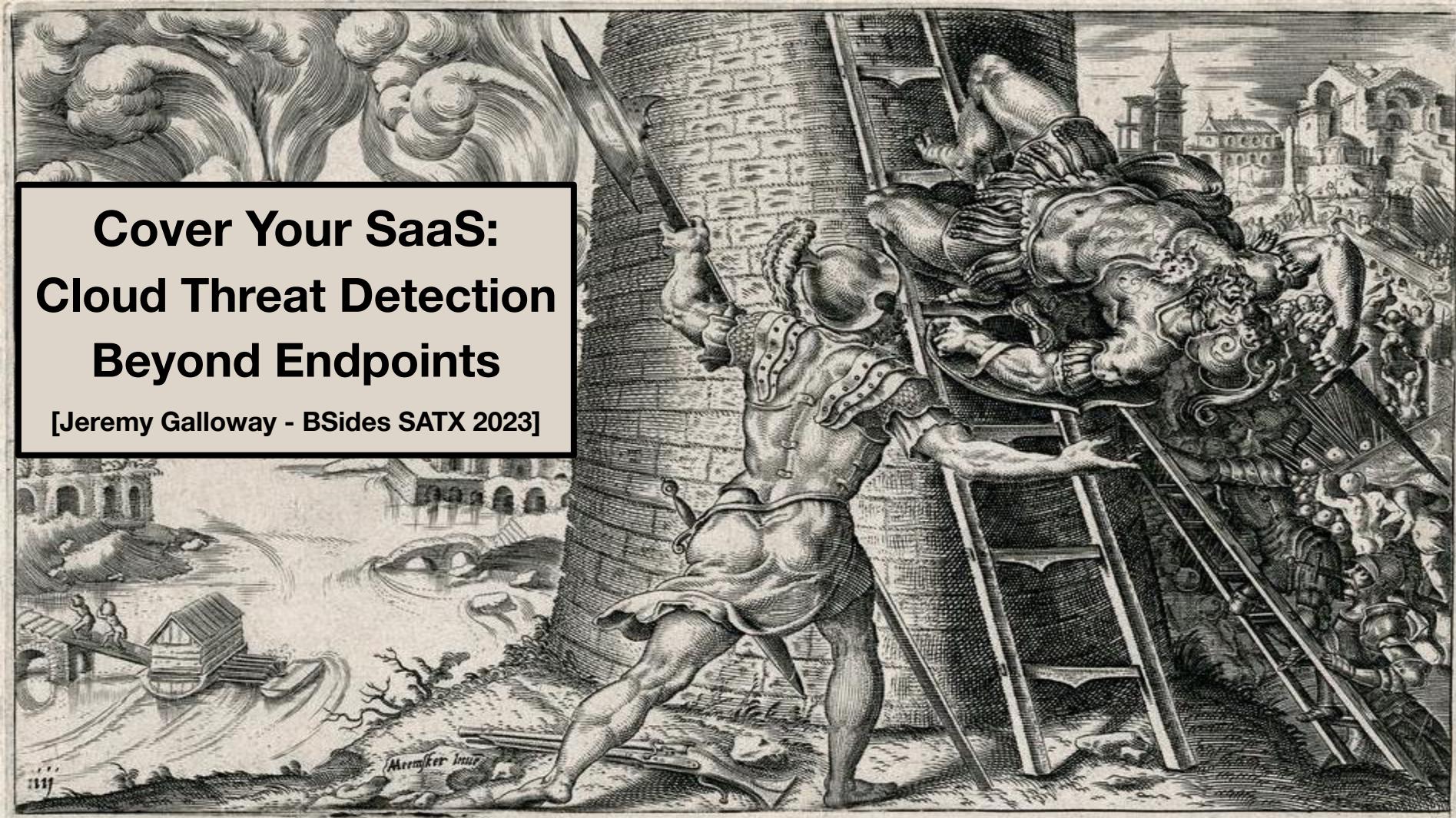


# Cover Your SaaS: Cloud Threat Detection Beyond Endpoints

[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**



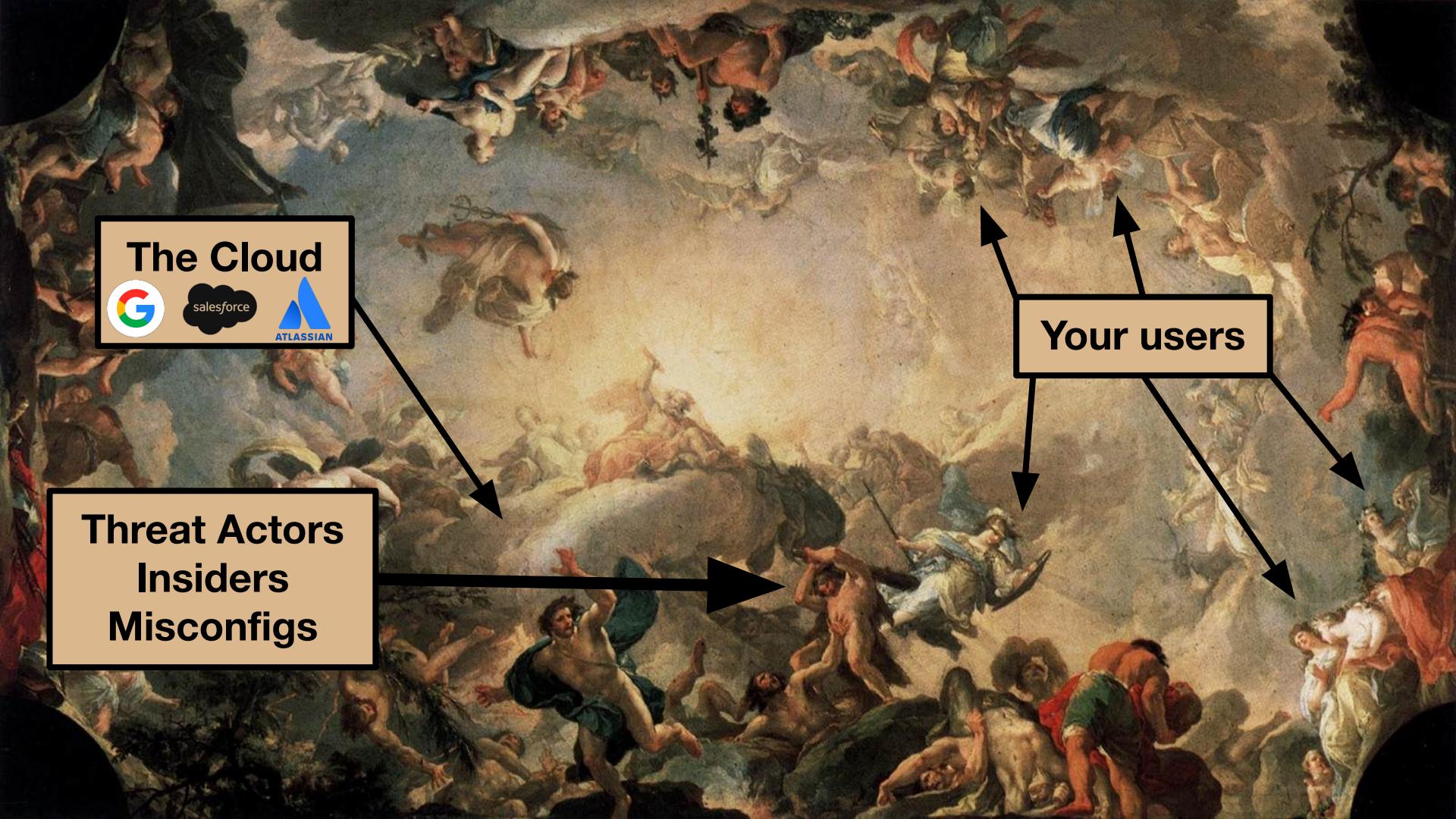


**What this talk is about...**





Your users

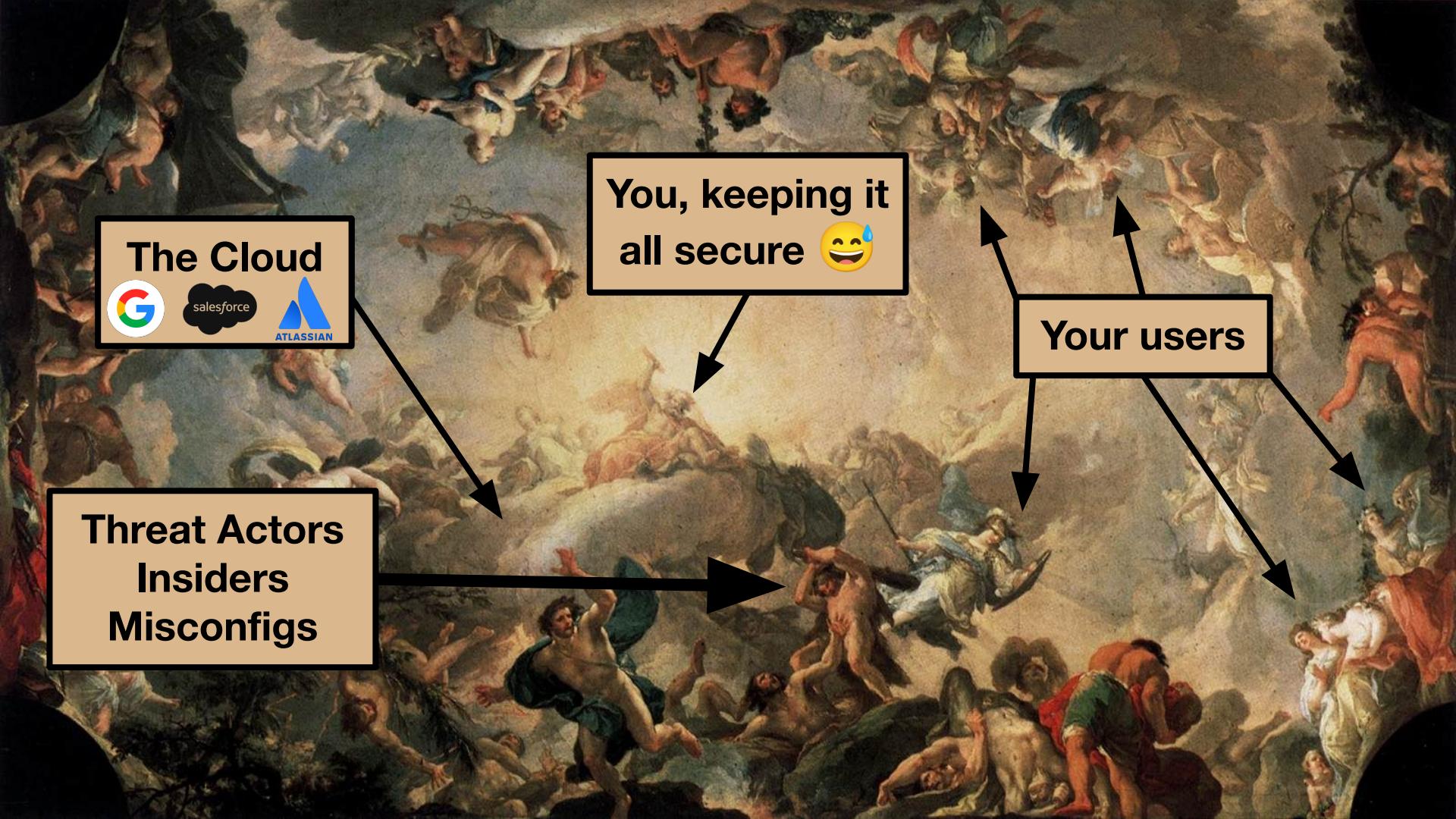


**The Cloud**



**Threat Actors  
Insiders  
Misconfigs**

**Your users**



The Cloud



You, keeping it  
all secure 😅

Threat Actors  
Insiders  
Misconfigs

Your users



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

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

# Traditional Detections



INVE.

