Catching Data Exfiltration Early!

Stanislav Miskovic, PhD
Ignacio Bermudez Corrales, PhD

Security Markets Group | Splunk

splunk> .conf19

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

The New York Times

Equifax Says Cyberattack May Have Affected 143 Million in the U.S.

June 21, 2019

Insider exposes PII of 2.9 million Desjardins customers

Forbes Billionaires Innovation Leadership Money Consumer Industry Lifestyle

2,273 views | Aug 20, 2019, 06:31am

Data Breaches Expose 4.1 Billion Records In First Six Months Of 2019

TechRepublic. SEARCH IT Policy Downloads 5G Developer Security Cloud

60% of companies experienced insider attacks in the last year

Target Data Breach Spilled Info On As Many As 70 Million Customers

Forbes

April 20, 2018

Ex-Sun Trust employee helps compromise 1.5 million bank clients

SCmagazine

Attack Anatomy

External

Insider

Getting Foothold

Phishing
Malware
Account takeover
CVEs
Persistence …

Thinking & Planning

Searching

Reconnaissance
- Files
- Documents
- Databases

Lifting Data

$

Data Collection

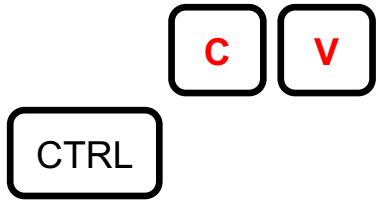
"Going stealth"
- Data splitting
- Time spreading
- File renaming
- Content obfuscation

Transfer

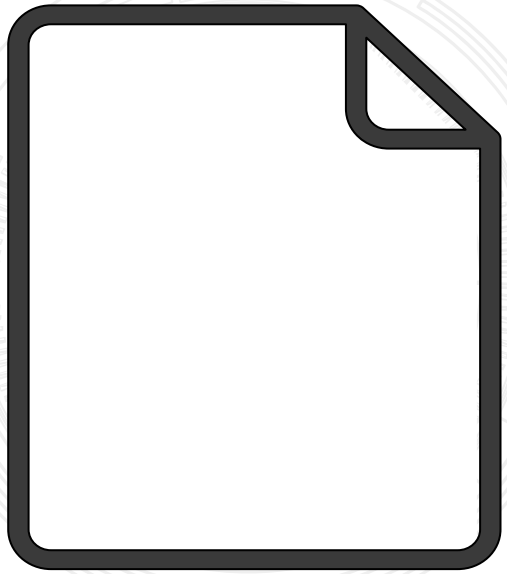
We act here!

Public **breaches** are over 2.5 times more likely to be **undiscovered for years**. Espionage-related breaches typically do take longer to discover … *DBIR 2019*

It’s All About Files



Copy-Pasting



```
psql -c "SELECT * FROM revenue"
     >> dayOnBeach.jpg
```

Querying

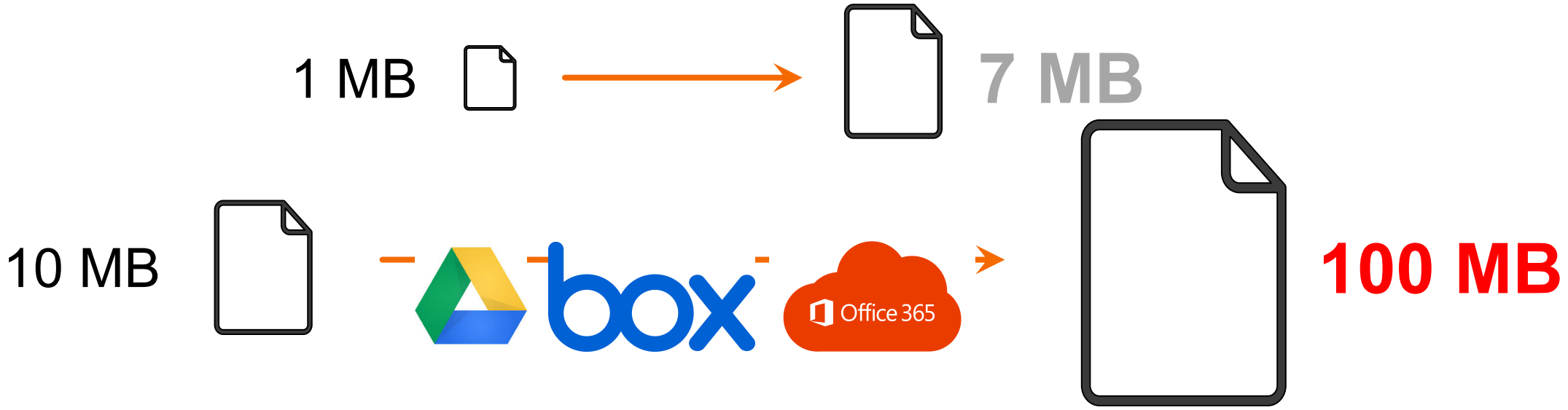
```
zip -rv
pwnedThis.zip addFile1.pdf
```

Archiving

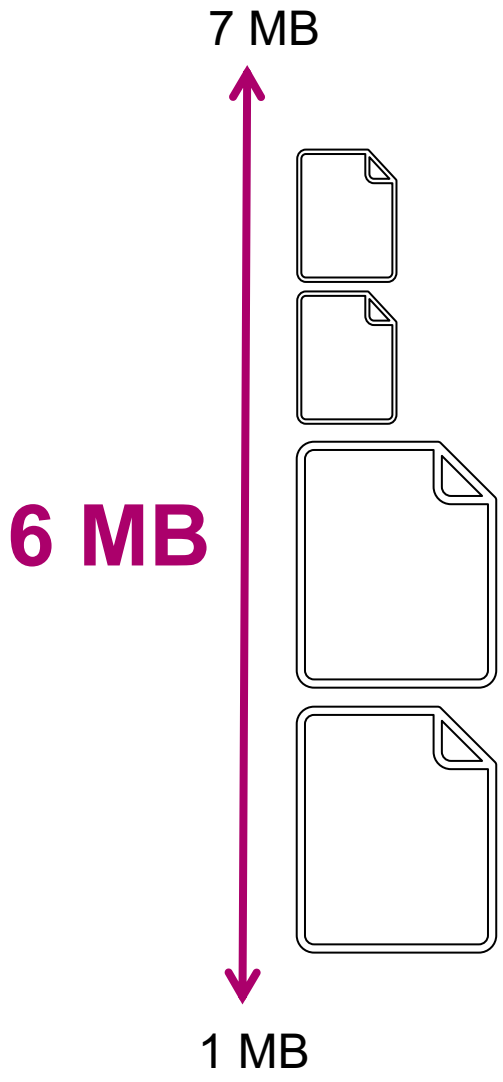
```
cat sourceCode/* |
 tee -a chores.rtf
```

Dumping

Goal: Which File Changes Are Exfiltration?



