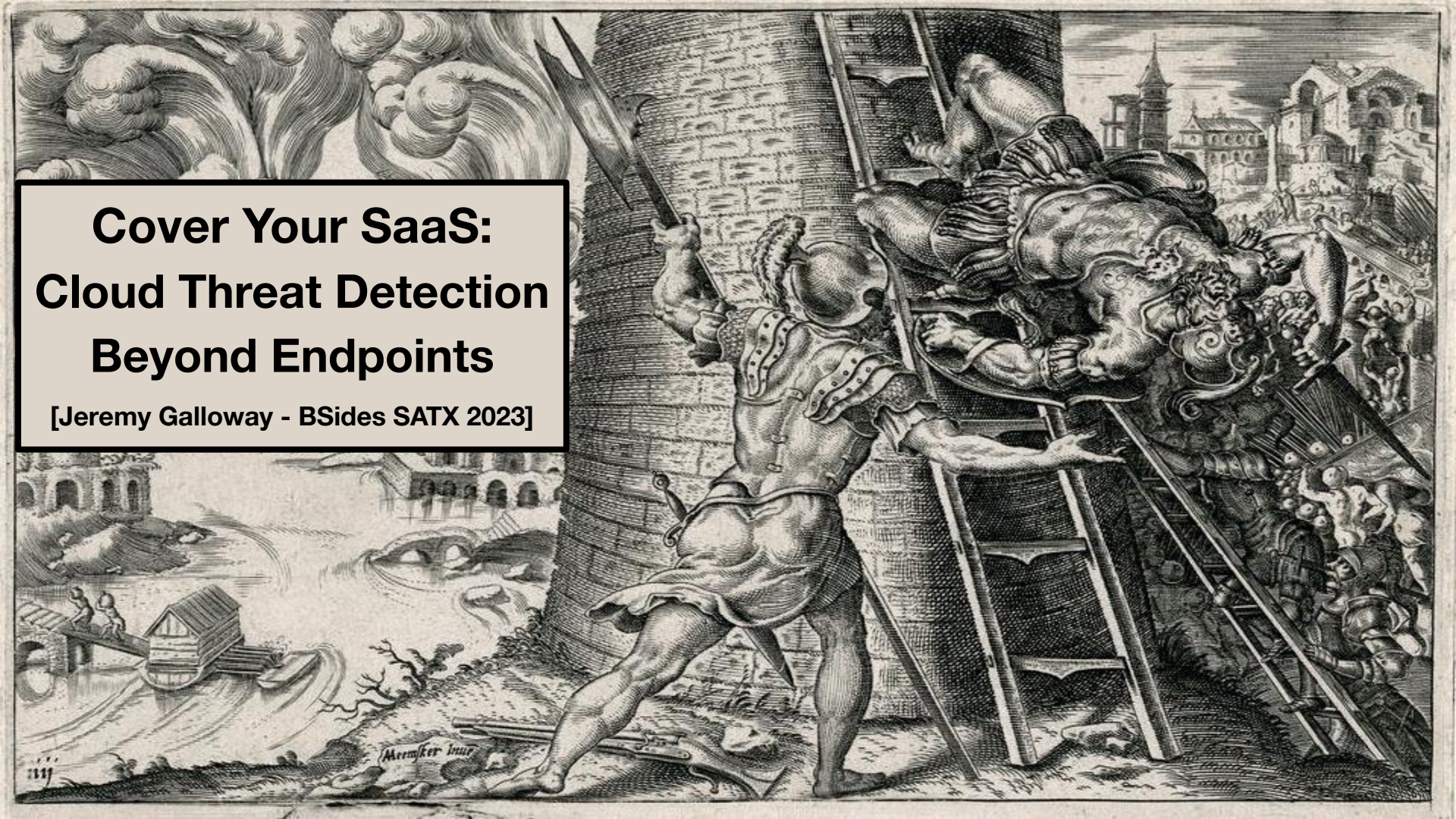


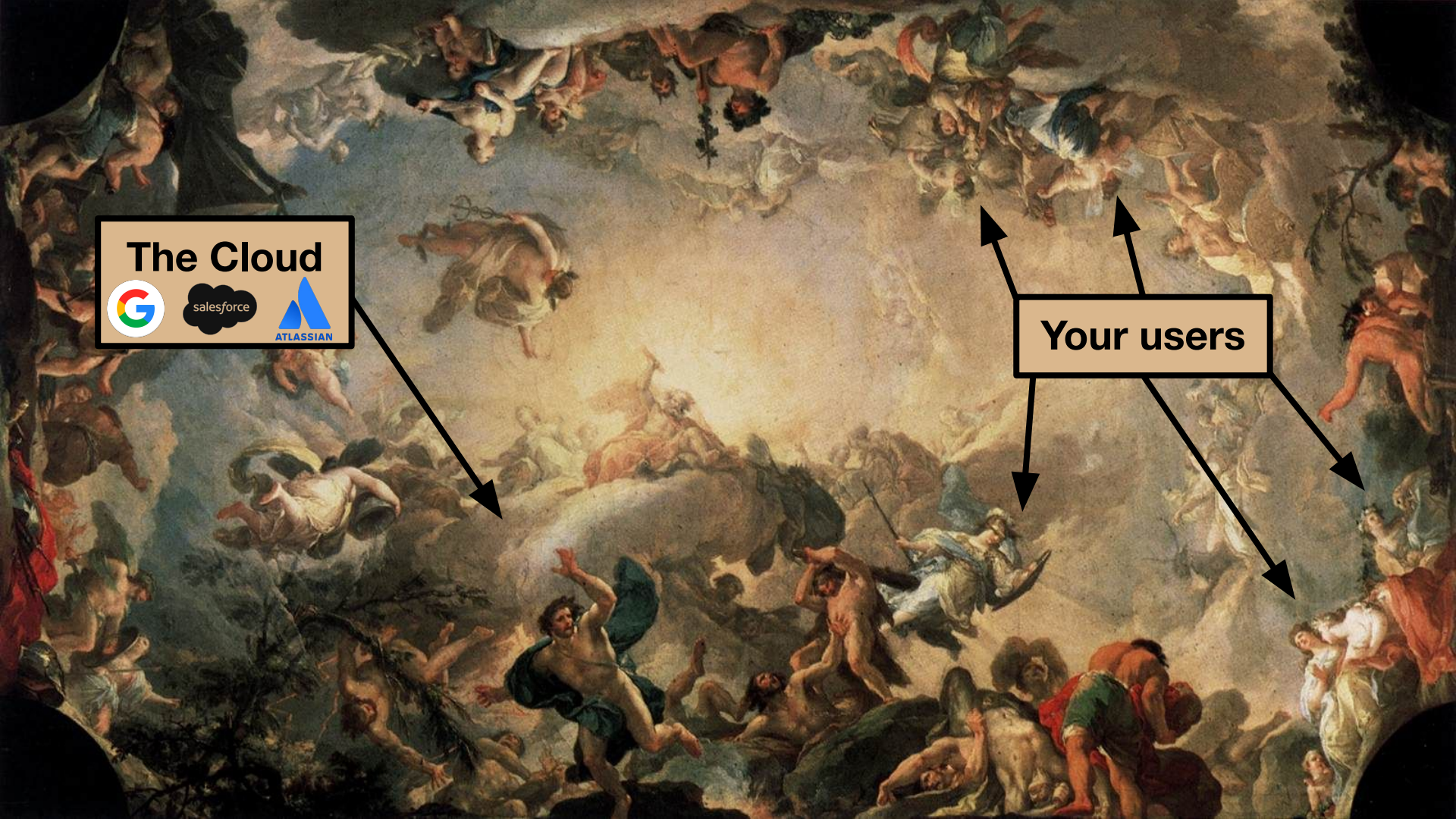
# Cover Your SaaS: Cloud Threat Detection Beyond Endpoints

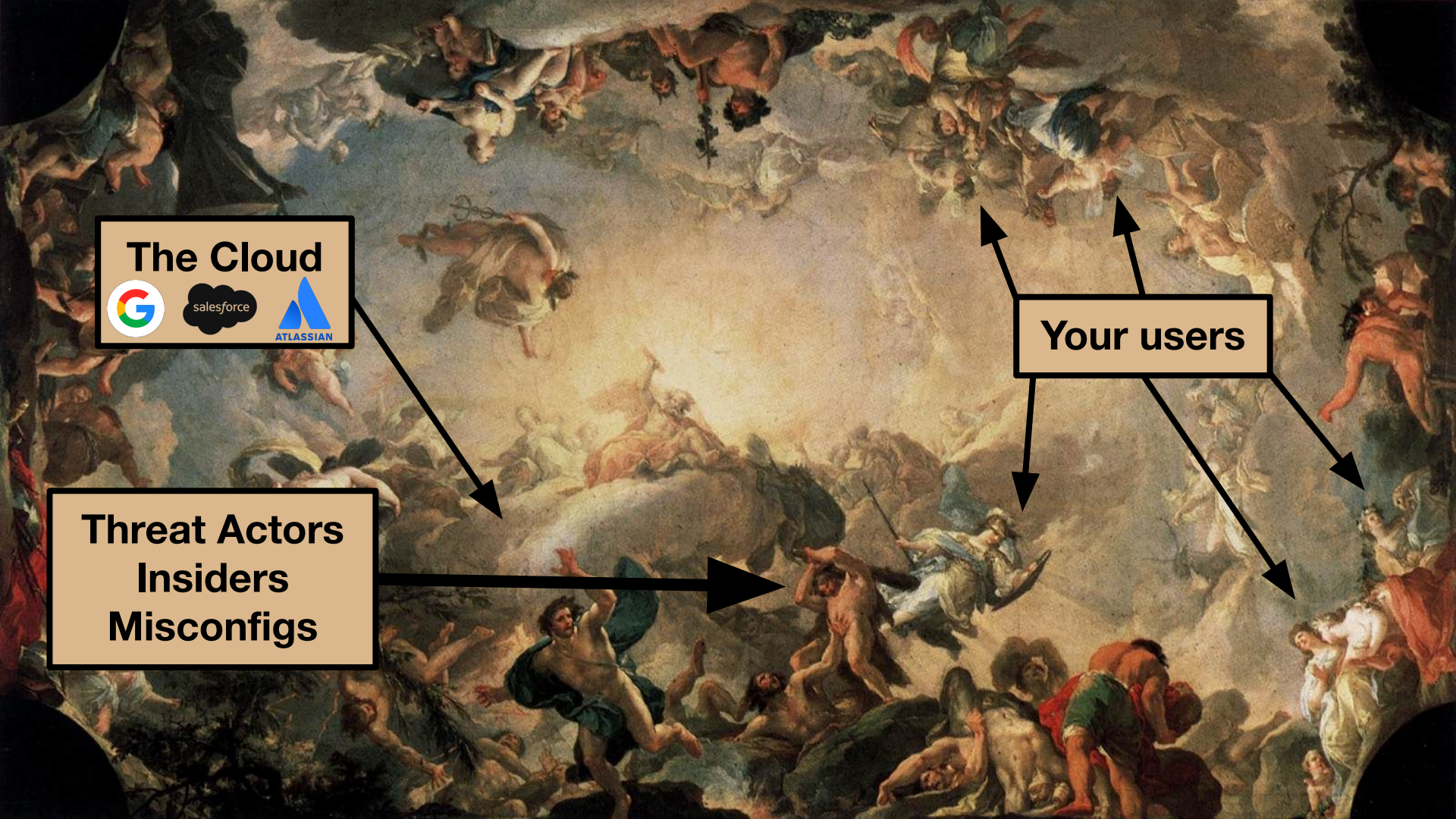
[Jeremy Galloway - BSides SATX 2023]

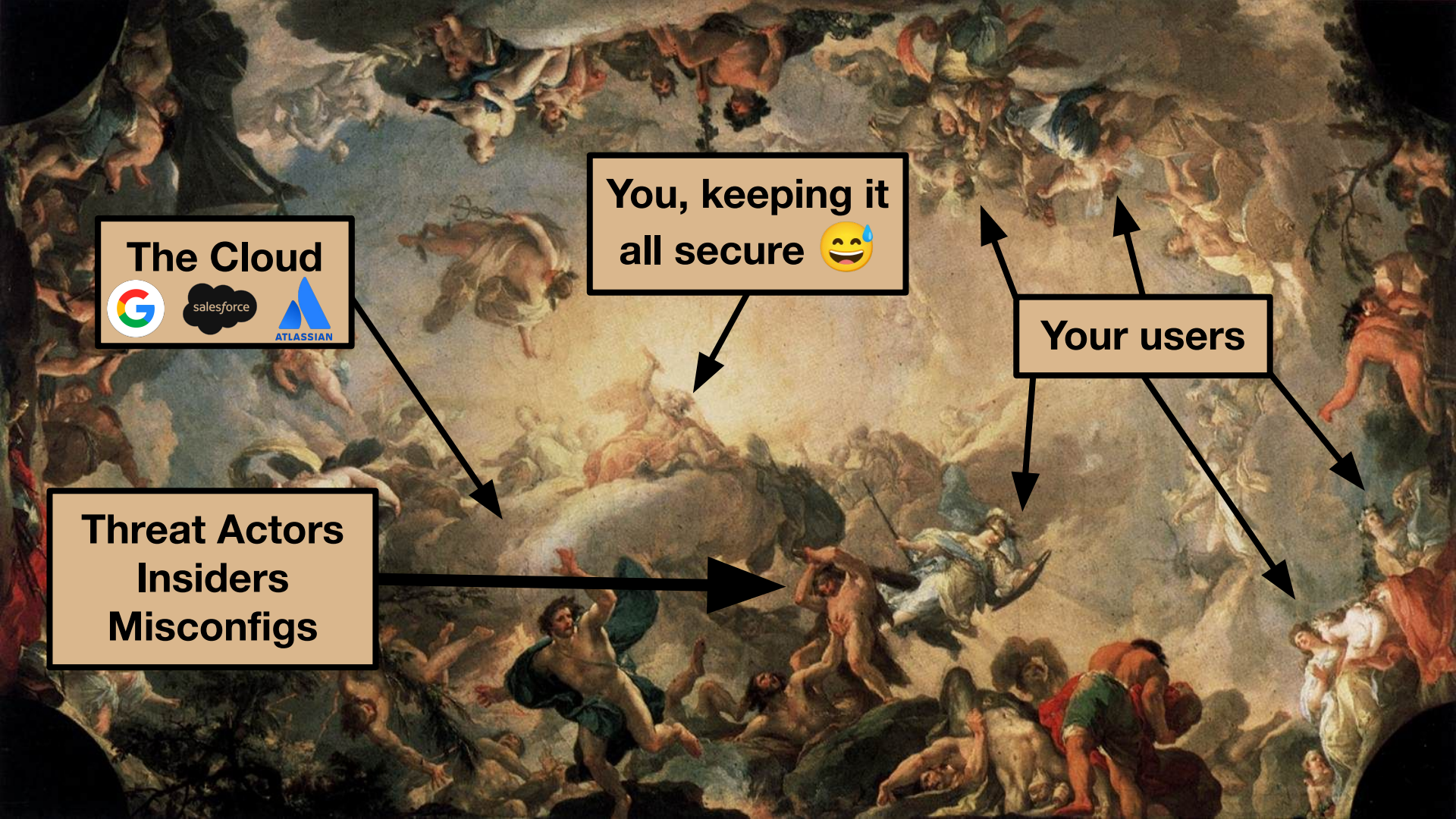
- Jeremy Galloway
- Breaking + Protecting since 2002
- Detection Engineering, Purple Teaming, DFIR, Cloud Security
- BSides LV + ATX + SATX SecTor, ISSW, BlackHat
- Atlassian since 2015


What this talk is about…


The Cloud
salesforce
ATLASSIAN


The Cloud
salesforce
ATLASSIAN
Your users


The Cloud
salesforce
ATLASSIAN
Your users
Threat Actors
Insiders
Misconfigs


The Cloud
salesforce
ATLASSIAN
You, keeping it all secure 😅
Your users
Threat Actors
Insiders
Misconfigs

## Always important but, not today's focus:

- Endpoint Security
- Cloud Infrastructure
- Malware
- Initial Access
- Vulnerability Exploitation

# Traditional Detections

# Traditional Detections

- Focused on Endpoints
  - Servers, laptops, desktops

# Traditional Detections

- Focused on Endpoints
  - Servers, laptops, desktops
- Monitor *system* activities
  - commands executed, filesystem, network traffic

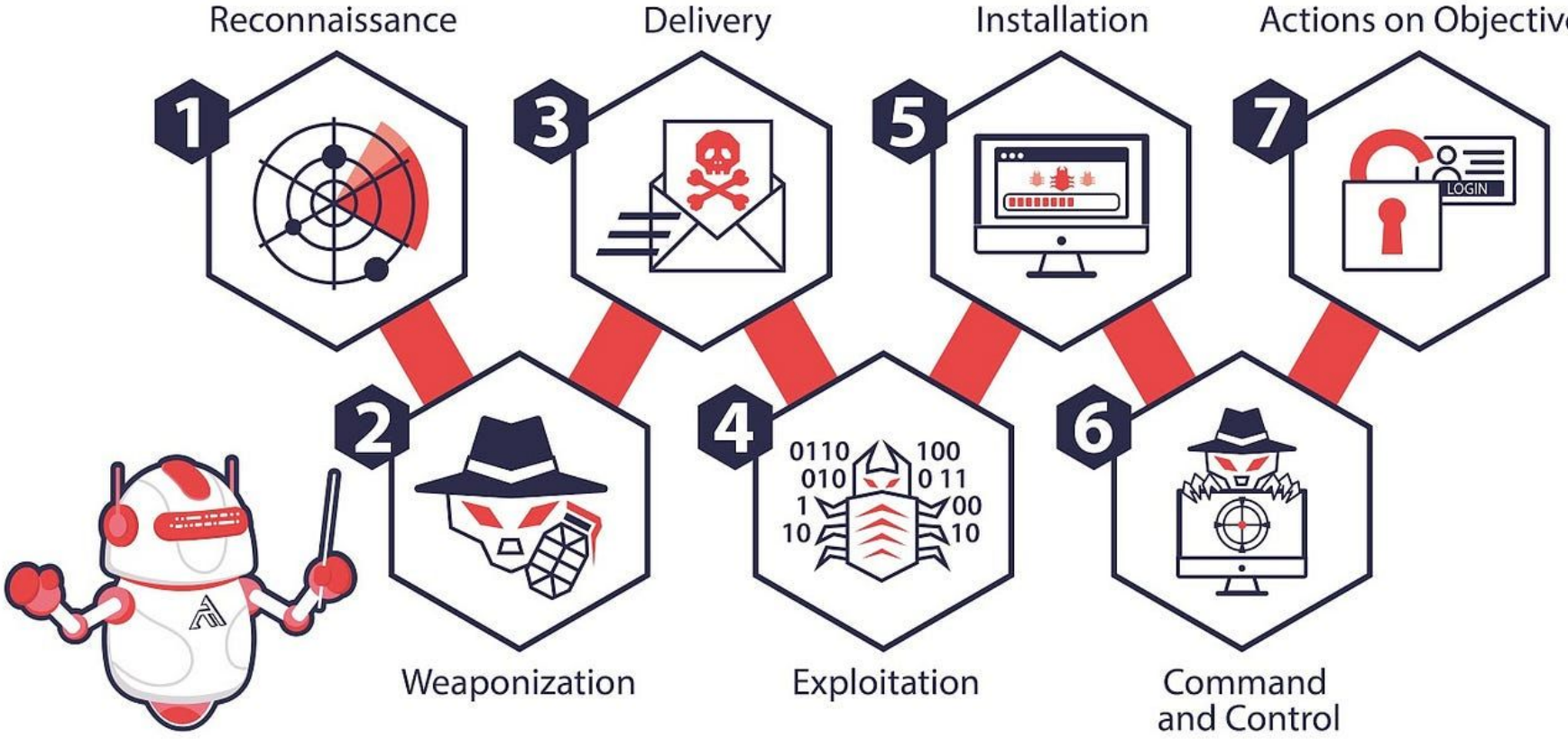
# Traditional Detections

- Focused on Endpoints
  - Servers, laptops, desktops
- Monitor *system* activities
  - commands executed, filesystem, network traffic
- Common log sources:
  - Sysmon, osquery, AV/EDR, DNS

