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

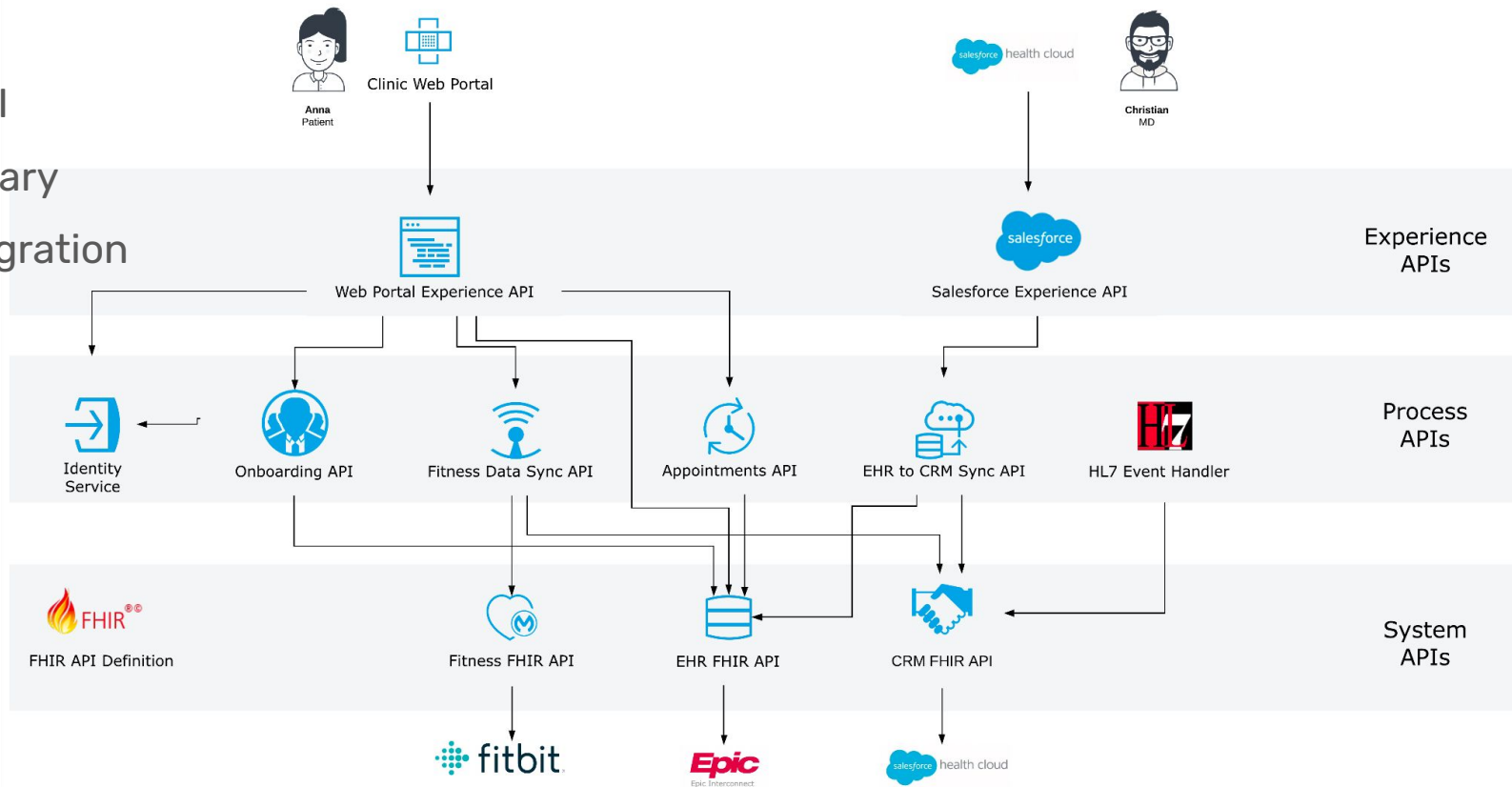
Location: Baltimore
Day: 11 July 2023

