SECURITY IN A MULTI-CLOUD WORLD

Ben Johnson
Co-founder and CTO

OBSIDIAN

BACKGROUND CHECK // BEN JOHNSON

Co-Founder and CTO, Obsidian Security

Co-founder and former CTO of Carbon Black, built the first EDR product; Previously, NSA CNO and AI Lab

1st Technical Advisor (Amicus Curiae) to US FISA Court

Employment

2000 → 2010 → 2017

National Security Agency → Carbon Black. → Obsidian

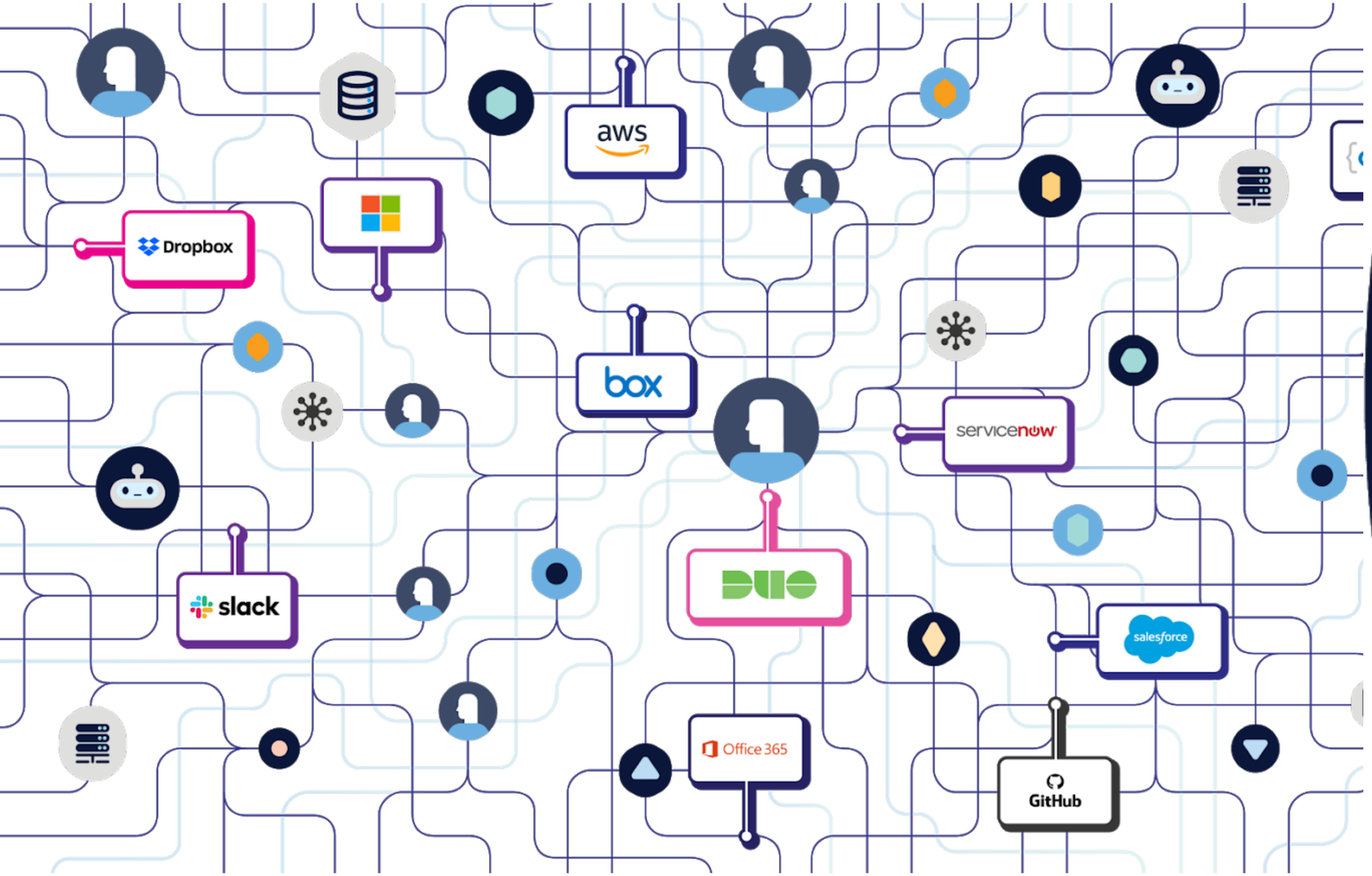
Startup Boards

Senrio

Capsule8

Evolve Security Academy

CLOUD IS ACCELERATING BUSINESS



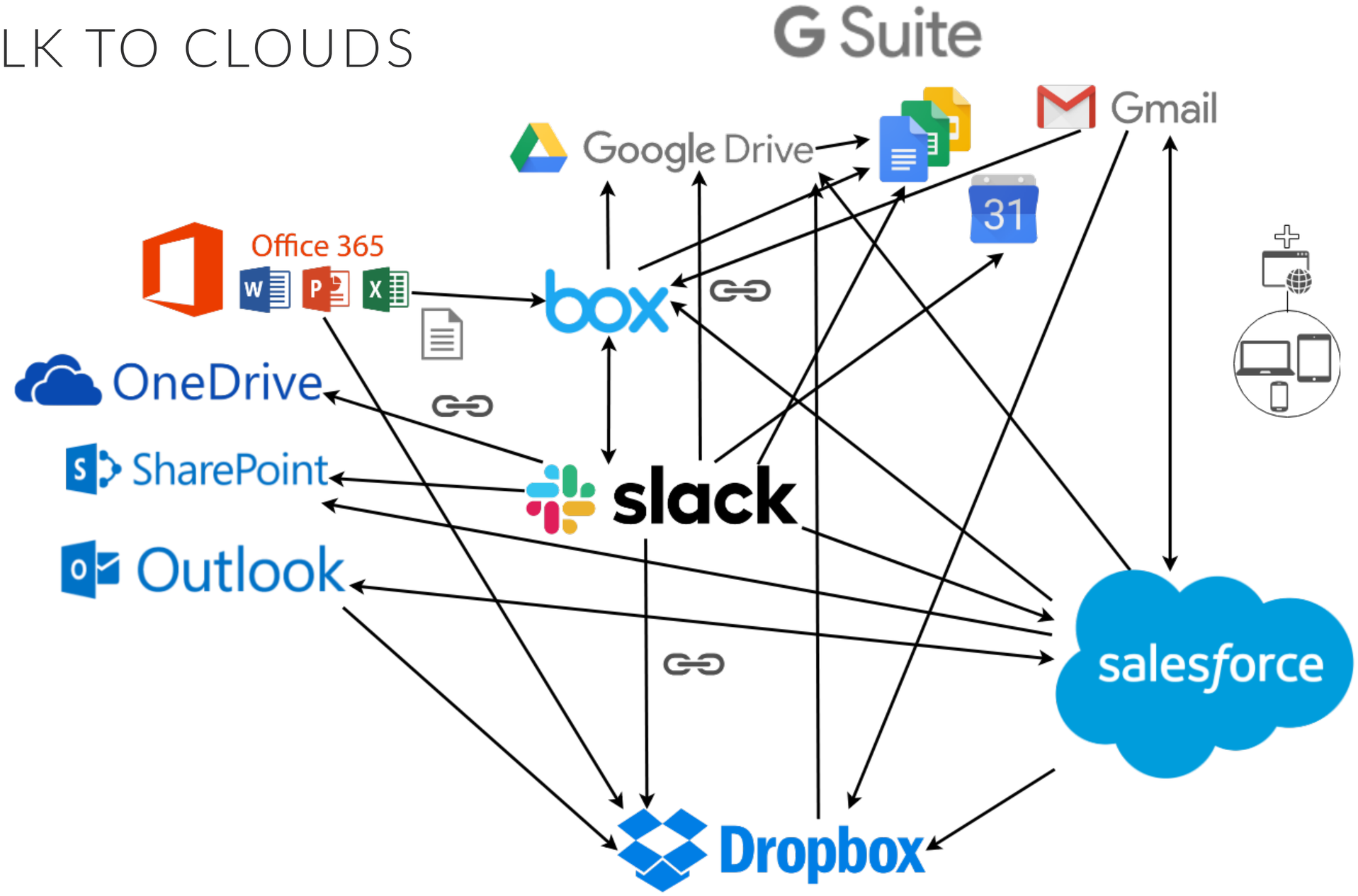
SECURITY IMPERATIVE:
ENABLE BUSINESS TO ADVANCE ITS MISSION … SAFELY!

