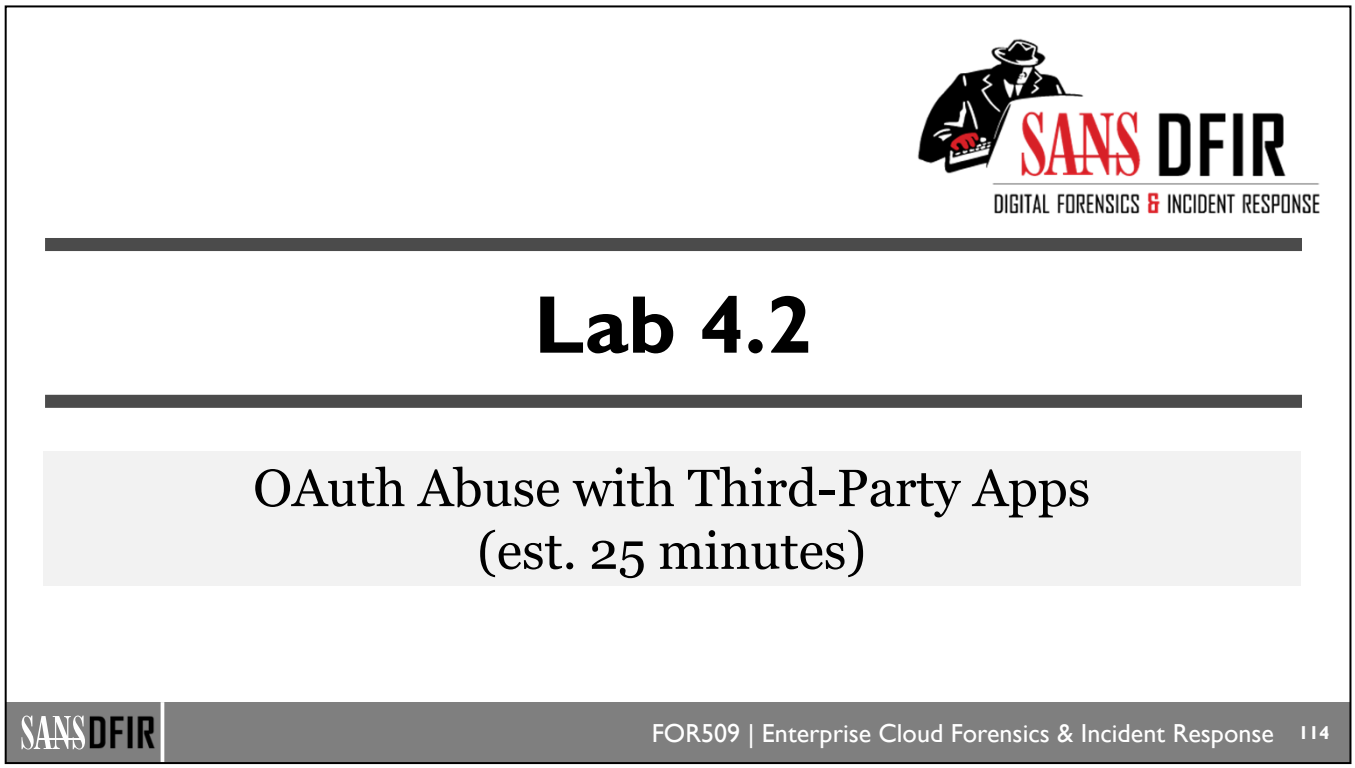
The data set under the "gws-*" index will hold all the Google Workspace data. When you're viewing this index, you will see all Google Workspace data loaded in SOF-ELK. Using the **Add filter** button below the search bar, create a new filter that uses the **event_parameters.app_name** field and **exists**. This will limit your data to only logs related to applications likely using OAuth. When you're reviewing authorized applications, this filter is simply the starting point. However, when you're looking for malicious activity, you will also need to pivot to other logs to determine actions that may have been taken by a threat actor.

The filter function at the top can be enabled and disabled by simply clicking on it. Set it to **Temporarily disable** if you want to see all Google Workspace data related to your search in the search bar at the top.

In addition to using the filter, you may also want to add specific fields to see summary values for the log entries. For user authorized application log events, the common fields that are useful are @time, event_parameters.app_name, username, and event_scope. These will provide you with a summary view of each log entry to better understand what is occurring in the logs.



Time	event_parameters.app_name	username	event_scope
2022-03-07 00:20:04.987 +00:00	Google Chrome	kurt@longconsecurity.com	https://www.google.com/accounts/OAuthLogin
2022-03-07 00:15:15.327 +00:00	Log Collection	kurt@longconsecurity.com	-
2022-03-07 00:15:15.194 +00:00	Log Collection	kurt@longconsecurity.com	-
2022-03-07 00:15:15.096 +00:00	Log Collection	kurt@longconsecurity.com	-
2022-03-07 00:15:14.984 +00:00	Log Collection	kurt@longconsecurity.com	-
2022-03-07 00:15:14.750 +00:00	Log Collection	kurt@longconsecurity.com	-
2022-03-07 00:15:14.492 +00:00	Log Collection	kurt@longconsecurity.com	-
2022-03-07 00:15:14.322 +00:00	Log Collection	kurt@longconsecurity.com	-
2022-03-07 00:15:14.205 +00:00	Log Collection	kurt@longconsecurity.com	https://www.googleapis.com/auth/admin.reports.audit.readonly, https://www.googleapis.com/auth/apps.alerts



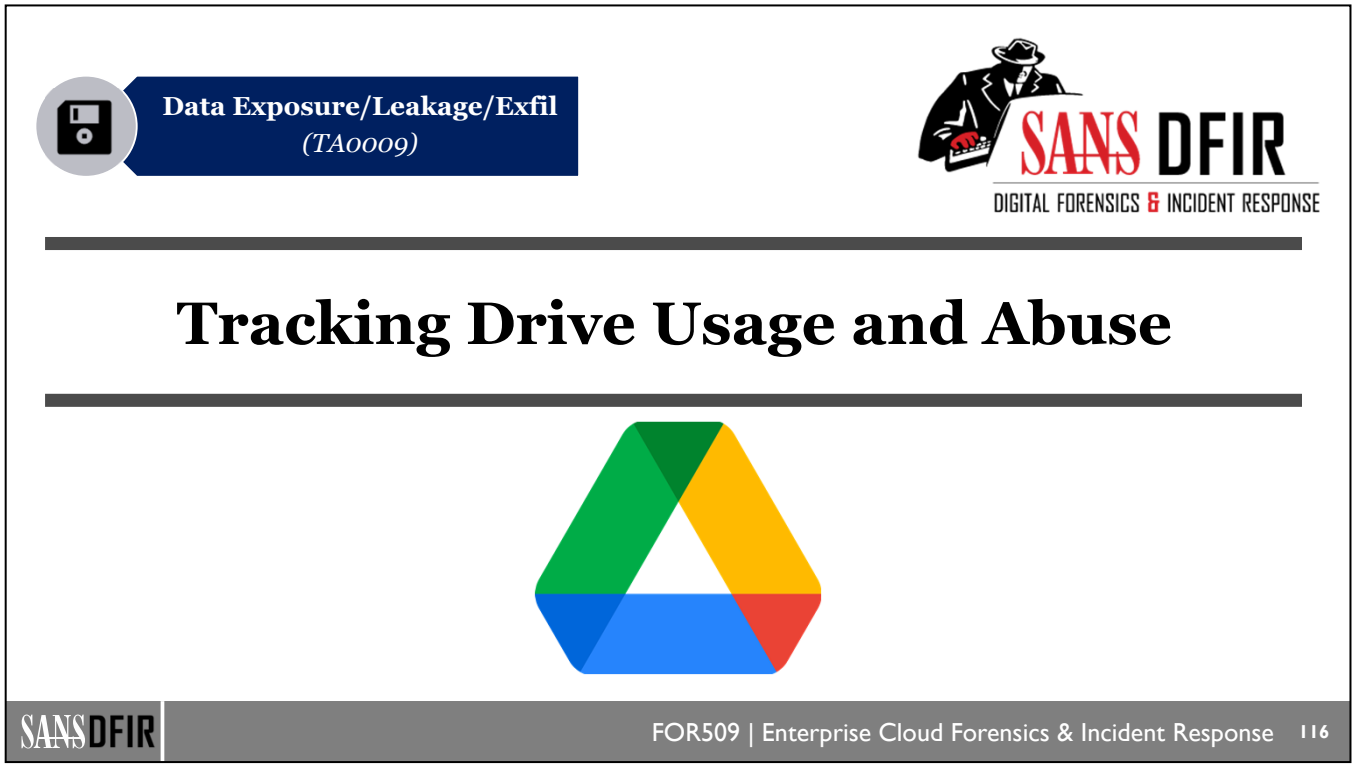
This page intentionally left blank.

Google Workspace Forensics and IR Roadmap

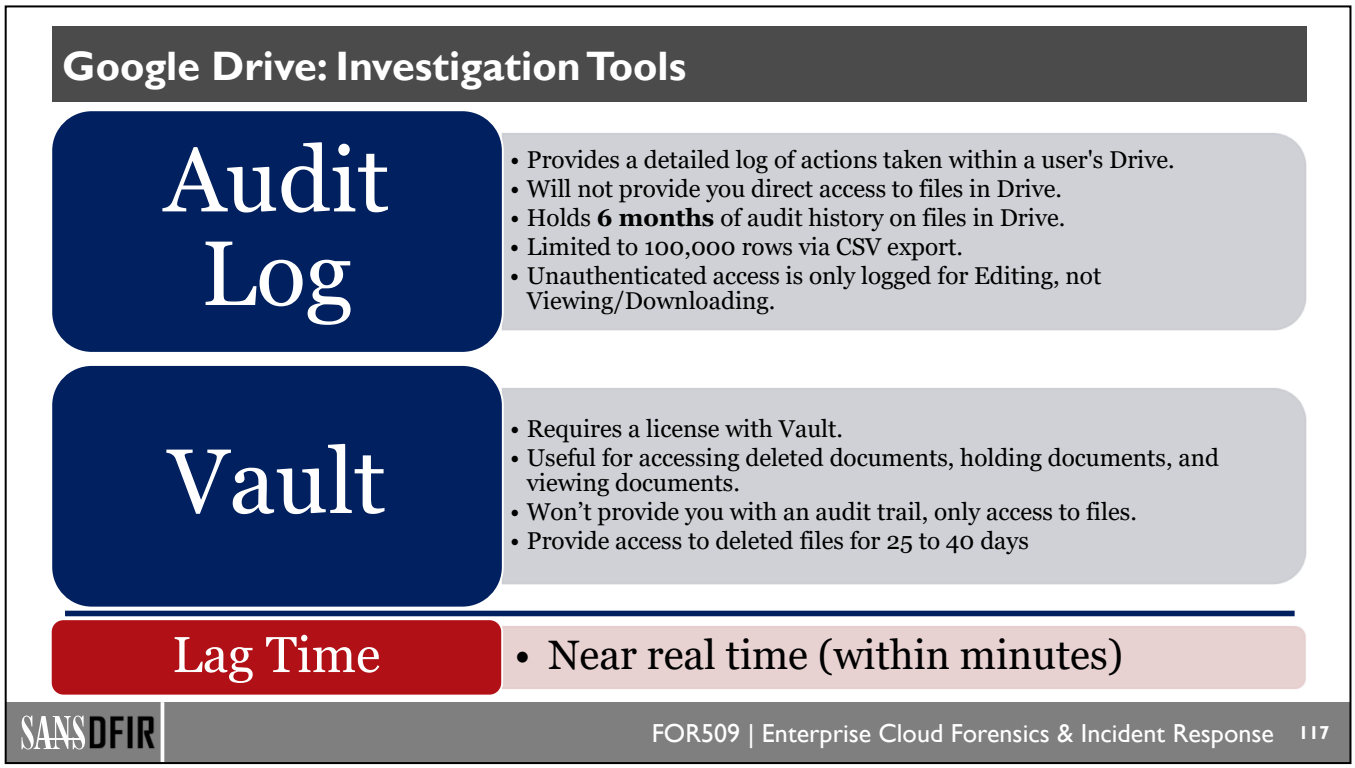
- 4.1: Understanding Google Workspace
- 4.2: Google Workspace Evidence
- 4.3: ATT&CKing Workspace
- 4.4: Workspace Evidence in Google Cloud

- Google Drive Investigation Tools
- Drive File Recovery
- Drive Audit and API Logging
- Takeout Data Exfil
- Takeout Audit and API Logging
- Customer Takeout Exfil
- **Lab 4.3**: Google Workspace Data Exposure

This page intentionally left blank.



This page intentionally left blank.