Things You Can Fit in a “Small” File



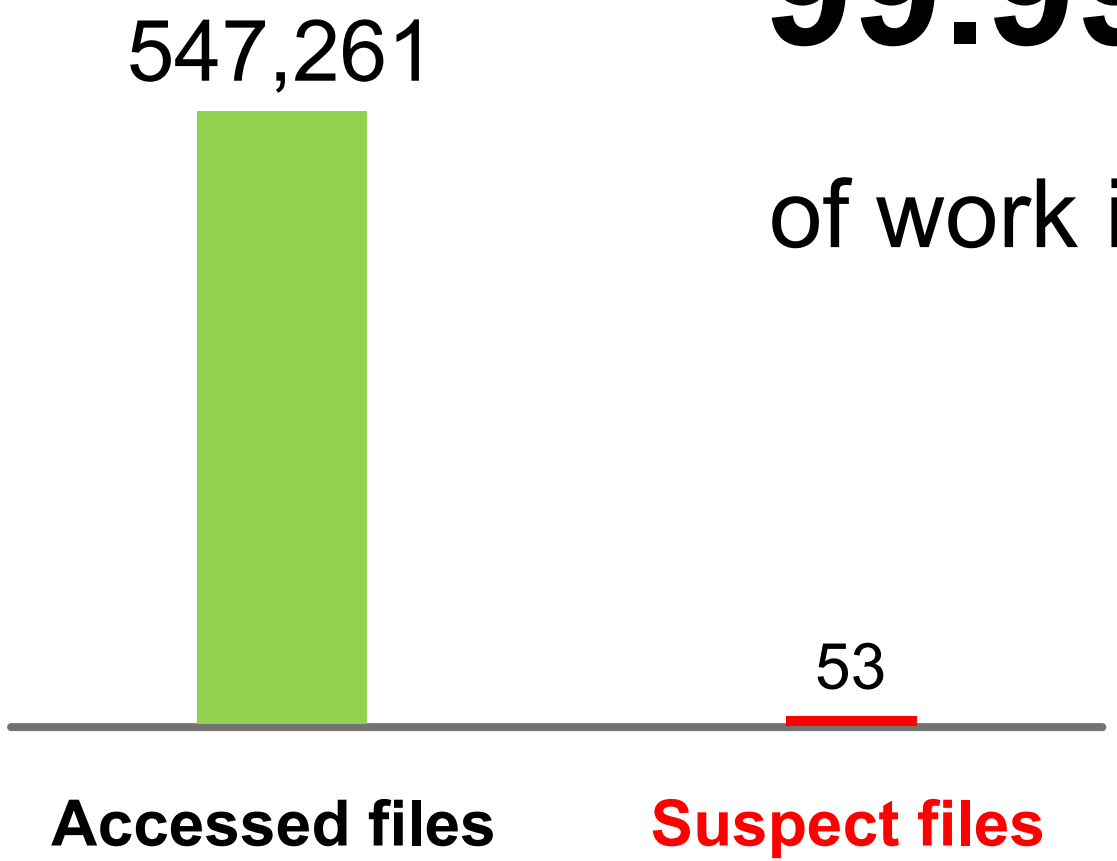
<*LargeTelecom*> - Exec Briefing Doc.docx (0.9MByte)

<*HealthProvider*> Security Posture Assessment-final.docx (0.9MByte)

<*GovSecurityAgency*> Meeting Notes & Solution.docx (1.9MByte)

<*PostalService*>Strategic Account Plan.docx (1.9MByte)

End Result



99.991%

of work is on us

Rest of the Talk

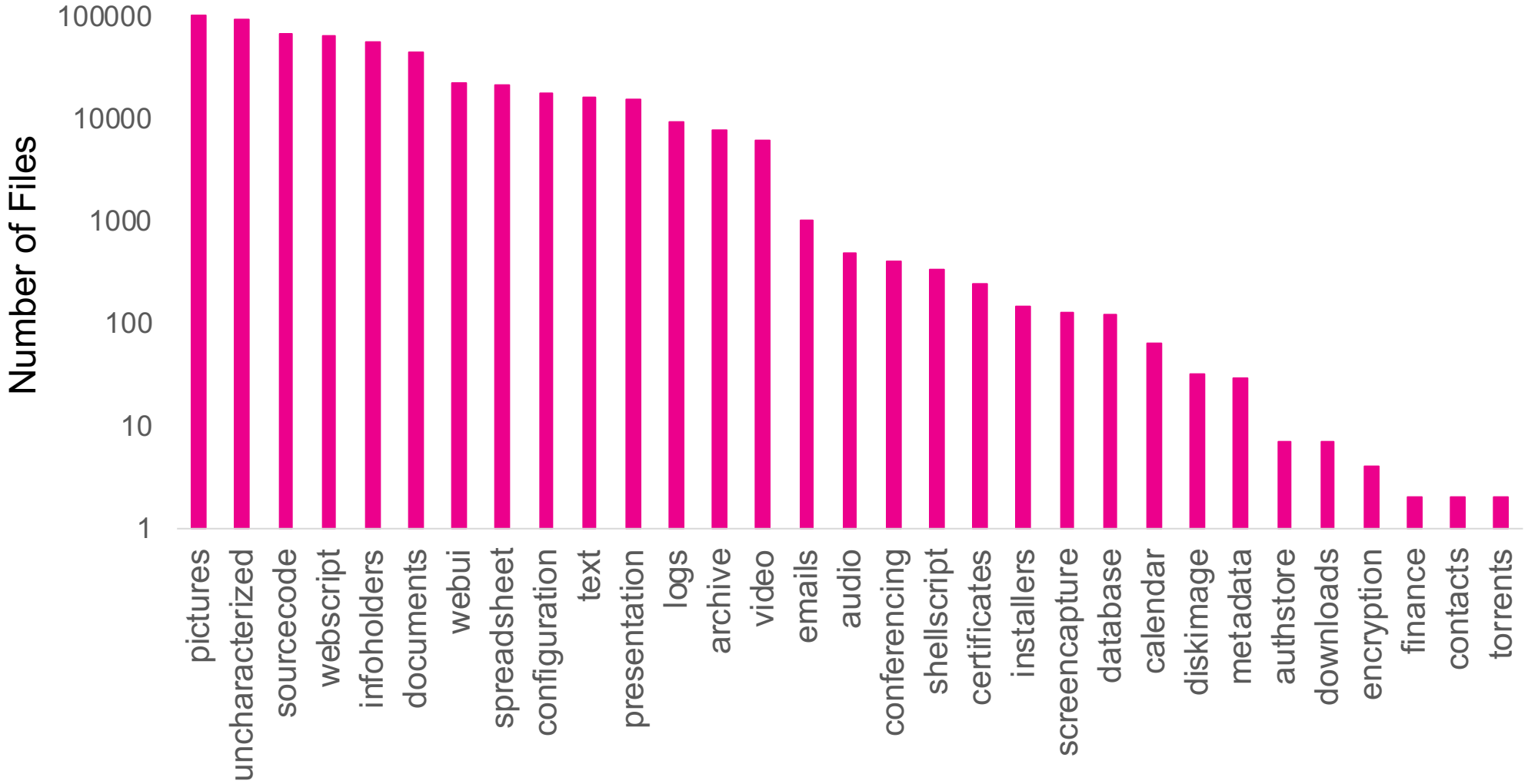
1. Cloud stores, what's in there?
2. Our early exfiltration detection
3. Results