AND IF YOU DON'T HAVE SAAS YET, IT'S COMING

Companies are picking a "cloud stack" of business services…the difference being these new technologies are cloud-based and designed for collaboration.

EMAIL	G Suite, Office 365, zimbra, PanTerra, INTERMEDIA
WORD PROCESSOR	Office 365, Google Docs, iWork, ATLASSIAN, Adobe Creative Cloud
COMMUNICATION	slack, RingCentral, ZOOM, asana, GoToMeeting
CONTENT MANAGEMENT	Google Drive, OneDrive, Dropbox, box, CITRIX ShareFile
INFORMATION TECHNOLOGY	happyfox, freshdesk, LogicMonitor, ManageEngine AssetExplorer, servicenow
SALES & MARKETING	HubSpot, salesforce, ZOHO, freshsales, Microsoft Dynamics CRM
FINANCE	intuit QuickBooks, NETSUITE, FRESHBOOKS, Acumatica The Cloud ERP
HUMAN RESOURCES	GUSTO, bambooHR, DEPUTY, zenefits, SAP SuccessFactors
SECURITY	DUO, okta, idaptive, dashlane, Acronis

CLOUDS TALK TO CLOUDS



WHO PROTECTS CLOUD? (HINT: YOU)

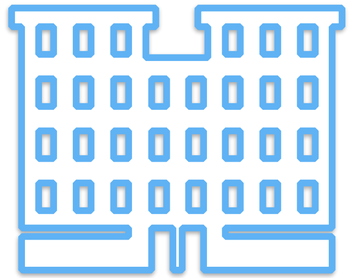
75% OF CLOUD IS SAAS … AND STILL YOUR PROBLEM

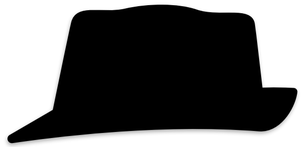
The SaaS Provider handles all aspects **except for identity and access management, client devices controls, and data accountability.**

The Customer (you), therefore, must **understand users, devices & data related to that service.**

CLOUD SECURITY NEEDS TO BE A PRIORITY

"89% of companies use SaaS" *





"Up to 95% of cloud breaches occur due to human errors." **

"...someone in your organization should do regular audits to detect potential abuse" - Salesforce

- ALWAYS ON, ALWAYS REACHABLE TARGETS
- USERS OVERSHARE AND AUTHORIZE APPS
- LACK OF EXPERTISE IN CLOUD DETECTION
- OVER-ACCESS INCREASES INSIDER RISK
- POORLY UNDERSTOOD, DISPARATE AUDIT LOGS

* Source: IDG

** Source: Gartner

CLOUD SECURITY IS THE SAME … AND DIFFERENT

- Enable the business to advance its mission … SAFELY.

- Protect the business but also allow for the business — productivity, cost savings, and innovation are largely why organizations are going to SaaS/PaaS/IaaS. If you (as security) hurt these, you will not be popular.

    - Review and monitor access
    - Review and monitor privileges
    - Review and monitor configurations
    - Review and monitor behavior

So not that different from on-premise?

Yet the networks, assets, applications might not be under any of your control.

WHAT'S SECURITY'S AIM FOR CLOUD?

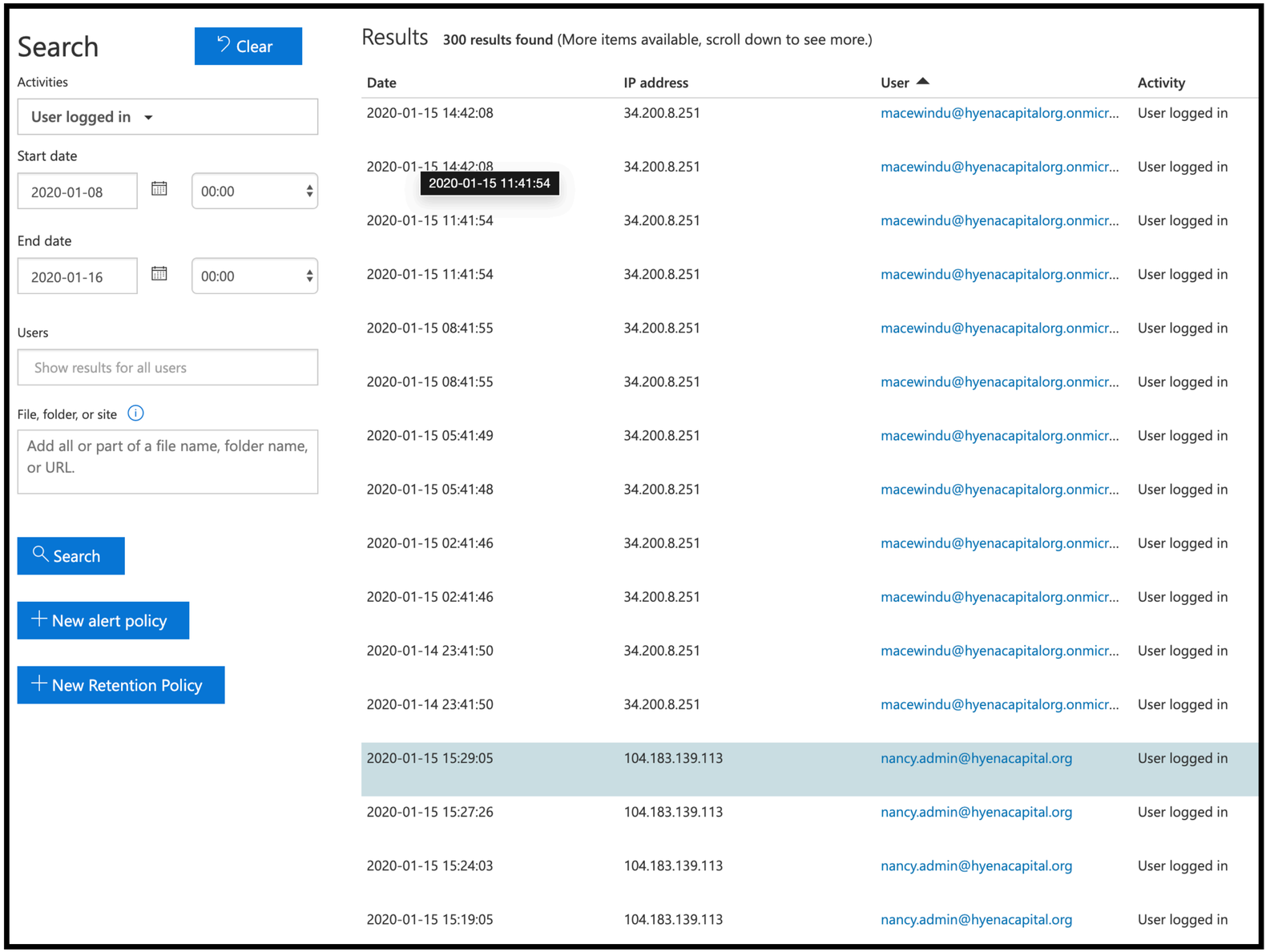
- Protect account access
- Enable responsible use
- Enable responsible collaboration
- Detect misuse, compromise, and other unwanted behavior
- Investigate and cleanup when there's a problem

"The absence of disease does not mean health."

