# Automating Google Workspace Incident Response

SANS Technology Institute

The best. Made better.

# Quick Introduction

# Objectives

- To increase IR capabilities in Google Workspace:
  - Provide better view of log data
  - Enrich log data for more context

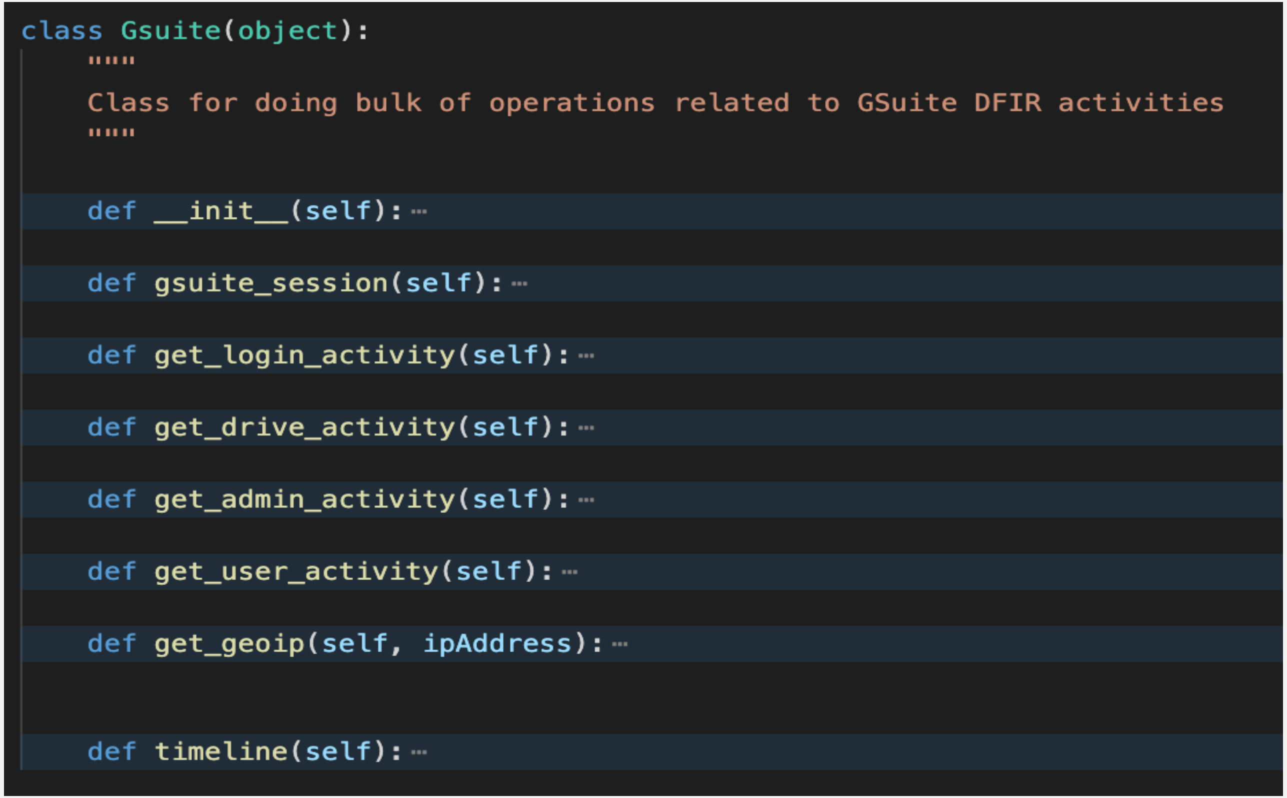
# Problem Statement

- Over 6 million business subscribed to Google Workspace
- No centralized logs, minimal context
- Leads to increased response time during intrusion

# Custom Tool Development

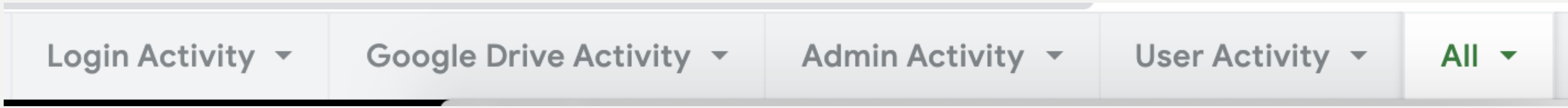
- Custom tool written in Python
    - Leverages Google Admin SDK API to pull logs
    - MaxMind GeoLite2 for geolocation
    - Pandas for data processing

# Custom Tool Structure



```
class Gsuite(object):
    """
    Class for doing bulk of operations related to GSuite DFIR activities
    """

    def __init__(self):⋯

    def gsuite_session(self):⋯

    def get_login_activity(self):⋯

    def get_drive_activity(self):⋯

    def get_admin_activity(self):⋯

    def get_user_activity(self):⋯

    def get_geoip(self, ipAddress):⋯


    def timeline(self):⋯
```

# Output File Structure



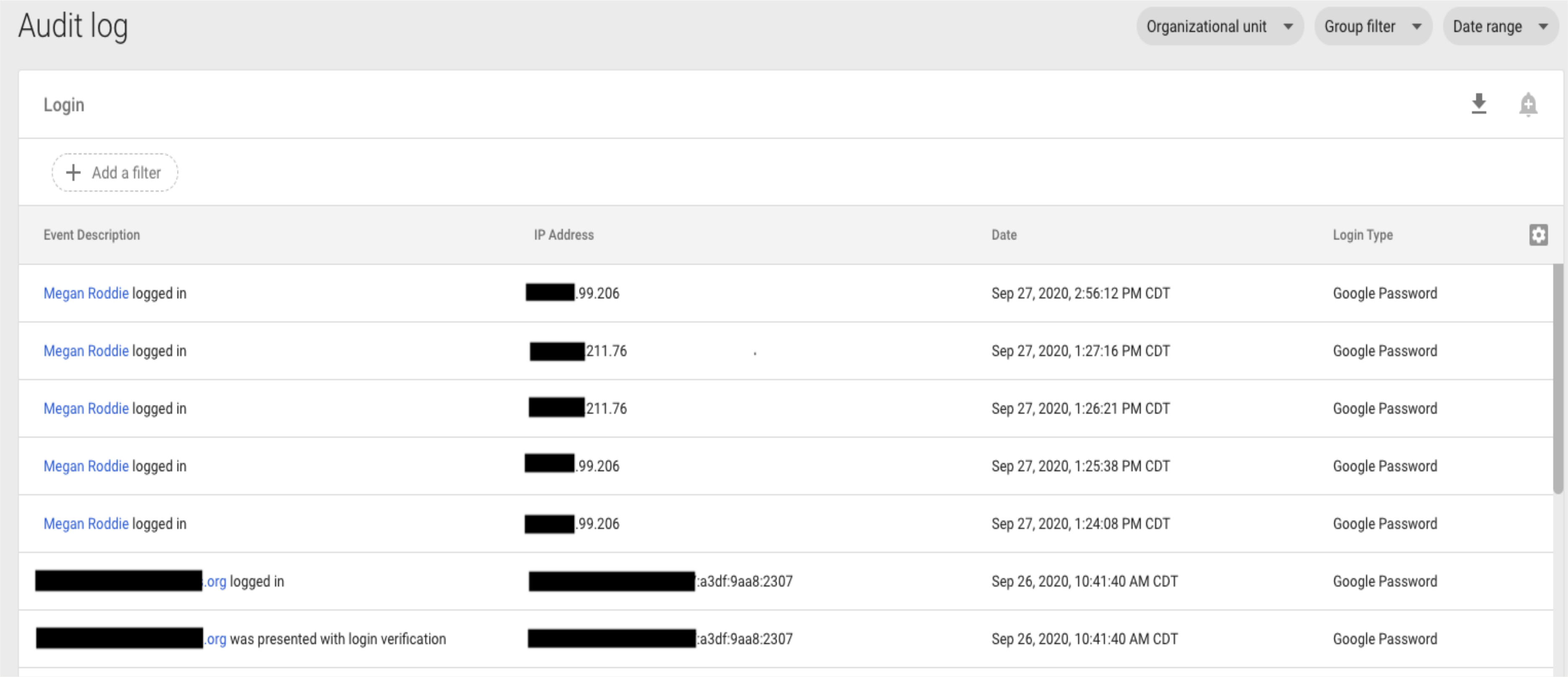
# Research Methodology

- Simulated account takeover in real Google Workspace environment
- Run custom tool after performing simulated activity
- Perform incident response process to compare usefulness of tool output vs. default logging

