Roles for working in Microsoft Sentinel

Microsoft Sentinel-specific roles

All Microsoft Sentinel built-in roles grant read access to the data in your Microsoft Sentinel workspace.

- Microsoft Sentinel Reader can view data, incidents, workbooks, and other Microsoft Sentinel resources.
- Microsoft Sentinel Responder can, in addition to the above, manage incidents (assign, dismiss, etc.)
- Microsoft Sentinel Contributor can, in addition to the above, create and edit workbooks, analytics rules, and other Microsoft Sentinel resources.
- Microsoft Sentinel Automation Contributor allows Microsoft Sentinel to add playbooks to automation rules. It is not meant for user accounts.
-
  - Just as with automation rules, to **run playbooks** on-demand Microsoft Sentinel must be granted **permissions** to **run playbooks**. The user who triggers the **playbook** needs to be able to view the Logic Apps workflows and trigger them. Currently the built-in **role** that grants these **permissions** is Logic Apps Contributor.

Microsoft Sentinel roles and allowed actions

The following table summarizes the Microsoft Sentinel roles and their allowed actions in Microsoft Sentinel.

Role	Create and run playbooks	Create and edit analytics rules, workbooks, and other Microsoft Sentinel resources	Manage incidents (dismiss, assign, etc.)	View data, incidents, workbooks, and other Micr Sentinel resources
Microsoft Sentinel Reader	--	--*	--	✓
Microsoft Sentinel Responder	--	--*	✓	✓
Microsoft Sentinel Contributor	--	✓	✓	✓
Microsoft Sentinel Contributor + Logic App Contributor	✓	✓	✓	✓

Role recommendations

After understanding how roles and permissions work in Microsoft Sentinel, you may want to use the following best practice guidance for applying roles to your users:

User type	Role	Resource group	Description
Security analysts	Microsoft Sentinel Responder	Microsoft Sentinel's resource group	View data, incidents, workbooks, and other Microsoft Sentinel resources. Manage incidents, such as assigning or dismissing incidents.
	Logic Apps Contributor	Microsoft Sentinel's resource group, or the resource group where your playbooks are stored	Attach playbooks to analytics and automation rules and run playbooks. **Note**: This role also allows users to modify playbooks.
Security engineers	Microsoft Sentinel Contributor	Microsoft Sentinel's resource group	View data, incidents, workbooks, and other Microsoft Sentinel resources. Manage incidents, such as assigning or dismissing incidents. Create and edit workbooks, analytics rules, and other Microsoft Sentinel resou
	Logic Apps Contributor	Microsoft Sentinel's resource group, or the resource group where your playbooks are stored	Attach playbooks to analytics and automation rules and run playbooks. **Note**: This role also allows users to modify playbooks.
Service Principal	Microsoft Sentinel Contributor	Microsoft Sentinel's resource group	Automated configuration for management tasks