INTRO TO SAAS CLOUD DETECTION

- Often, the primary goal for SaaS is to keep the adversaries out. This is a smart primary goal.
- Then you likely want to understand privileged activity, and any changes to privileged users.
- From here, understanding how your information might be exposed, such as sharing files broadly or buckets created.
- Then, observing any increases to the surface area by adding third party apps and/or new user accounts.
- Finally, insider threats, especially in IP-heavy companies and industries

DETECTION: LOGINS (O365)



Timestamps, IP-addresses, user, results; some search capabilities

DETECTION: LOGINS (GSUITE)

Login

Add a filter

Event Description	IP Address	Date	Login Type
Nancy Admin logged in	104.183.139.113	Jan 15, 2020, 2:45:05 PM PST	Google Password
Nancy Admin logged in	104.183.139.113	Jan 15, 2020, 9:19:39 AM PST	Google Password
Nancy Admin failed to login	104.183.139.113	Jan 15, 2020, 9:19:19 AM PST	Google Password
John User logged in	104.183.139.113	Jan 14, 2020, 11:45:22 AM PST	Google Password
John User logged in	104.183.139.113	Jan 14, 2020, 11:44:45 AM PST	Google Password
Nancy Admin logged in	104.183.139.113	Jan 10, 2020, 9:15:07 AM PST	Google Password
Mike Smith failed to login	104.183.139.113	Jan 9, 2020, 8:32:52 AM PST	Unknown
Mike Smith failed to login	104.183.139.113	Jan 9, 2020, 8:32:35 AM PST	Google Password
Mike Smith failed to login	104.183.139.113	Jan 9, 2020, 8:32:31 AM PST	Google Password
Nancy Admin logged in	2600:8802:2000:2360:dd83:4539:da9f:ec	Jan 9, 2020, 12:41:36 AM PST	Google Password
Nancy Admin logged in	104.183.139.113	Jan 8, 2020, 2:12:50 PM PST	Google Password

Some useful information but lacking a lot of context

DETECTION: LOGINS (SALESFORCE)

Login Time	Username	Source IP	Subdivision	City	Country	Login Type	Status	Browser	Platform	Application	Login URL
1/15/2020 5:28:30 PM PST	[redacted]@obsidiansecurity.com	52.26.[redacted]	Oregon	Boardman	United States	Remote Access 2.0	Success	Unknown	Unknown	Demisto	login.salesforce.com
1/15/2020 5:27:30 PM PST	[redacted]on@obsidiansecurity.com	54.174[redacted]	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:27:30 PM PST	[redacted]on@obsidiansecurity.com	54.174[redacted]	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:27:30 PM PST	[redacted]@obsidiansecurity.com	52.26.[redacted]	Oregon	Boardman	United States	Remote Access 2.0	Success	Unknown	Unknown	Demisto	login.salesforce.com
1/15/2020 5:27:30 PM PST	[redacted]on@obsidiansecurity.com	54.174[redacted]	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:27:30 PM PST	[redacted]on@obsidiansecurity.com	54.174[redacted]	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:27:30 PM PST	[redacted]on@obsidiansecurity.com	54.174[redacted]	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:27:30 PM PST	[redacted]on@obsidiansecurity.com	54.174[redacted]	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:27:30 PM PST	[redacted]on@obsidiansecurity.com	54.174[redacted]	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:27:30 PM PST	[redacted]on@obsidiansecurity.com	54.174[redacted]	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:27:30 PM PST	[redacted]on@obsidiansecurity.com	54.174[redacted]	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:27:30 PM PST	[redacted]on@obsidiansecurity.com	54.174[redacted]	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:27:30 PM PST	[redacted]on@obsidiansecurity.com	54.174[redacted]	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:26:30 PM PST	[redacted]@obsidiansecurity.com	52.26.[redacted]	Oregon	Boardman	United States	Remote Access 2.0	Success	Unknown	Unknown	Demisto	login.salesforce.com
1/15/2020 5:25:30 PM PST	[redacted]@obsidiansecurity.com	52.26.[redacted]	Oregon	Boardman	United States	Remote Access 2.0	Success	Unknown	Unknown	Demisto	login.salesforce.com
1/15/2020 5:24:30 PM PST	[redacted]@obsidiansecurity.com	52.26.[redacted]	Oregon	Boardman	United States	Remote Access 2.0	Success	Unknown	Unknown	Demisto	login.salesforce.com
1/15/2020 5:24:26 PM PST	[redacted]on@obsidiansecurity.com	54.174[redacted]	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:24:26 PM PST	[redacted]on@obsidiansecurity.com	54.174[redacted]	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:23:30 PM PST	[redacted]@obsidiansecurity.com	52.26.[redacted]	Oregon	Boardman	United States	Remote Access 2.0	Success	Unknown	Unknown	Demisto	login.salesforce.com
1/15/2020 5:22:30 PM PST	[redacted]@obsidiansecurity.com	52.26.[redacted]	Oregon	Boardman	United States	Remote Access 2.0	Success	Unknown	Unknown	Demisto	login.salesforce.com
1/15/2020 5:22:15 PM PST	[redacted]on@obsidiansecurity.com	54.174[redacted]	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:22:15 PM PST	[redacted]on@obsidiansecurity.com	54.174[redacted]	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:22:14 PM PST	[redacted]on@obsidiansecurity.com	54.174[redacted]	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:22:14 PM PST	[redacted]on@obsidiansecurity.com	54.174[redacted]	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:22:14 PM PST	[redacted]on@obsidiansecurity.com	54.174[redacted]	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com

Show me fewer / more records per list page

Providing more context than some other systems

DETECTION: LOGINS SUMMARY

- What should you care about when it comes to logins?
    - Admin login times, locations
    - Unusual login locations across user population
    - Spikes in failed logins for a particular user
    - IP or Geo targeting many users (password sprays, credential stuffing, etc)

DETECTION: ACCESS / PRIVILEGE CHANGES (O365)

Date	IP address	User	Activity	Item
2019-12-02 15:11:02	<null>	nancy.admin@hyenacapital....	Added member to Role	ben.johnson@hyenacapital....
2019-11-13 08:07:33	<null>	nancy.admin@hyenacapital....	Added member to Role	mmyers@hyenacapital.org
2019-11-13 08:07:32	<null>	nancy.admin@hyenacapital....	Added member to Role	mmyers@hyenacapital.org
2019-11-13 08:07:32	<null>	nancy.admin@hyenacapital....	Added member to Role	mmyers@hyenacapital.org
2019-11-13 08:07:32	<null>	nancy.admin@hyenacapital....	Added member to Role	mmyers@hyenacapital.org
2019-11-06 20:37:50	<null>	nancy.admin@hyenacapital....	Added member to Role	macewindu@hyenacapitalo...
2019-11-04 14:55:44	<null>	john.user@hyenacapital.org	Added member to group	john.user@hyenacapital.org
2019-10-23 12:16:31	<null>	nancy.admin@hyenacapital....	Added member to Role	se-demo@hyenacapital.org
2019-10-23 12:16:30	<null>	nancy.admin@hyenacapital....	Added member to Role	se-demo@hyenacapital.org
2019-10-23 12:16:30	<null>	nancy.admin@hyenacapital....	Added member to Role	se-demo@hyenacapital.org
2019-10-23 12:16:29	<null>	nancy.admin@hyenacapital....	Added member to Role	se-demo@hyenacapital.org
2019-10-23 12:16:29	<null>	nancy.admin@hyenacapital....	Added member to Role	se-demo@hyenacapital.org
2019-10-23 12:16:29	<null>	nancy.admin@hyenacapital....	Added member to Role	se-demo@hyenacapital.org
2019-10-23 12:16:28	<null>	nancy.admin@hyenacapital....	Added member to Role	se-demo@hyenacapital.org
2019-10-23 12:16:28	<null>	nancy.admin@hyenacapital....	Added member to Role	se-demo@hyenacapital.org
2019-10-22 20:29:26	<null>	nancy.admin@hyenacapital....	Added member to group	ben.johnson@hyenacapital....