# Simulating Activity

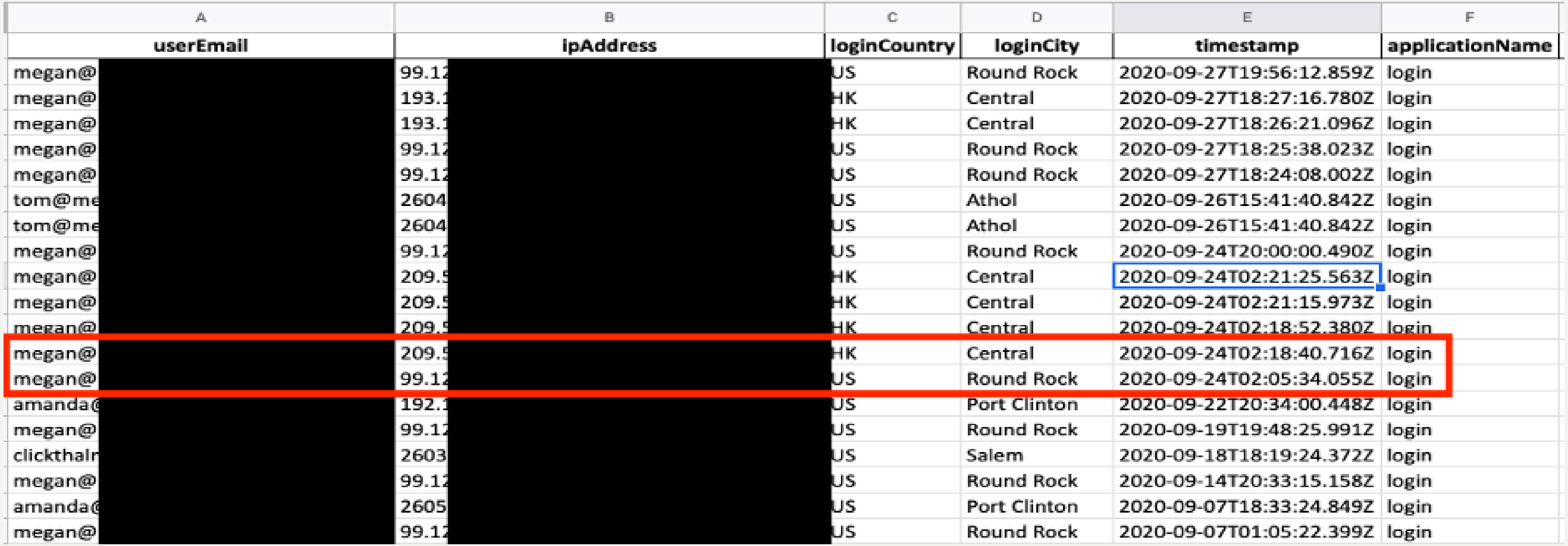
- VPN from Hong Kong
- Login to admin account w/o 2FA
- Perform post-compromise activities
    - Send emails
    - Look at/edit files
    - Change 2FA & recovery settings

# Login Audit Logs



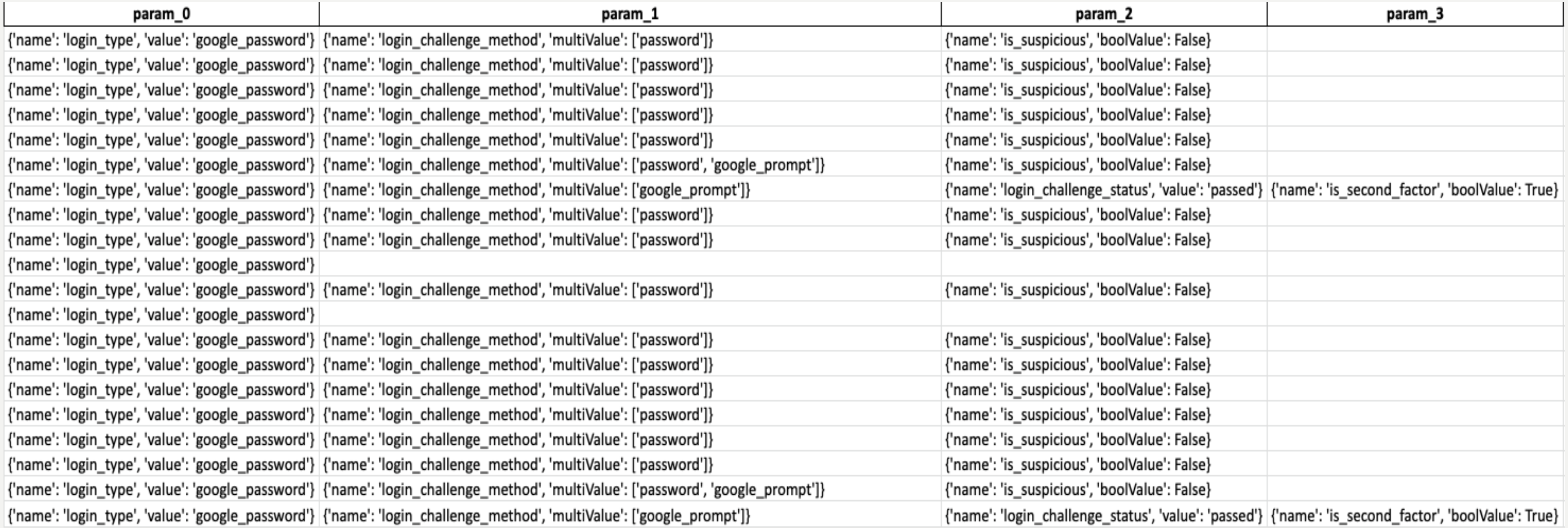
| Event Description | IP Address | Date | Login Type |
|---|---|---|---|
| Megan Roddie logged in | [redacted].99.206 | Sep 27, 2020, 2:56:12 PM CDT | Google Password |
| Megan Roddie logged in | [redacted]211.76 | Sep 27, 2020, 1:27:16 PM CDT | Google Password |
| Megan Roddie logged in | [redacted]211.76 | Sep 27, 2020, 1:26:21 PM CDT | Google Password |
| Megan Roddie logged in | [redacted].99.206 | Sep 27, 2020, 1:25:38 PM CDT | Google Password |
| Megan Roddie logged in | [redacted].99.206 | Sep 27, 2020, 1:24:08 PM CDT | Google Password |
| [redacted].org logged in | [redacted]:a3df:9aa8:2307 | Sep 26, 2020, 10:41:40 AM CDT | Google Password |
| [redacted].org was presented with login verification | [redacted]:a3df:9aa8:2307 | Sep 26, 2020, 10:41:40 AM CDT | Google Password |

