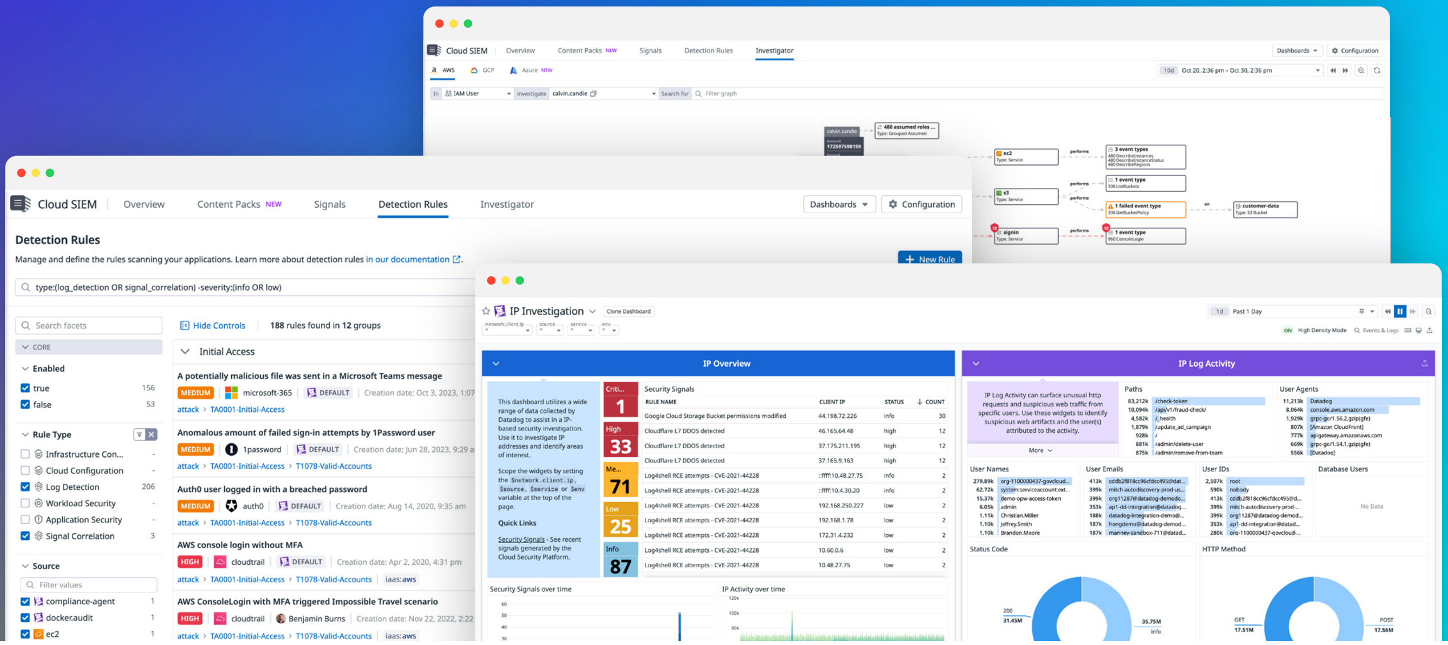
Datadog Cloud SIEM

Detect, investigate, and respond to threats across your applications, networks, and infrastructure.


Cloud SIEM
Overview
Content Packs NEW
Signals
Detection Rules
Investigator
Dashboards
Configuration
Detection Rules
Manage and define the rules scanning your applications. Learn more about detection rules in our documentation
type:(log_detection OR signal_correlation) -severity:(info OR low)
+ New Rule
Hide Controls
188 rules found in 12 groups
Initial Access
A potentially malicious file was sent in a Microsoft Teams message
Anomalous amount of failed sign-in attempts by 1Password user
Auth0 user logged in with a breached password
AWS console login without MFA
AWS ConsoleLogin with MFA triggered Impossible Travel scenario
IP Investigation
IP Overview
IP Log Activity
Security Signals
Security Signals over time
IP Activity over time
Paths
User Agents
User Names
User Emails
User IDs
Database Users
Status Code
HTTP Method

Introduction

As dynamic, cloud-native environments face increasingly sophisticated security threats, the boundaries between security, development, and operations teams are beginning to fade. Security teams need visibility into their applications, infrastructure, and network, while development and operations teams need the ability to secure the services they own. Entire engineering organizations therefore need access to a unified platform for their monitoring and security data so they can protect their environments from breaches and attacks.

Limitations of threat detection tools in the cloud

Businesses face mounting pressure with each new breach or attack, so it’s essential that they have the tools they need to proactively detect potential threats before they escalate. But legacy SIEM solutions often are not equipped to handle the inherent complexity of cloud-native environments, posing several challenges for teams that are trying to fortify their security posture:

SILOED TOOLS LIMIT VISIBILITY

- Cloud-native environments are fast-paced, and it’s important to capture all activity in order to identify security threats and remain compliant. Historically, teams have relied on multiple siloed tools to monitor these dynamic systems, but this process creates blind spots and slows down the investigation process.

LOGGING INCONSISTENCIES COMPLICATE THREAT DETECTION

- Authentication logs come from many different sources in your environment, which results in formatting inconsistencies. They may also be managed by different teams and implemented with different third-party services, such as Google, Okta, and Auth0. This can make it difficult to perform meaningful analysis of all authentication activity.

INVESTIGATIONS ARE MISTAKE-PRONE

- Organizations often struggle to assess the impact of security attacks across ephemeral entities and unknown users, and undetected attacks can lead to major security breaches. It's therefore critical that the teams responsible for securing cloud services can identify and respond to threats as soon as they occur.

MISCONFIGURATIONS CAN HAVE SEVERE CONSEQUENCES

- A single misconfigured security group in a cloud environment can have cascading consequences and lead to a serious data breach. This puts a lot of pressure on development and operations teams to properly secure their services.

INCOMPLETE CONTEXT DUE TO COSTLY LOG RETENTION

- Frequently, companies opt for shorter data retention periods due to cost constraints, infrastructure limitations, risk tolerance, and other factors. However, limiting log retention can result in blind spots and a lack of the necessary context required to comprehensively assess potential threats and expedite security investigations.

SLOW QUERIES FROM MULTIPLE INDEXES

- Many traditional SIEM systems use multiple indexes for search and analysis. For example, one index may handle daily activities (detections, investigations, user analytics, threat hunting) with a 3-month retention period, while another index might retain data for 3 to 12 months for intermittent needs like regulatory compliance and investigations, and require periodic rehydration. But using multiple indexes can lead to slower queries and disjointed investigations, especially when running scheduled queries with differing response times across indexes.

