

Uptycs - PagerDuty Integration Documentation

Uptycs Overview

Uptycs platform provides Security Analytics for the Modern Defender

Uptycs + PagerDuty helps teams solve incident response from detection to alert to action. The powerful detections and events framework from Uptycs gives teams deep visibility into their IT ecosystem. With PagerDuty, critical alerts from the Uptycs platform are getting into the right hands faster, helping expedite response and resolution times across endpoint, cloud, and container assets.

- Detect and Investigate Attacks: Uptycs extends beyond endpoints to cover managed container services environments and the cloud infrastructure — tying together attack activity as it crosses on-premises and cloud boundaries.
- Cloud Workload Protection Platform (CWPP): Complete security observability for your cloud workloads and collects and analyzes real-time workload activity in detail.
- Cloud Security Posture Management (CSPM): Use connected insights from across your cloud accounts to prioritize misconfigurations and vulnerabilities for remediation.
- Cloud Infrastructure and Entitlements Management (CIEM): Highlight risky policies and overly permissive configurations, and receive alerts for potential account misuse.
- eXtended Detection and Response (XDR): Correlated telemetry from productivity endpoints, server workloads, and other sources provide extended detection and response.

PagerDuty Integration Documentation Steps

Create a Service in PagerDuty

This agent supports sending events to “Generic API” services and a Generic API service can be created as follows:

1. Go to Services > Service Directory and click New Service

Service Directory

A service in PagerDuty represents a component, microservice or piece of infrastructure a team operates, manages, and monitors. Usually it's something you'd go on call for. [Learn more about the service directory.](#)

[+ New Service](#)

[Services](#) Maintenance Windows



Create your first service

To receive incidents and alerts, set up a service to represent the piece of infrastructure you're monitoring. You'll need an [escalation policy](#) before you begin to specify who will be going on call.

[+ New Service](#)

2. On the next screen, Enter a Name and Description based on the function that the service provides and click Next to continue

Create a Service

1 Name — **2 Assign** — **3 Reduce Noise** — **4 Integrations**

Name and Description

A technical service reflects a discrete piece of functionality that is wholly owned by one team. One or more technical services combine to deliver customer-facing or business capabilities.

Example names of technical services

- Payment Processing
- Checkout App Server
- Inventory Database
- Create Account
- Account Authentication
- Search - Suggest

Name*

Give your service a name

Tip: Avoid using PagerDuty or Alerts in the service name as this will appear in the notification

Description

Write a brief description for this service so that other users in your account will know what it is used for.

[Next](#)

[Cancel](#)

3. Assign an escalation policy either by “Generate a New Escalation Policy” or “Select an Existing Escalation Policy.” Click Next to continue

Create a Service

✓ Name ——— 2 Assign ——— 3 Reduce Noise ——— 4 Integrations

Assign an Escalation Policy

Generate or assign an Escalation Policy to this service. Escalation Policies connect services to individual users and/or schedules and they ensure the right people are notified at the right time.

☒ **Generate a new Escalation Policy**

Create a new Escalation Policy for this service where you will be the default on-call. The Escalation Policy can be updated at any time after you create the service.

☐ **Select an existing Escalation Policy**

Select an escalation policy

4. If you generate a new escalation policy, you will be placed as the first-level on-call for the service. You can edit the policy at any time after the service is created.
5. On the next screen, Reduce Noise: select Alert Grouping based on below options:
 - a. Intelligent: Group alerts based on alert content and past groups.
 - b. Content-Based: Group alerts when contents of specified alert fields match by clicking on Create Grouping and select your alert grouping criteria. You may choose to group alerts based on Any or All of the following fields, then select your preferred Field Name
 - c. Time-Based: Group alerts for a selected duration and select duration from dropdown
 - d. Turn Off Alert Grouping: Select this option if you would not like to use alert grouping.

Create a Service

✓ Name ——— ✓ Assign ——— 3 Reduce Noise ——— 4 Integrations

Reduce Noise

Alert Grouping

Combine similar alerts into a single incident to reduce notification noise and provide more context when responding to incidents.

☒ **Intelligent** Recommended
Intelligently based on alert content and past groups.

☐ **Content-Based**
When contents of specified alert fields match.

Create Grouping

☐ **Time-Based**
For a selected duration.

2 minutes ▼

☐ **Turn Off Alert Grouping**

6. Transient Alerts: Pause incident creation and notification for alerts that are transient. Alerts that typically auto-resolve through integrations within minutes will be suspended for the selected duration.

Transient Alerts

Pause incident creation and notification for alerts that are transient. Alerts that typically auto-resolve through integrations within minutes will be suspended for the selected duration.

☒ **Auto-pause incident notifications** Recommended

5 minutes ▼

Automatically detect transient alerts and pause notification

☐ **Do not auto-pause incident notifications**

- Click on Next. Search for “Uptycs,” in Add Integrations, click the check box for the Integration and click on Create Service

PagerDuty

Incidents Services People Automation Analytics Integrations Status

Search

SERVICE DIRECTORY > ACME.COM SECURITY SERVICE > ADD INTEGRATIONS

Add Integrations

Integrations

Alert feeds can come into PagerDuty from a number of sources. We apply our AI to these alerts and can trigger incidents and notify the right people at the right time.