File Cloud Store

2	3560	550k	0
Months	Users	Accessed Files	Personal Details

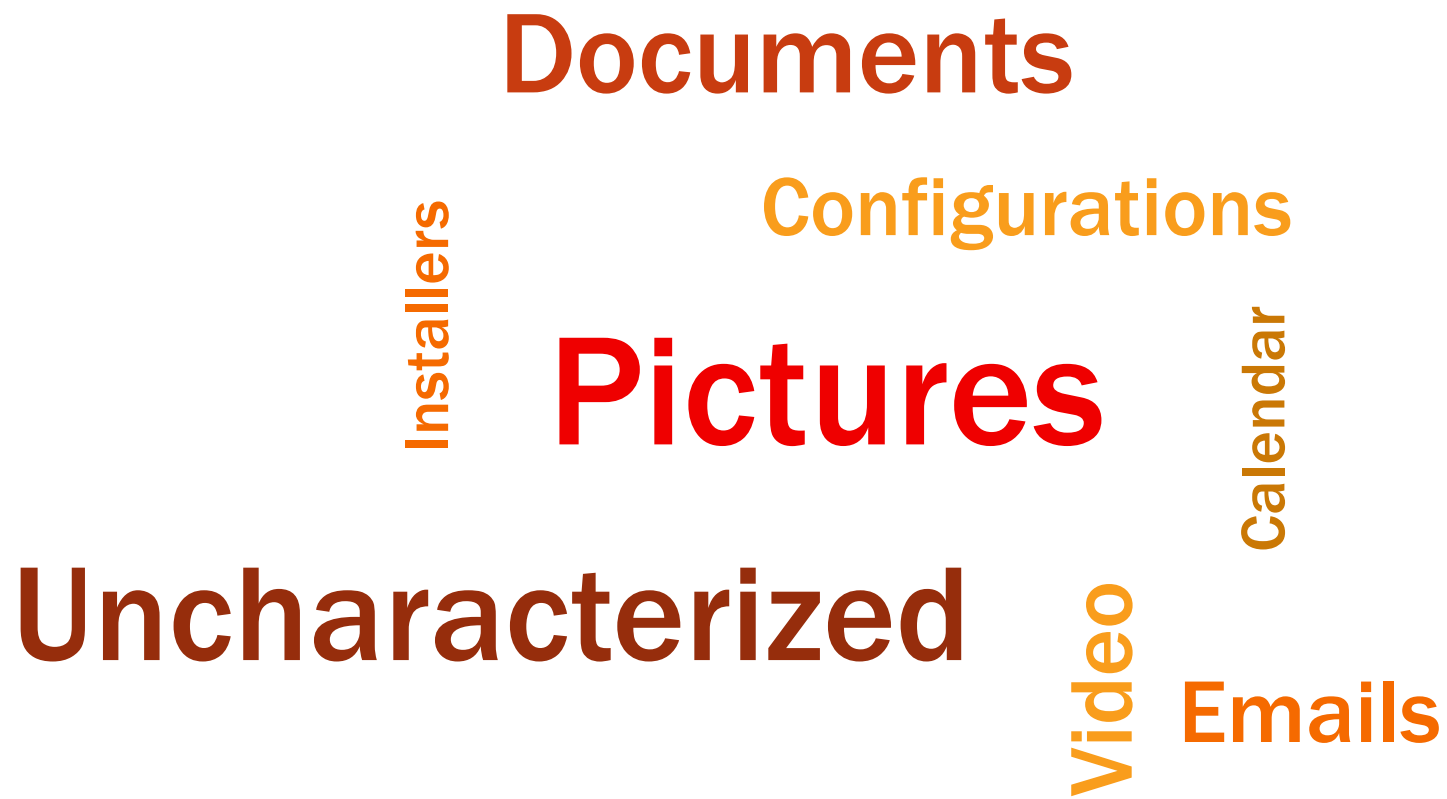
Privacy Respecting

Files



Files

Personal Use



30% personal photos

Content backup
- iPhone
- Android
- Workstations

Files

Source Code & Software

Key product

Company's web presence

Research

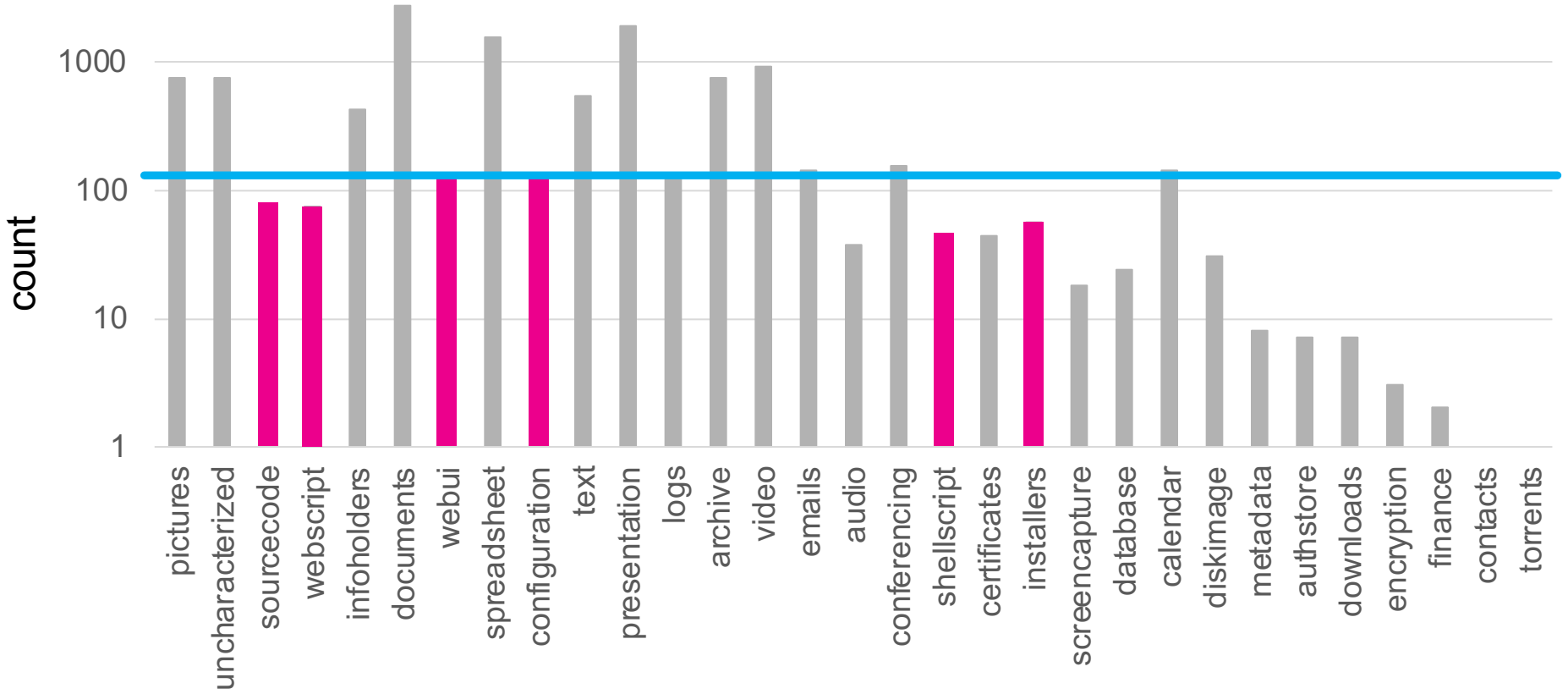
Operations (Jira, …)

Finance & Legal

IT ops

Users

Source Code & Software



TOTAL: 243 users - mostly field facing

Cloud file stores are new flash drives!

Ambiguity: Working with customers or exfiltration?

Motivates malicious actors to keep
exfiltration files in the cloud

Depth Gauging

Other Content

"Briefing"
293 Files

"Strategic"
71 Files

"Revenue"
657 Files

" FY1* "
6871 Files

<"Big Four">
241 Files

"Financ*"
560 Files

"Renewals"
352 Files

"Compensation"
82 Files

"Payroll"
552 Files

"Pension"
78 Files

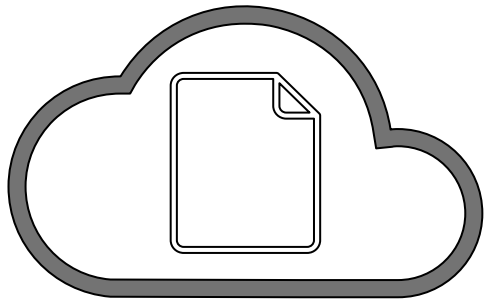
Probing with Keywords

What's at Stake?