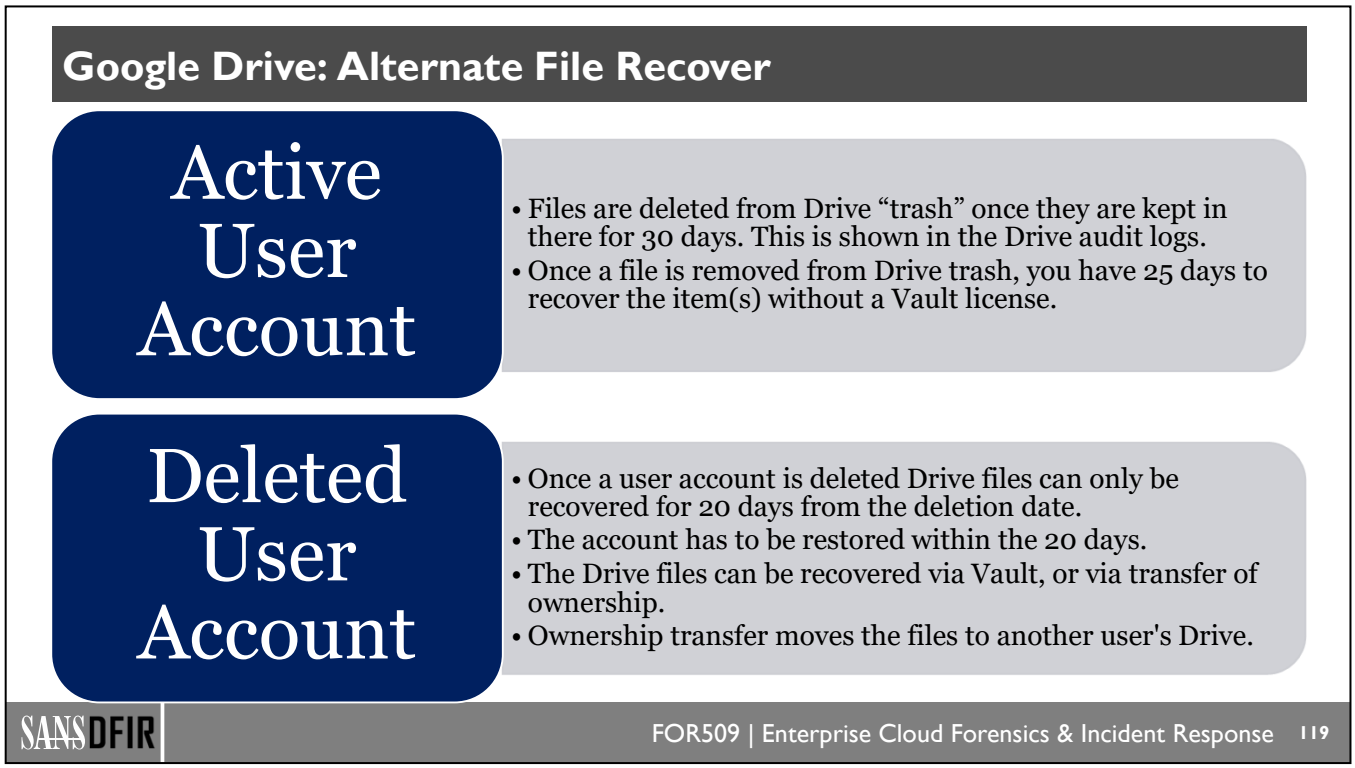
Google Drive is the primary storage service for users. Used as part of Google Workspace, it is also the main location where we predominantly find users mistakenly leaking data or inadvertently exposing data. In this section we're going to cover how to conduct an investigation where data inside of Google Drive has been exposed. The techniques shown within the section cover both mistaken data exposure along with malicious data exposure.

One of our primary tools when conducting an investigation with Google Drive is the audit log[1] for Google Drive. Audit log provides a near real time detailed list of actions taken by users over the last six months; however, it only provides us with details of actions that have occurred to files within Google Drive. It does not provide us with direct access to any files that are stored in a user account's Google Drive.[2] Additionally, the events recorded within the audit log are limited to authenticated actions by users. Actions that are taken by authenticated users are limited to editing. There is no ability to see logging related to unauthenticated viewing or downloading of files from Google Drive.

As mentioned previously, there are limitations to using the audit log within the Google Admin Console. Our main limitation is that data will only export to a maximum of 100,000 rows. Shortly we will look at how to extract Google Drive activity logs via the API.

If the Google Drive audit log will not provide us access to files directly within Google Drive, we can instead use Vault to directly access files from user accounts. This can also include the ability to access files that have since been deleted by users. However, this is limited to at least 25 days from when the file was deleted and may be extended out an additional 15 days depending on when Google purges the file from the storage. While the files remain purged by Google, after they have been deleted by the user, you are still able to search and access those files within Vault.[3] If, however, you have enabled additional or custom retention rules within Vault, then files will be kept based on how long you have determined within your custom retention rules. Furthermore, any user accounts that have had a hold applied to their Google Drive service will also retain deleted files until the hold is removed.

1. https://for509.com/nk7iw (Drive audit log)
2. https://for509.com/fngm6 (Data Retention and Lag Times)
3. https://for509.com/ocnk6 (How Retention Works)

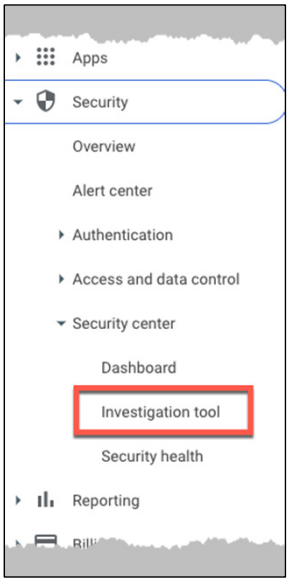


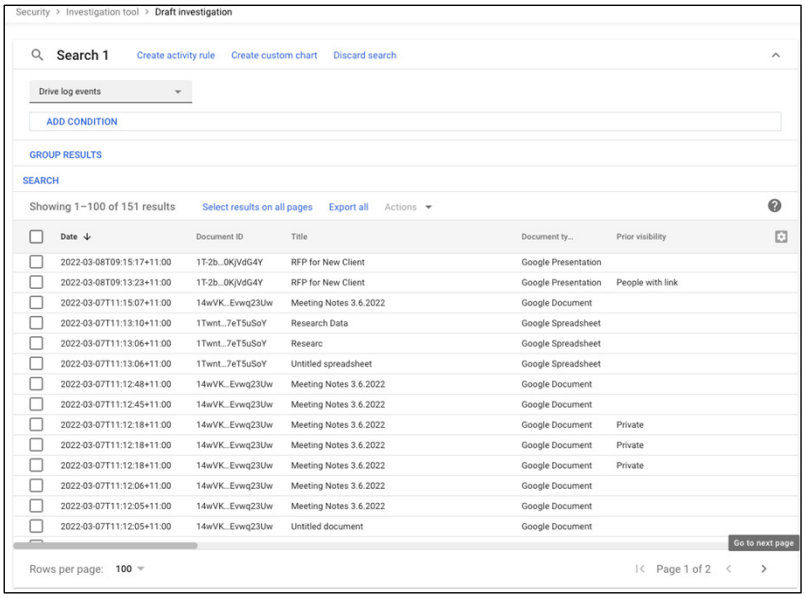
When a user deletes files within their Google Drive they move into a location called "trash". If a user does not manually delete items within the trash location, they are kept there for 30 days from the date of deletion, before Google or the user deletes them out of trash. Once they have been deleted from trash, administrators have an additional 25 days to be able to recover the items if they do not have a Vault license. When restoring data that has been removed from the trash you either have the option of restoring it back to its original location, in the user's Google Drive service, or to a shared drive.[1] Without a Vault, license administrators cannot recover any data from a user account after 25 days from it being deleted.

There may also be the scenario where there is a requirement to recover Google Drive data from a deleted user's account. If you delete a user account within Google Workspace, you have up to 20 days to be able to recover any files that were stored or owned by the user account that has been deleted. This requires the restoration of the deleted user account before any data can be recovered from it. If, however, you have a Vault license, you could recover data via Vault without the need to recover the original user account that was deleted.[2]

1. https://for509.com/0gi9m (Recover deleted files and folders for Drive users)
2. https://for509.com/5rxcl (Restore a deleted user's Drive files)

Google Drive: Audit Log (1)

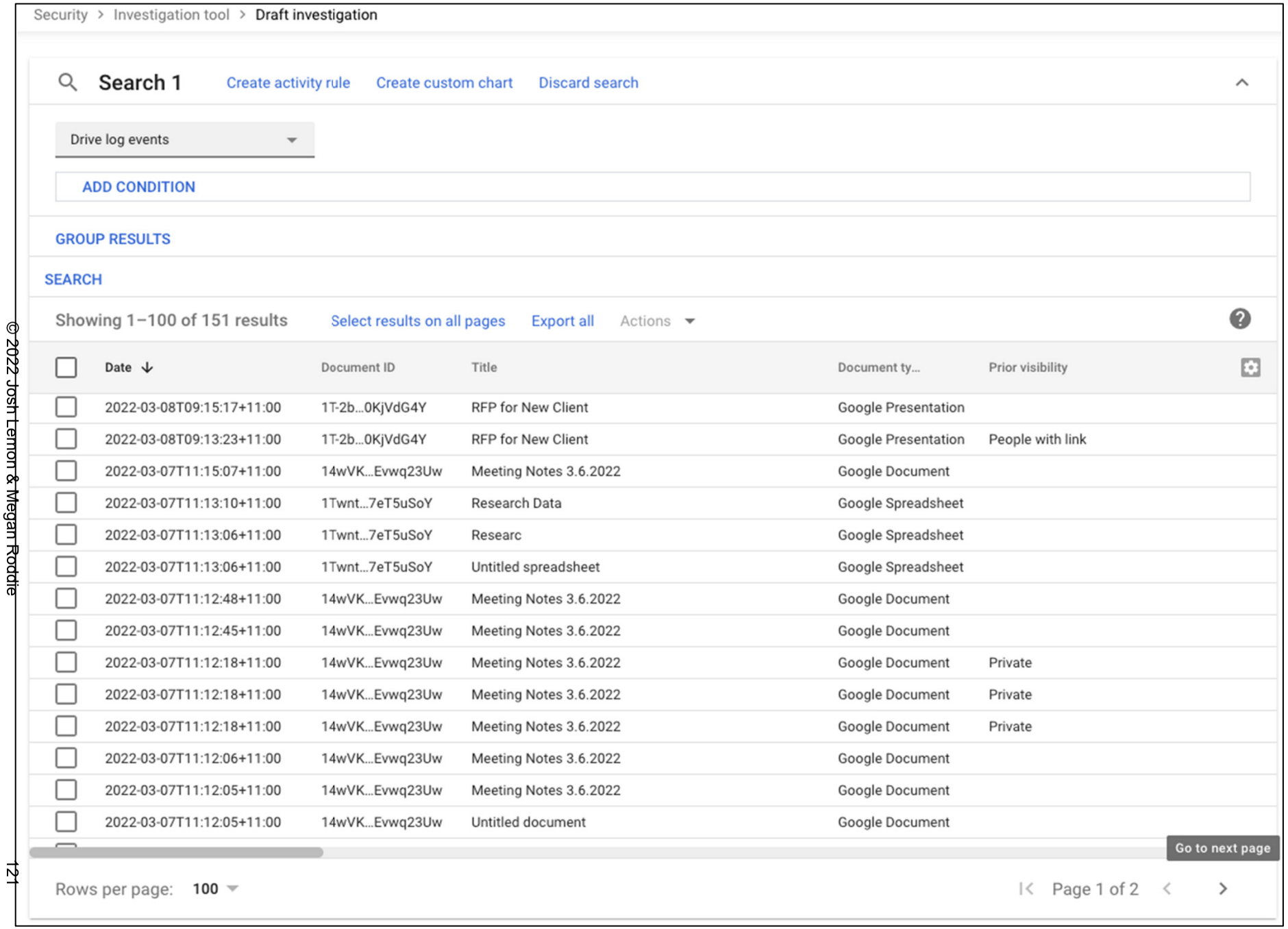




Google Drive Audit Logs are now contained within the Investigation tool in the Google admin console. Until March 2022, the Google Drive Audit Logs were separated out on their own. They have since been relocated together with all other audit logs inside of the Investigation tool. The previous menu that provided access to the Google Drive Audit Logs still exists at the time of publishing. When you click on the previous menu option for where they used to be, or were accessed from, you are redirected to the investigation tool with the Google Drive audit logs already selected.