Own{backup}

Sample SaaS Solution

SaaS Data

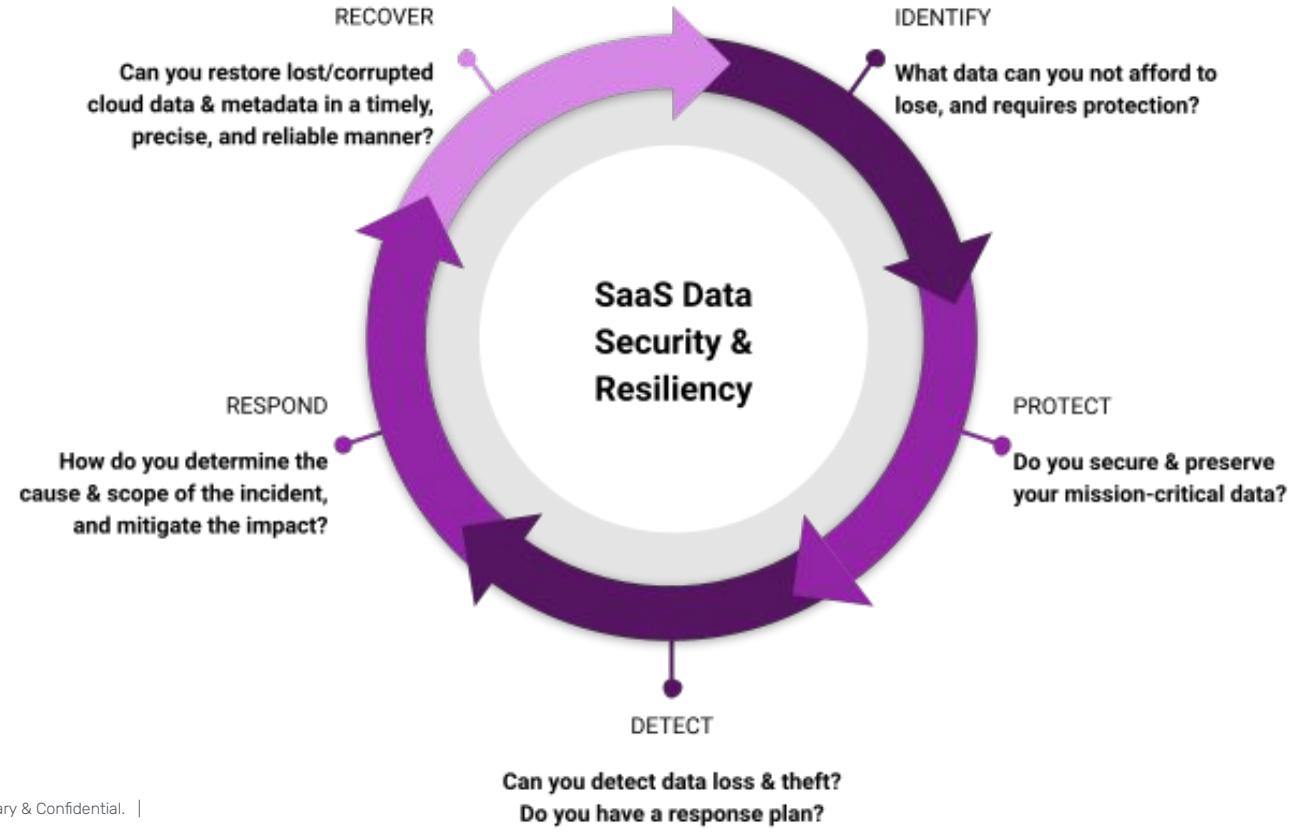
- PII & PHI
- Proprietary
- API integration



