

5557

Summative Exam



Thato legoale

CSAS632

5557

Table of Contents

Project.....	2
• Start collecting data from Azure Activity and Security Center.	2
• Add built in and custom alerts.....	2
• Review how Playbooks can be used to automate a response to an incident.....	2
Task 1: On-board Azure Sentinel	2
Task 2: Configure Azure Sentinel to use the Azure Activity data connector.	6
Task 3: Create a rule that uses the Azure Activity data connector.....	11
Task 4: Create a playbook	16
Task 5 Create a custom alert and configure a playbook as an automated response	25
Task 6: Invoke an incident and review the associated actions.	29
2. On the Security Center Azure Defender blade, click Just-in-time vm access section.....	30
4. In the Azure portal, in the Search resources, services, and docs text box at the top of the Azure portal page, type Activity log and press the Enter key.	30
Conclusion.....	31

Summative Exam CSAS632

Screenshots

Project

- Start collecting data from Azure Activity and Security Center.
- Add built in and custom alerts
- Review how Playbooks can be used to automate a response to an incident.

Task 1: On-board Azure Sentinel

The screenshot shows the Microsoft Azure portal home page. The browser address bar displays 'https://portal.azure.com/#home'. The page features a search bar and a navigation menu. Under 'Azure services', there are icons for 'Create a resource', 'Log Analytics workspaces', 'Virtual networks', 'Subscriptions', 'Azure Active Directory', 'Policy', 'All resources', 'SQL databases', 'Azure SQL', and 'More services'. The 'Recent resources' section contains a table with the following data:

Name	Type	Last Viewed
ga5-cs95632	Log Analytics workspace	6 days ago
myVM	Virtual machine	2 weeks ago
AZ500LAB131415	Resource group	2 weeks ago
Azure for Students	Subscription	a month ago
myResourceGroup	Resource group	2 months ago
defaultadventure	Resource group	2 months ago

Below the table is a 'See all' link. The 'Navigate' section includes icons for 'Subscriptions', 'Resource groups', 'All resources', and 'Dashboard'. The Windows taskbar at the bottom shows the system tray with a temperature of 17°C, cloud weather, and the date 2021/11/22.

Azure Sentinel - Microsoft Azure

https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/microsoft.securityinsightsarg%2Fsentinel

Microsoft Azure Search resources, services, and docs (G+)

Home > Azure Sentinel


CTU Career (ctucareer.co.za)

+ Create Manage view Refresh Export to CSV Open query View incidents Feedback

Filter for any field... Subscription == all Resource group == all Location == all Add filter

Showing 0 to 0 of 0 records.

No grouping List view

Name	Resource group	Location	Subscription	Directory
 <h3>No Azure Sentinel to display</h3> <p>See and stop threats before they cause harm, with SIEM reinvented for a modern world. Azure Sentinel is your birds-eye view across the enterprise.</p> <p>Create Azure Sentinel</p> <p>Learn more</p>				

Windows taskbar: 17°C Cloudy 10:32 2021/11/22

Add Azure Sentinel to a workspace

https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/microsoft.securityinsightsarg%2Fsentinel

Microsoft Azure Search resources, services, and docs (G+)

Home > Azure Sentinel > Add Azure Sentinel to a workspace

+ Create a new workspace Refresh

Azure Sentinel offers a 31-day free trial. See Azure Sentinel pricing for more details.

Filter by name...

Workspace	Location	ResourceGroup	Subscription	Directory
ga5-csa632	eastus	az500lab131415	Azure for Students	CTU Career

Add Cancel

Windows taskbar: 17°C Cloudy 10:33 2021/11/22

Home - Microsoft Azure | Create Log Analytics workspace

https://portal.azure.com/?quickstart=True#blade/HubsExtension/BrowseResource/resourceType/microsoft.securityinsightsarg%2Fsentinel

Microsoft Azure | Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace

Create Log Analytics workspace

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#)

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * [Create new](#)

Instance details

Name *

Region *

[Review + Create](#) [Previous](#) [Next: Tags >](#)

17°C Cloudy 11:14 2021/11/23

Home - Microsoft Azure | Add Microsoft Sentinel to a work

https://portal.azure.com/?quickstart=True#blade/HubsExtension/BrowseResource/resourceType/microsoft.securityinsightsarg%2Fsentinel

Microsoft Azure | Search resources, services, and docs (G+)

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.

Filter by name...

Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription ↑↓	Directory ↑↓
sa-examcsas632	eastus	az500lab131415	Azure subscription 1	CTU Career

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

17°C Cloudy 11:16 2021/11/23

Home - Microsoft Azure x Microsoft Sentinel - Microsoft A x +

https://portal.azure.com/?quickstart=True#blade/Microsoft_Azure_Security_Insights/MainMenuBlade/3/subscriptionId/e987c85c-2802-427d-a463-0bb4ab93940e/r...

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel

Microsoft Sentinel | News & guides ...

Selected workspace: 'sa-examcsa632'

Search (Ctrl+J)

General

- Overview
- Logs
- News & guides

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence

Content management

- Solutions (Preview)
- Repositories (Preview)
- Community

Configuration

Successfully added Microsoft Sentinel

Successfully added Microsoft Sentinel to workspace 'sa-examcsa632'. It might take a few minutes for your workspace to appear in Microsoft Sentinel workspaces list.

17°C Cloudy 11:18 2021/11/23

Home - Microsoft Azure x Microsoft Sentinel - Microsoft A x +

https://portal.azure.com/?quickstart=True#blade/Microsoft_Azure_Security_Insights/MainMenuBlade/3/subscriptionId/e987c85c-2802-427d-a463-0bb4ab93940e/r...

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel

Microsoft Sentinel | News & guides ...

Selected workspace: 'sa-examcsa632'

Search (Ctrl+J)

Documentation

General

- Overview
- Logs
- News & guides

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence

Content management

- Content hub (Preview)
- Repositories (Preview)
- Community

Configuration

Microsoft Sentinel free trial activated

The free trial is active on this workspace from 11/23/2021 to 12/24/2021 at 11:59:59 PM UTC. During the trial, up to 10 GB/day are free for both Microsoft Sentinel and Log Analytics. Data beyond the 10 GB/day included quantity will be billed. [Learn more.](#)

OK

Microsoft Sentinel

A cloud-native SIEM to help you focus on what matters most

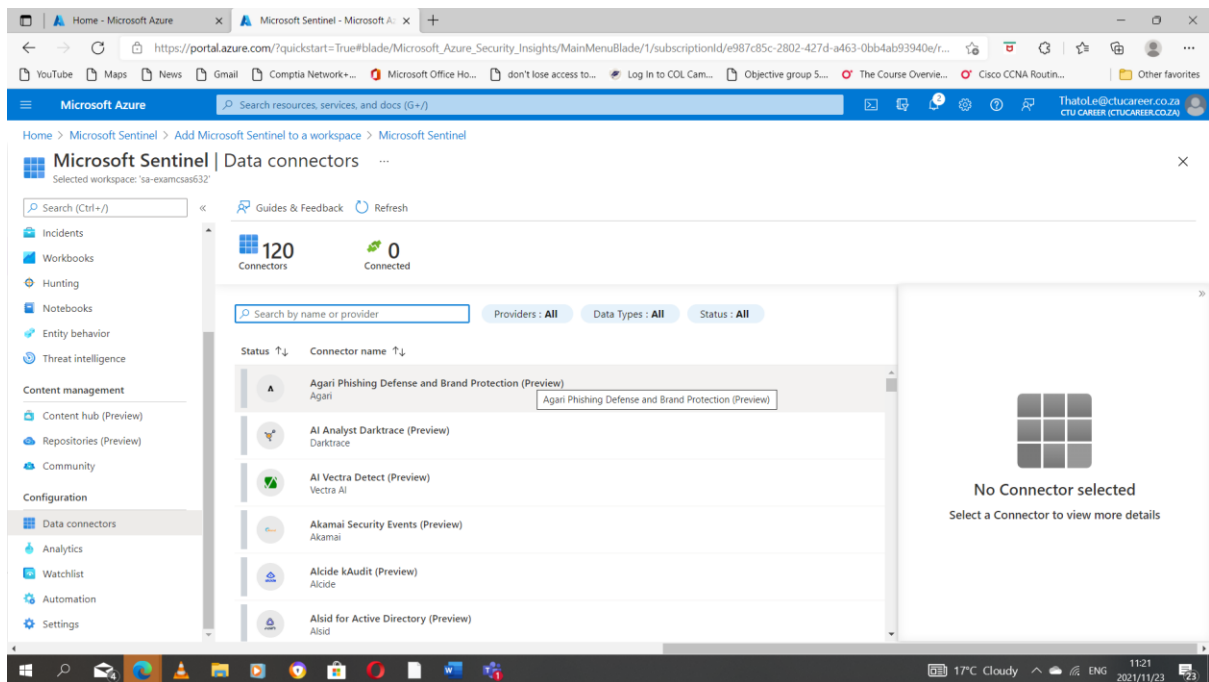
Collect and analyze data from any source, cloud or on-premises, in any format, at cloud scale. With AI on your side, find, investigate, and respond to real threats in minutes, with built-in knowledge and intelligence from decades of Microsoft security experience.