H. COCK EXCVD.

# 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

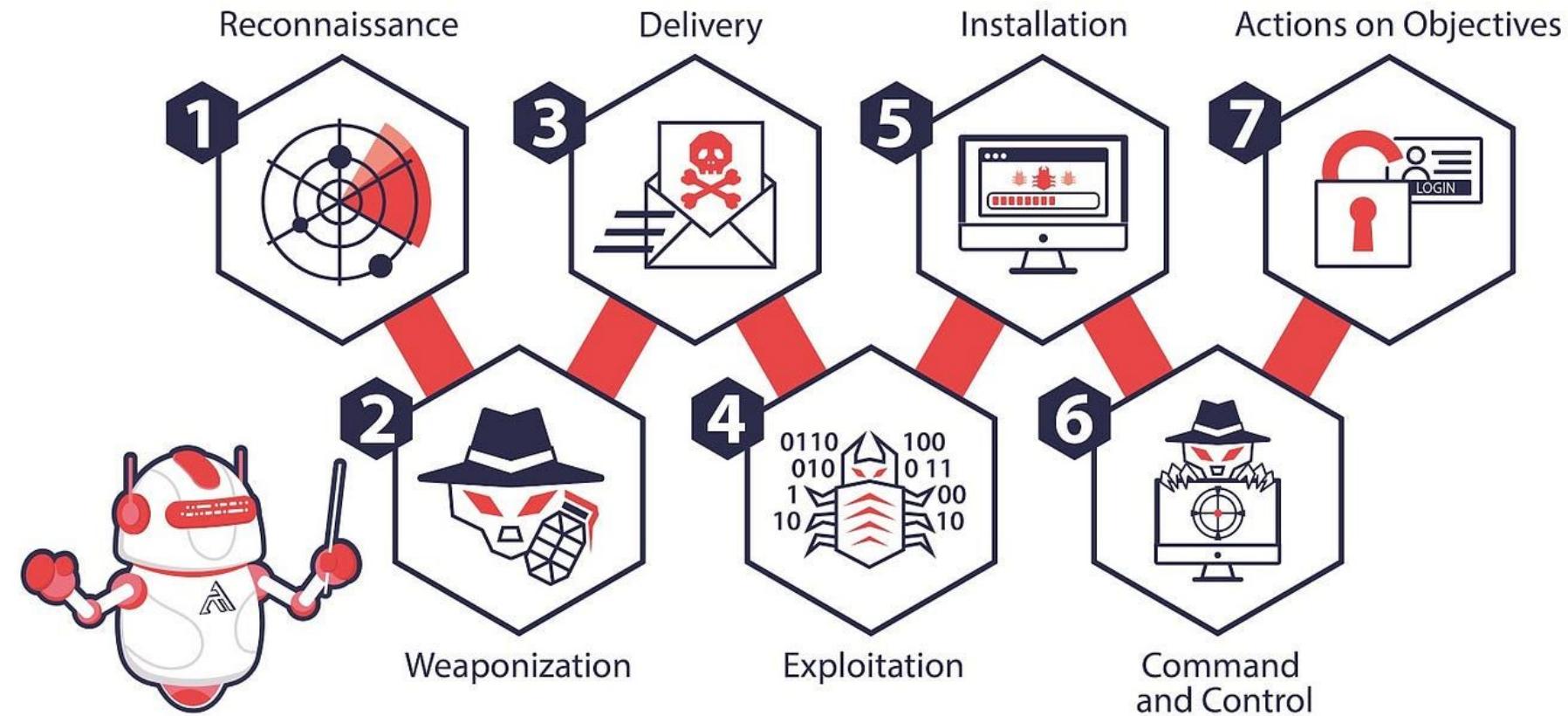


# Traditional Detections

- **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



A dark, dramatic painting of a screaming figure, possibly Christ on the cross, with a red banner across it.

# 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

The screenshot shows a list of compromised bot names from the Genesis Market. Each entry includes a timestamp, a list of compromised resources, and a summary of known data.

- D80F17C4D17CD33A3FA6034ADFC9B9**  
2023-03-09 18:05:28  
2023-03-09 19:36:08  
2x   
github, spotify, live, paypal, discord.com, eu.battle.net, eu.account.battle.net, google, yahoo, facebook, netflix, snapchat, messenger, instagram, se, 87.227..., windows 10 enterprise, 16.00, ...known 50, ...other 12
- 93C1887865137A88A04B55175A33AA3**  
2022-12-27 16:13:58  
2023-03-09 19:35:58  
3x   
binance, facebook, google, com.findhdmusic.app.radio, com.netflix.mediaclient, yahoo, wehkamp, cloudfare, wishstore, twitter, nl, 82.217..., windows 11 pro, 20.00, ...known 32, ...other 61
- F0DCD65892D5D87B33613D8A6541AEF**  
2019-12-28 20:53:23  
2023-03-09 19:35:58  
3x   
paypal, operaaccount, android, alibaba, wishstore, com.audiomack, dell, facebook, ebay, pornhub, linkedin, amazon, live, meganz, orange, olx, pl, 78.88..., windows 7 sp1, 21.00, ...known 186, ...other 907
- 8991A4F-9414907A-D367557F-09271558-C3F43P16**  
2019-08-02 16:51:46  
2023-03-09 19:35:55  
3x   
live, carrefourstore, dealo, nvidiastore, movistar, pinterest, ebaystore, netflix, xiaomi, steam, amazon, google, aliexpress, instagram, spotify, es, 188.76, windows 10 enterprise, 10.20, ...known 75, ...other 211
- 82D7BEFB8E8933E1C68372396CB062FD8**  
2023-03-09 18:59:05  
2023-03-09 19:34:55  
  
animedix.net, destek.sonyuncu.network, gameplus.com.tr, netflix, spotify, auth0.openai.com, discord.com, sonoyuncu.com.tr, tr, 46.196..., windows 10 home, 8.00, ...known 6, ...other 10

# THIS WEBSITE HAS BEEN SEIZED



## OPERATION COOKIE MONSTER

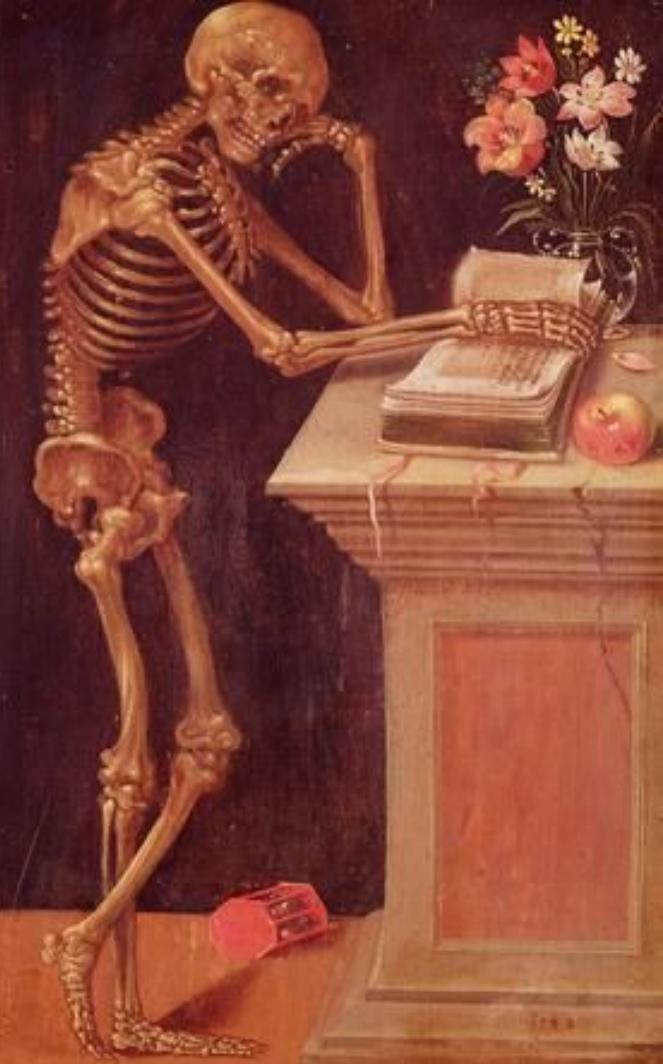
Genesis Market's domains have been seized by the FBI pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Wisconsin. These seizures were possible because of international law enforcement and private sector coordination involving the partners listed below.



To determine if you have been victimized  
[haveibeenpwned.com](http://haveibeenpwned.com) or [politie.nl/checky](http://politie.nl/checky)

