INVICTUS
INCIDENT RESPONSE

Detecting malicious actors in **Google Workspace**

Korstiaan Stam, Founder
korstiaan@invictus-ir.com

Did you know?

Google Workspace is not the same as Google Cloud

INVICTUS
INCIDENT RESPONSE

Did you know?

Google Workspace is a suite of productivity tools like Microsoft 365 and had over 6 million users in 2020

INVICTUS
INCIDENT RESPONSE

Did you know?

Google Workspace has almost 50 out of the box security rules that can trigger alerts?

INVICTUS
INCIDENT RESPONSE

Did you know?

Most of the security alerts do **not** generate an alert?
e.g. Changing email route settings or granting a user admin privilege

INVICTUS
INCIDENT RESPONSE

Did you know?

That you cannot disable audit logging in Google Workspace

INVICTUS
INCIDENT RESPONSE

About

Korstiaan Stam

- **PwC**
- **Northwave**
- **University of Applied Sciences Amsterdam**
- **Invictus Incident Response**
- **SANS**
- **Education**
  - MSc. Digital Investigation & Forensic Computing
  - BSc. Information Technology

INVICTUS INCIDENT RESPONSE

Background
Security research

- Did a lot of work on Office/Microsoft 365 incidents resulting in several open-source projects
- (Microsoft365-Extractor-Suite, Blue team app for Office 365 and Azure and the BEC Guide)
- Nothing on Google Workspace yet
- Original goal, acquire all logs for forensic analysis
- This idea led to additional research together with students to see if we can go a step further
- Analyst time is valuable, see if we can bring it down

https://twitter.com/BertJanCyber

https://www.linkedin.com/in/charitonos/

Google Workspace

INVICTUS
INCIDENT RESPONSE

Google Workspace

Introduction

Google Workspace is the name of the commercial offering of the Google productivity software suite

Google Workspace
Audit logs

Audit logs records the following log types:

- Admin
- Group
- Login
- OAuth
- SAML
- Service specific events (Drive, Meet, Chrome, Calendar and more)

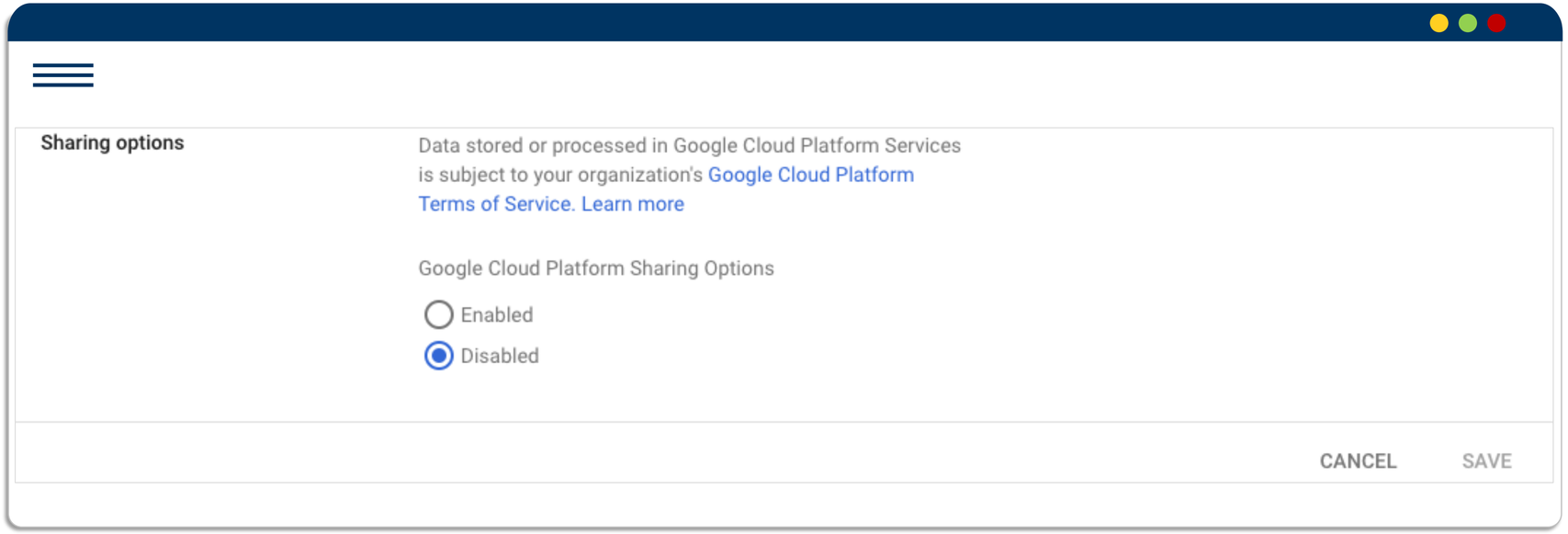
Retention

6 months in Google Workspace and up to 400 days in Google Cloud

Google Workspace
Audit logs

There is a few ways to look at the Audit logs

- Google Workspace Admin Center

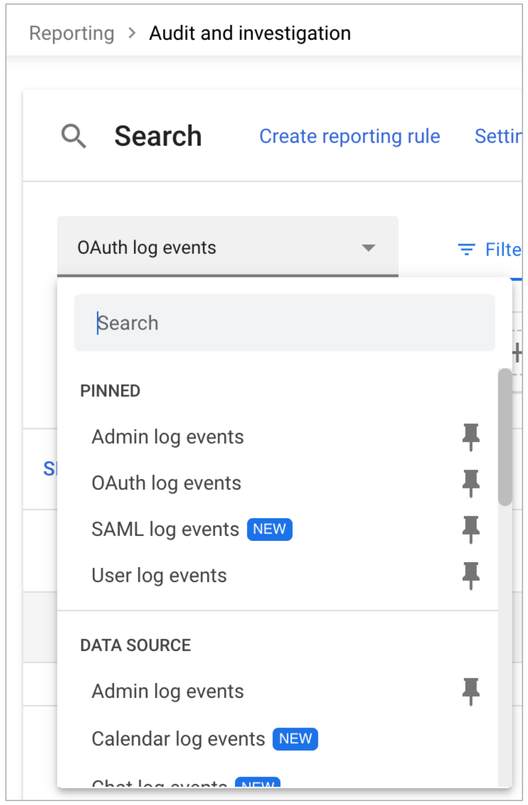


You can also enable sharing between GWS and GCP, which allows you to analyze the logs in GCP as well.