# Traditional Detections

- Focused on Endpoints
  - Servers, laptops, desktops
- Monitor *system* activities
  - commands executed, filesystem, network traffic
- Common log sources:
  - Sysmon, osquery, AV/EDR, DNS
- Highly abstracted from users' actions

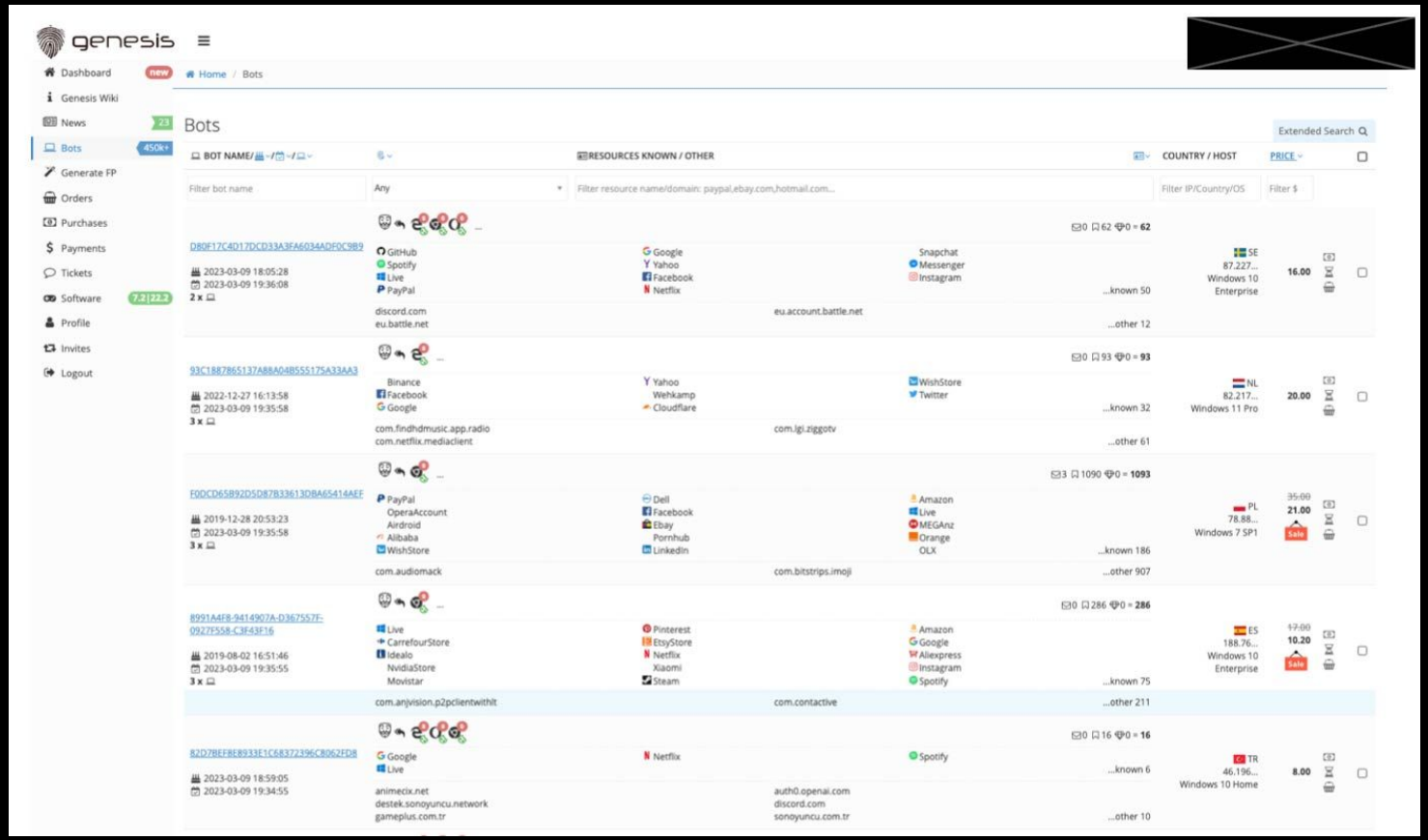
# THE CYBER KILL CHAIN




THE CYBER KILL CHAIN

# Assume Compromise

# Genesis Market Offered Access to Data Stolen From Over 1.5M Compromised Computers Worldwide and Was a Key Enabler of Ransomware



# THIS WEBSITE HAS BEEN SEIZED

## OPERATION COOKIE MONSTER

Genesis Market's domains have been seized by the FBI pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Wisconsin. These seizures were possible because of international law enforcement and private sector coordination involving the partners listed below.

To determine if you have been victimized haveibeenpwned.com or politie.nl/checky

Been active on Genesis Market? In contact with Genesis I
Email us, we're interested: FBIMW-Genesis

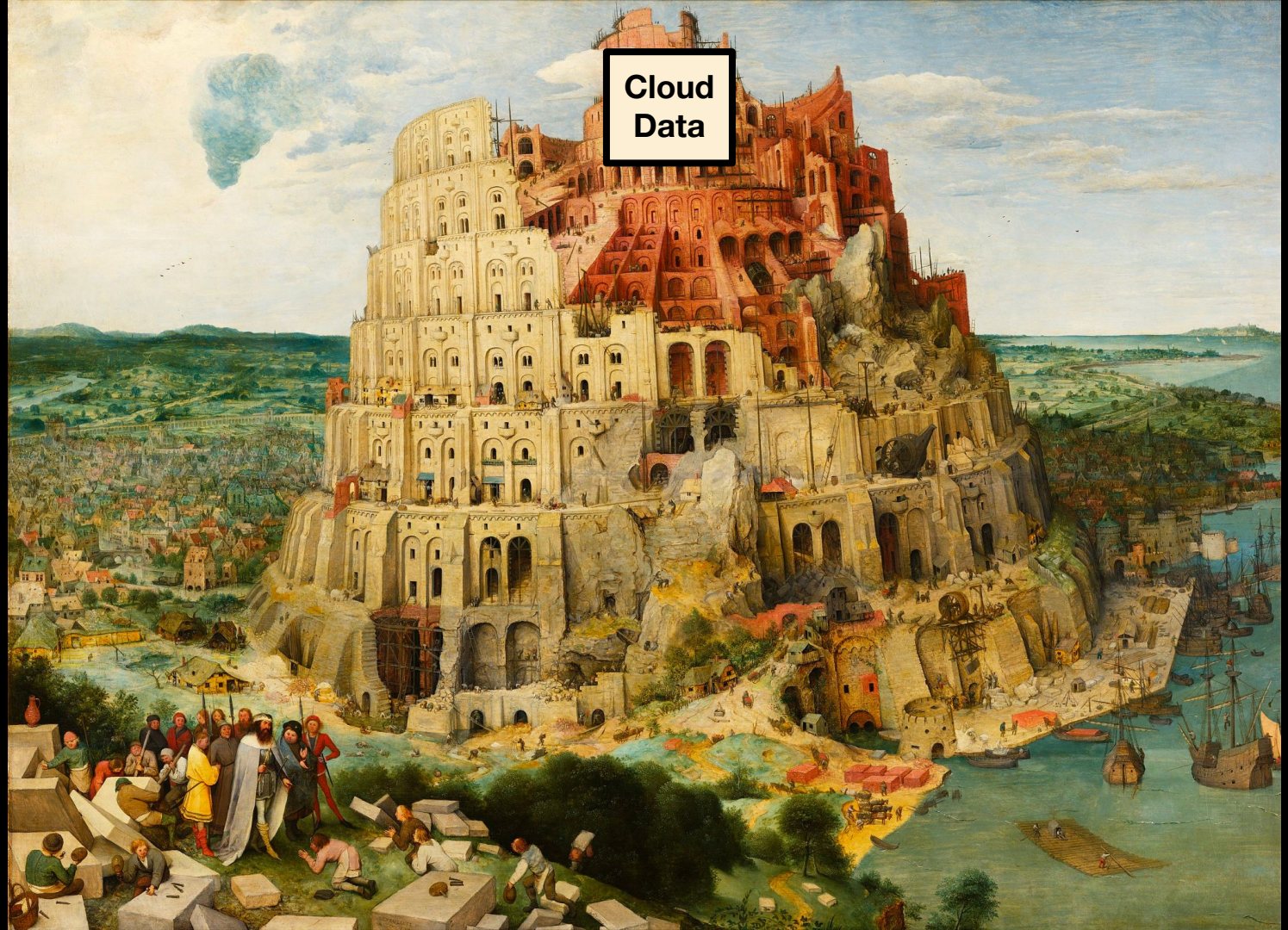


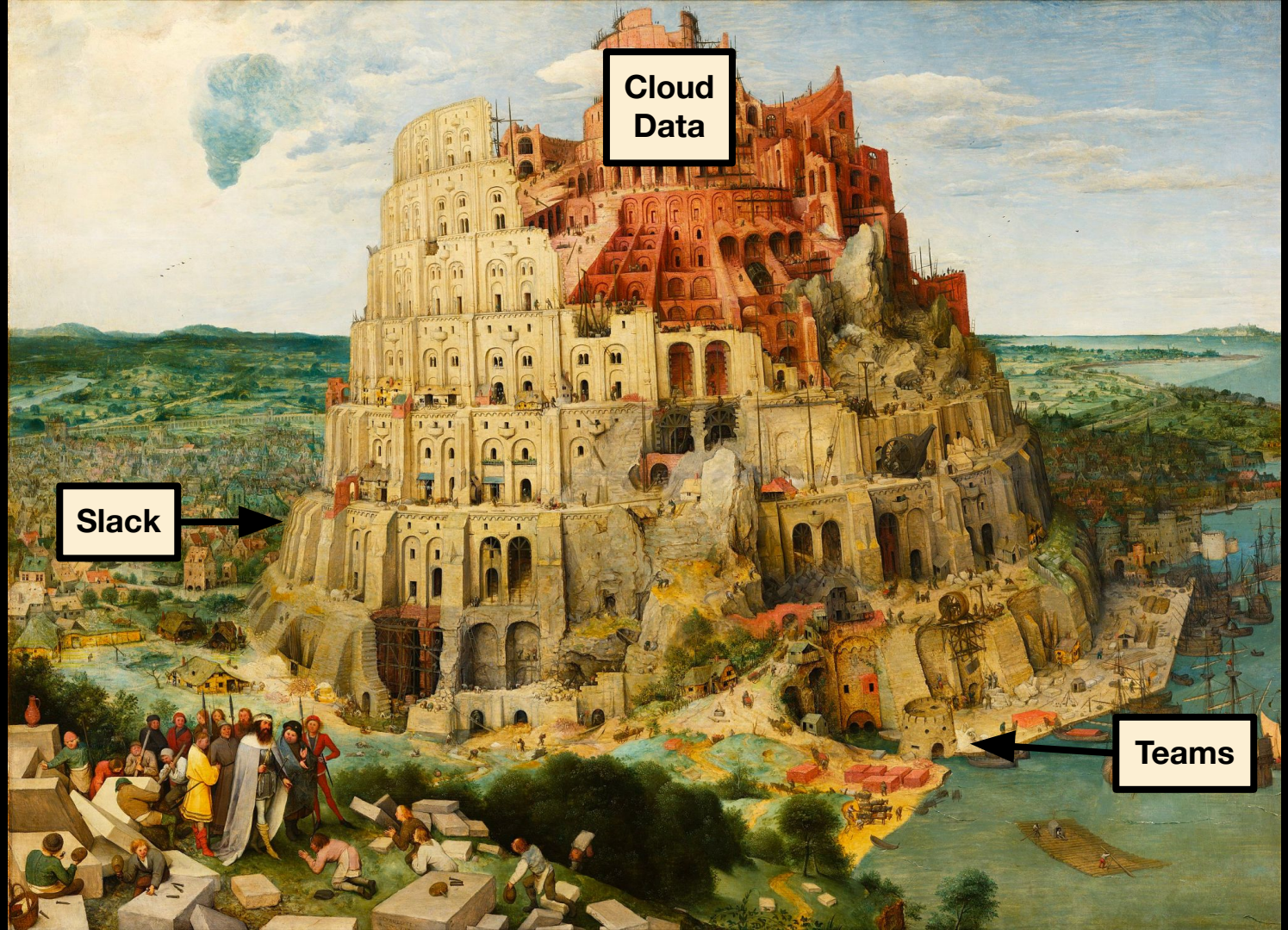
POLITI
AFP
CBZC
GUARDIA CIVIL
NCA National Crime Agency
Federal Criminal Police Office
EUROPOL
EUROJUST
POLIISI
KESKUSRIKOSPOLIISI
Centralkriminalpolisen
National Bureau of Investigation
POLITIE
Polisen
Swedish Police
Qintel

