Role–Scope Access Matrix for Metrics for Custom Patterns

Overview

Metrics for custom patterns provide a 30–day view of alert and push–protection activity for each custom pattern. Access to these metrics depends on both:

- The *scope* at which the custom pattern was created: repository, organization, or enterprise.
- The *role* of the user viewing the metrics.

Symbols used in the matrix:

- **Y** = Direct access by default.
- **C** = Conditional access; requires additional admin/security permissions at that scope.
- – = No access by default.

Role–Scope Access Matrix

Scope (where pattern is defined)	**Metric view**	**Repo owner**	**Repo admin**	**Org owner**	**Security manager**	**Enterprise admin**
Repository level	Activity for a custom pattern defined in a single repository	**Y**	**Y**	**C**	**C**	**C**
Organization level	Aggregated activity for a custom pattern defined at org scope	–	–	**Y**	**Y**	**C**
Enterprise level	Aggregated activity for a custom pattern defined at enterprise scope	–	–	–	**C**	**Y**

Table 1: Decision table for who can view metrics for custom patterns at each scope.

Decision Rules

1. Any user with *admin permission on a repository* (including the repository owner) can view metrics for repository-scoped custom patterns in that repository.
2. Organization owners and designated security managers can view metrics for organization-scoped custom patterns for their organization.
3. Enterprise administrators can view metrics for enterprise-scoped custom patterns across the enterprise.
4. Users in roles marked **C** may view metrics at that scope only if they have been explicitly granted admin or security permissions for the relevant repository, organization, or enterprise.