

DFRWS USA 2023

SaaS Forensics & Response

Forensic Preservation, Recovery, and Analysis of SaaS Data

Eoghan Casey, VP, Cybersecurity Strategy & Product Development
with support of Ariel Berkman & others at OwnBackup

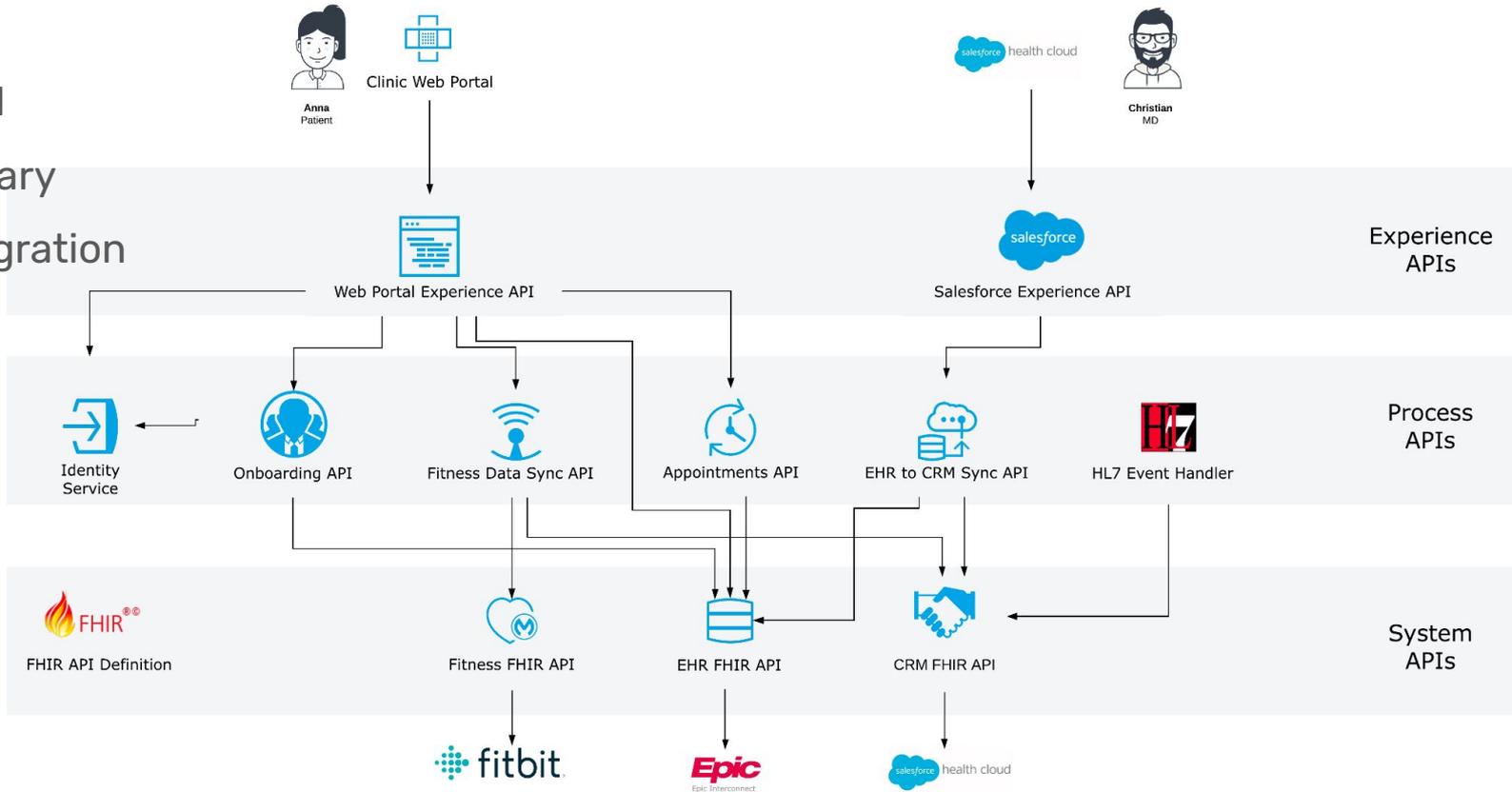
Location: Baltimore
Day: 11 July 2023

Own{backup}

Sample SaaS Solution

SaaS Data

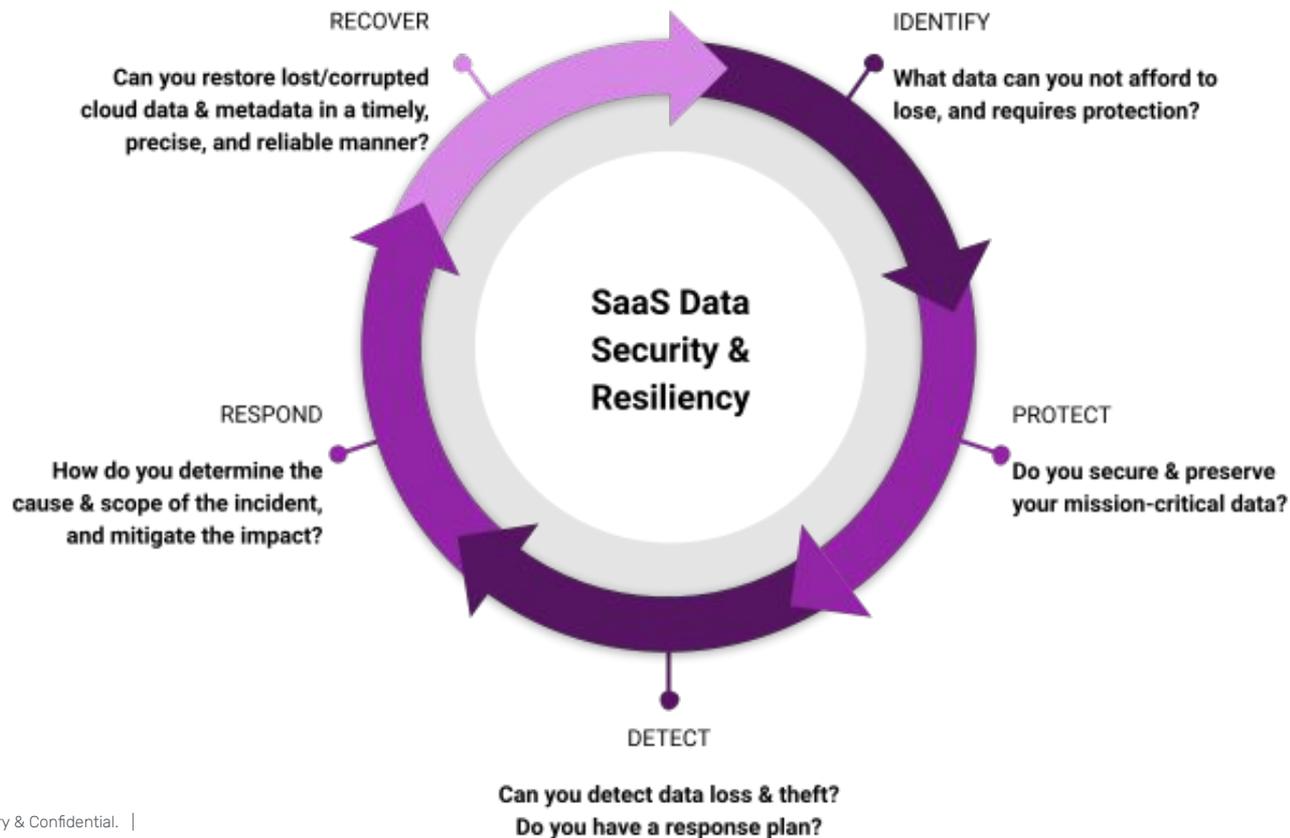
- PII & PHI
- Proprietary
- API integration