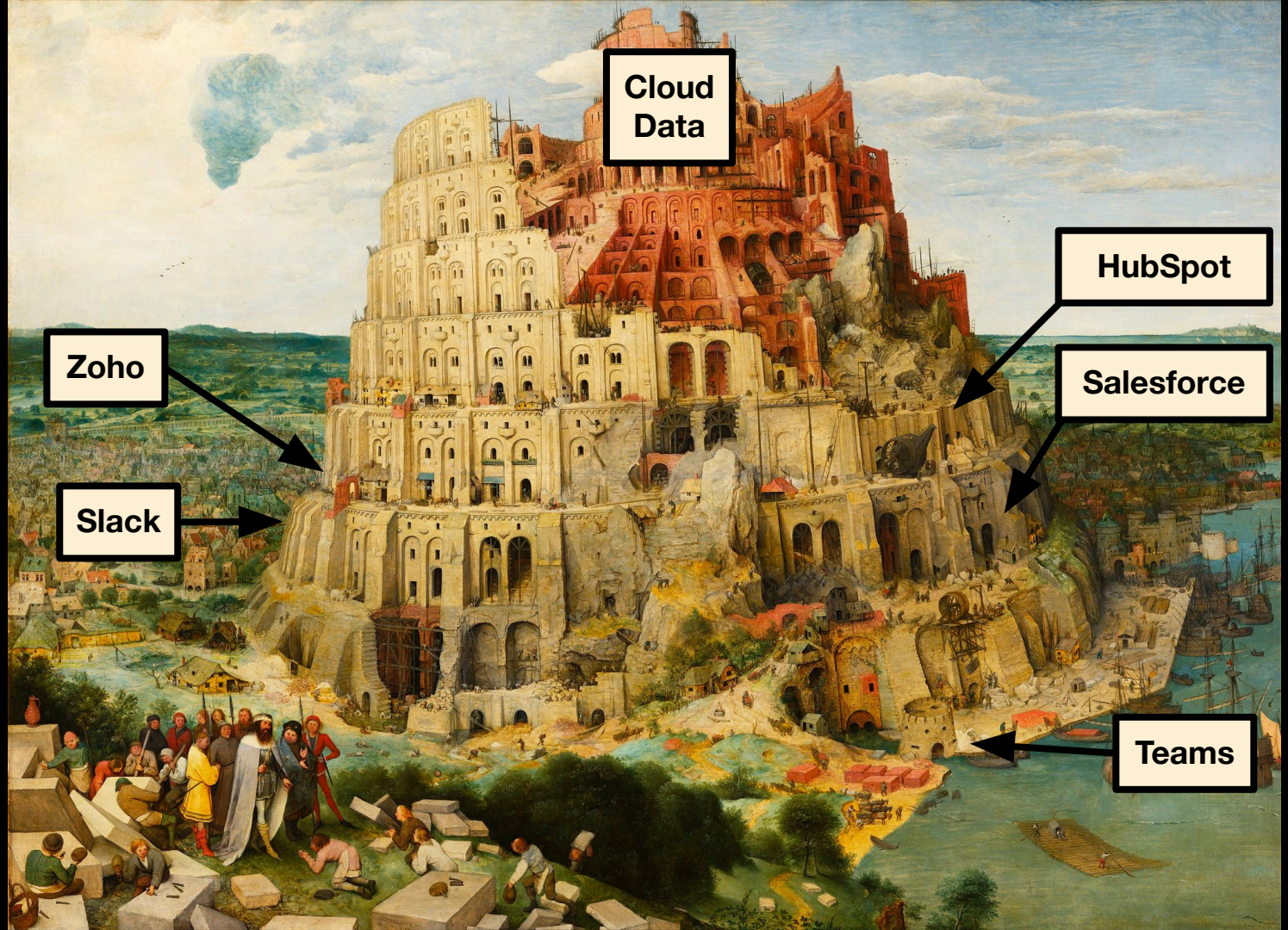
# Threat Actors don’t want shells*

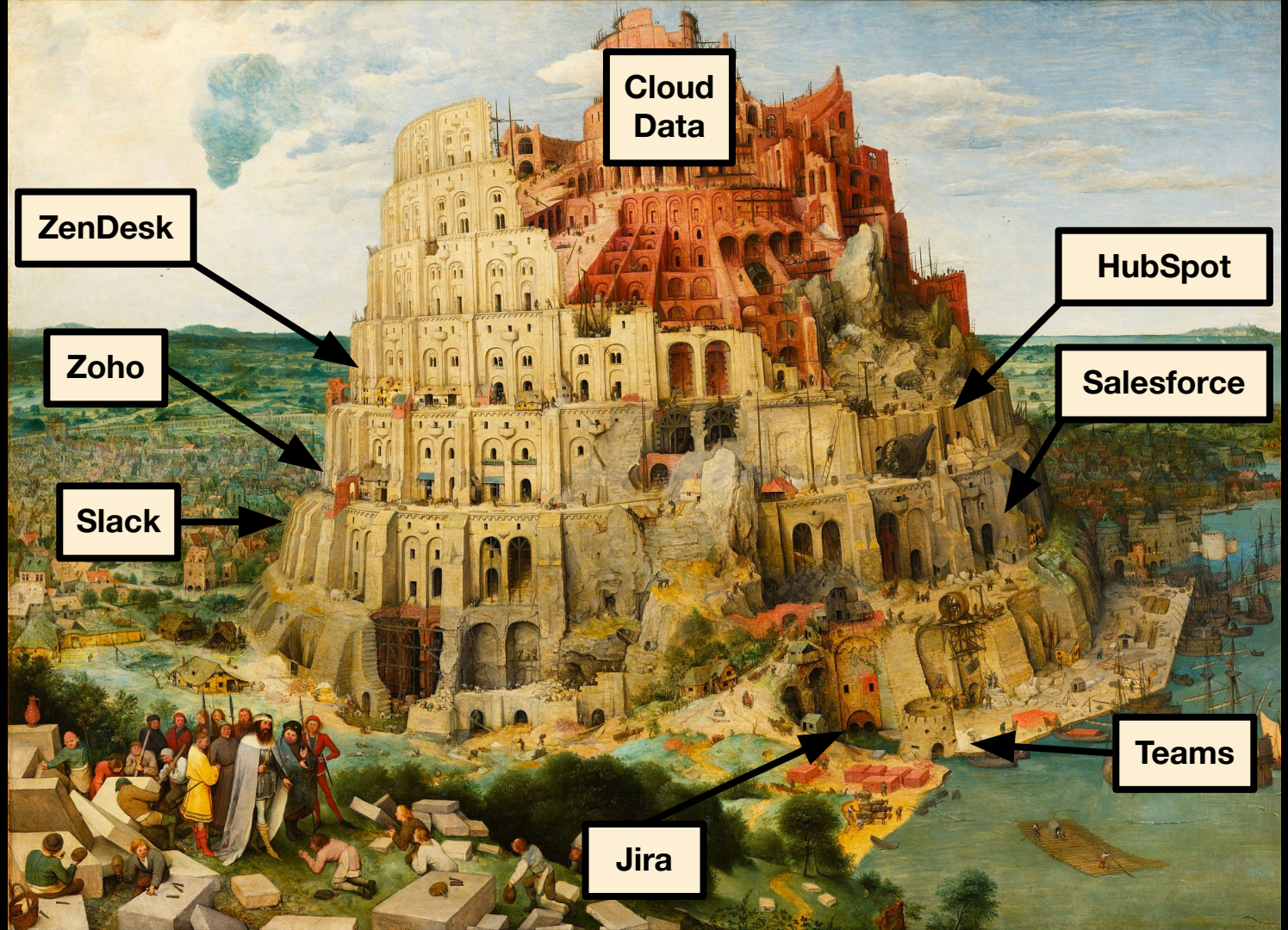
-

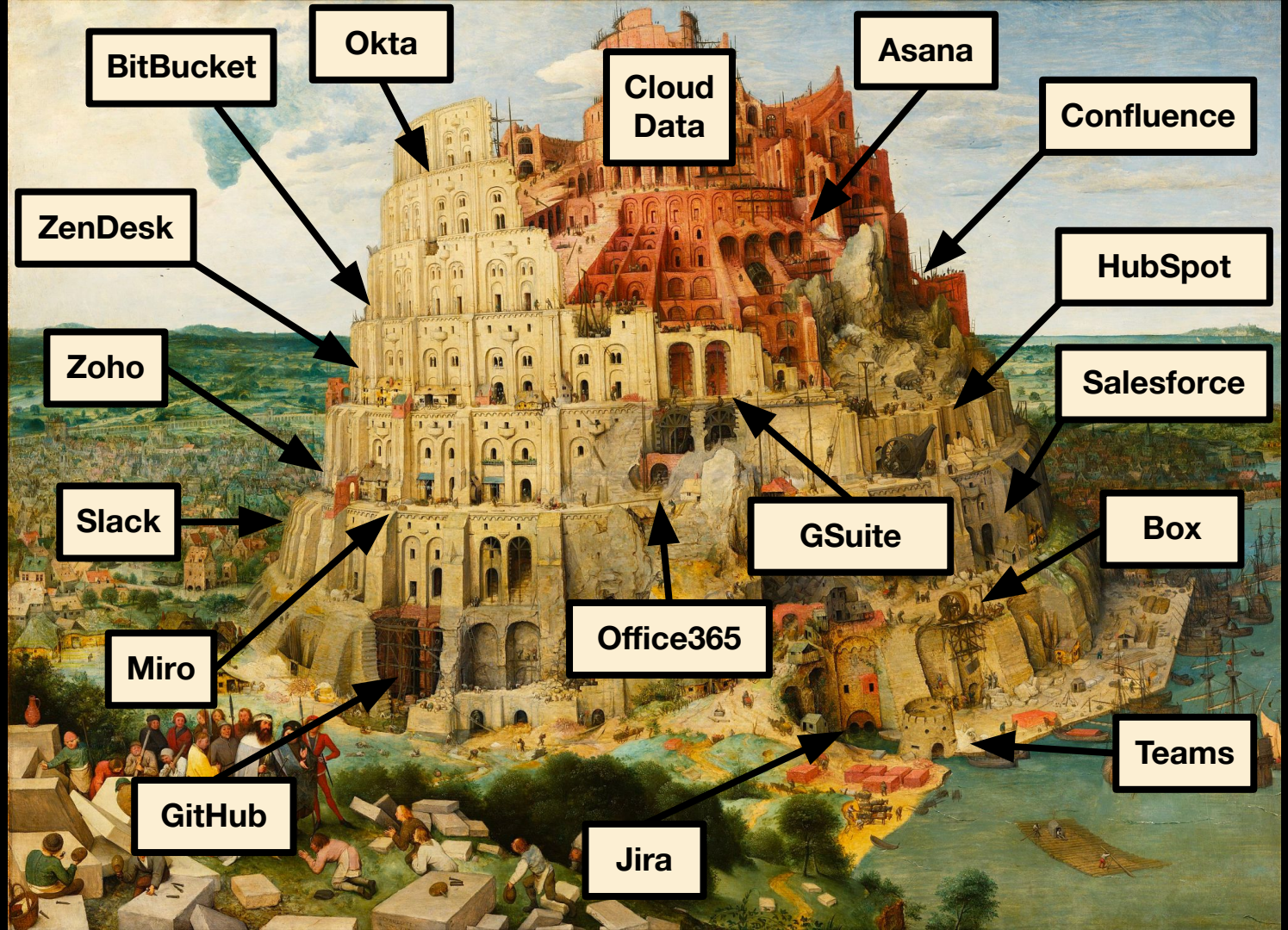
# They want <u>access to Data</u>

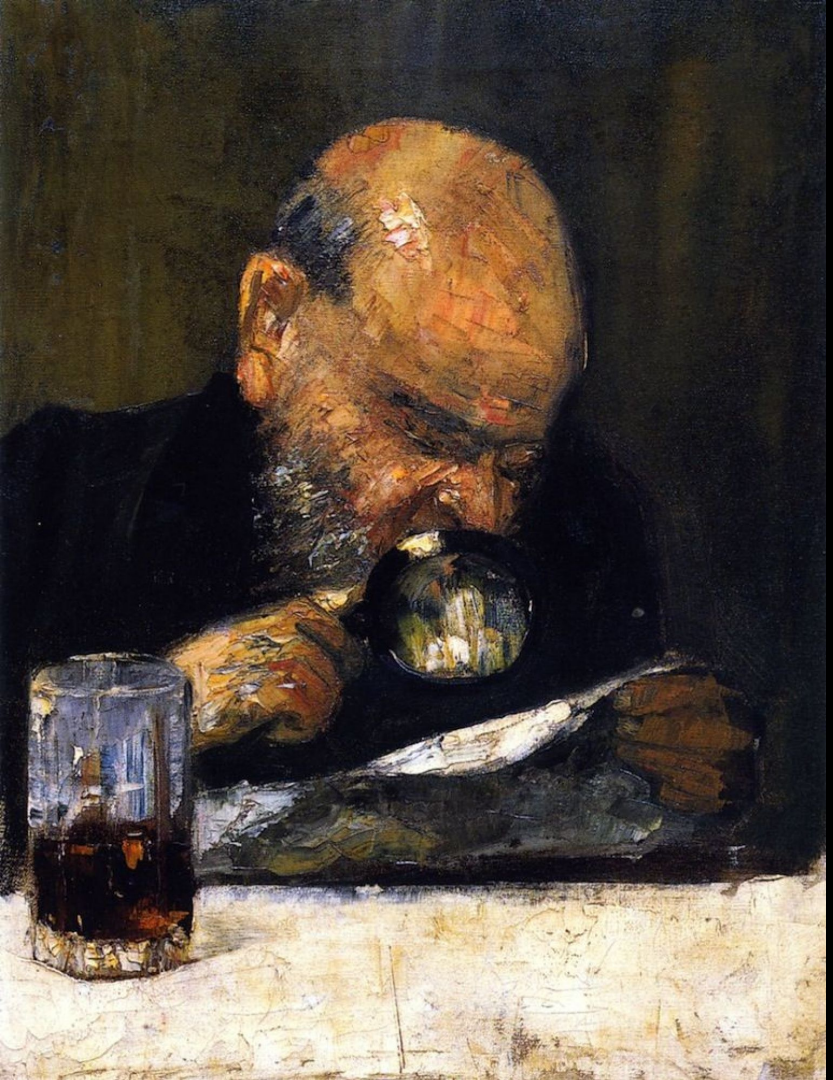

Cloud
Data


Cloud
Data
Slack
Teams

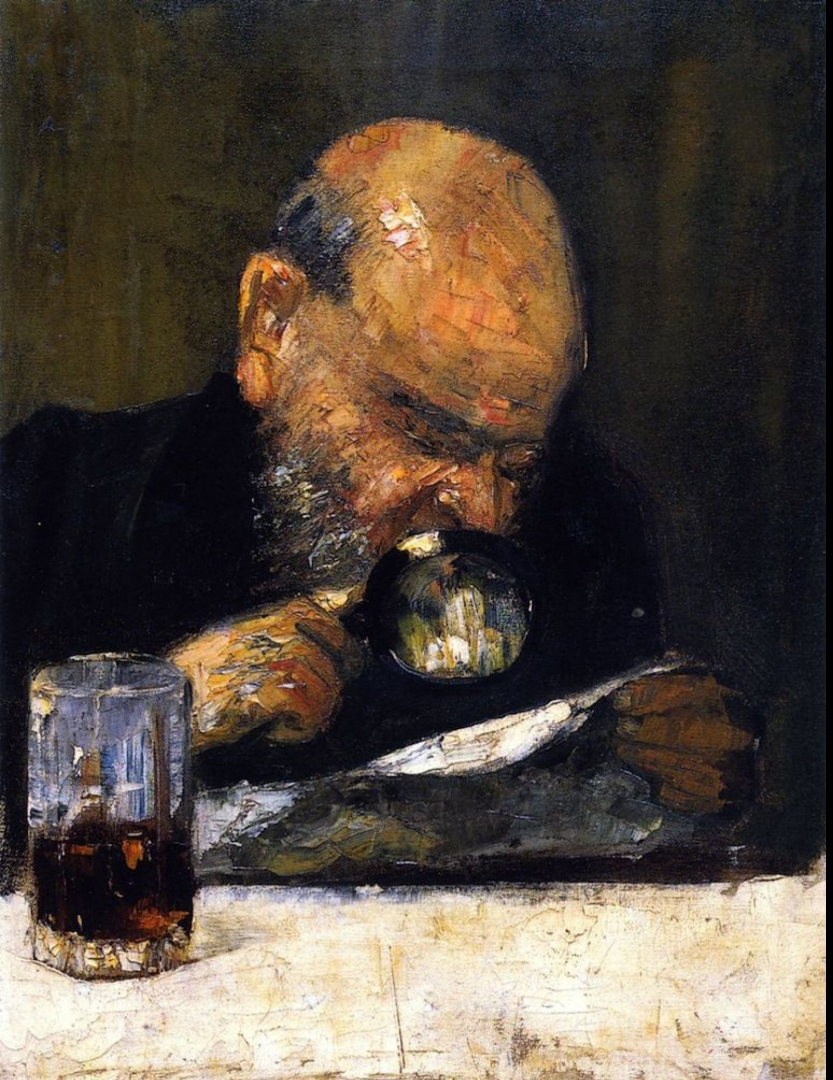

Cloud Data
HubSpot
Zoho
Salesforce
Slack
Teams


Cloud Data
ZenDesk
Zoho
Slack
HubSpot
Salesforce
Teams
Jira


BitBucket
Okta
Cloud Data
Asana
Confluence
ZenDesk
HubSpot
Zoho
Salesforce
Slack
GSuite
Box
Office365
Miro
Teams
GitHub
Jira

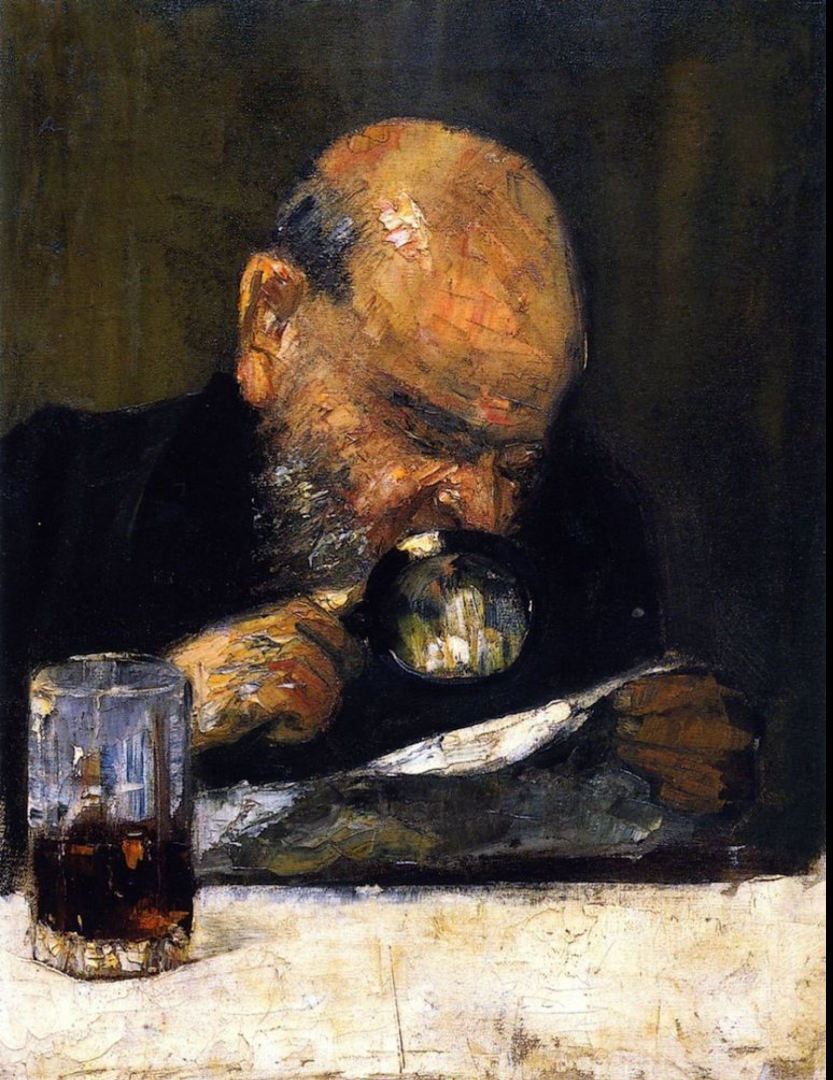


# Detection Engineering 101



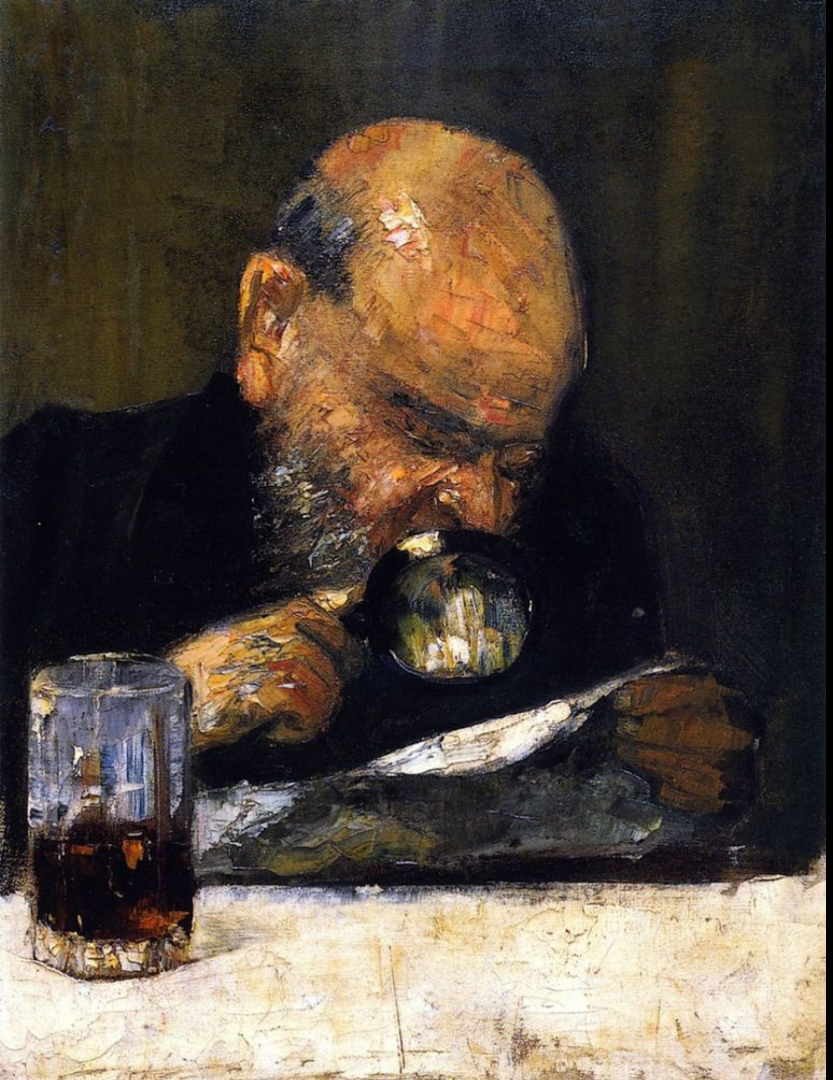
# Detection Engineering 101

- Find all the devices connected to your organization



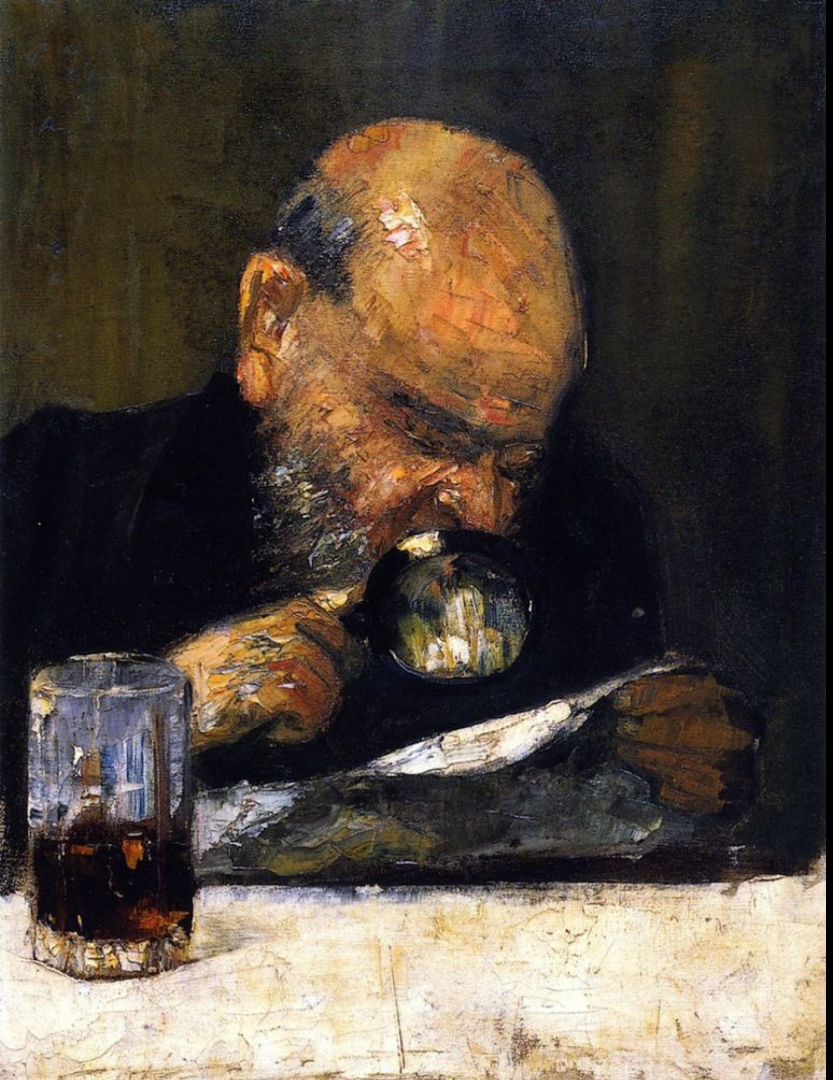
# Detection Engineering 101

- Find all the devices connected to your organization
- Find all the cloud services used in your organization