SaaS DFIR <> Cybersecurity Lifecycle

DFIR

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



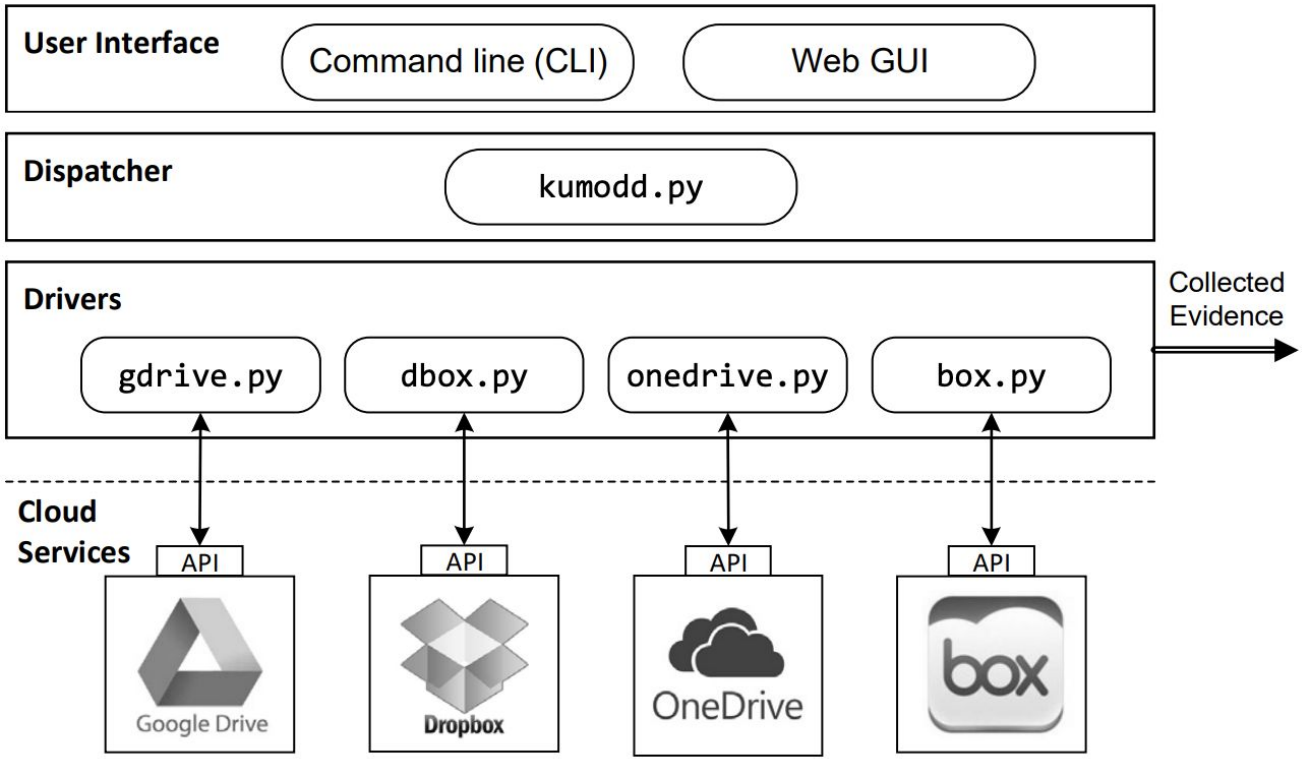
2016: Google Drive Preservation

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

Auditing

Filter audited events by user or service:

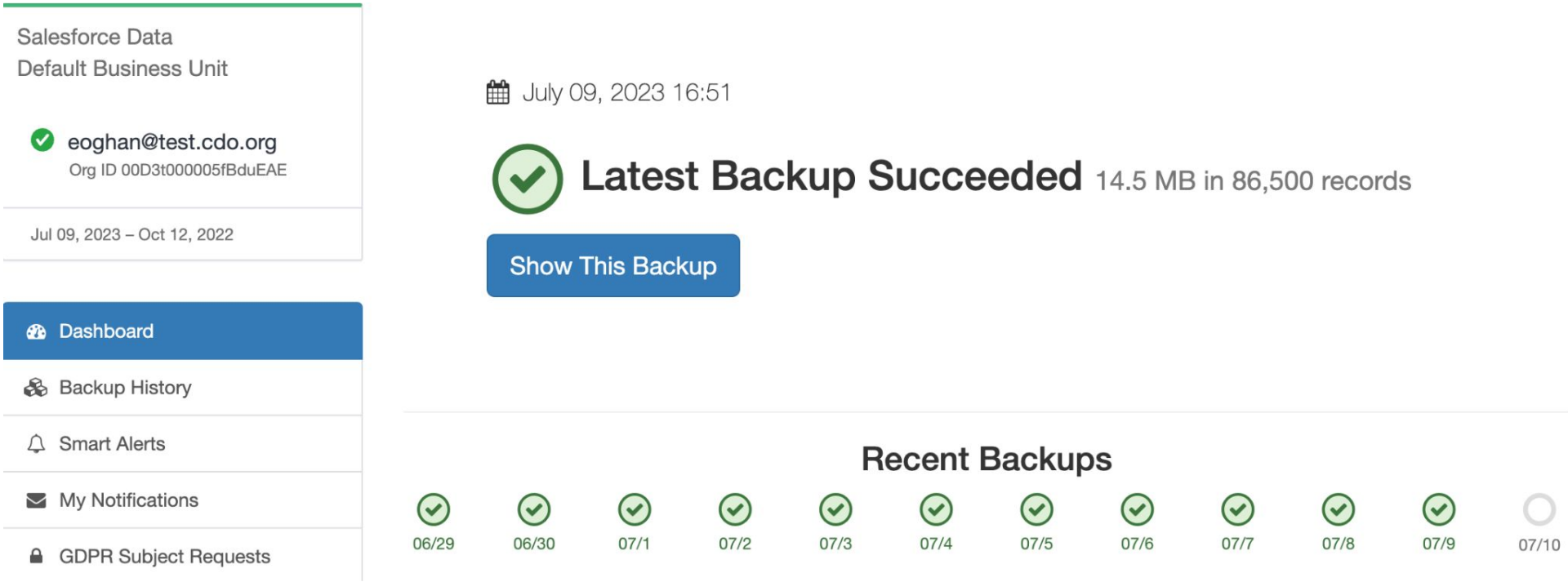
eoghan.casey@ownbackup.com | All services