Personally Identifiable Information

Intellectual Property

Infrastructure



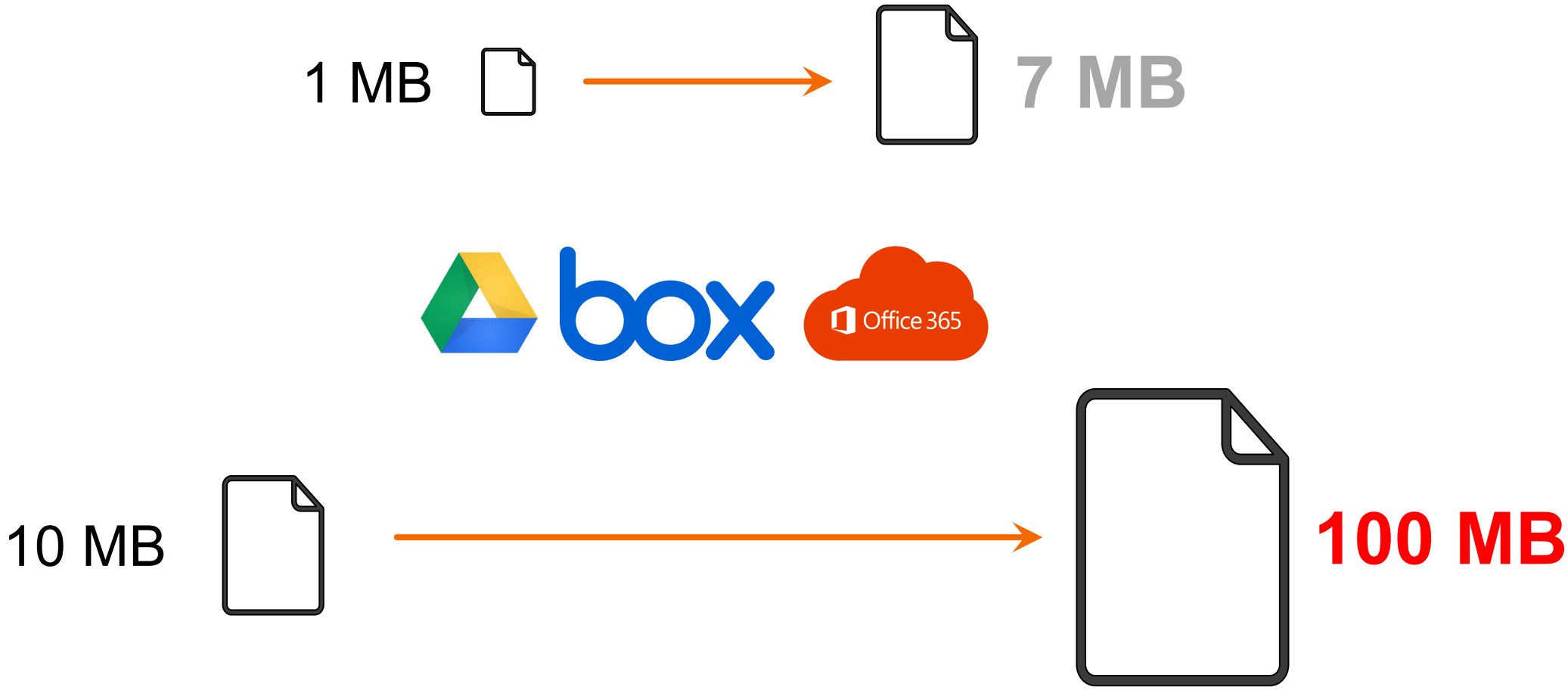
Legal Information

Credentials

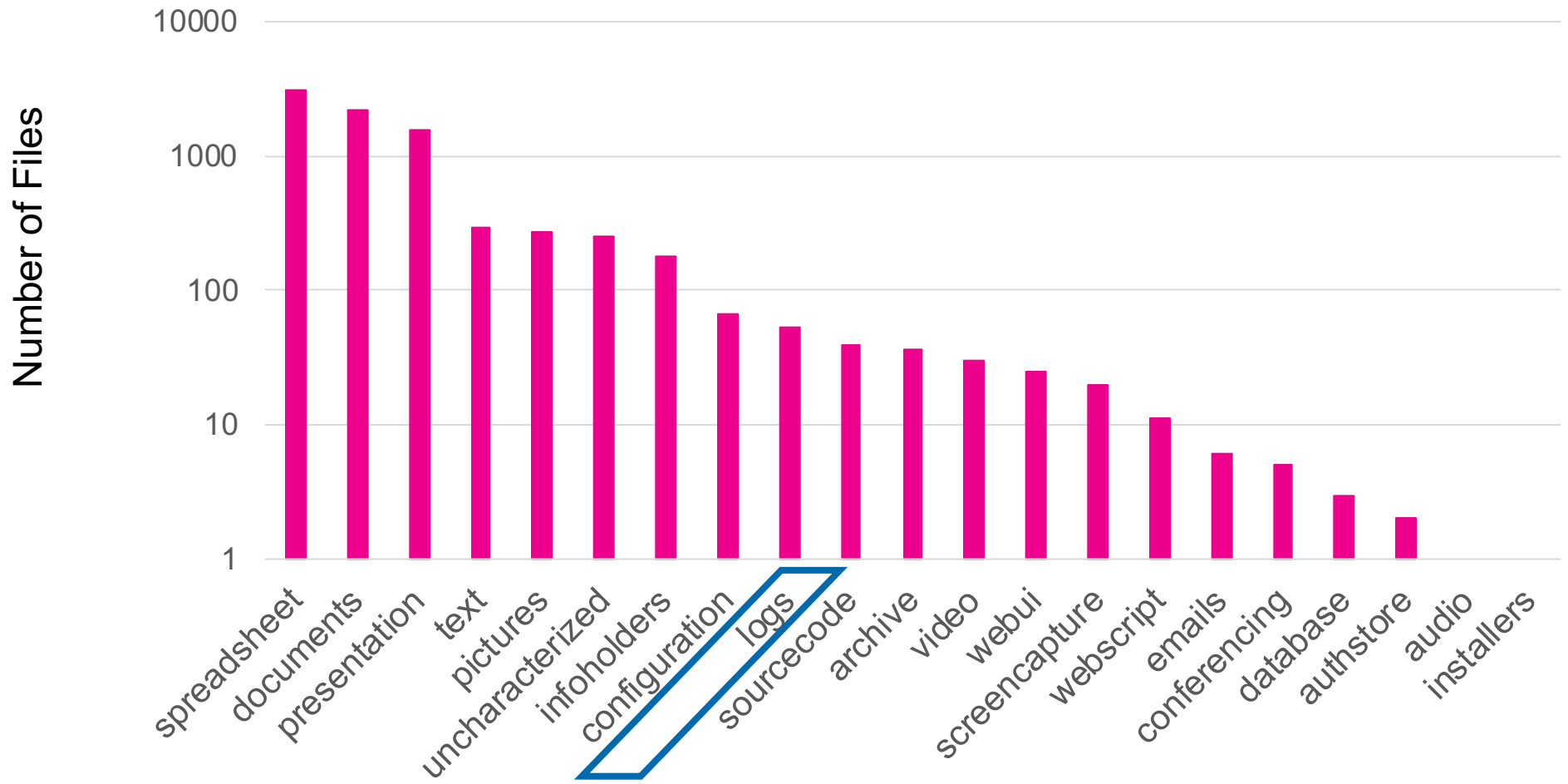
Financial Information

Sensitive Information

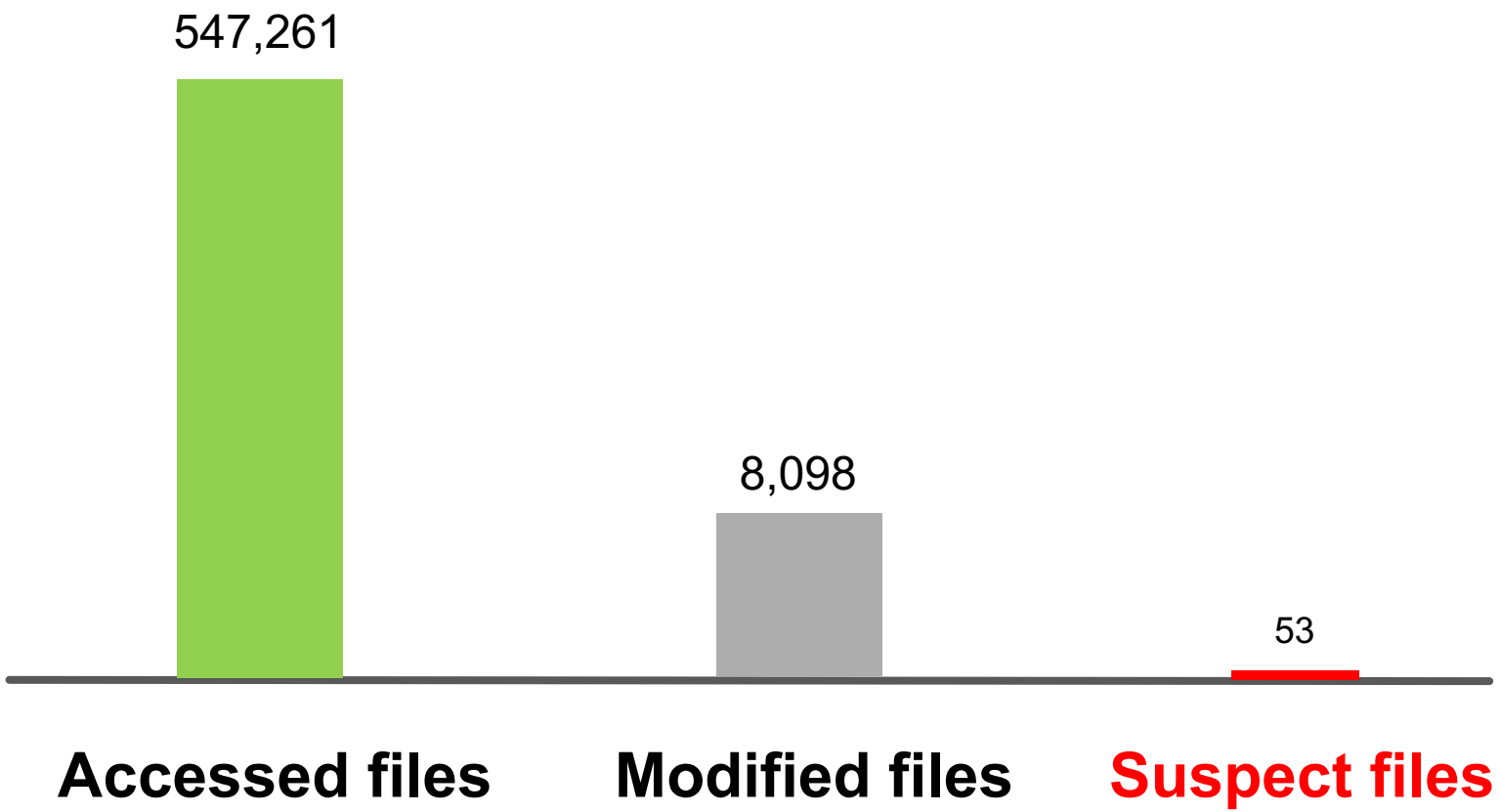
Reminder: We're After Suspicious File Changes…



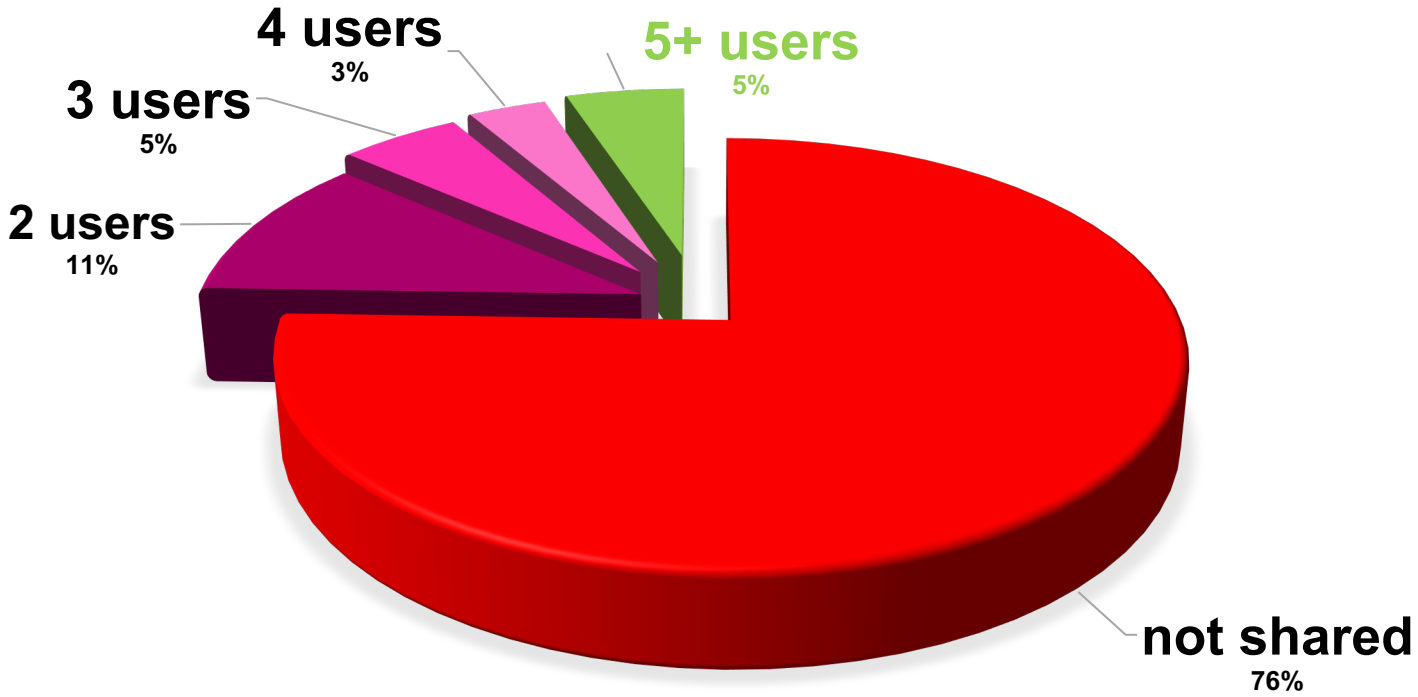
Modified Files