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

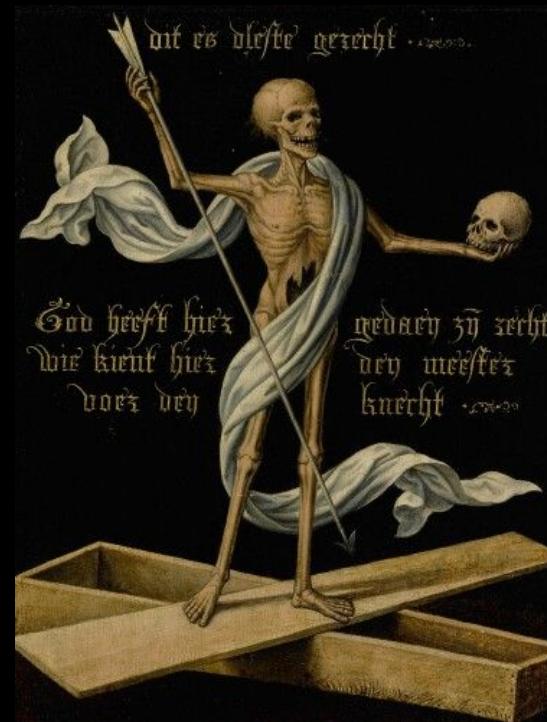


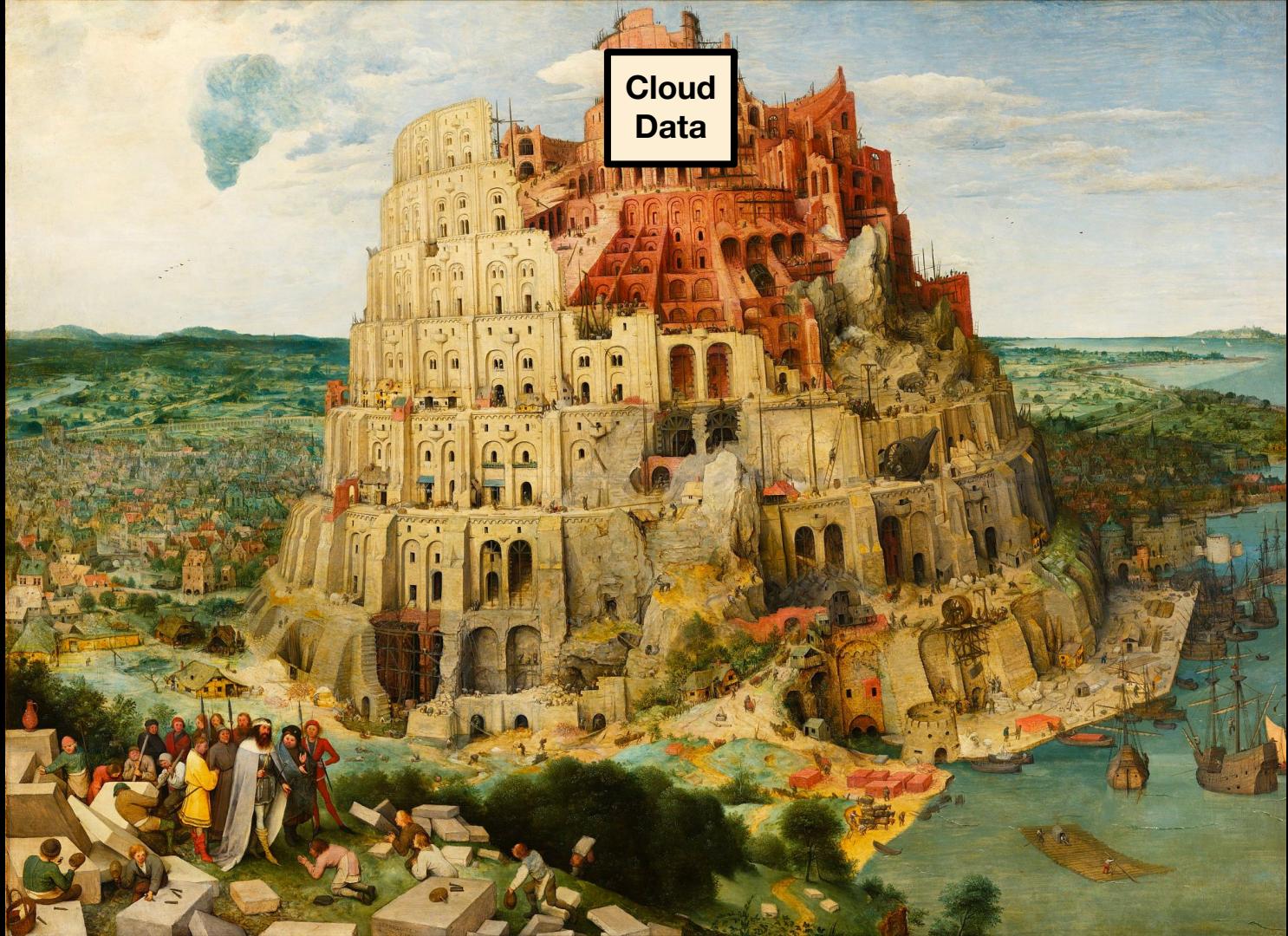


# Threat Actors don't want shells\*

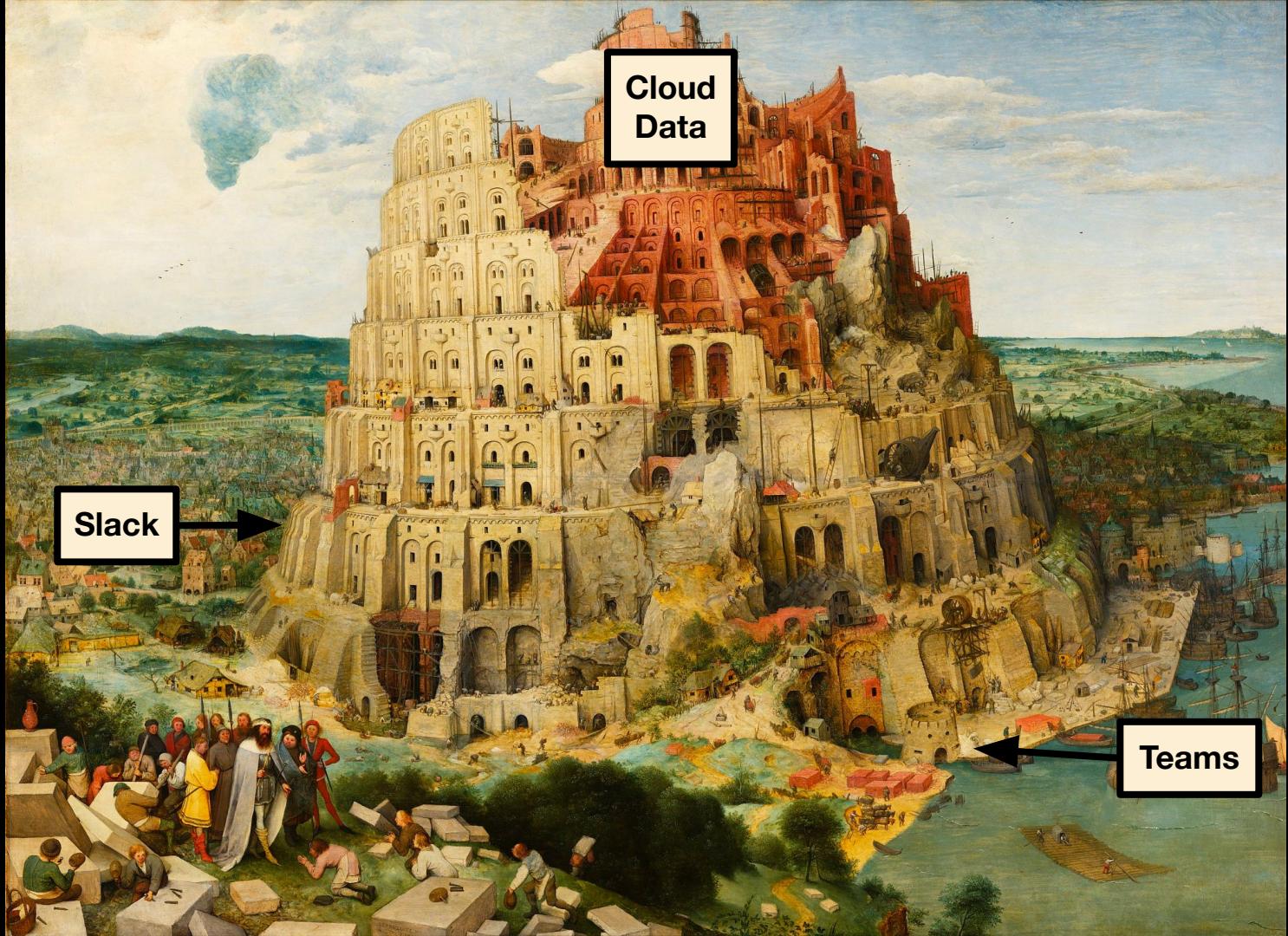
-

## They want access to Data





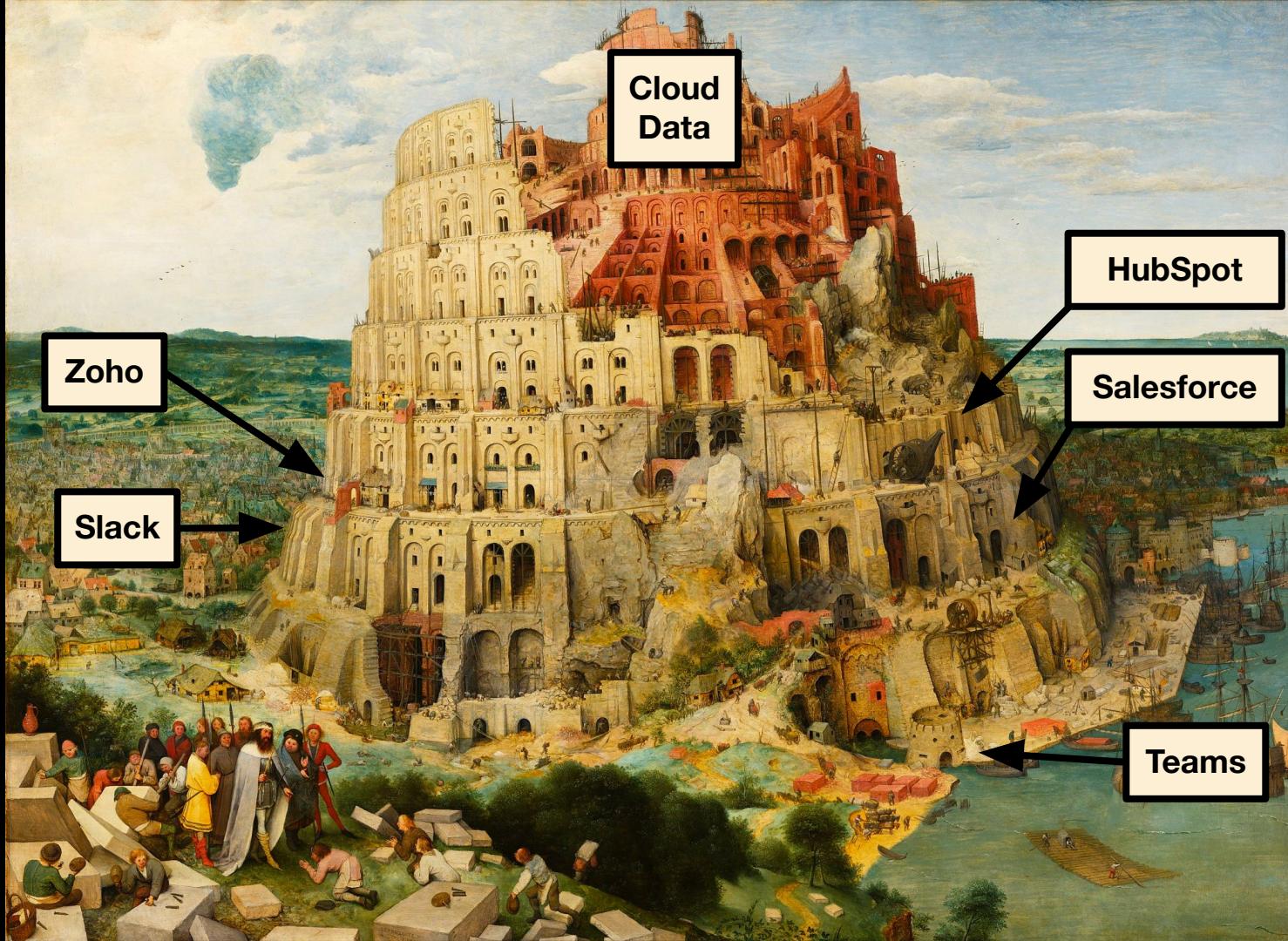
Cloud  
Data



Cloud  
Data

Slack

Teams



Cloud  
Data

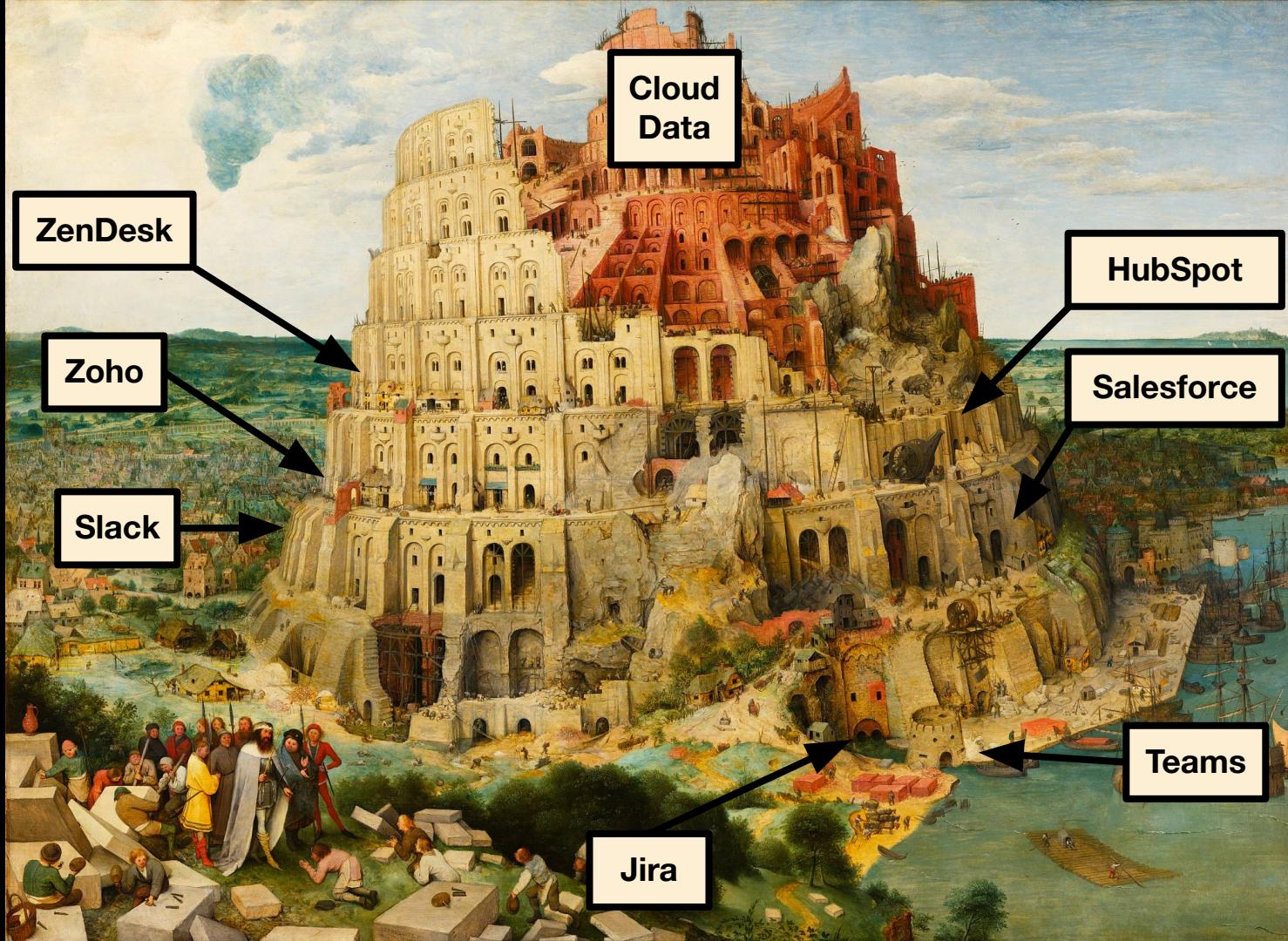
HubSpot

Salesforce

Zoho

Slack

Teams



Cloud  
Data

ZenDesk

HubSpot

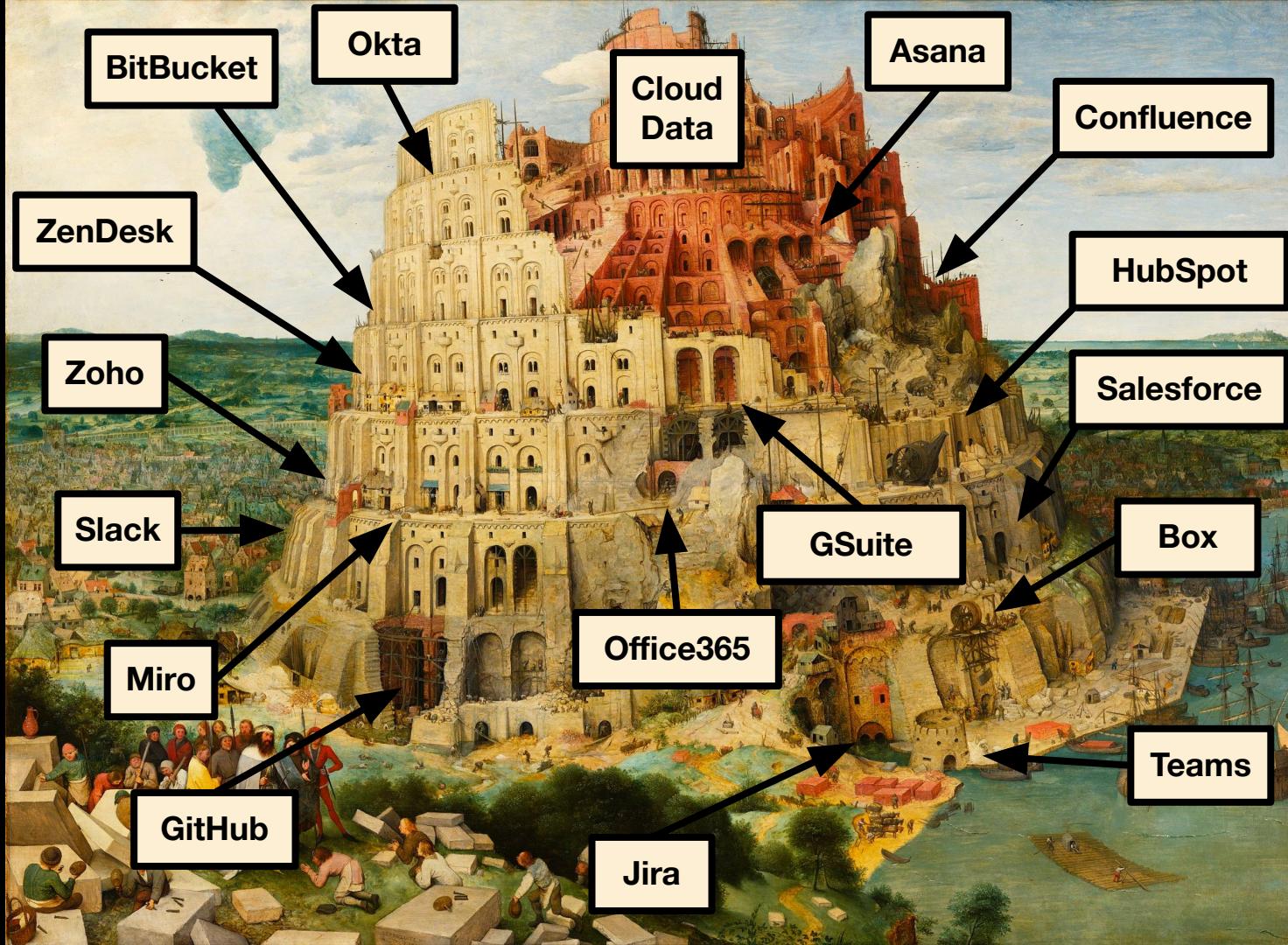
Zoho

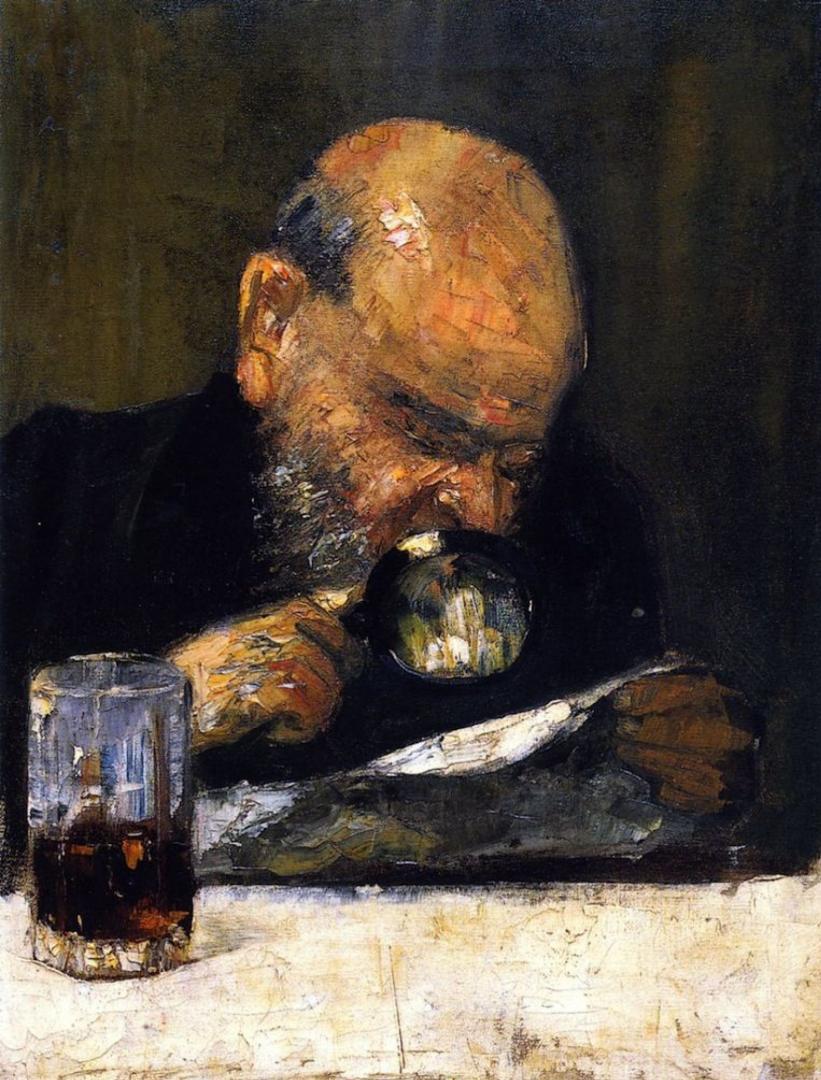
Salesforce

Slack

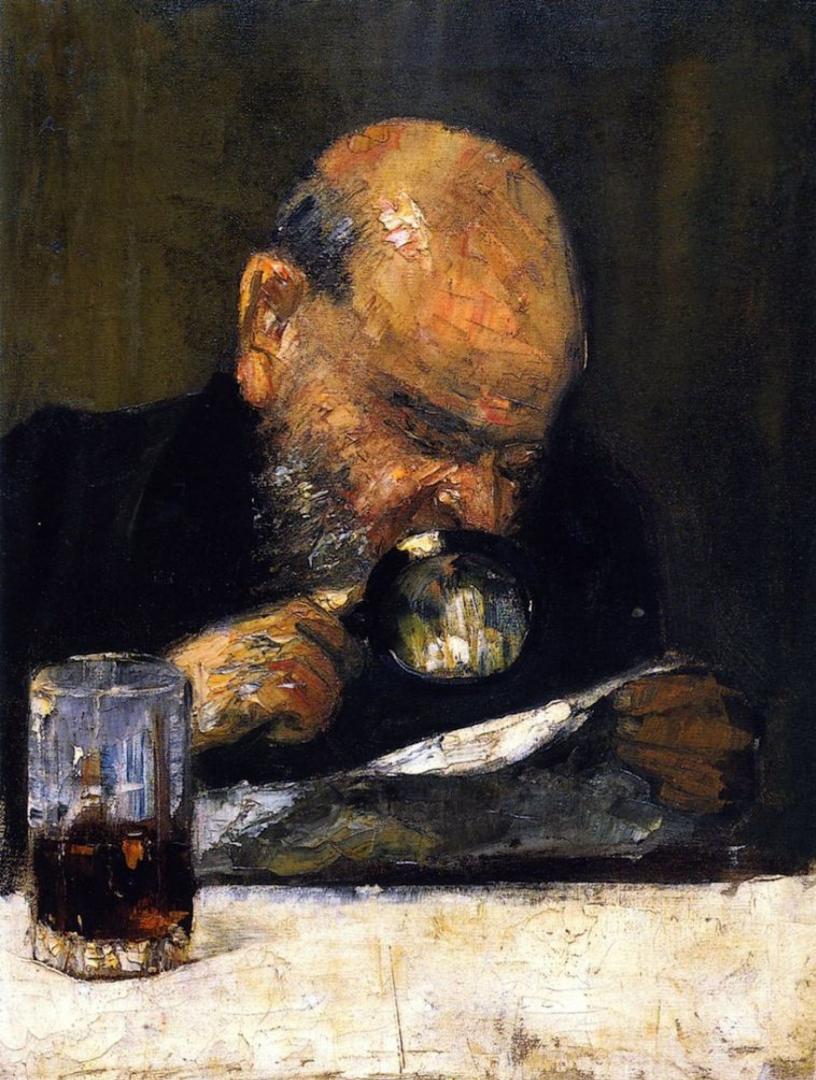
Teams

Jira



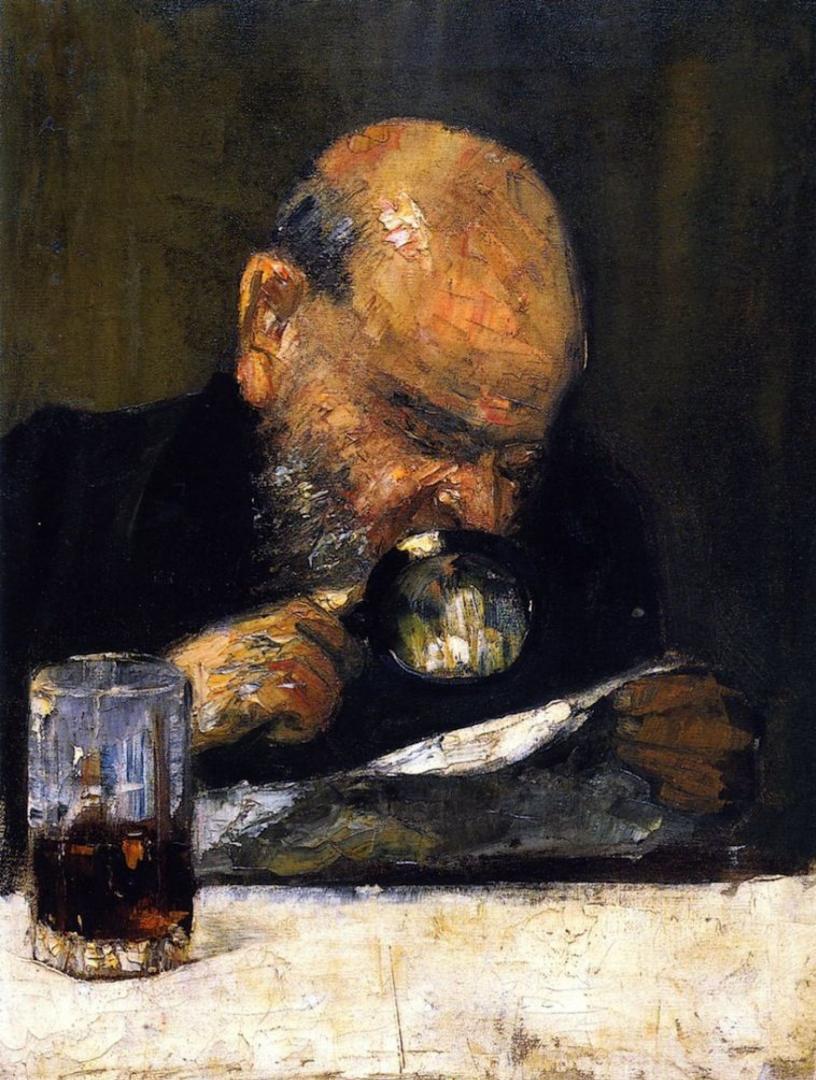


# Detection Engineering 101



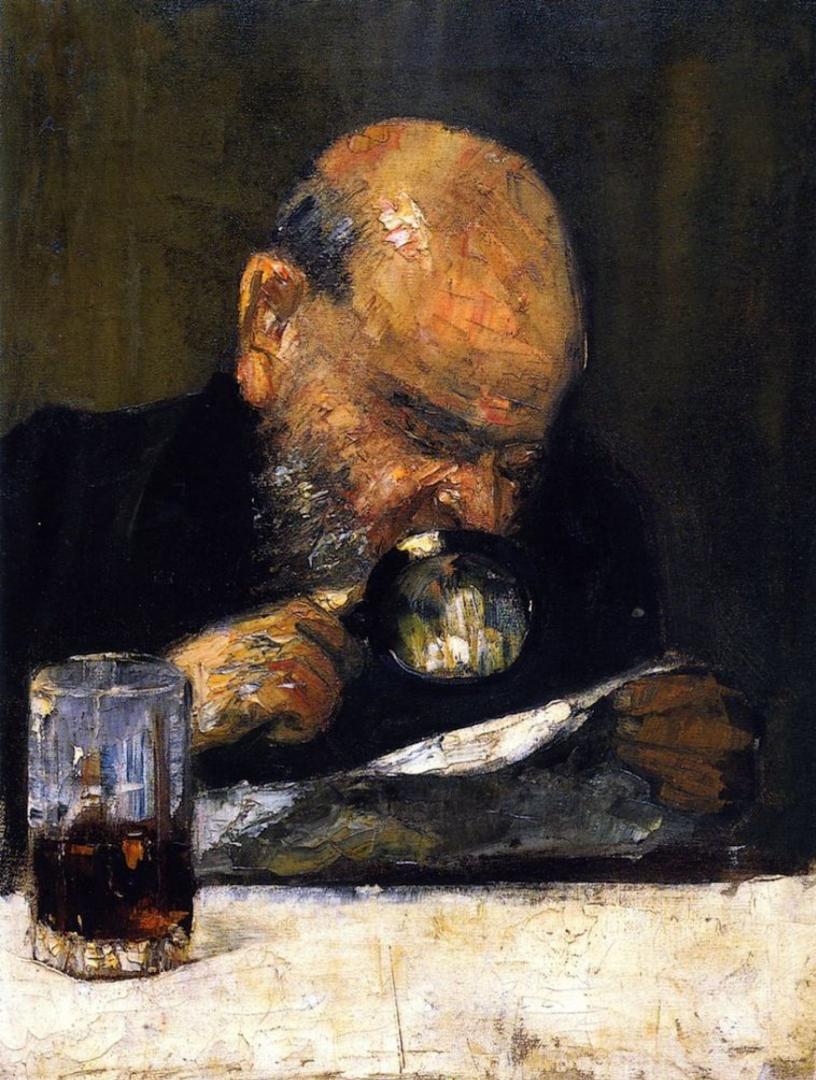
# Detection Engineering 101

- Find all the devices connected to your organization

A painting of a skull and a pipe on a dark surface. The skull is the central focus, with its eye sockets and nasal cavity clearly visible. It is surrounded by a dark, textured background. In the foreground, a pipe lies across the base of the skull, and a small, dark object, possibly a cigarette or a piece of debris, rests near the pipe's stem.

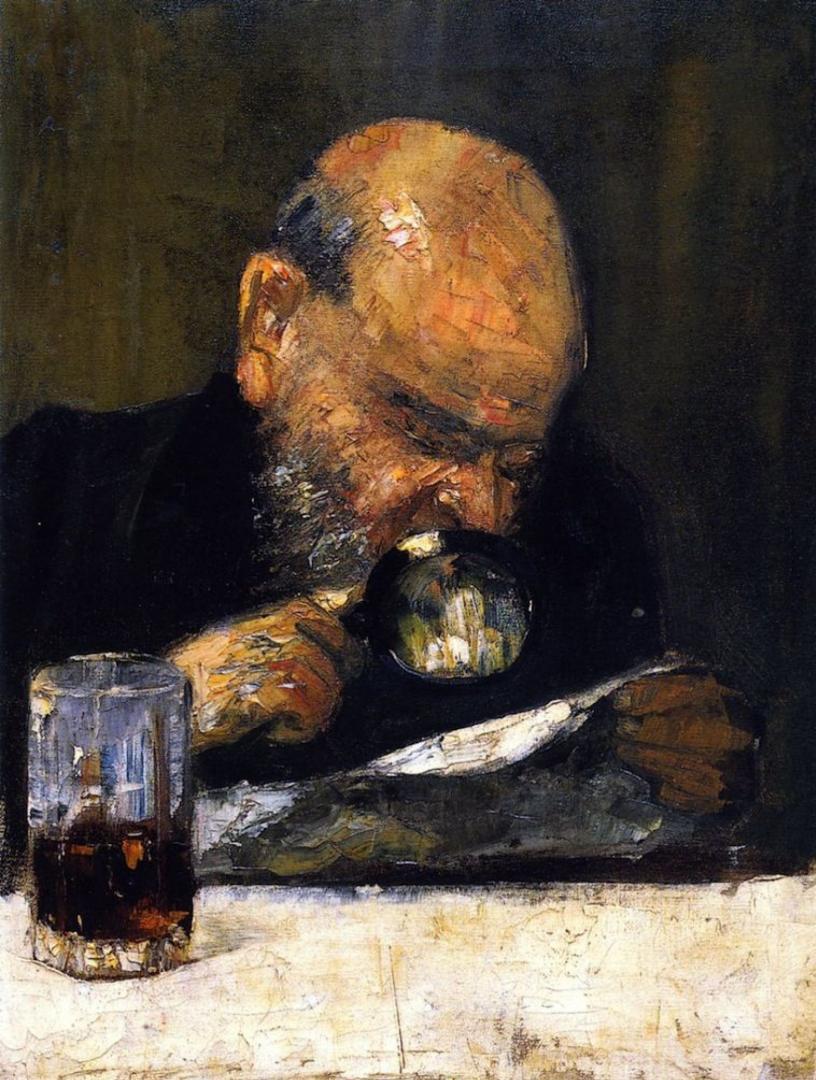
# Detection Engineering 101

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

A painting of a skull and a pipe on a dark surface. The skull is the central focus, with its eye sockets and nasal cavity clearly visible. It is surrounded by a dark, textured background. A pipe lies next to the skull, partially obscured by shadow. The lighting is dramatic, highlighting the contours of the skull and the texture of the pipe.