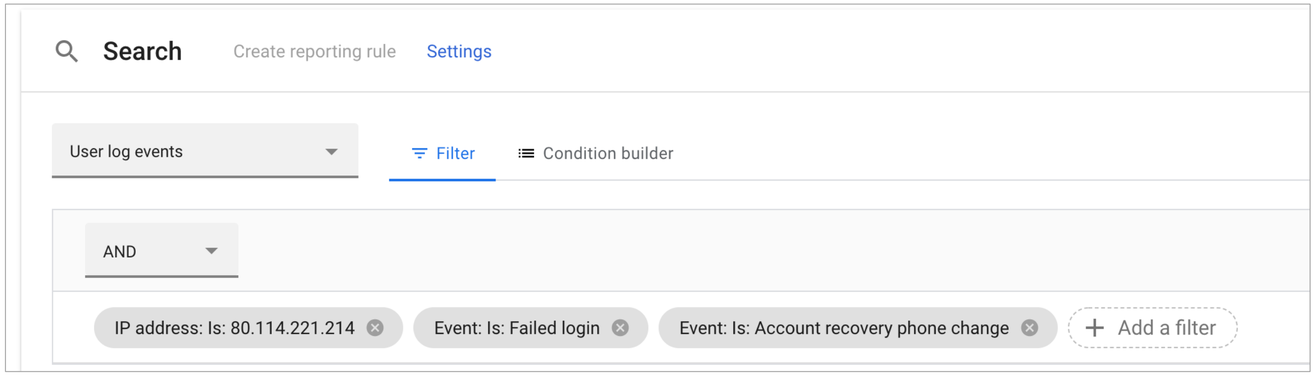
Google Workspace
Audit logs

Using the admin center on admin.google.com navigate ‘Reporting’ -> ‘Audit and Investigation’