ExtendedProperties:


```
[
  {
    "Name": "resultType",
    "Value": "Success"
  },
  {
    "Name": "auditEventCategory",
    "Value": "RoleManagement"
  },
  {
    "Name": "nCloud",
    "Value": "<null>"
  },
  {
    "Name": "actorContextId",
    "Value": "fccf267d-8661-42ed-8bd7-8a34a7cf8646"
  },
  {
    "Name": "actorObjectId",
    "Value": "f901fa8c-b955-469a-ad49-d960d742867c"
  },
  {
    "Name": "actorObjectClass",
    "Value": "User"
  },
  {
    "Name": "actorUPN",
    "Value": "nancy.admin@hyenacapital.org"
  },
  {
    "Name": "actorPUID",
    "Value": "10037FFEAA677314"
  },
  {
    "Name": "teamName",
    "Value": "MSODS."
  },
  {
    "Name": "targetContextId",
    "Value": "fccf267d-8661-42ed-8bd7-8a34a7cf8646"
  },
  {
    "Name": "targetObjectId",
    "Value": "6dec3fe0-9127-458d-84d1-ae75b950a3b9"
  },
  {
    "Name": "extendedAuditEventCategory",
    "Value": "Role"
  },
  {
    "Name": "targetUPN",
    "Value": "mmyers@hyenacapital.org"
  },
```

DETECTION: ACCESS / PRIVILEGE CHANGES (G SUITE)

Role Assign	Role **Threat Hunter** assigned to user **threat.hunter@hyenacapital.net**	Nancy Admin	Sep 11, 2019, 2:25:06 PM PDT	104.183.139.113
Role Creation	New role **Threat Hunter** created (role_id: {25916594752323600})	Nancy Admin	Sep 11, 2019, 2:24:43 PM PDT	104.183.139.113
Assign User License	A license for **G Suite** product and **G Suite Enterprise** sku was assigned to the user **threat.hunter@hyenacapital.net**	Google System	Sep 11, 2019, 2:23:40 PM PDT	
User Creation	**threat.hunter@hyenacapital.net** created	Nancy Admin	Sep 11, 2019, 2:23:30 PM PDT	104.183.139.113

User Suspension	**rchavali@hyenacapital.net** suspended	Nancy Admin	Oct 29, 2019, 2:28:48 PM PDT	104.183.139.113
Assign User License	A license for **G Suite** product and **G Suite Enterprise** sku was assigned to the user **rchavali@hyenacapital.net**	Google System	Oct 29, 2019, 2:23:48 PM PDT	
User Creation	**rchavali@hyenacapital.net** created	Nancy Admin	Oct 29, 2019, 2:23:38 PM PDT	104.183.139.113
Revoke User License	A license for **G Suite** product and **G Suite Enterprise** sku was revoked from user **rchavali@hyenacapital.net**	Google System	Oct 29, 2019, 1:25:30 PM PDT	
User Deletion	**rchavali@hyenacapital.net** deleted	Nancy Admin	Oct 29, 2019, 1:25:19 PM PDT	

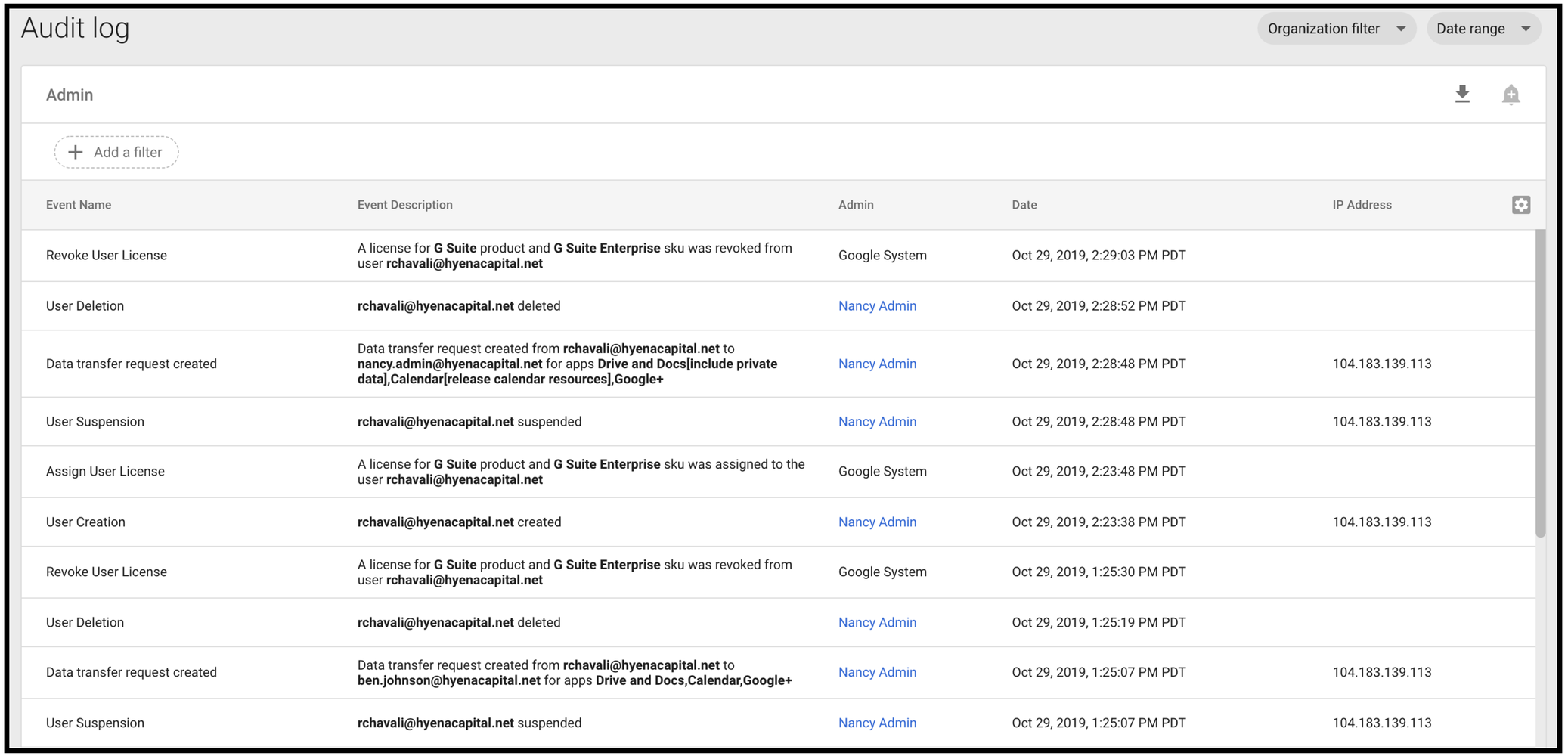
New user added A new user has been added to the domain.	Active	Send Notification	--	System defined	1/30/19 7:40 PM

User granted Admin privilege A user is granted an admin privilege.	Active	Send Notification	--	System defined	1/30/19 7:39 PM

DETECTION: ACCESS / PRIVILEGE SUMMARY

- What should you care about when it comes to access / privilege changes?
  - New privileges granted! (New admins, additional roles, etc)
  - Removal of privileged access (should be rare, want to scrutinize)
  - Specific grants, like Mailbox delegation
  - If possible, correlate new accounts to a source of truth (HR system)
  - Keep an eye on those contractors, consultants, and service providers

DETECTION: ADMIN ACTIVITY (GSUITE)