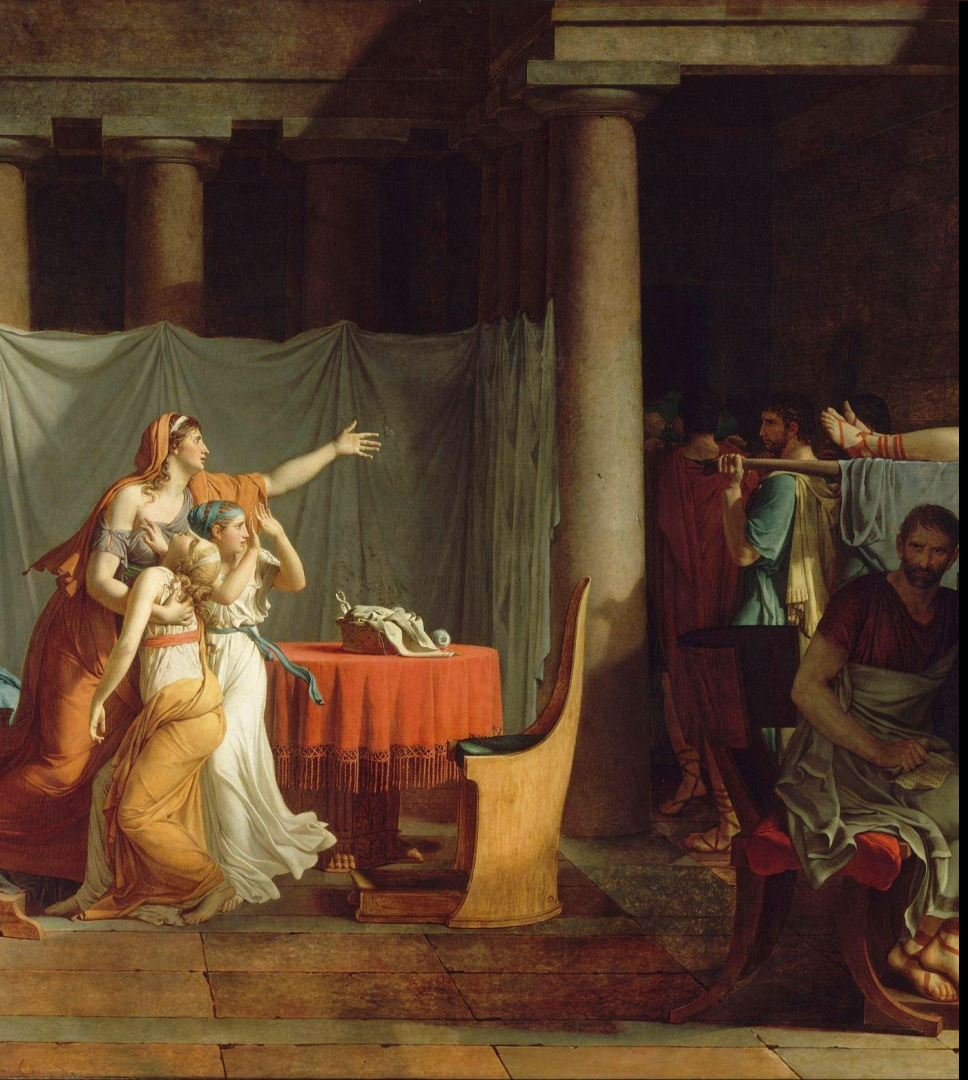
# Detection Engineering 101

- Find all the devices connected to your organization
- Find all the cloud services used in your organization
- Forward logs into a centralized, searchable, portal

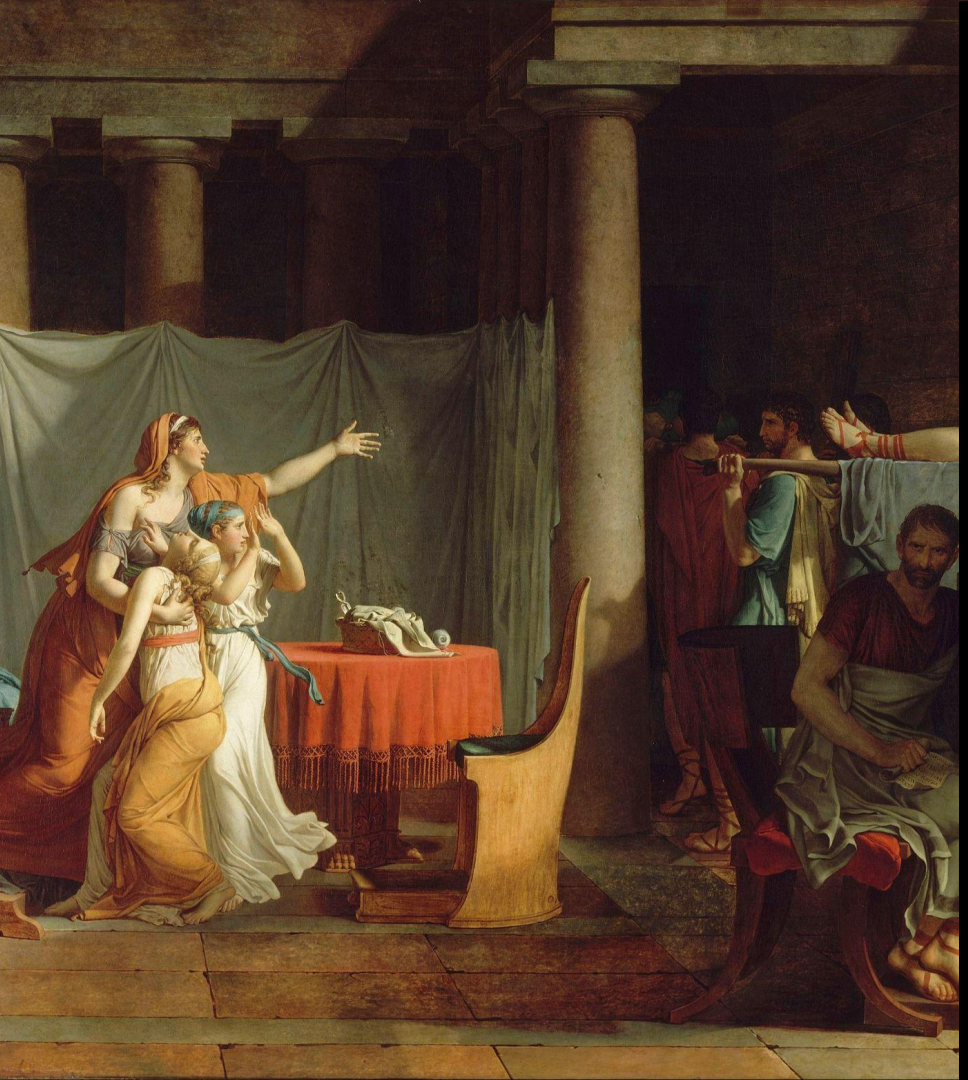


# Detection Engineering 101

- Find all the devices connected to your organization
- Find all the cloud services used in your organization
- Forward logs into a centralized, searchable, portal
- Correlate, correlate, correlate!

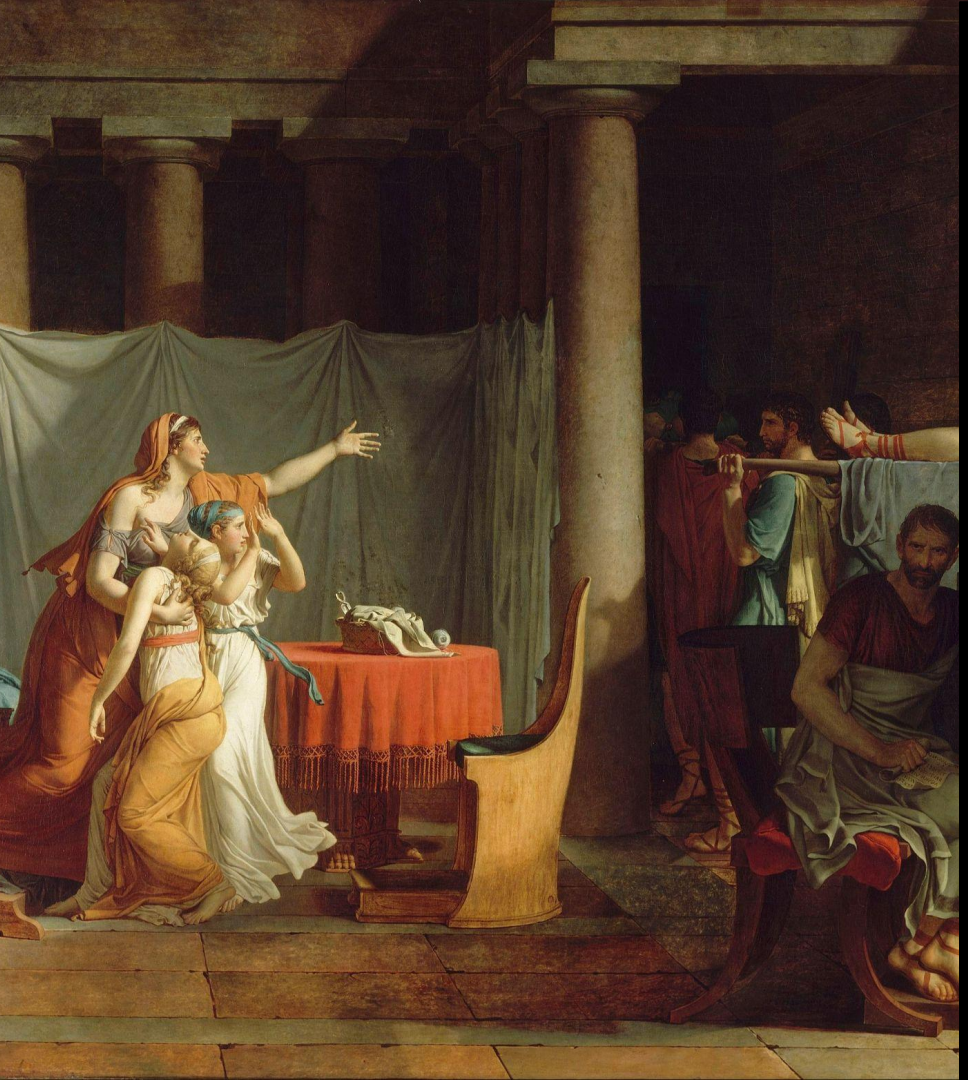


# Audit Logs



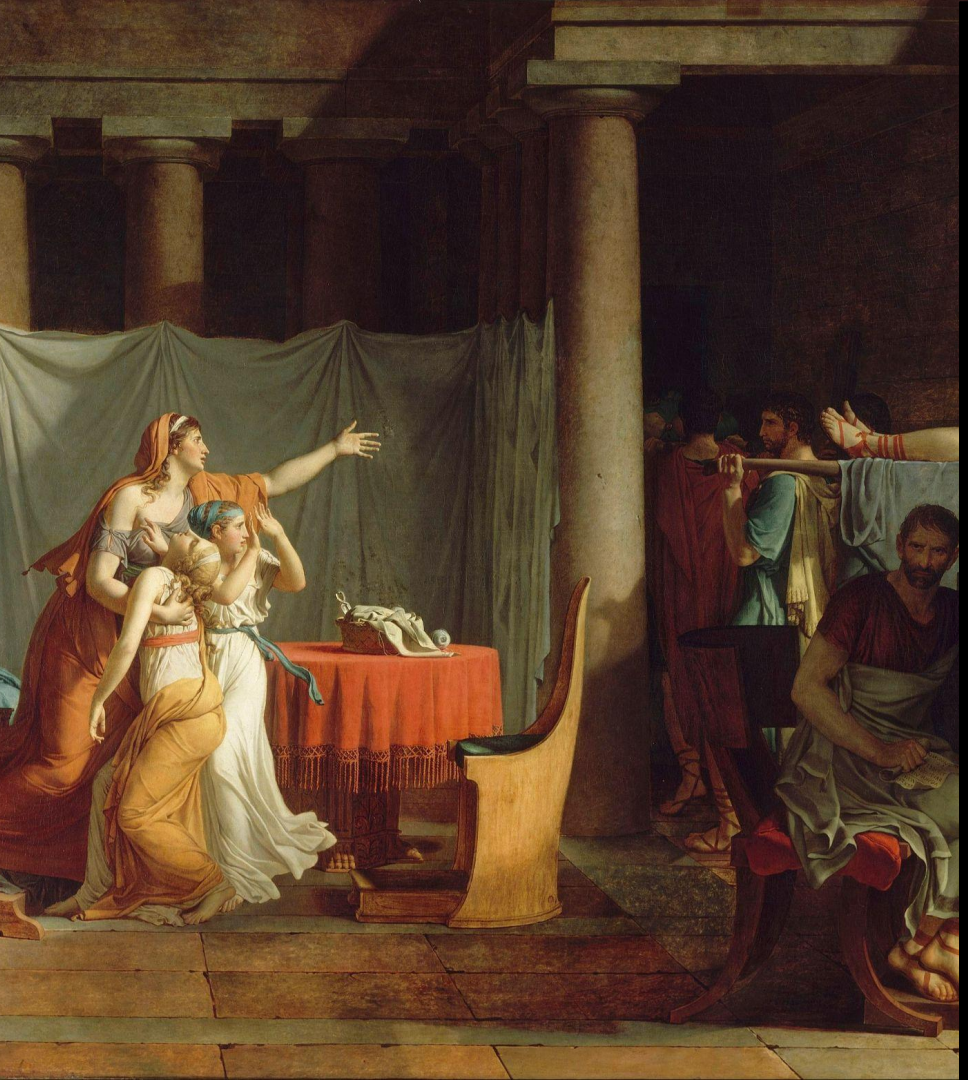
# Audit Logs

- Often cost extra $$$
  Ensure they’re budgeted for



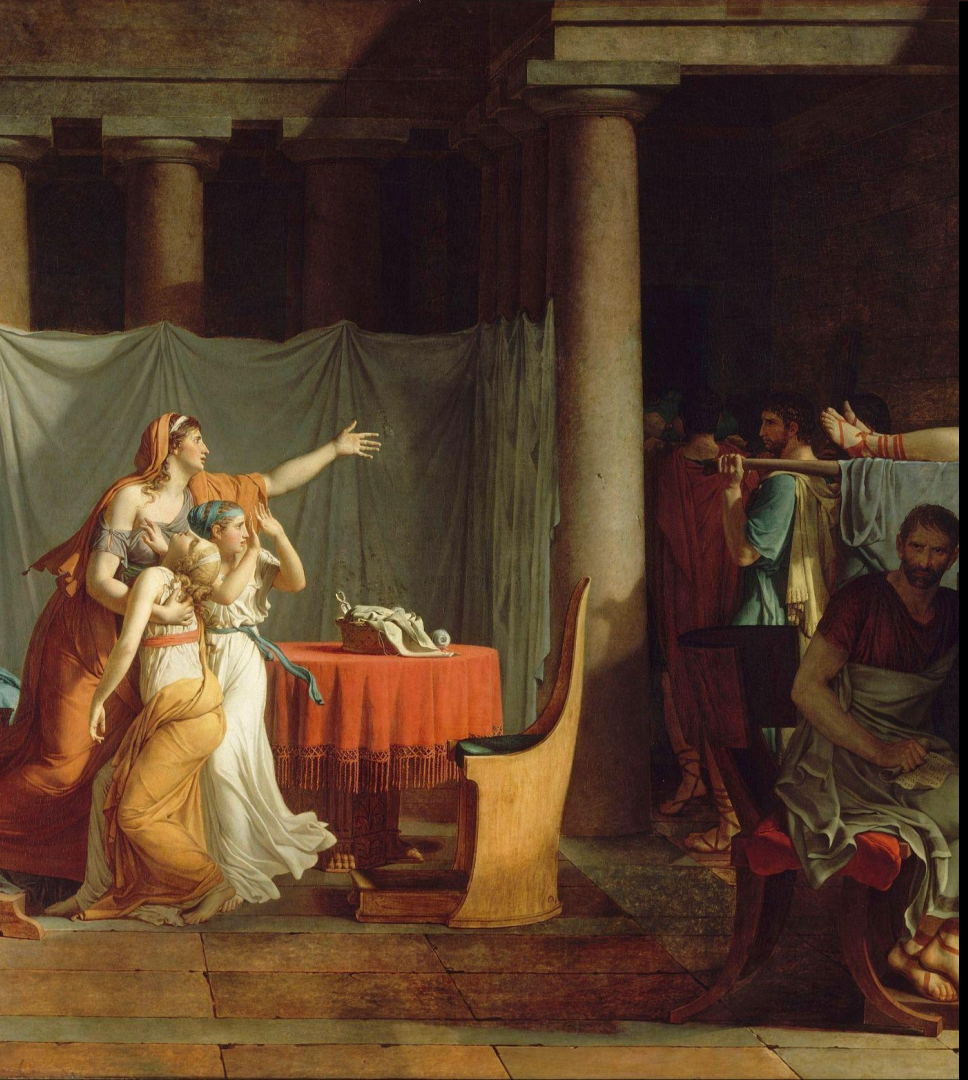
# Audit Logs

- Often cost extra $$$
  Ensure they're budgeted for
- May require apps, scripts, or addt'l steps to acquire



# Audit Logs

- Often cost extra $$$
  Ensure they're budgeted for
- May require apps, scripts, or addt'l steps to acquire
- Often need expertise to fully understand



## Audit Logs

- Often cost extra $$$
  Ensure they're budgeted for
- May require apps, scripts, or addt'l steps to acquire
- Often need expertise to fully understand
- Analysts may lack app permissions to administer

# Audit Logs

# Audit Logs

- Record *who* did *what*, *when*, within an application

# Audit Logs

- Record *who* did *what*, *when*, within an application
- Help create a narrative and timeline of activity

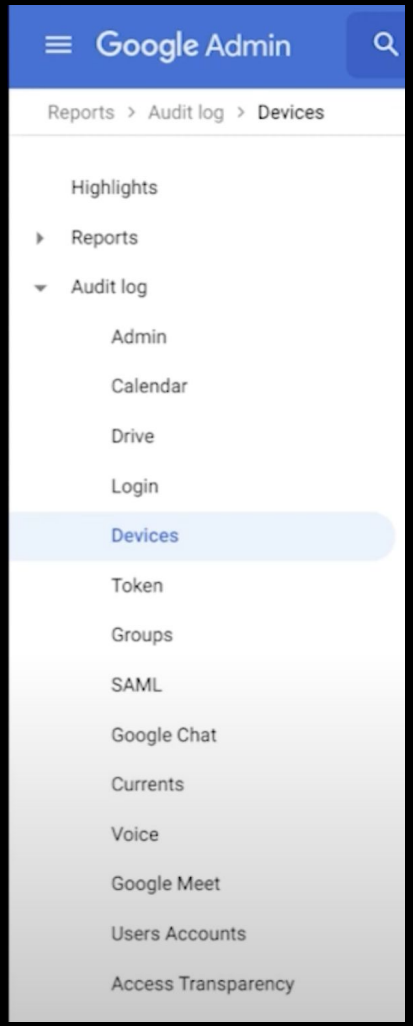
# Audit Logs

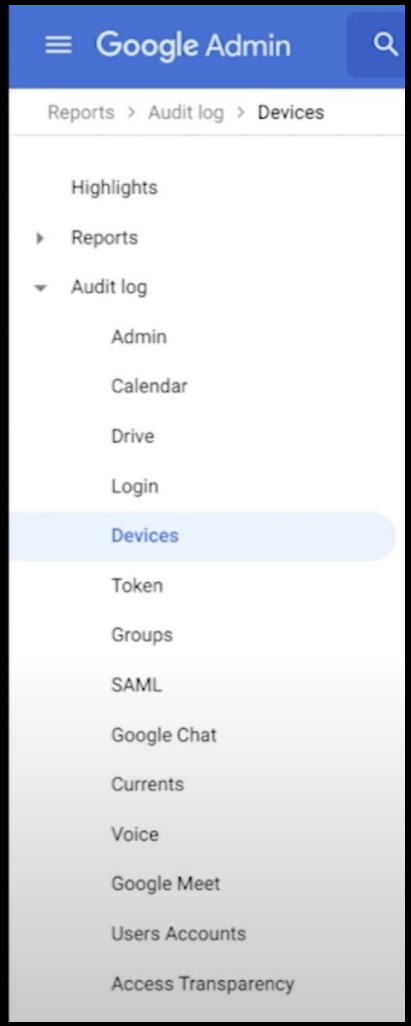
- Record *who* did *what*, *when*, within an application
- Help create a narrative and timeline of activity
- Often the only evidence of specific activity