# Login Audit Logs



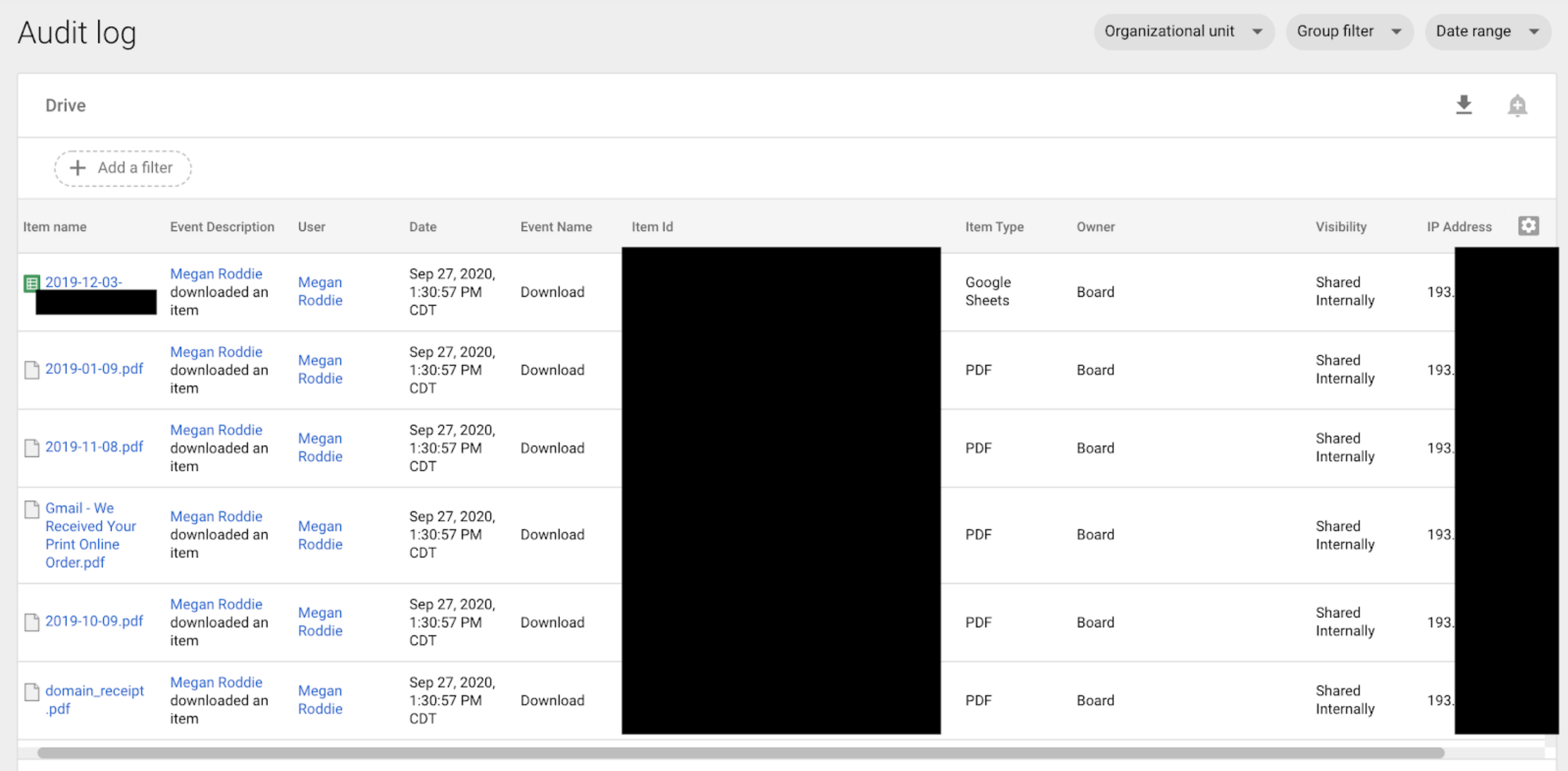
| A | B | C | D | E | F |
|---|---|---|---|---|---|
| userEmail | ipAddress | loginCountry | loginCity | timestamp | applicationName |
| megan@[redacted] | 99.12[redacted] | US | Round Rock | 2020-09-27T19:56:12.859Z | login |
| megan@[redacted] | 193.1[redacted] | HK | Central | 2020-09-27T18:27:16.780Z | login |
| megan@[redacted] | 193.1[redacted] | HK | Central | 2020-09-27T18:26:21.096Z | login |
| megan@[redacted] | 99.12[redacted] | US | Round Rock | 2020-09-27T18:25:38.023Z | login |
| megan@[redacted] | 99.12[redacted] | US | Round Rock | 2020-09-27T18:24:08.002Z | login |
| tom@me[redacted] | 2604[redacted] | US | Athol | 2020-09-26T15:41:40.842Z | login |
| tom@me[redacted] | 2604[redacted] | US | Athol | 2020-09-26T15:41:40.842Z | login |
| megan@[redacted] | 99.12[redacted] | US | Round Rock | 2020-09-24T20:00:00.490Z | login |
| megan@[redacted] | 209.5[redacted] | HK | Central | 2020-09-24T02:21:25.563Z | login |
| megan@[redacted] | 209.5[redacted] | HK | Central | 2020-09-24T02:21:15.973Z | login |
| megan@[redacted] | 209.5[redacted] | HK | Central | 2020-09-24T02:18:52.380Z | login |
| megan@[redacted] | 209.5[redacted] | HK | Central | 2020-09-24T02:18:40.716Z | login |
| megan@[redacted] | 99.12[redacted] | US | Round Rock | 2020-09-24T02:05:34.055Z | login |
| amanda@[redacted] | 192.1[redacted] | US | Port Clinton | 2020-09-22T20:34:00.448Z | login |
| megan@[redacted] | 99.12[redacted] | US | Round Rock | 2020-09-19T19:48:25.991Z | login |
| clickthal[redacted] | 2603[redacted] | US | Salem | 2020-09-18T18:19:24.372Z | login |
| megan@[redacted] | 99.12[redacted] | US | Round Rock | 2020-09-14T20:33:15.158Z | login |
| amanda@[redacted] | 2605[redacted] | US | Port Clinton | 2020-09-07T18:33:24.849Z | login |
| megan@[redacted] | 99.12[redacted] | US | Round Rock | 2020-09-07T01:05:22.399Z | login |