The investigation tool allows you to run searches and group your results based on different field types for Google Drive. The Investigation tool will allow you to run searches with the AND or OR search operators, along with the ability to use partial matches for some fields. Although events are logged almost immediately, events shown in this preview can be delayed by 12 hours or more from the time the event occurred.[1]

1. https://for509.com/nk7iw (Drive Audit Log)



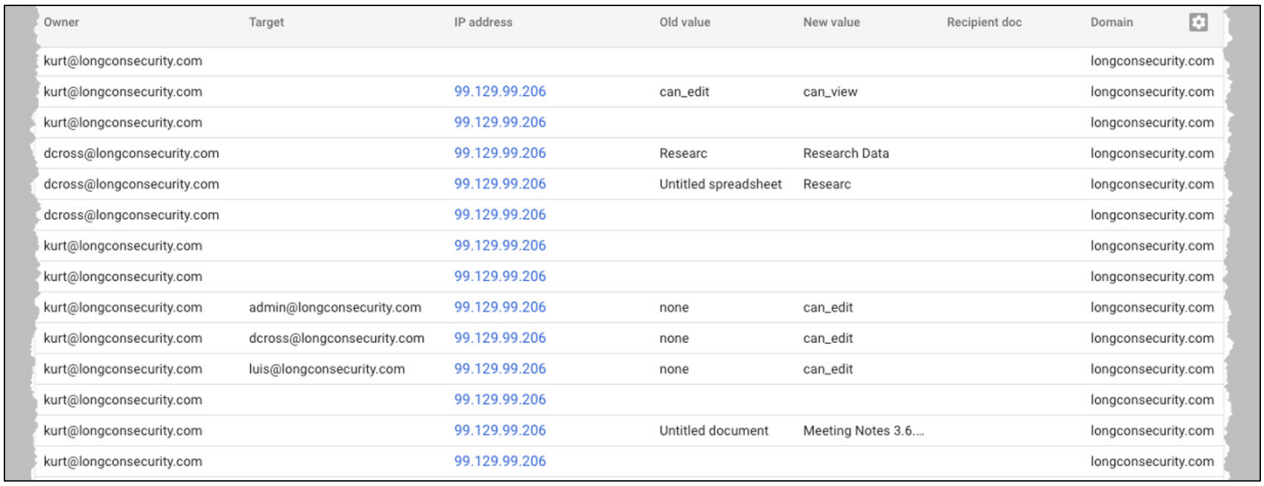
Google Drive: Audit Log (2)

Visibility	Event	Description	Actor
People with link	View	Anonymous user viewed an item	
People with link	Change access scope	Kurt Goreshter changed link sharing access type fro	kurt@longconsecurity.com
Shared internally	Edit	Darren Cross edited an item	dcross@longconsecurity.com
Private	Rename	Darren Cross renamed Researc to Research Data	dcross@longconsecurity.com
Private	Rename	Darren Cross renamed Untitled spreadsheet to Rese	dcross@longconsecurity.com
Private	Create	Darren Cross created an item	dcross@longconsecurity.com
Shared internally	Edit	Darren Cross edited an item	dcross@longconsecurity.com
Shared internally	View	Darren Cross viewed an item	dcross@longconsecurity.com
Shared internally	Change user access	Kurt Goreshter changed sharing permissions for adı	kurt@longconsecurity.com
Shared internally	Change user access	Kurt Goreshter changed sharing permissions for dcı	kurt@longconsecurity.com
Shared internally	Change user access	Kurt Goreshter changed sharing permissions for luis	kurt@longconsecurity.com
Private	Edit	Kurt Goreshter edited an item	kurt@longconsecurity.com
Private	Rename	Kurt Goreshter renamed Untitled document to Meeti	kurt@longconsecurity.com
Private	Create	Kurt Goreshter created an item	kurt@longconsecurity.com

When running a search within the investigator tool a large number of columns are returned. This is a view of the same data shown from the previous slide scrolled along to the right.

Visibility	Event	Description	Actor
People with link	View	Anonymous user viewed an item	
People with link	Change access scope	Kurt Goreshter changed link sharing access type fro	kurt@longconsecurity.com
Shared internally	Edit	Darren Cross edited an item	dcross@longconsecurity.com
Private	Rename	Darren Cross renamed Researc to Research Data	dcross@longconsecurity.com
Private	Rename	Darren Cross renamed Untitled spreadsheet to Rese	dcross@longconsecurity.com
Private	Create	Darren Cross created an item	dcross@longconsecurity.com
Shared internally	Edit	Darren Cross edited an item	dcross@longconsecurity.com
Shared internally	View	Darren Cross viewed an item	dcross@longconsecurity.com
Shared internally	Change user access	Kurt Goreshter changed sharing permissions for adı	kurt@longconsecurity.com
Shared internally	Change user access	Kurt Goreshter changed sharing permissions for dcı	kurt@longconsecurity.com
Shared internally	Change user access	Kurt Goreshter changed sharing permissions for luis	kurt@longconsecurity.com
Private	Edit	Kurt Goreshter edited an item	kurt@longconsecurity.com
Private	Rename	Kurt Goreshter renamed Untitled document to Meeti	kurt@longconsecurity.com
Private	Create	Kurt Goreshter created an item	kurt@longconsecurity.com

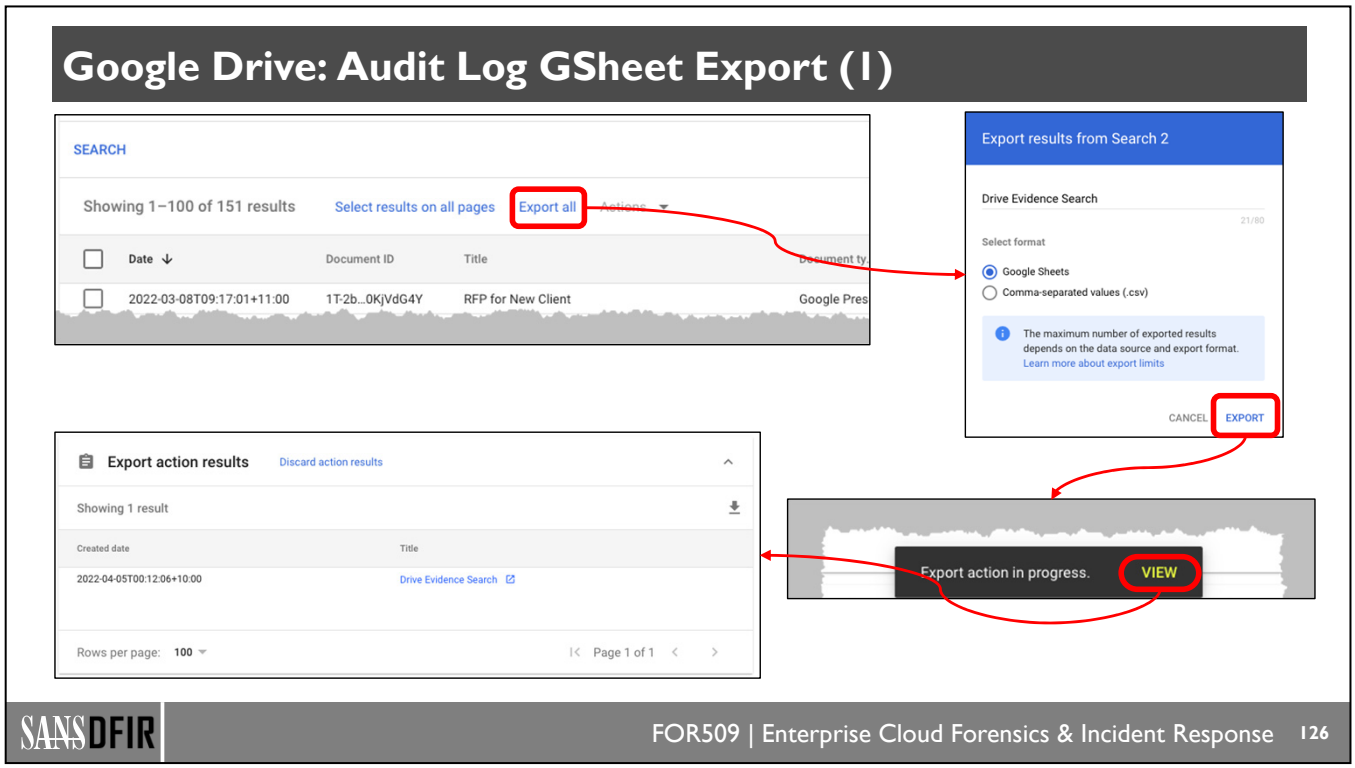
Google Drive: Audit Log (3)



Owner	Target	IP address	Old value	New value	Recipient doc	Domain
kurt@longconsecurity.com						longconsecurity.com
kurt@longconsecurity.com		99.129.99.206	can_edit	can_view		longconsecurity.com
kurt@longconsecurity.com		99.129.99.206				longconsecurity.com
dcross@longconsecurity.com		99.129.99.206	Researc	Research Data		longconsecurity.com
dcross@longconsecurity.com		99.129.99.206	Untitled spreadsheet	Researc		longconsecurity.com
dcross@longconsecurity.com		99.129.99.206				longconsecurity.com
kurt@longconsecurity.com		99.129.99.206				longconsecurity.com
kurt@longconsecurity.com		99.129.99.206				longconsecurity.com
kurt@longconsecurity.com	admin@longconsecurity.com	99.129.99.206	none	can_edit		longconsecurity.com
kurt@longconsecurity.com	dcross@longconsecurity.com	99.129.99.206	none	can_edit		longconsecurity.com
kurt@longconsecurity.com	luis@longconsecurity.com	99.129.99.206	none	can_edit		longconsecurity.com
kurt@longconsecurity.com		99.129.99.206				longconsecurity.com
kurt@longconsecurity.com		99.129.99.206	Untitled document	Meeting Notes 3.6....		longconsecurity.com
kurt@longconsecurity.com		99.129.99.206				longconsecurity.com

This still shows the same results, further scrolled along again, so yes—it's a lot of fields contained within the Investigator tool for Google Drive.

Owner	Target	IP address	Old value	New value	Recipient doc	Domain
kurt@longconsecurity.com						longconsecurity.com
kurt@longconsecurity.com		99.129.99.206	can_edit	can_view		longconsecurity.com
kurt@longconsecurity.com		99.129.99.206				longconsecurity.com
dcross@longconsecurity.com		99.129.99.206	Researc	Research Data		longconsecurity.com
dcross@longconsecurity.com		99.129.99.206	Untitled spreadsheet	Researc		longconsecurity.com
dcross@longconsecurity.com		99.129.99.206				longconsecurity.com
kurt@longconsecurity.com		99.129.99.206				longconsecurity.com
kurt@longconsecurity.com		99.129.99.206				longconsecurity.com
kurt@longconsecurity.com	admin@longconsecurity.com	99.129.99.206	none	can_edit		longconsecurity.com
kurt@longconsecurity.com	dcross@longconsecurity.com	99.129.99.206	none	can_edit		longconsecurity.com
kurt@longconsecurity.com	luis@longconsecurity.com	99.129.99.206	none	can_edit		longconsecurity.com
kurt@longconsecurity.com		99.129.99.206				longconsecurity.com
kurt@longconsecurity.com		99.129.99.206	Untitled document	Meeting Notes 3.6....		longconsecurity.com
kurt@longconsecurity.com		99.129.99.206				longconsecurity.com



When it comes to exporting the results from the Investigator tool, where you've searched for in Google Drive results, you have the ability to export via Google Sheets (GSheets) or CSV. For this example, we're going to export to GSheets to show how you can collect, sort and manipulate the data all within Google Workspace.

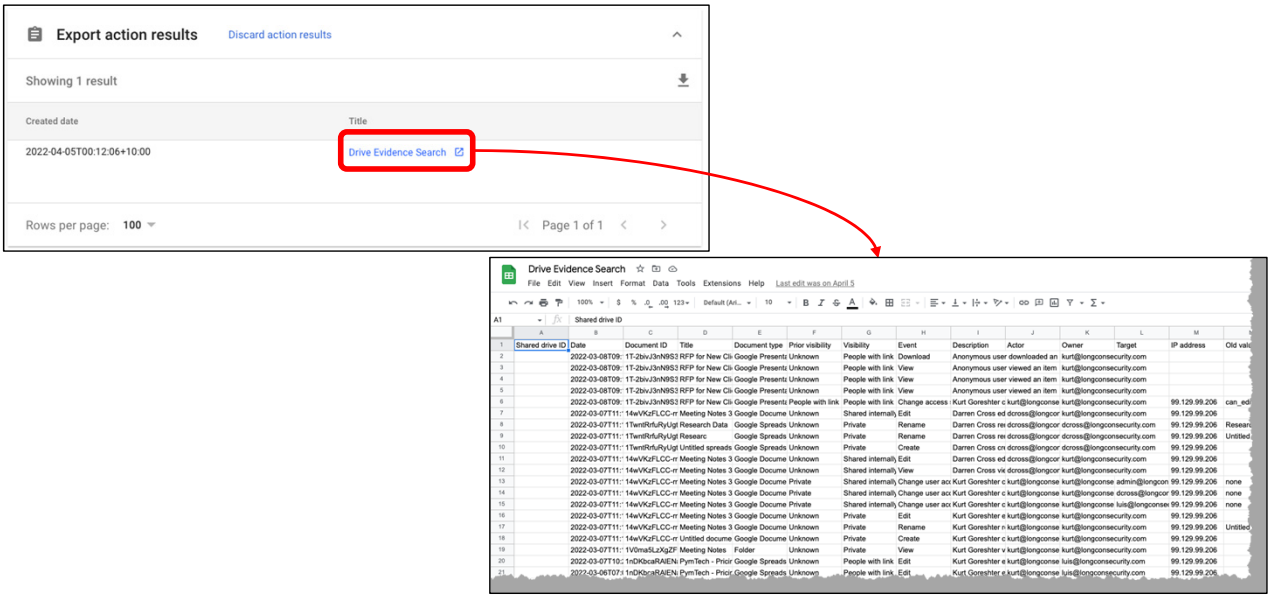
To do this, we can **Export all** which will allow admins to select a name for their results and export them. It's worth understanding that the results will export to the user account you currently use—there is no way to change this. Once the export job starts, a popup at the bottom of the screen will allow you to click **VIEW** to see your export job in the "Export action results" window. This will give you details of the progress of the export, in most cases, this is relatively quick. From the Export action results window, you can also click through to see the GSheet within the Google Drive account for the user you've currently logged in as.