Audit log

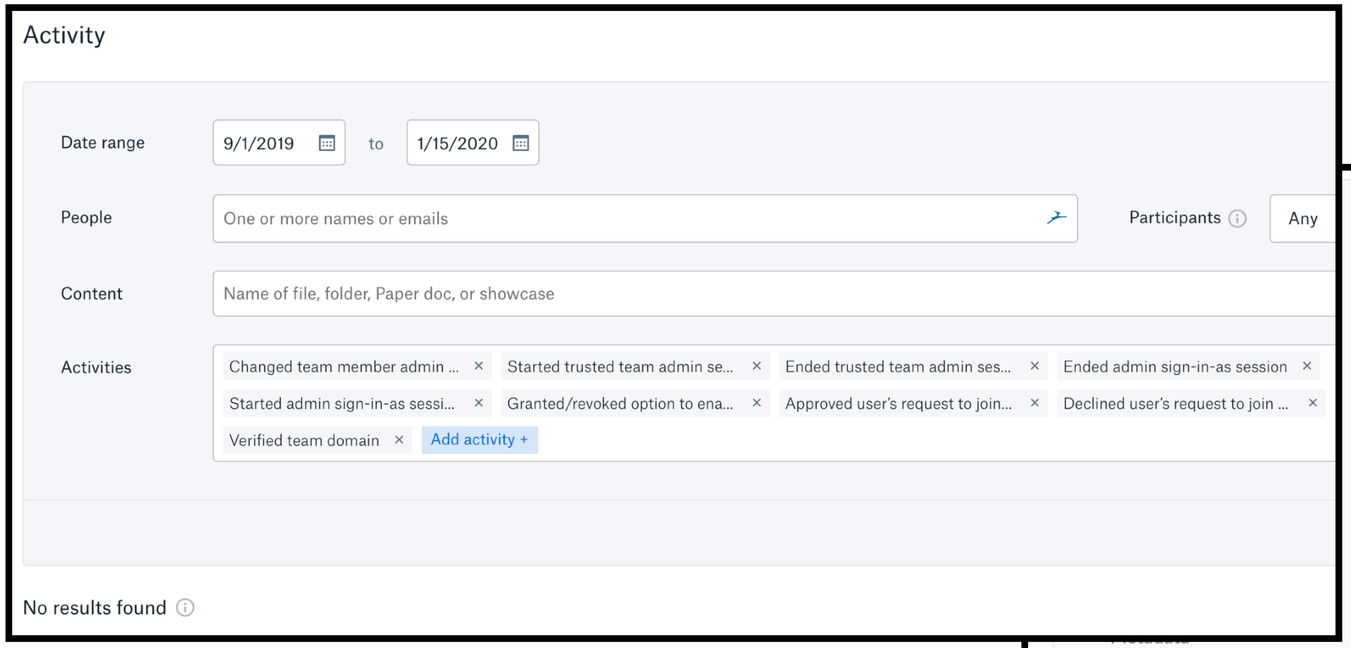
Organization filter | Date range

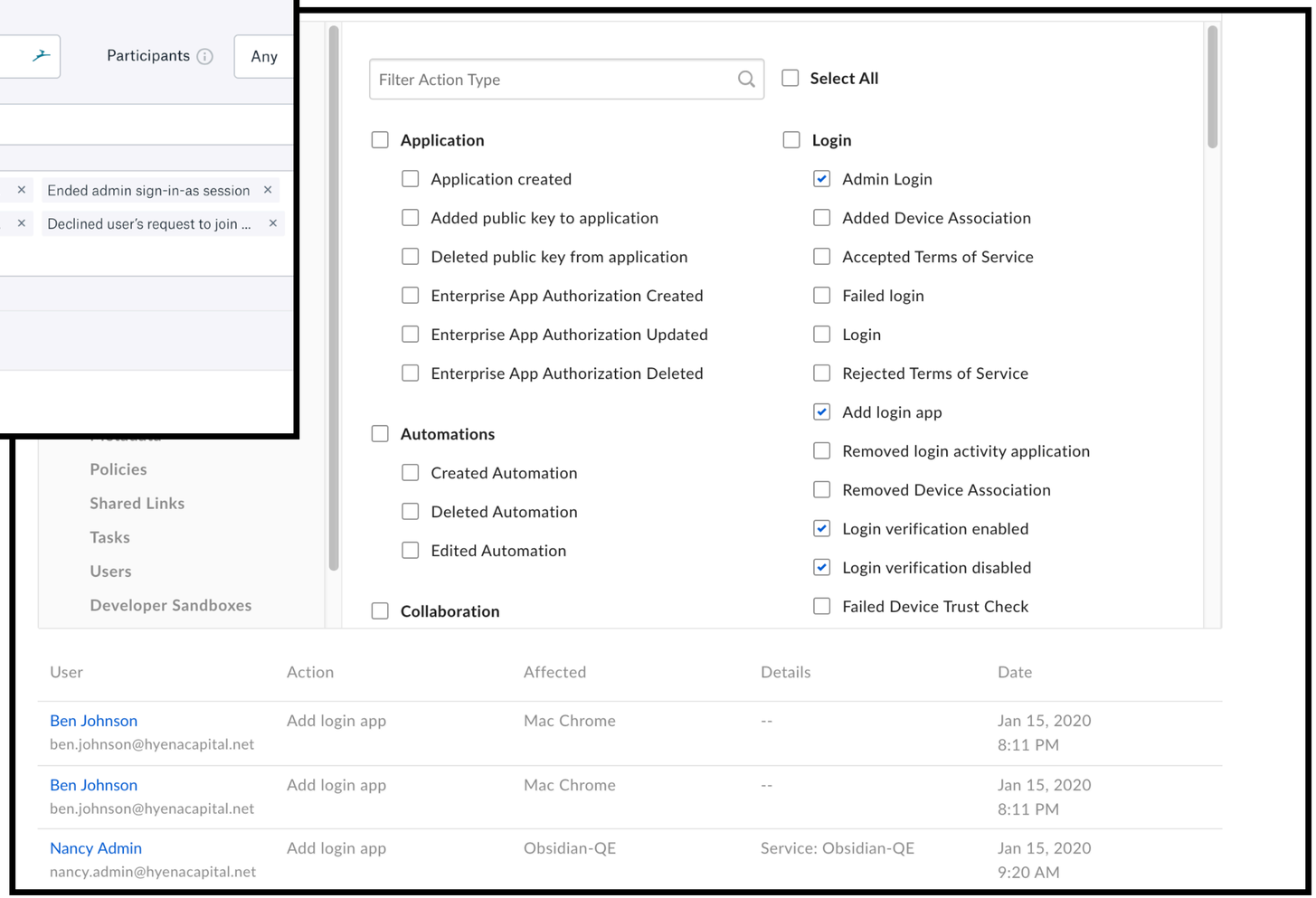
Admin

Add a filter

Event Name	Event Description	Admin	Date	IP Address
Revoke User License	A license for **G Suite** product and **G Suite Enterprise** sku was revoked from user **rchavali@hyenacapital.net**	Google System	Oct 29, 2019, 2:29:03 PM PDT	
User Deletion	**rchavali@hyenacapital.net** deleted	Nancy Admin	Oct 29, 2019, 2:28:52 PM PDT	
Data transfer request created	Data transfer request created from **rchavali@hyenacapital.net** to **nancy.admin@hyenacapital.net** for apps **Drive and Docs[include private data],Calendar[release calendar resources],Google+**	Nancy Admin	Oct 29, 2019, 2:28:48 PM PDT	104.183.139.113
User Suspension	**rchavali@hyenacapital.net** suspended	Nancy Admin	Oct 29, 2019, 2:28:48 PM PDT	104.183.139.113
Assign User License	A license for **G Suite** product and **G Suite Enterprise** sku was assigned to the user **rchavali@hyenacapital.net**	Google System	Oct 29, 2019, 2:23:48 PM PDT	
User Creation	**rchavali@hyenacapital.net** created	Nancy Admin	Oct 29, 2019, 2:23:38 PM PDT	104.183.139.113
Revoke User License	A license for **G Suite** product and **G Suite Enterprise** sku was revoked from user **rchavali@hyenacapital.net**	Google System	Oct 29, 2019, 1:25:30 PM PDT	
User Deletion	**rchavali@hyenacapital.net** deleted	Nancy Admin	Oct 29, 2019, 1:25:19 PM PDT	
Data transfer request created	Data transfer request created from **rchavali@hyenacapital.net** to **ben.johnson@hyenacapital.net** for apps **Drive and Docs,Calendar,Google+**	Nancy Admin	Oct 29, 2019, 1:25:07 PM PDT	104.183.139.113
User Suspension	**rchavali@hyenacapital.net** suspended	Nancy Admin	Oct 29, 2019, 1:25:07 PM PDT	104.183.139.113

DETECTION: ADMIN ACTIVITY (DROPBOX, BOX)





DETECTION: BROADLY SHARED FILES (GSUITE)