# Login Audit Logs



| param_0 | param_1 | param_2 | param_3 |
|---|---|---|---|
| {'name': 'login_type', 'value': 'google_password'} | {'name': 'login_challenge_method', 'multiValue': ['password']} | {'name': 'is_suspicious', 'boolValue': False} | |
| {'name': 'login_type', 'value': 'google_password'} | {'name': 'login_challenge_method', 'multiValue': ['password']} | {'name': 'is_suspicious', 'boolValue': False} | |
| {'name': 'login_type', 'value': 'google_password'} | {'name': 'login_challenge_method', 'multiValue': ['password']} | {'name': 'is_suspicious', 'boolValue': False} | |
| {'name': 'login_type', 'value': 'google_password'} | {'name': 'login_challenge_method', 'multiValue': ['password']} | {'name': 'is_suspicious', 'boolValue': False} | |
| {'name': 'login_type', 'value': 'google_password'} | {'name': 'login_challenge_method', 'multiValue': ['password']} | {'name': 'is_suspicious', 'boolValue': False} | |
| {'name': 'login_type', 'value': 'google_password'} | {'name': 'login_challenge_method', 'multiValue': ['password', 'google_prompt']} | {'name': 'is_suspicious', 'boolValue': False} | |
| {'name': 'login_type', 'value': 'google_password'} | {'name': 'login_challenge_method', 'multiValue': ['google_prompt']} | {'name': 'login_challenge_status', 'value': 'passed'} | {'name': 'is_second_factor', 'boolValue': True} |
| {'name': 'login_type', 'value': 'google_password'} | {'name': 'login_challenge_method', 'multiValue': ['password']} | {'name': 'is_suspicious', 'boolValue': False} | |
| {'name': 'login_type', 'value': 'google_password'} | {'name': 'login_challenge_method', 'multiValue': ['password']} | {'name': 'is_suspicious', 'boolValue': False} | |
| {'name': 'login_type', 'value': 'google_password'} | | | |
| {'name': 'login_type', 'value': 'google_password'} | {'name': 'login_challenge_method', 'multiValue': ['password']} | {'name': 'is_suspicious', 'boolValue': False} | |
| {'name': 'login_type', 'value': 'google_password'} | | | |
| {'name': 'login_type', 'value': 'google_password'} | {'name': 'login_challenge_method', 'multiValue': ['password']} | {'name': 'is_suspicious', 'boolValue': False} | |
| {'name': 'login_type', 'value': 'google_password'} | {'name': 'login_challenge_method', 'multiValue': ['password']} | {'name': 'is_suspicious', 'boolValue': False} | |
| {'name': 'login_type', 'value': 'google_password'} | {'name': 'login_challenge_method', 'multiValue': ['password']} | {'name': 'is_suspicious', 'boolValue': False} | |
| {'name': 'login_type', 'value': 'google_password'} | {'name': 'login_challenge_method', 'multiValue': ['password']} | {'name': 'is_suspicious', 'boolValue': False} | |
| {'name': 'login_type', 'value': 'google_password'} | {'name': 'login_challenge_method', 'multiValue': ['password']} | {'name': 'is_suspicious', 'boolValue': False} | |
| {'name': 'login_type', 'value': 'google_password'} | {'name': 'login_challenge_method', 'multiValue': ['password']} | {'name': 'is_suspicious', 'boolValue': False} | |
| {'name': 'login_type', 'value': 'google_password'} | {'name': 'login_challenge_method', 'multiValue': ['password', 'google_prompt']} | {'name': 'is_suspicious', 'boolValue': False} | |
| {'name': 'login_type', 'value': 'google_password'} | {'name': 'login_challenge_method', 'multiValue': ['google_prompt']} | {'name': 'login_challenge_status', 'value': 'passed'} | {'name': 'is_second_factor', 'boolValue': True} |

# Drive Audit Logs



Audit log

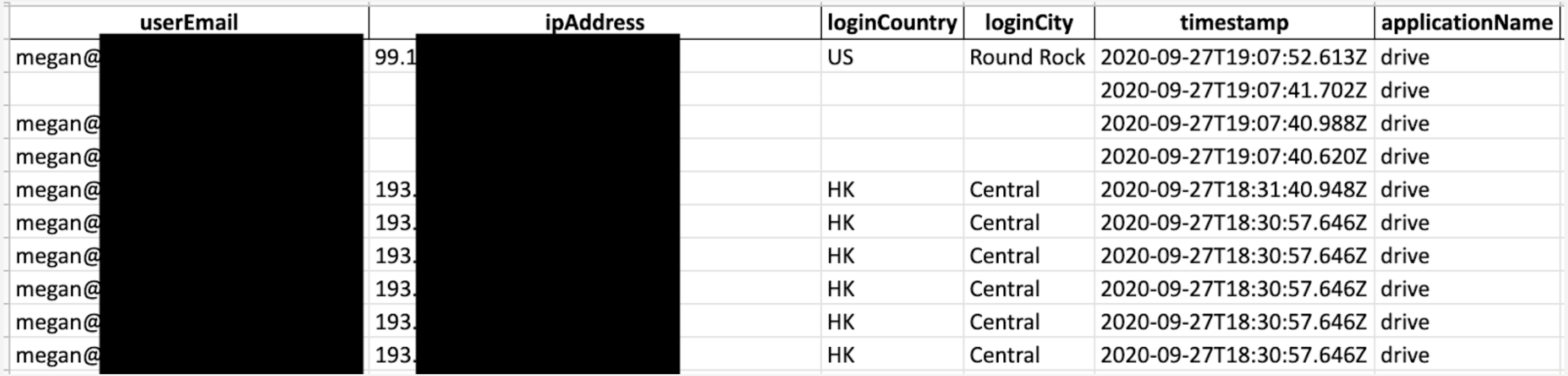
Organizational unit ▾ Group filter ▾ Date range ▾

Drive

+ Add a filter

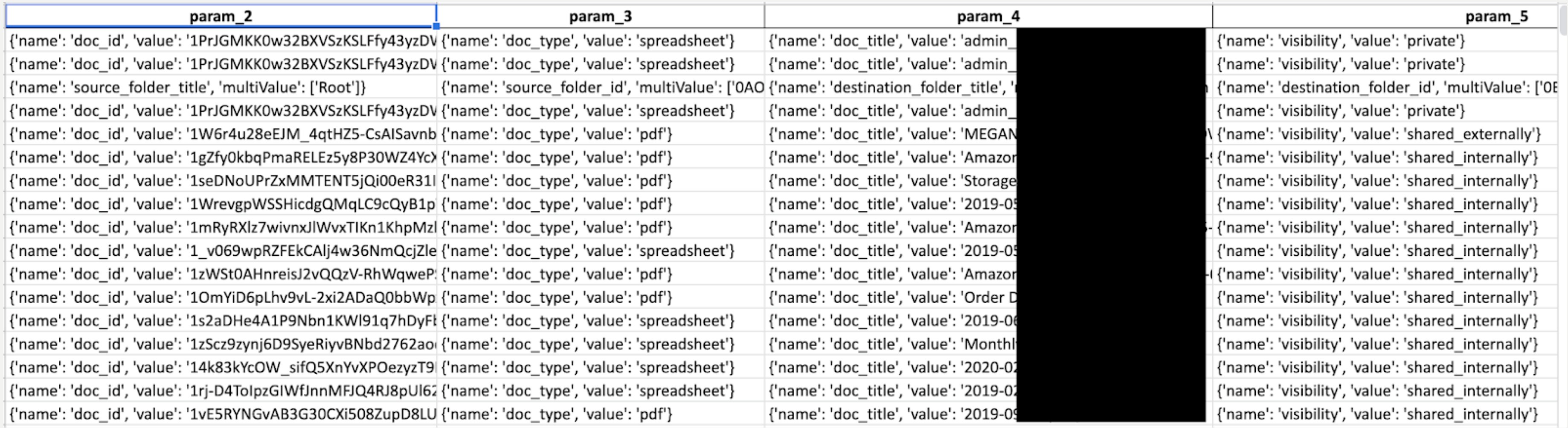
| Item name | Event Description | User | Date | Event Name | Item Id | Item Type | Owner | Visibility | IP Address |
|---|---|---|---|---|---|---|---|---|---|
| 2019-12-03-[redacted] | Megan Roddie downloaded an item | Megan Roddie | Sep 27, 2020, 1:30:57 PM CDT | Download | [redacted] | Google Sheets | Board | Shared Internally | 193.[redacted] |
| 2019-01-09.pdf | Megan Roddie downloaded an item | Megan Roddie | Sep 27, 2020, 1:30:57 PM CDT | Download | [redacted] | PDF | Board | Shared Internally | 193.[redacted] |
| 2019-11-08.pdf | Megan Roddie downloaded an item | Megan Roddie | Sep 27, 2020, 1:30:57 PM CDT | Download | [redacted] | PDF | Board | Shared Internally | 193.[redacted] |
| Gmail - We Received Your Print Online Order.pdf | Megan Roddie downloaded an item | Megan Roddie | Sep 27, 2020, 1:30:57 PM CDT | Download | [redacted] | PDF | Board | Shared Internally | 193.[redacted] |
| 2019-10-09.pdf | Megan Roddie downloaded an item | Megan Roddie | Sep 27, 2020, 1:30:57 PM CDT | Download | [redacted] | PDF | Board | Shared Internally | 193.[redacted] |
| domain_receipt.pdf | Megan Roddie downloaded an item | Megan Roddie | Sep 27, 2020, 1:30:57 PM CDT | Download | [redacted] | PDF | Board | Shared Internally | 193.[redacted] |