It's important to understand that if you're investigating a Google Workspace that you think may have another admin account compromised, you should be careful when exporting investigation results to your own Google Drive, as other admins would be able to access your Drive. Hopefully, this can be bypassed with a direct CSV export discussed in the upcoming slides.

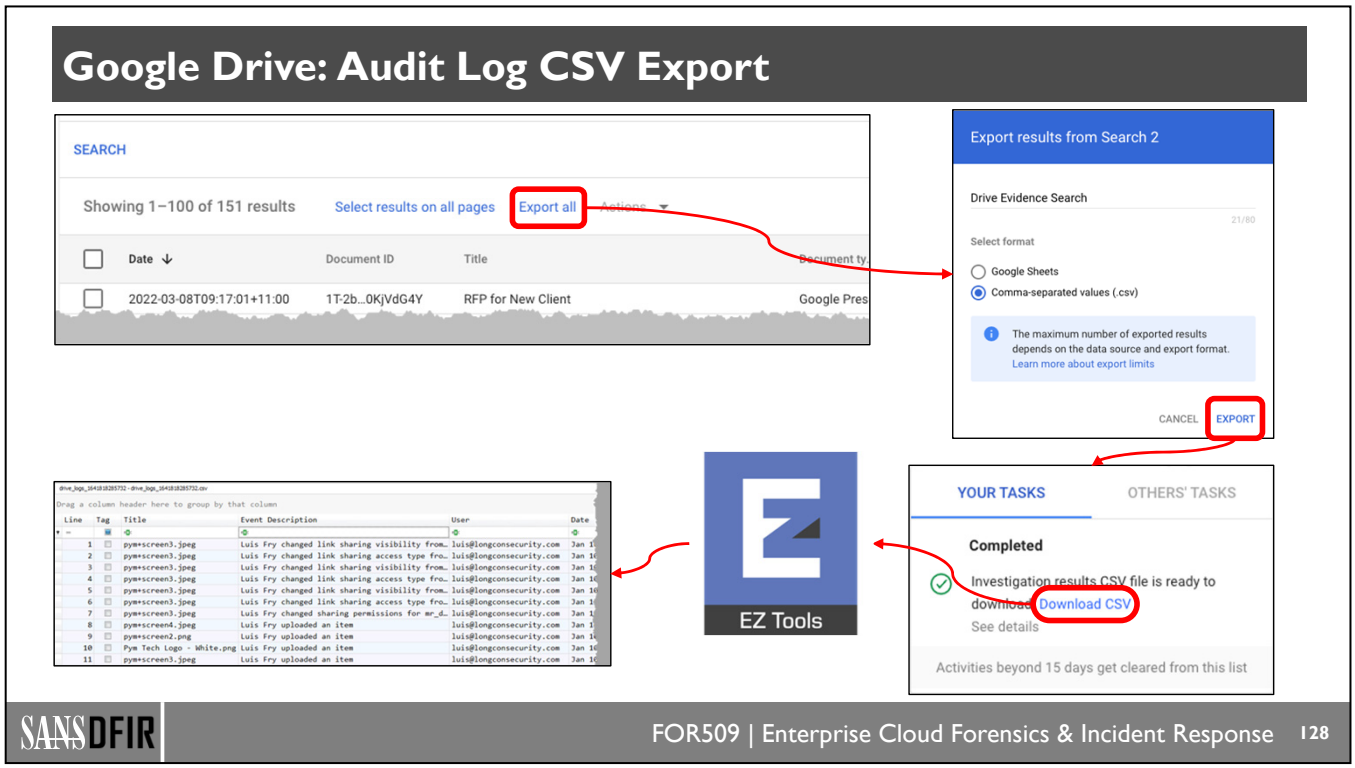
Reference:

https://for509.com/nk7iw (Drive Audit Log)

Google Drive: Audit Log GSheet Export (2)



Once you access the GSheet where your search results are exported, you can now manipulate the results the same way you can manipulate data within a standard GSheet. Commonly, investigators apply a filter with the top row of headings so you can sort, or search specific fields.



When it comes to exporting the results outside of Google Workspace, we can use the export to CSV functionality. This will allow users to produce a CSV that is directly downloadable and is not stored with GDrive.

To do this, we can "Export all" which will allow admins to select a name for their results and export them. Once the export job starts a popup in the top right of the Admin Console called "Your Tasks" will appear. This will give you details of the progress of the export; in most cases this is relatively quick. From the Your Tasks window, you can Download the CSV file and store it on your local computer.

Once you have an exported CSV file, you can also review and search your data within Eric Zimmerman's Timeline Explorer. Timeline Explorer will allow you to manipulate the CSV data and narrow down what you're searching for. Additionally, if you're dealing with a compromised Google Workspace, it's always better to do your analysis outside of a suspect compromised environment.

References:

https://for509.com/nk7iw (Drive Audit Log)

https://for509.com/ztools (Eric Zimmerman's Tools)

Google Drive: Audit Log

Field	Description
Title	Document that the event relates to.
Event Description	Summary of the event that occurred.
User	The user account that performed the action.
Date	Timestamp in the user's browser default time zone.
Event	Action that occurred to the Drive document.
Document ID	Unique ID for all Drive documents.
Document Type	File type.
Owner	The user account that owns the document.
Prior Visibility	Visibility/access to the document prior to the current event.
Visibility	Visibility/access to the document after the current event has occurred.
IP Address	IP address of the actor that caused the event log.
Billable	Is the document counting toward the user's storage. Only used for Essentials edition.

Above are some of the common fields that are included with both a GSheet export and an export of the Google Drive logs via the API. Most of the above fields are fairly self-explanatory, although there are some that are a little unique to Google Drive.

Document ID: This is the unique identifier for each document on Google Drive. It is unique across all Google Workspace accounts. Additionally, it's also the unique identifier you see in the URL when accessing a document. This can be helpful when matching URL analysis to a document in Google Drive.

Owner: As the name suggests, this is the owner of the document. Just ensure you don't confuse this with the account that may have triggered an event/log entry to occur—that would be the "Actor".

Prior Visibility and Visibility: Both the "Prior Visibility" and "Visibility" field work together to show you changes to permissions on a file related to access for users. Remember that "Visibility" is what access is granted from that point forward for the document.

Reference:

https://for509.com/nk7iw (Drive Audit Log)

Google Drive: Audit Log API Export: Download Item


```
{"kind": "admin#reports#activity",
"id":
        {"time": "2022-03-07T22:17:01.282Z", "uniqueQualifier": "-3477046602842742256", "applicationName":
"drive", "customerId": "C02mvk4dm"},
"etag": "\"UMvHtdUQGju4SaKTK2kLjj-ZwxshlPj9bXaU2gdcugA/581xt0tbsL12BHhfvOdf8CC6RC0\"",
"actor":
        {"email": "", "profileId": "105250506097979753968"},
"events": [
        {"type": "access", "name": "download",
        "parameters":
                [{"name": "primary_event", "boolValue": true},
                {"name": "billable", "boolValue": false},
                {"name": "doc_id", "value": "1T-2bivJ3nN9S3ErPmkeG7yFOAKvF6lsyehi0KjVdG4Y"},
                {"name": "doc_type", "value": "presentation"},
                {"name": "is_encrypted", "boolValue": false},
                {"name": "doc_title", "value": "RFP for New Client"},
                {"name": "visibility", "value": "people_with_link"},
                {"name": "actor_is_collaborator_account", "boolValue": false},
                {"name": "owner", "value": "kurt@longconsecurity.com"},
                {"name": "owner_is_shared_drive", "boolValue": false},
                {"name": "owner_is_team_drive", "boolValue": false}]}]
}
```


When you export Google Drive data via the API, above is a representation of what it will look like for a file that is downloaded from Google Drive. Keep in mind the above JSON data has been re-formatted to fit better on this page. It will actually look like correctly formatted JSON data.

You'll notice that the API logs provide a lot more detail than the Admin Console's Investigation tool. If given the choice you should export Google Drive data via API to get access to the additional telemetry that it provides.

Of importance within the data above are details around what type of event you're actually looking at. You can find this under the "events" and "type" fields. In the example above, you'll see the "type" is "access" with the sub-type "name" being "download", means the file was downloaded.

It's important to understand that if a file is accessed, and its permissions allow unauthenticated access (i.e., it's a publicly accessible file) then Google Workspace will not record individual unauthenticated view only access; however, they will report edits and downloads for unauthenticated users. A download in this context is accessing the file in the web browser, or direct link, and then initiating a Download/Export.

Google Drive: Audit Log API Export: Edit Item


```
{"kind": "admin#reports#activity",
  "id": {
    "time": "2022-03-07T22:13:23.021Z",
    "uniqueQualifier": "-4454720330609995273",
    "applicationName": "drive",
    "customerId": "C02mvk4dm"},
  "etag": "\"UMvHtdUQGju4SaKTK2kLjj-
ZwxshlPj9bXaU2gdcugA/SUMnR4odC9AiV_iLFmsM9uMSieA\"",
  "actor": {
    "email": "kurt@longconsecurity.com",
    "profileId": "112036045880884988161"},
  "ipAddress": "99.129.99.206",
  "events": [
    {"type": "access", "name": "edit",
      "parameters": [
        {"name": "primary_event", "boolValue": false},
        {"name": "billable", "boolValue": true},
        {"name": "doc_id", "value": "1T-
2bivJ3nN9S3ErPmkeG7yFOAKvF6lsyehi0KjVdG4Y"},
        {"name": "doc_type", "value": "presentation"},
        {"name": "is_encrypted", "boolValue": false},
        {"name": "doc_title", "value": "RFP for New
Client"},
        {"name": "visibility", "value":
"people_with_link"},
        {"name": "originating_app_id",
          "value": "1095901163807"},
        {"name": "actor_is_collaborator_account",
          "boolValue": false},
        {"name": "owner",
          "value": "kurt@longconsecurity.com"},
        {"name": "owner_is_shared_drive",
          "boolValue": false},
        {"name": "owner_is_team_drive",
          "boolValue": false}]},
    {"type": "acl_change",
  "name": "change_document_access_scope",
      "parameters": [
        {"name": "primary_event", "boolValue": true},
        {"name": "billable", "boolValue": true},
        {"name": "visibility_change", "value": "none"},
        {"name": "target_domain", "value": "all"},
        {"name": "old_value",
          "multiValue": ["can_edit"]},
        {"name": "new_value",
          "multiValue": [
            "can_view"]},
        {"name": "old_visibility",
          "value": "people_with_link"},
<SNIP>
```


Similar to the previous page, this is another log example from the data that is provided by the Audit API from Google Workspace for a Google Drive event. In this example a Google Drive item was edited and saved. You can tell this from the following section:

```
{"type": "access", "name": "edit",
```

There is also a permission change occurring with this event as well. If you look further through the JSON data, you will see an ACL change that starts with this line:

```
 {"type": "acl_change", "name": "change_document_access_scope",
```

Following the above line, we have details of the ACL permissions that were changed by the editor.

```
{"kind": "admin#reports#activity",
  "id": {
    "time": "2022-03-07T22:13:23.021Z",
    "uniqueQualifier": "-4454720330609995273",
    "applicationName": "drive",
    "customerId": "C02mvk4dm"},
  "etag": "\"UMvHtdUQGju4SaKTK2kLjj-ZwxshlPj9bXaU2gdcugA/SUMnR4odC9AiV_iLFmsM9uMSieA\"",
  "actor": {
    "email": "kurt@longconsecurity.com",
    "profileId": "112036045880884988161"},
  "ipAddress": "99.129.99.206",
  "events": [
    {"type": "access",
      "name": "edit",
      "parameters": [
        {"name": "primary_event",
          "boolValue": false},
        {"name": "billable",
          "boolValue": true},
        {"name": "doc_id",
          "value": "1T-2bivJ3nN9S3ErPmkeG7yFOAKvF6lsyehi0KjVdG4Y"},
        {"name": "doc_type",
          "value": "presentation"},
        {
          "name": "is_encrypted",
          "boolValue": false
        },
        {
          "name": "doc_title",
          "value": "RFP for New Client"
        },
        {
          "name": "visibility",
          "value": "people_with_link"
        },
        {
          "name": "originating_app_id",
          "value": "1095901163807"
        },
        {
          "name": "actor_is_collaborator_account",
          "boolValue": false
        },
        {
          "name": "owner",
          "value": "kurt@longconsecurity.com"
        },
        {
          "name": "owner_is_shared_drive",
          "boolValue": false
        },
        {
          "name": "owner_is_team_drive",
          "boolValue": false
        }
      ]
    },

 {
      "type": "acl_change",
      "name": "change_document_access_scope",
      "parameters": [
        {
          "name": "primary_event",
          "boolValue": true
        },
        {
          "name": "billable",
          "boolValue": true
<continued next page>
```

```
},
        {
          "name": "visibility_change",
          "value": "none"
        },
        {
          "name": "target_domain",
          "value": "all"
        },
        {
          "name": "old_value",
          "multiValue": [
            "can_edit"
          ]
        },
        {
          "name": "new_value",
          "multiValue": [
            "can_view"
          ]
        },
        {
          "name": "old_visibility",
          "value": "people_with_link"
        },
        {
          "name": "doc_id",
          "value": "1T-2bivJ3nN9S3ErPmkeG7yFOAKvF6lsyehi0KjVdG4Y"
        },
        {
          "name": "doc_type",
          "value": "presentation"
        },
        {
          "name": "is_encrypted",
          "boolValue": false
        },
        {
          "name": "doc_title",
          "value": "RFP for New Client"
        },
        {
          "name": "visibility",
          "value": "people_with_link"
        },
        {
          "name": "originating_app_id",
          "value": "1095901163807"
        },
        {
          "name": "actor_is_collaborator_account",
          "boolValue": false
        },
        {
          "name": "owner",
          "value": "kurt@longconsecurity.com"
        },
        {
          "name": "owner_is_shared_drive",
          "boolValue": false
        },
        {
          "name": "owner_is_team_drive",
          "boolValue": false
        }
<SNIP>
```