Drive

Item Visibility Change: Internal to External ⊗ + Add a filter

Item name	Event Description	User	Date	Event Name	Item Id	Item Type	Owner	Prior Visibility	Visibility
DO_NOT_GET_LOST	Nancy Admin changed link sharing visibility from **Anyone with the link within the domain** to **Private** for **hyenacapital.net**	Nancy Admin	Oct 29, 2019, 3:25:28 PM PDT	Link Sharing visibility change	1L2VfsYE__XkwUBgw9U80SLyjznfJrgyugI9SBYyiGmM	Google Docs	nancy.admin@hyenacapital.net	Anyone with the link within the domain	Public on the web
DO_NOT_GET_LOST	Nancy Admin changed link sharing access type from **Can view** to **None** for **hyenacapital.net**	Nancy Admin	Oct 29, 2019, 3:25:28 PM PDT	Link Sharing Access Type Change	1L2VfsYE__XkwUBgw9U80SLyjznfJrgyugI9SBYyiGmM	Google Docs	nancy.admin@hyenacapital.net	Anyone with the link within the domain	Public on the web
DO_NOT_GET_LOST	Nancy Admin changed link sharing visibility from **Private** to **Public on the web** for **all**	Nancy Admin	Oct 29, 2019, 3:25:28 PM PDT	Link Sharing visibility change	1L2VfsYE__XkwUBgw9U80SLyjznfJrgyugI9SBYyiGmM	Google Docs	nancy.admin@hyenacapital.net	Anyone with the link within the domain	Public on the web
DO_NOT_GET_LOST	Nancy Admin changed link sharing access type from **None** to **Can view** for **all**	Nancy Admin	Oct 29, 2019, 3:25:28 PM PDT	Link Sharing Access Type Change	1L2VfsYE__XkwUBgw9U80SLyjznfJrgyugI9SBYyiGmM	Google Docs	nancy.admin@hyenacapital.net	Anyone with the link within the domain	Public on the web

DETECTION: OAUTH / THIRD-PARTY APPLICATIONS

APP SCOPE USER

OAuth grant activity by user
Jan 9, 2020 - Jan 15, 2020

Select filter

User	Grants	Grant change	Scopes Granted	Scope change
nancy.admin@hyenacapital.net	6,661	7% ↑	25	19% ↑
ben.johnson@hyenacapital.net	107	-6% ↓	25	25% ↑
jondoe@hyenacapital.net	103	-8% ↓	20	0%
emilyevernote@hyenacapital.net	103	-9% ↓	20	0%
george.harrison@hyenacapital.net	103	-9% ↓	20	0%
john.user@hyenacapital.net				
eddie.nimda@hyenacapital.net				
mickjagger@hyenacapital.net				
mike.smith@hyenacapital.net				

Privileged OAuth apps

20 privileged OAuth ...

Apps that users gave permissions to. Discovered by Cloud App Security

High Medium Low

App	Permission l...
pwnauth	High
DROPBOX	High
Obsidian Security MS Graph [te...	High
My Python App	High

App name	Type	ID	Users	Requested services	Access
Box	Web Application	371608620635-lsbr3prap4hae8kl0netf6r...	3	Other	Limited
Google APIs Explorer	Web Application	292824132082.apps.googleusercontent....	2	Drive, Gmail, +4	Limited
Evernote	Web Application	447407681759.apps.googleusercontent....	2	Drive, Calendar, +2	Limited
GSuite SA Extended POC	Web Application	1092078371667-9a3vpnib3pajvqbqcj8nh...	1	G Suite Admin, Other	Limited
Slack	Web Application	19570130570-tfuuvh6hutjd09bq64is5sa...	1	Drive, Other	Limited
GAM Project Creation	Unknown Applicat...	297408095146-fug707qsjv4ikron0hugpe...	1	Cloud Platform	Limited

OBSIDIAN

DETECTION: SHARING SUMMARY

- What should you care about when it comes to sharing and third-party apps?
    - Sensitive scopes/grants (i.e. full GMail access)
    - Sharing externally with no expiration
    - Sharing externally with no password or restrictions
    - System-level apps that grant access to all accounts

WHAT DOES OBSIDIAN DO (INTERNALLY)?

- SaaS and IaaS heavy
- Worry about threats and excessive risk but try to always say YES to the business
- Visibility, detection, and response mindset
- Enable auditing on SaaS applications, pull telemetry into our own product (you could connect up to Splunk, Snowflake, Elasticsearch, datalake, etc)
- Enable cloudtrail, similar to SaaS ^^
- IP-Geo enrichment (IPs often mean very little but countries or states DO mean something)
- Send GuardDuty and Macie alerts to Slack
- Send all other alerts (Obsidian, Carbon Black, etc) to Slack
- Operators see alerts in Slack and pivot to domain specific tools
- We correlate either on Identity or IP
- Operators don’t need production access if the right data is flowing to the right place
- Turn review tasks into alert tasks (get to good state and alert on drift/violation)!!!

WHAT DOES OBSIDIAN DO (EXTERNALLY)?

Act

- **Review file sharing policy.** Nancy Admin publicly shared a document with a sensitive title "secret meeting notes - internal"..
- **Validate impossible travel activity.** Nancy Admin performed activity in distant locations (United States, Netherlands) in short time frame from IP-addresses (173.61.136.169, 185.107.95.230) not normally observed for organization or user.
- **Review file sharing policy.** Hannah Guidroz publicly shared a document with a sensitive title "Obsidian-Privileged-Activity-Monitoring-Solution-Brief.pdf"..
- **Review insider activity.** Nancy Admin downloaded 1236 files. That is unusually high compared to recent user activity.
- **Review user activity.** Nancy Admin logged in via a TOR anonymizing proxy with IP address 23.129.64.209.
- **Review file sharing policy.** Nancy Admin publicly shared a document with a sensitive title "secret plan to win"..
- **Reset account password.** Thomas Anderson failed multi-factor authentication from a new country.

Improve

- **Resolve tickets.** There are many (97) unresolved alert tickets.
- **Enable MFA for Administrators.** There are 3 Administrators on Google without MFA enabled.
- **Disable basic authentication.** There are 4 instances of Microsoft basic authentication use which bypasses MFA.
- **Review Salesforce hygiene.** 18 settings are marked as HIGH RISK.
- **Review Salesforce hygiene.** 4 settings are marked as MEDIUM RISK.
- **Review broadly shared files.** There are 7 files shared broadly on Microsoft.
- **Review broadly shared files.** There are 11 files shared broadly on Google.
- **Review external user file access.** 5 external users accessed shared files within your system over the past 7 days.
- **Review stale users.** There are 2 users with two or more inactive accounts and no active accounts over the past 30 days.
- **Review users with multiple privileged roles.** There are 9 users with multiple privileged roles.

Monitor

Service	Alerts	Accounts: Total accounts	Accounts: 1d change	Accounts: Active / inactive accounts	Accounts: Activity (7d)	Privileged Accounts: Total accounts	Privileged Accounts: 1d change	Privileged Accounts: Active / inactive accounts	Privileged Accounts: Activity (7d)
	0 Critical 5 High 58 Others	76	-3 -3.9%	82% Active 62 -2 -3.2% 18% Inactive 14 -1 -7.1%	Apr 23	10	No change	70% Active 7 No change 30% Inactive 3 No change	Apr 23
Salesforce	0 Critical 0 High 0 Others	39	-1 -2.6%	62% Active 24 -4 -16.7% 38% Inactive 15 3 20.0%	Apr 23	17	10 58.8%	76% Active 13 8 61.5% 41% Inactive 7 5 71.4%	Apr 23
	0 Critical 1 High 32 Others	38	-3 -7.9%	39% Active 15 1 6.7% 61% Inactive 23 -4 -17.4%	Apr 23	12	4 33.3%	50% Active 6 No change 50% Inactive 6 4 66.7%	Apr 23

PLAYBOOK

- Create awareness
- Enable SSO & Require MFA
- Enable Audit logs
- Can you implement conditional access?
- Reduce privileges
- Require passwords / expiration on shared resources and guest accounts
- Adjust human behavior
- Monitor behavior for threats and repeat

OBSIDIAN

Thank You

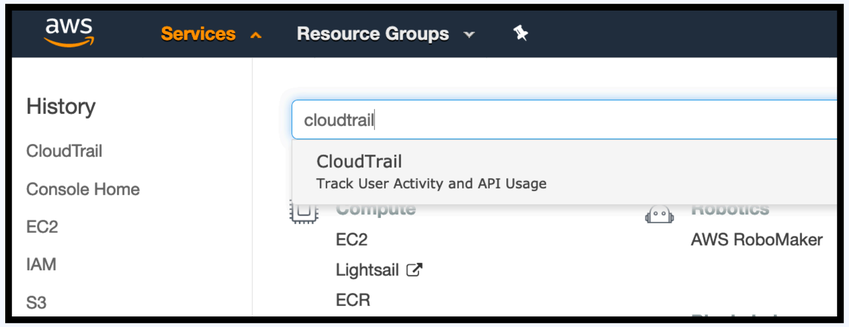
Ben Johnson I ben@obsidiansecurity.com I@chicagoben