# Drive Audit Logs



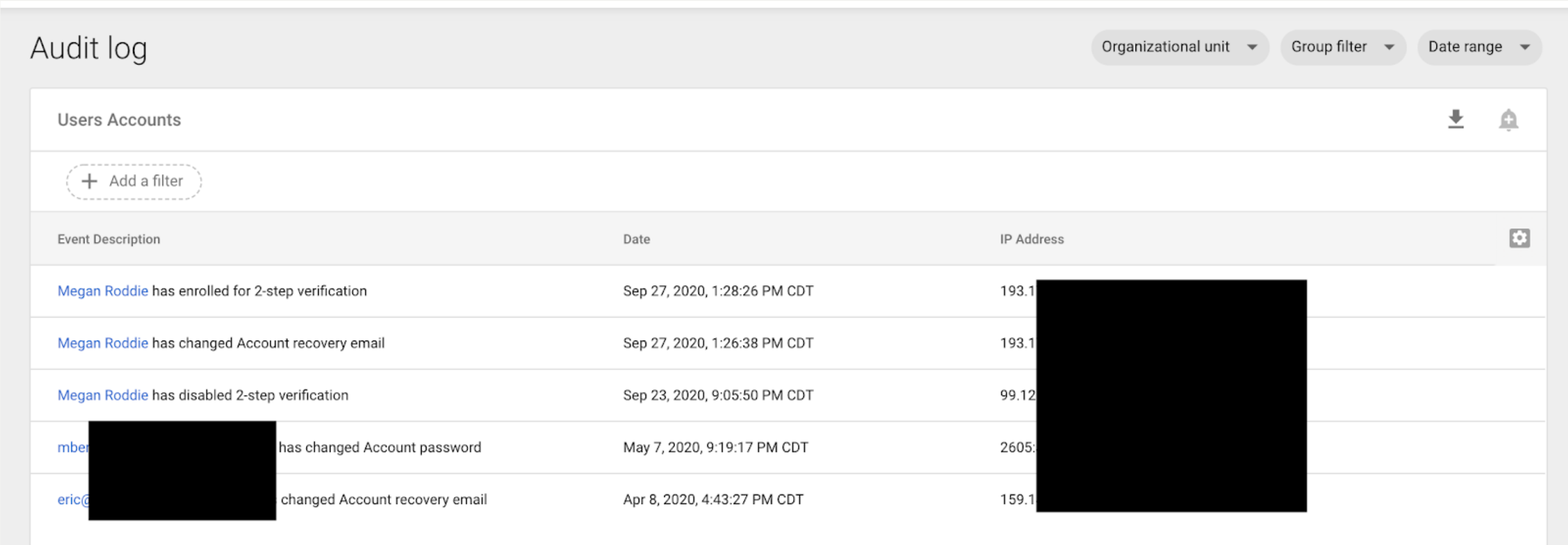
| userEmail | ipAddress | loginCountry | loginCity | timestamp | applicationName |
|---|---|---|---|---|---|
| megan@[redacted] | 99.1[redacted] | US | Round Rock | 2020-09-27T19:07:52.613Z | drive |
| [redacted] | [redacted] | | | 2020-09-27T19:07:41.702Z | drive |
| megan@[redacted] | [redacted] | | | 2020-09-27T19:07:40.988Z | drive |
| megan@[redacted] | [redacted] | | | 2020-09-27T19:07:40.620Z | drive |
| megan@[redacted] | 193.[redacted] | HK | Central | 2020-09-27T18:31:40.948Z | drive |
| megan@[redacted] | 193.[redacted] | HK | Central | 2020-09-27T18:30:57.646Z | drive |
| megan@[redacted] | 193.[redacted] | HK | Central | 2020-09-27T18:30:57.646Z | drive |
| megan@[redacted] | 193.[redacted] | HK | Central | 2020-09-27T18:30:57.646Z | drive |
| megan@[redacted] | 193.[redacted] | HK | Central | 2020-09-27T18:30:57.646Z | drive |
| megan@[redacted] | 193.[redacted] | HK | Central | 2020-09-27T18:30:57.646Z | drive |

# Drive Audit Logs



| param_2 | param_3 | param_4 | param_5 |
|---|---|---|---|
| {'name': 'doc_id', 'value': '1PrJGMKK0w32BXVSzKSLFfy43yzDV | {'name': 'doc_type', 'value': 'spreadsheet'} | {'name': 'doc_title', 'value': 'admin_ [redacted] | {'name': 'visibility', 'value': 'private'} |
| {'name': 'doc_id', 'value': '1PrJGMKK0w32BXVSzKSLFfy43yzDV | {'name': 'doc_type', 'value': 'spreadsheet'} | {'name': 'doc_title', 'value': 'admin_ [redacted] | {'name': 'visibility', 'value': 'private'} |
| {'name': 'source_folder_title', 'multiValue': ['Root']} | {'name': 'source_folder_id', 'multiValue': ['0AO | {'name': 'destination_folder_title', ' [redacted] | {'name': 'destination_folder_id', 'multiValue': ['0E |
| {'name': 'doc_id', 'value': '1PrJGMKK0w32BXVSzKSLFfy43yzDV | {'name': 'doc_type', 'value': 'spreadsheet'} | {'name': 'doc_title', 'value': 'admin_ [redacted] | {'name': 'visibility', 'value': 'private'} |
| {'name': 'doc_id', 'value': '1W6r4u28eEJM_4qtHZ5-CsAISavnb | {'name': 'doc_type', 'value': 'pdf'} | {'name': 'doc_title', 'value': 'MEGAN [redacted] | {'name': 'visibility', 'value': 'shared_externally'} |
| {'name': 'doc_id', 'value': '1gZfy0kbqPmaRELEz5y8P30WZ4YcX | {'name': 'doc_type', 'value': 'pdf'} | {'name': 'doc_title', 'value': 'Amazon [redacted] | {'name': 'visibility', 'value': 'shared_internally'} |
| {'name': 'doc_id', 'value': '1seDNoUPrZxMMTENT5jQi00eR31I | {'name': 'doc_type', 'value': 'pdf'} | {'name': 'doc_title', 'value': 'Storage [redacted] | {'name': 'visibility', 'value': 'shared_internally'} |
| {'name': 'doc_id', 'value': '1WrevgpWSSHicdgQMqLC9cQyB1p | {'name': 'doc_type', 'value': 'pdf'} | {'name': 'doc_title', 'value': '2019-05 [redacted] | {'name': 'visibility', 'value': 'shared_internally'} |
| {'name': 'doc_id', 'value': '1mRyRXlz7wivnxJlWvxTIKn1KhpMzl | {'name': 'doc_type', 'value': 'pdf'} | {'name': 'doc_title', 'value': 'Amazon [redacted] | {'name': 'visibility', 'value': 'shared_internally'} |
| {'name': 'doc_id', 'value': '1_v069wpRZFEkCAlj4w36NmQcjZle | {'name': 'doc_type', 'value': 'spreadsheet'} | {'name': 'doc_title', 'value': '2019-05 [redacted] | {'name': 'visibility', 'value': 'shared_internally'} |
| {'name': 'doc_id', 'value': '1zWSt0AHnreisJ2vQQzV-RhWqweP | {'name': 'doc_type', 'value': 'pdf'} | {'name': 'doc_title', 'value': 'Amazon [redacted] | {'name': 'visibility', 'value': 'shared_internally'} |
| {'name': 'doc_id', 'value': '1OmYiD6pLhv9vL-2xi2ADaQ0bbWp | {'name': 'doc_type', 'value': 'pdf'} | {'name': 'doc_title', 'value': 'Order D [redacted] | {'name': 'visibility', 'value': 'shared_internally'} |
| {'name': 'doc_id', 'value': '1s2aDHe4A1P9Nbn1KWl91q7hDyFt | {'name': 'doc_type', 'value': 'spreadsheet'} | {'name': 'doc_title', 'value': '2019-06 [redacted] | {'name': 'visibility', 'value': 'shared_internally'} |
| {'name': 'doc_id', 'value': '1zScz9zynj6D9SyeRiyvBNbd2762ao | {'name': 'doc_type', 'value': 'spreadsheet'} | {'name': 'doc_title', 'value': 'Monthl [redacted] | {'name': 'visibility', 'value': 'shared_internally'} |
| {'name': 'doc_id', 'value': '14k83kYcOW_sifQ5XnYvXPOezyzT9 | {'name': 'doc_type', 'value': 'spreadsheet'} | {'name': 'doc_title', 'value': '2020-02 [redacted] | {'name': 'visibility', 'value': 'shared_internally'} |
| {'name': 'doc_id', 'value': '1rj-D4ToIpzGIWfJnnMFJQ4RJ8pUl62 | {'name': 'doc_type', 'value': 'spreadsheet'} | {'name': 'doc_title', 'value': '2019-02 [redacted] | {'name': 'visibility', 'value': 'shared_internally'} |
| {'name': 'doc_id', 'value': '1vE5RYNGvAB3G30CXi508ZupD8LU | {'name': 'doc_type', 'value': 'pdf'} | {'name': 'doc_title', 'value': '2019-09 [redacted] | {'name': 'visibility', 'value': 'shared_internally'} |