# Audit Logs

- Record *who* did *what*, *when*, within an application
- Help create a narrative and timeline of activity
- Often the only evidence of specific activity
- Unfeasible for threat actors to evade or wipe

# Audit Log Examples


Google Admin
Reports > Audit log > Devices
Highlights
Reports
Audit log
Admin
Calendar
Drive
Login
Devices
Token
Groups
SAML
Google Chat
Currents
Voice
Google Meet
Users Accounts
Access Transparency



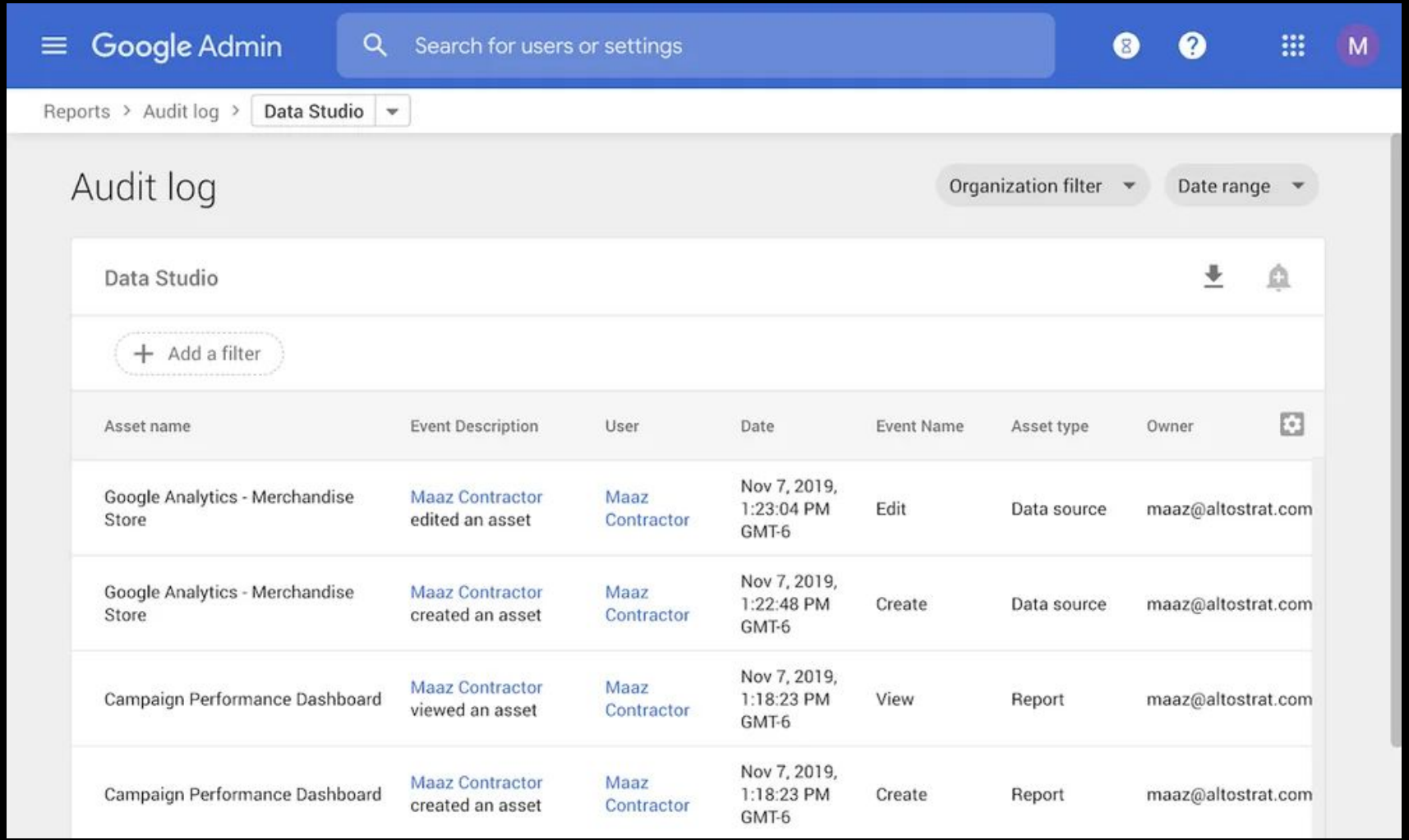

# Audit log

Organisational unit | Group filter | Date range

## Devices

+ Add a filter

| Device Id | Event Description | Date | Event Name | User | Device Type | Application hash | Policy Sta |
|---|---|---|---|---|---|---|---|
| fddd5ee2-0c4f-4ca2-a028-04193afe1209 | John Doe's account synced on **nami** | 9 Mar 2021, 07:37:01 GMT+8 | Device Sync | John Doe | Desktop Chrome | | |
| 314b2d2b5fe67554 | Joseph Yeo's account **registered on SM-G955N with device administrator privilege** | 9 Mar 2021, 06:57:00 GMT+8 | Account registration change | Joseph Yeo | Android | | |
| 6c64b5a2-4b63-4f52-b601-e112b71473e4 | Sally Chong's account synced on **nami** | 9 Mar 2021, 00:26:15 GMT+8 | Device Sync | Sally Chong | Desktop Chrome | | |
| 86acd673-4894-4634-9950-5d12f9a64b58 | Hu Fengshan Sheralyn's account synced on **nami** | 8 Mar 2021, 22:21:47 GMT+8 | Device Sync | Hu Fengshan Sheralyn | Desktop Chrome | | |
| 1d6c0234-244f-43c6-a9ca-36ee444a5183 | Joseph Yeo's account synced on **nami** | 8 Mar 2021, 20:49:54 GMT+8 | Device Sync | Joseph Yeo | Desktop Chrome | | |
| 084cacff-b677-4310-9d9a-b5a5c410f5cc | Jonathan Lim's account synced on **nami** | 8 Mar 2021, 17:41:37 GMT+8 | Device Sync | Jonathan Lim | Desktop Chrome | | |


Google Admin
Search for users or settings
M
Reports > Audit log > Data Studio
Audit log
Organization filter
Date range
Data Studio
Add a filter
Asset name
Event Description
User
Date
Event Name
Asset type
Owner
Google Analytics - Merchandise Store
Maaz Contractor edited an asset
Maaz Contractor
Nov 7, 2019, 1:23:04 PM GMT-6
Edit
Data source
maaz@altostrat.com
Google Analytics - Merchandise Store
Maaz Contractor created an asset
Maaz Contractor
Nov 7, 2019, 1:22:48 PM GMT-6
Create
Data source
maaz@altostrat.com
Campaign Performance Dashboard
Maaz Contractor viewed an asset
Maaz Contractor
Nov 7, 2019, 1:18:23 PM GMT-6
View
Report
maaz@altostrat.com
Campaign Performance Dashboard
Maaz Contractor created an asset
Maaz Contractor
Nov 7, 2019, 1:18:23 PM GMT-6
Create
Report
maaz@altostrat.com

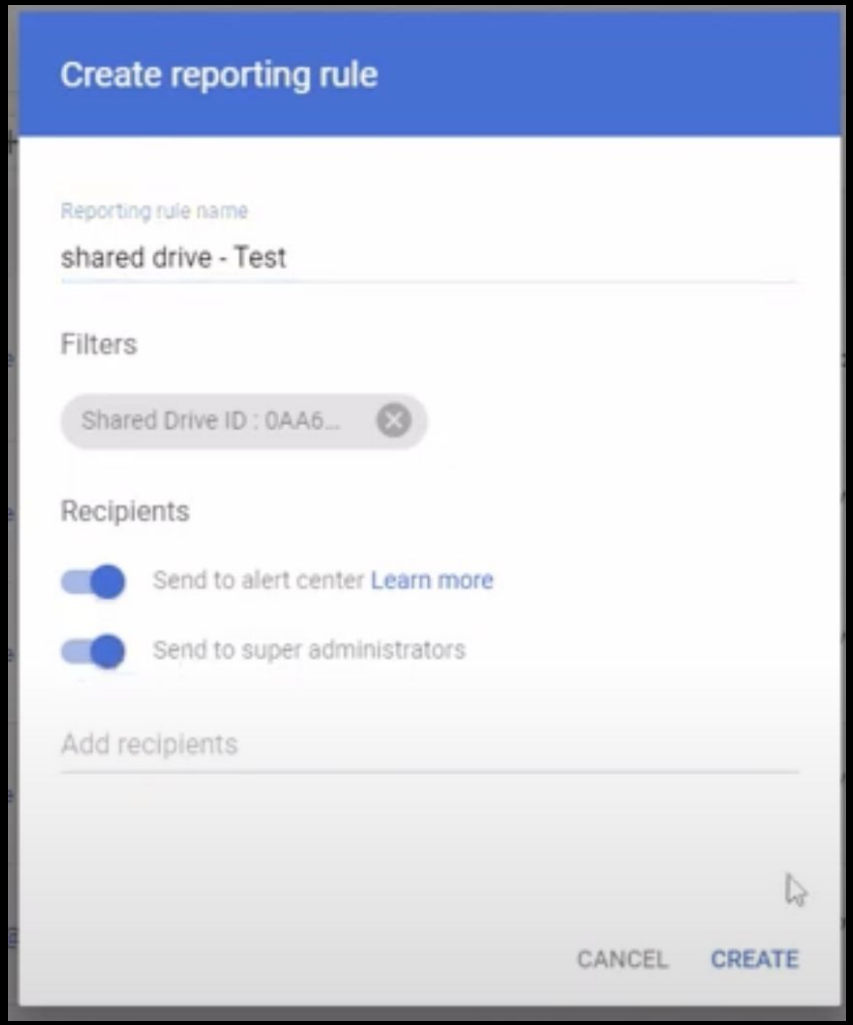
# Audit log

Organizational unit | Group filter | Date range

Drive

Shared Drive ID: "0AA6h9EEpubKPUk9PVA" | CLEAR FILTERS

| Title | Event Description | User | Date | Event | Document ID | Document type | Owner | Prior visibility | Visibility |
|---|---|---|---|---|---|---|---|---|---|
| Test Between Roger's | Gsuite admin made a membership change of type **Remove** for **roger@centralcoastrealestateco.com** by removing role(s) **Content manager** and adding role(s) **None** | Gsuite admin | Nov 24, 2021, 1:19:09 PM CST | Shared Drive Membership Change | 0AA6h9EEpubKPUk9PVA | Shared drive | Test Between Roger's | | Shared Internally |
| Test from GSuite Admin | Gsuite admin changed link sharing visibility from **Private** to **Anyone with the link within the audience** for **hiviewdev.com** | Gsuite admin | Aug 25, 2021, 10:50:12 AM CST | Link Sharing visibility change | 11z6Y1o5c4VPyHbbJjXf_Enj0pl9nj9BGbH0Yx_ahRJA | Google Docs | Test Between Roger's | Shared Externally | Shared Externally |
| Test from GSuite Admin | Gsuite admin changed link sharing access type from **None** to **Can view** for **hiviewdev.com** | Gsuite admin | Aug 25, 2021, 10:50:12 AM CST | Link Sharing Access Type Change | 11z6Y1o5c4VPyHbbJjXf_Enj0pl9nj9BGbH0Yx_ahRJA | Google Docs | Test Between Roger's | Shared Externally | Shared Externally |
| Test from GSuite Admin | Gsuite admin edited an item | Gsuite admin | Aug 5, 2021, 10:36:47 AM CST | Edit | 11z6Y1o5c4VPyHbbJjXf_Enj0pl9nj9BGbH0Yx_ahRJA | Google Docs | Test Between Roger's | | Shared Externally |
| Test From Roger's | roger@centralcoastrealestateco.com edited an item | roger@centralcoastrealestateco.com | Aug 5, 2021, 10:36:22 AM CST | Edit | 1UhR8q8SKtbwGOlSOCDLpOt8HxYgBD8ohppMYodyq08U | Google Docs | Test Between Roger's | | Shared Externally |
| Test from GSuite Admin | Gsuite admin edited an item | Gsuite admin | Aug 5, 2021, 10:33:46 AM CST | Edit | 11z6Y1o5c4VPyHbbJjXf_Enj0pl9nj9BGbH0Yx_ahRJA | Google Docs | Test Between Roger's | | Shared Externally |


Create reporting rule
Reporting rule name
shared drive - Test
Filters
Shared Drive ID : 0AA6...
Recipients
Send to alert center Learn more
Send to super administrators
Add recipients
CANCEL
CREATE

Rules | Create rule | Templates | Investigate | Download

+ Add a filter

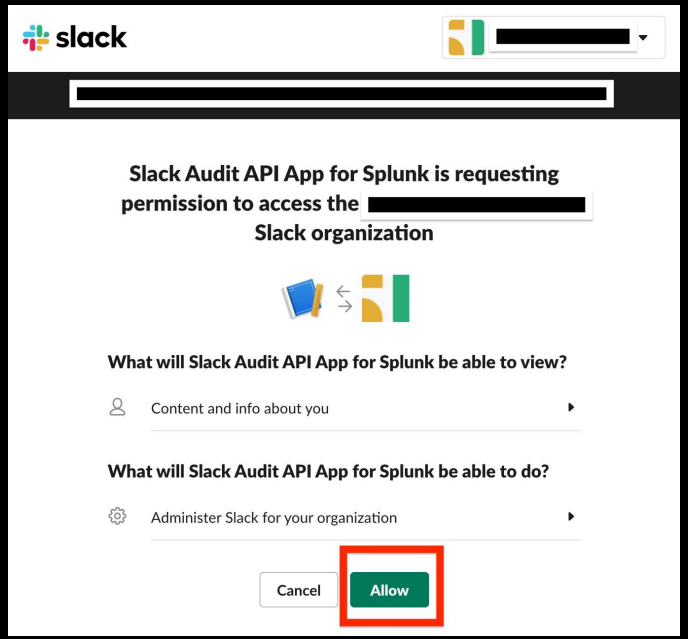
| Name | Status | Actions | Alerts | Rule type |
|---|---|---|---|---|
| shared drive - Test<br>Custom reporting alert | Active | Send Notification | On | Reporting |
| important document<br>Custom reporting alert | Active | Send Notification | On | Reporting |
| shared outside<br>Custom reporting alert | Active | Send Notification | On | Reporting |
| important confidential doc<br>Custom reporting alert | Active | Send Notification | On | Reporting |
| Prevent PII information sharing (US)<br>Protect your organization from leaking PII data (US) | Inactive | Block external sharing | On | Data protection |
| failed login<br>Custom reporting alert | Active | Send Notification | On | Reporting |
| Prevent PII information sharing (US)<br>Protect your organization from leaking PII data (US) | Inactive | Block external sharing | On | Data protection |
| Test | Active | Send to quarantine | On | Activity |
| Prevent financial information sharing (International)<br>Protect your organization from leak of financial information (Internation... | Inactive | Block external sharing | On | Data protection |

# Slack Audit App for Splunk

The Slack Audit App for Splunk provides interactive searches and visualizations for monitoring what is happening in your Enterprise Grid organization. It works in conjunction with the Slack Add-on for Splunk, which is used to retrieve Slack Audit logs for your organization. While this…

Built by Splunk Works

Login to Download



IP [redacted] There were 2 additional logins from this device, with the most recent at 10:14.

**Henry**
10:14 with the Android App
IP [redacted]

**Taylor**
10:13 with the Mac Desktop App
IP [redacted] There were 3 additional logins from this device, with the most recent at 10:13.

**mark**
10:06 from App Donut
IP [redacted]

**mark**
10:06 from App Donut
IP [redacted]

**mark**
10:06 from App Donut
IP [redacted]

**Kathleen**
10:06 with the Mac Desktop App
IP [redacted] There were 2 additional logins from this device, with the most recent at 10:06.

**max**
10:06 with the Android App
IP [redacted] There was one additional login from this device, at 10:06.

**quip**
10:03 from App Quip
IP [redacted]

**max**
10:01 from App WorkOS
IP [redacted]

Copy


```
{
   "entries":[
      {
         "id":"0123a45b-6c7d-8900-e12f-3456789gh0i1",
         "date_create":1521214343,
         "action":"user_login",
         "actor":{
            "type":"user",
            "user":{
               "id":"W123AB456",
               "name":"Charlie Parker",
               "email":"bird@slack.com"
            }
         },
         "entity":{
            "type":"user",
            "user":{
               "id":"W123AB456",
               "name":"Charlie Parker",
               "email":"bird@slack.com"
            }
         },
         "context":{
            "location":{
               "type":"enterprise",
               "id":"E1701NCCA",
               "name":"Birdland",
               "domain":"birdland"
            },
            "ua":"Mozilla\/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/64.0.3282.1
            "session_id": "847288190092",
            "ip_address":"1.23.45.678"
         }
      }
    ]
}
```

```
    },
    "context": {
        "location": {
            "type": "workspace",
            "id": "T123ABC456",
            "name": "birdland",
            "domain": "birdland"
        },
        "ua": "Mozilla\/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/64.0.3282.1
        "ip_address": "1.23.45.678",
        "session_id": null,
        "app": {
            "id": "AT123AB456",
            "name": "Channel Spinner App",
            "scopes": [],
            "scopes_bot": [
               "channels:manage",
               "groups:write",
               "im:write",
               "mpim:write"
            ],
            "creator": "W123ABC456",
            "team": "T123ABC456"
```

# User

| Action | Description |
| --- | --- |
| `anomaly` | An anomalous user behavior was detected. |
| `custom_tos_accepted` | A team member accepted a custom terms of service agreement. |
| `guest_created` | A guest was created. |
| `guest_deactivated` | A guest was deactivated. |
| `guest_expiration_cleared` | A guest had an expiration time cleared (before this time arrived). |
| `guest_expiration_set` | A guest had an account expiration time set. |
| `guest_expired` | A guest was deactivated when the expiration time was reached. |
| `guest_joined_workspace` | A guest joined a workspace. |
| `guest_reactivated` | A guest was reactivated after having been deactivated. |
| `owner_transferred` | An owner was transferred. |
| `permissions_assigned` | A team member was assigned a permission. |
| `permissions_removed` | A team member was unassigned a permission. |
| `role_assigned` | A team member was assigned a role. |
| `role_change_to_admin` | A team member was made an admin. |