AWS // IAAS

- AWS has added a lot of built-in capabilities
  - Security Hub - centralized place
  - GuardDuty - continuous monitoring
  - Inspector - assessment service
  - Macie - classify data
  - Access Analyzer - understand access

- AWS is also a BEAST
  - Lots of data
  - You need to invest time into it
  - Interpreting results from the tools above can still be a lot of work

AWS // CLOUDTRAIL




```
{"additionalEventData":{"AuthenticationMethod":"AuthHeader","CipherSuite":"ECDHE-RSA-AES128-SHA","SignatureVersion":"SigV4","vpcEndpointId":"vpce-a0d039c9"},"awsRegion":"us-west
-2","eventID":"6d010820-ebb1-4a74-971b-24045023543e","eventName":"GetBucketLogging","eventSource":"s3.amazonaws.com","eventTime":"2019-08-20T20:12:05Z","eventType":"AwsApiCall",
"eventVersion":"1.05","recipientAccountId":"724943626193","requestID":"C883D84ACFB7BD1A","requestParameters":{"bucketName":"this-is-hyena","host":["s3-us-west-2.amazonaws.com"],
"logging":[""]},"responseElements":null,"sourceIPAddress":"104.183.139.113","userAgent":"signin.amazonaws.com","userIdentity":{"accessKeyId":"ASIA2RSQB37IXLQS33MG","accountId":"
724943626193","arn":"arn:aws:iam::724943626193:root","invokedBy":"signin.amazonaws.com","principalId":"724943626193","sessionContext":{"attributes":{"creationDate":"2019-08-20T2
0:11:41Z","mfaAuthenticated":"false"}},"type":"Root"},"vpcEndpointId":"vpce-a0d039c9"}
{"additionalEventData":{"AuthenticationMethod":"AuthHeader","CipherSuite":"ECDHE-RSA-AES128-SHA","SignatureVersion":"SigV4","vpcEndpointId":"vpce-a0d039c9"},"awsRegion":"us-west
-2","errorCode":"NoSuchBucketPolicy","errorMessage":"The bucket policy does not exist","eventID":"3a291610-27a2-4790-9912-72dbfc5d7c35","eventName":"GetBucketPolicy","eventSourc
e":"s3.amazonaws.com","eventTime":"2019-08-20T20:12:06Z","eventType":"AwsApiCall","eventVersion":"1.05","recipientAccountId":"724943626193","requestID":"13EC120284C6CD51","reque
stParameters":{"bucketName":"this-is-hyena","host":["s3-us-west-2.amazonaws.com"],"policy":[""]},"responseElements":null,"sourceIPAddress":"104.183.139.113","userAgent":"signin.
amazonaws.com","userIdentity":{"accessKeyId":"ASIA2RSQB37IXLQS33MG","accountId":"724943626193","arn":"arn:aws:iam::724943626193:root","invokedBy":"signin.amazonaws.com","princip
alId":"724943626193","sessionContext":{"attributes":{"creationDate":"2019-08-20T20:11:41Z","mfaAuthenticated":"false"}},"type":"Root"},"vpcEndpointId":"vpce-a0d039c9"}
{"additionalEventData":{"AuthenticationMethod":"AuthHeader","CipherSuite":"ECDHE-RSA-AES128-SHA","SignatureVersion":"SigV4","vpcEndpointId":"vpce-a0d039c9"},"awsRegion":"us-west
-2","errorCode":"NoSuchCORSConfiguration","errorMessage":"The CORS configuration does not exist","eventID":"a7f2e67b-4f60-4ecc-a893-7152ff650420","eventName":"GetBucketCors","ev
entSource":"s3.amazonaws.com","eventTime":"2019-08-20T20:12:06Z","eventType":"AwsApiCall","eventVersion":"1.05","recipientAccountId":"724943626193","requestID":"6ED32BD0A0412206
","requestParameters":{"bucketName":"this-is-hyena","cors":[""],"host":["s3-us-west-2.amazonaws.com"]},"responseElements":null,"sourceIPAddress":"104.183.139.113","userAgent":"s
ignin.amazonaws.com","userIdentity":{"accessKeyId":"ASIA2RSQB37IXLQS33MG","accountId":"724943626193","arn":"arn:aws:iam::724943626193:root","invokedBy":"signin.amazonaws.com","p
rincipalId":"724943626193","sessionContext":{"attributes":{"creationDate":"2019-08-20T20:11:41Z","mfaAuthenticated":"false"}},"type":"Root"},"vpcEndpointId":"vpce-a0d039c9"}
{"additionalEventData":{"AuthenticationMethod":"AuthHeader","CipherSuite":"ECDHE-RSA-AES128-SHA","SignatureVersion":"SigV4","vpcEndpointId":"vpce-a0d039c9"},"awsRegion":"us-west
-2","errorCode":"ServerSideEncryptionConfigurationNotFoundError","errorMessage":"The server side encryption configuration was not found","eventID":"053664c9-6da7-4125-a591-5f95f
f967c7","eventName":"GetBucketEncryption","eventSource":"s3.amazonaws.com","eventTime":"2019-08-20T20:12:05Z","eventType":"AwsApiCall","eventVersion":"1.05","recipientAccountId
":"724943626193","requestID":"CCAFE541C9871D2F","requestParameters":{"bucketName":"this-is-hyena","encryption":[""],"host":["s3-us-west-2.amazonaws.com"]},"responseElements":nul
l,"sourceIPAddress":"104.183.139.113","userAgent":"signin.amazonaws.com","userIdentity":{"accessKeyId":"ASIA2RSQB37IXLQS33MG","accountId":"724943626193","arn":"arn:aws:iam::7249
43626193:root","invokedBy":"signin.amazonaws.com","principalId":"724943626193","sessionContext":{"attributes":{"creationDate":"2019-08-20T20:11:41Z","mfaAuthenticated":"false"}}
,"type":"Root"},"vpcEndpointId":"vpce-a0d039c9"}
{"additionalEventData":{"AuthenticationMethod":"AuthHeader","CipherSuite":"ECDHE-RSA-AES128-SHA","SignatureVersion":"SigV4","vpcEndpointId":"vpce-a0d039c9"},"awsRegion":"us-west
-2","errorCode":"ServerSideEncryptionConfigurationNotFoundError","errorMessage":"The server side encryption configuration was not found","eventID":"4a2dea83-fcc0-4a5c-b78e-f30f3
aaf173c","eventName":"GetBucketEncryption","eventSource":"s3.amazonaws.com","eventTime":"2019-08-20T20:12:04Z","eventType":"AwsApiCall","eventVersion":"1.05","recipientAccountId
":"724943626193","requestID":"E50634684783A3BF","requestParameters":{"bucketName":"this-is-hyena","encryption":[""],"host":["s3-us-west-2.amazonaws.com"]},"responseElements":nul
l,"sourceIPAddress":"104.183.139.113","userAgent":"signin.amazonaws.com","userIdentity":{"accessKeyId":"ASIA2RSQB37IXLQS33MG","accountId":"724943626193","arn":"arn:aws:iam::7249
43626193:root","invokedBy":"signin.amazonaws.com","principalId":"724943626193","sessionContext":{"attributes":{"creationDate":"2019-08-20T20:11:41Z","mfaAuthenticated":"false"}}
,"type":"Root"},"vpcEndpointId":"vpce-a0d039c9"}
{"additionalEventData":{"AuthenticationMethod":"AuthHeader","CipherSuite":"ECDHE-RSA-AES128-SHA","SignatureVersion":"SigV4","vpcEndpointId":"vpce-a0d039c9"},"awsRegion":"us-west
-2","eventID":"f562bbf7-a008-46b7-99e6-aa903bcf1f9b","eventName":"GetBucketPolicyStatus","eventSource":"s3.amazonaws.com","eventTime":"2019-08-20T20:11:45Z","eventType":"AwsApiC
all","eventVersion":"1.05","recipientAccountId":"724943626193","requestID":"FCBD2C5A3668D185","requestParameters":{"bucketName":"obs-cloudtrail-logs-724943626193-bk9842o8s7o0sae
257jg","host":["obs-cloudtrail-logs-724943626193-bk9842o8s7o0sae257jg.s3.us-west-2.amazonaws.com"],"policyStatus":[""]},"responseElements":null,"sourceIPAddress":"104.183.139.11
3","userAgent":"signin.amazonaws.com","userIdentity":{"accessKeyId":"ASIA2RSQB37IXLQS33MG","accountId":"724943626193","arn":"arn:aws:iam::724943626193:root","invokedBy":"signin.
amazonaws.com","principalId":"724943626193","sessionContext":{"attributes":{"creationDate":"2019-08-20T20:11:41Z","mfaAuthenticated":"false"}},"type":"Root"},"vpcEndpointId":"vp
ce-a0d039c9"}
{"additionalEventData":{"AuthenticationMethod":"AuthHeader","CipherSuite":"ECDHE-RSA-AES128-SHA","SignatureVersion":"SigV4","vpcEndpointId":"vpce-a0d039c9"},"awsRegion":"us-west
-2","eventID":"12e22c1d-011f-48e4-b379-8ea2e56a1d17","eventName":"GetAccountPublicAccessBlock","eventSource":"s3.amazonaws.com","eventTime":"2019-08-20T20:11:45Z","eventType":"A
wsApiCall","eventVersion":"1.05","recipientAccountId":"724943626193","requestID":"2E0132CDFA92B38F","requestParameters":{"host":["724943626193.s3-control.us-west-2.amazonaws.com
"]},"responseElements":null,"sourceIPAddress":"104.183.139.113","userAgent":"signin.amazonaws.com","userIdentity":{"accessKeyId":"ASIA2RSQB37IXLQS33MG","accountId":"724943626193
","arn":"arn:aws:iam::724943626193:root","invokedBy":"signin.amazonaws.com","principalId":"724943626193","sessionContext":{"attributes":{"creationDate":"2019-08-20T20:11:41Z","m
faAuthenticated":"false"}},"type":"Root"},"vpcEndpointId":"vpce-a0d039c9"}
{"additionalEventData":{"AuthenticationMethod":"AuthHeader","CipherSuite":"ECDHE-RSA-AES128-SHA","SignatureVersion":"SigV4","vpcEndpointId":"vpce-a0d039c9"},"awsRegion":"us-west
-2","eventID":"4e0ffa7f-b472-42cd-a934-6b4ca83b7069","eventName":"GetBucketPolicyStatus","eventSource":"s3.amazonaws.com","eventTime":"2019-08-20T20:11:45Z","eventType":"AwsApiC
all","eventVersion":"1.05","recipientAccountId":"724943626193","requestID":"AAECA52009EB7A74","requestParameters":{"bucketName":"test-bucket-0306","host":["test-bucket-0306.s3.u
s-west-2.amazonaws.com"],"policyStatus":[""]},"responseElements":null,"sourceIPAddress":"104.183.139.113","userAgent":"signin.amazonaws.com","userIdentity":{"accessKeyId":"ASIA2
RSQB37IXLQS33MG","accountId":"724943626193","arn":"arn:aws:iam::724943626193:root","invokedBy":"signin.amazonaws.com","principalId":"724943626193","sessionContext":{"attributes"
:{"creationDate":"2019-08-20T20:11:41Z","mfaAuthenticated":"false"}},"type":"Root"},"vpcEndpointId":"vpce-a0d039c9"}
{"additionalEventData":{"AuthenticationMethod":"AuthHeader","CipherSuite":"ECDHE-RSA-AES128-SHA","SignatureVersion":"SigV4","vpcEndpointId":"vpce-a0d039c9"},"awsRegion":"us-west
-2","eventID":"44a5bdc2-df60-4b62-96be-ae8dbd6bda60","eventName":"GetAccountPublicAccessBlock","eventSource":"s3.amazonaws.com","eventTime":"2019-08-20T20:11:45Z","eventType":"A
wsApiCall","eventVersion":"1.05","recipientAccountId":"724943626193","requestID":"02857DAC4D8455D4","requestParameters":{"host":["724943626193.s3-control.us-west-2.amazonaws.com
"]},"responseElements":null,"sourceIPAddress":"104.183.139.113","userAgent":"signin.amazonaws.com","userIdentity":{"accessKeyId":"ASIA2RSQB37IXLQS33MG","accountId":"724943626193
","arn":"arn:aws:iam::724943626193:root","invokedBy":"signin.amazonaws.com","principalId":"724943626193","sessionContext":{"attributes":{"creationDate":"2019-08-20T20:11:41Z","m
faAuthenticated":"false"}},"type":"Root"},"vpcEndpointId":"vpce-a0d039c9"}
{"additionalEventData":{"AuthenticationMethod":"AuthHeader","CipherSuite":"ECDHE-RSA-AES128-SHA","SignatureVersion":"SigV4","vpcEndpointId":"vpce-a0d039c9"},"awsRegion":"us-west
-2","errorCode":"NoSuchPublicAccessBlockConfiguration","errorMessage":"The public access block configuration was not found","eventID":"a252d08e-832a-4231-9b1e-a31c64ab438c","eve
ntName":"GetBucketPublicAccessBlock","eventSource":"s3.amazonaws.com","eventTime":"2019-08-20T20:11:45Z","eventType":"AwsApiCall","eventVersion":"1.05","recipientAccountId":"724
943626193","requestID":"6D214C29810F7B7F","requestParameters":{"bucketName":"obs-cloudtrail-logs-724943626193-bk57h8o8s7o0sae257ag","host":["obs-cloudtrail-logs-724943626193-bk5
7h8o8s7o0sae257ag.s3.us-west-2.amazonaws.com"],"publicAccessBlock":[""]},"responseElements":null,"sourceIPAddress":"104.183.139.113","userAgent":"signin.amazonaws.com","userIden
tity":{"accessKeyId":"ASIA2RSQB37IXLQS33MG","accountId":"724943626193","arn":"arn:aws:iam::724943626193:root","invokedBy":"signin.amazonaws.com","principalId":"724943626193","se
ssionContext":{"attributes":{"creationDate":"2019-08-20T20:11:41Z","mfaAuthenticated":"false"}},"type":"Root"},"vpcEndpointId":"vpce-a0d039c9"}
```