Select the integration(s) you use to send alerts to this service

Uptycs X

Your selections (1)

☒ Uptycs

Most popular integrations

<input type="checkbox"/> Events API V2	<input type="checkbox"/> Prometheus	<input type="checkbox"/> Amazon CloudWatch	<input type="checkbox"/> Splunk	<input type="checkbox"/> Nagios
<input type="checkbox"/> Zabbix	<input type="checkbox"/> Datadog	<input type="checkbox"/> SolarWinds Orion	<input type="checkbox"/> New Relic	<input type="checkbox"/> System Center Operations Manager
<input type="checkbox"/> Microsoft Azure	<input type="checkbox"/> AlertSite UXM	<input type="checkbox"/> Pingdom	<input type="checkbox"/> SignalFx	<input type="checkbox"/> Email

Add Cancel

© 2009–2022 PagerDuty, Inc. All rights reserved. Patents issued and pending.

- Once the Service is created, go to the Integrations page and you will see the Integration name, Integration key and Integration key and Integration URL which is required when you send events to PagerDuty. The Integration Key and URL is hidden for security reasons, you will see the full Key and URL in your environment.

Activity
Integrations
Settings
Service Dependencies

Integrations (1)

Follow the steps below to integrate and test each integration, or [add an integration](#).

Uptycs

Integration Documentation

Integration Name

Integration Key

Integration URL

Working Example

1. In your Uptycs Platform, Create or select an Event Rule and Alert rule under configurations and generate an alert

Alert Rules
Search
Bryan Sadowski

Configurations / Alert Rules
CREATE

Advanced Filters

1 FILTERED
ANY
ALL
CLEAR FILTERS

Resource
Operating System
Public Cloud
Standards and Frameworks

Cloud
Endpoint
Container
Kubernetes
MacOS
Linux
Windows
AWS
GCP
Azure
ATTACK
CIS
FedRAMP
SOC2

MITRE Tactic
Cloud Services

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact
ACM
API_GATEWAY
CLOUDFORMATION
CLOUDFRONT
CLOUDTRAIL
CLOUDWATCH
CODECOMMIT
CODEDEPLOY
CODEPIPELINE
CODEBUILD
CONFIG
DIRECTORY
EBS
EC2
ECR
ECS
EFS
EKS
ELASTICACHE
ELB
GLACIER
GUARDDUTY
IAM
KINESIS
KMS

0 selected

<input type="checkbox"/>	Name ↑	Code	Grouping	Tags	Status	Updated By	Last Updated (G...	Actions
<input type="checkbox"/>	User can expose credentials	AWS_THREAT_INL_ACC_1	ATTACK	ATTN... AWS +5		System User	07/06/2022 04:32:10	

2. Go to Alert rule and click on Send Notifications



Enabled

VIEW EVENTRULE

DISABLE

Name
User can expose credentialsCode
AWS_THREAT_INI_ACC_1Framework
ATTACKCategory 1
Initial AccessCategory 2
T1078Description
User has permissions which can expose the access credentials.Created By
ramakrishnaCreated At
05/06/2022 17:23:39Alert tags
ATTACK AWS Cloud IAM Initial Access T1078 THREAT

Type a value and press [Enter]

Type
BuilderRule
1 Auto create alert rule for User can expose credentials

Click + to add destination

Send notifications to

Type	Name	Details	Notify Every Alert	Close After Delivery	Actions
	Demo	Webhook URL: https://hooks.slack.com/services/T1PASAU59/B02D... Token:	Yes	No	

+

3. Select the Destination type as PagerDuty in the dropdown menu. Then provide a Name for the destination and paste in your PagerDuty Integration Key that you copied from the earlier steps above into the Service Key field.

Add alert notification

Select an existing destination to add

☐ Notify on Every Alert☐ Close After Delivery

Search destinations

- KubeQuery
https://hooks.slack.com/services/T01LH9UQ23T/B02CWCJIKFB/ByILMYbxXjQU4tjge66gdAh
- Splunk
https://inputs.pr-d-pw18w.splunkcloud.com:8088/services/collector/raw
- Splunk_one
https://inputs.pr-d-pw18w.splunkcloud.com:8088/services/collector/raw
- Test
https://f369-108-7-206-64.ngrok.io
- Test 1212
http://test1.com
- Uptycs Admin
gdaya@uptycs.com

Create and add new destination

Destination Type
pagerduty

Please select destination type

Name

Name is required.

Service Key

SAVE


CANCEL

4. Click on Notify on Every Alert and Close After Delivery. Then click Save.
5. Generate an alert and go to PagerDuty > Incidents > All Incidents and check if your alert has been triggered.

SERVICE DIRECTORY > MONITOR ALERTS - UPTYCS > ACTIVITY

Monitor alerts - Uptycs Edit

[+ New Incident](#) [More ▾](#)

STATUS  Awaiting response

ON CALL NOW Sowjanya Yenduri

ESCALATION POLICY sowjanya-ep

TEAM No team is assigned to the sowjanya-ep escalation policy.

COMMUNICATION CHANNEL Edit
No channel for this service. [Add one.](#)

[Activity](#) [Integrations](#) [Settings](#) [Service Dependencies](#)

Open Incidents (1)

[! Acknowledge](#) [✓ Resolve](#) [⌚ Snooze ▾](#) [Merge Incidents](#) [Go to incident #](#)

<input type="checkbox"/>	Status	Priority ▾	Urgency	Alerts	Title	Assigned To	Created ▾
<input type="checkbox"/>	Triggered		High	26	Uptycs Alert: #2 <small>+ SHOW DETAILS (26 triggered alerts)</small>	Sowjanya Yenduri	Today at 11:48 AM

Note: Service Name here is “Monitor alerts - Uptycs”

Useful Links

<https://support.pagerduty.com/docs/services-and-integrations>

Please contact support@uptycs.com if you need assistance.