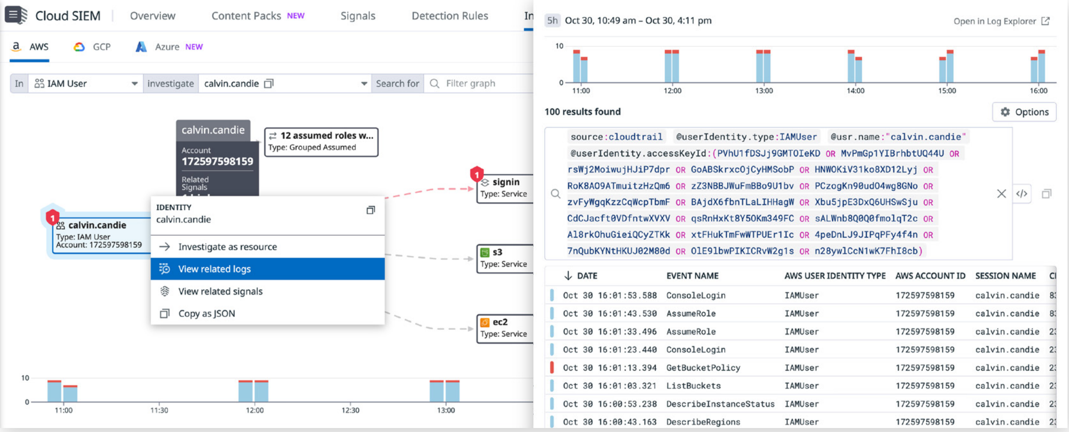
Detect and analyze security threats anywhere in your stack

Datadog Cloud SIEM provides end-to-end security coverage of dynamic, distributed systems in a unified platform. This enables DevOps, SecOps, and GRC teams to work together to detect and respond to threats and misconfigurations in real time, without having to switch contexts. Cloud SIEM is fully integrated with all of Datadog's application and infrastructure monitoring products, which allows users to seamlessly pivot from a potential threat to associated monitoring data in order to quickly triage security alerts.

With Datadog Cloud SIEM, you can:

UNIFY YOUR OBSERVABILITY AND SECURITY EFFORTS

- **See all of your data in one place.** Easily correlate security data with runtime events, application and service logs, and more.
- **Break down silos between teams.** Development, security, and operations teams can access the same observability data and drive security investigations in a single, unified platform.

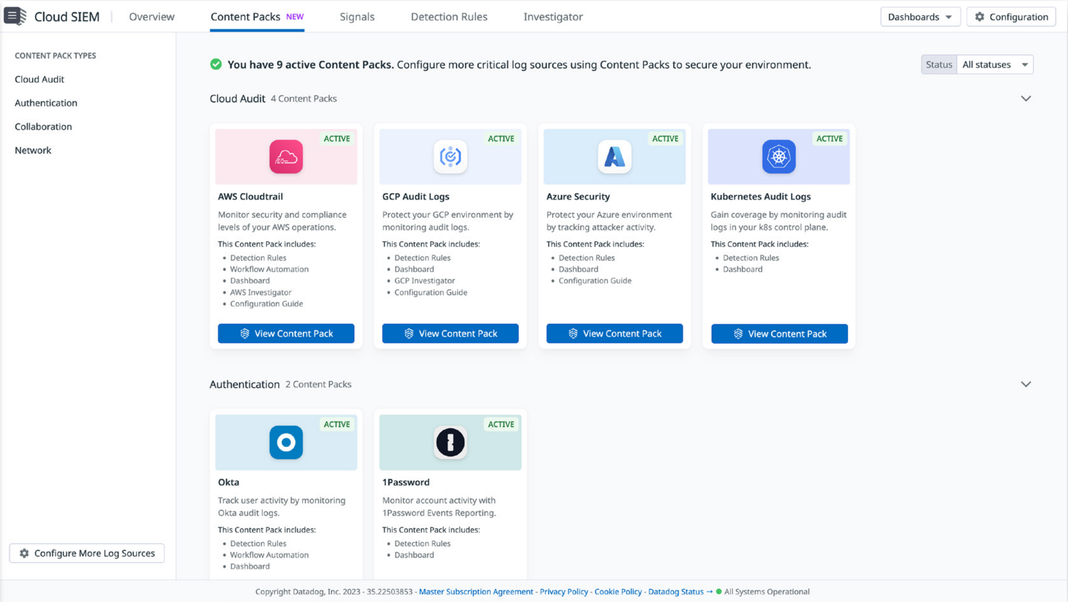


```
source:cloudtrail  @userIdentity.type:IAMUser  @usr.name:"calvin.candie"
@userIdentity.accessKeyId:(PVhU1fDSJj9GMTOIeKD OR MvPmGp1YIBrhbtUQ44U OR
rsWj2MoiwujHJiP7dpr OR GoABSkrxcOjCyHMSobP OR HNWOKiV31ko8XD12Lyj OR
RoK8AO9ATmuitzHzQm6 OR zZ3NBBJWuFmBBo9U1bv OR PCzogKn90udO4wg8GNo OR
zvFyWgqKzzCqWcpTbmF OR BAjdX6fbnTLaLIHHagW OR Xbu5jpE3DxQ6UHSwSju OR
CdCJacft0VDfntwXVXV OR qsRnHxKt8Y5OKm349FC OR sALWnb8Q0Q0fmolqT2c OR
Al8rkOhuGieiQCyZTKk OR xtFHukTmFwWTPUEr1Ic OR 4peDnLJ9JIPqPFy4f4n OR
7nQubKYNtHKUJ02M80d OR OlE9lbwPIKICRvW2g1s OR n28ywlCcN1wK7FhI8cb)
```

DATE	EVENT NAME	AWS USER IDENTITY TYPE	AWS ACCOUNT ID	SESSION NAME	CI
Oct 30 16:01:53.588	ConsoleLogin	IAMUser	172597598159	calvin.candie	83
Oct 30 16:01:43.530	AssumeRole	IAMUser	172597598159	calvin.candie	83
Oct 30 16:01:33.496	AssumeRole	IAMUser	172597598159	calvin.candie	23
Oct 30 16:01:23.440	ConsoleLogin	IAMUser	172597598159	calvin.candie	23
Oct 30 16:01:13.394	GetBucketPolicy	IAMUser	172597598159	calvin.candie	23
Oct 30 16:01:03.321	ListBuckets	IAMUser	172597598159	calvin.candie	23
Oct 30 16:00:53.238	DescribeInstanceStatus	IAMUser	172597598159	calvin.candie	23
Oct 30 16:00:43.163	DescribeRegions	IAMUser	172597598159	calvin.candie	23

EASILY INGEST LOG DATA AND CONFIGURE LOG SOURCES

- **Onboard teams quickly with an intuitive platform and a hub for out-of-the-box content.** Content Packs simplify the process of getting started with Datadog Cloud SIEM, providing a centralized hub for accessing security-specific integration content with out-of-the-box detection rules, interactive dashboards, a visual investigator, workflow automation blueprints, and written content such as blogs, configuration guides, and more. This means you can go from zero to operational quickly, with minimal effort to ingest data, configure log sources, and access critical content.



You have 9 active Content Packs. Configure more critical log sources using Content Packs to secure your environment.