# App

| Action | Description |
| --- | --- |
| `app_approved` | On workspaces that have admin approved apps enabled, an app has been approved but not yet installed. |
| `app_installed` | An app has been installed. If a custom integration had been disabled, this event will also be triggered if it is re-enabled. |
| `app_removed_from_whitelist` | An app was removed from the allowed list. |
| `app_resources_added` | Workspace apps have the ability to request access to a specific resource on a workspace, such as a channel or a DM, including wildcard resources (such as all public channels). This event is triggered when access has been granted. |
| `app_resources_granted` | An app resource was granted. |
| `app_restricted` | On workspaces that have admin approved apps enabled, an app has been restricted and cannot be installed. |
| `app_scopes_expanded` | An app has been granted additional access to resources on a workspace, via OAuth scopes. For most apps, this requires a re-install. For workspace apps, this may also happen via the permissions API. |
| `app_token_preserved` | An app's token was preserved instead of revoked, usually due to an app owner or installer being removed from an organization. |
| `app_uninstalled` | A Slack app was uninstalled. |
| `bot_token_downgraded` | A bot app's token was downgraded to non-granular permissions. |
| `bot_token_upgraded` | A bot app's token was upgraded with granular permissions. |

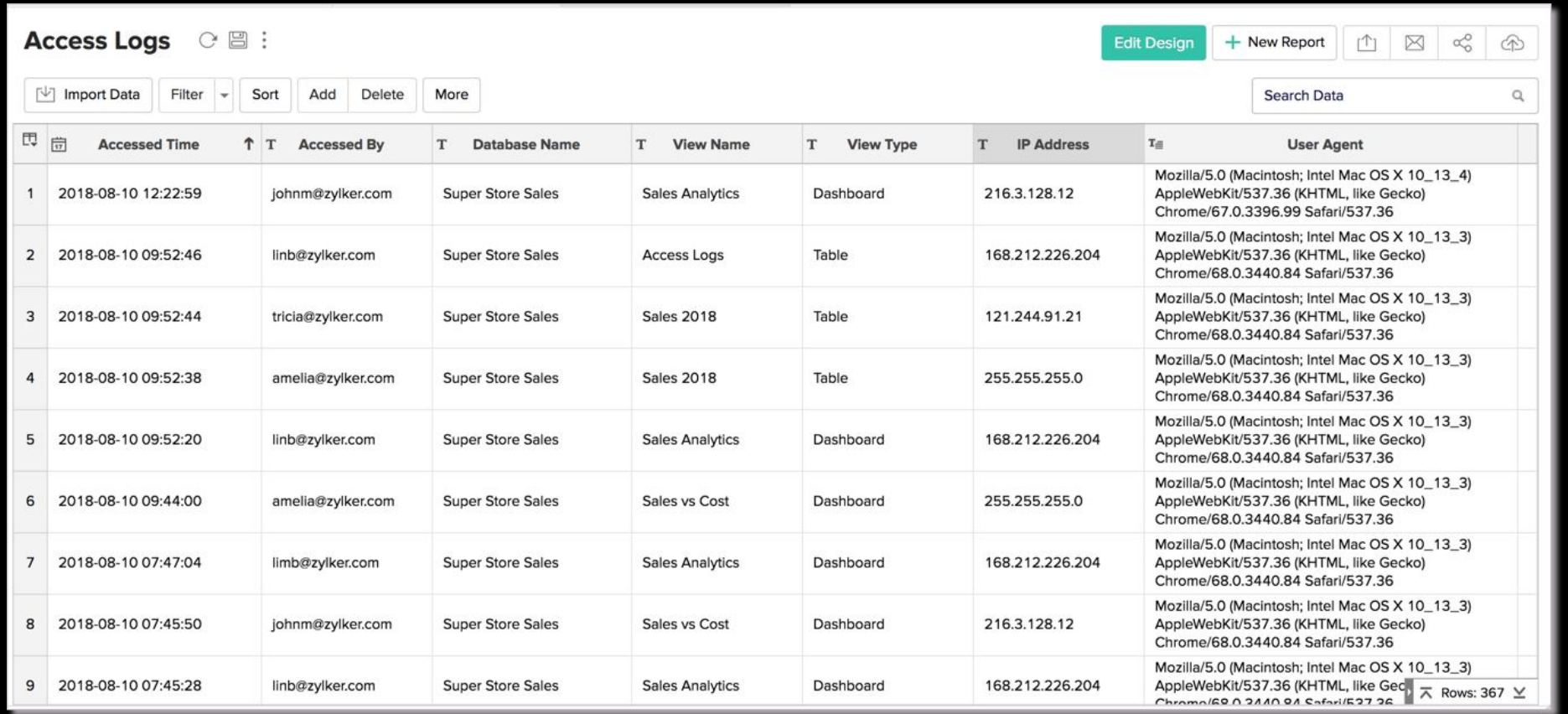
# File

| Action | Description |
| --- | --- |
| `file_deleted` | A file was deleted. |
| `file_download_blocked` | A file was blocked from being downloaded. |
| `file_downloaded` | A file was downloaded or viewed within Slack. |
| `file_malicious_content_detected` | Malware scanning found malicious content in the file. |
| `file_public_link_created` | A public link was created for a file. This action contains a `team` identifier so that you can see which team the creating user comes from (useful for externally shared channels). |
| `file_public_link_revoked` | A public link was revoked from a file. This action contains a `team` identifier so that you can see which team the revoking user comes from (useful for externally shared channels). |
| `file_shared` | A file was shared in another channel. This action contains a `team` identifier so that you can see which team the uploading user comes from (useful for externally shared channels). |
| `file_uploaded` | A file was uploaded. |

You can enable the API logs using the **API Logs** toggle button in the **Audit** tab.

An API Log table will be created in the Zoho Analytics Audits  workspace with the below columns.

- **Date** - Date activity was performed.
- **API Name** - Name of the API call
- **User EmailID** - Email address of the user who perfomed the activity.
- **Rows Processed** - Number of rows imported or exported.
- **Units Consumed** - API Units consumed by the call.
- **API Count** - Number of API count.
- **IP** - IP Address from where the user performed the activity.
- **Version** - Zoho Analytics API Version used
- **API Group** - The API grou the API action falles under such as Embed.



# Access Logs

Edit Design | + New Report

Import Data | Filter | Sort | Add | Delete | More

Search Data

| | Accessed Time | Accessed By | Database Name | View Name | View Type | IP Address | User Agent |
|---|---|---|---|---|---|---|---|
| 1 | 2018-08-10 12:22:59 | johnm@zylker.com | Super Store Sales | Sales Analytics | Dashboard | 216.3.128.12 | Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36 |
| 2 | 2018-08-10 09:52:46 | linb@zylker.com | Super Store Sales | Access Logs | Table | 168.212.226.204 | Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.84 Safari/537.36 |
| 3 | 2018-08-10 09:52:44 | tricia@zylker.com | Super Store Sales | Sales 2018 | Table | 121.244.91.21 | Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.84 Safari/537.36 |
| 4 | 2018-08-10 09:52:38 | amelia@zylker.com | Super Store Sales | Sales 2018 | Table | 255.255.255.0 | Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.84 Safari/537.36 |
| 5 | 2018-08-10 09:52:20 | linb@zylker.com | Super Store Sales | Sales Analytics | Dashboard | 168.212.226.204 | Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.84 Safari/537.36 |
| 6 | 2018-08-10 09:44:00 | amelia@zylker.com | Super Store Sales | Sales vs Cost | Dashboard | 255.255.255.0 | Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.84 Safari/537.36 |
| 7 | 2018-08-10 07:47:04 | limb@zylker.com | Super Store Sales | Sales Analytics | Dashboard | 168.212.226.204 | Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.84 Safari/537.36 |
| 8 | 2018-08-10 07:45:50 | johnm@zylker.com | Super Store Sales | Sales vs Cost | Dashboard | 216.3.128.12 | Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.84 Safari/537.36 |
| 9 | 2018-08-10 07:45:28 | linb@zylker.com | Super Store Sales | Sales Analytics | Dashboard | 168.212.226.204 | Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_3) AppleWebKit/537.36 (KHTML, like Gec |

Rows: 367

## Configure the capture of IP Address and source information

You can capture the **IP address and source information** of users who make changes to your application records as well as export and print reports. By default, the option to capture IP Address and source information will be **disabled**. You can choose to enable it in the Settings tab as follows:

# Auditing & Monitoring Tools in Salesforce

# Audit log

Filters ▾ | Search audit logs | Export ▾

JSON

CSV

## Recent events

**axilleas – profile_picture.update**

Updated profile picture for github-essentials

France | 7 minutes ago

**axilleas – repo.add_member**

Added axil44 to the github-essentials/symmetrical-bassoon repository

France | 23 minutes ago

**axilleas – org.update_default_repository_permission**

Changed the GitHub Essentials book organization's default repository permission from write to none

France | 32 minutes ago

**axilleas – org.update_default_repository_permission**

Changed the GitHub Essentials book organization's default repository permission from read to write

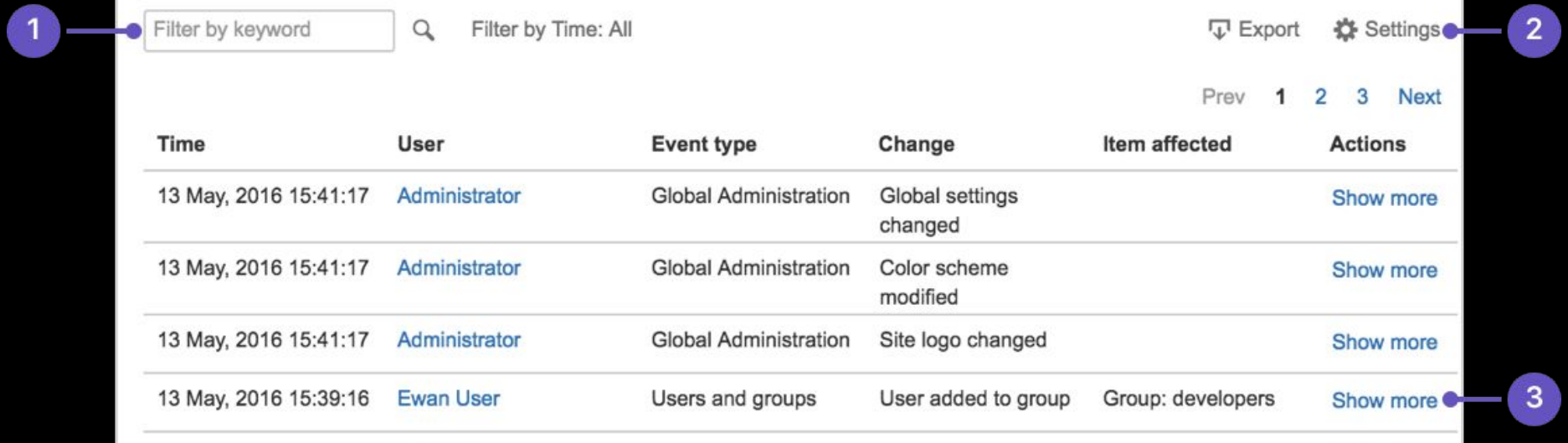
France | 34 minutes ago

**axilleas – team.add_repository**

Gave github-essentials/documentation access to github-essentials/symmetrical-bassoon

# Audit Log

The audit log gives you a history of changes to your Confluence site. It can be very useful for tracking down things like permissions, global settings, or add-on changes.




| Time | User | Event type | Change | Item affected | Actions |
|---|---|---|---|---|---|
| 13 May, 2016 15:41:17 | Administrator | Global Administration | Global settings changed | | Show more |
| 13 May, 2016 15:41:17 | Administrator | Global Administration | Color scheme modified | | Show more |
| 13 May, 2016 15:41:17 | Administrator | Global Administration | Site logo changed | | Show more |
| 13 May, 2016 15:39:16 | Ewan User | Users and groups | User added to group | Group: developers | Show more |
| 13 May, 2016 15:38:59 | Ewan User | Users and groups | Group created | Group: developers | Show more |
| 13 May, 2016 15:38:59 | Ewan User | Users and groups | Group created | Group: developers | Show more |
| 13 May, 2016 15:38:13 | Administrator | Spaces | Space created | Space: Audit log space | Show more |

| Date | Location | Actor | Activity |
| --- | --- | --- | --- |
| Nov 04, 2021<br>09:48 PDT | Unavailable | Jane Rotanson<br>jrotanson@acme.com | Viewed Jira issue **UAL-14** |
| Nov 04, 2021<br>09:47 PDT | Unavailable | Jane Rotanson<br>jrotanson@acme.com | Viewed Confluence blog **Janes blog update** |
| Nov 04, 2021<br>09:46 PDT | Unavailable | Jane Rotanson<br>jrotanson@acme.com | Viewed Jira issue **UAL-16** |

Admin / Xtreme, Inc.

# Audit log

Export log

Your organization's audit log tracks activities that occurred from your organization and across your sites within the past 180 days. For product-specific activity, visit the product's audit log. Learn more about your organization's audit log

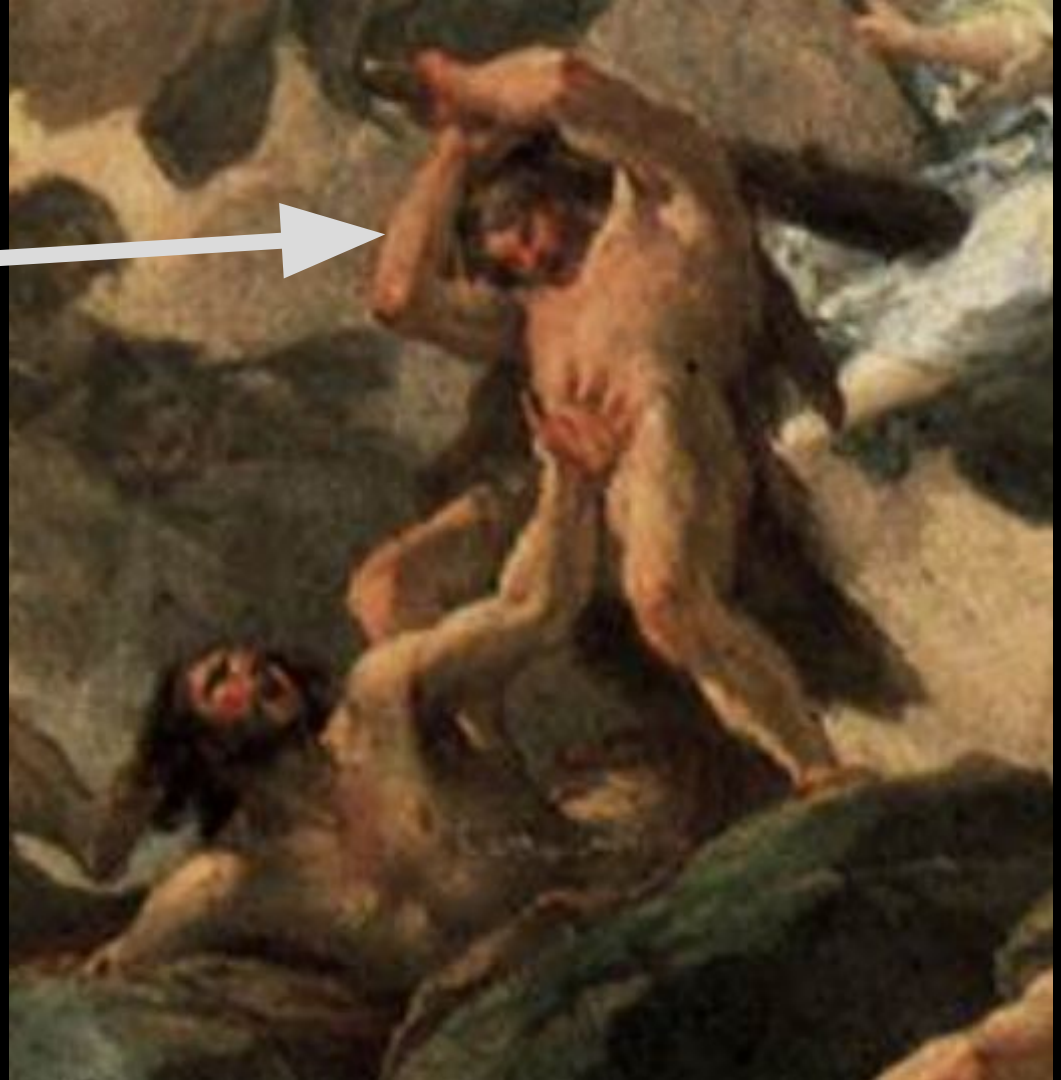
To save activities before they pass 180 days, regularly export the log or use the organization REST API to store activities to another location. Learn more about the organization REST API

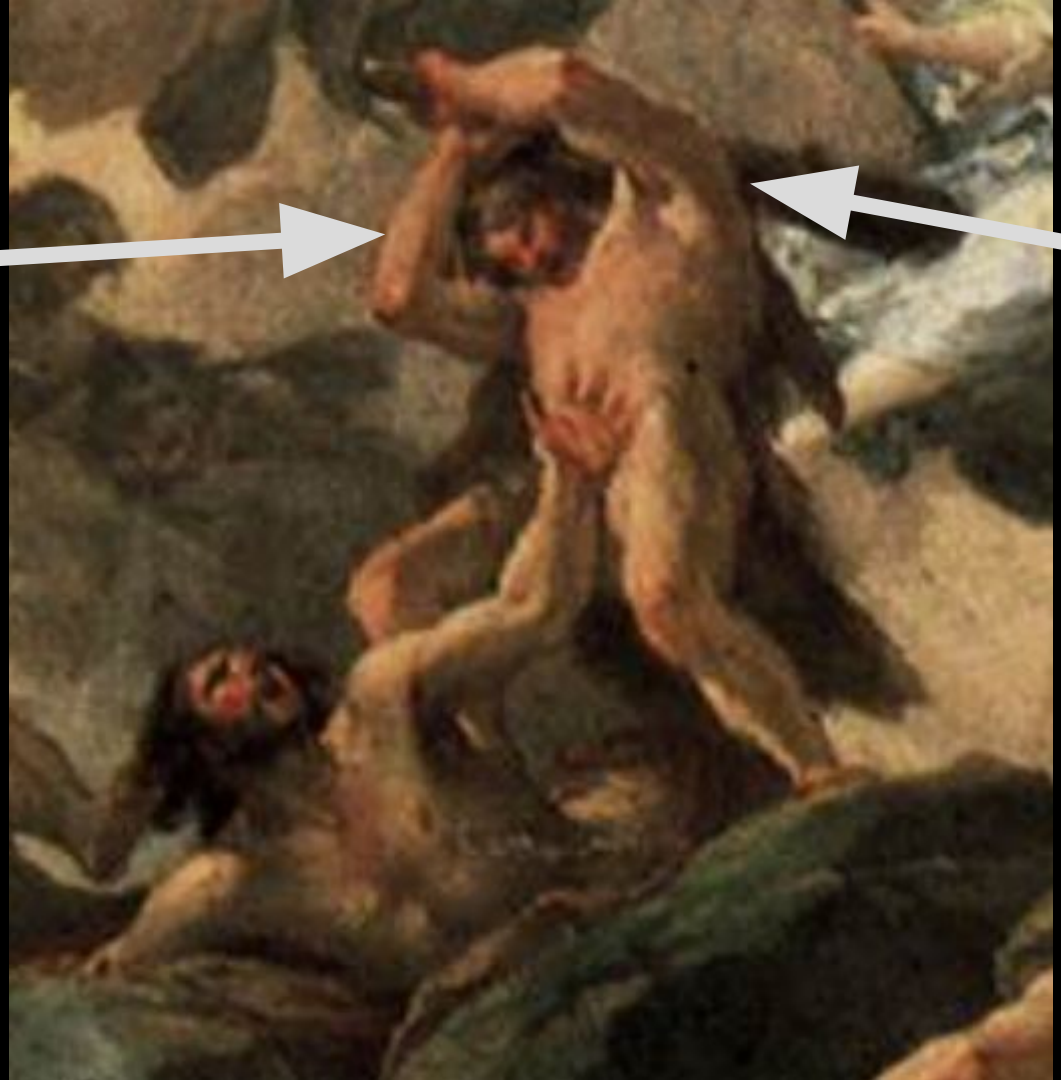
Search by name, group, or site | e.g. YYYY/MM/DD | to | e.g. YYYY/MM/DD | All activities | Apply

| Date | Location | Actor | Activity |
|---|---|---|---|
| Mar 25, 2021 16:44 PDT | San Jose 73.71.116.94 | Atlassian Demo atlsummitdemo@gmail.com | Updated settings (SSO=**None**, two-step-verification=**Optional**, password strength=**Weak**, password expires=**Never**, idle session duration=**30 days**) for authentication policy **Not so special users** |
| Mar 25, 2021 16:44 PDT | San Jose 73.71.116.94 | Atlassian Demo atlsummitdemo@gmail.com | Added settings (SSO=**None**, two-step-verification=**Optional**, password strength=**Weak**, password expires=**Never**, idle session duration=**30 days**) for authentication policy **Not so special users** |
| Mar 25, 2021 16:43 PDT | San Jose 73.71.116.94 | Atlassian Demo atlsummitdemo@gmail.com | Updated settings (SSO=**SAML SSO**, two-step-verification=**null**, password strength=**null**, password expires=, idle session duration=**1 hour**) for authentication policy **Special Users** |
| Mar 25, 2021 16:43 PDT | San Jose 73.71.116.94 | Atlassian Demo atlsummitdemo@gmail.com | Changed **amberclayton@x-inc.net**'s authentication policy to **Special Users** |