SaaS DFIR <> Cybersecurity Lifecycle

DFIR

- Survey
- Preserve
- Analyse
- Integrate
- Interpret
- Document



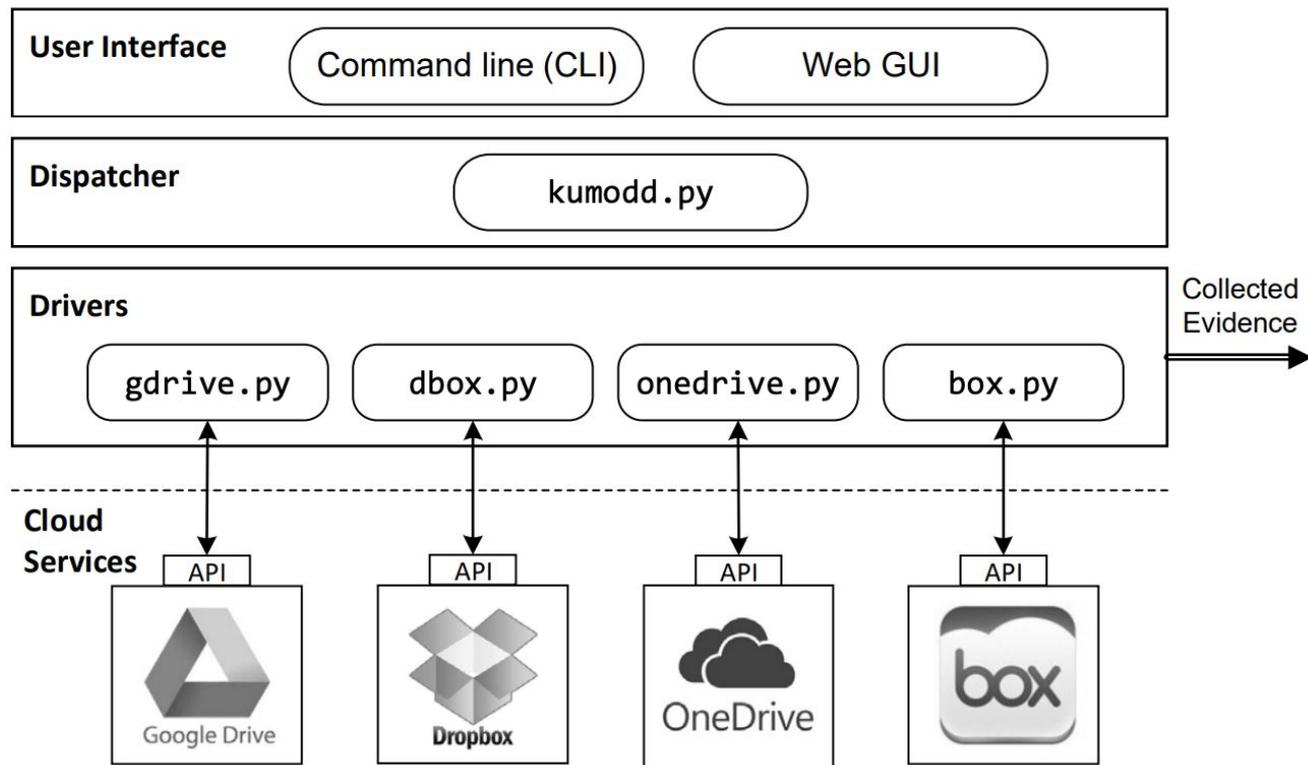
2016: Google Drive Preservation

API-Based Forensic Acquisition of Cloud Drives

- Vassil Roussev
- Andres Barreto
- Irfan Ahmed

➤ kumodd

No deleted data recovery



API gymnastics, audit logging, and integrity checking

Own{backup}

BACKUP AND RECOVERY

How to Capture Forensic- Quality Copies of SaaS Data



Auditing

Filter audited events by user or service:

eoghan.casey@ownbackup.com ▼	All services ▼
------------------------------	----------------

 Export All as CSV → **Event ID, Source IP Address, User, User ID, Event Date, Description**

2022-10-12

eoghan.casey@ownbackup.com opened the compare view for auth_sessions between 12:17 PM, 73.87.185.31
the backup from [Oct 12, 2022 \(11:46 AM\)](#) and the backup from [Oct 12, 2022 \(12:01 PM\)](#)
of [\[Salesforce Data\] eoghan@test.cdo.org](#)

eoghan.casey@ownbackup.com opened the compare view for field_permissions 12:17 PM, 73.87.185.31
between the backup from [Oct 12, 2022 \(11:46 AM\)](#) and the backup from [Oct 12, 2022 \(12:01 PM\)](#) of [\[Salesforce Data\] eoghan@test.cdo.org](#)

eoghan.casey@ownbackup.com initiated a Data Compare on All between the backup 12:04 PM, 73.87.185.31
from [Oct 12, 2022 \(11:46 AM\)](#) and the backup from [Oct 12, 2022 \(12:01 PM\)](#) of [\[Salesforce Data\] eoghan@test.cdo.org](#)

