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.

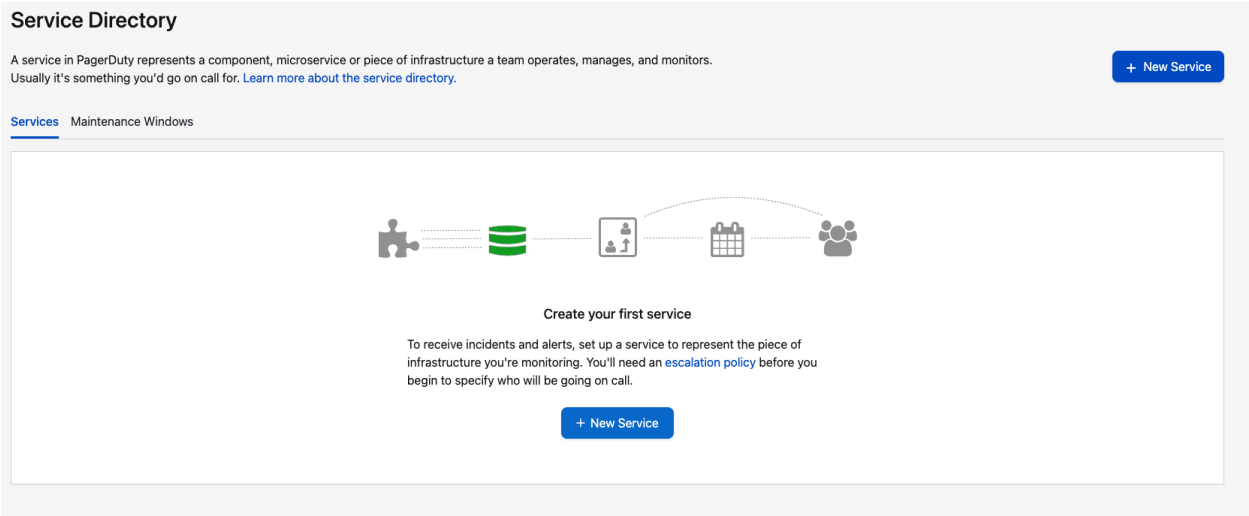
- Detect and Investigate Attacks: Uptycs extends beyond endpoints to cover managed container services environments and the cloud infrastructure — tying together attack activity as it crosses on-premises and cloud boundaries.
- Cloud Workload Protection Platform (CWPP): Complete security observability 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