Cloud Audit 4 Content Packs

AWS Cloudtrail
Monitor security and compliance levels of your AWS operations.
This Content Pack includes:
- Detection Rules
- Workflow Automation
- Dashboard
- AWS Investigator
- Configuration Guide

GCP Audit Logs
Protect your GCP environment by monitoring audit logs.
This Content Pack includes:
- Detection Rules
- Dashboard
- GCP Investigator
- Configuration Guide

Azure Security
Protect your Azure environment by tracking attacker activity.
This Content Pack includes:
- Detection Rules
- Dashboard
- Configuration Guide

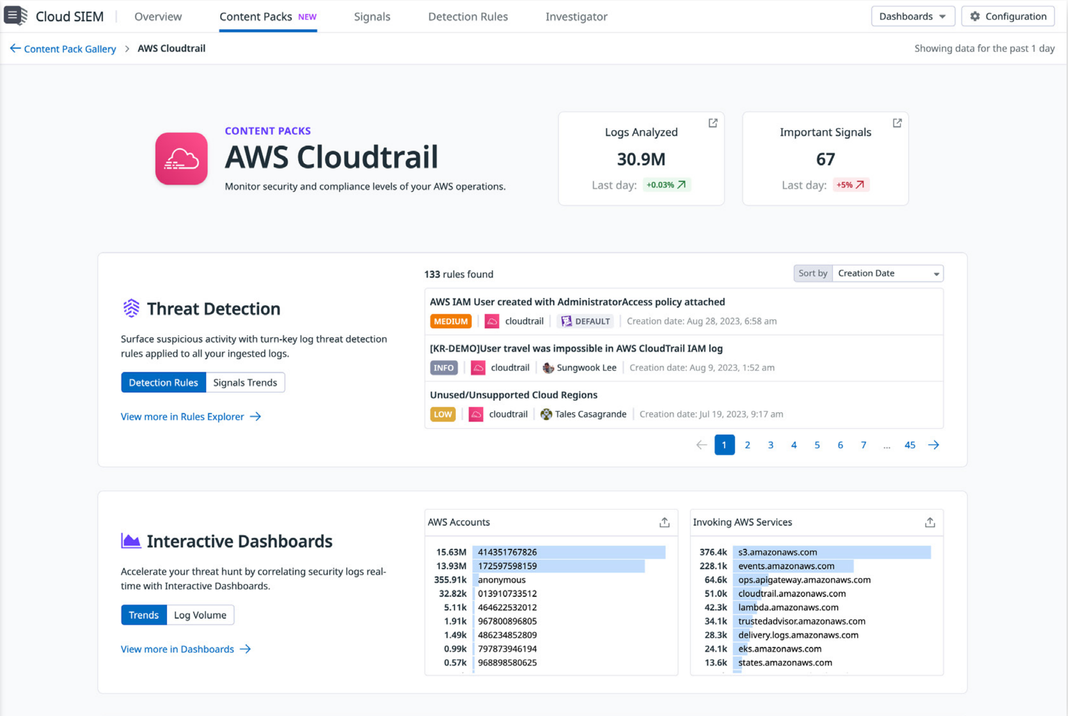
Kubernetes Audit Logs
Gain coverage by monitoring audit logs in your k8s control plane.
This Content Pack includes:
- Detection Rules
- Dashboard

Authentication 2 Content Packs

Okta
Track user activity by monitoring Okta audit logs.
This Content Pack includes:
- Detection Rules
- Workflow Automation
- Dashboard

1Password
Monitor account activity with 1Password Events Reporting.
This Content Pack includes:
- Detection Rules
- Dashboard

Copyright Datadog, Inc. 2023 - 35.22503853 - Master Subscription Agreement - Privacy Policy - Cookie Policy - Datadog Status → ● All Systems Operational



Showing data for the past 1 day

CONTENT PACKS
AWS Cloudtrail
Monitor security and compliance levels of your AWS operations.

Logs Analyzed
30.9M
Last day: +0.03%

Important Signals
67
Last day: +5%

Threat Detection
Surface suspicious activity with turn-key log threat detection rules applied to all your ingested logs.

133 rules found

AWS IAM User created with AdministratorAccess policy attached
MEDIUM | cloudtrail | DEFAULT | Creation date: Aug 28, 2023, 6:58 am

[KR-DEMO]User travel was impossible in AWS CloudTrail IAM log
INFO | cloudtrail | Sungwook Lee | Creation date: Aug 9, 2023, 1:52 am

Unused/Unsupported Cloud Regions
LOW | cloudtrail | Tales Casagrande | Creation date: Jul 19, 2023, 9:17 am

Interactive Dashboards
Accelerate your threat hunt by correlating security logs real-time with Interactive Dashboards.

AWS Accounts

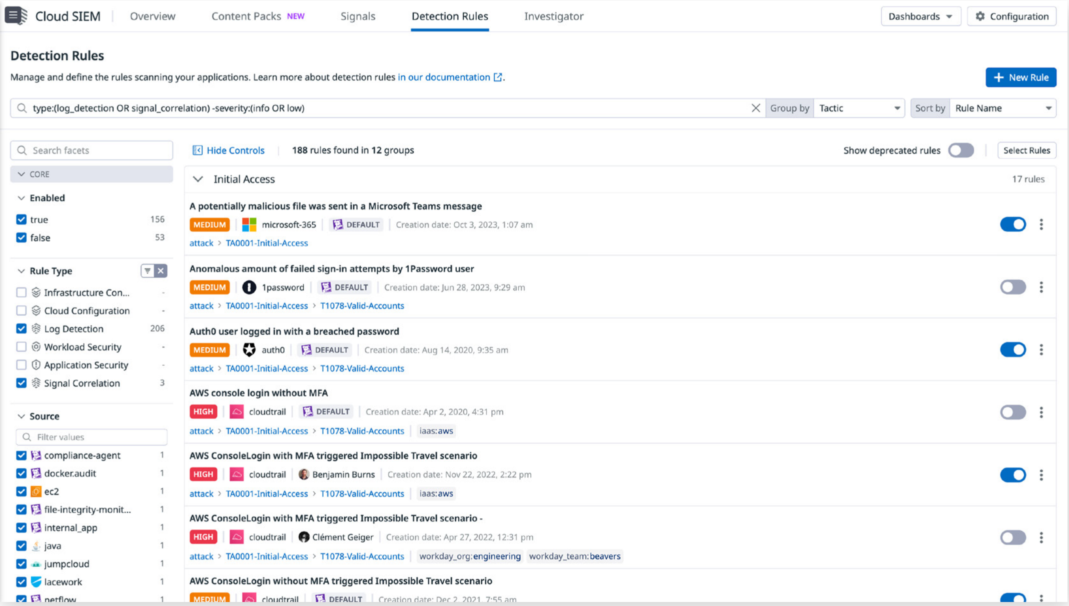
15.63M	414351767826
13.93M	172597598159
355.91k	anonymous
32.82k	013910733512
5.11k	464622532012
1.91k	967800896805
1.49k	486234852809
0.99k	797873946194
0.57k	968898580625

Invoking AWS Services

376.4k	s3.amazonaws.com
228.1k	events.amazonaws.com
64.6k	ops.apigateway.amazonaws.com
51.0k	cloudtrail.amazonaws.com
42.3k	lambda.amazonaws.com
34.1k	trustedadvisor.amazonaws.com
28.3k	delivery.logs.amazonaws.com
24.1k	eks.amazonaws.com
13.6k	states.amazonaws.com

LEVERAGE THREAT DETECTION RULES THAT DON’T REQUIRE A QUERY LANGUAGE

- **Get started quickly with turnkey detection rules.** Datadog Cloud SIEM comes equipped with out-of-the-box threat detection rules for widespread attacker techniques and misconfigurations that are mapped to the MITRE ATT&CK® framework. This means you can improve your security posture in minutes, without any subject matter expertise. Out-of-the-box rules can also be customized to fit your organization’s needs.