# 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**

A painting of a skull and a pipe on a dark surface. The skull is the central focus, with its eye sockets and nasal cavity clearly visible. It is surrounded by shadows and highlights that emphasize its form. To the left of the skull, a portion of a pipe is visible, resting on a dark, textured surface. The background is dark and indistinct, making the skull stand out.

# 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

A painting depicting a scene from ancient Greek or Roman life. In the foreground, a woman in a red and white robe is seated at a table covered with a red cloth, engaged in some activity. Behind her, another woman in a yellow and white robe is kneeling. In the background, several men are visible, one of whom is carrying a large object on his shoulder. The setting includes classical architecture with columns.

# Audit Logs

- Often cost extra \$\$\$  
Ensure they're budgeted for
- May require apps, scripts,  
or add'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





Highlights

Reports

Audit log

Admin

Calendar

Drive

Login

Devices

Token

Groups

SAML

Google Chat

Currents

Voice

Google Meet

Users Accounts

Access Transparency

## 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 Status
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		



## 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@centralcoastalestateco.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	11z6Y1o5c4VPyHbbJXf_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	11z6Y1o5c4VPyHbbJXf_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	11z6Y1o5c4VPyHbbJXf_Enj0pl9nj9BGbH0Yx_aHRJA	Google Docs	Test Between Roger's		Shared Externally
Test From Roger's	roger@centralcoastalestateco.com edited an item	roger@centralcoastalestateco.com	Aug 5, 2021, 10:36:22 AM CST	Edit	1UhR8q8SKtbwGOISOCDLpOt8HxYgBD8ohppM Yodyq08U	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	11z6Y1o5c4VPyHbbJXf_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

+ Add a filter

Name	Status	Actions	Alerts	Rule type
shared drive - Test Custom reporting alert	Active	Send Notification		Reporting
important document Custom reporting alert	Active	Send Notification	On	Reporting
shared outside Custom reporting alert	Active	Send Notification	On	Reporting
important confidential doc Custom reporting alert	Active	Send Notification	On	Reporting
Prevent PII information sharing (US) Protect your organization from leaking PII data (US)	Inactive	Block external sharing	On	Data protection
failed login Custom reporting alert	Active	Send Notification	On	Reporting
Prevent PII information sharing (US) 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) 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](#)



slack

Slack Audit API App for Splunk is requesting permission to access the [REDACTED] Slack organization

What will Slack Audit API App for Splunk be able to view?

Content and info about you

What will Slack Audit API App for Splunk be able to do?

Administer Slack for your organization

Cancel Allow

A red rectangular box highlights the "Allow" button at the bottom of the dialog.