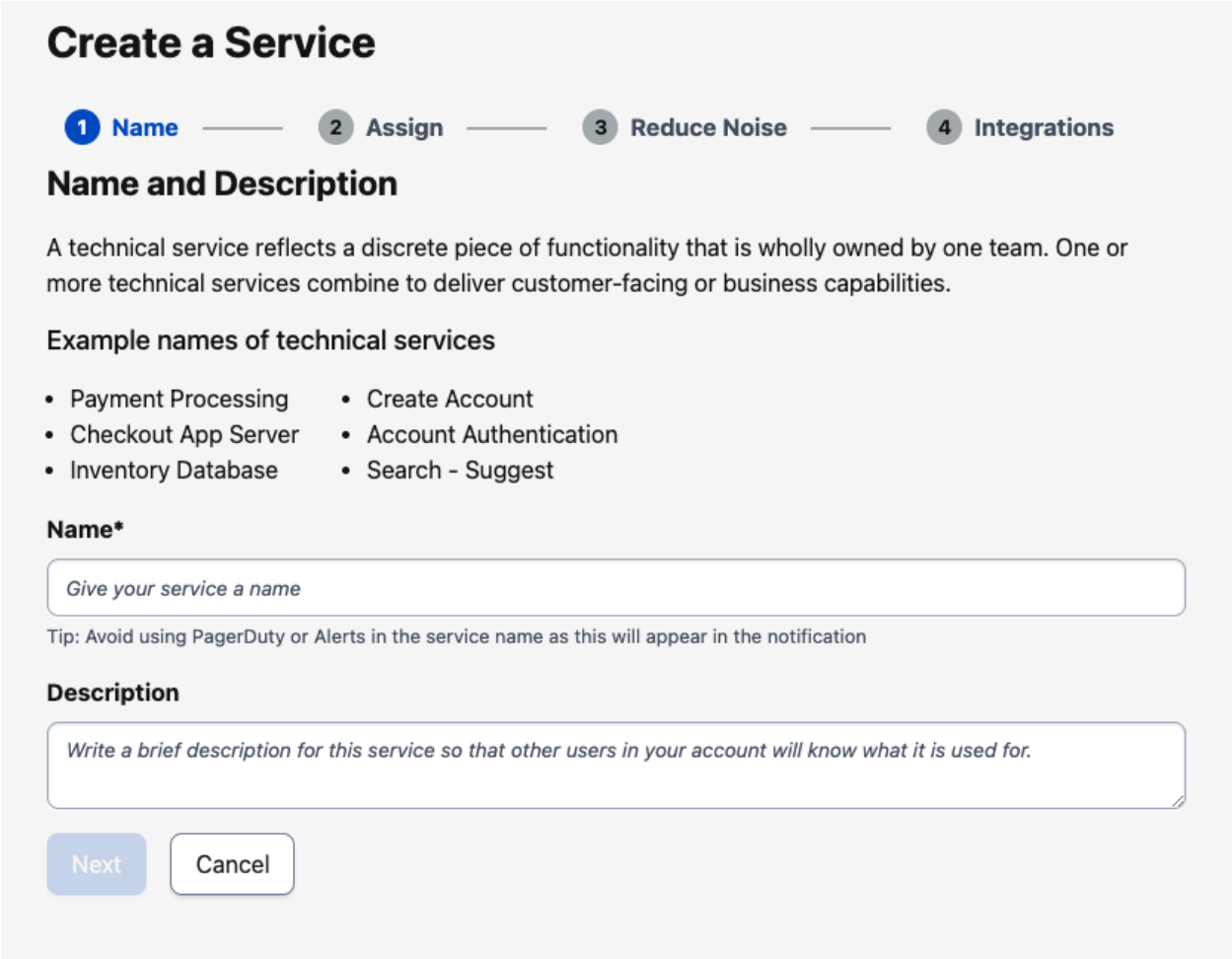
Create a Service in PagerDuty

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

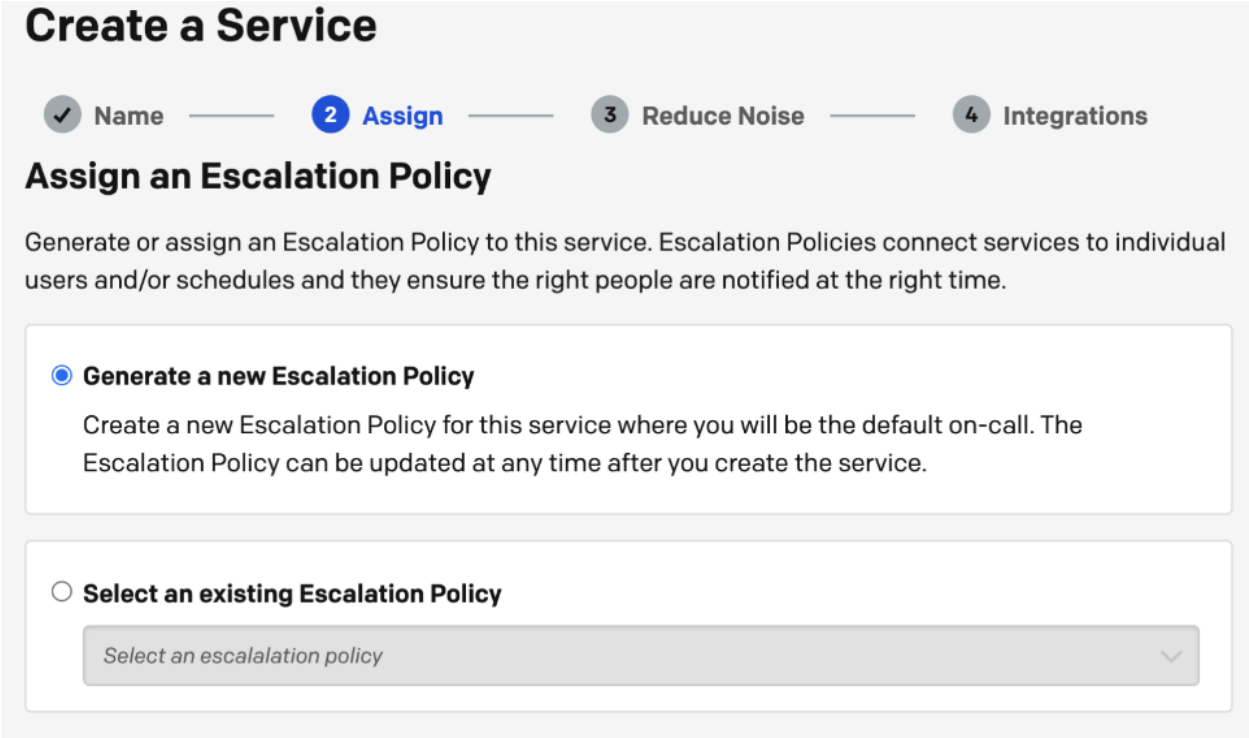
1. Go to Services > Service Directory and click New Service



