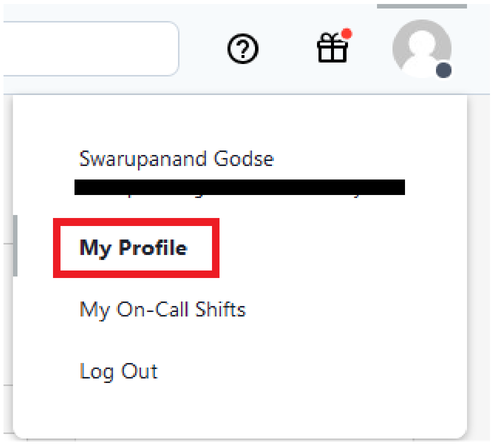
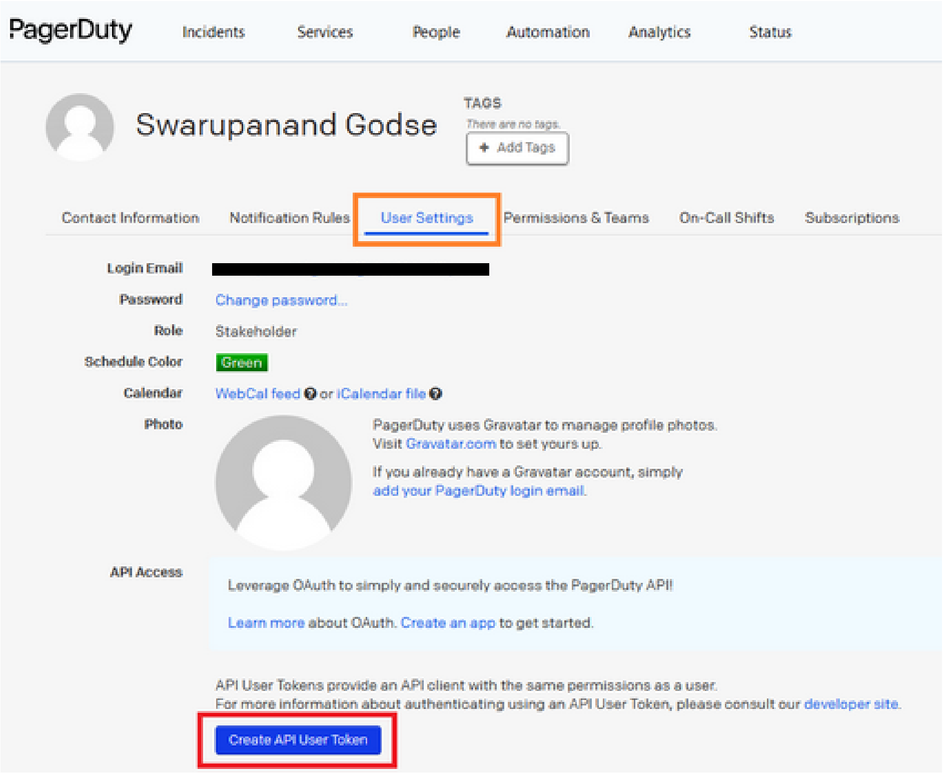
PagerDuty Integration

Part-1: PagerDuty Credentials

Step1: Login to the PagerDuty Account and select ‘My Profile’ from the profile icon.



Step2: Select ‘User Settings’ tab and click on ‘Create API User Token’ button.



Swarupanand Godse

Login Email [redacted]

Password Change password...

Role Stakeholder

Schedule Color 🟩 Green

Calendar WebCal feed or iCalendar file

Photo PagerDuty uses Gravatar to manage profile photos. Visit Gravatar.com to set yours up.

If you already have a Gravatar account, simply add your PagerDuty login email.

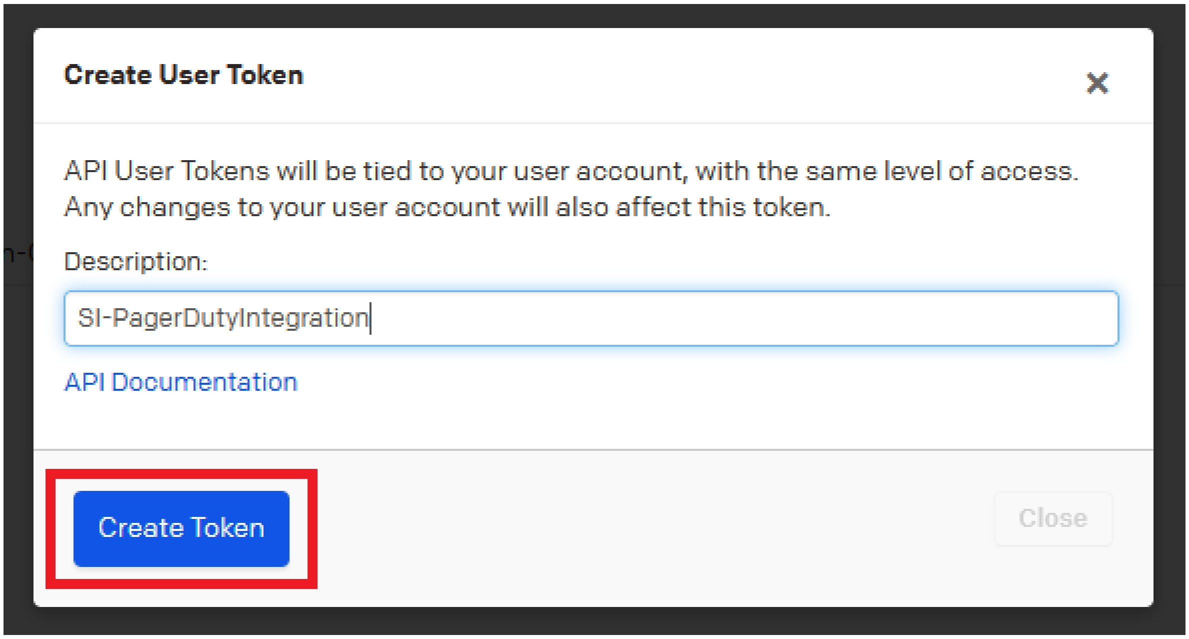
API Access Leverage OAuth to simply and securely access the PagerDuty API!

Learn more about OAuth. Create an app to get started.

API User Tokens provide an API client with the same permissions as a user.
For more information about authenticating using an API User Token, please consult our developer site.

PagerDuty Integration

Step3: Provide description and Click on the ‘Create Token’ button.

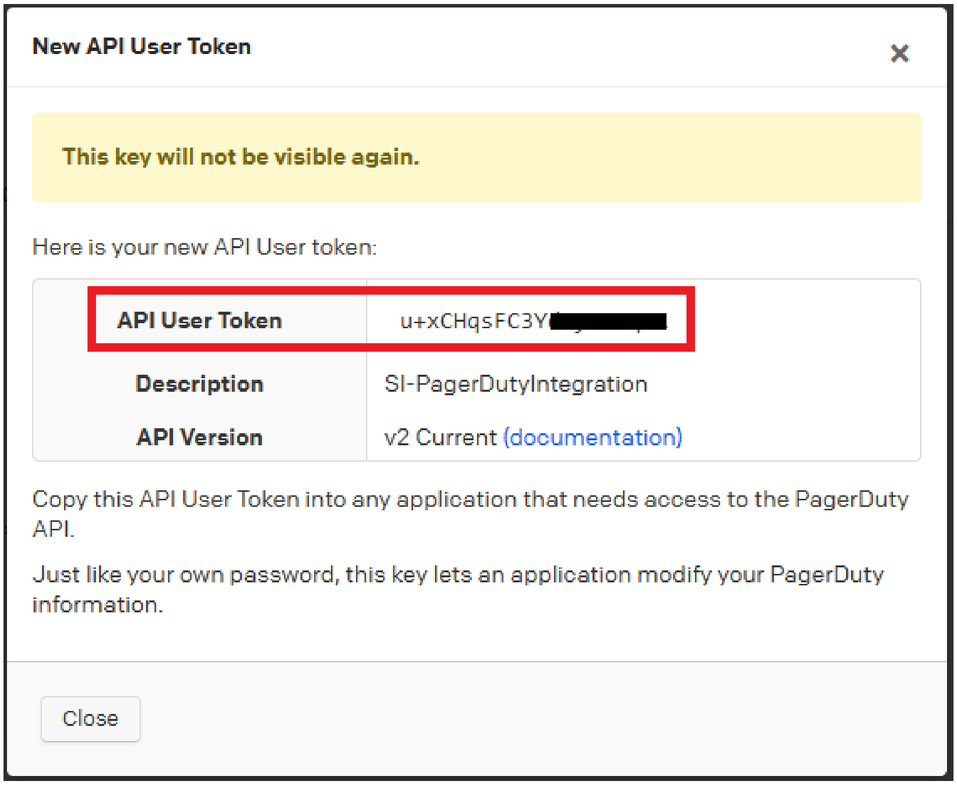


Create User Token

API User Tokens will be tied to your user account, with the same level of access. Any changes to your user account will also affect this token.

Description: SI-PagerDutyIntegration

Step4: Copy the generated API token. **Remember, you will be able to view this token One time only.**



New API User Token

This key will not be visible again.

Here is your new API User token:

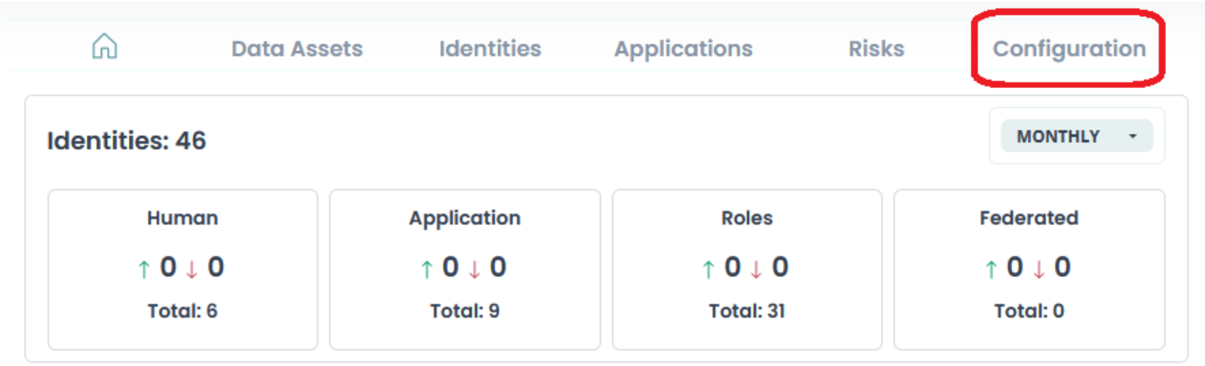
API User Token	u+xCHqsFC3Y[redacted]
Description	SI-PagerDutyIntegration
API Version	v2 Current (documentation)

Copy this API User Token into any application that needs access to the PagerDuty API.

Just like your own password, this key lets an application modify your PagerDuty information.

PagerDuty Integration

Step5: Now, login to SI platform then select the onboarded cloud account and navigate to the ‘Configuration’ page.

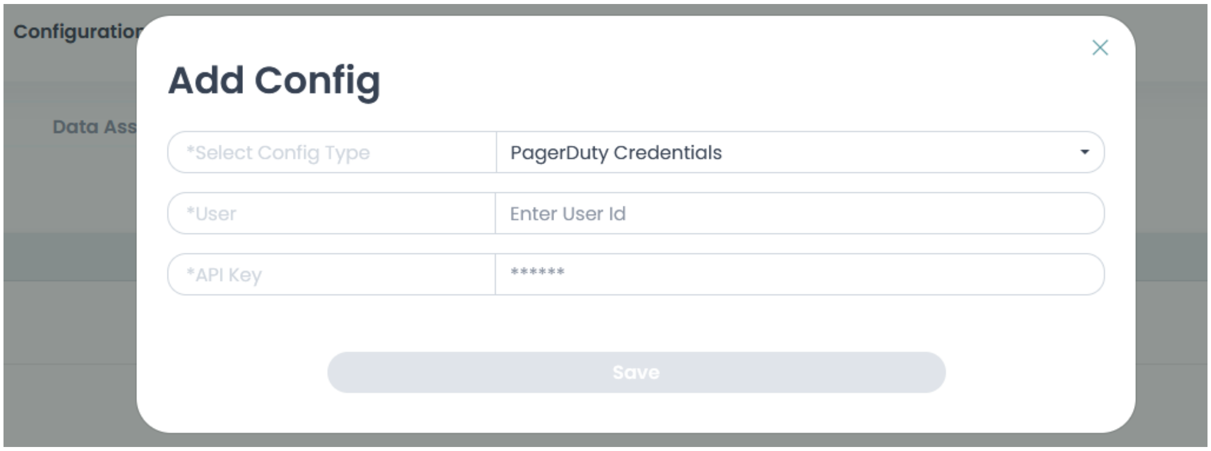


Identities: 46

Human	Application	Roles	Federated
↑ 0 ↓ 0	↑ 0 ↓ 0	↑ 0 ↓ 0	↑ 0 ↓ 0
Total: 6	Total: 9	Total: 31	Total: 0

Step6: Select the ‘Add Config’ button of the Advanced Settings and select the ‘PagerDuty Credentials’ from the drop down. Fill in the below details and Save:

User: Enter PagerDuty User mail ID.
API Key: Paste the copied API token from Step4.

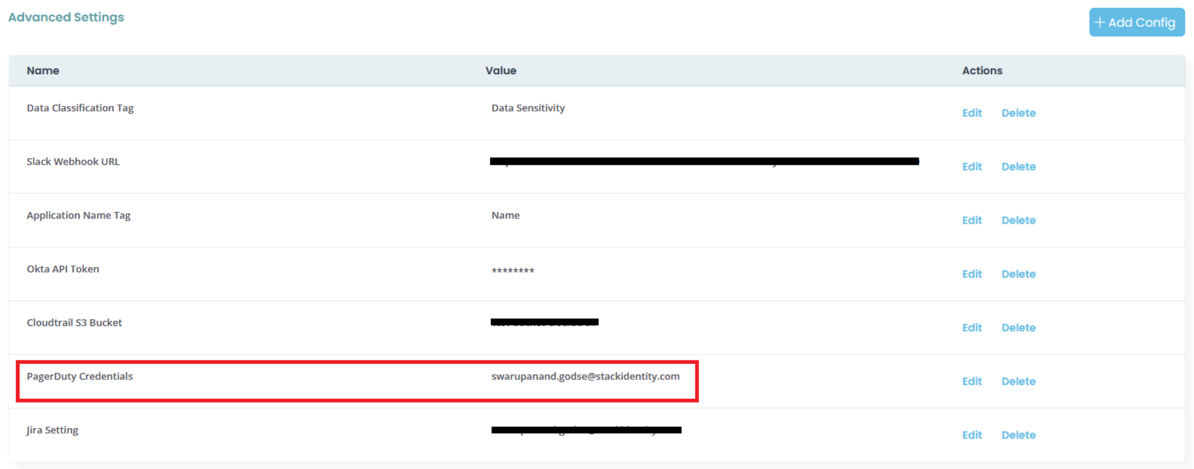


Add Config

*Select Config Type	PagerDuty Credentials
*User	Enter User Id
*API Key	******

Step7: Upon successful saving user will be able to see an entry in the Advanced Settings.

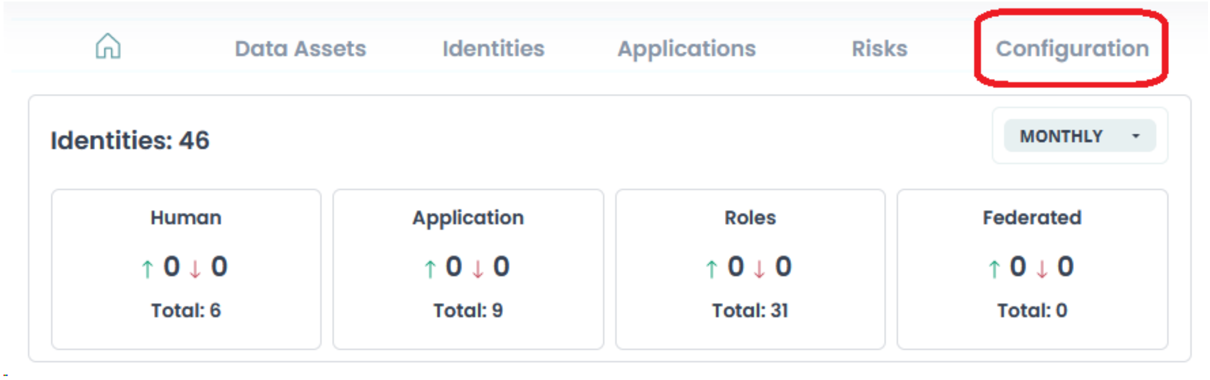
PagerDuty Integration



Name	Value	Actions
Data Classification Tag	Data Sensitivity	Edit Delete
Slack Webhook URL	[redacted]	Edit Delete
Application Name Tag	Name	Edit Delete
Okta API Token	********	Edit Delete
Cloudtrail S3 Bucket	[redacted]	Edit Delete
PagerDuty Credentials	swarupanand.godse@stackidentity.com	Edit Delete
Jira Setting	[redacted]	Edit Delete

Part-2: PagerDuty Settings

Step1: Login to SI platform then select the onboarded cloud account and navigate to the ‘Configuration’ page.



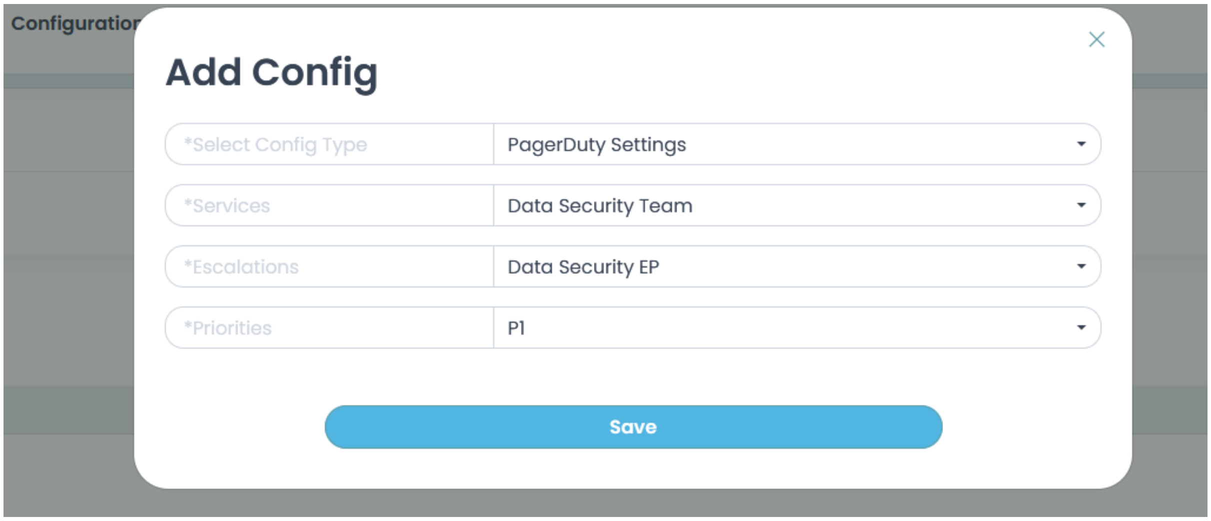
Identities: 46

Human	Application	Roles	Federated
↑ 0 ↓ 0	↑ 0 ↓ 0	↑ 0 ↓ 0	↑ 0 ↓ 0
Total: 6	Total: 9	Total: 31	Total: 0

Step2: Select the ‘Add Config’ button of the Advanced Settings and select the ‘PagerDuty Settings’ from the drop down. Fill in the below details and Save:

Services: List will be fetched from Part-1 configured account.
Escalations: List will be fetched from Part-1 configured account.
Priorities: Select a value from P1-P5.

PagerDuty Integration

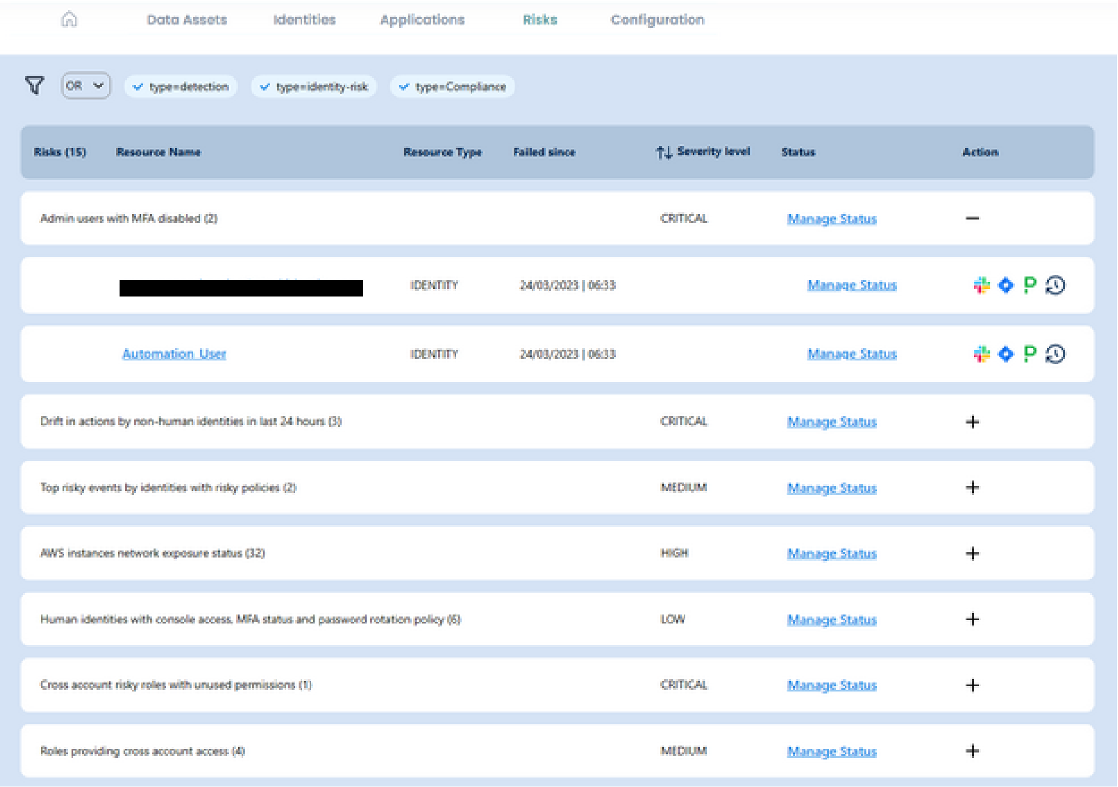


Add Config

*Select Config Type	PagerDuty Settings
*Services	Data Security Team
*Escalations	Data Security EP
*Priorities	P1

Part-3: PagerDuty Settings Creating Incidents in PagerDuty from Stack Platform

After you login to the Stack Platform and view an on-boarded Cloud account, you need to goto the ‘Risks’ view.

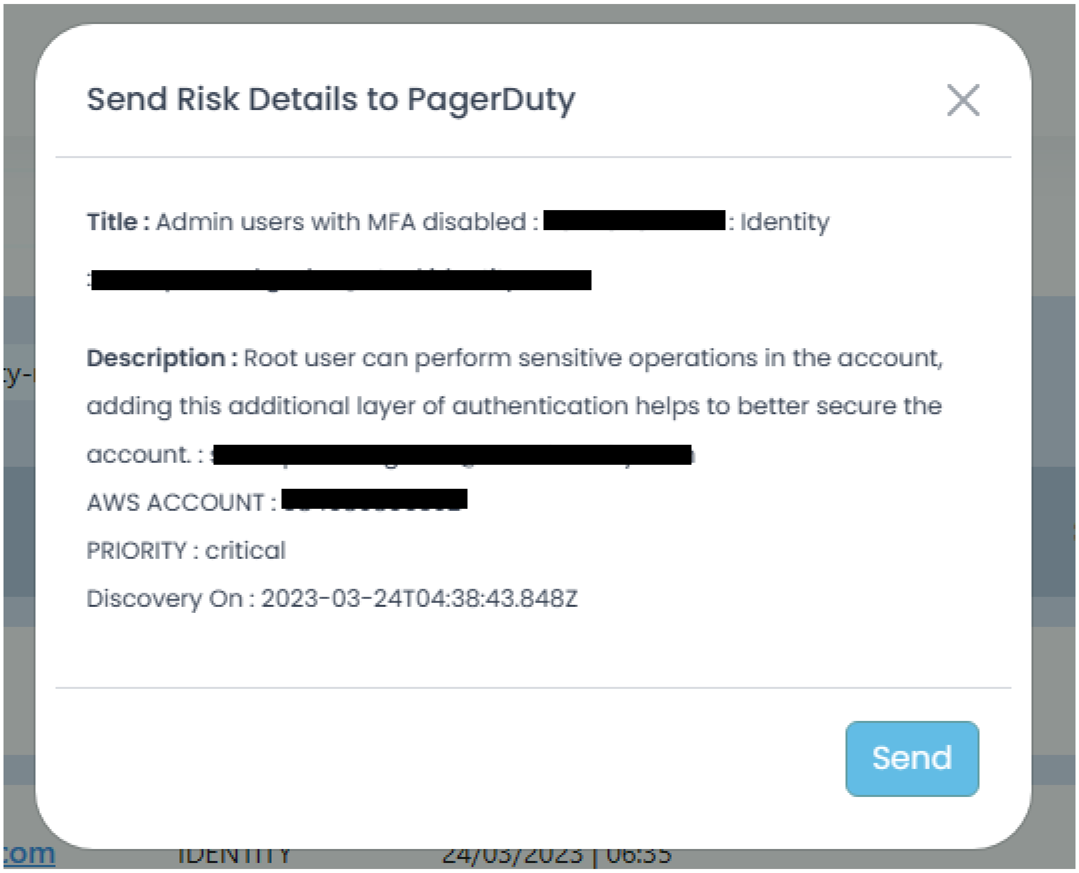


OR ✓ type=detection ✓ type=identity-risk ✓ type=Compliance

Risks (15)	Resource Name	Resource Type	Failed since	Severity level	Status	Action
Admin users with MFA disabled (2)				CRITICAL	Manage Status	−
	[redacted]	IDENTITY	24/03/2023 | 06:33		Manage Status	
	Automation User	IDENTITY	24/03/2023 | 06:33		Manage Status	
Drift in actions by non-human identities in last 24 hours (3)				CRITICAL	Manage Status	+
Top risky events by identities with risky policies (2)				MEDIUM	Manage Status	+
AWS instances network exposure status (32)				HIGH	Manage Status	+
Human identities with console access, MFA status and password rotation policy (6)				LOW	Manage Status	+
Cross account risky roles with unused permissions (1)				CRITICAL	Manage Status	+
Roles providing cross account access (4)				MEDIUM	Manage Status	+

PagerDuty Integration

From here, you need to click on the PagerDuty icon which will pop-up the risk details.



Send Risk Details to PagerDuty

Title : Admin users with MFA disabled : [redacted] : Identity : [redacted]

Description : Root user can perform sensitive operations in the account, adding this additional layer of authentication helps to better secure the account. : [redacted]

AWS ACCOUNT : [redacted]

PRIORITY : critical

Discovery On : 2023-03-24T04:38:43.848Z

When you hit the 'Send' button, it will create an incident in the PagerDuty with the default configuration you have done. You can view the created incidents in your PagerDuty tenant.