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 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	12:17 PM, 73.87.185.31
eoghan.casey@ownbackup.com opened the compare view for field_permissions 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	12:17 PM, 73.87.185.31
eoghan.casey@ownbackup.com initiated a Data Compare on All 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	12:04 PM, 73.87.185.31
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 to business unit Default Business Unit	11:42 AM, 73.87.185.31
eoghan.casey@ownbackup.com logged in (web app)	11:31 AM, 73.87.185.31

SaaS Preservation

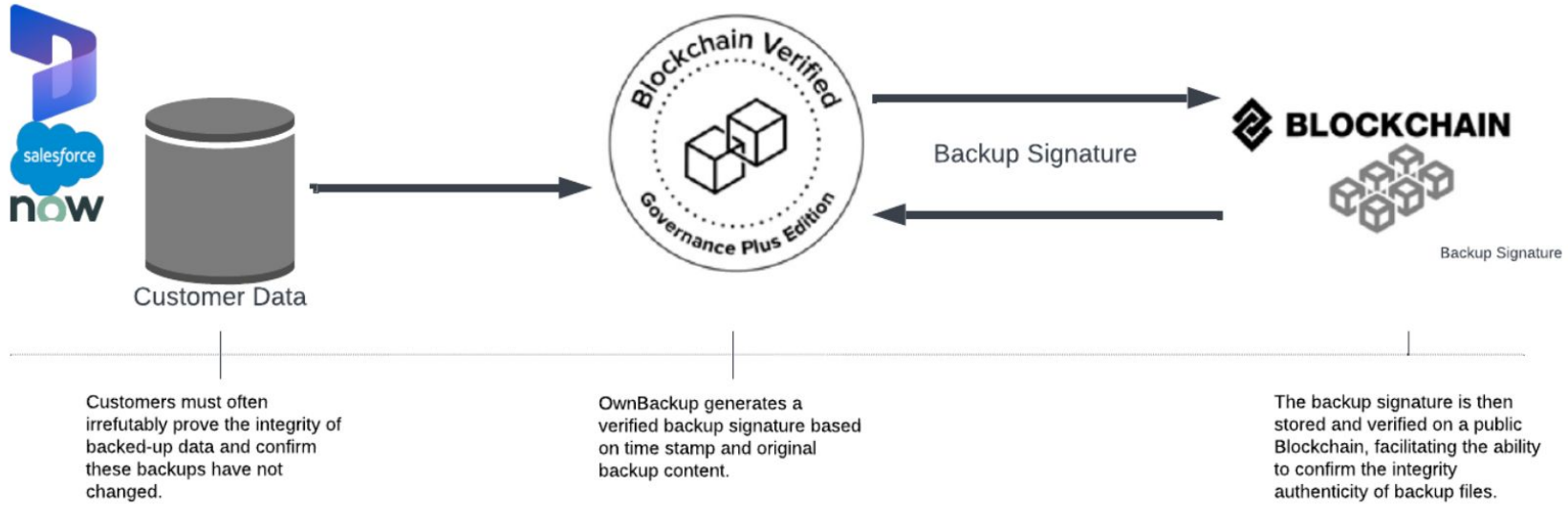


Own{backup}

Deleted data recovery

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



Capturing Complete Change

ELSEVIER

Forensic Science International

Volume 327, October 2021, 110941

A formalized model of the Trace

David-Olivier Jaquet-Chiffelle, Eoghan Casey

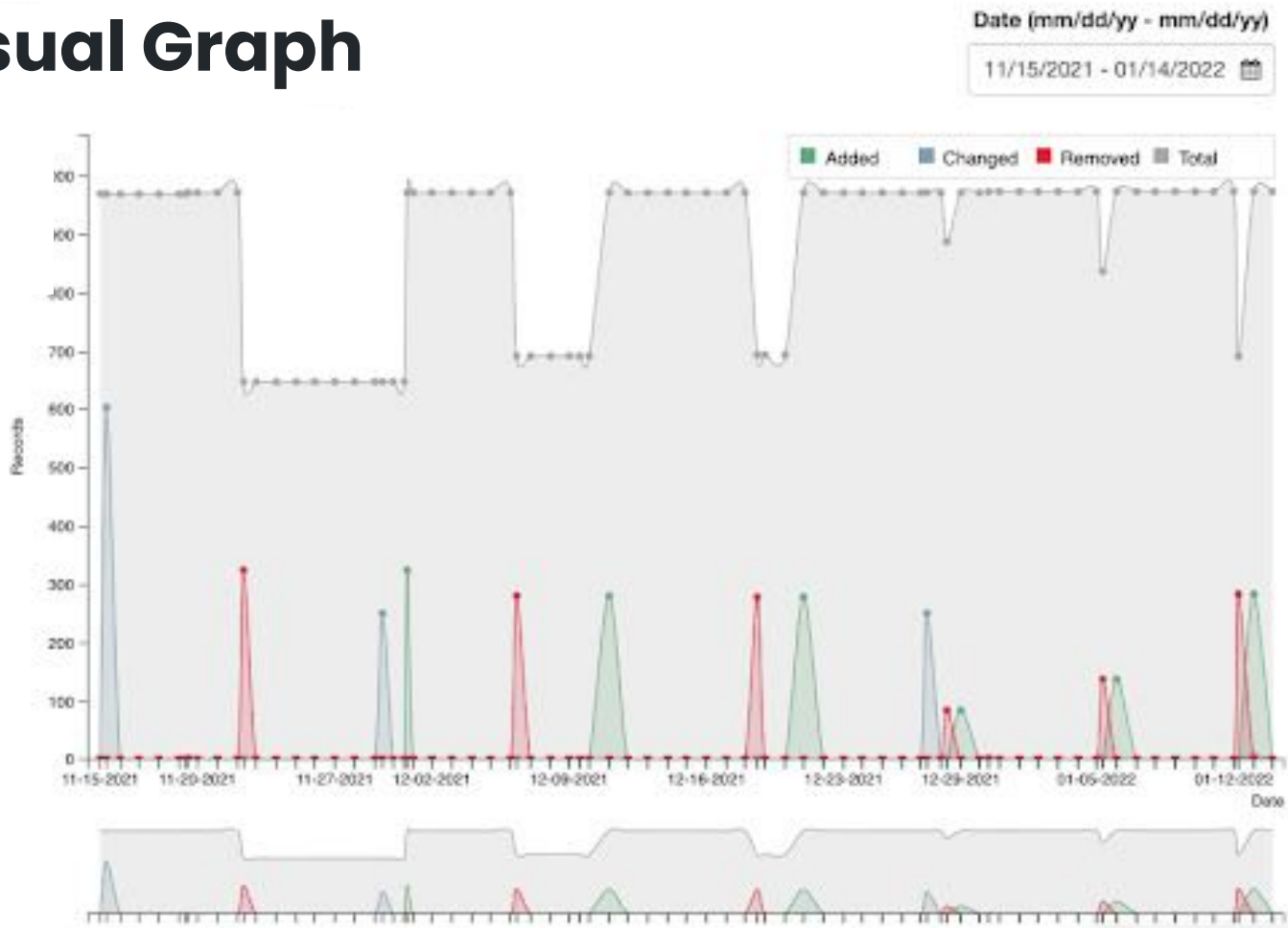
https://doi.org/10.1016/j.forsciint.2021.110941