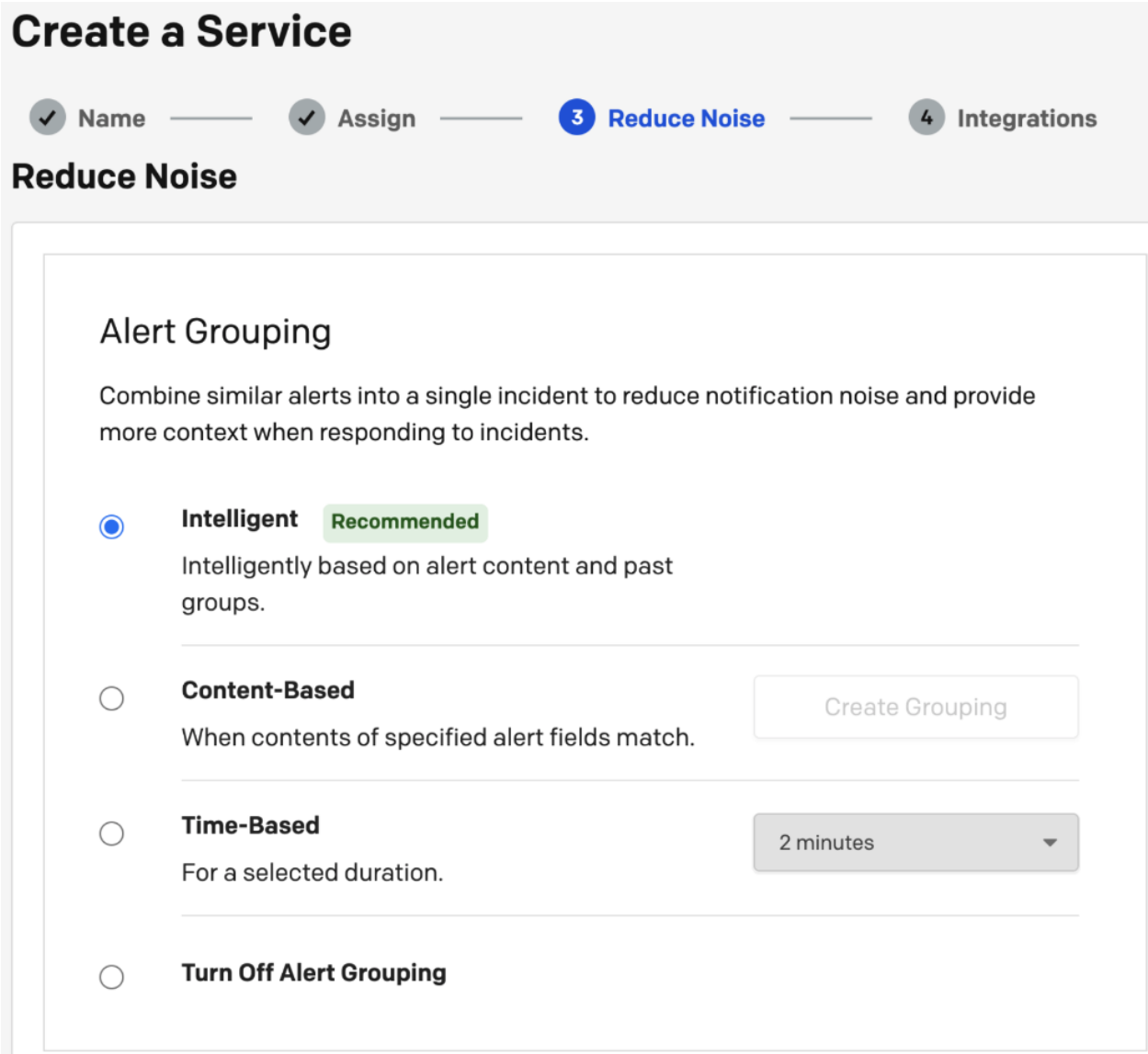
2. On the next screen, Enter a Name and Description based on the function that the service provides and click Next to continue



