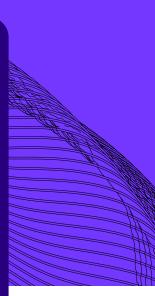


	111111111111111111111111111111111111111		~
INVESTIGATION WORKBENCH	0		
USER v bill@kaizen.io	🖻 04/18/2024 - 04/24/2024 🛛 🐸 🔥 🔕 🧄		State) Last Event
14 Forensic Events 10 Forensic Stories 2	Cloud Resources / 3 Categories		
V Platforms v Forensic stories v	MITRE ATTRCK v Importance v Category v 💿 🏦 CLEAR		
Date & Time (UTC) E4 Source Entities	Forensic Event	Platform Cloud Resource	Importance
Apr 24, 2024 14:12:30 bill@kaizen.io	Bucket policy of bucket 'client-data-eu-region' was modified	Kaizen Fin Prod	Mediu
Apr 24, 2024 07:13:30 bill@kaizen.io	Snapshot snap-6e86a99a1e82568e5 was copied from snap-76a4fdc2f43e015f5	Kaizen Fin Prod	Mediu
Apr 24, 2024 04:40:30 bill@kaizen.io	Bucket policy of bucket 'finance-docs-backup' was modified	Kaizen Fin Prod	Mediu
Apr 23, 2024 20:43:02 bill@kaizen.io	Inbox rule created to allow forwarding outside of the user's or sender's domain 'kaizen.lo'	S Kaizen AAD Prod	Mediu
Apr 23, 2024 18:43:02 bill@kaizen.io	5 objects were downloaded from 'https://kaizen- my.sharepoint.com/personal/bill_kaizen_io/' site	S Kaizen AAD Prod	Mediu
Apr 23, 2024 17:43:02 bill@kaizen.io	2 objects were accessed from 'https://kaizen- my.sharepoint.com/personal/bill_kaizen_io/' site	Kaizen AAD Prod	• Mediu
Apr 23, 2024 16:43:02 bill@kaizen.io	User registered Authenticator App with Notification and Code	🚸 Kaizen AAD Prod	• Low
Apr 23, 2024 16:43:02 bill@kaizen.io	User successfuly signed-in	🚸 Kaizen AAD Prod	• Low
Apr 23, 2024 15:43:02 bill@kaizen.io	User changed password from a new country - 'Mexico'	🚸 Kaizen AAD Prod	• High
Apr 23, 2024 10:13:00 bill@kaizen.io	1 object was accessed from `https://kaizen-io.sharepoint.com/personol/bill_kaizen site	Lio/" 🔇 Kaizen AAD Prod	Mediu



Supercharging SOC teams for the Cloud Era

The only complete solution for cloud threat detection, investigation & response



Broad coverage

Enabling full visibility across clouds and SaaS



Rich context Connecting the dots for better threat detection

-	
_	

Fast answers

Automating investigation to accelerate response 70x



Specialized teams

Unlimited access to experts elevating SOC cloud capabilities

Featuring

Cloud Security Data Lake

Gain full visibility into your cloud and SaaS logs, even as environments change. Mitiga amasses, enriches, and correlates the specific, forensic-level data needed for investigations in a single pane of glass.

Cloud Threat Detection

Uncover threats across your cloud and SaaS. Mitiga leverages our Cloud Attack Scenario Library to correlate activities from your entire digital footprint and triage areas of concern.

Cloud Investigation

Enable your cloud and SaaS hunts with Investigation Workbench to create fast, detailed timelines of forensic events, while Mitiga's threat hunters serve as your extra set of eyes.

Cloud Incident Response

Accelerate investigation 70x. Mitiga automates time-intensive processes to deliver immediate answers on breach causes, impacts, timelines, and recommended remediation.

"Mitiga has a very elegant solution that enables companies to respond to sophisticated attacks in their SaaS and Cloud environments immediately."



John Watters Former COO and President, Mandiant "When something bad happens and you need to activate Mitiga, within an hour they already have people looking at your logs for the past year or even more."



SSPM Closing the gap. DSPM Completing CNAPP cloud security. CSPM CIEM CWPP at the Vulnerability & EP/EDR/MDR DFIR Tools Patch Management NDR Breach & Attack Simulation Firewalls IR Services

Where your CNAPP stops, Mitiga begins.



mitiga.io