Update: End Result



Other Features: Sharing?



95% of changing files may be exfiltration

HARD WORK

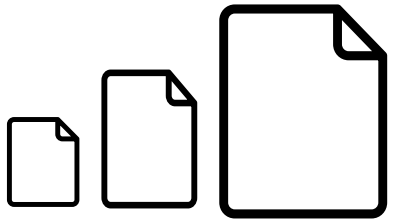
Cloud file stores are dark data

... And file changes are “outliers”

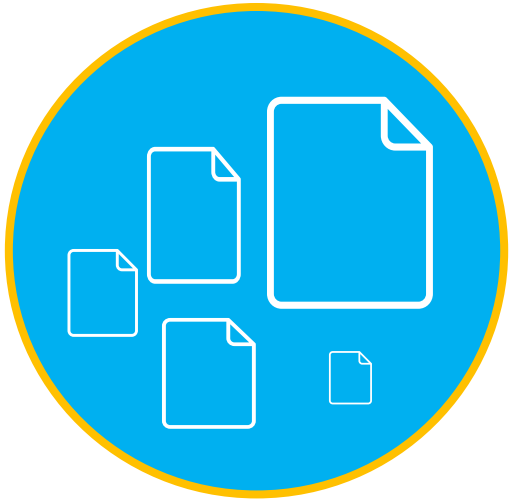
Rest of the Talk

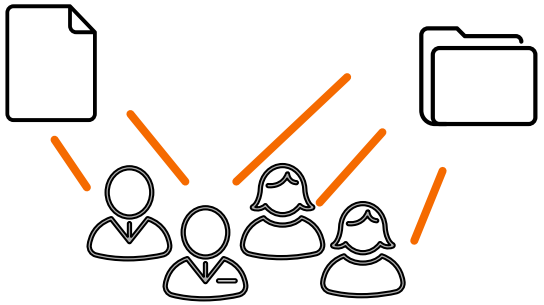
1. Cloud stores, what's in there?
2. Our early exfiltration detection
3. Results