eoghan.casey@ownbackup.com forced a backup for [\[Salesforce Data\] eoghan@test.cdo.org](#) 11:55 AM, 73.87.185.31

eoghan.casey@ownbackup.com added [\[Salesforce Data\] eoghan@test.cdo.org](#) assigned 11:42 AM, 73.87.185.31
to business unit Default Business Unit

eoghan.casey@ownbackup.com logged in (web app) 11:31 AM, 73.87.185.31

SaaS Preservation

Salesforce Data
Default Business Unit

✓ eoghan@test.cdo.org
Org ID 00D3t000005fBduEAE

Jul 09, 2023 – Oct 12, 2022

Dashboard

Backup History

Smart Alerts

My Notifications

GDPR Subject Requests

📅 July 09, 2023 16:51



Latest Backup Succeeded 14.5 MB in 86,500 records

Show This Backup

Recent Backups



06/29



06/30



07/1



07/2



07/3



07/4



07/5



07/6



07/7



07/8



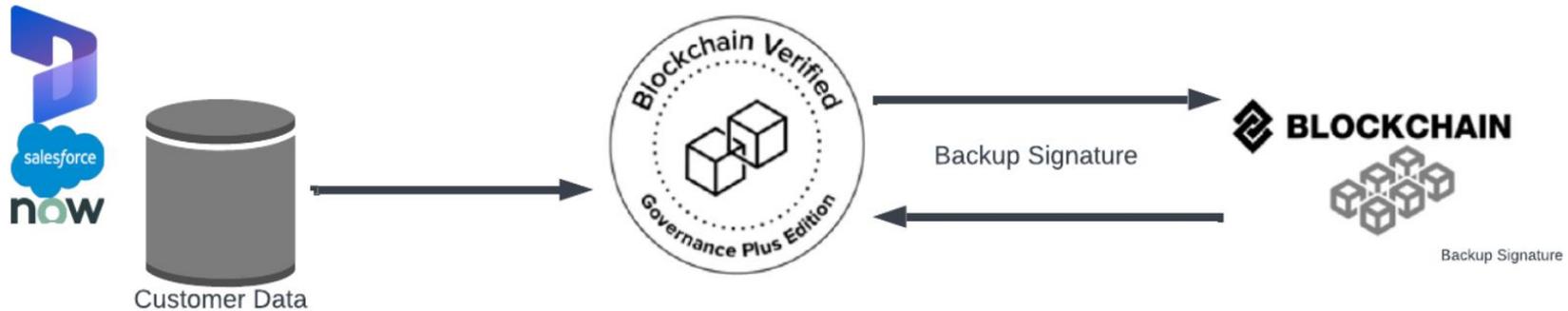
07/9



07/10

SaaS Data Integrity

- Preserving complete copies of SaaS data, including metadata
- Computing cryptographic hash of copies for integrity verification
- Registering hashes on a public blockchain for 3rd party verification
- Comparing current data against known good version



Customers must often irrefutably prove the integrity of backed-up data and confirm these backups have not changed.

OwnBackup generates a verified backup signature based on time stamp and original backup content.

The backup signature is then stored and verified on a public Blockchain, facilitating the ability to confirm the integrity authenticity of backup files.

Capturing Complete Change



Forensic Science
International

Volume 327, October 2021, 110941



A formalized model of the Trace

[David-Olivier Jaquet-Chiffelle](#)  , [Eoghan Casey](#)

<https://doi.org/10.1016/j.forsciint.2021.110941>

the *Trace* of an Event E within a region R is *the **full** modification of the Scene bounded by R , resulting from the Event E , completed or not, and subsequent intrinsic events.*