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.*

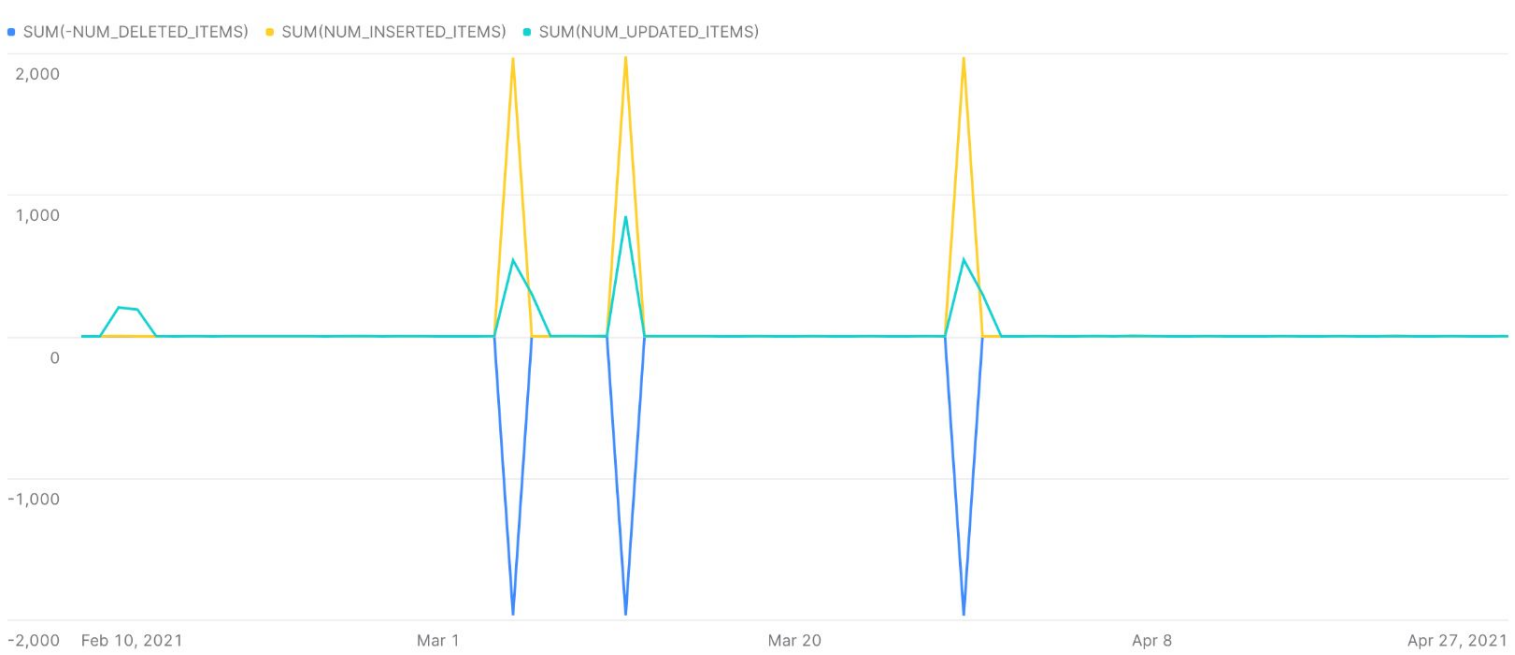
Compare Visual Graph

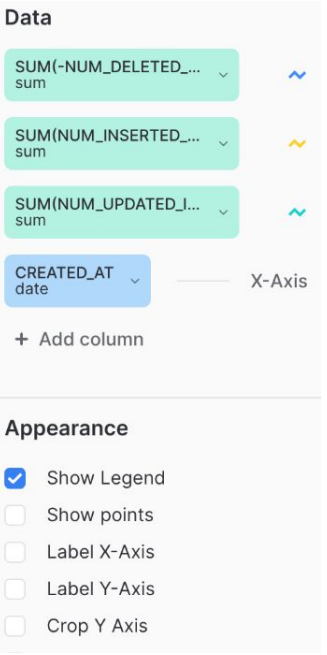
SaaS Data Forensics

- Find
- Compare
- Recover



Statistical Analysis of Change

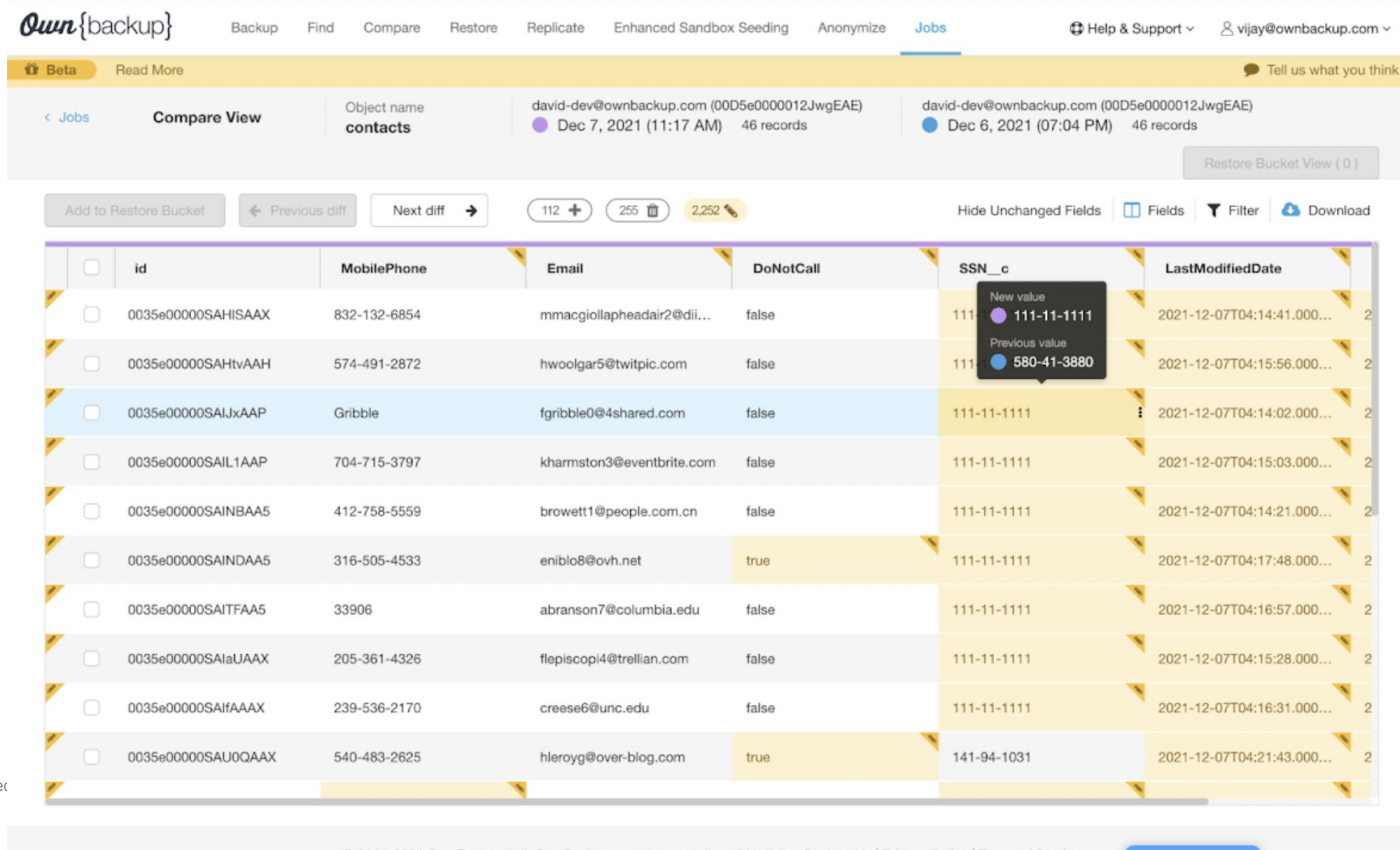




SaaS Database Forensic Analysis

Compare

- Change
- LastModifiedBy
- LastModifiedDate



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","4q50QUyCLHfiKOG-mMN9x-","00D20000000opmF","0056900000B1d3q","104","99","Api","DG+xn6IqUxpbL44G","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+xn6IqUxpbL44G","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+xn6IqUxpbL44G","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+xn6IqUxpbL44G","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+xn6IqUxpbL44G","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