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

```
1  {
2      "entries": [
3          {
4              "id": "0123a45b-6c7d-8900-e12f-3456789gh0i1",
5              "date_create": 1521214343,
6              "action": "user_login",
7              "actor": {
8                  "type": "user",
9                  "user": {
10                      "id": "W123AB456",
11                      "name": "Charlie Parker",
12                      "email": "bird@slack.com"
13                  }
14              },
15              "entity": {
16                  "type": "user",
17                  "user": {
18                      "id": "W123AB456",
19                      "name": "Charlie Parker",
20                      "email": "bird@slack.com"
21                  }
22              },
23              "context": {
24                  "location": {
25                      "type": "enterprise",
26                      "id": "E1701NCCA",
27                      "name": "Birdland",
28                      "domain": "birdland"
29                  },
30                  "ua": "Mozilla\\5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit\\537.36 (KHTML, like Gecko) Chrome\\64.0.3282.1",
31                  "session_id": "847288190092",
32                  "ip_address": "1.23.45.678"
33              }
34          }
35      ]
36  }
```

```
},
"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\64.0.3282.186 Safari\537.36",
  "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
<a href="#">app_approved</a>	On workspaces that have <a href="#">admin approved apps</a> enabled, an app has been approved but not yet installed.
<a href="#">app_installed</a>	An app has been installed. If a custom integration had been disabled, this event will also be triggered if it is re-enabled.
<a href="#">app_removed_from_whitelist</a>	An app was removed from the allowed list.
<a href="#">app_resources_added</a>	<a href="#">Workspace apps</a> have the ability to request access to a <a href="#">specific resource on a workspace</a> , such as a channel or a DM, including wildcard resources (such as all public channels). This event is triggered when access has been granted.
<a href="#">app_resources_granted</a>	An app resource was granted.
<a href="#">app_restricted</a>	On workspaces that have <a href="#">admin approved apps</a> enabled, an app has been restricted and cannot be installed.
<a href="#">app_scopes_expanded</a>	An app has been granted additional access to resources on a workspace, via OAuth scopes. For most apps, this requires a re-install. For <a href="#">workspace apps</a> , this may also happen via the <a href="#">permissions API</a> .
<a href="#">app_token_preserved</a>	An app's token was preserved instead of revoked, usually due to an app owner or installer being removed from an organization.
<a href="#">app_uninstalled</a>	A Slack app was uninstalled.
<a href="#">bot_token_downgraded</a>	A bot app's token was downgraded to non-granular permissions.
<a href="#">bot_token_upgraded</a>	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 <code>team</code> 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 <code>team</code> 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 <code>team</code> 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 performed 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 group the API action falls under such as Embed.

## Access Logs



Edit Design

+ New Report



 Import Data Filter Sort Add Delete More

## Search Data

9

	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	lmb@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	lmb@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	lmb@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	lmb@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

## 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.

1



Filter by Time: All

Export

Settings

2

Prev

1

2

3

Next

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

3

Date	Location	Actor	Activity
Nov 04, 2021 09:48 PDT	Unavailable	Jane Rotanson jrotanson@acme.com	Viewed Jira issue <b>UAL-14</b>  <span data-bbox="1852 437 1872 459">1</span>
Nov 04, 2021 09:47 PDT	Unavailable	Jane Rotanson jrotanson@acme.com	Viewed Confluence blog <b>Janes blog update</b>
Nov 04, 2021 09:46 PDT	Unavailable	Jane Rotanson jrotanson@acme.com	Viewed Jira issue <b>UAL-16</b>

## 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](#)

to

 [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=Optional, two-step-verification=Optional, password strength=Weak, password expires=Never, idle session duration=30 days) for authentication policy <b>Not so special users</b>