AWS // CLOUDTRAIL

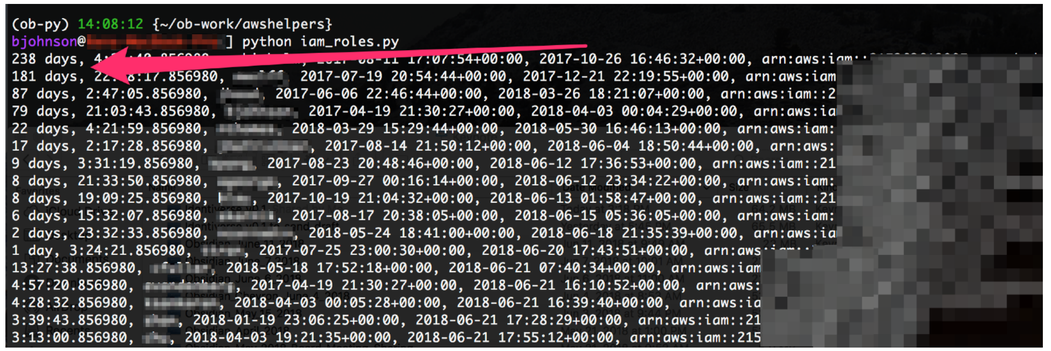
- Cloudtrail logs give you ability to see lots of activity
- They’re often easy to enable
- The question is what to do with them?
- And be careful… first one is free but… charges after that

- Some interesting events to potentially look at:
  - ConsoleLogin
  - CreateBucket
  - RunInstances
  - ModifySnapshotAttribute

AWS // ACCESS?

DORMANT ACCOUNTS

```
238 days
181 days
87 days
79 days
22 days
17 days
9 days
8 days
```



Checking for MFA?
(ConsoleLogin events)