- Spaces
  - Created, archived, or deleted
  - Exported or imported
  - Configuration updated
  - Logo uploaded
  - Trash emptied
- Users and groups
  - User created, deactivated, or reactivated
  - User details updated
  - User added to or removed from group
  - Group added or deleted
- Global administration
  - Global settings changed
  - Site logo changed
  - Color scheme modified
- Permissions
  - Global permission added or removed
    - including “anonymous” access
  - Space permission added or removed
    - including “anonymous” access
  - Content restriction added or removed
- Public links
  - Enabled or disabled
- Page
  - Archived or restored
  - Viewed with admin key
- Page templates
  - Created or updated

Insiders




Insiders
Misconfigs


# Insiders

# Insiders

- Inherently trusted

# Insiders

- Inherently trusted
- Primarily associated with data theft before leaving the company

# Insiders

- Inherently trusted
- Primarily associated with data theft before leaving the company
- Often non-technical users using simple techniques

# Insiders

- Inherently trusted
- Primarily associated with data theft before leaving the company
- Often non-technical users using simple techniques
- May require working with HR and Legal teams

# Misconfigs

# Misconfigs

- Requires app/platform specific knowledge

# Misconfigs

- Requires app/platform specific knowledge
- Initiated by legitimate administrators

# Misconfigs

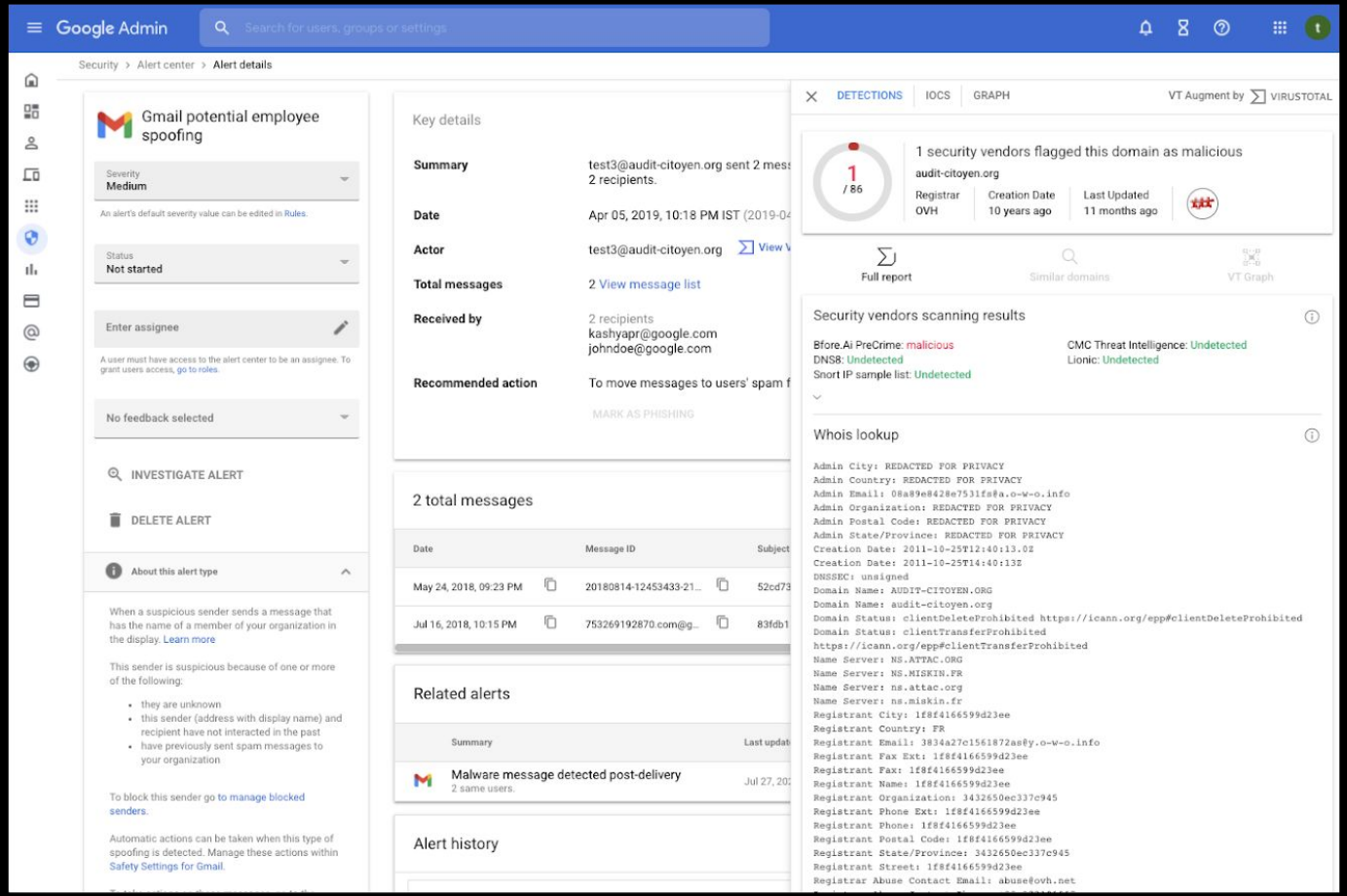
- Requires app/platform specific knowledge
- Initiated by legitimate administrators
- Associated w/inadvertent data exposure

# Misconfigs

- Requires app/platform specific knowledge
- Initiated by legitimate administrators
- Associated w/inadvertent data exposure
- Highly time sensitive

# SaaS Defenses

# SaaS Defenses First-Party



# SaaS Defenses First-Party

## Salesforce Shield

- Platform Encryption
- Event Monitoring
- Field Audit Trail

## Application Services

- Classic Encryption
- Identity & Single Sign On
- Password Policies
- Two Factor Authentication
- User Roles & Permissions
- Field Level Security
- Field History Tracking

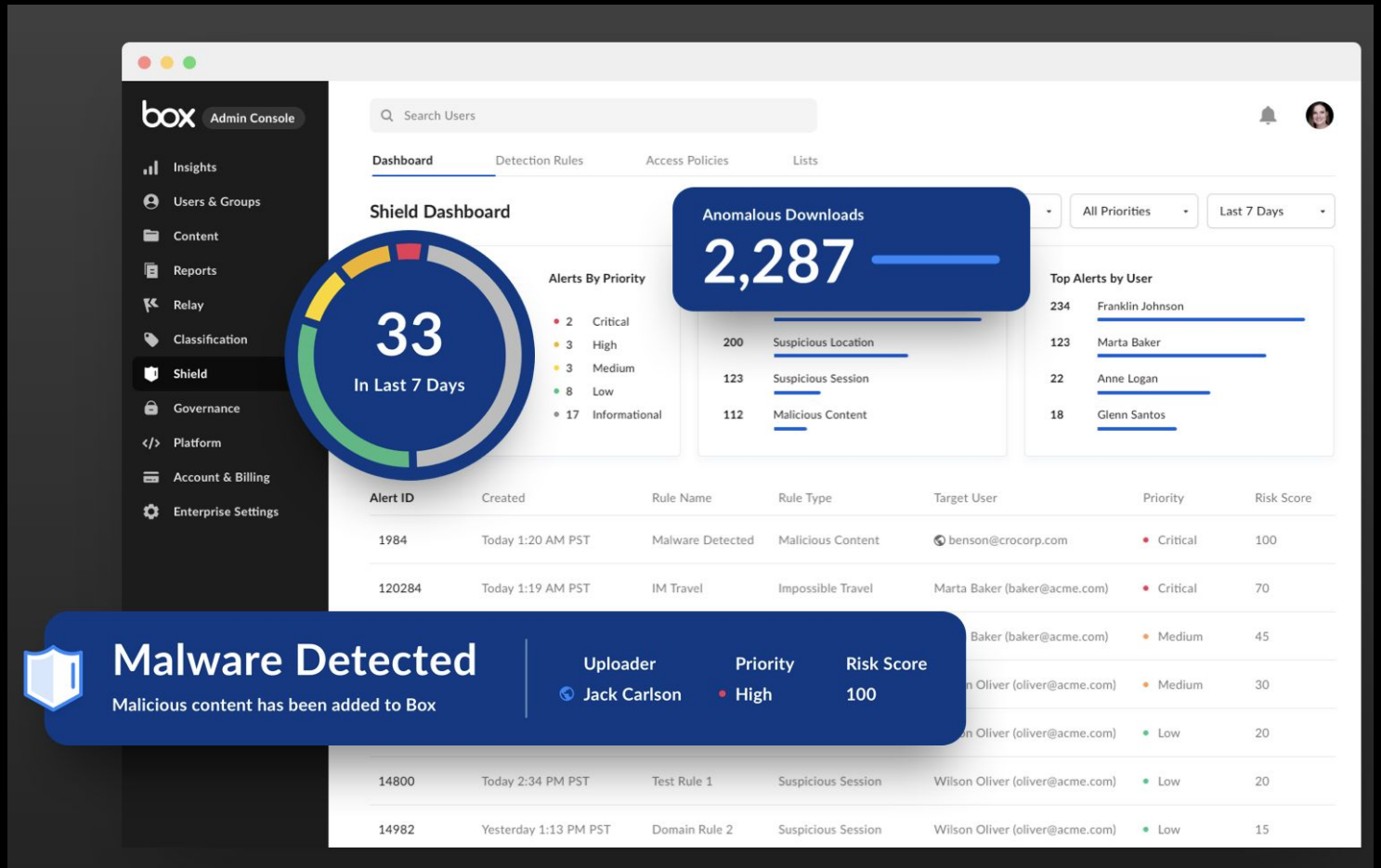
## Network Services

- HTTPS Encryption
- Penetration Testing
- Monitor Login History
- Advanced Threat Detection
- Secure Firewalls
- IP Login Restrictions

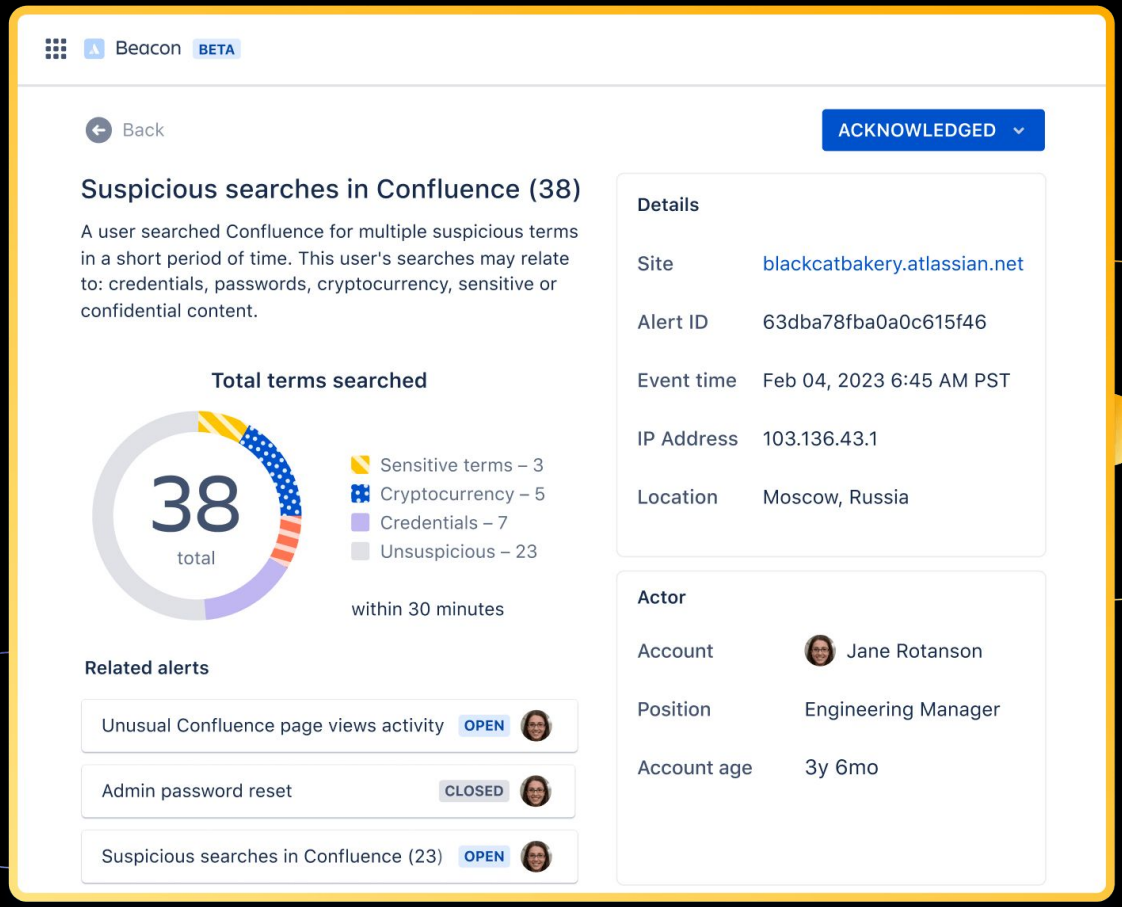
## Infrastructure Services

- Secure Data Centers
- Backup and Disaster Recovery
- Real-time replication
- Third Party Certifications
- Customer Audits

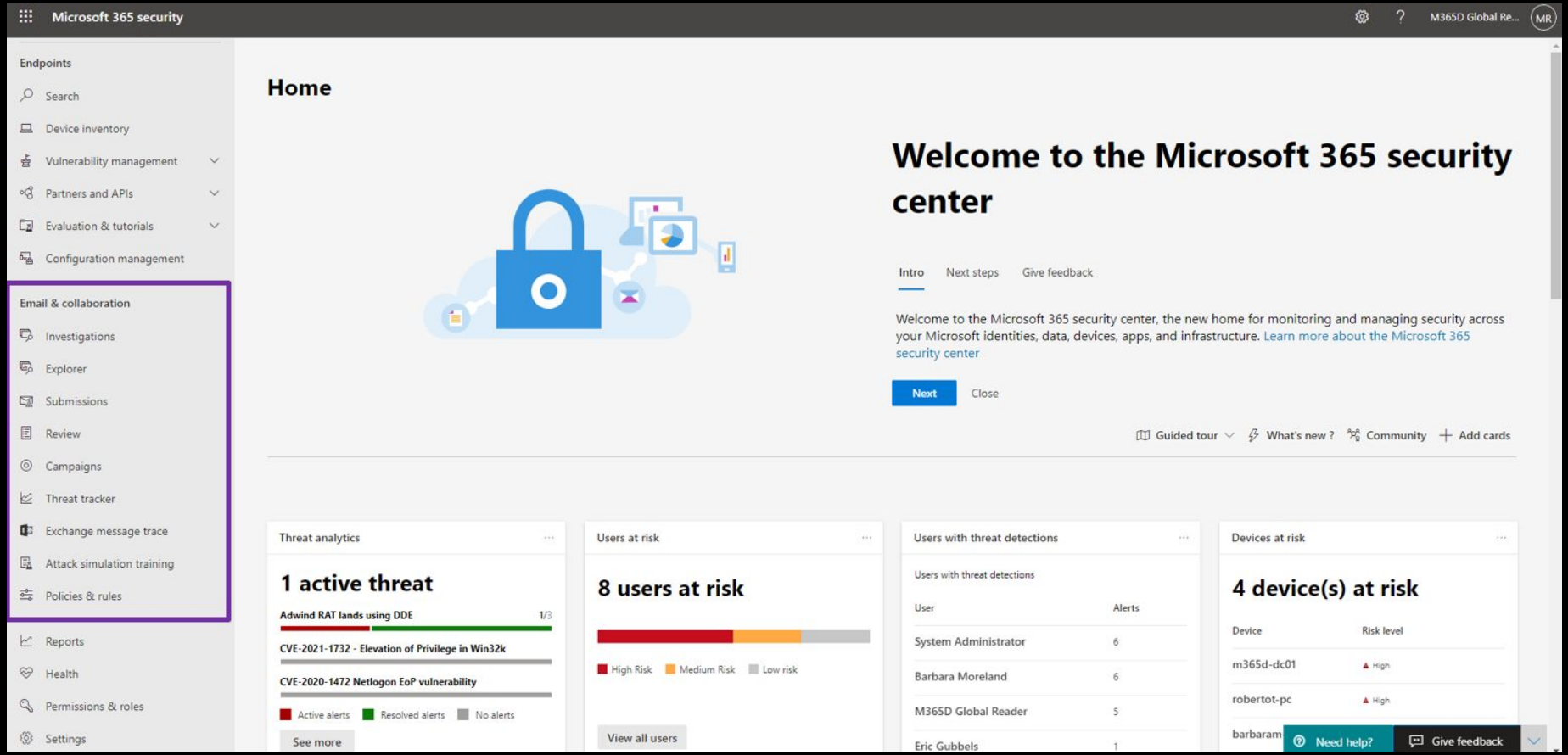
# SaaS Defenses First-Party



# SaaS Defenses First-Party



# SaaS Defenses First-Party



# SaaS App Detections

# SaaS App Detections

- **Unusual IP or Device**
  - **geo? datacenter? OS?**

# SaaS App Detections

- Unusual IP or Device
  - geo? datacenter? OS?
- Anomalous count
  - crawling, exports, api calls

# SaaS App Detections

- Unusual IP or Device
  - geo? datacenter? OS?
- Anomalous count
  - crawling, exports, api calls
- Uncommon feature use
  - best combined w/other signals

# SaaS App Detections

- **Unusual IP or Device**
  - geo? datacenter? OS?
- **Anomalous count**
  - crawling, exports, api calls
- **Uncommon feature use**
  - best combined w/other signals
- **Configuration changes**
  - can weaken security/privacy