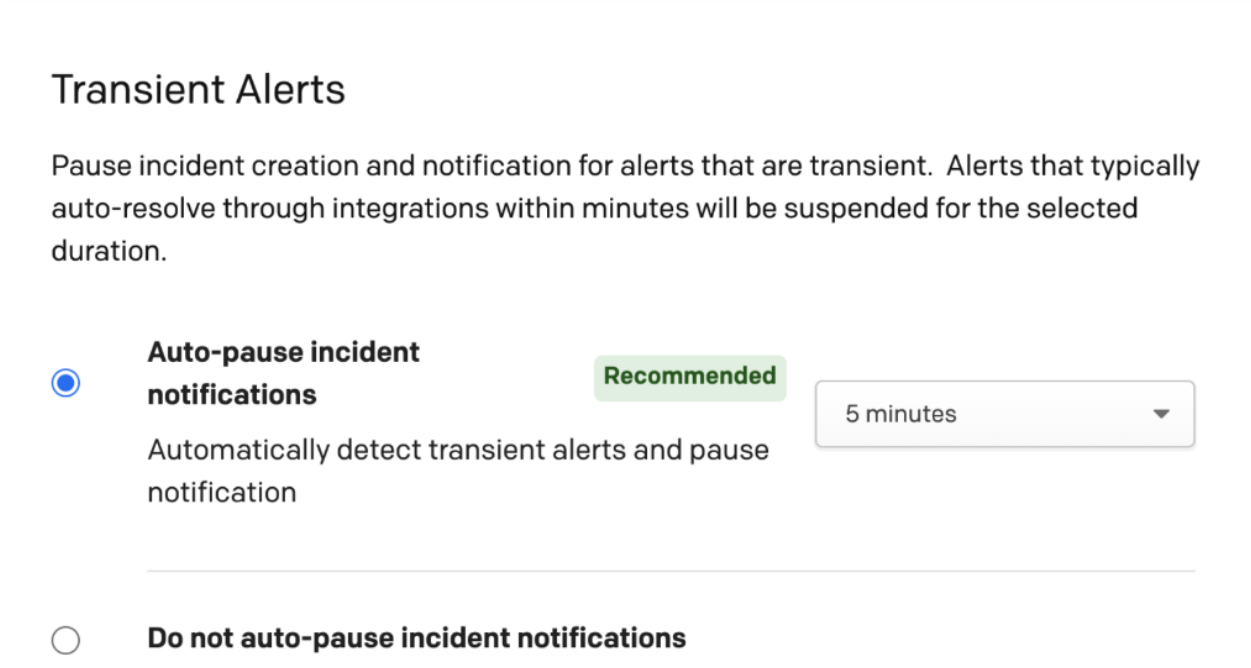
3. Assign an escalation policy either by “Generate a New Escalation Policy” or “Select an Existing Escalation Policy.” Click Next to continue