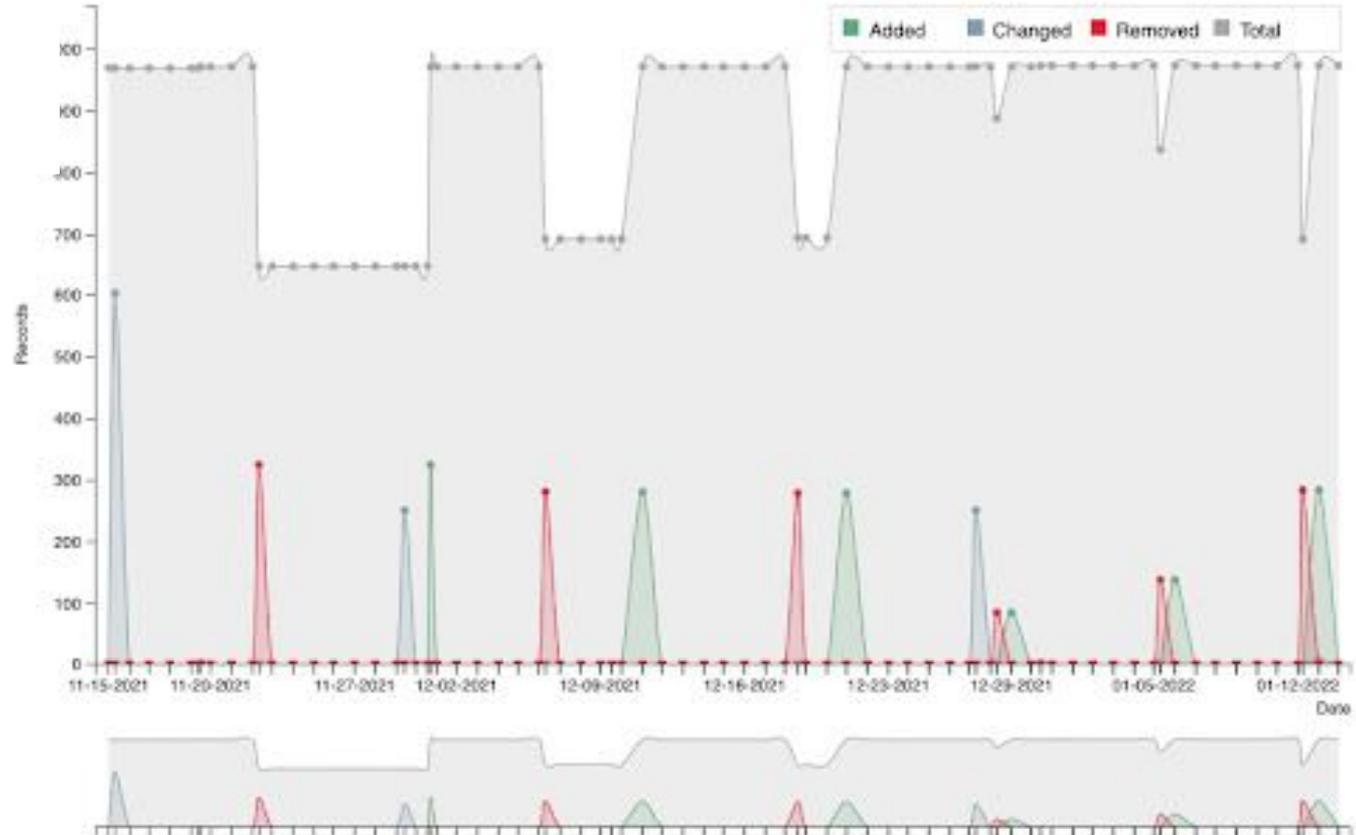
Compare Visual Graph

Date (mm/dd/yy - mm/dd/yy)