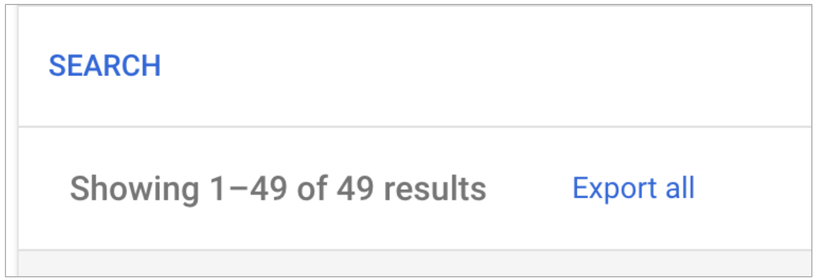
1. Filter on log types



2. Advanced Filtering

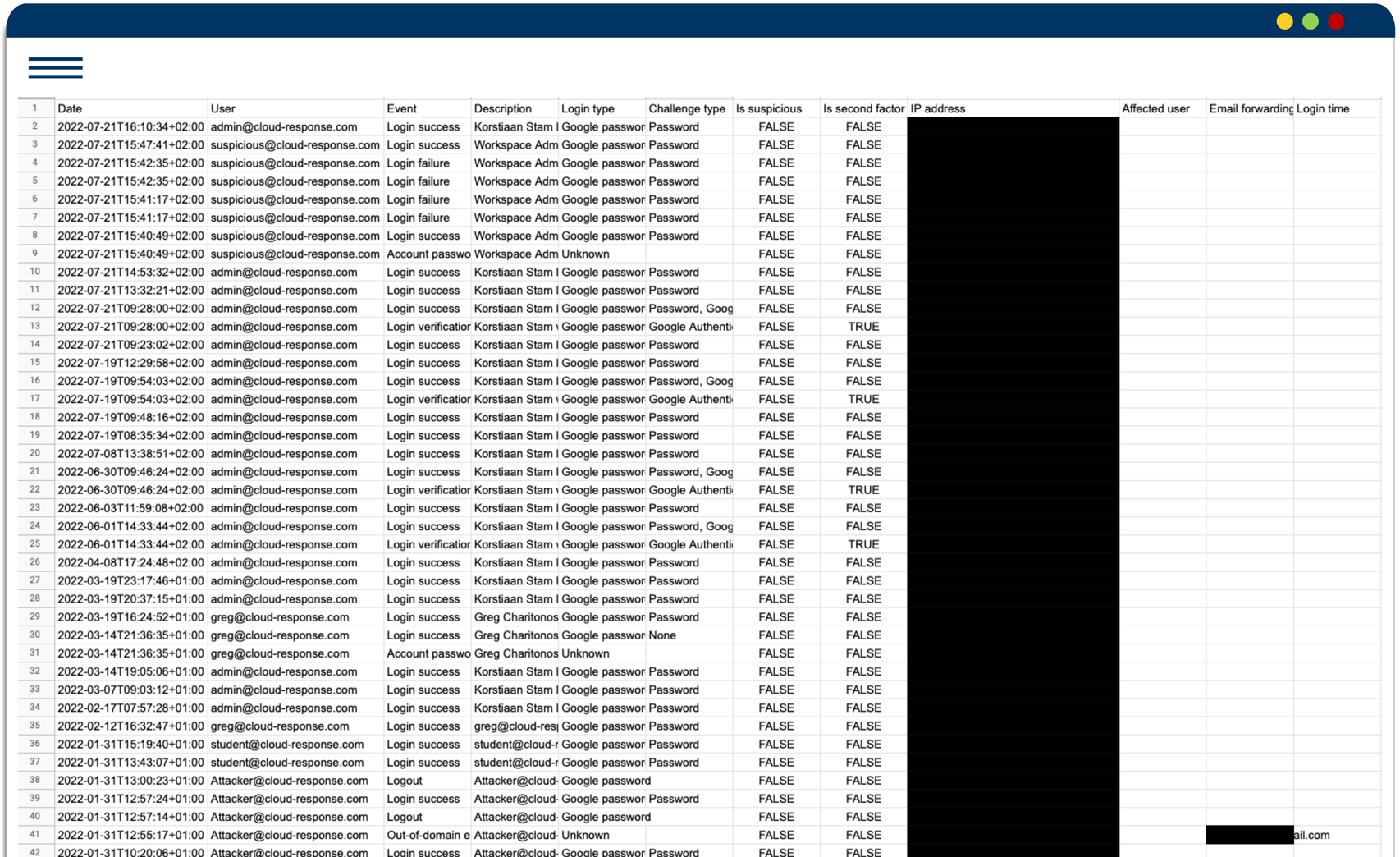


3. Export events (Google Sheets/CSV)



Google Workspace

Audit logs



	Date	User	Event	Description	Login type	Challenge type	Is suspicious	Is second factor	IP address	Affected user	Email forwarding	Login time
2	2022-07-21T16:10:34+02:00	admin@cloud-response.com	Login success	Korstiaan Stam l	Google passwor	Password	FALSE	FALSE	[redacted]			
3	2022-07-21T15:47:41+02:00	suspicious@cloud-response.com	Login success	Workspace Adm	Google passwor	Password	FALSE	FALSE				
4	2022-07-21T15:42:35+02:00	suspicious@cloud-response.com	Login failure	Workspace Adm	Google passwor	Password	FALSE	FALSE				
5	2022-07-21T15:42:35+02:00	suspicious@cloud-response.com	Login failure	Workspace Adm	Google passwor	Password	FALSE	FALSE				
6	2022-07-21T15:41:17+02:00	suspicious@cloud-response.com	Login failure	Workspace Adm	Google passwor	Password	FALSE	FALSE				
7	2022-07-21T15:41:17+02:00	suspicious@cloud-response.com	Login failure	Workspace Adm	Google passwor	Password	FALSE	FALSE				
8	2022-07-21T15:40:49+02:00	suspicious@cloud-response.com	Login success	Workspace Adm	Google passwor	Password	FALSE	FALSE				
9	2022-07-21T15:40:49+02:00	suspicious@cloud-response.com	Account passwo	Workspace Adm	Unknown		FALSE	FALSE				
10	2022-07-21T14:53:32+02:00	admin@cloud-response.com	Login success	Korstiaan Stam l	Google passwor	Password	FALSE	FALSE				
11	2022-07-21T13:32:21+02:00	admin@cloud-response.com	Login success	Korstiaan Stam l	Google passwor	Password	FALSE	FALSE				
12	2022-07-21T09:28:00+02:00	admin@cloud-response.com	Login success	Korstiaan Stam l	Google passwor	Password, Goog	FALSE	FALSE				
13	2022-07-21T09:28:00+02:00	admin@cloud-response.com	Login verificatior	Korstiaan Stam \	Google passwor	Google Authenti	FALSE	TRUE				
14	2022-07-21T09:23:02+02:00	admin@cloud-response.com	Login success	Korstiaan Stam l	Google passwor	Password	FALSE	FALSE				
15	2022-07-19T12:29:58+02:00	admin@cloud-response.com	Login success	Korstiaan Stam l	Google passwor	Password	FALSE	FALSE				
16	2022-07-19T09:54:03+02:00	admin@cloud-response.com	Login success	Korstiaan Stam l	Google passwor	Password, Goog	FALSE	FALSE				
17	2022-07-19T09:54:03+02:00	admin@cloud-response.com	Login verificatior	Korstiaan Stam \	Google passwor	Google Authenti	FALSE	TRUE				
18	2022-07-19T09:48:16+02:00	admin@cloud-response.com	Login success	Korstiaan Stam l	Google passwor	Password	FALSE	FALSE				
19	2022-07-19T08:35:34+02:00	admin@cloud-response.com	Login success	Korstiaan Stam l	Google passwor	Password	FALSE	FALSE				
20	2022-07-08T13:38:51+02:00	admin@cloud-response.com	Login success	Korstiaan Stam l	Google passwor	Password	FALSE	FALSE				
21	2022-06-30T09:46:24+02:00	admin@cloud-response.com	Login success	Korstiaan Stam l	Google passwor	Password, Goog	FALSE	FALSE				
22	2022-06-30T09:46:24+02:00	admin@cloud-response.com	Login verificatior	Korstiaan Stam \	Google passwor	Google Authenti	FALSE	TRUE				
23	2022-06-03T11:59:08+02:00	admin@cloud-response.com	Login success	Korstiaan Stam l	Google passwor	Password	FALSE	FALSE				
24	2022-06-01T14:33:44+02:00	admin@cloud-response.com	Login success	Korstiaan Stam l	Google passwor	Password, Goog	FALSE	FALSE				
25	2022-06-01T14:33:44+02:00	admin@cloud-response.com	Login verificatior	Korstiaan Stam \	Google passwor	Google Authenti	FALSE	TRUE				
26	2022-04-08T17:24:48+02:00	admin@cloud-response.com	Login success	Korstiaan Stam l	Google passwor	Password	FALSE	FALSE				
27	2022-03-19T23:17:46+01:00	admin@cloud-response.com	Login success	Korstiaan Stam l	Google passwor	Password	FALSE	FALSE				
28	2022-03-19T20:37:15+01:00	admin@cloud-response.com	Login success	Korstiaan Stam l	Google passwor	Password	FALSE	FALSE				
29	2022-03-19T16:24:52+01:00	greg@cloud-response.com	Login success	Greg Charitonos	Google passwor	Password	FALSE	FALSE				
30	2022-03-14T21:36:35+01:00	greg@cloud-response.com	Login success	Greg Charitonos	Google passwor	None	FALSE	FALSE				
31	2022-03-14T21:36:35+01:00	greg@cloud-response.com	Account passwo	Greg Charitonos	Unknown		FALSE	FALSE				
32	2022-03-14T19:05:06+01:00	admin@cloud-response.com	Login success	Korstiaan Stam l	Google passwor	Password	FALSE	FALSE				
33	2022-03-07T09:03:12+01:00	admin@cloud-response.com	Login success	Korstiaan Stam l	Google passwor	Password	FALSE	FALSE				
34	2022-02-17T07:57:28+01:00	admin@cloud-response.com	Login success	Korstiaan Stam l	Google passwor	Password	FALSE	FALSE				
35	2022-02-12T16:32:47+01:00	greg@cloud-response.com	Login success	greg@cloud-res	Google passwor	Password	FALSE	FALSE				
36	2022-01-31T15:19:40+01:00	student@cloud-response.com	Login success	student@cloud-r	Google passwor	Password	FALSE	FALSE				
37	2022-01-31T13:43:07+01:00	student@cloud-response.com	Login success	student@cloud-r	Google passwor	Password	FALSE	FALSE				
38	2022-01-31T13:00:23+01:00	Attacker@cloud-response.com	Logout	Attacker@cloud-	Google password		FALSE	FALSE				
39	2022-01-31T12:57:24+01:00	Attacker@cloud-response.com	Login success	Attacker@cloud-	Google passwor	Password	FALSE	FALSE				
40	2022-01-31T12:57:14+01:00	Attacker@cloud-response.com	Logout	Attacker@cloud-	Google password		FALSE	FALSE				
41	2022-01-31T12:55:17+01:00	Attacker@cloud-response.com	Out-of-domain e	Attacker@cloud-	Unknown		FALSE	FALSE			[redacted]ail.com	
42	2022-01-31T10:20:06+01:00	Attacker@cloud-response.com	Login success	Attacker@cloud-	Google passwor	Password	FALSE	FALSE				

ALFA

INVICTUS
INCIDENT RESPONSE

Automated Audit Log Forensic Analysis for Google Workspace

ALFA..

- Is an open-source tool (https://github.com/invictus-ir/ALFA)
- Acquires all Google Workspace audit logs
- Leverages the MITRE ATT&CK Cloud Framework to classify events
- Identifies ‘interesting’ activity based on the mapping
- Identifies kill chains based on Google Workspace audit logs
- Is able to export identified kill chains to separate files for quicker analysis
- Uses super complex algorithms to perform this magic ;)

Prerequisites
Acquisition

ALFA uses the Reports API* to get information on:

- Activity, service based (e.g. Drive events or Admin events)
- Usage, user based (e.g. all events for a certain user)

ALFA leverages the Activity API for log acquisition

Google Workspace

- The default Super Administrator role or;
- A custom administrator role with the ‘Reports administrator’

Google Cloud

- (Optional) Create a Google API Console project**
- Enable the Admin SDK API
- Register an OAuth application

*API Reference: https://developers.google.com/admin-sdk/reports/v1/get-start/overview
** Prerequisites: https://developers.google.com/admin-sdk/reports/v1/guides/prerequisites

Setup
Ready to go

- We can now interact with the API, however we want to programatically retrieve data
- We will use an OAuth application to authorize and connect to the API to retrieve the logs

- Instructions on how to do this are available on our **GitHub** and **YouTube**
- In the end you'll end up with a .json file with credentials for the OAuth application which is required for the next phase.