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 <b>Not so special users</b>
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 <b>Special Users</b>
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 <b>Special Users</b>

- 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



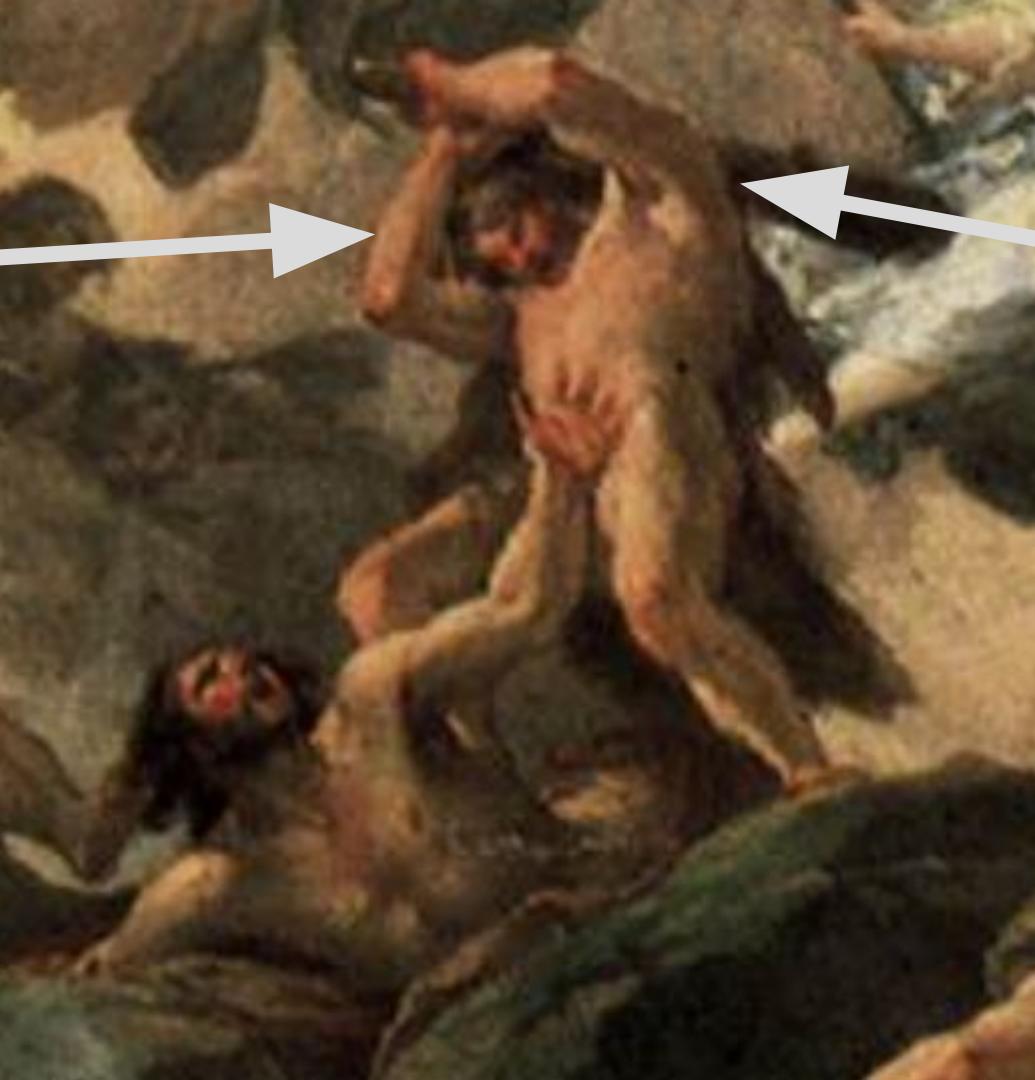
**Insiders**



**Insiders**



**Misconfigs**



# Insiders



A detailed black and white engraving depicting a group of scholars or philosophers in a study. In the center, a man is seated at a large wooden desk, intently focused on writing or drawing on a large sheet of paper. Several other figures are gathered around him; some are standing and looking down at his work, while others are seated in the background. The room is filled with classical elements, including a bust of a man on a pedestal and several small, idealized figures of men and women in various poses. A large, open book is visible on the right side of the desk. The floor is littered with objects that suggest a scholarly environment: a human skull, a zebra skull, a large ribcage, and other bones. The overall atmosphere is one of intense concentration and intellectual pursuit.

# 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

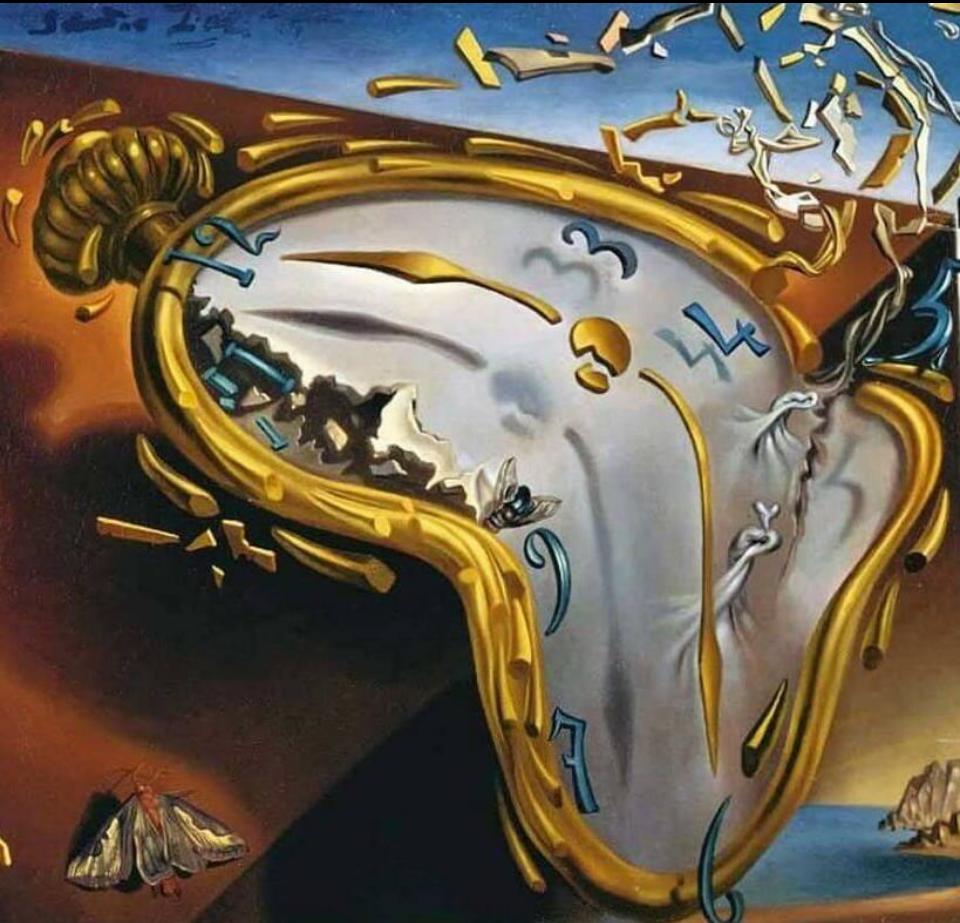
- **Inherently trusted**
- **Primarily associated with data theft before leaving the company**
- **Often non-technical users using simple techniques**
- **May require working with HR and Legal teams**

# 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

Google Admin    Search for users, groups or settings

Security > Alert center > Alert details

Gmail potential employee spoofing

Severity: Medium

Status: Not started

Enter assignee

No feedback selected

INVESTIGATE ALERT

DELETE ALERT

About this alert type

When a suspicious sender sends a message that has the name of a member of your organization in the display. [Learn more](#)

This sender is suspicious because of one or more of the following:

- they are unknown
- this sender (address with display name) and recipient have not interacted in the past
- have previously sent spam messages to your organization

To block this sender go to [manage blocked senders](#).

Automatic actions can be taken when this type of spoofing is detected. Manage these actions within [Safety Settings for Gmail](#).

Key details

Summary: test3@audit-citoyen.org sent 2 messages to 2 recipients.

Date: Apr 05, 2019, 10:18 PM IST (2019-04-05T22:18:00+05:30)

Actor: test3@audit-citoyen.org

Total messages: 2 [View message list](#)

Received by: 2 recipients  
kashyapp@google.com  
johndoe@google.com

Recommended action: To move messages to users' spam folder  
[MARK AS SPAM](#)

Detections: 1 security vendor flagged this domain as malicious

audit-citoyen.org

Registrar: OVH

Creation Date: 10 years ago

Last Updated: 11 months ago

Full report

Similar domains

VT Graph

Security vendors scanning results

Bfore.Ai PreCrime: malicious  
DNSB: Undetected  
Snort IP sample list: Undetected

CMC Threat Intelligence: Undetected  
Lionic: Undetected

Whois lookup

Admin City: REDACTED FOR PRIVACY  
Admin Country: REDACTED FOR PRIVACY  
Admin Email: 08a89e428e7531f8@a.o-w-o.info  
Admin Organization: REDACTED FOR PRIVACY  
Admin Postal Code: REDACTED FOR PRIVACY  
Admin State/Province: REDACTED FOR PRIVACY  
Creation Date: 2011-10-25T12:40:13Z  
Creation Date: 2011-10-25T14:40:13Z  
DNSSEC: unsigned  
Domain Name: AUDIT-CITOYEN.ORG  
Domain Name: audit-citoyen.org  
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited  
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited  
Name Server: NS.ATTAC.ORG  
Name Server: NS.MISKIN.FR  
Name Server: ns.attac.org  
Name Server: ns.miskin.fr  
Registrant City: lf84f166599d23ee  
Registrant Country: FR  
Registrant Email: 3834a27c1561872asfy.o-w-o.info  
Registrant Fax Ext: lf84f166599d23ee  
Registrant Fax: lf84f166599d23ee  
Registrant Name: lf84f166599d23ee  
Registrant Organization: 3432650ec37c945  
Registrant Phone Ext: lf84f166599d23ee  
Registrant Phone: lf84f166599d23ee  
Registrant Postal Code: lf84f166599d23ee  
Registrant State/Province: 3432650ec337c945  
Registrant Street: lf84f166599d23ee  
Registrant Abuse Contact Email: abuse@ovh.net

Related alerts

Summary Last update

Malware message detected post-delivery 2 same users. Jul 27, 2020

Alert history