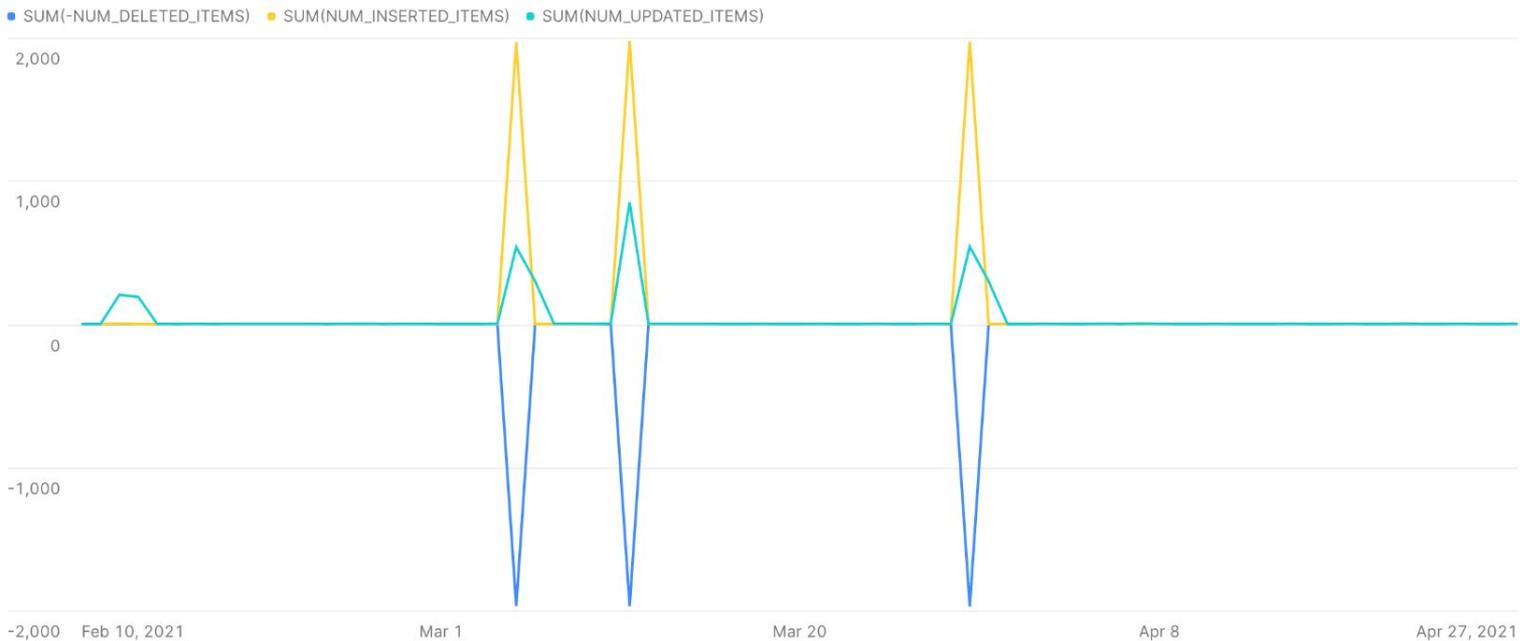
11/15/2021 - 01/14/2022 

SaaS Data Forensics

- Find
- Compare
- Recover



Statistical Analysis of Change



Data

SUM(-NUM_DELETED_ITEMS) sum

SUM(NUM_INSERTED_ITEMS) sum

SUM(NUM_UPDATED_ITEMS) sum

CREATED_AT date

X-Axis

+ Add column

Appearance

- Show Legend
- Show points
- Label X-Axis
- Label Y-Axis
- Crop Y Axis

SaaS Database Forensic Analysis

Compare

- Change
- LastModifiedBy
- LastModifiedDate

The screenshot displays the OwnBackup web interface for comparing two database backups. The interface includes a navigation bar with tabs for Backup, Find, Compare, Restore, Replicate, Enhanced Sandbox Seeding, Anonymize, and Jobs. The current view is 'Compare View' for the 'contacts' table. Two backup versions are compared: 'Dec 7, 2021 (11:17 AM)' with 46 records and 'Dec 6, 2021 (07:04 PM)' with 46 records. The table below shows the data comparison, with a tooltip highlighting a change in the 'SSN_c' column.

	id	MobilePhone	Email	DoNotCall	SSN_c	LastModifiedDate
<input type="checkbox"/>	0035e0000SAHISAAX	832-132-6854	mmacgjollapheadair2@dii...	false	New value 111-11-1111	2021-12-07T04:14:41.000...
<input type="checkbox"/>	0035e0000SAHtvAAH	574-491-2872	hwoolgar5@twitpic.com	false	Previous value 580-41-3880	2021-12-07T04:15:56.000...
<input type="checkbox"/>	0035e0000SAIxAAP	Gribble	fgribble0@4shared.com	false	111-11-1111	2021-12-07T04:14:02.000...
<input type="checkbox"/>	0035e0000SAIL1AAP	704-715-3797	khamston3@eventbrite.com	false	111-11-1111	2021-12-07T04:15:03.000...
<input type="checkbox"/>	0035e0000SAINBAA5	412-758-5559	browett1@people.com.cn	false	111-11-1111	2021-12-07T04:14:21.000...
<input type="checkbox"/>	0035e0000SAINDAA5	316-505-4533	enibio8@ovh.net	true	111-11-1111	2021-12-07T04:17:48.000...
<input type="checkbox"/>	0035e0000SAITFAA5	33906	abranson7@columbia.edu	false	111-11-1111	2021-12-07T04:16:57.000...
<input type="checkbox"/>	0035e0000SAIaUAAX	205-361-4326	flepiscopi4@trellian.com	false	111-11-1111	2021-12-07T04:15:28.000...
<input type="checkbox"/>	0035e0000SAIffAAAX	239-536-2170	creese6@unc.edu	false	111-11-1111	2021-12-07T04:16:31.000...
<input type="checkbox"/>	0035e0000SAU0QAAX	540-483-2625	hleroyg@over-blog.com	true	141-94-1031	2021-12-07T04:21:43.000...