Detection Rules

Manage and define the rules scanning your applications. Learn more about detection rules in our documentation.

type:(log_detection OR signal_correlation) -severity:(info OR low)

Group by: Tactic | Sort by: Rule Name

188 rules found in 12 groups

CORE

Enabled

☑ true	156
☑ false	53

Rule Type

□ Infrastructure Con...	-
□ Cloud Configuration	-
☑ Log Detection	206
□ Workload Security	-
□ Application Security	-
☑ Signal Correlation	3

Source

☑ compliance-agent	1
☑ docker.audit	1
☑ ec2	1
☑ file-integrity-monit...	1
☑ internal_app	1
☑ java	1
☑ jumpcloud	1
☑ lacework	1
☑ netflow	1

Initial Access — 17 rules

A potentially malicious file was sent in a Microsoft Teams message
MEDIUM | microsoft-365 | DEFAULT | Creation date: Oct 3, 2023, 1:07 am
attack › TA0001-Initial-Access

Anomalous amount of failed sign-in attempts by 1Password user
MEDIUM | 1password | DEFAULT | Creation date: Jun 28, 2023, 9:29 am
attack › TA0001-Initial-Access › T1078-Valid-Accounts

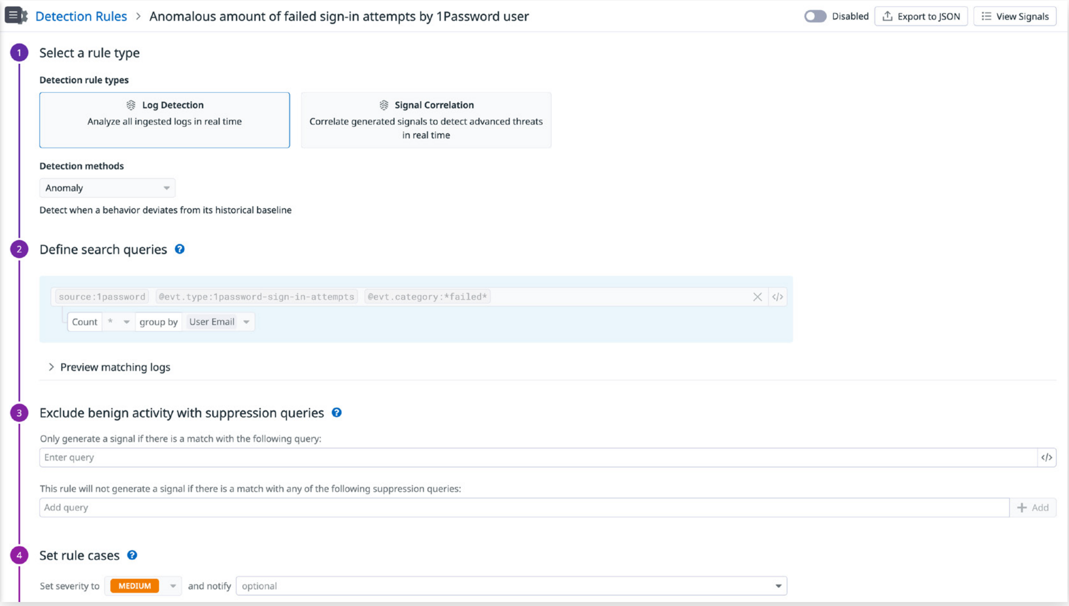
Auth0 user logged in with a breached password
MEDIUM | auth0 | DEFAULT | Creation date: Aug 14, 2020, 9:35 am
attack › TA0001-Initial-Access › T1078-Valid-Accounts

AWS console login without MFA
HIGH | cloudtrail | DEFAULT | Creation date: Apr 2, 2020, 4:31 pm
attack › TA0001-Initial-Access › T1078-Valid-Accounts | iaas:aws

AWS ConsoleLogin with MFA triggered Impossible Travel scenario
HIGH | cloudtrail | Benjamin Burns | Creation date: Nov 22, 2022, 2:22 pm
attack › TA0001-Initial-Access › T1078-Valid-Accounts | iaas:aws

AWS ConsoleLogin with MFA triggered Impossible Travel scenario -
HIGH | cloudtrail | Clément Geiger | Creation date: Apr 27, 2022, 12:31 pm
attack › TA0001-Initial-Access › T1078-Valid-Accounts | workday_org:engineering | workday_team:beavers

AWS ConsoleLogin without MFA triggered Impossible Travel scenario
MEDIUM | cloudtrail | DEFAULT | Creation date: Dec 2, 2021, 7:55 am



Detection Rules › Anomalous amount of failed sign-in attempts by 1Password user

1 Select a rule type

Detection rule types

Log Detection — Analyze all ingested logs in real time

Signal Correlation — Correlate generated signals to detect advanced threats in real time

Detection methods: Anomaly

Detect when a behavior deviates from its historical baseline

2 Define search queries

```
source:1password  @evt.type:1password-sign-in-attempts  @evt.category:*failed*
Count  *  group by  User Email
```

3 Exclude benign activity with suppression queries

Only generate a signal if there is a match with the following query:

Enter query

This rule will not generate a signal if there is a match with any of the following suppression queries:

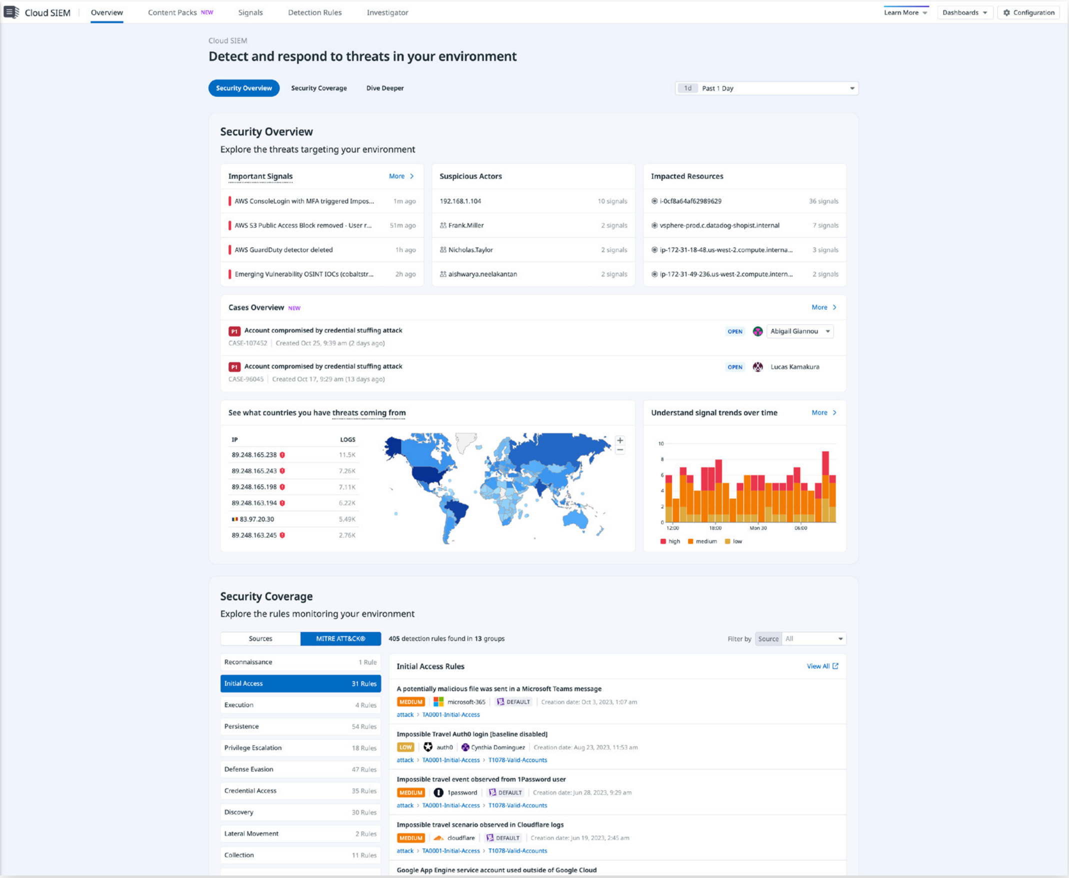
Add query

4 Set rule cases

Set severity to MEDIUM and notify optional

VISUALIZE YOUR SECURITY DATA WITH OUT-OF-THE-BOX DASHBOARDS

- **Get a high-level overview of your security posture.** The Security Overview dashboard allows anyone in your company to review system-wide security signals at a glance.
- **Pivot from a bird’s-eye view to granular details.** The IP Investigation and User Investigation dashboards enable users to correlate specific IP addresses and users with security signals, events, and logs, so they can quickly hone in on malicious activity patterns.



Cloud SIEM

Detect and respond to threats in your environment

Security Overview

Explore the threats targeting your environment

Important Signals	More
AWS ConsoleLogin with MFA triggered Impos...	1m ago
AWS S3 Public Access Block removed - User r...	51m ago
AWS GuardDuty detector deleted	1h ago
Emerging Vulnerability OSINT IOCs (cobaltstr...	2h ago

Suspicious Actors	
192.168.1.104	10 signals
Frank.Miller	2 signals
Nicholas.Taylor	2 signals
aishwarya.neelakantan	2 signals

Impacted Resources	
i-0cf8a64af62989629	36 signals
vsphere-prod.c.datadog-shopist.internal	7 signals
ip-172-31-18-48.us-west-2.compute.interna...	3 signals
ip-172-31-49-236.us-west-2.compute.intern...	2 signals

Cases Overview NEW — More

P1 Account compromised by credential stuffing attack — OPEN — Abigail Giannou
CASE-107452 | Created Oct 25, 9:39 am (2 days ago)

P1 Account compromised by credential stuffing attack — OPEN — Lucas Kamakura
CASE-96045 | Created Oct 17, 9:29 am (13 days ago)

See what countries you have threats coming from

IP	LOGS
89.248.165.238	11.5K
89.248.165.243	7.26K
89.248.165.198	7.11K
89.248.163.194	6.22K
83.97.20.30	5.49K
89.248.163.245	2.76K

Understand signal trends over time — More

Security Coverage

Explore the rules monitoring your environment

405 detection rules found in 13 groups — Filter by Source All

Reconnaissance	1 Rule
Initial Access	31 Rules
Execution	4 Rules
Persistence	54 Rules
Privilege Escalation	18 Rules
Defense Evasion	47 Rules
Credential Access	35 Rules
Discovery	30 Rules
Lateral Movement	2 Rules
Collection	11 Rules

Initial Access Rules — View All

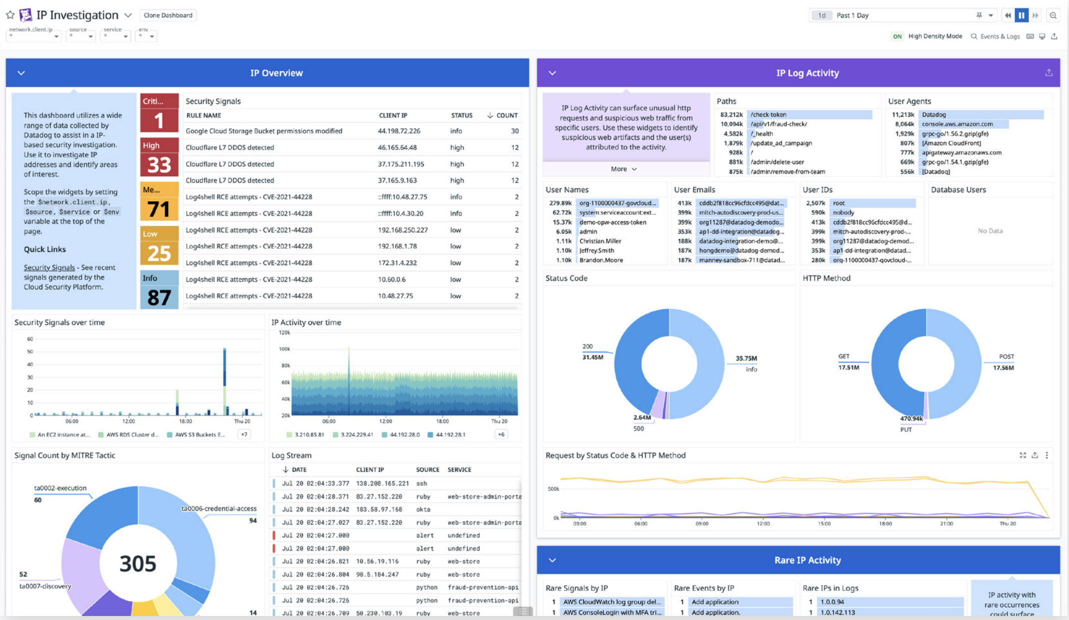
A potentially malicious file was sent in a Microsoft Teams message
MEDIUM | microsoft-365 | DEFAULT | Creation date: Oct 3, 2023, 1:07 am
attack › TA0001-Initial-Access

Impossible Travel Auth0 login [baseline disabled]
LOW | auth0 | Cynthia Dominguez | Creation date: Aug 23, 2023, 11:53 am
attack › TA0001-Initial-Access › T1078-Valid-Accounts

Impossible travel event observed from 1Password user
MEDIUM | 1password | DEFAULT | Creation date: Jun 28, 2023, 9:29 am
attack › TA0001-Initial-Access › T1078-Valid-Accounts

Impossible travel scenario observed in Cloudflare logs
MEDIUM | cloudflare | DEFAULT | Creation date: Jun 19, 2023, 2:45 am
attack › TA0001-Initial-Access › T1078-Valid-Accounts

Google App Engine service account used outside of Google Cloud



IP Overview

This dashboard utilizes a wide range of data collected by Datadog to assist in a IP-based security investigation. Use it to investigate IP addresses and identify areas of interest.

Scope the widgets by setting the `$network.client.ip`, `$source`, `$service` or `$env` variable at the top of the page.

Quick Links

Security Signals - See recent signals generated by the Cloud Security Platform.

