

Solve Cloud Forensics at Scale

Archived: 2026-04-06 01:52:35 UTC

10,000

Darktrace customers



MUSEE DU
LOUVRE

FRANCAIS

STEVE MADDEN





MUSTERD

LOUVRE

GUINNESS

STEVE MADDEN







The challenge

Multi-cloud investigations are manual and slow, and data disappears fast

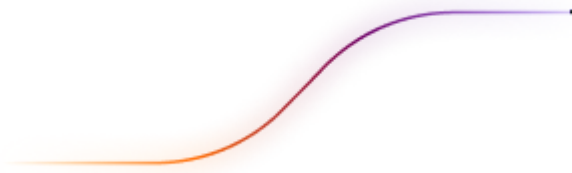
1/3rd

of alerts in cloud environments do not get investigated due to lack of information

89%

of organizations suffer damage before containing and investigating incidents

Darktrace's report: "Organizations require a new approach to handle investigations and response in the cloud"



Automated data capture across your business

Integrates with any alert source and deploys via API to enable fast, low-overhead response within existing workflows.

Support containers and ephemeral assets

Leverage automation to ensure incident data is captured and preserved before it disappears. Automatically collect key data sources and memory from individual processes for forensic analysis.

Parallel collection and processing

Capture more data in less time, resulting in deep forensic insight delivered in minutes, not days.

inv-0025 Import Search

Overview Automated Investigation Insights Evidence Events Vulnerabilities

Import into inv-0025 from the Cloud
Select one of the added Accounts to begin importing from a variety of cloud services.

Choose a Cloud Account
Supported Cloud Providers

AWS GCP Azure All

Select an Access Method
Account Security Token

Selected Account: No account selected
+ Account

Account Name	Cloud Provider	Credential Identifier	Last Used	Status
Default Acquisition	Amazon Web Services		10 days ago	Health ■ ■
Azure - demo	Microsoft Azure		1 month ago	Health ■
Cado Project	Google Cloud Platform		3 months ago	Health ■
XDR Dev Account	Amazon Web Services		4 months ago	Health ■ ■
	Amazon Web Services		-	Health ■ ■

Full attack timelines in minutes, not hours

Timelines enriched with context to shows exactly what happened, when, and how

Eliminate tedious manual work

Get root cause analysis for cloud security alerts without combing through logs or artifacts manually.

Accelerate investigations

A visual timeline links files, commands, and lateral movement.

Reduce uncertainty

Ensure response decisions are informed by a complete and accurate picture of the threat.

The screenshot shows the Cado Security interface for an automated investigation. At the top, there's a search bar with the query 'auto_investigate_score:[0.99 TO 1.0]'. Below it are navigation tabs: Overview, Automated Investigation (selected), Insights, Evidence, Vulnerabilities, Alarms, and Events. The main section is titled 'Automated Investigation' and contains a brief description: 'These events represent the most significant findings identified by Cado's automated investigation machine learning model. Events are more likely to be shown if they are tagged by our alarm system or similar to other alarmed events in terms of shared fields or proximity in time.' Below this is a 'Timeline Results' section showing 16/50 items. The timeline table has columns for Timestamp, Details, User, and Alarms. The events listed are:

- 2020-07-19 (11 items)**
- 20:46:30**: Content Modification Time, Last Access Time, Change Time, Creation Time. Details: /root/.bash_history, A File Was Created. User: root. Alarms: WannaMine, XMRig Installer, Wget In Cron, Reference To XMRig, Reference To Known Monero Mining Pool, Possible Cronjob Downloading From Pastebin, Mining Pool Detected.
- 20:44:52**: Event time. Details: Action type: DNS_REQUEST, Title: Bitcoin-related domain name queried by EC2 instance i-027fb097e7edaccad, Resource type: Instance, Resource name/id: i-027fb097e7edaccad, Local IP: xmr-asia1.nanopool.org. Alarms: Bitcoin-Related Domain Name Queried By EC2 Instance I-027fb097e7edaccad.
- 20:44:46**: Event time. Details: Action type: NETWORK_CONNECTION, Title: EC2 instance i-027fb097e7edaccad communicating with a known Bitcoin-related IP Address, Resource type: Instance, Resource name/id: i-027fb097e7edaccad, Local IP: 172.31.64.171, Remote IP: 139.99.101.198, Direction: OUTBOUND. Alarms: TOR IP ADDRESS, EC2 Instance I-027fb097e7edaccad Communicating With A Known Bitcoin-Related IP.
- 20:44:28**: Last Access Time. Details: /var/www/html/wp-content/plugins/trace. Alarms: XMRig.
- 20:42:18**: Content Modification Time, Last Access Time, Change Time, Creation Time. Details: /var/www/html/wp-content/uploads/a.sh, A File Was Created. Alarms: WannaMine, Pastebin Download, Pastebin B64, Reference To XMRig.

Use cases

Empowers organizations to respond to threats faster

Better understand risk across complex environments, reduce MTTR, and rapidly deploy with this first-of-its-kind technology

SOC triage

Get immediate insights into malicious activity, saving analysts precious time during event triage. Perform automated triage of acquisitions of endpoint resources to gain deeper context in a shorter period of time.

Cross-cloud investigations

Investigate incidents identified in any cloud environment in a single solution. Findings are unified in one timeline to allow seamless investigation and response.

Container & K8 investigations

Perform investigation and response in ephemeral environments, leveraging automation to ensure incident data is captured and preserved before it disappears.

SaaS investigations

Investigate key SaaS logs, alongside other sources captured across on-premises and cloud assets to gain a better understanding of the scope and impact of malicious activity.

Cloud detection & response

Marry threat detection with automated collection and investigation - with critical forensic-level context - to expedite response to cloud threats as soon as malicious activity is detected.

Evidence preservation

Automate the collection, processing, analysis, and preservation of evidence so it's accessible to all teams when needed, every time – before it disappears.



“We resolve hundreds of potential incidents in minutes. By assisting analyst investigations, we've been able to drastically increase efficiency by 250%.”

Global Gaming Company

Head of Security Operations

“We have a cloud team that takes countless manual steps to capture and process forensic data...I can't wait to tell them I can do this in just a few clicks!”

Fortune 500 US Company

DFIR Team Lead

“The fact that I no longer have to wait 24 hours to start a forensics investigation is game changing.”

Top Cybersecurity Consulting Firm

DFIR Manager

Resource

Read the solution brief

250%

increase in capacity

Discover how Darktrace / Forensic Acquisition & Investigation enables faster and deeper investigations in the cloud



Source: <https://www.cadosecurity.com/blog/the-nine-lives-of-commando-cat-analysing-a-novel-malware-campaign-targeting-docker>