ALFA
Using ALFA

ALFA has three modes

1. `ALFA acquire, acquire logs`
2. `ALFA analyze, analyze acquired logs`
3. `ALFA load, analyze previously acquired logs`

Before we can use the tool we need to install and initialize it.

- Run `pip install -e .`
- Run `alfa init` **`project_name`**
- Copy the `credentials.json` containing your OAuth credentials to the **project_name/config** directory

ALFA
Acquire

Acquire available logging from a Google Workspace:

All logging

```
$ alfa acquire
```

Specific log types

```
$ alfa acquire --logtype=admin
```

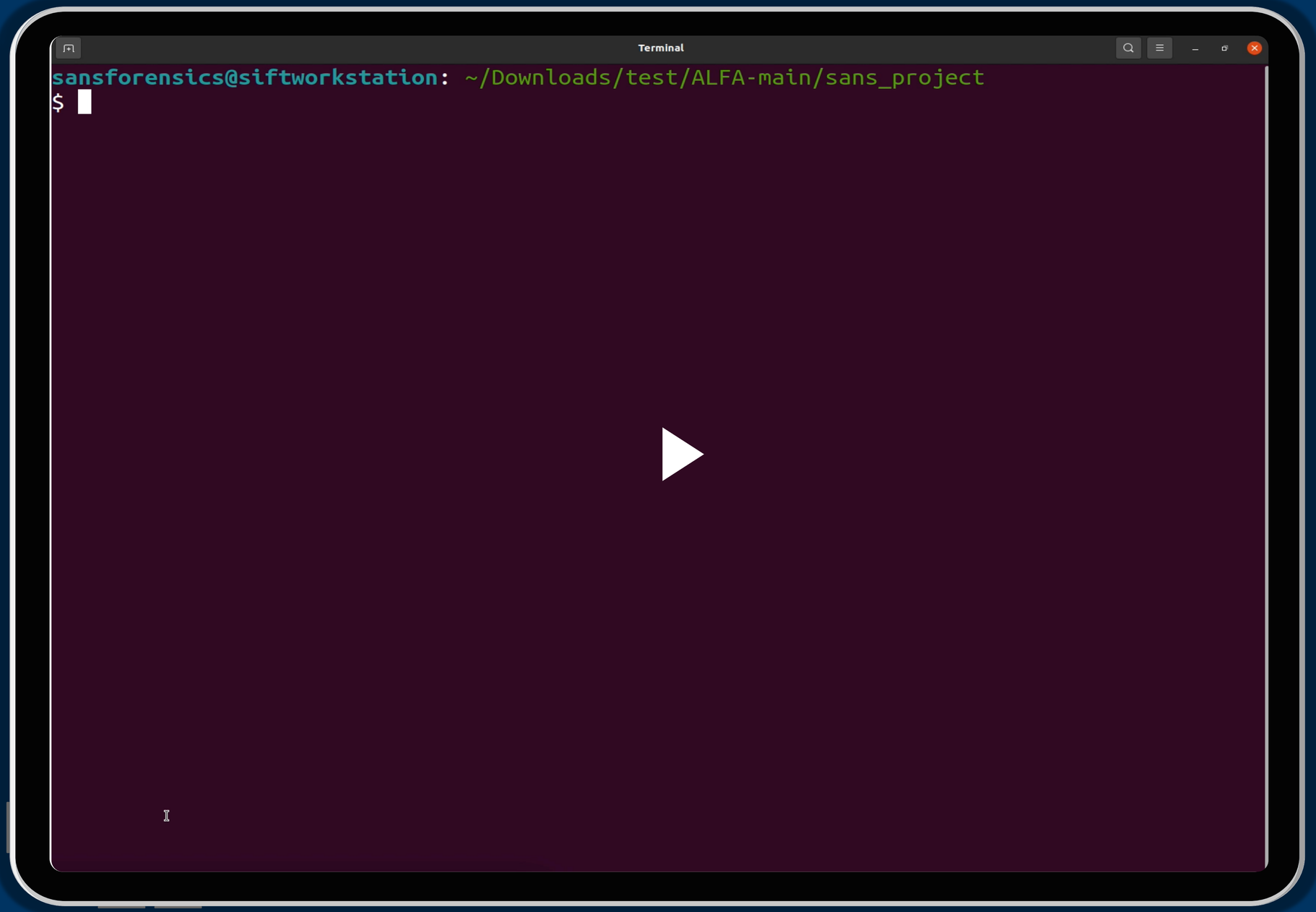
Specific users

```
$ alfa acquire --user=insert_username
```

Specific timeframe

```
$ alfa acquire --start-time=2022-07-10T10:00:00Z --end-time=2022-07-11T14:26:01Z
```

This is what it looks like



ALFA
Acquire

```
sansforensics@siftworkstation: ~/Downloads/ALFA/ALFA-main/sans_demo
$ ls
config  data
sansforensics@siftworkstation: ~/Downloads/ALFA/ALFA-main/sans_demo
$ cd data/
sansforensics@siftworkstation: ~/Downloads/ALFA/ALFA-main/sans_demo/data
$ ls
220719.081628
sansforensics@siftworkstation: ~/Downloads/ALFA/ALFA-main/sans_demo/data
$ cd 220719.081628/
sansforensics@siftworkstation: ~/Downloads/ALFA/ALFA-main/sans_demo/data/220719.081628
$ ls -al
total 1836
drwxrwxr-x 2 sansforensics sansforensics    4096 Jul 19 08:16 .
drwxrwxr-x 3 sansforensics sansforensics    4096 Jul 19 08:16 ..
-rw-rw-r-- 1 sansforensics sansforensics      18 Jul 19 08:16 access_transparency.json
-rw-rw-r-- 1 sansforensics sansforensics   32727 Jul 19 08:16 admin.json
-rw-rw-r-- 1 sansforensics sansforensics 1162914 Jul 19 08:16 calendar.json
-rw-rw-r-- 1 sansforensics sansforensics      18 Jul 19 08:16 chat.json
-rw-rw-r-- 1 sansforensics sansforensics      18 Jul 19 08:16 chrome.json
-rw-rw-r-- 1 sansforensics sansforensics      18 Jul 19 08:16 context_aware_access.json
-rw-rw-r-- 1 sansforensics sansforensics      18 Jul 19 08:16 data_studio.json
-rw-rw-r-- 1 sansforensics sansforensics    7562 Jul 19 08:16 drive.json
-rw-rw-r-- 1 sansforensics sansforensics      18 Jul 19 08:16 gcp.json
-rw-rw-r-- 1 sansforensics sansforensics      18 Jul 19 08:16 gplus.json
-rw-rw-r-- 1 sansforensics sansforensics      18 Jul 19 08:16 groups_enterprise.json
-rw-rw-r-- 1 sansforensics sansforensics      18 Jul 19 08:16 groups.json
-rw-rw-r-- 1 sansforensics sansforensics      18 Jul 19 08:16 jamboard.json
-rw-rw-r-- 1 sansforensics sansforensics      18 Jul 19 08:16 keep.json
-rw-rw-r-- 1 sansforensics sansforensics   30087 Jul 19 08:16 login.json
-rw-rw-r-- 1 sansforensics sansforensics  473637 Jul 19 08:16 meet.json
-rw-rw-r-- 1 sansforensics sansforensics      18 Jul 19 08:16 mobile.json
-rw-rw-r-- 1 sansforensics sansforensics      18 Jul 19 08:16 rules.json
-rw-rw-r-- 1 sansforensics sansforensics      18 Jul 19 08:16 saml.json
-rw-rw-r-- 1 sansforensics sansforensics   95676 Jul 19 08:16 token.json
-rw-rw-r-- 1 sansforensics sansforensics      18 Jul 19 08:16 user_accounts.json
```