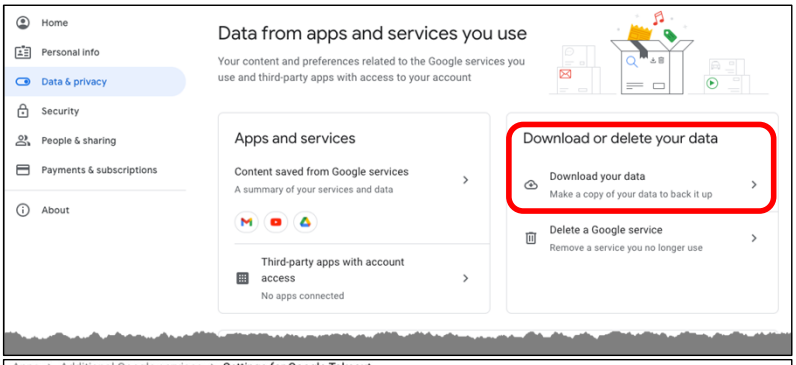
Data Exposure/Leakage/Exfil
(TA0009)

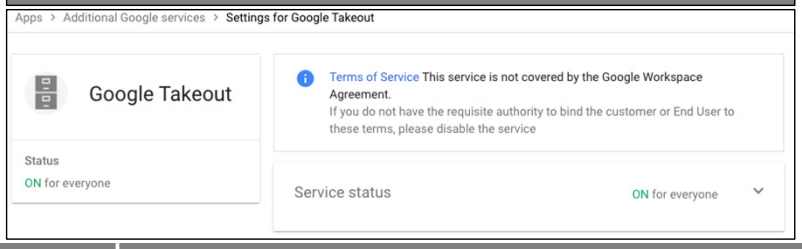
SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Data Exfil with Takeout

This page intentionally left blank.

Takeout: Initial Setup





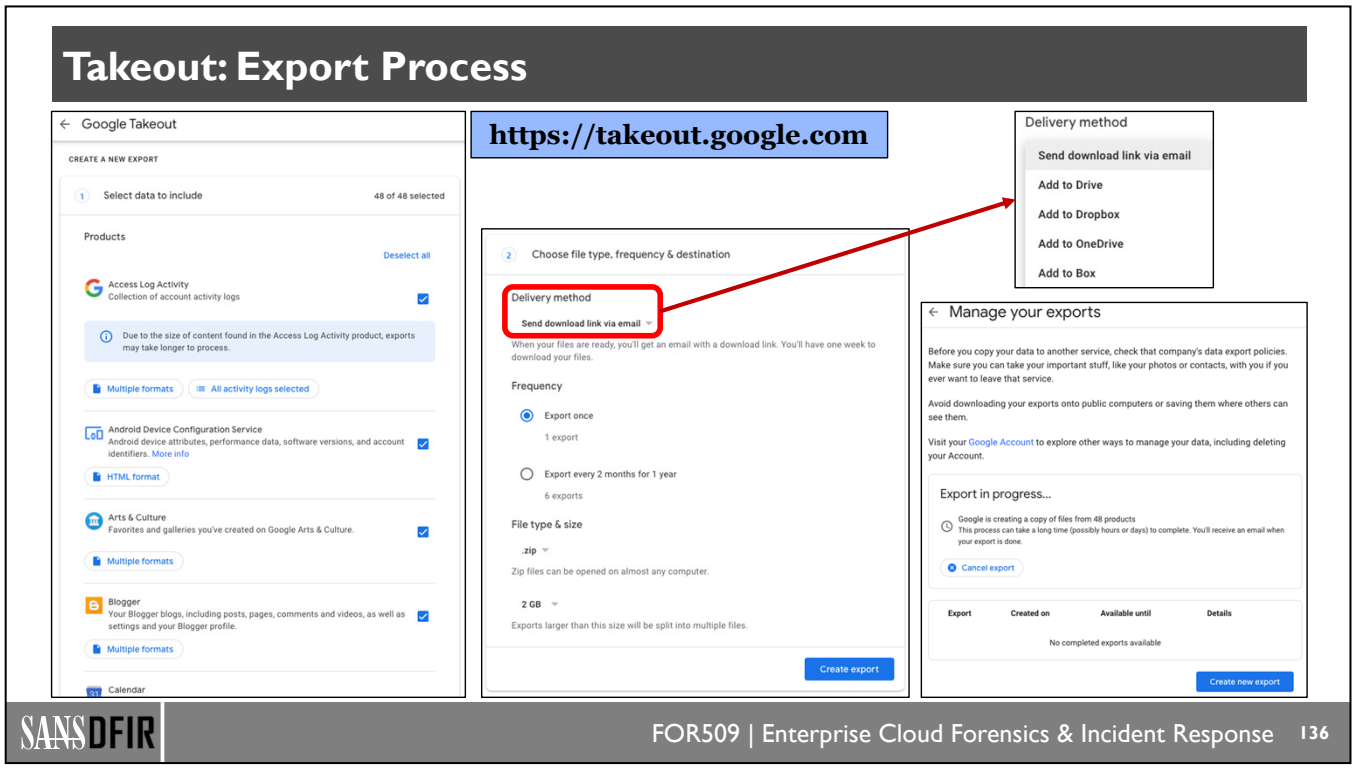
Accessing Takeout

- Each user has the ability to export or transfer their Workspace data out of an Organization.
- Takeout is ON by default for new Organizations, even Enterprise licenses.
- Group Owners can export all Group contents, including email.

Google account holders, including Google Workspace accounts, have the ability to export all the data from within their account as a single archive.[1] This feature is known within Workspace as "Google Takeout"; however, it's also known as "Download Your Data".[2] Originally this service was set up to allow users to access the various APIs within Google products to allow them to download a more human friendly version of their data. Additionally, this service could be used to transfer data from one Google account to another. Consider if a user wanted to move from the free Gmail service over to a paid Google Workspace account.

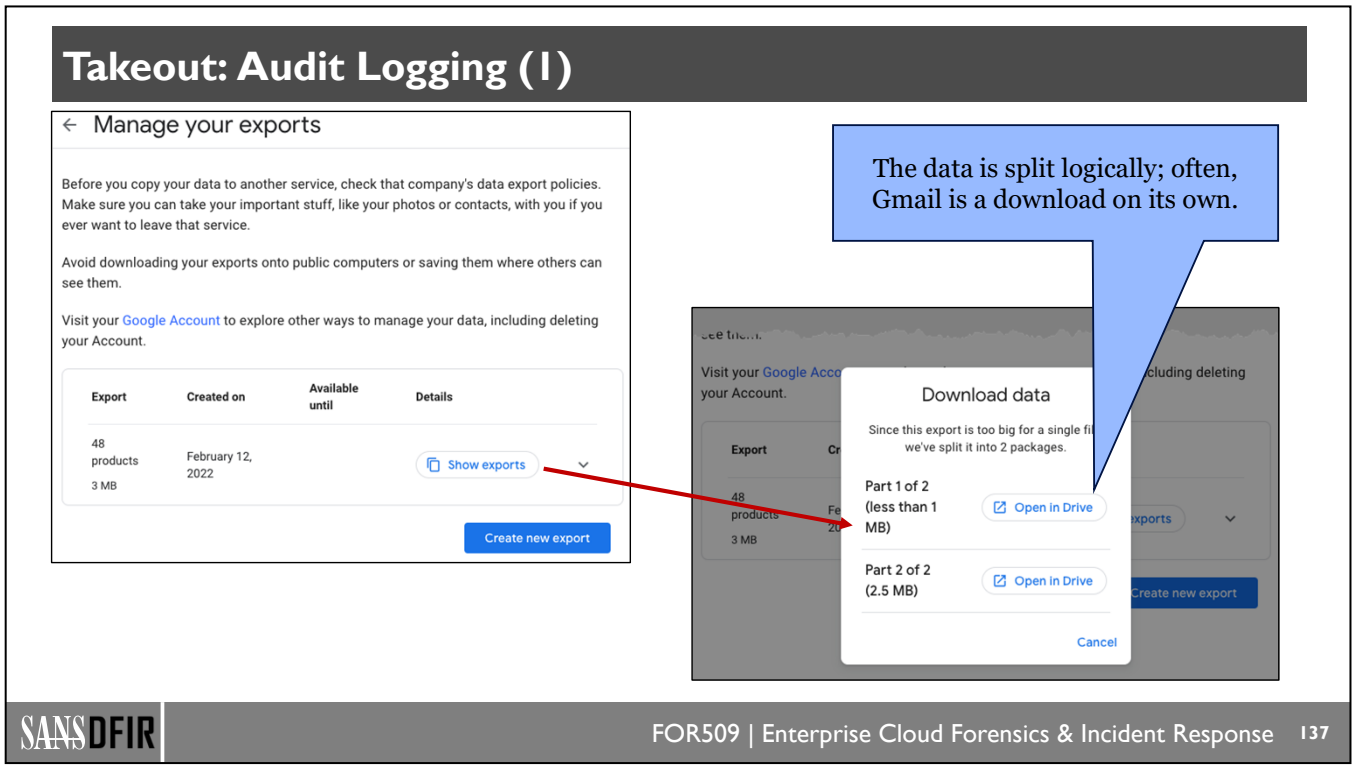
The challenge presented by Google Takeout is that it is enabled by default in Google Workspace accounts which can present a risk of a user exporting all the data they have within their account, including email, documents, and sites. Furthermore, any user that is also a Group Owner, within Workspace, is able to export all the content that is contained within the group. In most enterprises this is email, but it can be group documents depending how your Workspace Groups are set up.

1. https://for509.com/mzalx (How to download your Google data)
2. https://for509.com/9dgtz (Introducing Data Transfer Project: an open-source platform promoting universal data portability)



The above provides a view of what a user would see when they perform an export with Takeout. Initially they would need to access the Takeout address (takeout.google.com), then select all the services they wish to export, then select the method of how they would like the export to be organized. Users can choose to break up their Takeout export into smaller zip files based on size of time. Lastly users can also choose where they would like their export delivered. Because Takeout was intended to provider users with an export of all their data, it is possible to export your Takeout data to non-Google based services—for example, Drobox, OneDrive, and Box. From a forensics perspective this can be challenging as a Workspace data would be directly leaving Workspace and possibly outside the scope of what an investigator may have access to. If users stick with the default option, they will end up with an email pointing them to a link in the mailbox to download the contents from the export.

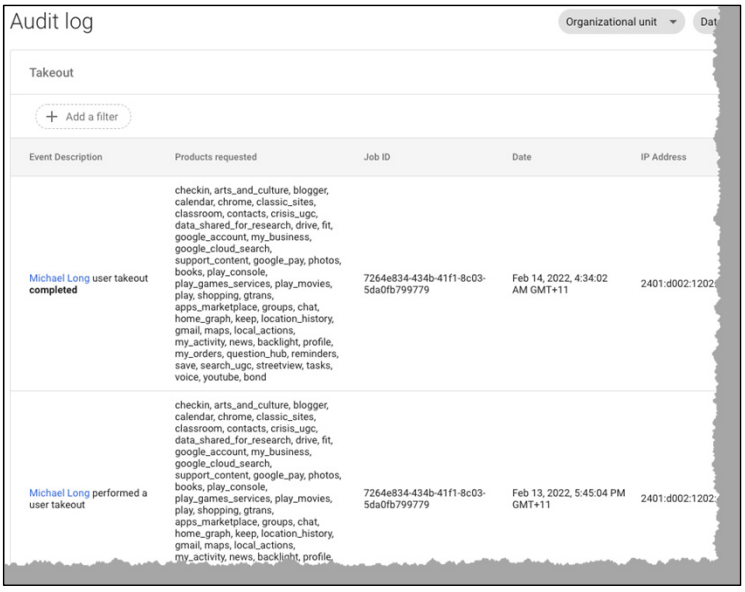
A Takeout export is not immediate; it will take some time in the background. Users can see the status of their export in the "Manage your exports" section of Takeout. Additionally, this section will also show users previous exports that have occurred. The time for an export to complete is highly dependent on the number of services they selected to export, and the amount of data they have in each service.