Criti...	1
High	33
Me...	71
Low	25
Info	87

Security Signals

RULE NAME	CLIENT IP	STATUS	COUNT
Google Cloud Storage Bucket permissions modified	44.198.72.226	info	30
Cloudflare L7 DDOS detected	46.165.64.48	high	12
Cloudflare L7 DDOS detected	37.175.211.195	high	12
Cloudflare L7 DDOS detected	37.165.9.163	high	12
Log4shell RCE attempts - CVE-2021-44228	::ffff:10.48.27.75	info	2
Log4shell RCE attempts - CVE-2021-44228	::ffff:10.4.30.20	info	2
Log4shell RCE attempts - CVE-2021-44228	192.168.250.227	low	2
Log4shell RCE attempts - CVE-2021-44228	192.168.1.78	low	2
Log4shell RCE attempts - CVE-2021-44228	172.31.4.232	low	2
Log4shell RCE attempts - CVE-2021-44228	10.60.0.6	low	2
Log4shell RCE attempts - CVE-2021-44228	10.48.27.75	low	2

Security Signals over time

IP Activity over time

Signal Count by MITRE Tactic

Log Stream

```
DATE                    CLIENT IP        SOURCE   SERVICE
Jul 20 02:04:33.377     138.208.165.221  ssh
Jul 20 02:04:28.371     83.27.152.220    ruby     web-store-admin-porta
Jul 20 02:04:28.242     183.58.97.168    okta
Jul 20 02:04:27.027     83.27.152.220    ruby     web-store-admin-porta
Jul 20 02:04:27.000                      alert    undefined
Jul 20 02:04:27.000                      alert    undefined
Jul 20 02:04:26.821     10.56.19.116     ruby     web-store
Jul 20 02:04:26.804     98.5.184.247     ruby     web-store
Jul 20 02:04:26.726                      python   fraud-prevention-api
Jul 20 02:04:26.726                      python   fraud-prevention-api
Jul 20 02:04:26.709     50.230.103.19    ruby     web-store
```

IP Log Activity

IP Log Activity can surface unusual http requests and suspicious web traffic from specific users. Use these widgets to identify suspicious web artifacts and the user(s) attributed to the activity.

Paths	
83,212k	/check-token
10,094k	/api/v1/fraud-check/
4,582k	/_health
1,879k	/update_ad_campaign
928k	/
881k	/admin/delete-user
875k	/admin/remove-from-team

User Agents	
11,213k	Datadog
8,064k	console.aws.amazon.com
1,929k	grpc-go/1.56.2,gzip(gfe)
807k	[Amazon CloudFront]
777k	apigateway.amazonaws.com
669k	grpc-go/1.54.1,gzip(gfe)
556k	[Datadog]

User Names	
279.89k	org-1100000437-govcloud...
62.72k	system:serviceaccount:ext...
15.37k	demo-opw-access-token
6.05k	admin
1.11k	Christian.Miller
1.10k	Jeffrey.Smith
1.10k	Brandon.Moore

User Emails	
413k	cddb2f818cc96cfdcc495@dat...
399k	mitch-autodiscovery-prod-us...
399k	org11287@datadog-demodo...
353k	ap1-dd-integration@datadog...
188k	datadog-integration-demo@...
187k	hongdemo@datadog-demod...
187k	manney-sandbox-711@datad...

User IDs	
2,507k	root
590k	nobody
413k	cddb2f818cc96cfdcc495@d...
399k	mitch-autodiscovery-prod-...
399k	org11287@datadog-demod...
353k	ap1-dd-integration@datad...
280k	org-1100000437-govcloud-...

Database Users

No Data

Status Code

HTTP Method

Request by Status Code & HTTP Method

Rare IP Activity

Rare Signals by IP	
1	AWS CloudWatch log group del...
1	AWS ConsoleLogin with MFA tri...

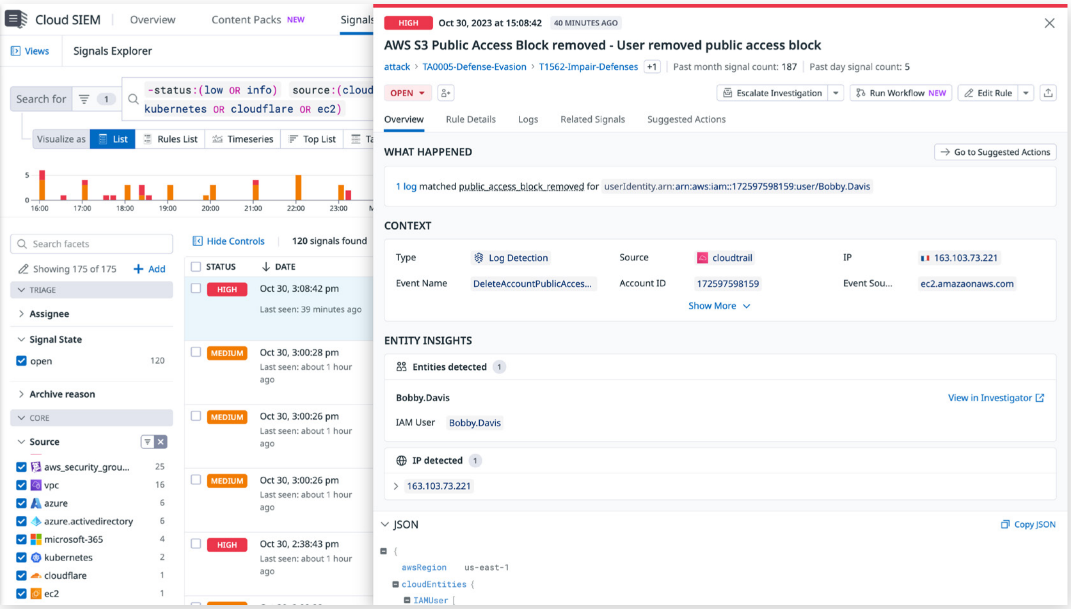
Rare Events by IP	
1	Add application
1	Add application.

Rare IPs in Logs	
1	1.0.0.94
1	1.0.142.113

IP activity with rare occurrences could surface

EXPLORE YOUR SECURITY SIGNALS

- **Access insights that help you correlate and triage security signals.** The Signals Explorer in Datadog Cloud SIEM enables you to easily configure and filter your security signals with facets such as “source” and “status.” Investigate signals further by viewing rich details and context on severity, origination, and more. Modify status or rule settings for specific signals, and share or assign them to teammates to collaborate on investigations.



```
-status:(low OR info) source:(cloud
kubernetes OR cloudflare OR ec2)
```

120 signals found

Signal State	
☑ open	120

Source	
☑ aws_security_grou...	25
☑ vpc	16
☑ azure	6
☑ azure.activedirectory	6
☑ microsoft-365	4
☑ kubernetes	2
☑ cloudflare	1
☑ ec2	1

STATUS	DATE
□ HIGH	Oct 30, 3:08:42 pm Last seen: 39 minutes ago
□ MEDIUM	Oct 30, 3:00:28 pm Last seen: about 1 hour ago
□ MEDIUM	Oct 30, 3:00:26 pm Last seen: about 1 hour ago
□ MEDIUM	Oct 30, 3:00:26 pm Last seen: about 1 hour ago
□ HIGH	Oct 30, 2:38:43 pm Last seen: about 1 hour ago

HIGH Oct 30, 2023 at 15:08:42 40 MINUTES AGO

AWS S3 Public Access Block removed - User removed public access block

attack › TA0005-Defense-Evasion › T1562-Impair-Defenses +1 | Past month signal count: 187 | Past day signal count: 5