Feature Engineering

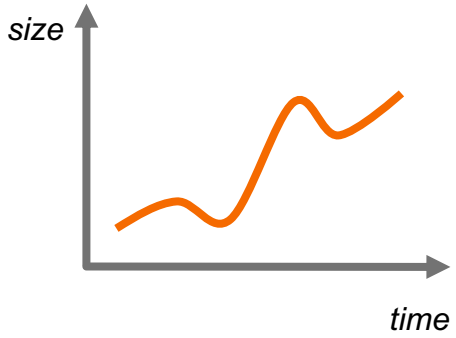


Size Classes

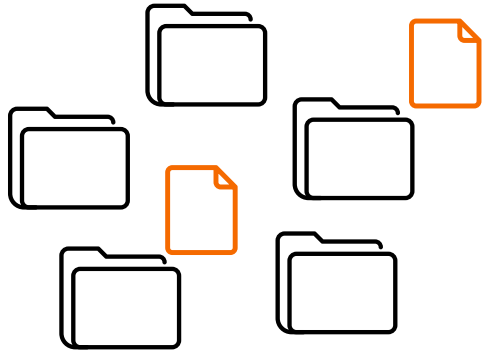




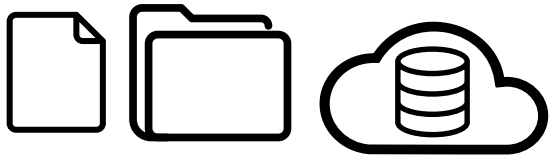
User Associations



Temporal Size Changes

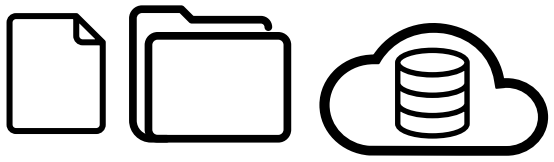


Spatial Properties



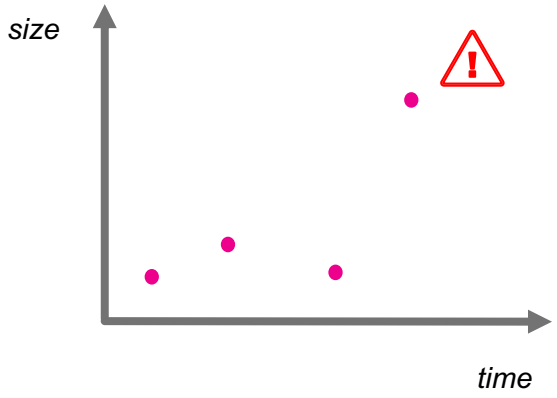
Scope

Scope Features

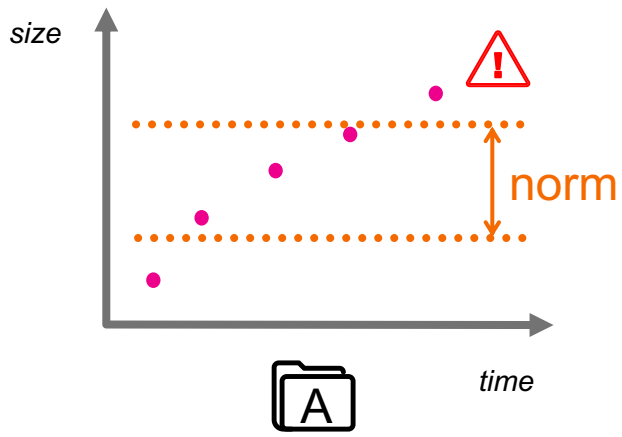


Scope

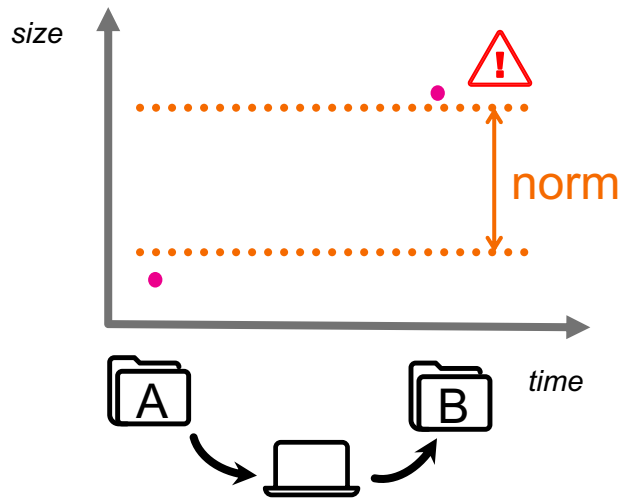
File Scope



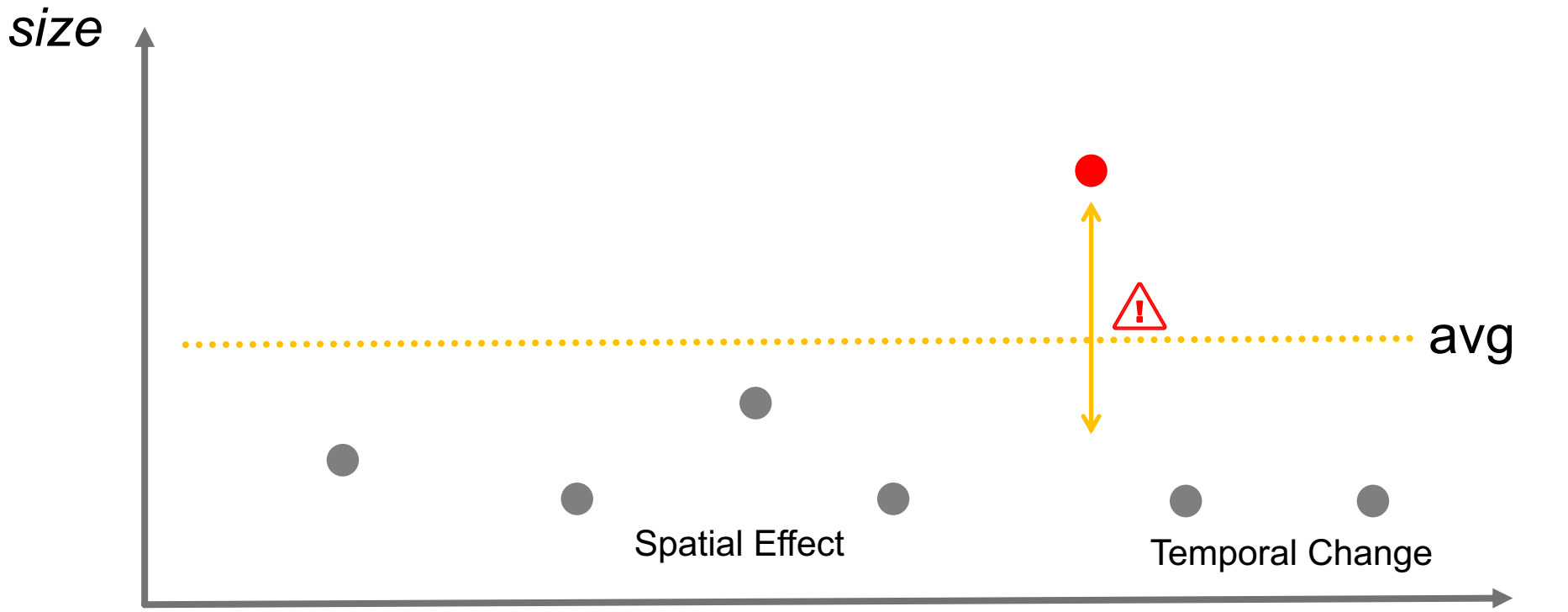
Folder Scope

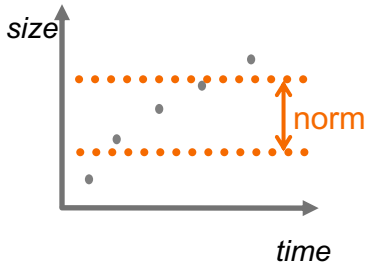


Cloud Store Scope



Temporal Norm Selection





Running Average & Max

… Other Things We Tried

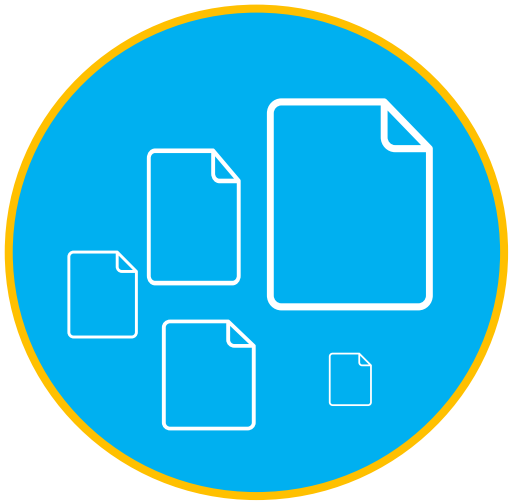
Do's & Don'ts

~~DSC00365.JPG~~
~~Readme.txt~~

File Names

~~If(After Midnight) then {Attack}~~

Guesswork



~~.json .docx~~

File Types

.extA -> .extB

Type Changes

.txt -> .sh
.doc -> .docx
.tmp$ -> .png
.doc -> .pdf
.pdf -> .doc ⚠

.spl -> .tgz
.doc -> .flac ⚠

Locations

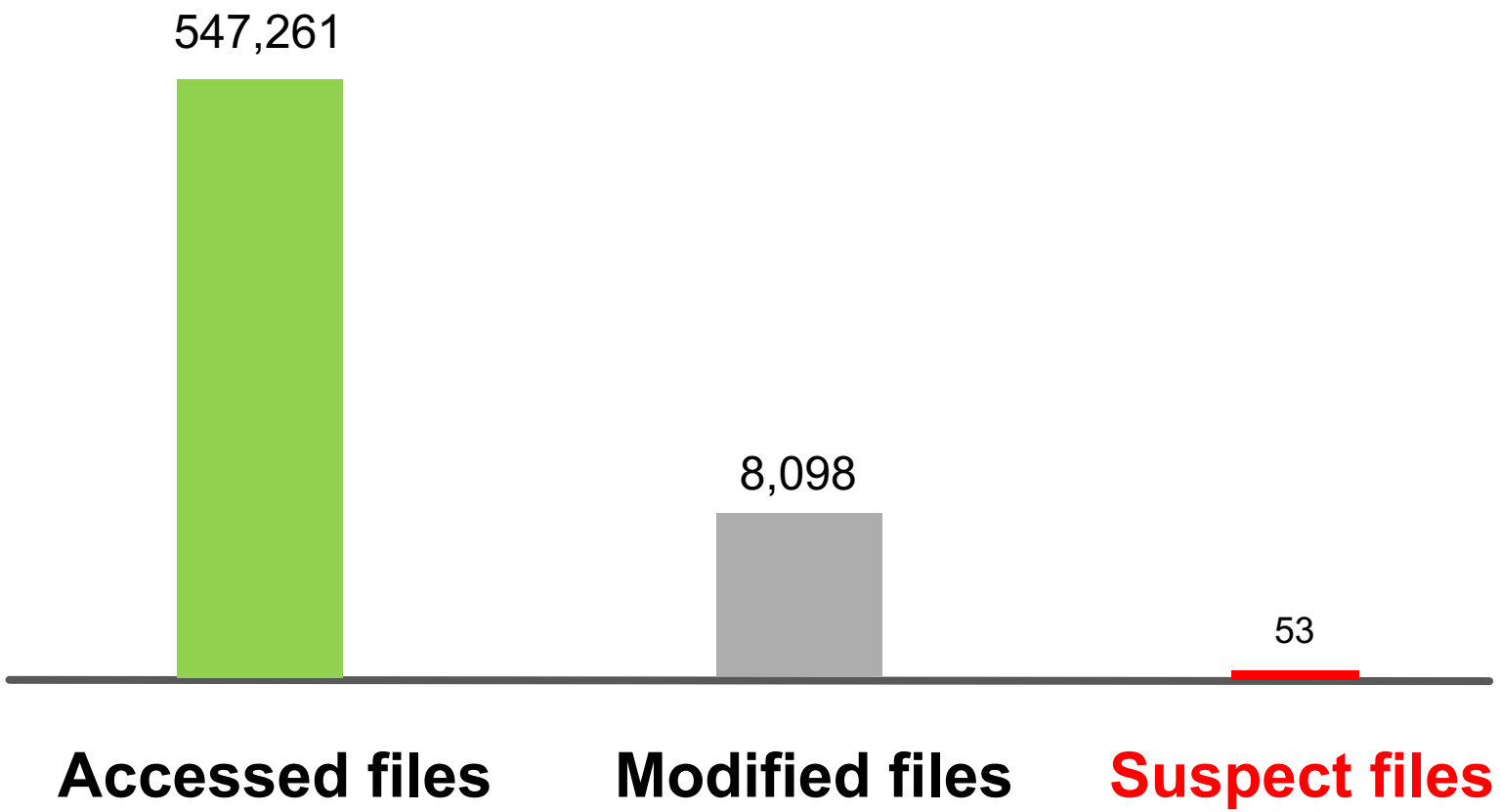
External access/handling

76% reported files
81% modified files

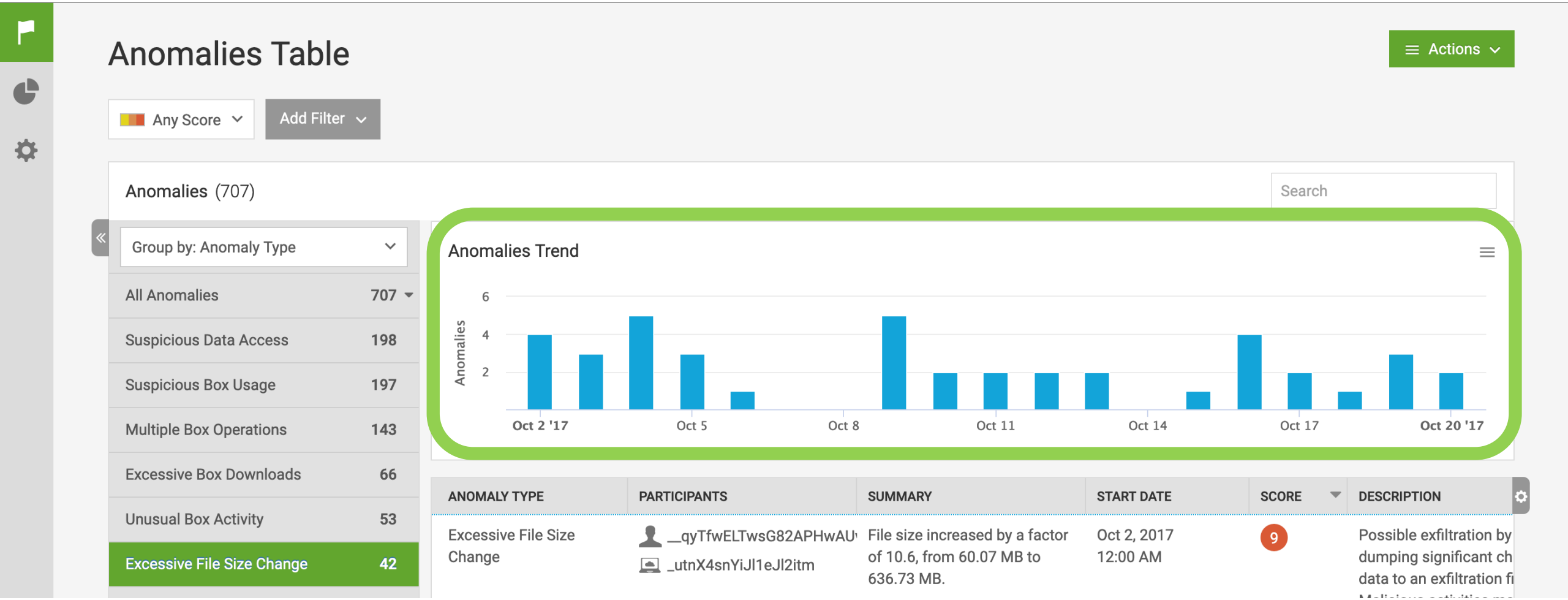
Rest of the Talk

1. Cloud stores, what's in there?
2. Our early exfiltration detection
3. Results

End Result



Alert Fatigue



splunk> .conf19

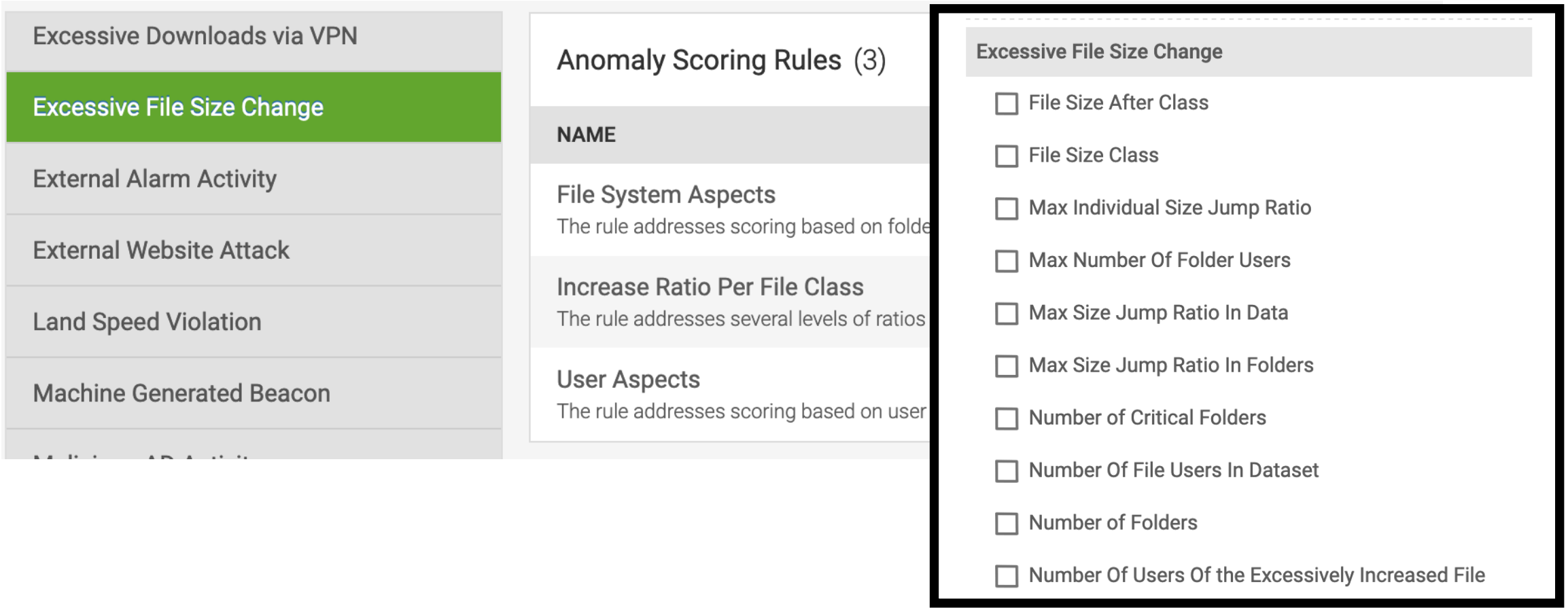
Scoring

Group by: Anomaly Type

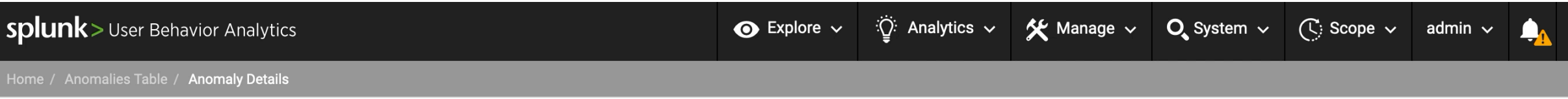
Suspicious Data Access	198
Suspicious Box Usage	197
Multiple Box Operations	143
Excessive Box Downloads	66
Unusual Box Activity	53
Excessive File Size Change	42
Unusual Activity Time	5
Multiple Logins	3
Blacklisted Application	0
Blacklisted Domain	0
Blacklisted IP Address	0
Brute Force Attack	0
Download From Internal Server	0
Excessive Data Printed	0
Excessive Data Transmission	0
Excessive Database Administration Tasks	0

ANOMALY TYPE	PARTICIPANTS	SUMMARY	START DATE	SCORE	DESCRIPTION
