



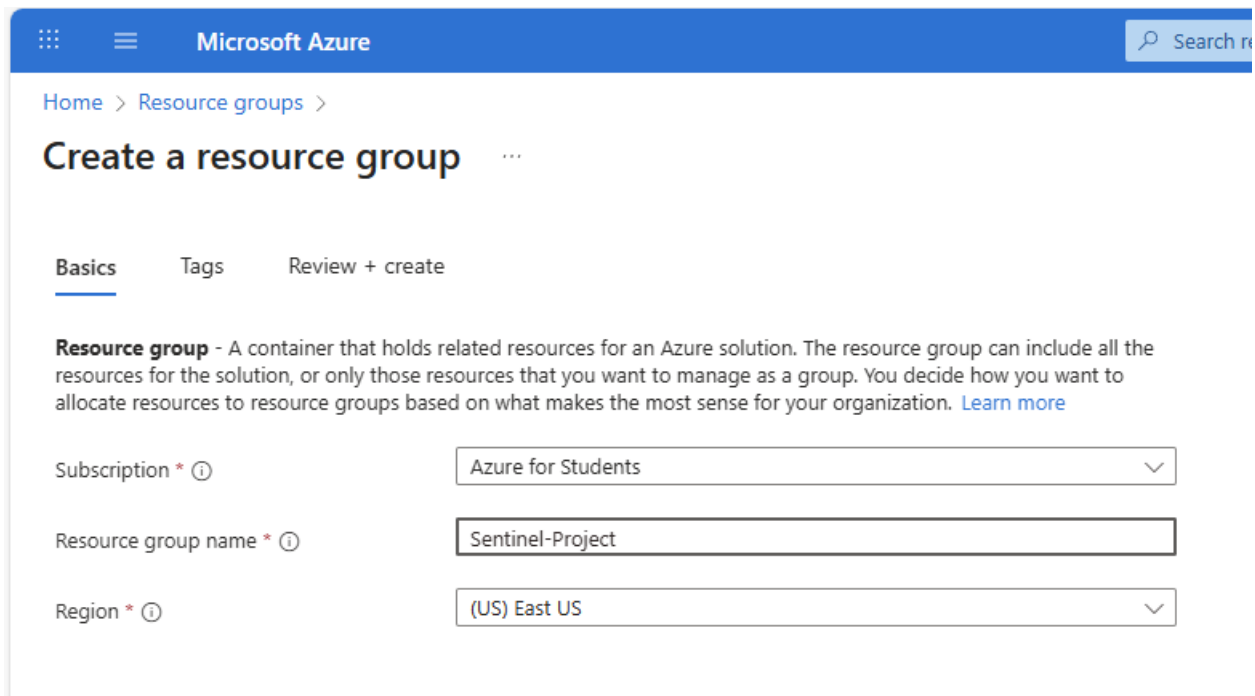
# Microsoft Sentinel Set Up

Adrian Cortez

## Overview

Microsoft Sentinel is a cloud-native SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response) solution built on Azure. It enables organizations to collect security data at cloud scale from multiple sources. This includes users, applications, servers, and devices. Sentinel uses advanced analytics, threat intelligence, and AI-driven detection to identify potential threats in real time. It also provides built-in automation and orchestration tools to streamline incident investigation and response, helping security teams quickly prioritize and mitigate risks. Because it's cloud-based, Sentinel offers scalability, integration with many Microsoft and third-party services, and reduces the overhead of managing traditional on-prem SIEM infrastructure.

## Create a Resource Group



The screenshot shows the 'Create a resource group' page in the Microsoft Azure portal. The page has a blue header with the 'Microsoft Azure' logo and a search bar. Below the header, there is a breadcrumb trail: 'Home > Resource groups >'. The main heading is 'Create a resource group'. There are three tabs: 'Basics' (selected), 'Tags', and 'Review + create'. A description of a 'Resource group' is provided, stating it is a container for related resources and that users can decide how to allocate resources based on organizational needs. Below the description, there are three form fields: 'Subscription \*' with a dropdown menu showing 'Azure for Students', 'Resource group name \*' with a text input field containing 'Sentinel-Project', and 'Region \*' with a dropdown menu showing '(US) East US'. Each field has an information icon (i) next to it.

Microsoft Azure

Home > Resource groups >

### Create a resource group

Basics Tags Review + create

**Resource group** - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

Subscription \* ⓘ Azure for Students

Resource group name \* ⓘ Sentinel-Project

Region \* ⓘ (US) East US

## Create a Log Analytics Workspace

[Home](#) >



## Microsoft.LogAnalyticsOMS | Overview ...

Deployment

✕ <<



Delete



Cancel



Redeploy



Download



Refresh



Overview



Inputs



Outputs



Template



### Your deployment is complete



Deployment name : Microsoft.LogAnalyticsOMS

Subscription : [Azure for Students](#)

Resource group : [Sentinel-Project](#)



Deployment details



Next steps

[Go to resource](#)

Give feedback



[Tell us about your experience with deployment](#)

## Create Microsoft Sentinel in Azure

[Home](#) > [Microsoft Sentinel](#) >

### Add Microsoft Sentinel to a workspace ...

[+ Create a new workspace](#) [Refresh](#)

Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.

New Microsoft Sentinel workspaces created by authorized users are automatically onboarded and redirected to the Defender portal. [Learn more](#)

Filter by name...				
Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription ↑↓	Directory ↑↓
Sentinel-Project-Workspace	eastus	sentinel-project	Azure for Students	Olivet Nazarene University

[Add](#) [Cancel](#)

Add to the workspace you created