# Stopping Attackers & Incidents

# Stopping Attackers & Incidents

- 2FA/MFA required on apps

# Stopping Attackers & Incidents

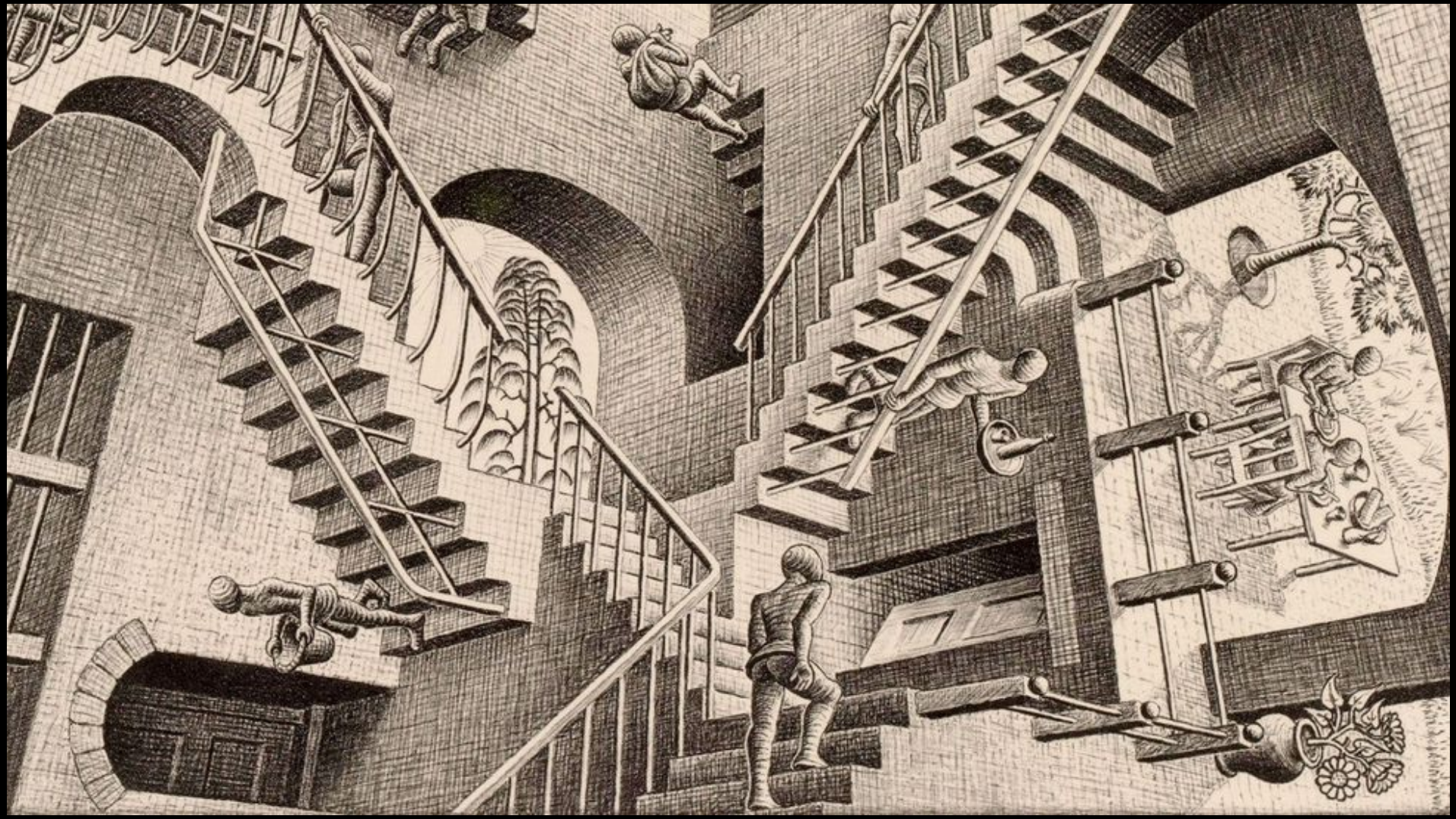
- 2FA/MFA required on apps
- Reduce Session durations

# Stopping Attackers & Incidents

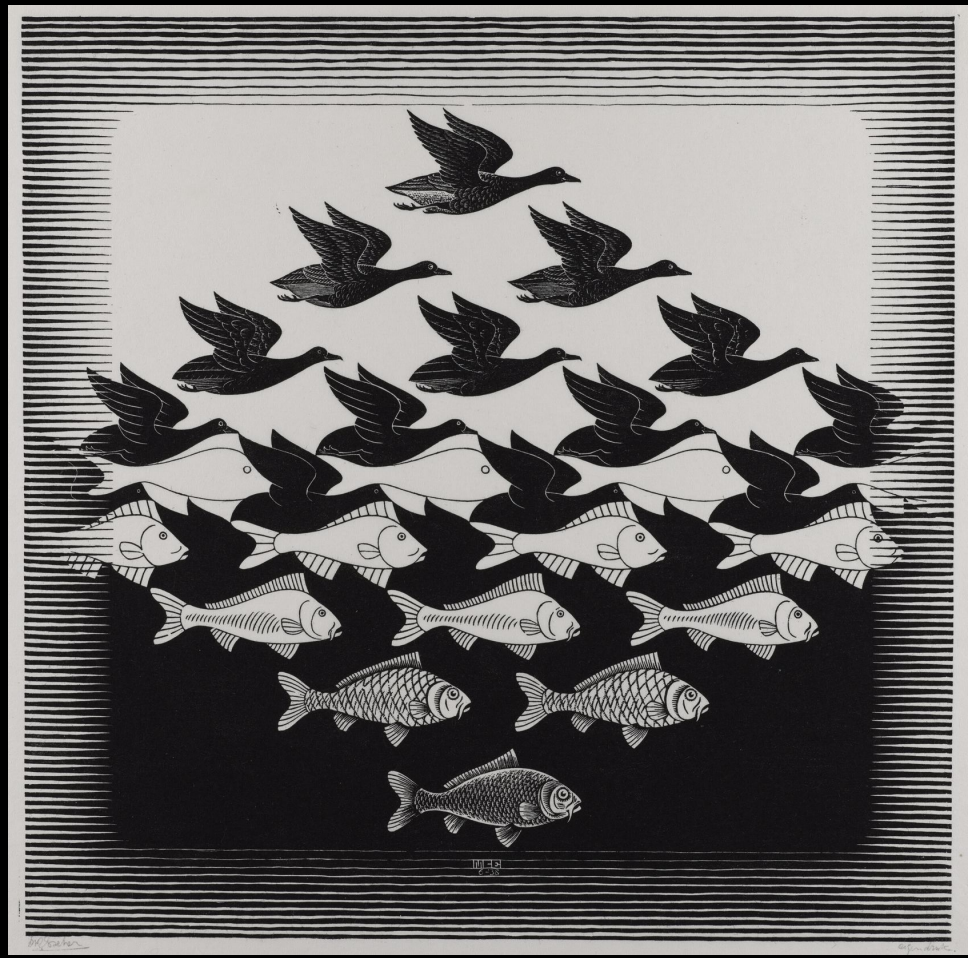
- 2FA/MFA required on apps
- Reduce Session durations
- Work with app admins to better understand the apps

# Stopping Attackers & Incidents

- 2FA/MFA required on apps
- Reduce Session durations
- Work with app admins to better understand the apps
- Require VPN connectivity by default

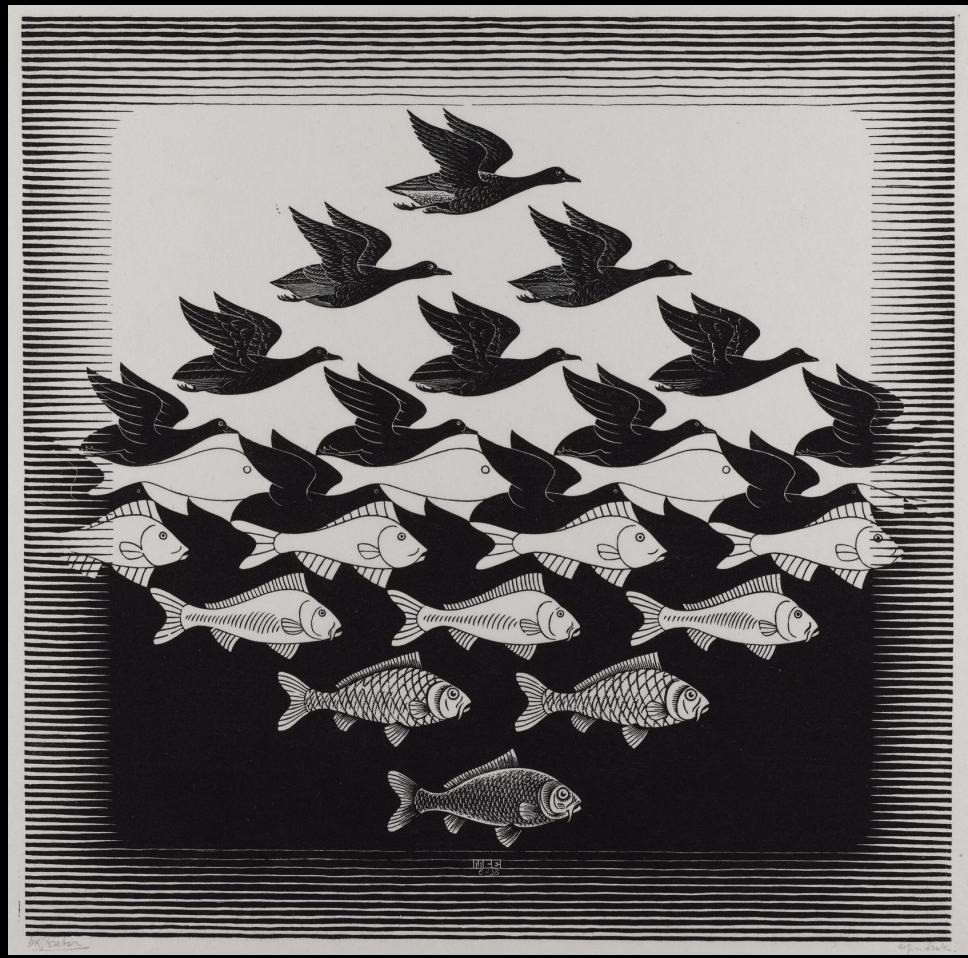


# Advanced Detections with Audit Logs: DECEPTION



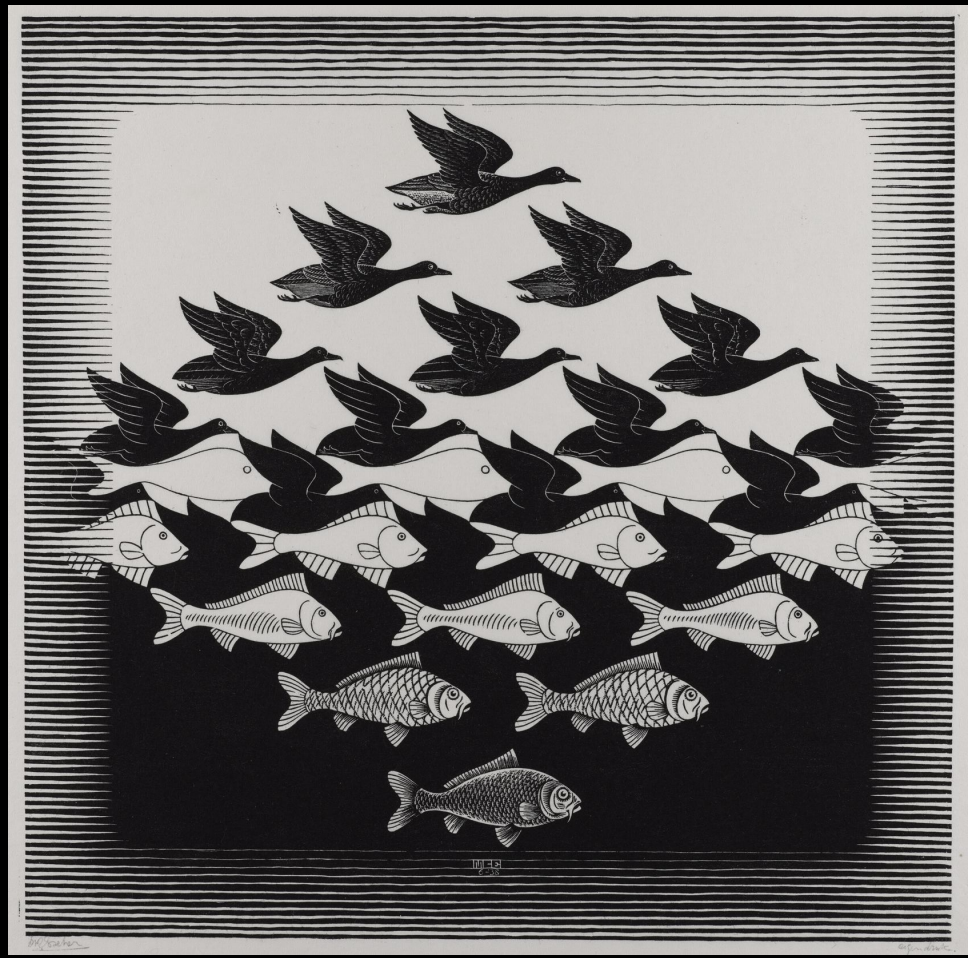
# Advanced Detections with Audit Logs: DECEPTION

- Cover the basics first



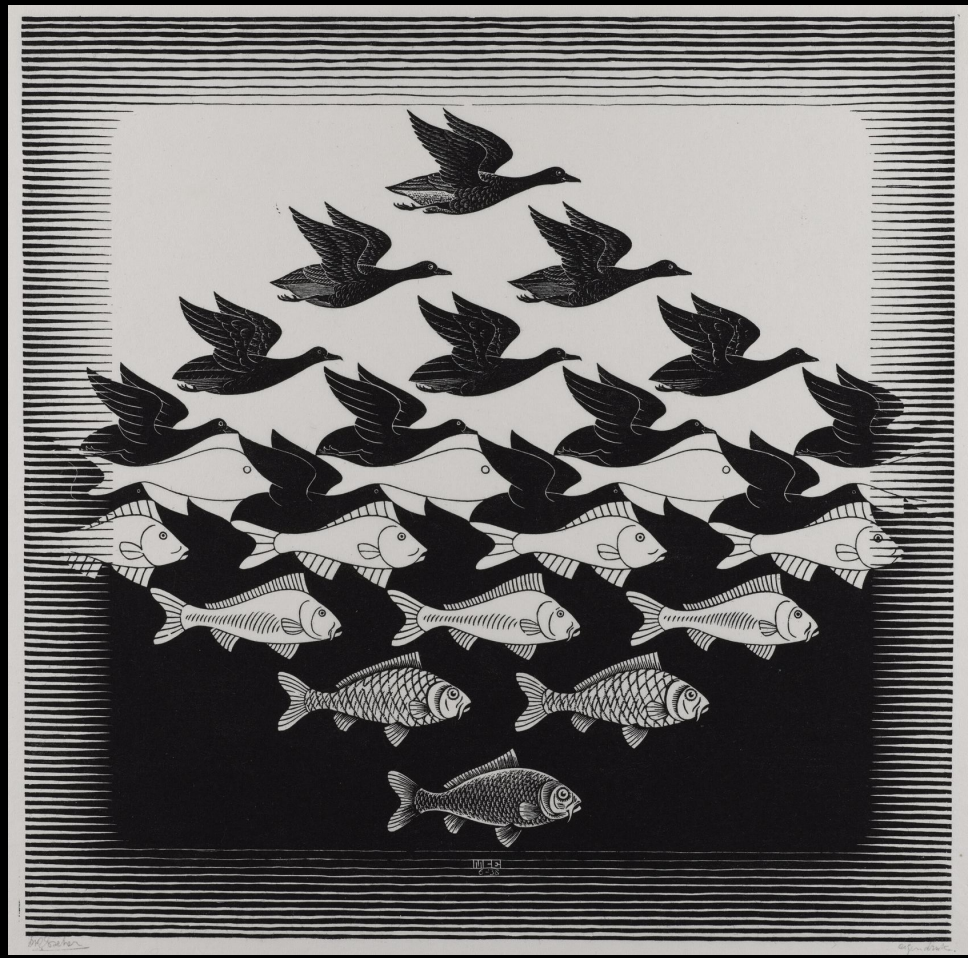
# Advanced Detections with Audit Logs: DECEPTION

- Cover the basics first
- Requires high signal-to-noise ratio



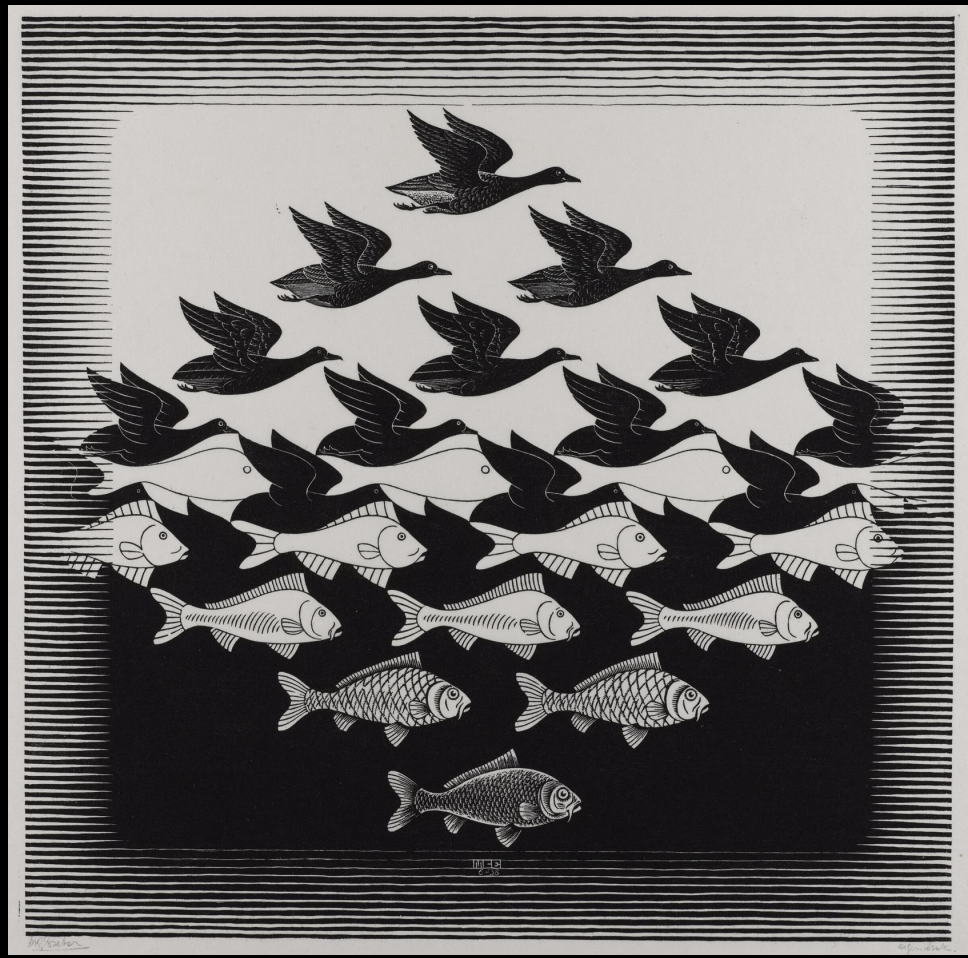
# Advanced Detections with Audit Logs: DECEPTION

- Cover the basics first
- Requires high signal-to-noise ratio
- Honeytokens, honeycreds, honeypages, honeyfiles



# Advanced Detections with Audit Logs: DECEPTION

- Cover the basics first
- Requires high signal-to-noise ratio
- Honeytokens, honeycreds, honeypages, honeyfiles
- Even advanced attackers cannot resist 😈



# Recap

# Recap

- Monitoring SaaS activity is high-cost but high-value

# Recap

- Monitoring SaaS activity is high-cost but high-value
- Security is so much more than vulnz and shellz

# Recap

- Monitoring SaaS activity is high-cost but high-value
- Security is so much more than vulnz and shellz
- The world works in SaaS, it's part of your battleground

# Recap

- Monitoring SaaS activity is high-cost but high-value
- Security is so much more than vulnz and shellz
- The world works in SaaS, it's part of your battleground
- Logs mean nothing without skilled, motivated, analysts

# Thanks Y’all

JeremyNGalloway@gmail.com