Excessive File Size Change	__qyTfwELTwsG82APHwAU _utnX4snYiJl1eJl2itm	File size increased by a factor of 10.6, from 60.07 MB to 636.73 MB.	Oct 2, 2017 12:00 AM	9	Possible exfiltration by dumping significant ch data to an exfiltration fi Malicious activities ma include copy-pasting, appending or archiving chunks from one or mo
Excessive File Size Change	KXwyYjxzibsz2fgr XitmUGtmUKZmUeZn	File size increased by a factor of 112.2, from 10.35 MB to 1.13 GB.	Oct 13, 2017 12:00 AM	9	Possible exfiltration by dumping significant ch data to an exfiltration fi Malicious activities ma include copy-pasting, appending or archiving chunks from one or mo
Excessive File Size Change	YvMBYf2rGS2yPjxz2fwt _aJl3eJmUCtmUudn	File size increased by a factor of 51.3, from 1.95 MB to 99.89 MB.	Oct 17, 2017 12:00 AM	8	Possible exfiltration by dumping significant ch data to an exfiltration fi Malicious activities ma include copy-pasting, appending or archiving chunks from one or mo
Excessive File Size Change	__qBVnMlR5wDSb3Ca5wyT ZmtmUiZmY4YnZiJlXutm	File size increased by a factor of 26.2, from 2.76 MB to 72.42 MB.	Oct 3, 2017 12:00 AM	8	Possible exfiltration by dumping significant ch data to an exfiltration fi Malicious activities ma include copy-pasting, appending or archiving chunks from one or mo
Excessive File Size Change	_mNCLXgAbbIBHLNu UvgAdbIBHLgv	File size increased by a factor of 14.1, from 39.28 MB to	Oct 5, 2017 12:00 AM	8	Possible exfiltration by dumping significant ch

Scoring Adjustments



Example Anomaly



Excessive File Size Change 9

Actions

Detects and de-noises excessive increases in file sizes.

Start Date Oct 2, 2017 12:00 AM **End Date** Oct 3, 2017 12:00 AM

Watchlists

Categories Cloud Data | Cloud Storage Anomalies | Exfiltration | Network Detection

Possible exfiltration by dumping significant chunks of data to an exfiltration file. Malicious activities may include copy-pasting, appending or archiving data in chunks from one or more sources.