Once an export is complete users can **Show exports** to see the data and how it's been broken up. Even if a user has not opted for the data to be broken into multiple files based on size or time, Takeout will logically break up the export often based on service. A lot of the time, the Gmail data is broken out into a zip file on its own, with all other data in another zip file.

Users can then choose to access their data within Google Drive, unless they have directly exported it to a third-party storage service.

Takeout: Audit Logging (2)



Takeout Audit Logging

- Takeout has a dedicated Audit Log in the Admin Console.
- Takeout Audit Logs **are not** (currently) **accessible via the Google Workspace API.**
- Aside from the event occurring and the services used to extract data, all other useful DFIR information will be in other Audit Logs.
- The IP address in this log is most useful when matching up other user events in other Audit Logs.

Google Workspace accounts will log every user that started a Takeout export and the services they included within the Takeout export, along with details like the time and IP address it was initiated from. A log is also generated when the export packaging of all the files is complete.

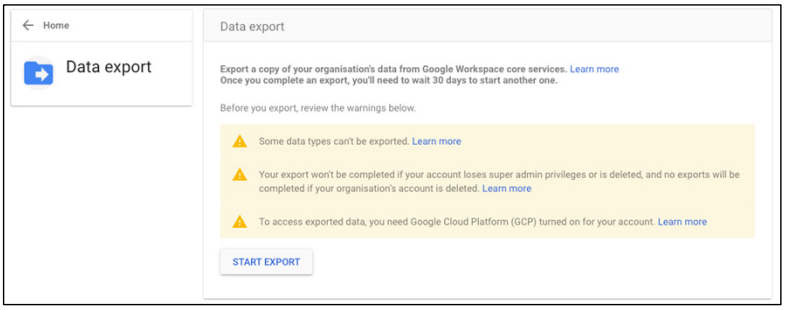
The Takeout audit log does not provide details about users downloading or accessing the data packaged up by Takeout. If a user had selected to keep the export within their Google account details of accessing the downloaded zip files will be in the Google Drive audit log. However, if a user decided to export their data to a third-party cloud storage service, once the "completed" log occurs you should assume that all data has been pushed to the third-party cloud storage services.

The Takeout audit log is one of the few forensically relevant logs that is not included within the logs you can access via the API. This is important to remember as if you only use API access to collect relevant data from Google Workspace you will be missing information related to exports with Takeout.

Reference:

https://for509.com/lakr8 (Takeout audit log)

Customer Takeout: Export Whole Organization



https://admin.google.com/ac/customertakeout

Customer Takeout/Exfil

- Customer Takeout lets an Organization Super Admin export all of the Workspace data.
- This includes all data in Vault that is subject to a **Hold** or any deleted retention policies.
- To do this you need an admin account with MFA enabled and less than 1000 users.
- The Workspace account also has to be more than 30 days old.

In addition to individual user exports via Takeout, there is also a service within Workspace called "Customer Takeout" which allows you to export all data from your whole organization. This includes any data that you have specific retention rules set up for, include any users or files you have a "Hold" set up for in Vault. This action can only be performance by a Workspace administrator, so it's not something that most users will have access to.

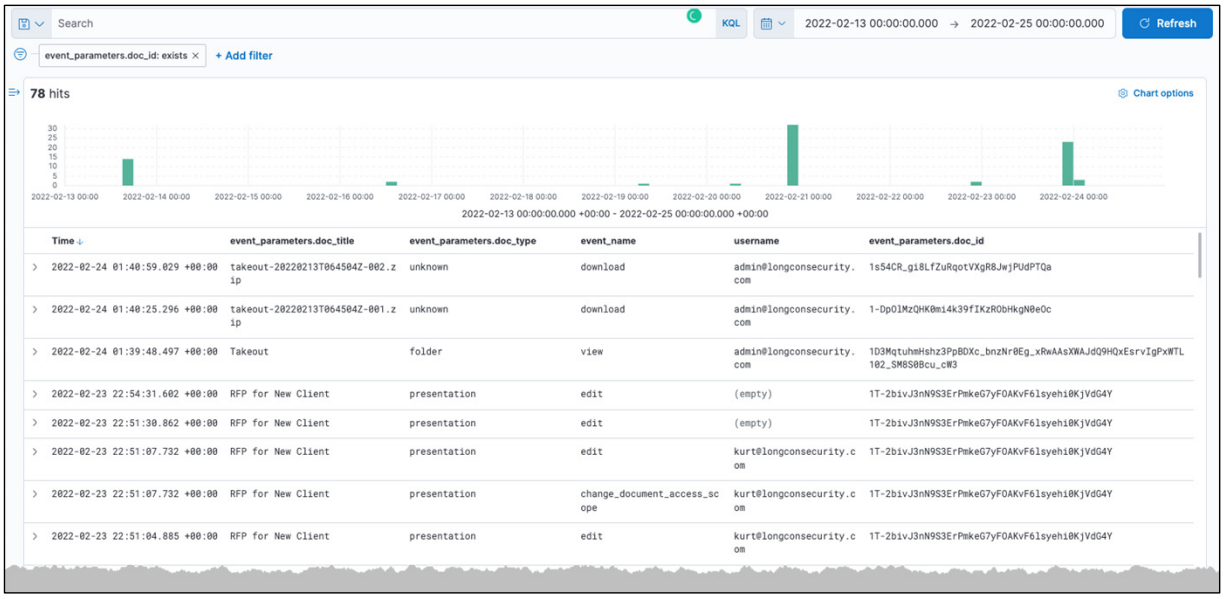
There are a few restrictions on being able to perform this task. Not only do you need to be an administrator for the organization, you also need to have MFA enabled on your account, and your workspace must be older than 30 days. Lastly, you can only perform this action on Workspace organizations that have less than 1000 active user accounts.

The challenge with both the user version of Takeout and Customer Takeout is it gives a threat actor a fast and easy way to exfil data out of an organization's Workspace. It is beneficial that these tasks can't be performed immediately and do take some processing time in the background.

Reference:

https://for509.com/lfmqg (Export your organization's data)

Lab 4.3: Google Workspace Data Exposure

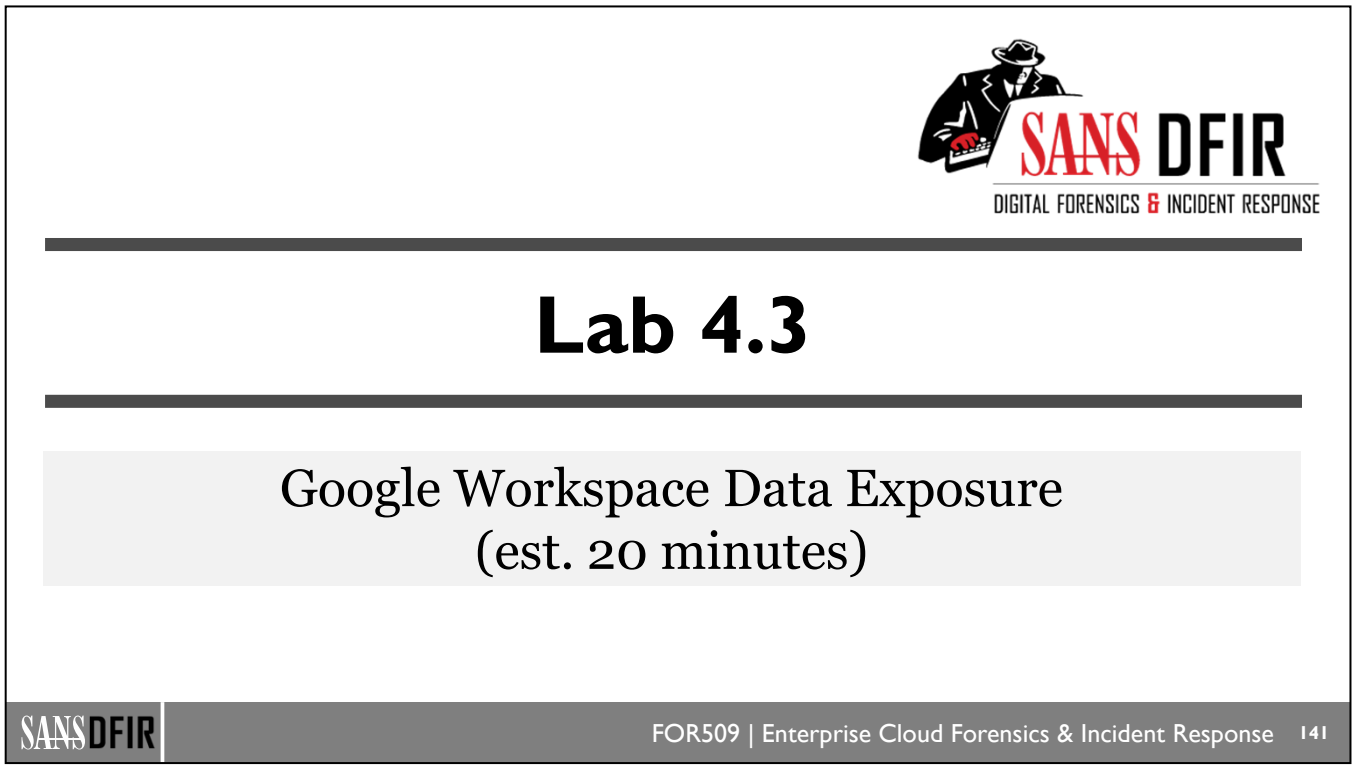


The example above shows you SOF-ELK with the Google Drive logs extracted from Google Workspace in JSON format via an API request and loaded into SOF-ELK. In the upcoming lab, you will need to limit your data set if you have loaded other data into SOF-ELK already.

The data set under the "gws-*" index will hold all the Google Workspace data. When you're viewing this index, you will see all Google Workspace data loaded in SOF-ELK. Using the **Add filter** button below the search bar, create a new filter that uses the **event_parameters.doc_id** field and **exists**. This will limit your data to only logs related to documents or files within Google Drive. When you're reviewing Google Drive activity, this filter is simply the starting point. However, when you're looking for malicious activity, you will also need to pivot to other logs to determine actions that may have been taken by a threat actor.

The filter function at the top can be enabled and disabled by simply clicking on it. Set it to "Temporarily disable" if you want to see all Google Workspace data related to your search in the search bar at the top.

In addition to using the filter, you may also want to add specific fields to see summary values for the log entries. For user authorized application log events, the common fields that are useful are @time, event_parameters.doc_title, event_parameters.doc_type, event_name, username, and event_parameters.doc_id. These will provide you with a summary view of each log entry to better understand what is occurring in the logs.



This page intentionally left blank.

Google Workspace Forensics and IR Roadmap

4.1: Understanding Google Workspace

4.2: Google Workspace Evidence

4.3: ATT&CKing Workspace

4.4: Workspace Evidence in Google Cloud

- Google Cloud CLI Tools for Log Collection
- Setting up CLI Access to Google Cloud
- gcloud Log Collection
- **Lab 4.4**: Collecting Workspace Logs in Google Cloud via CLI

This page intentionally left blank.

This page intentionally left blank.