# 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

The screenshot shows the Box Admin Console's Shield Dashboard. On the left, a sidebar menu includes Insights, Users & Groups, Content, Reports, Relay, Classification, Shield (selected), Governance, Platform, Account & Billing, and Enterprise Settings. The main dashboard features a large circular gauge indicating 33 alerts in the last 7 days. To the right, a prominent callout box displays "Anomalous Downloads" with a count of 2,287. Below this, a table lists four types of alerts: Suspicious Location (200), Suspicious Session (123), Malicious Content (112), and Malicious Location (2). A separate section titled "Top Alerts by User" shows activity for Franklin Johnson, Marta Baker, Anne Logan, and Glenn Santos. At the bottom, a blue banner highlights a "Malware Detected" event where a file was added by Jack Carlson with a priority of High and a risk score of 100.

Alert ID	Created	Rule Name	Rule Type	Target User	Priority	Risk Score
1984	Today 1:20 AM PST	Malware Detected	Malicious Content	benson@crocorp.com	Critical	100
120284	Today 1:19 AM PST	IM Travel	Impossible Travel	Marta Baker (baker@acme.com)	Critical	70
				Baker (baker@acme.com)	Medium	45
				Wilson Oliver (oliver@acme.com)	Medium	30
				Wilson Oliver (oliver@acme.com)	Low	20
14800	Today 2:34 PM PST	Test Rule 1	Suspicious Session	Wilson Oliver (oliver@acme.com)	Low	20
14982	Yesterday 1:13 PM PST	Domain Rule 2	Suspicious Session	Wilson Oliver (oliver@acme.com)	Low	15

# SaaS Defenses First-Party

Beacon BETA

Back ACKNOWLEDGED

## Suspicious searches in Confluence (38)

A user searched Confluence for multiple suspicious terms in a short period of time. This user's searches may relate to: credentials, passwords, cryptocurrency, sensitive or confidential content.

Total terms searched



Category	Count
Sensitive terms	3
Cryptocurrency	5
Credentials	7
Unuspicious	23

within 30 minutes

Related alerts

- Unusual Confluence page views activity OPEN
- Admin password reset CLOSED
- Suspicious searches in Confluence (23) OPEN

Details

Site	blackcatbakery.atlassian.net
Alert ID	63dba78fba0a0c615f46
Event time	Feb 04, 2023 6:45 AM PST
IP Address	103.136.43.1
Location	Moscow, Russia

Actor

Account	Jane Rotanson
Position	Engineering Manager
Account age	3y 6mo

# SaaS Defenses First-Party

Microsoft 365 security

Endpoints

- Search
- Device inventory
- Vulnerability management
- Partners and APIs
- Evaluation & tutorials
- Configuration management

Email & collaboration

- Investigations
- Explorer
- Submissions
- Review
- Campaigns
- Threat tracker
- Exchange message trace
- Attack simulation training
- Policies & rules

Reports

Health

Permissions & roles

Settings

## Home



Welcome to the Microsoft 365 security center

Intro Next steps Give feedback

Welcome to the Microsoft 365 security center, the new home for monitoring and managing security across your Microsoft identities, data, devices, apps, and infrastructure. [Learn more about the Microsoft 365 security center](#)

Next Close

Guided tour What's new? Community Add cards

Threat analytics	
<b>1 active threat</b>	
Adwind RAT lands using DDE	
CVE-2021-1732 - Elevation of Privilege in Win32k	
CVE-2020-1472 Netlogon EoP vulnerability	
Active alerts	Resolved alerts
See more	

Users at risk	
<b>8 users at risk</b>	
	
High Risk	Medium Risk
Low risk	
View all users	

Users with threat detections	
Users with threat detections	
User	Alerts
System Administrator	6
Barbara Moreland	6
M365D Global Reader	5
Eric Gubbels	1

Devices at risk	
<b>4 device(s) at risk</b>	
Device	Risk level
m365d-dc01	High
robertot-pc	High
barbaram	

Need help? Give feedback



# SaaS App Detections

A dramatic painting by Georges de la Tour, titled "The Operation," depicting a surgeon operating on a patient's arm while another man looks on. The scene is set in a dimly lit room with a table covered in surgical instruments.

# 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**



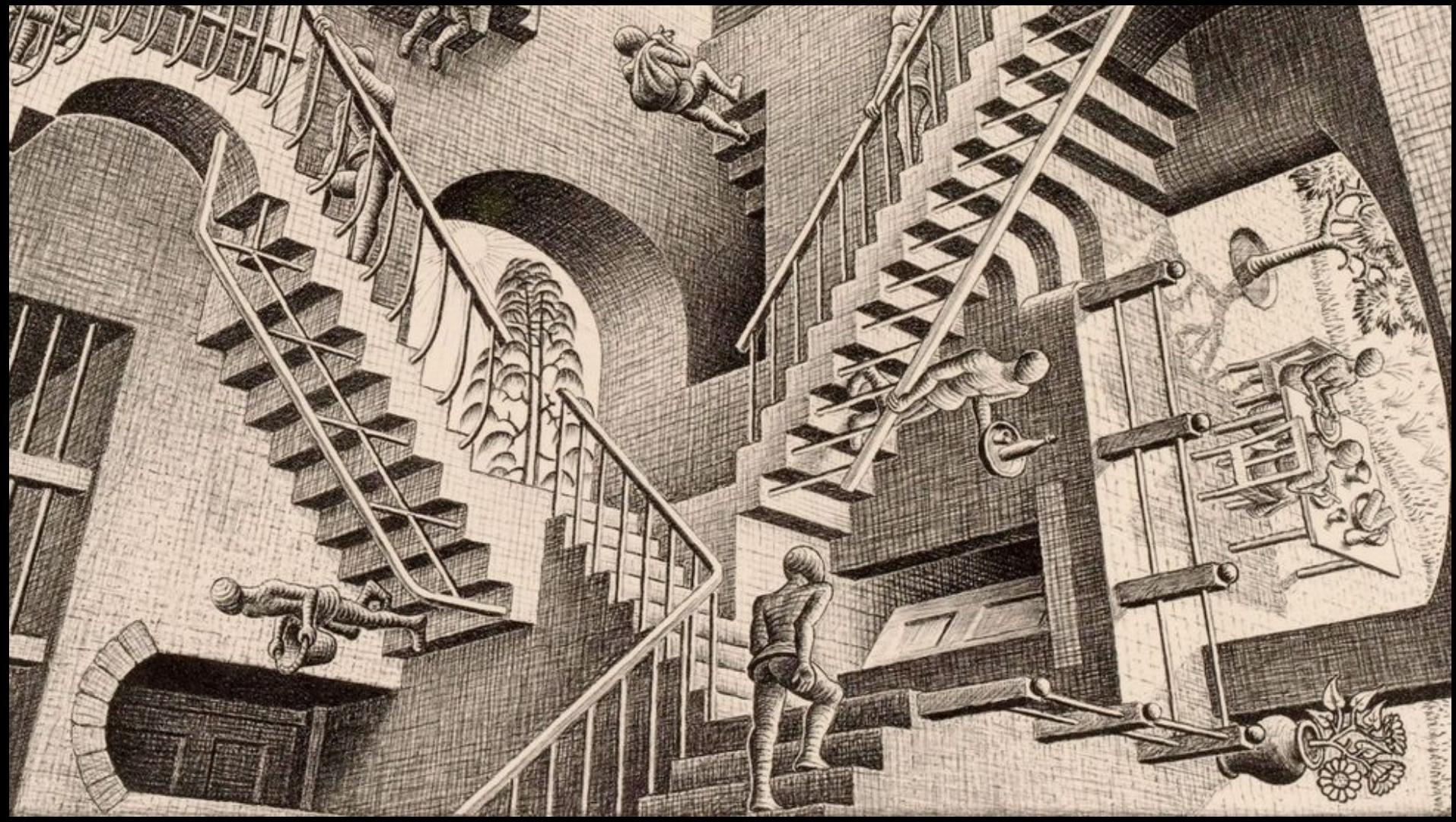
## Stopping Attackers & Incidents

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

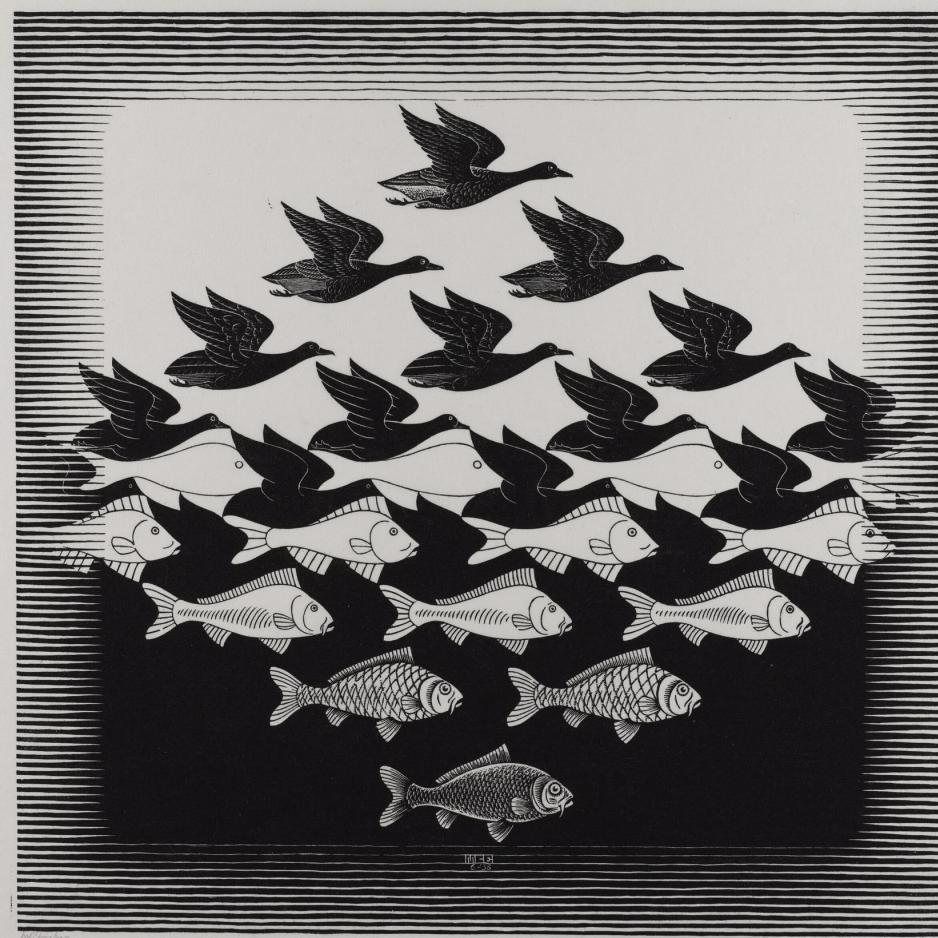


## Stopping Attackers & Incidents

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

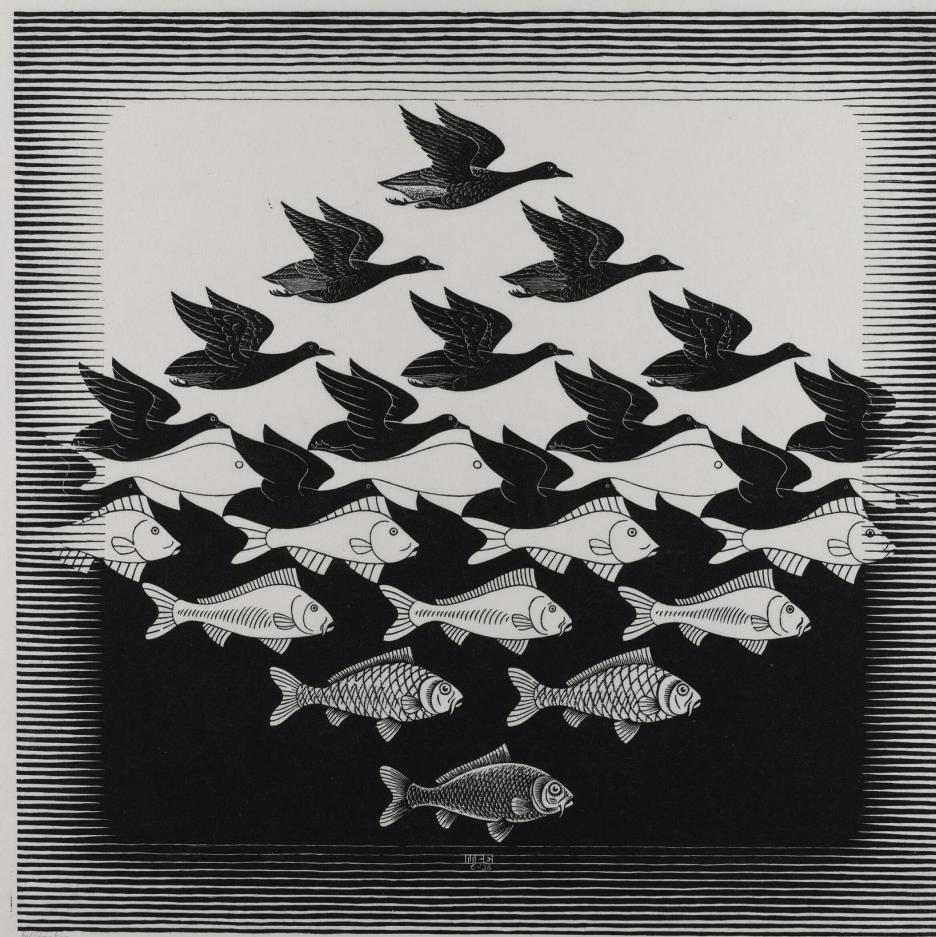


# Advanced Detections with Audit Logs: DECEPTION



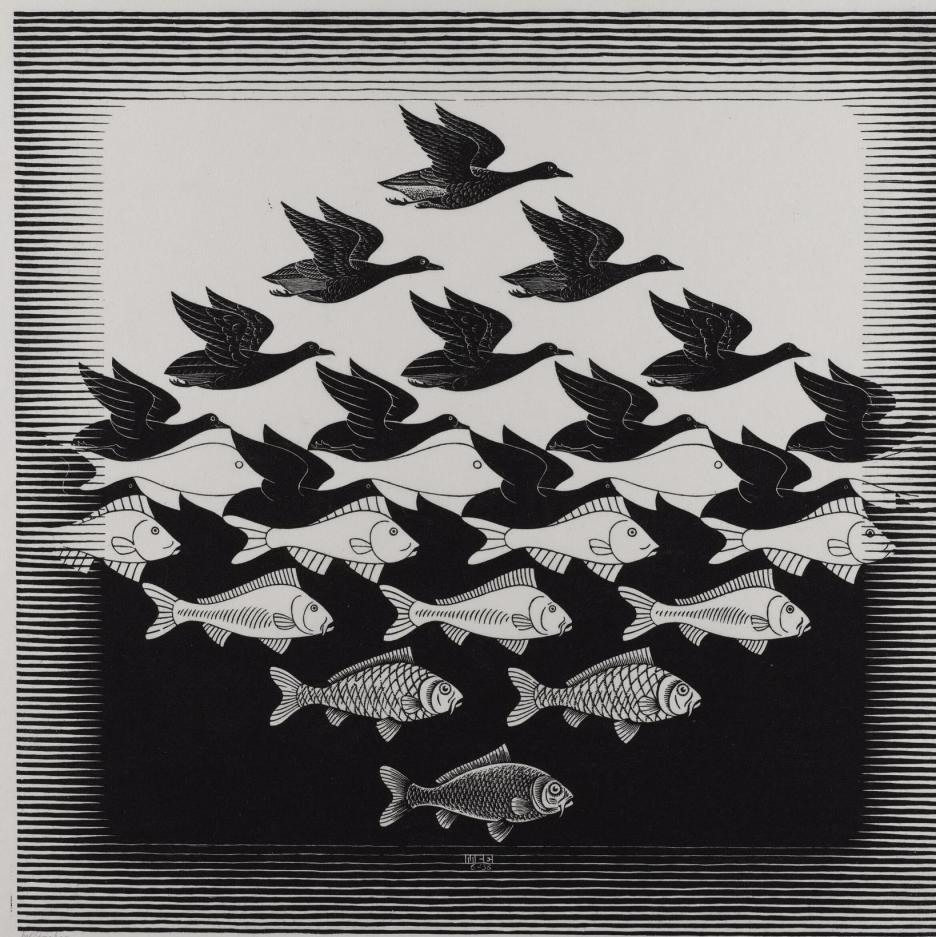
# Advanced Detections with Audit Logs: DECEPTION

- Cover the basics first



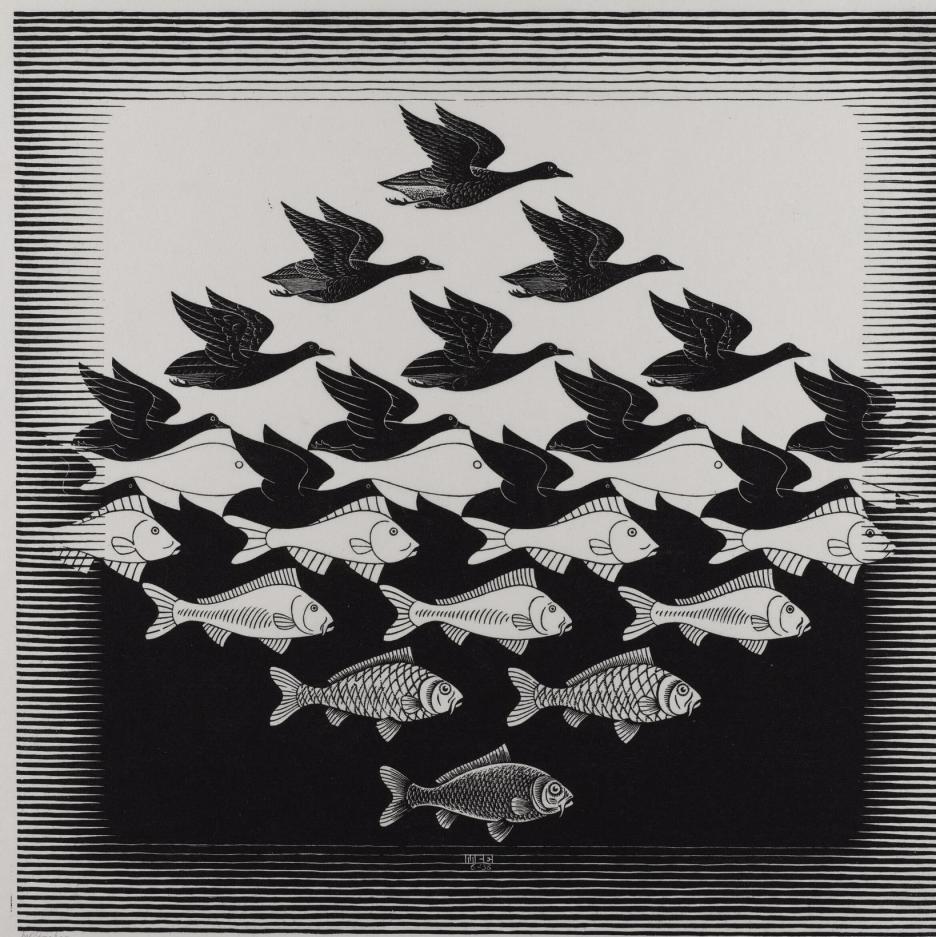
# Advanced Detections with Audit Logs: DECEPTION

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



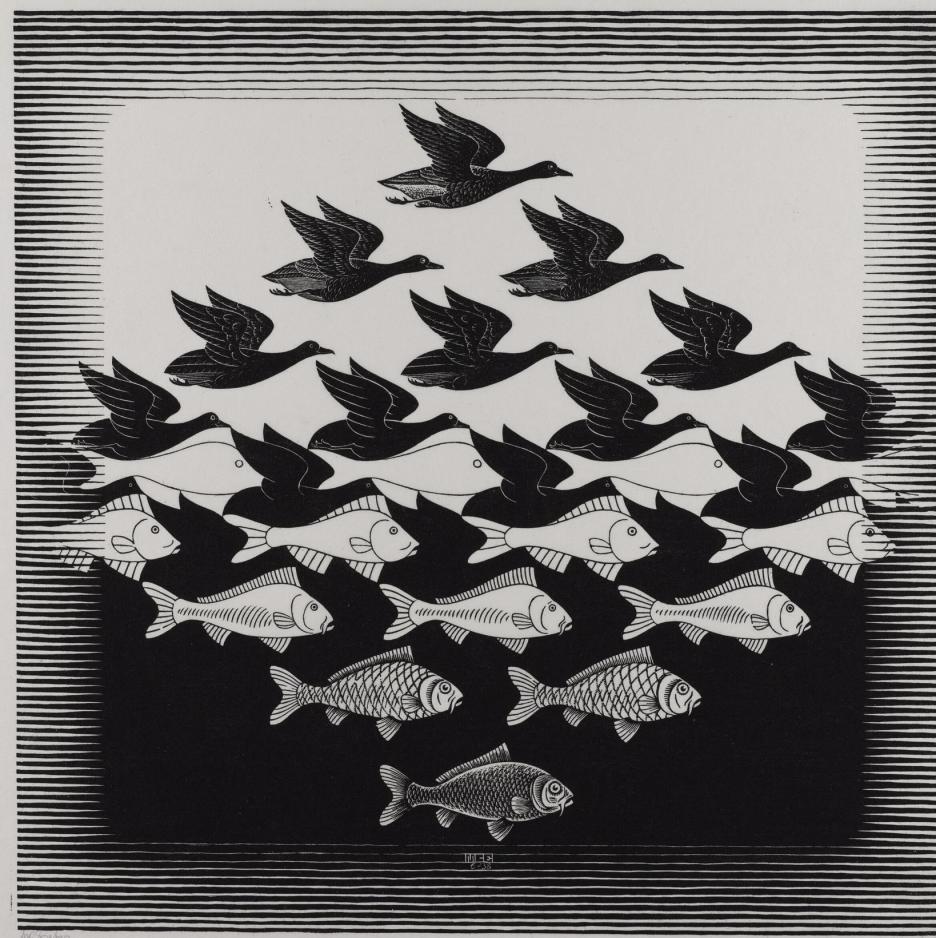
# Advanced Detections with Audit Logs: DECEPTION

- 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 😈

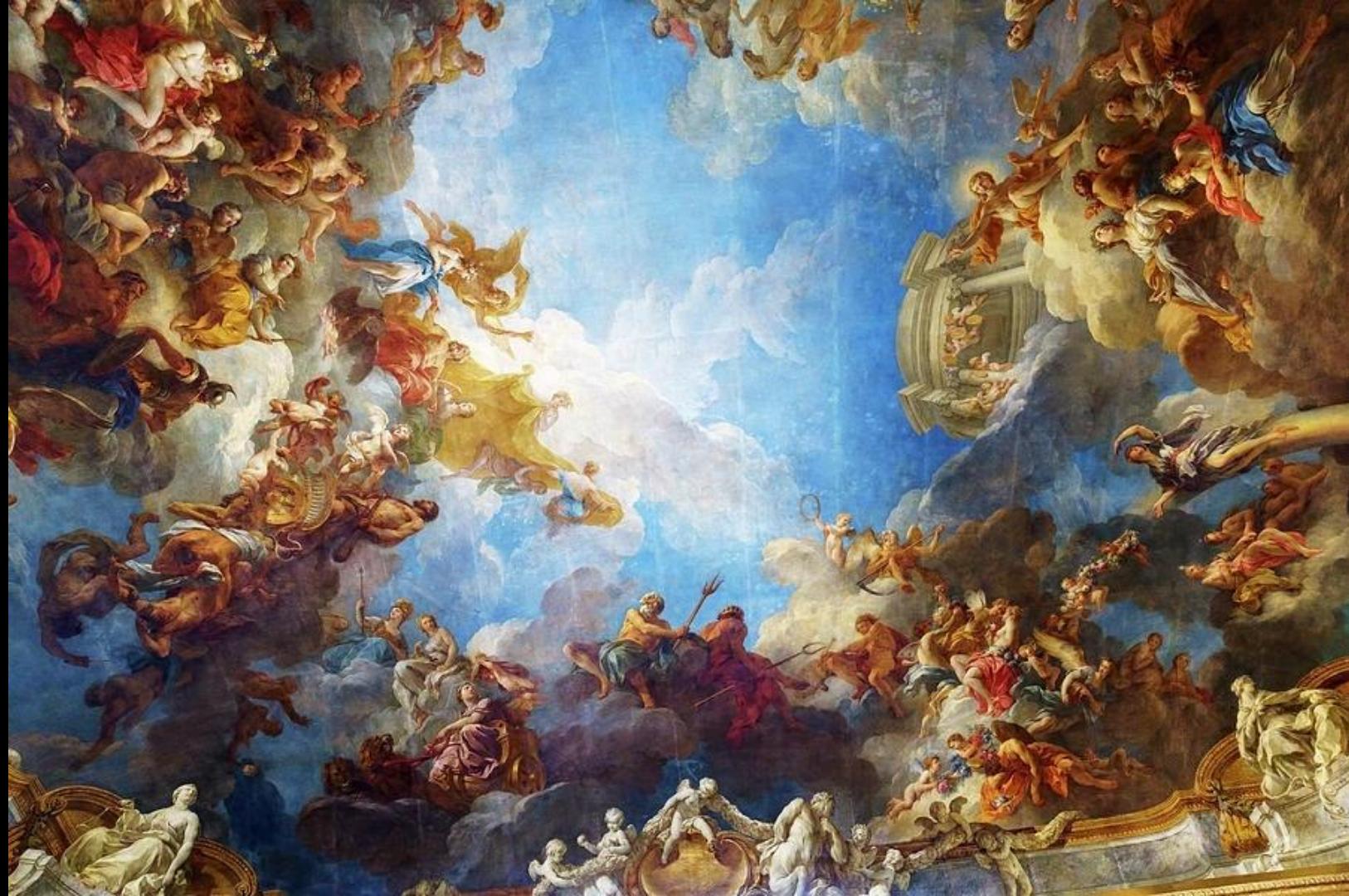












# Recap



# 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](mailto:JeremyNGalloway@gmail.com)