- ALFA generates a data folder
- Folder name is date/time of acquisition
- Folder contains output stored in .json files

ALFA
Analyze

ALFA analyze leverages the MITRE ATT&CK Cloud Framework to map events

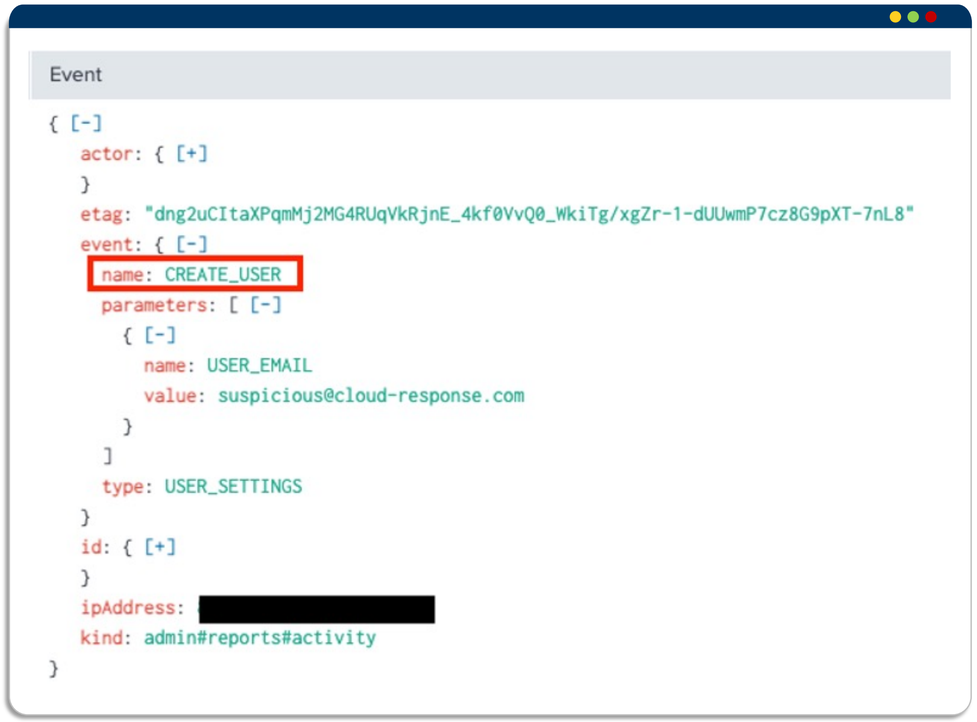
https://attack.mitre.org/matrices/enterprise/cloud/googleworkspace/

ALFA
Analyze

ALFA analyze leverages the MITRE ATT&CK Cloud Framework to map events

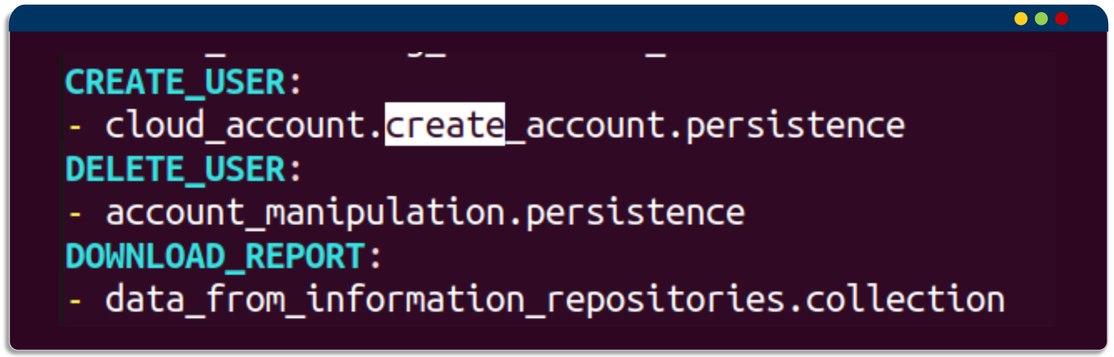
Step 1

Original event



Step 2

Event is mapped to MITRE



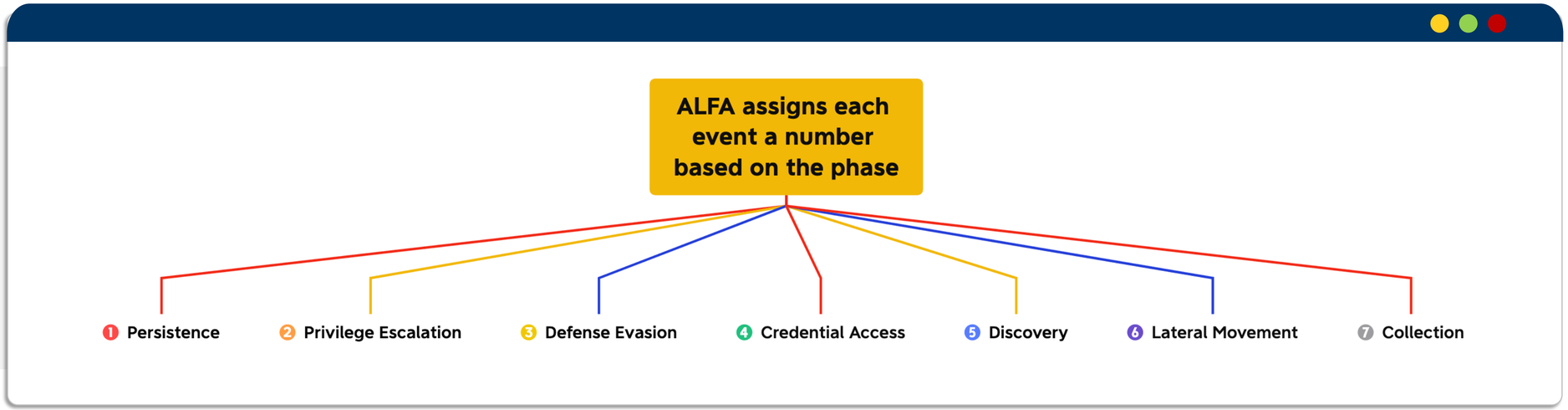
(sub-technique)-(technique)-(phase)

https://attack.mitre.org/techniques/T1136/003/

ALFA
Analyze

Step 3

Each event is assigned a value based on the associated MITRE phase



Step 4

To identify chains, ALFA compares value of the event with the previous event and increases the value with 1 if it follows the kill chain. Or decreases with 1 if the kill chain is not followed

Step 5

Next the kill chain statistic is calculated, by dividing the sum of events with the number of events.