# User Account Audit Logs



## Audit log

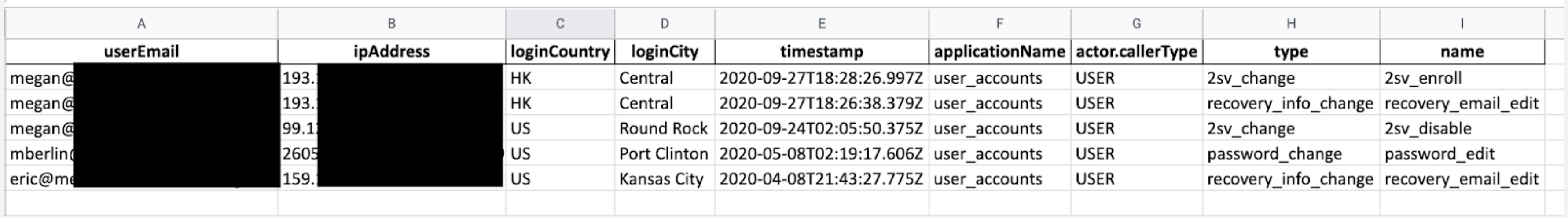
Organizational unit ▾ Group filter ▾ Date range ▾

### Users Accounts

+ Add a filter

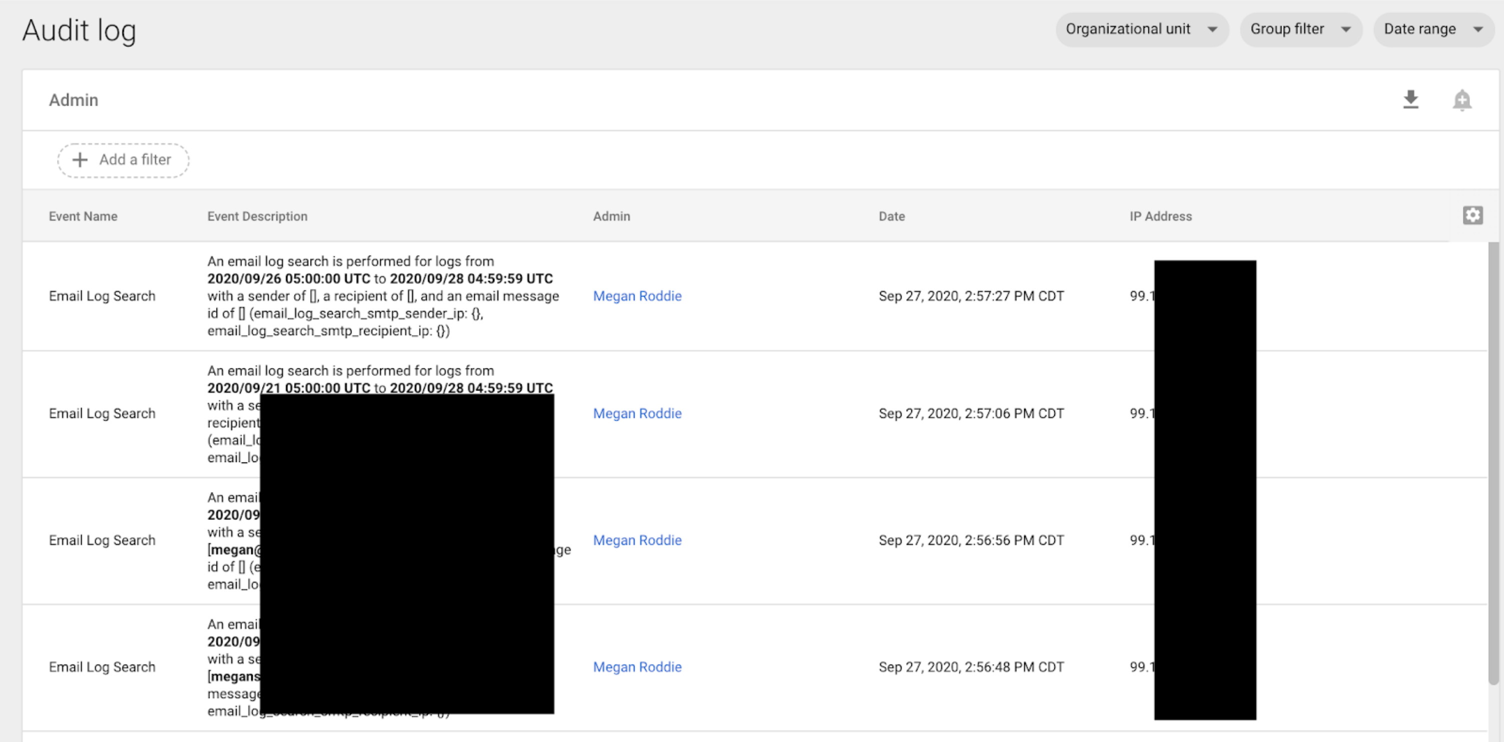
| Event Description | Date | IP Address |
|---|---|---|
| Megan Roddie has enrolled for 2-step verification | Sep 27, 2020, 1:28:26 PM CDT | 193.1[redacted] |
| Megan Roddie has changed Account recovery email | Sep 27, 2020, 1:26:38 PM CDT | 193.1[redacted] |
| Megan Roddie has disabled 2-step verification | Sep 23, 2020, 9:05:50 PM CDT | 99.12[redacted] |
| mber[redacted] has changed Account password | May 7, 2020, 9:19:17 PM CDT | 2605:[redacted] |
| eric@[redacted] changed Account recovery email | Apr 8, 2020, 4:43:27 PM CDT | 159.1[redacted] |