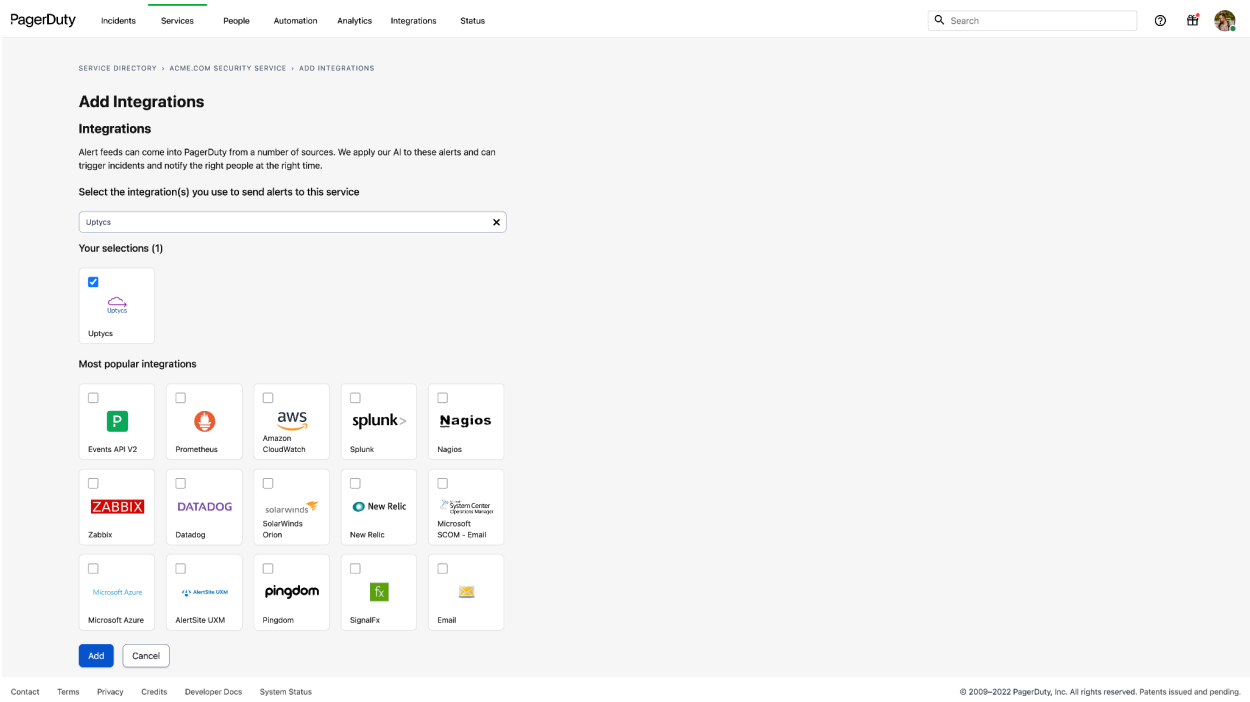
4. If you generate a new escalation policy, you will be placed as the first-level on-call for the service. You can edit the policy at any time after the service is created.
5. On the next screen, Reduce Noise: select Alert Grouping based on below options:
    a. Intelligent: Group alerts based on alert 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.