Step 6

The resulting value is a number between -1 and 1. Where -1 is a (reverse kill chain) 0 (random events) 1 (perfect kill chain)

E.G., a kill chain statistic of 0.8 means that a number of events are closely aligned with the direction of a kill chain.

ALFA

Analyze

Step 7

A sub chain is created for events with a kill chain statistic of > 0.60 (can be changed)

Step 8

The events within the identified subchains can stored to separate .json files for further analysis.

Important

Interesting events ≠ malicious events

ALFA
Analyze

Acquire and analyze available logs this drops you in a shell for interactive commands

```
$ alfa analyze
```

Calculate kill chain statistic over the whole dataset

```
$ A.kcs()
```

Show available subchains

```
$ A.subchains()
```

Get a summary of interesting events

```
$ summary(A.events[0:10])
```

Export all subchains to separate file for further analysis

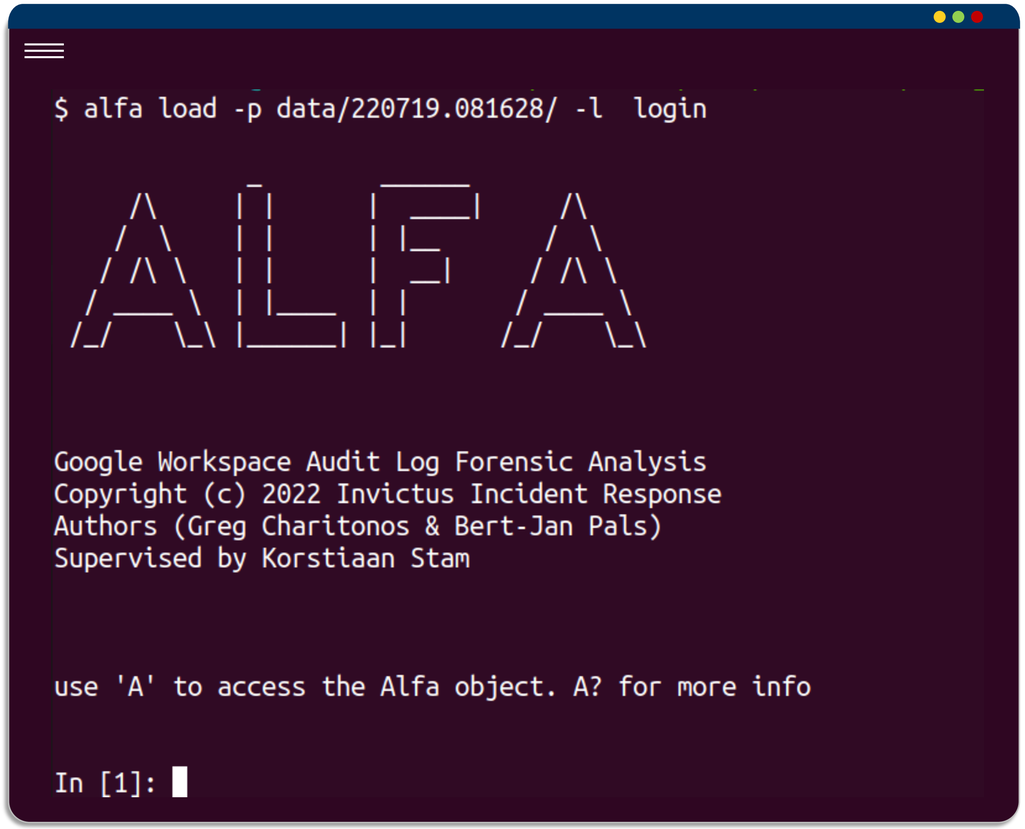
```
$ A.aoi(export='activities.json’)
```

ALFA
Analyze

```
In [7]: A.subchains()
Out[7]: [[9389, 9399, 0.9], [75, 85, 0.65], [35, 45, 0.6499999999999999]]


In [8]: summary(A.events[9389:9399])
      name                          activity_time                       activity_id
----  ----------------------------  ----------------------------------  -------------------
9389  change_user_access            2022-07-27 08:23:18.846000+00:00  -6413985416944962783
9390  change_acl_editors            2022-07-27 08:23:18.846000+00:00  -6413985416944962783
9391  edit                          2022-07-27 08:23:18.846000+00:00  -6413985416944962783
9392  add_to_folder                 2022-07-27 08:23:18.846000+00:00  -6413985416944962783
9393  create                        2022-07-27 08:23:18.846000+00:00  -6413985416944962783
9394  create                        2022-07-27 09:30:07.836000+00:00   3665549089345089280
9395  change_user_access            2022-07-27 09:30:07.836000+00:00   3665549089345089280
9396  change_acl_editors            2022-07-27 09:30:07.836000+00:00   3665549089345089280
9397  add_to_folder                 2022-07-27 09:30:07.836000+00:00   3665549089345089280
9398  email_forwarding_out_of_domain 2022-07-27 09:31:13.944000+00:00  -2121597430569433497
```

ALFA
Load



Does the same as ALFA analyze, however you can use previously acquired data

`$ alfa load -p path_to_audit_logs`

Load logins only

- `$ alfa load -p path_to_audit_logs -l login`

Scenarios

INVICTUS
INCIDENT RESPONSE

Scenarios

Show me the money!

Attack 1 - BEC

Business email compromise which leads to data exfiltration and/or follow up attacks.