# User Account Audit Logs



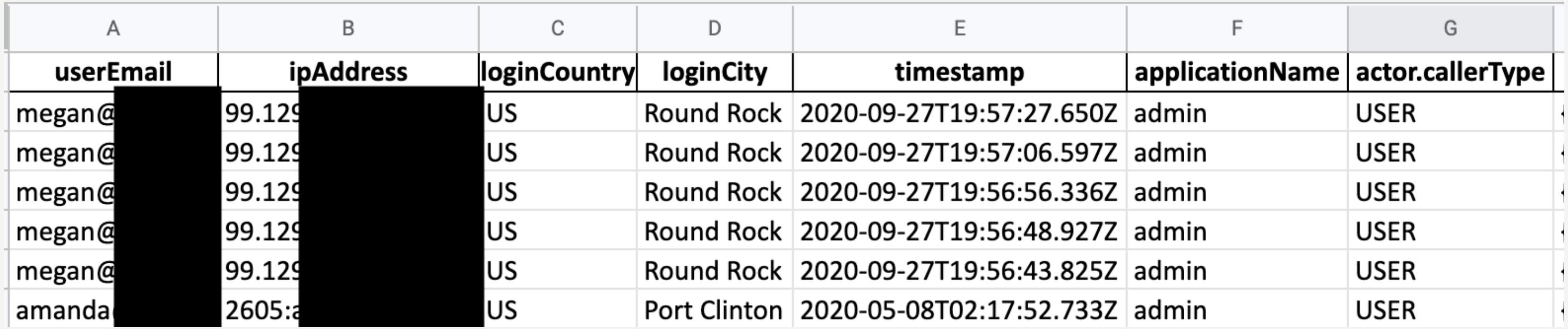
| A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|
| userEmail | ipAddress | loginCountry | loginCity | timestamp | applicationName | actor.callerType | type | name |
| megan@[redacted] | 193.[redacted] | HK | Central | 2020-09-27T18:28:26.997Z | user_accounts | USER | 2sv_change | 2sv_enroll |
| megan@[redacted] | 193.[redacted] | HK | Central | 2020-09-27T18:26:38.379Z | user_accounts | USER | recovery_info_change | recovery_email_edit |
| megan@[redacted] | 99.1[redacted] | US | Round Rock | 2020-09-24T02:05:50.375Z | user_accounts | USER | 2sv_change | 2sv_disable |
| mberlin[redacted] | 2605[redacted] | US | Port Clinton | 2020-05-08T02:19:17.606Z | user_accounts | USER | password_change | password_edit |
| eric@me[redacted] | 159.[redacted] | US | Kansas City | 2020-04-08T21:43:27.775Z | user_accounts | USER | recovery_info_change | recovery_email_edit |

# Admin Audit Logs



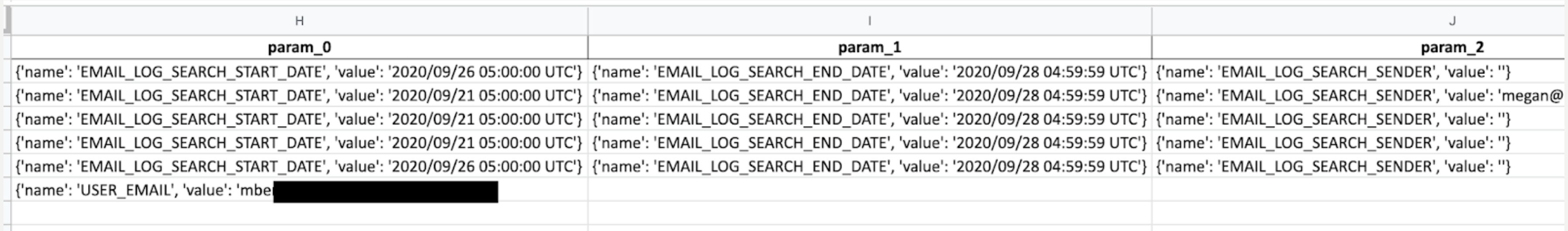
| Event Name | Event Description | Admin | Date | IP Address |
|---|---|---|---|---|
| Email Log Search | An email log search is performed for logs from **2020/09/26 05:00:00 UTC** to **2020/09/28 04:59:59 UTC** with a sender of [], a recipient of [], and an email message id of [] (email_log_search_smtp_sender_ip: {}, email_log_search_smtp_recipient_ip: {}) | Megan Roddie | Sep 27, 2020, 2:57:27 PM CDT | 99.1[redacted] |
| Email Log Search | An email log search is performed for logs from **2020/09/21 05:00:00 UTC** to **2020/09/28 04:59:59 UTC** with a se[redacted] recipient (email_l email_lo | Megan Roddie | Sep 27, 2020, 2:57:06 PM CDT | 99.1[redacted] |
| Email Log Search | An email **2020/09**[redacted] with a se **[megan@** ge id of [] (e email_lo | Megan Roddie | Sep 27, 2020, 2:56:56 PM CDT | 99.1[redacted] |
| Email Log Search | An email **2020/09**[redacted] with a se **[megans** message email_lo | Megan Roddie | Sep 27, 2020, 2:56:48 PM CDT | 99.1[redacted] |

# Admin Audit Logs



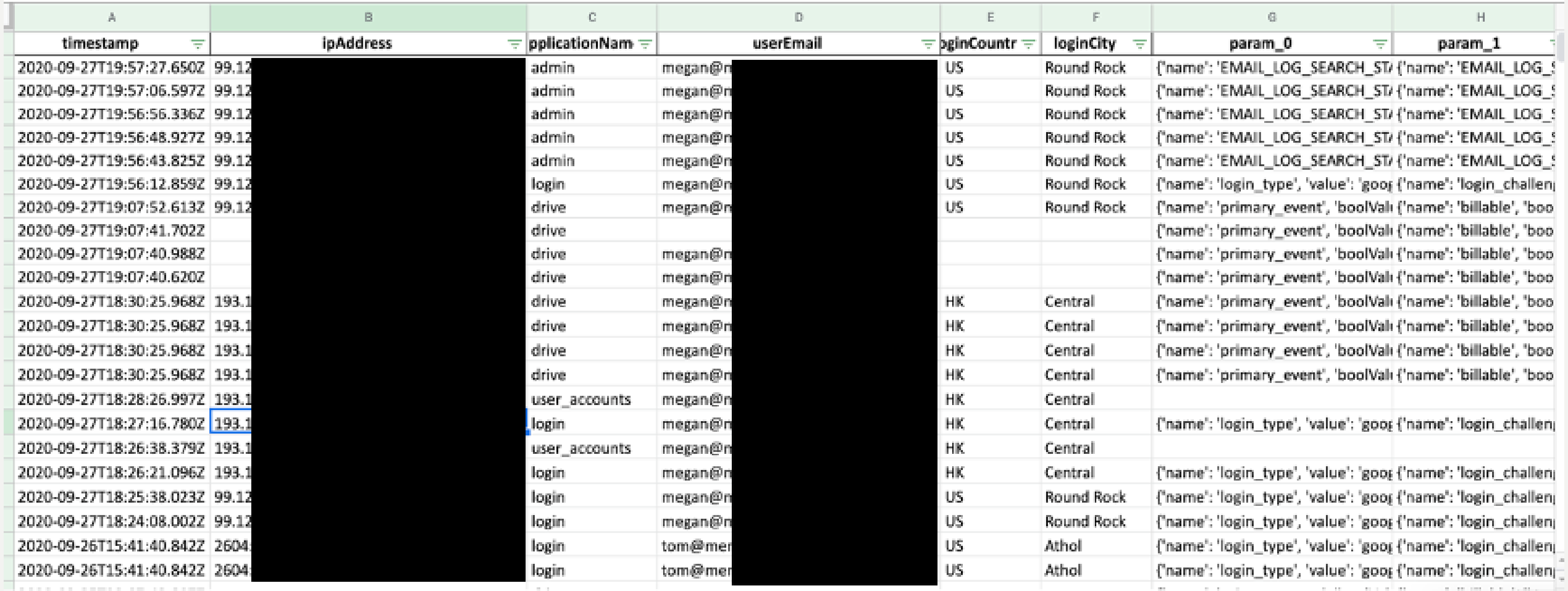
| A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|
| **userEmail** | **ipAddress** | **loginCountry** | **loginCity** | **timestamp** | **applicationName** | **actor.callerType** |
| megan@[redacted] | 99.12[redacted] | US | Round Rock | 2020-09-27T19:57:27.650Z | admin | USER |
| megan@[redacted] | 99.12[redacted] | US | Round Rock | 2020-09-27T19:57:06.597Z | admin | USER |
| megan@[redacted] | 99.12[redacted] | US | Round Rock | 2020-09-27T19:56:56.336Z | admin | USER |
| megan@[redacted] | 99.12[redacted] | US | Round Rock | 2020-09-27T19:56:48.927Z | admin | USER |
| megan@[redacted] | 99.12[redacted] | US | Round Rock | 2020-09-27T19:56:43.825Z | admin | USER |
| amanda[redacted] | 2605:[redacted] | US | Port Clinton | 2020-05-08T02:17:52.733Z | admin | USER |