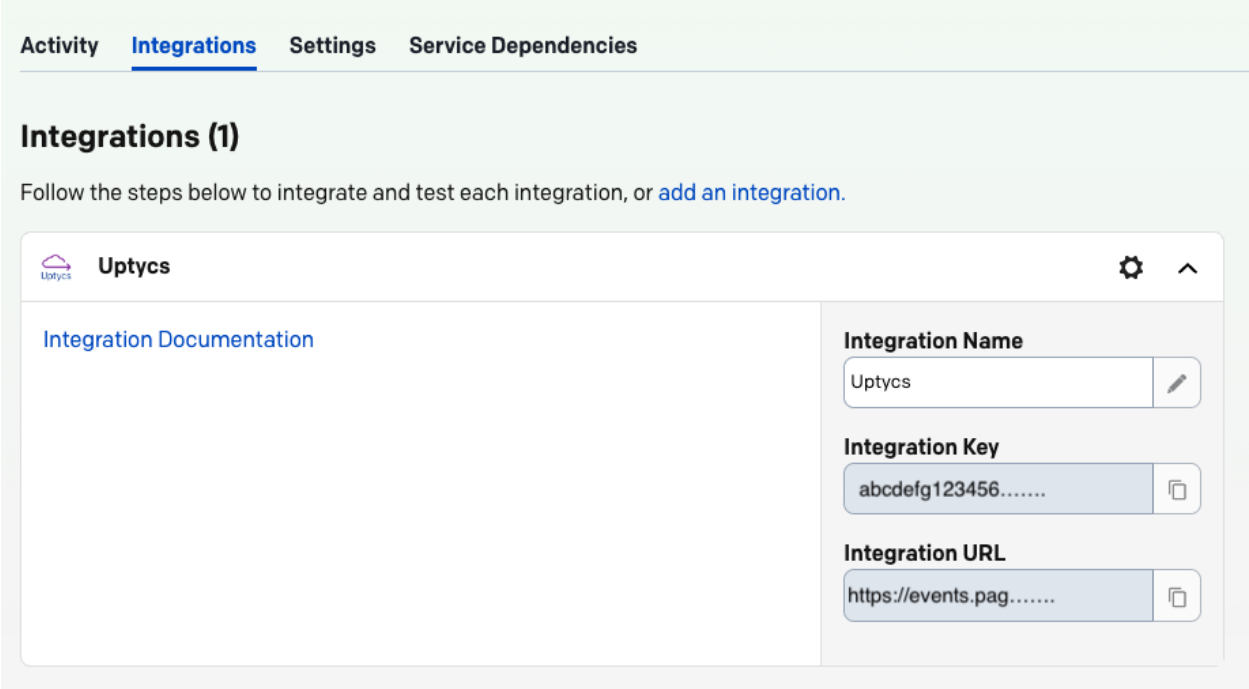
6. Transient Alerts: Pause incident creation and notification for alerts that are transient. Alerts that typically auto-resolve through integrations within minutes will be suspended for the selected duration.



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

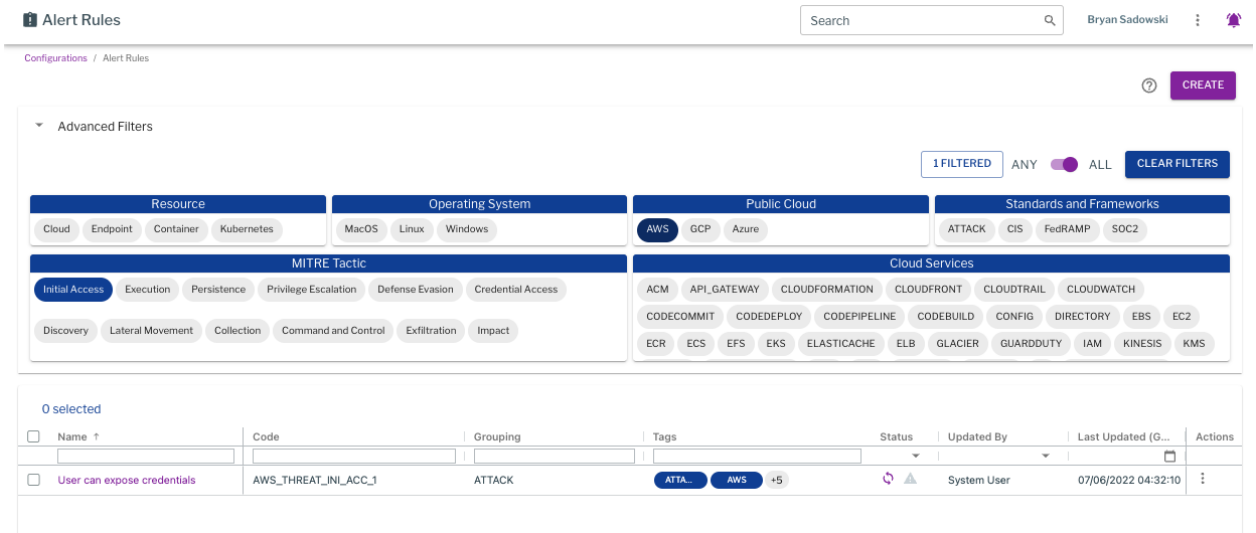


8. Once the Service is created, go to the Integrations page and you will see the Integration name, Integration key and Integration key and Integration URL which is required when you send events to PagerDuty. The Integration Key and URL is hidden for security reasons, you will see the full Key and URL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

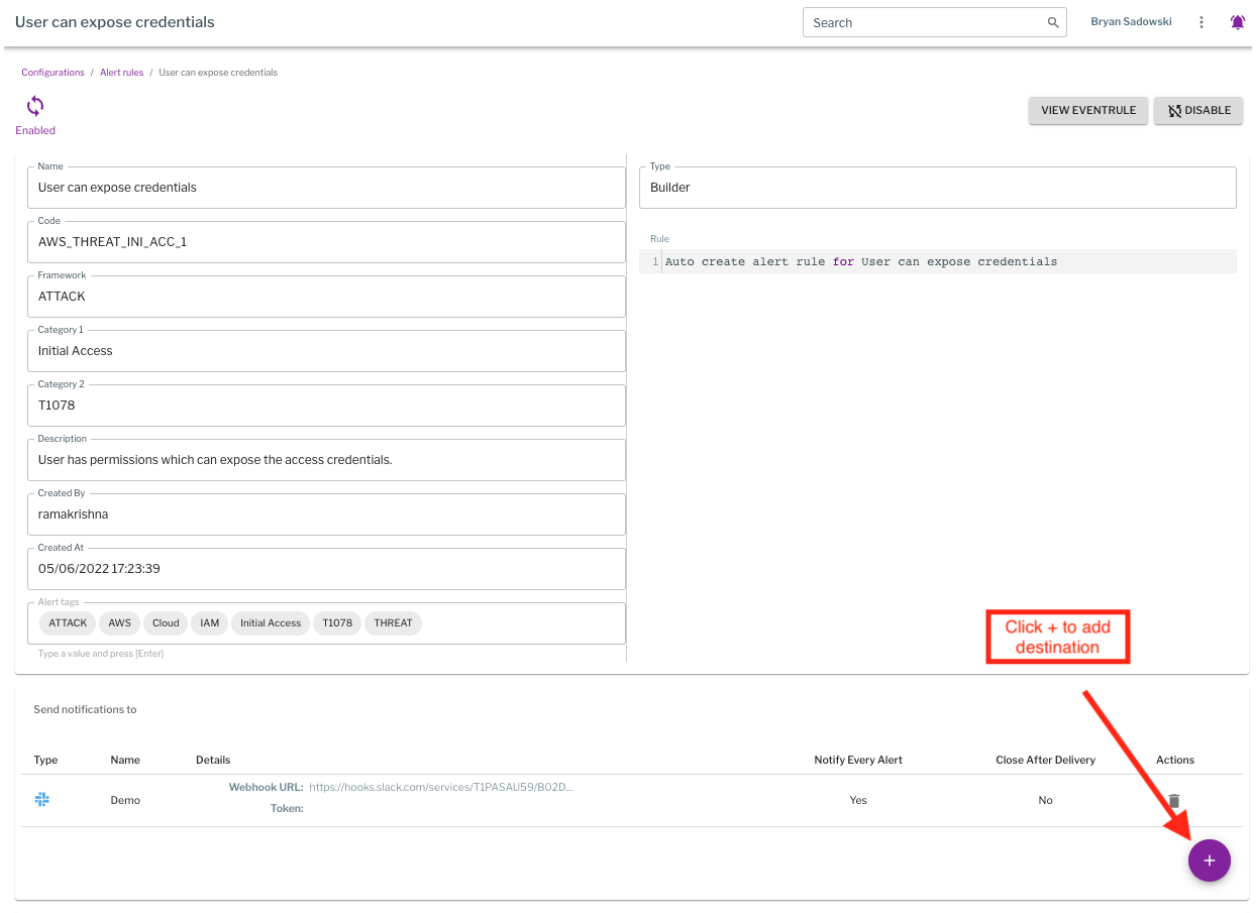


Working Example

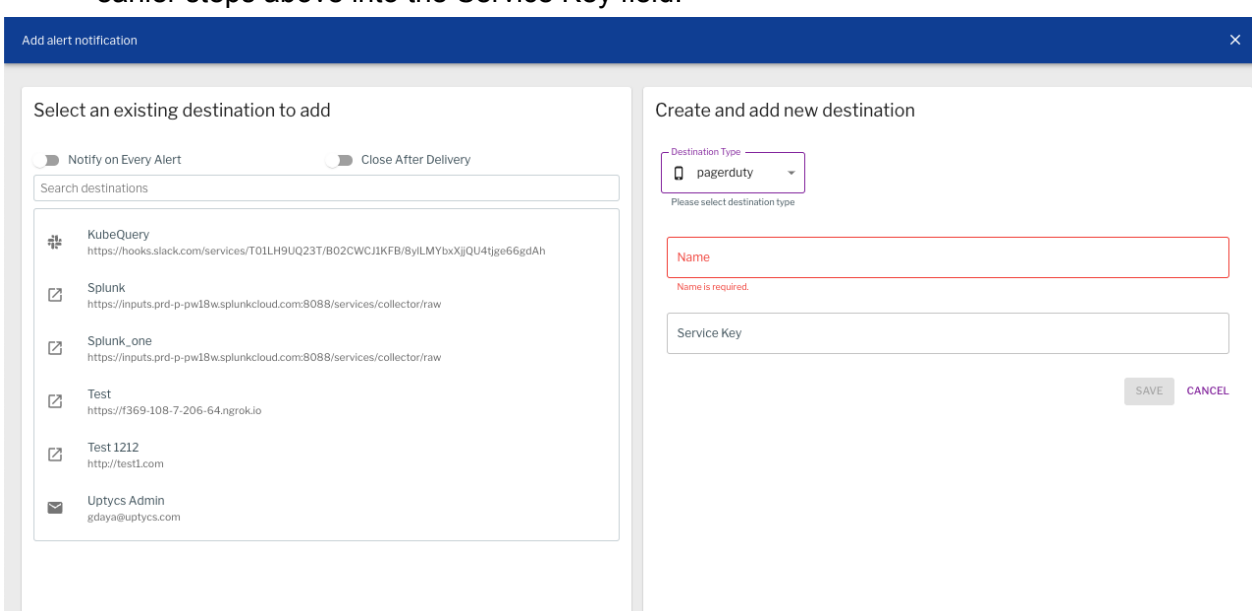
1. In your Uptycs Platform, Create or select an Event Rule and Alert rule under configurations and generate an alert



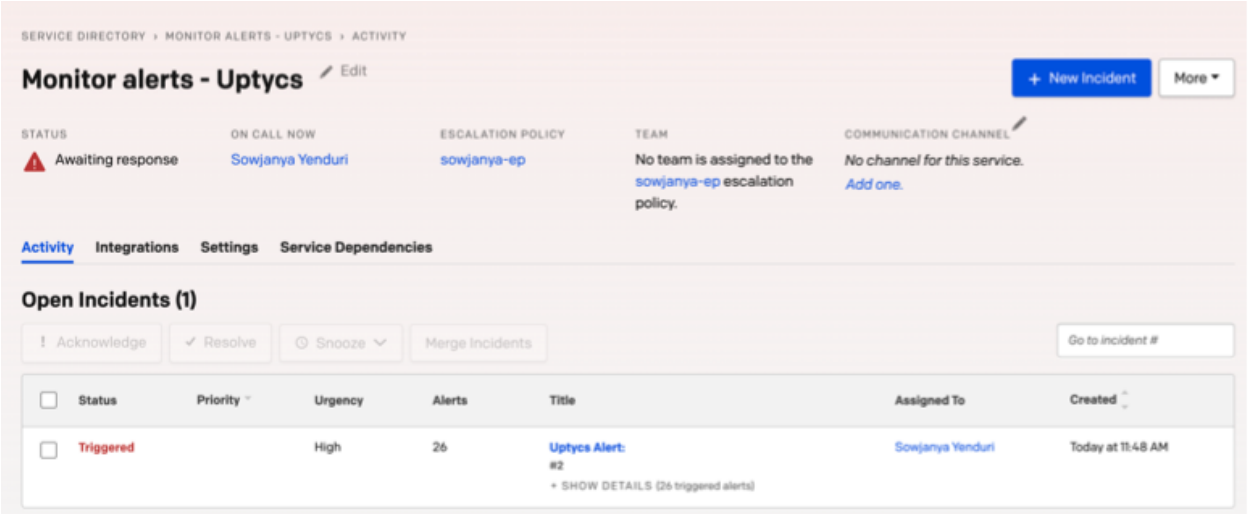
2. Go to Alert rule and click on Send Notifications



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.



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.



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.