OPEN

WHAT HAPPENED

1 log matched public_access_block_removed for userIdentity.arn:arn:aws:iam::172597598159:user/Bobby.Davis

CONTEXT

Type	Log Detection	Source	cloudtrail	IP	163.103.73.221
Event Name	DeleteAccountPublicAcces...	Account ID	172597598159	Event Sou...	ec2.amazaonaws.com

ENTITY INSIGHTS

Entities detected 1

Bobby.Davis

IAM User Bobby.Davis

IP detected 1

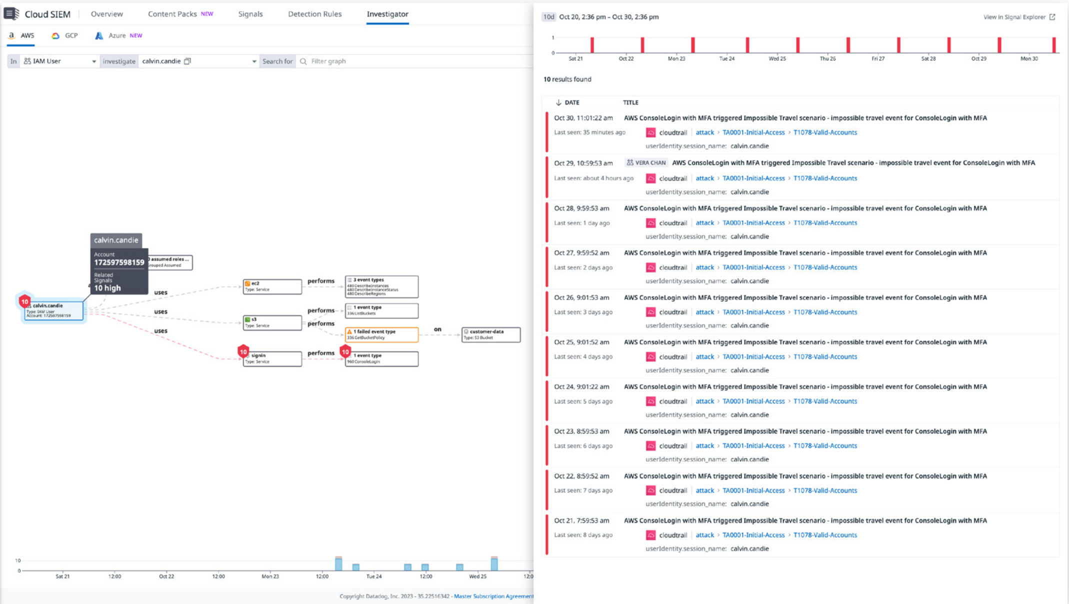
163.103.73.221

JSON

```
{
  awsRegion   us-east-1
  cloudEntities {
    IAMUser {
```

COST EFFECTIVELY RETAIN DATA FOR INVESTIGATIONS

- **Visually investigate and search across 15 months of log data at a low cost.** With Datadog Cloud SIEM, you can cost-effectively visualize a history of logs from up to 15 months in the past to understand the course of malicious activity and the impact of security breaches to build context for investigations. Use filters to focus on only the most relevant user or account activity during investigations, see which services attackers interacted with, and better understand attackers’ methods.



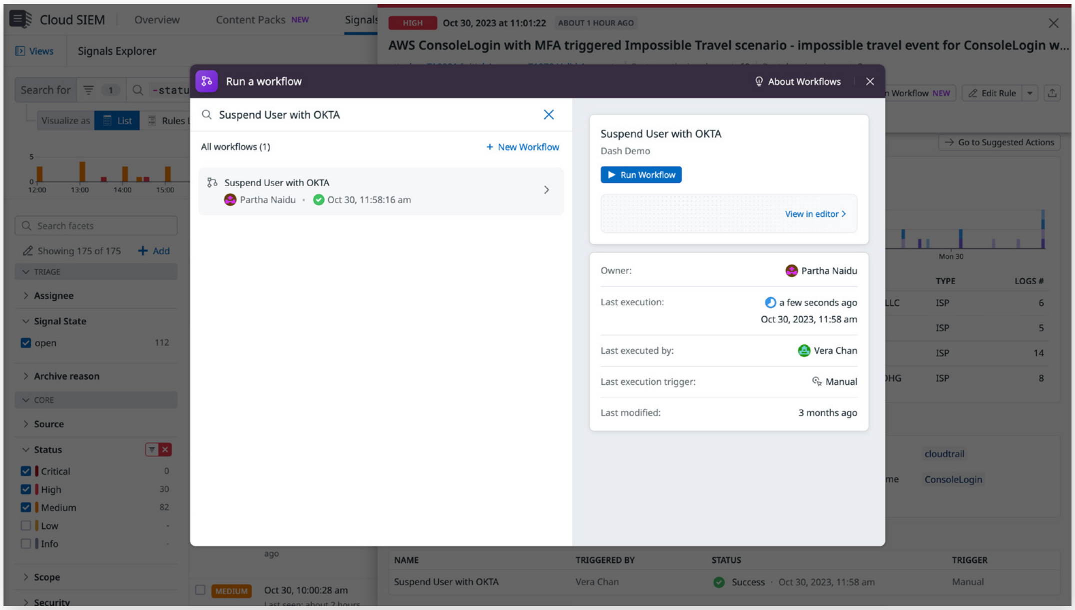
10d Oct 20, 2:36 pm – Oct 30, 2:36 pm

10 results found

DATE	TITLE
Oct 30, 11:01:22 am Last seen: 35 minutes ago	AWS ConsoleLogin with MFA triggered Impossible Travel scenario - impossible travel event for ConsoleLogin with MFA cloudtrail | attack › TA0001-Initial-Access › T1078-Valid-Accounts userIdentity.session_name: calvin.candie
Oct 29, 10:59:53 am Last seen: about 4 hours ago	VERA CHAN AWS ConsoleLogin with MFA triggered Impossible Travel scenario - impossible travel event for ConsoleLogin with MFA cloudtrail | attack › TA0001-Initial-Access › T1078-Valid-Accounts userIdentity.session_name: calvin.candie
Oct 28, 9:59:53 am Last seen: 1 day ago	AWS ConsoleLogin with MFA triggered Impossible Travel scenario - impossible travel event for ConsoleLogin with MFA cloudtrail | attack › TA0001-Initial-Access › T1078-Valid-Accounts userIdentity.session_name: calvin.candie
Oct 27, 9:59:52 am Last seen: 2 days ago	AWS ConsoleLogin with MFA triggered Impossible Travel scenario - impossible travel event for ConsoleLogin with MFA cloudtrail | attack › TA0001-Initial-Access › T1078-Valid-Accounts userIdentity.session_name: calvin.candie
Oct 26, 9:01:53 am Last seen: 3 days ago	AWS ConsoleLogin with MFA triggered Impossible Travel scenario - impossible travel event for ConsoleLogin with MFA cloudtrail | attack › TA0001-Initial-Access › T1078-Valid-Accounts userIdentity.session_name: calvin.candie
Oct 25, 9:01:52 am Last seen: 4 days ago	AWS ConsoleLogin with MFA triggered Impossible Travel scenario - impossible travel event for ConsoleLogin with MFA cloudtrail | attack › TA0001-Initial-Access › T1078-Valid-Accounts userIdentity.session_name: calvin.candie
Oct 24, 9:01:22 am Last seen: 5 days ago	AWS ConsoleLogin with MFA triggered Impossible Travel scenario - impossible travel event for ConsoleLogin with MFA cloudtrail | attack › TA0001-Initial-Access › T1078-Valid-Accounts userIdentity.session_name: calvin.candie
Oct 23, 8:59:53 am Last seen: 6 days ago	AWS ConsoleLogin with MFA triggered Impossible Travel scenario - impossible travel event for ConsoleLogin with MFA cloudtrail | attack › TA0001-Initial-Access › T1078-Valid-Accounts userIdentity.session_name: calvin.candie
Oct 22, 8:59:52 am Last seen: 7 days ago	AWS ConsoleLogin with MFA triggered Impossible Travel scenario - impossible travel event for ConsoleLogin with MFA cloudtrail | attack › TA0001-Initial-Access › T1078-Valid-Accounts userIdentity.session_name: calvin.candie
Oct 21, 7:59:53 am Last seen: 8 days ago	AWS ConsoleLogin with MFA triggered Impossible Travel scenario - impossible travel event for ConsoleLogin with MFA cloudtrail | attack › TA0001-Initial-Access › T1078-Valid-Accounts userIdentity.session_name: calvin.candie