# Admin Audit Logs



| H | I | J |
|---|---|---|
| **param_0** | **param_1** | **param_2** |
| {'name': 'EMAIL_LOG_SEARCH_START_DATE', 'value': '2020/09/26 05:00:00 UTC'} | {'name': 'EMAIL_LOG_SEARCH_END_DATE', 'value': '2020/09/28 04:59:59 UTC'} | {'name': 'EMAIL_LOG_SEARCH_SENDER', 'value': ''} |
| {'name': 'EMAIL_LOG_SEARCH_START_DATE', 'value': '2020/09/21 05:00:00 UTC'} | {'name': 'EMAIL_LOG_SEARCH_END_DATE', 'value': '2020/09/28 04:59:59 UTC'} | {'name': 'EMAIL_LOG_SEARCH_SENDER', 'value': 'megan@ |
| {'name': 'EMAIL_LOG_SEARCH_START_DATE', 'value': '2020/09/21 05:00:00 UTC'} | {'name': 'EMAIL_LOG_SEARCH_END_DATE', 'value': '2020/09/28 04:59:59 UTC'} | {'name': 'EMAIL_LOG_SEARCH_SENDER', 'value': ''} |
| {'name': 'EMAIL_LOG_SEARCH_START_DATE', 'value': '2020/09/21 05:00:00 UTC'} | {'name': 'EMAIL_LOG_SEARCH_END_DATE', 'value': '2020/09/28 04:59:59 UTC'} | {'name': 'EMAIL_LOG_SEARCH_SENDER', 'value': ''} |
| {'name': 'EMAIL_LOG_SEARCH_START_DATE', 'value': '2020/09/26 05:00:00 UTC'} | {'name': 'EMAIL_LOG_SEARCH_END_DATE', 'value': '2020/09/28 04:59:59 UTC'} | {'name': 'EMAIL_LOG_SEARCH_SENDER', 'value': ''} |
| {'name': 'USER_EMAIL', 'value': 'mbe[redacted] | | |
| | | |

# Consolidated Log View



| A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|
| timestamp | ipAddress | pplicationNam | userEmail | oginCountr | loginCity | param_0 | param_1 |
| 2020-09-27T19:57:27.650Z | 99.12[redacted] | admin | megan@[redacted] | US | Round Rock | {'name': 'EMAIL_LOG_SEARCH_ST | {'name': 'EMAIL_LOG_ |
| 2020-09-27T19:57:06.597Z | 99.12[redacted] | admin | megan@[redacted] | US | Round Rock | {'name': 'EMAIL_LOG_SEARCH_ST | {'name': 'EMAIL_LOG_ |
| 2020-09-27T19:56:56.336Z | 99.12[redacted] | admin | megan@[redacted] | US | Round Rock | {'name': 'EMAIL_LOG_SEARCH_ST | {'name': 'EMAIL_LOG_ |
| 2020-09-27T19:56:48.927Z | 99.12[redacted] | admin | megan@[redacted] | US | Round Rock | {'name': 'EMAIL_LOG_SEARCH_ST | {'name': 'EMAIL_LOG_ |
| 2020-09-27T19:56:43.825Z | 99.12[redacted] | admin | megan@[redacted] | US | Round Rock | {'name': 'EMAIL_LOG_SEARCH_ST | {'name': 'EMAIL_LOG_ |
| 2020-09-27T19:56:12.859Z | 99.12[redacted] | login | megan@[redacted] | US | Round Rock | {'name': 'login_type', 'value': 'goo | {'name': 'login_challen |
| 2020-09-27T19:07:52.613Z | 99.12[redacted] | drive | megan@[redacted] | US | Round Rock | {'name': 'primary_event', 'boolVal | {'name': 'billable', 'boo |
| 2020-09-27T19:07:41.702Z | [redacted] | drive | [redacted] |  |  | {'name': 'primary_event', 'boolVal | {'name': 'billable', 'boo |
| 2020-09-27T19:07:40.988Z | [redacted] | drive | megan@[redacted] |  |  | {'name': 'primary_event', 'boolVal | {'name': 'billable', 'boo |
| 2020-09-27T19:07:40.620Z | [redacted] | drive | megan@[redacted] |  |  | {'name': 'primary_event', 'boolVal | {'name': 'billable', 'boo |
| 2020-09-27T18:30:25.968Z | 193.1[redacted] | drive | megan@[redacted] | HK | Central | {'name': 'primary_event', 'boolVal | {'name': 'billable', 'boo |
| 2020-09-27T18:30:25.968Z | 193.1[redacted] | drive | megan@[redacted] | HK | Central | {'name': 'primary_event', 'boolVal | {'name': 'billable', 'boo |
| 2020-09-27T18:30:25.968Z | 193.1[redacted] | drive | megan@[redacted] | HK | Central | {'name': 'primary_event', 'boolVal | {'name': 'billable', 'boo |
| 2020-09-27T18:30:25.968Z | 193.1[redacted] | drive | megan@[redacted] | HK | Central | {'name': 'primary_event', 'boolVal | {'name': 'billable', 'boo |
| 2020-09-27T18:28:26.997Z | 193.1[redacted] | user_accounts | megan@[redacted] | HK | Central |  |  |
| 2020-09-27T18:27:16.780Z | 193.1[redacted] | login | megan@[redacted] | HK | Central | {'name': 'login_type', 'value': 'goo | {'name': 'login_challen |
| 2020-09-27T18:26:38.379Z | 193.1[redacted] | user_accounts | megan@[redacted] | HK | Central |  |  |
| 2020-09-27T18:26:21.096Z | 193.1[redacted] | login | megan@[redacted] | HK | Central | {'name': 'login_type', 'value': 'goo | {'name': 'login_challen |
| 2020-09-27T18:25:38.023Z | 99.12[redacted] | login | megan@[redacted] | US | Round Rock | {'name': 'login_type', 'value': 'goo | {'name': 'login_challen |
| 2020-09-27T18:24:08.002Z | 99.12[redacted] | login | megan@[redacted] | US | Round Rock | {'name': 'login_type', 'value': 'goo | {'name': 'login_challen |
| 2020-09-26T15:41:40.842Z | 2604[redacted] | login | tom@me[redacted] | US | Athol | {'name': 'login_type', 'value': 'goo | {'name': 'login_challen |
| 2020-09-26T15:41:40.842Z | 2604[redacted] | login | tom@me[redacted] | US | Athol | {'name': 'login_type', 'value': 'goo | {'name': 'login_challen |

# Findings

- Benefits of Custom Tool:
    - Single pane view of all logs
    - Geolocation context
    - No cred sharing required
    - Common Format

# Findings

- Downsides of Custom Tool:
  - Some views are more complicated/cluttered
  - Requires API set up
- Proposed improvements:
  - Clean up views
  - Add enrichment
  - Expand log categories
  - Contextual Highlighting

# Summary

- Custom tool added a single pane view and geolocation context
    - Allows quicker identification of certain malicious activity
- Further development needed to increase its value over built in logging

# Questions?

- Check out the code:
    - https://github.com/megan201296/gsuite-dfir