Google Cloud: gcloud

gcloud Overview

- gcloud is a command line utility that is part of Google Cloud's SDK
- gcloud is intended to interact with Google Cloud via command line on multiple platforms
- gcloud is intended to be used for command line scripting and automation; it is not intended for integration into larger applications

gcloud for Log Access

- gcloud has better integration for collection and querying logs from outside of Google Cloud's web interface
- gcloud can use standard Google Cloud accounts for Service Accounts for authentication
- gcloud can also perform an interactive OAuth login, or a console-based OAuth login—which still requires access to a browser

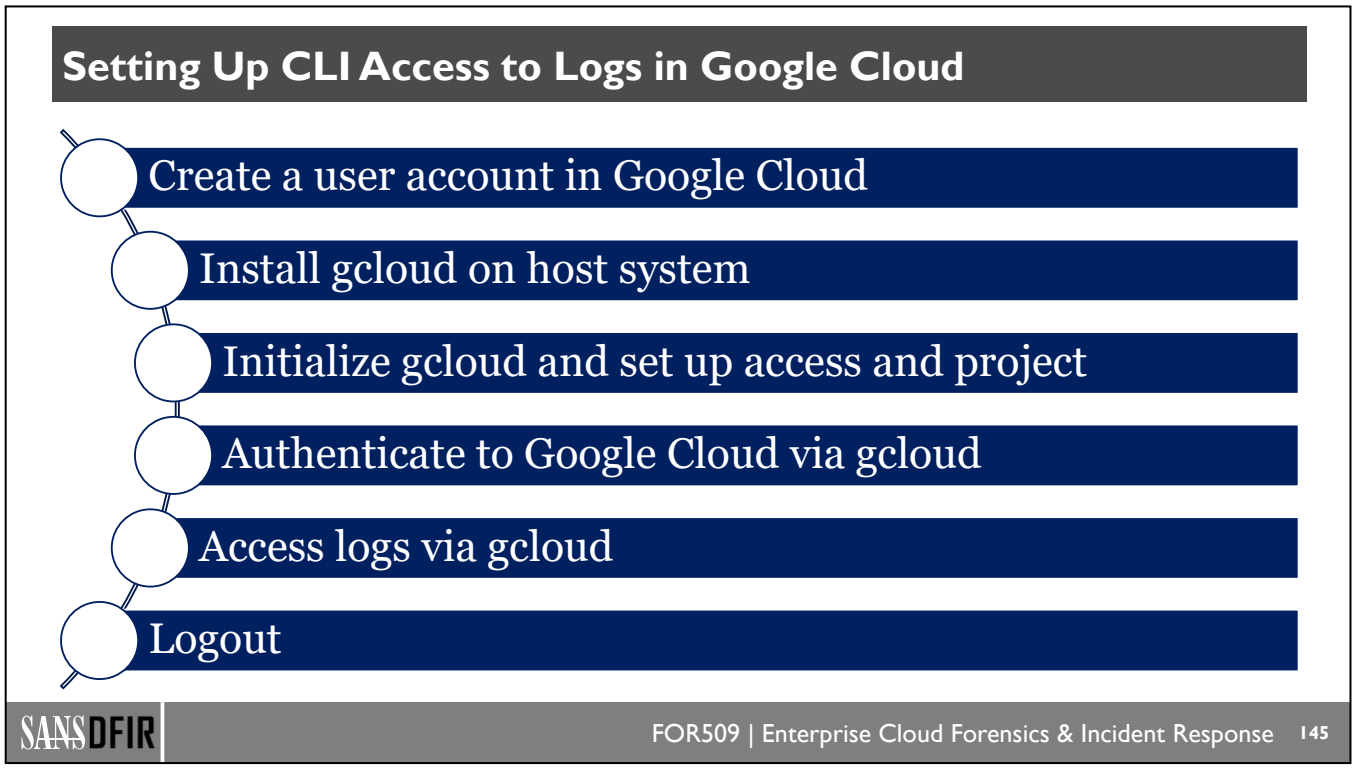
So far within this section we've looked largely at extracting information by the Workspace Admin Console or via the Workspace APIs. Earlier in this section we also looked at how to have our Workspace logs pushed in the Google Cloud. In Section 5 of the course we're going to explore more about Google Cloud; however, in this part we wanted to show investigators how they can retrieve their Google Workspace logs from Google Cloud's logging platform.

To access Google Cloud, we're going to use "gcloud", which is a cross platform command line utility for interacting with Google Cloud. In Section 5 of this course we'll also look at how to access the logs from Google Cloud's web interface.

To use the gcloud utility, we will need either a Service Account, similar to what we've look at previously, or we will need a user account which has "Private Log Viewer" access. This would allow us to OAuth with Google Cloud for authorization with gcloud.

Reference:

https://for509.com/gcloud (gcloud CLI overview)



Above are the summary steps we're going to use for accessing our Workspace logs are that being stored over in Google Cloud.

1. We will need a user account within the Google Cloud where are logs are being sent. This can either be a Service Account or a standard user account with the correct permissions.

2. We will need to install the gcloud CLI package on the host system we intend to use to collect the logs from Google Cloud.

3. We then need to use gcloud to provide it details for the Project within Google Cloud we wish to access. More details on how Projects work in Section 5.

4. Using the account we have for Google Cloud, we will need to authenticate with gcloud.

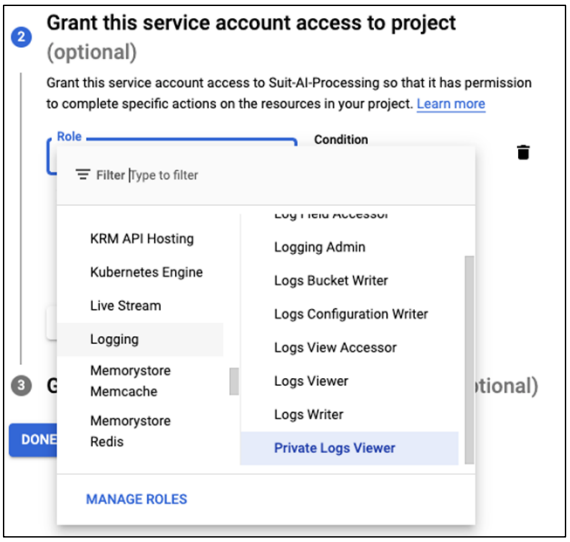
5. We can review the logs we have access to, search the logs for specific details, or collect the logs to the host we are using gcloud from.

6. Lastly, we need to ensure we log off correctly and don't leave an open session. As we'll be using the Google Cloud API access to fetch log data, there is no simple way for an API to know we have finished unless we specifically tell it.

Reference:

https://for509.com/2eol7 (Create a service account)

Google Cloud CLI Access: Service Account Permissions



Account Permissions

- When setting up a dedicated Service Account you can specify the permission for accessing logs.
- DFIR staff will require **Private Logs Viewer** when accessing logs via gconsole.
- There is a **Logs Viewer;** however, it does not include access to audit logs. This will be more relevant in the Google Cloud section.
- **Logs Viewer** could be used if you only want to access your Google Workspace logs in Google Cloud.

Regardless of if you are using a Service Account or a standard user account, you will need "Private Logs Viewer" permissions on the account you want to use to query and collect logs with gcloud. This permission is ideal for investigators as it provides access to some logs which are considered sensitive, including those with IP addresses in them for tracking user accounts. There is also a "Logs Viewer" permission; however, it will not provide access to audit logs within Google Cloud, but it would provide access to the Google Workspace logs that were imported. Based on Section 5 of the course, you may be better off with "Private Logs Viewer" access.

Both the "Private Logs Viewer" and "Logs Viewer" access only provide read access to logs. You cannot alter logs with either of these permissions.

References:

https://for509.com/k7iru (Access control with IAM)

https://for509.com/7moq1 (Create a service account)

Google Cloud CLI Access: Setup Process

gcloud Setup

- Using gcloud with a normal Google Cloud user account is the preferred option when using gcloud. This will give you greater control over user access.
- Any user account intended to access Google Cloud logs will require at least **Private Logs Viewer** access.
- There are access permissions to delete and add to logs—this is not needed for DFIR.

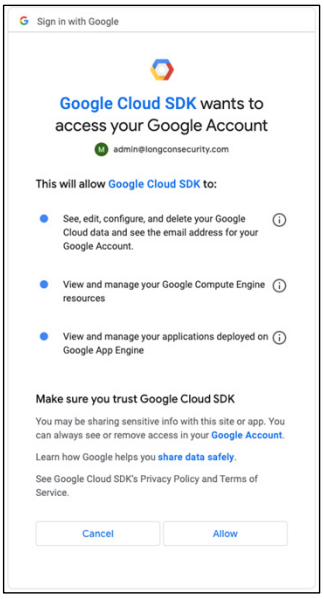
```
$ gcloud init --no-browser

Go to the following link in your browser:
    https://accounts.google.com/o/oauth2/auth?response_type=code&client_id=<SNIP>

Enter verification code: 4/1AX4XfWhplaHZ2uDVKzwbRN6_<SNIP>
You are logged in as: [admin@longconsecurity.com].
```

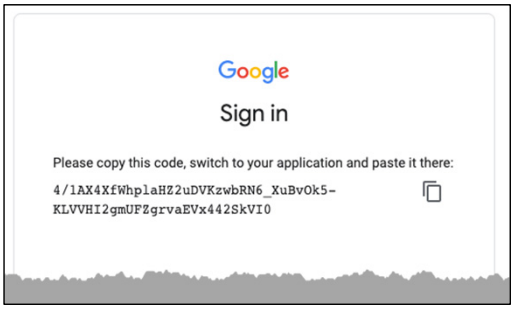

Once you have installed gcloud on your host[1] you can then attempt to initialize gcloud so it connects to Google Cloud and prompts you for authentication. You can even use gcloud on systems that don't have a graphical user interface or web browser with the "--no-browers" command to give you a URL to paste into another browser. In most cases this is ideal when you're using gcloud.

The example above assumes you're using a standard user account from Google Cloud, not a Service Account. We will look at the process for using a Service Account within the upcoming lab.

1. https://for509.com/y7te6 (gcloud SDK Installation)

Google Cloud CLI Access: OAuth Setup Process





API Library Permissions

- Unlike the Service Account you used with Workspace Logs, Google Cloud can use an existing account.
- When you initialize gconsole it will force an OAuth request on your Google Cloud account.
- After accepting the request, you are presented with a verification code to paste into gconsole.

Once you paste the provided URL from gcloud into a web browser you are prompted to authenticate with your standard user account, then you're asked to provide OAuth approval for the Google Cloud SDK. Once you select **Allow** an authorization code is provided in the web browser that needs to be copied and pasted back into gcloud. It is this code, in combination with the initial URL from gcloud, that authorizes the CLI sessions to start accessing Google Cloud with your user account.

Google Cloud CLI Access: Collect Logs (1)

gcloud

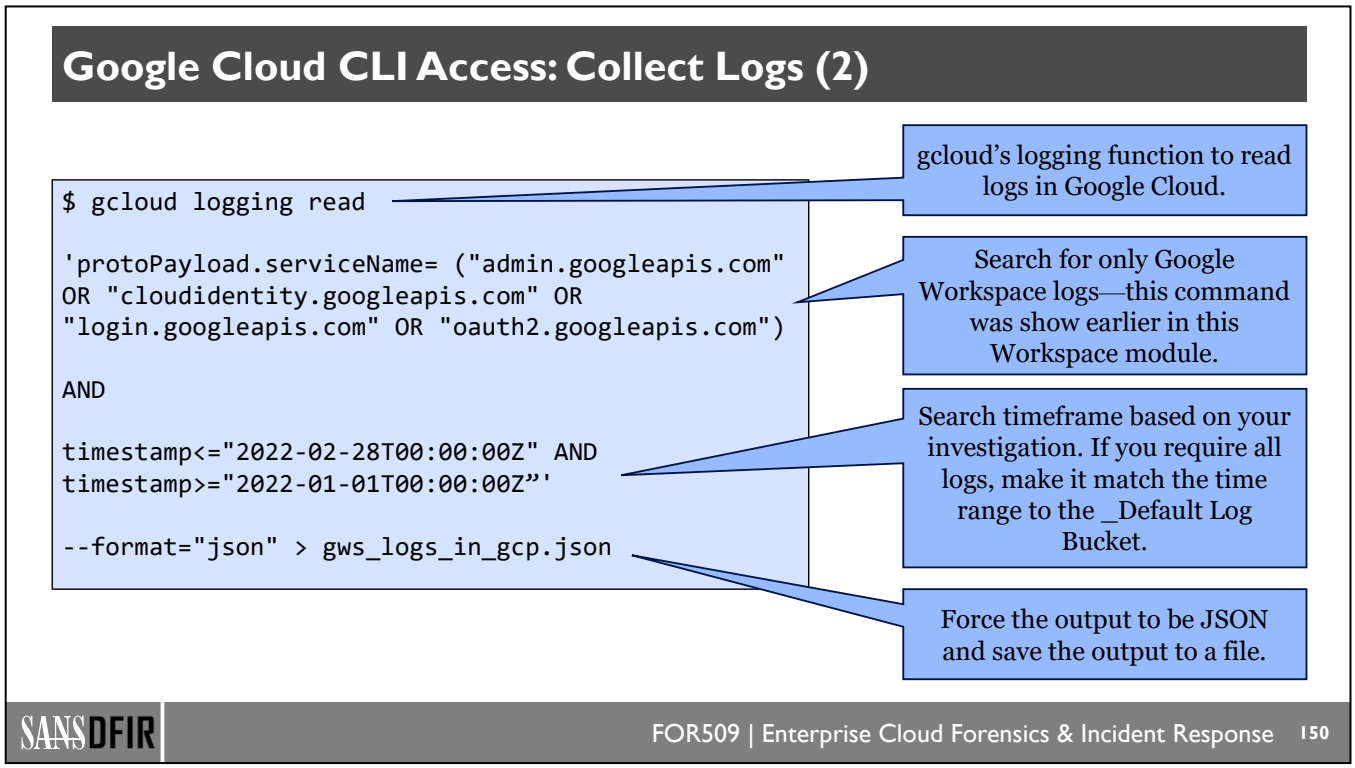
- Once you have authenticated to Google Cloud via gcloud you can directly query the resources in Google Cloud that you have access to.
- Start by determining what Logging Buckets exist and their time range. This will determine how far back in time you can collect logs.
- The **logging read** command only returns limited results and is not JSON formatted by default.
- To force **logging read** to return all results and in JSON format we have to provide additional commands.

```
$ gcloud logging buckets list
LOCATION  BUCKET_ID        RETENTION_DAYS  RESTRICTED_FIELDS  LIFECYCLE_STATE  LOCKED  CREATE_TIME                    UPDATE_TIME
global    All_Logs_Bucket  90                                 ACTIVE                   2021-04-26T12:34:57.409376887Z  2021-04-26T12:34:57.409376887Z
global    DFIR_Bucket      90                                 ACTIVE                   2021-03-30T13:35:21.843425950Z  2021-03-30T13:35:21.843425950Z
global    _Default         30                                 ACTIVE
global    _Required        400                                ACTIVE           True

$ gcloud logging read 'protoPayload.serviceName= ("admin.googleapis.com" OR
"cloudidentity.googleapis.com" OR "login.googleapis.com" OR "oauth2.googleapis.com")
AND timestamp<="2022-02-28T00:00:00Z" AND timestamp>="2022-01-01T00:00:00Z"' --
format="json" > gws_logs_in_gcp.json
```


Once you have completed the authentication steps with gcloud you can then perform CLI requests to Google Cloud based on the permissions your account has. For now, we'll just focus on the log functionality within Google Cloud as it relates to Google Workspace; however, you could perform any Google Cloud actions you are authorized to do from this point.

When it comes to logging in Google Cloud it is first best to understand what Logging Buckets you have access to. Logging Buckets are where Google Cloud stores all logs unless you specifically tell it to store them somewhere else. Logging Buckets are sized based on number of days—they are not based on data quantity.

You will likely always see "_Required" and "_Default"—these are set up as part of every Project within Google Cloud. Any Logging Buckets you see in additional to those are Logging Buckets added by a user account. When reviewing the Logging Buckets available, it's important to note the "retention_days" as we'll need this later to collect all the logs from a Logging Bucket.



As mentioned previously in this section, there are only specific Google Workspace log sources that are sent over to Google Cloud, so we can narrow our search to only them:

```
'protoPayload.serviceName= ("admin.googleapis.com" OR
"cloudidentity.googleapis.com" OR "login.googleapis.com" OR
"oauth2.googleapis.com")
```

To extract all the logs from Google Cloud, or logs from a specific timeframe, we have to tell gcloud exactly the time range we want:

```
timestamp<="2022-02-28T00:00:00Z" AND timestamp>="2022-01-01T00:00:00Z"
```

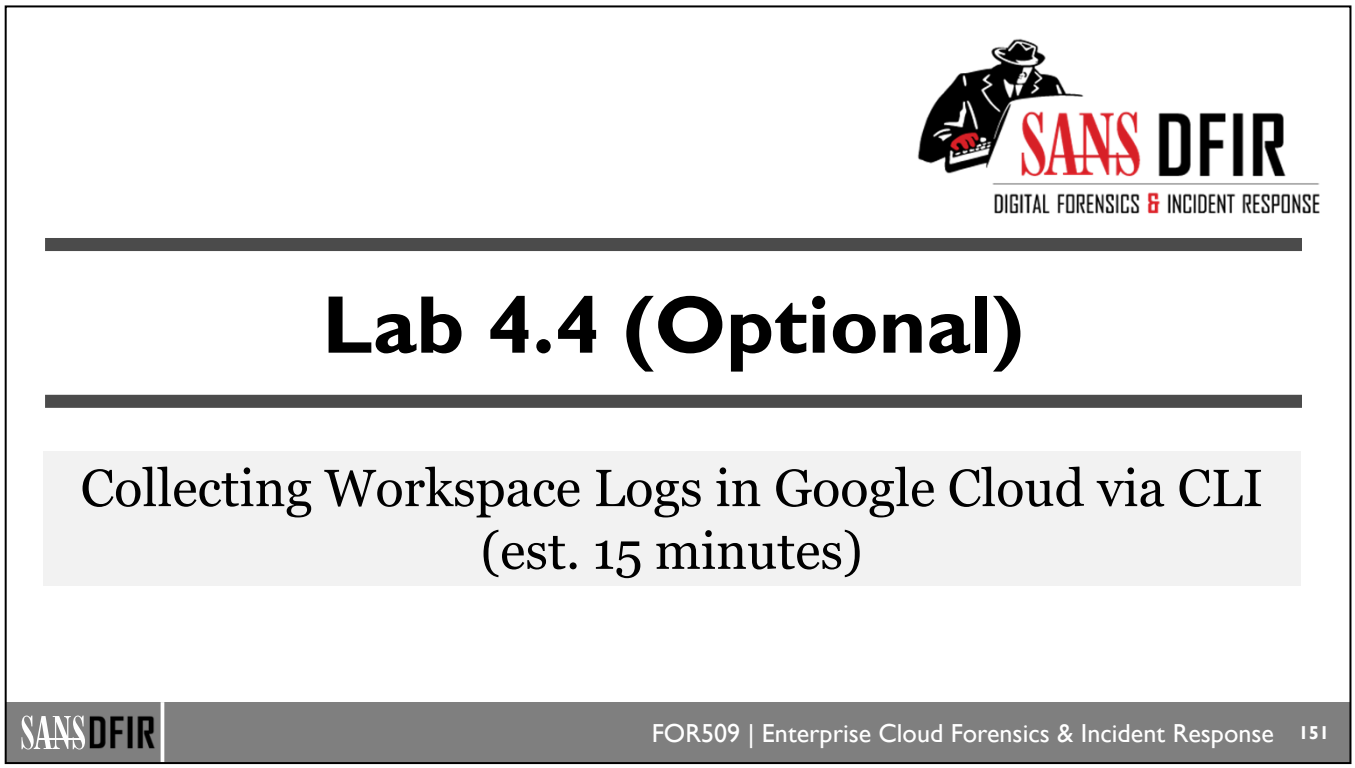
Additionally, we also need to ensure that gcloud will output the logs in a JSON format so we can consume them directly into SOF_ELK, with:

```
--format="json"
```

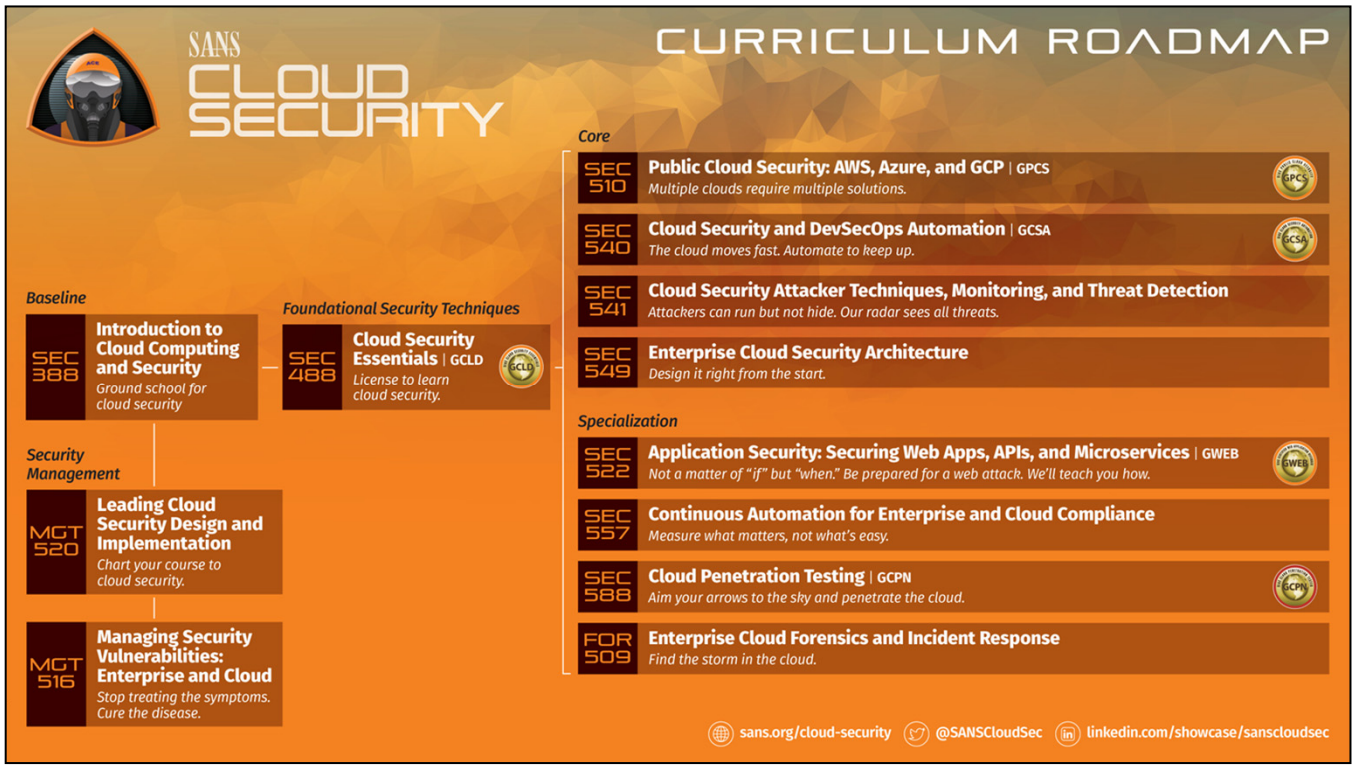
We can then use all these parameters together and have gcloud pull all logs from any Logging Bucket that match our Google Workspace logs and the timeframe we're after, with:

```
gcloud logging read 'protoPayload.serviceName= ("admin.googleapis.com" OR
"cloudidentity.googleapis.com" OR "login.googleapis.com" OR
"oauth2.googleapis.com") AND timestamp<="2022-02-28T00:00:00Z" AND
timestamp>="2022-01-01T00:00:00Z"' --format="json" > gws_logs_in_gcp.json
```

Ensure you always include the time range, as gcloud will default to only giving you 10 log lines if you don't include a time range.



This page intentionally left blank.



The SANS Institute, established in 1989 as a cooperative research and education organization, is the most trusted and by far the largest source for information security training and security certification in the world. It also develops, maintains, and makes available at no cost the largest collection of research documents about various aspects of information security, and it operates the internet's early warning system—the Internet Storm Center. Its programs now reach more than 165,000 security professionals around the world.

SANS offers a number of courses that teach developers, architects, testers, security professionals, and managers how to build more secure applications. Anyone involved in developing, securing, and defending applications can benefit from the following courses in the SANS Cloud Security Curriculum:

SEC388: Introduction to Cloud Computing and Security | 3 Sections

Advise and speak about a wide range of cloud security topics and help your organization successfully navigate both the security challenges as well as the opportunities presented by cloud services.

SEC488: Cloud Security Essentials | GCLD | 6 Sections

Advise and speak about a wide range of cloud security topics and help your organization successfully navigate both the security challenges as well as the opportunities presented by cloud services.

SEC510: Public Cloud Security: AWS, Azure, and GCP | GPCS | 5 Sections + Extended Lab Hours

Perform multicloud security assessments across AWS, Azure, and GCP clouds identifying key weaknesses and hardened configurations in core cloud services.

SEC540: Cloud Security & DevSecOps Automation | GCSA | 5 Sections + Extended Lab Hours

Provides development, operations, and security professionals with a methodology to build and deliver secure infrastructure and software using cloud services and DevSecOps workflows.

SEC541: Cloud Security, Attacker Techniques, Monitoring, and Threat Detection | 5 Sections

Leverage cloud security tools and services to monitor your environment and look for adversaries.

SEC549: Enterprise Cloud Security Architecture | 2 Sections

Ensure you have the necessary foundation, tools, and skills to utilize cloud services in architectural design and can use them in a real-world example.

SEC522: Application Security: Securing Web Apps, APIs, and Microservices | GWEB | 6 Sections

For anyone who wants to get up to speed on web application security issues and the best ways to prevent common web application vulnerabilities.

SEC557: Continuous Automation for Enterprise and Cloud Compliance | 5 Sections

Teaching professionals tasked with ensuring security and compliance how to stop being a roadblock and work at the speed of the modern enterprise.

SEC588: Cloud Penetration Testing | GCPN | 6 Sections

Prepares penetration testers to assess infrastructure and applications hosted in the public using platforms such as AWS, Azure, and Kubernetes.

FOR509: Enterprise Cloud Forensics and Incident Response | 4 Sections

Designed to address today's need to bring examiners up to speed with the rapidly changing world of enterprise cloud environments.

MGT520: Leading Cloud Security Design & Implementation | 3 Sections

Learn to build your cloud security program and roadmap.

MGT516: Managing Security Vulnerabilities: Enterprise and Cloud | 5 Sections

Highlights why organizations struggle with enterprise and cloud vulnerability management and shows how to solve these challenges.

Review our Job Role Flight Plan at **sans.org/cloud-security.**

Course Resources and Contact Information

Here is my lens. You know my methods. —Sherlock Holmes

SLIDE AUTHOR CONTACT
Josh Lemon
josh@joshlemon.com.au
Twitter: @joshlemon

SANS INSTITUTE
11200 Rockville Pike, Suite 200
North Bethesda, MD 20852
301.654.SANS(7267)

LAB AUTHOR CONTACT
Megan Roddie
megansroddie@gmail.com
Twitter: @megan_roddie

SANS EMAIL
GENERAL INQUIRIES: info@sans.org
REGISTRATION: registration@sans.org
TUITION: tuition@sans.org
PRESS/PR: press@sans.org

Slide Author: Josh Lemon
Email: josh@joshlemon.com.au
Twitter: @joshlemon

Lab Author: Megan Roddie
Email: megansroddie@gmail.com
Twitter: @megan_roddie