AUTOMATE SECURITY RESPONSE WITH SECURITY WORKFLOW BLUEPRINTS AND CASE MANAGEMENT

- **Keep up with threats.** Datadog Workflow Automation and Case Management help you reduce the burden on security engineers. Use workflow blueprints to automate security signal triage, perform retro-hunts, create detection rules for emerging vulnerabilities, automatically block a suspicious IP address with Cloudflare, or suspend suspicious Okta users while you automatically open cases for collaborative investigation. String together any of 500+ workflow actions to create custom workflows that can execute with just a single click.



HIGH Oct 30, 2023 at 11:01:22 ABOUT 1 HOUR AGO

AWS ConsoleLogin with MFA triggered Impossible Travel scenario - impossible travel event for ConsoleLogin w...

Run a workflow

Suspend User with OKTA

All workflows (1)

Suspend User with OKTA
Partha Naidu • Oct 30, 11:58:16 am

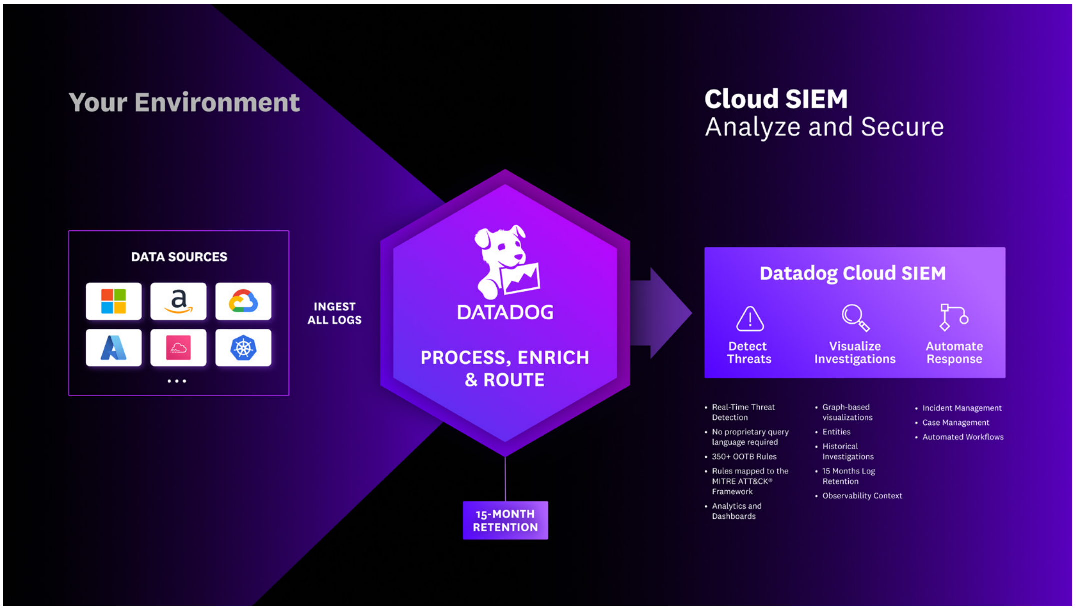
Suspend User with OKTA
Dash Demo

Owner:	Partha Naidu
Last execution:	a few seconds ago Oct 30, 2023, 11:58 am
Last executed by:	Vera Chan
Last execution trigger:	Manual
Last modified:	3 months ago

NAME	TRIGGERED BY	STATUS	TRIGGER
Suspend User with OKTA	Vera Chan	Success · Oct 30, 2023, 11:58 am	Manual

JUMPSTART YOUR INVESTIGATIONS WITH MORE THAN 650 VENDOR-BACKED INTEGRATIONS

- **Collaborate easily during investigations.** Datadog integrates with Slack and PagerDuty, enabling you to automatically loop in relevant teams when a high-severity rule detects a threat. You can also export security signals to collaboration tools like JIRA or ServiceNow.
- **Security integrations provide additional context.** Built-in security integrations with cloud audit, authentication, collaboration, and network data sources—such as AWS CloudTrail, Azure, Google Cloud, Kubernetes, Okta, 1Password, Cloudflare, Office 365, Google Workspace, and more—enable users to ingest additional security data in minutes, providing deeper context and accelerating investigations.



- Real-Time Threat Detection
- No proprietary query language required
- 350+ OOTB Rules
- Rules mapped to the MITRE ATT&CK® Framework
- Analytics and Dashboards

- Graph-based visualizations
- Entities
- Historical Investigations
- 15 Months Log Retention
- Observability Context

- Incident Management
- Case Management
- Automated Workflows

Security for dynamic environments

Security threats in cloud-native environments move fast, which means that security, development, and operations teams all need visibility into their infrastructure, network, and applications. Datadog Cloud SIEM is a SaaS solution that provides end-to-end security coverage of dynamic, distributed systems. It enables real-time threat detection across the entire stack, as well as deeper collaboration between teams.

MITRE | ATT&CK®

Security teams use Datadog Cloud SIEM daily

"It's like a Swiss Army Knife for security and observability with so many features available out of the box, which translates to fast time to value. The rules are intuitive and easy to understand, and it's easy to onboard new team members. The investigator accelerates triage and investigations, and the SOAR-like workflows help automate response."

1Password

Melanie Masterson
GCWIN, Information Security Engineering Manager, 1Password

"The onboarding process with Datadog was a breeze as we were already using their other products. We were up and running in a few days time. We were able to ingest all of our initial set of data sources in a matter of weeks. We reduced the number of account takeover (ATO) attacks to save millions for the company."

POSHMARK

Kapileshwar Punna
Security Operations Manager, Poshmark

"Datadog is by far the easiest and most integrated platform to get all of our disparate data into one spot. Datadog reduces the mean time to respond from hours down to minutes!"

INDIGOV

Constantine Macris
CISO, Indigov

DATADOG