Attack 2– Malicious app

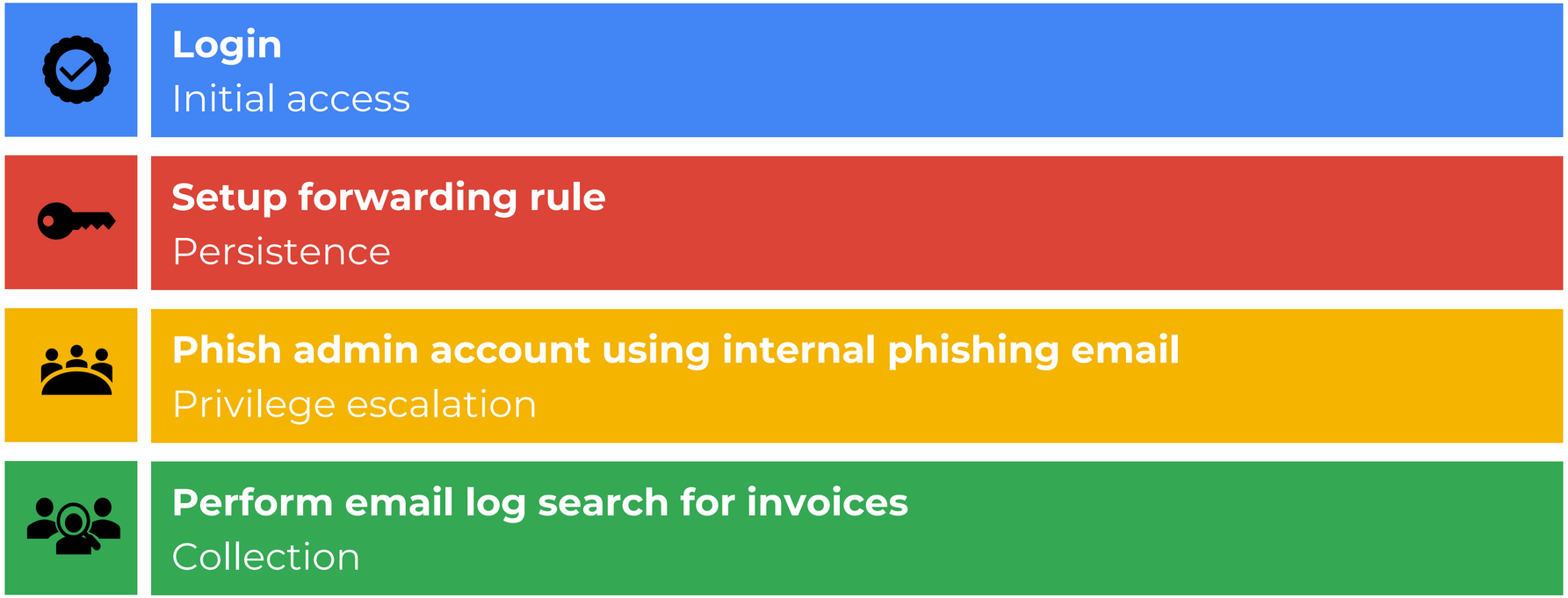
Malicious OAuth app registration which leads to unauthorized access of user data by an application in the background.

Attack 3 – APT style

Perform recon activity and export out users. Download Using the Google Drive data for unauthorized file sharing to external parties.