Excessive file size change has been detected in **individual increases** for a file **ci-20170906.json** in Box date source.

The largest observed change was by a factor of **10.6**, from a previous size of **60.07 MB** to **636.73 MB**.

The file has been observed at its excessively increased size:

- In 1 folder
- Under 1 file name
- Manipulated by 1 user

This is one of only 53 files suspected for exfiltration in a file store containing 63398 files.

Recomendation: Find instances of this file at its excessively increased file size(s), open them, and inspect their content to confirm whether exfiltration took place.Investigation may require searching through employee devices or storage snapshots of Box file repository.

Advice: Don't get mislead by seemingly benign file types or ordinary file sizes. Malicious actors can give any names and extensions to files, i.e., a file having .docx extension may not be a Microsoft Word document at all. Similarly, malicious actors can easily distribute exfiltration information over inconspicuously sized chunks to bypass detection.

Context Building

splunk> User Behavior Analytics | Explore | Analytics | Manage | System | Scope | admin

Home / Anomalies Table / Anomaly Details / __qyTfwELTwsG82APHwAUv3s

__qyTfwELTwsG82APHwAUv3s 0

Last Update Oct 16, 2017 7:07 PM

Watchlists

Account Normal (_ewBHLxzRL2A)

User Anomalies

Anomalies (5)

Excessive File Size Change (2)	9
Multiple Box Operations (1)	6
Suspicious Box Usage (1)	3
Suspicious Data Access (1)	3

Devices in Anomalies (6)

Internal

_CZmX4Im0iJl1eJl2itm	0
_qJmUytmX4YnZiJl2itm	0
3etmUuZmUqtoUmtm	0

External

_qZmUmdoX4ImWeJlXatm	0

Summary

1. Effective early exfiltration detection
2. Cloud stores are new “flash drives”
3. Extreme security risks
4. Don’t guess, design data-driven defense!

Available in Splunk UBA since 4.3.3

.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION