The Snowflake Trust Center is a comprehensive framework designed to assess and monitor security compliance within your Snowflake account. It leverages metadata-based rules derived from the CIS Snowflake Benchmarks documents ensuring that your Snowflake environment adheres to industry best practices.

The Trust Center operates as a metadata-driven system. It executes predefined rules against your Snowflake account, evaluating security configurations and practices.

* The Trust Center operates as a metadata-driven system. It executes predefined rules against your Snowflake account, evaluating security configurations and practices.
* Each rule corresponds to a specific security check, covering aspects such as access controls, encryption, authentication, and data protection.

When a violation is detected, the Trust Center raises alerts based on severity levels:

Low: Minor issues that require attention.

1. Medium: More significant issues that need prompt resolution.
2. High: Critical issues that demand immediate action.
3. Critical: Severe vulnerabilities that pose a significant risk.
4. These alerts help prioritize remediation efforts.

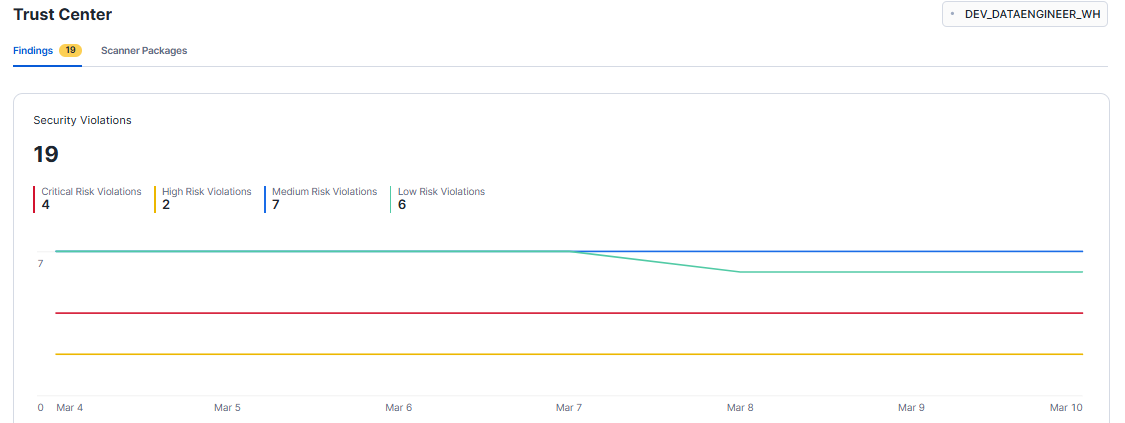
Users can enable Trust center in Snowflake by clicking on Monitoring—------>TrustCenter —--->Scanner packages and click on CIS Benchmark and click on Enable button

Currently, the Trust Center evaluates 38 check points, as detailed in the CIS benchmark documents.

Trust center has mainly 2 tabs

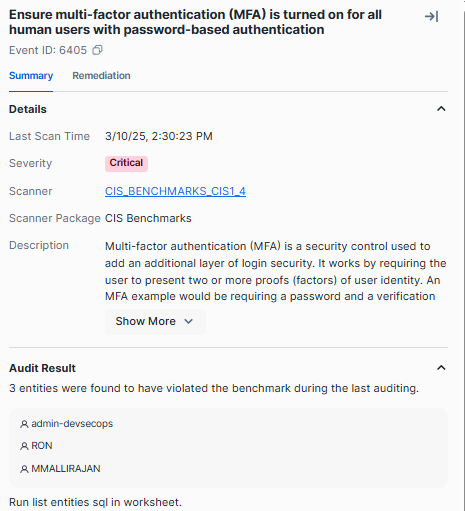
**Finding Tab** — This tab takes care of all outcomes of security scan. To get access to this tab you need to either have ACCOUNTADMIN role privilege or should have access to SNOWFLAKE.TRUST\_CENTER\_VIEWER or SNOWFLAKE.TRUST\_CENTER\_ADMIN to custom role.

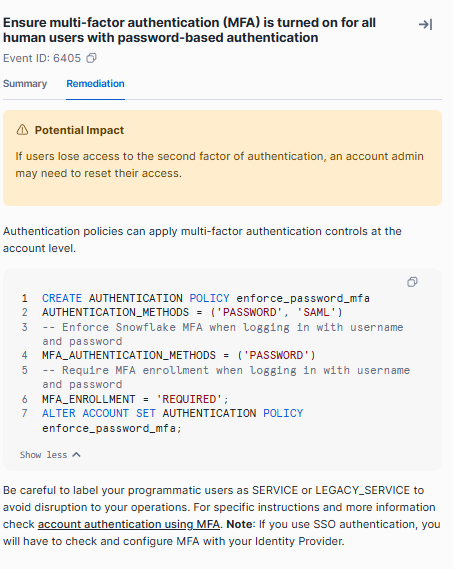
Finding tab also builds a predefined graph to showcase the CIS Benchmark violation on a day-to-day basis with separate color coding per severity.



When a user clicks on any violation, user can view Summary and Remediation.

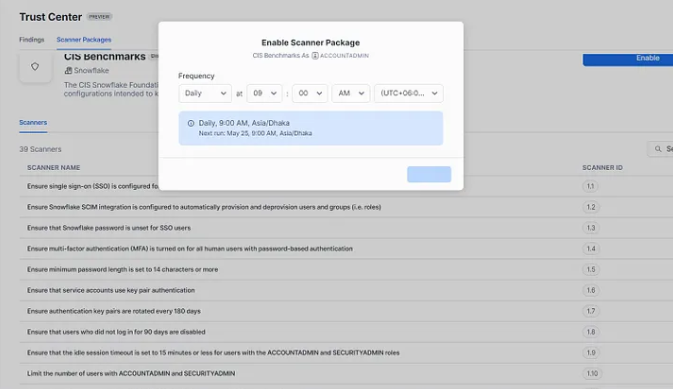
In Summary, user can find the reason behind rule violation and In the Remediation section, can find list of steps needs to be executed to resolve the violation.



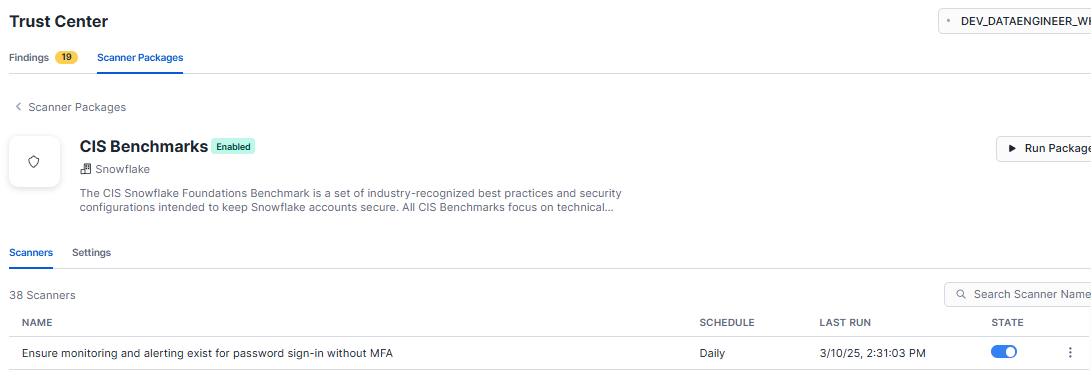


**2. Scanner Packages** — This tab take care of enabling the scanner service. You have to enable this scanner package to get them run every 24 hours (default setup).

You can always change the schedule as per your choice. The moment you click on Enable button it will ask you for a schedule of your choice.



By default all 38 check points are enabled in Trust center which is a best practice. If user want to disable any check points they can disable by turning off the toggle button.



If a user like to know about each rule, they can know about it by reading the description about it as shown in below picture.