Attack 1
BEC/Data exfiltration

Attack overview

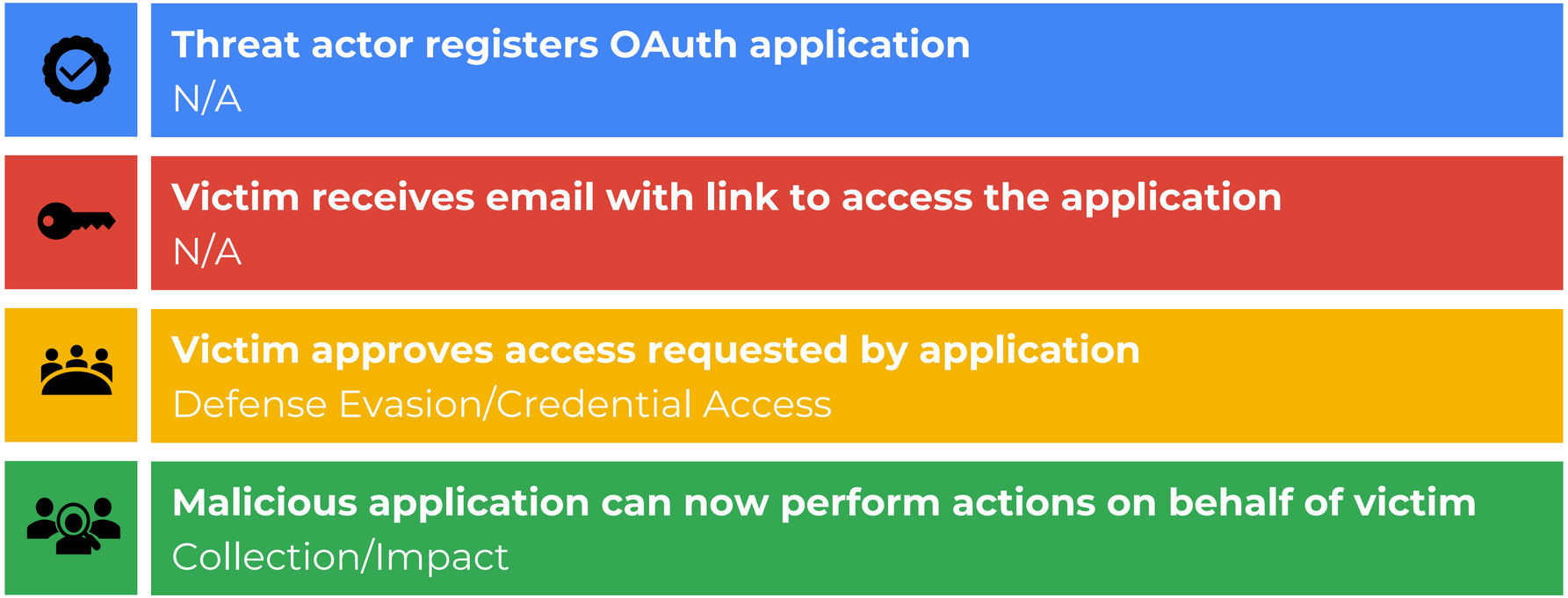


Number of events generated in audit log = **47**

Kill chain statistic = **0.9**

Attack 2
Malicious app

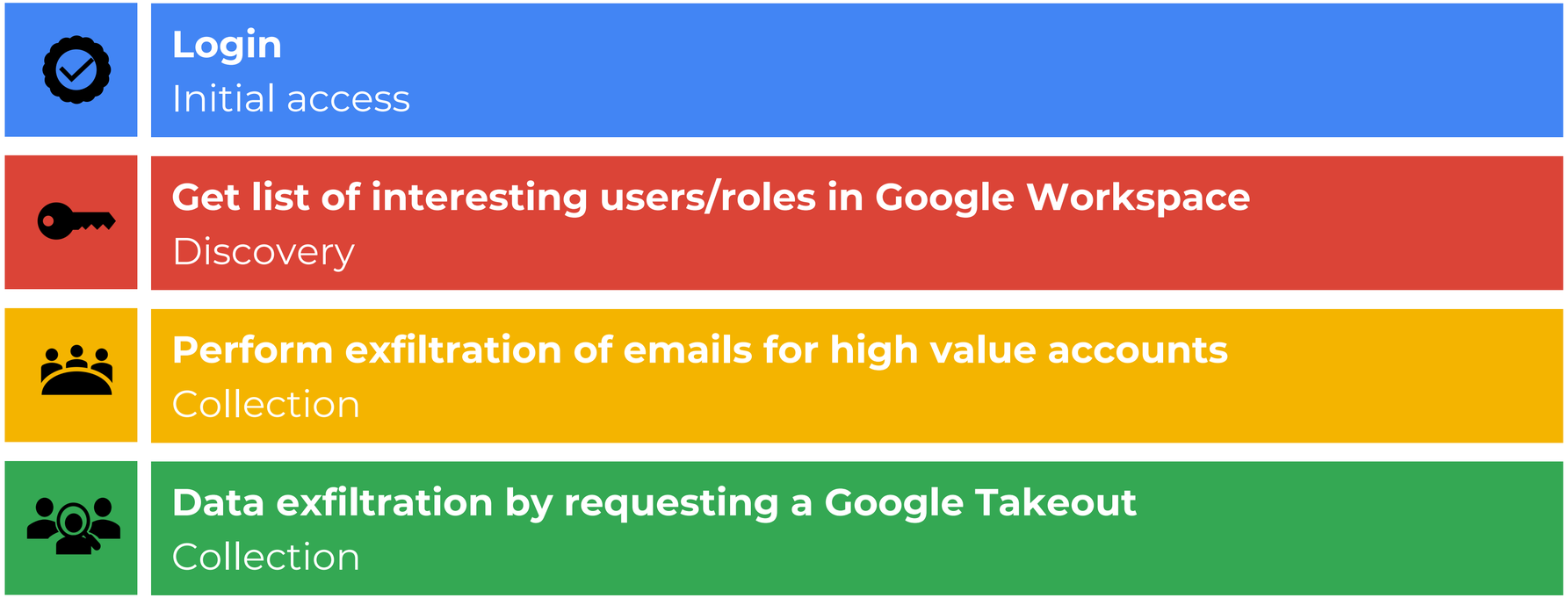
Attack overview



Number of events generated in audit log = **14**
Kill chain statistic = **not identified**

Attack 3
APT style

Attack overview



Number of events generated in audit log = **7**
Kill chain statistic = **0.65**

Conclusion
By the numbers

Overall results

- Good performance in detecting attacks
- Tuning might be required for your environment

Areas of improvement

- Larger datasets and environments
- Test more attacks
- Continuous improvement of event mapping

Most important slide coming up..

INVICTUS
INCIDENT RESPONSE

TLDL

Too Long Didn’t Listen

The most important takeaways

- Google Workspace(GWS) is relevant for DFIR, entry point in many businesses
- GWS audit logging is on by default and is critical for your investigation
- Not a lot of resources available on GWS
- Automated Audit Log Forensic Analysis for Google Workspace (ALFA) is an open-source tool that aids in acquisition and analysis of GWS audit logging
- ALFA attempts to perform automated analysis of GWS audit logging using the MITRE ATT&CK Cloud Framework
- Grab your copy of ALFA now on GitHub https://github.com/invictus-ir/ALFA
- Feedback is very welcome!

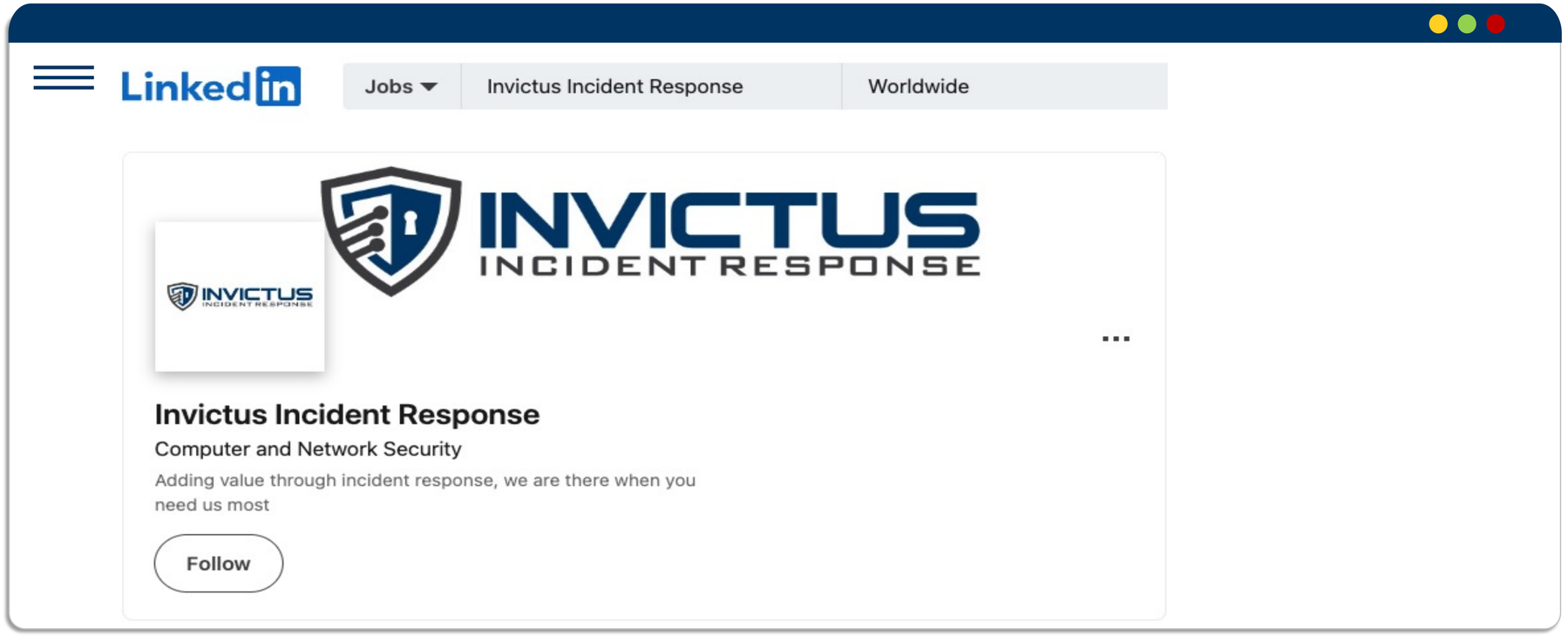
Want to help?

This is your chance

GitHub	https://github.com/invictus-ir/ALFA https://github.com/invictus-ir/gws_dataset
YouTube	https://www.youtube.com/watch?v=UMTP3bt532Q
Medium	https://invictus-ir.medium.com/

The challenge

- I would love to have 1000 followers on LinkedIn this year and I think we can do it today!
- So please follow my company (https://www.linkedin.com/company/invictus-incident-response)



Questions for a T-Shirt!

THANK YOU

INVICTUS
INCIDENT RESPONSE

Korstiaan Stam
Founder, Invictus Incident Response
M: +31 (0)800 - 6010
E: korstiaan@invictus-ir.com
W: invictus-ir.com

Backup slides

INVICTUS
INCIDENT RESPONSE

ALFA
Analyze

Some thoughts and limitations from the analyze function

- Number of events, the chain needs to be at least 5 events long, this can be modified.
- Multiple phase events, some events are part of multiple phases get assigned the highest score, example below will get a score of (3)

```
suspicious_login:
- cloud_accounts.valid_accounts.persistence
- cloud_accounts.valid_accounts.privilege_escalation
- cloud_accounts.valid_accounts.defense_evasion
```

- *Chronological order of events*, output is based on timestamp and the order Google presents it in
- *Mapping of events*, need to keep updated to account for new event types and MITRE ATT&CK updates
- *Slow attacks,* events spread out over multiple days can fall outside of the algorithm