SaaS Event Logs

High volume and variety

- Api Usage
- Api Anomaly
- Bulk Api Result
- Credential Stuffing
- Identity Verification
- Identity Provider
- List View
- Login As
- Login
- Logout
- Permission Set
- Report Anomaly
- Report
- Session Hijacking

```
"EVENT_TYPE","TIMESTAMP","REQUEST_ID","ORGANIZATION_ID","USER_ID","RUN_TIME","CPU_TIME","URI","SESSION_KEY","LOGIN_KEY","USER_TYPE","REQUEST_STATUS","DB_TOTAL_TIME","API_TYPE","API_VERSION","CLIENT_NAME","METHOD_NAME","ENTITY_NAME","ROWS_PROCESSED","REQUEST_SIZE","RESPONSE_SIZE","DB_BLOCKS","DB_CPU_TIME","EXCEPTION_MESSAGE","TIMESTAMP_DERIVED","USER_ID_DERIVED","CLIENT_IP","URI_ID_DERIVED"
"API","20230522230033.437","4q50QUyCLHfKOG-mMN9x-","00D20000000opmF","0056900000B1d3q","104","99","Api","DG+xn6lqUxpbL44G","1SPMvj7fpnDi2QMg","Standard","","1151081","P","57.0","Pardot/","describe","pi__ObjectChangeLog__c","","685","28337","","","2023-05-22T23:00:33.437Z","0056900000B1d3qAAB","XX.172.247.215",""
"API","20230522230035.328","4q50QaRK_Qp1BtG-mMP04-","00D20000000opmF","0056900000B1d3q","204","24","Api","DG+xn6lqUxpbL44G","1SPMvj7fpnDi2QMg","Standard","","7851814","P","57.0","Pardot/","query","pi__ObjectChangeLog__c","1","1043","1130","11","0","","2023-05-22T23:00:35.328Z","0056900000B1d3qAAB","XX.172.247.215",""
"API","20230522230036.379","4q50QeWuh-6cm8G-mMQ8t-","00D20000000opmF","0056900000B1d3q","205","109","Api","DG+xn6lqUxpbL44G","1SPMvj7fpnDi2QMg","Standard","","67297517","P","57.0","Pardot/","delete","pi__ObjectChangeLog__c","1","647","461","2220","50","","2023-05-22T23:00:36.379Z","0056900000B1d3qAAB","XX.172.247.215",""
"API","20230522230045.365","4q50RBhj1JQvgtG-mMihV-","00D20000000opmF","0056900000B1d3q","21","13","Api","DG+xn6lqUxpbL44G","1SPMvj7fpnDi2QMg","Standard","","5257963","P","57.0","Pardot/","get_updated","Lead","0","765","482","11","0","","2023-05-22T23:00:45.365Z","0056900000B1d3qAAB","XX.21.28.50",""
"API","20230522230045.487","4q50RCALW3zWndG-mMju7-","00D20000000opmF","0056900000B1d3q","19","13","Api","DG+xn6lqUxpbL44G","1SPMvj7fpnDi2QMg","Standard","","4511520","P","57.0","Pardot/","get_updated","Lead","0","765","482","8","0","","2023-05-22T23:00:45.487Z","0056900000B1d3qAAB","XX.21.28.50",""
```

Future Work: ML/AI Applied to SaaS Forensics

Approaches & Challenges

- Anomaly detection
 - Never seen before
- Classification
 - Data quality and labelling
 - Compound event & precursors
- Rule-based detection
 - Generating and maintaining rules
 - Compound rules