- 1. Collect data**
Collect data at cloud scale across the enterprise, both on-premises and in multiple clouds
- 2. Create security alerts**
Focus on what's important using analytics to create alerts
- 3. Automate & orchestrate**
Use or customize built-in playbooks to automate common tasks

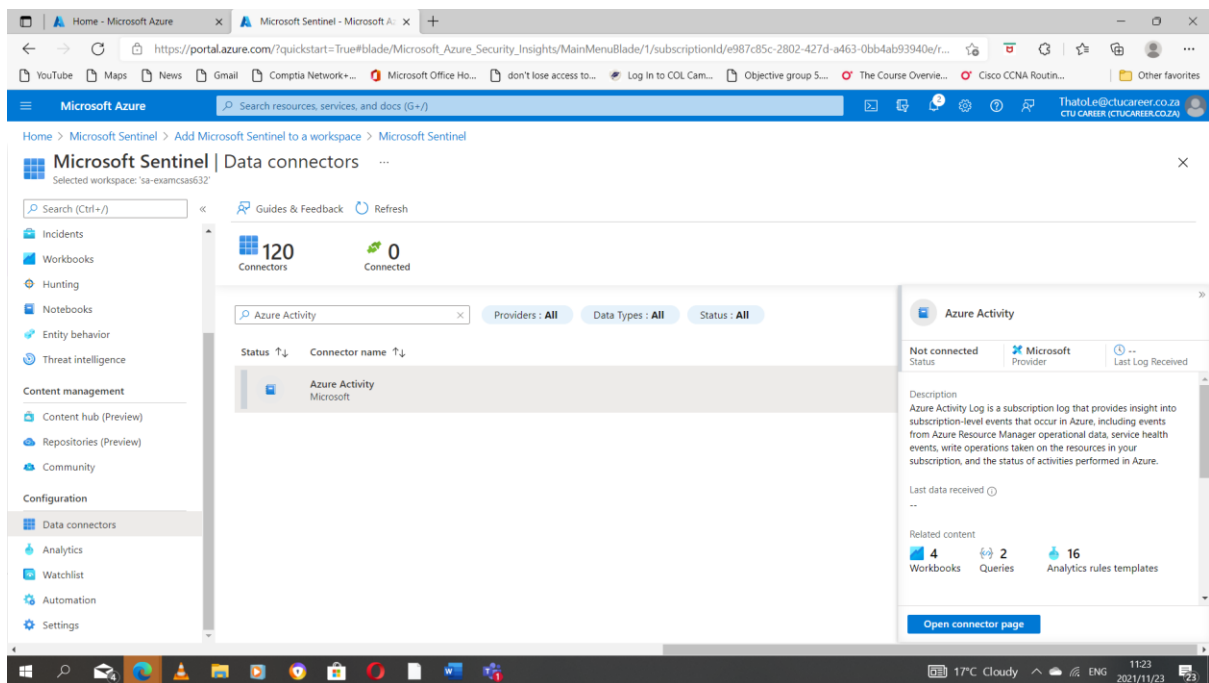
https://portal.azure.com/?quickstart=True#

17°C Cloudy 11:18 2021/11/23

Task 2: Configure Azure Sentinel to use the Azure Activity data connector.



The screenshot shows the Microsoft Sentinel 'Data connectors' page. At the top, it displays '120 Connectors' and '0 Connected'. A search bar is present with the text 'Search by name or provider'. Below the search bar, there are filters for 'Providers: All', 'Data Types: All', and 'Status: All'. A table lists several connectors, including 'Agari Phishing Defense and Brand Protection (Preview)', 'AI Analyst Darktrace (Preview)', 'AI Vectra Detect (Preview)', 'Akamai Security Events (Preview)', 'Alcide kAudit (Preview)', and 'Alsid for Active Directory (Preview)'. On the right side of the page, a large white box contains a grid icon and the text 'No Connector selected. Select a Connector to view more details'. The left sidebar shows navigation options like 'Incidents', 'Workbooks', 'Hunting', 'Notebooks', 'Entity behavior', 'Threat intelligence', 'Content management', 'Configuration', 'Data connectors', 'Analytics', 'Watchlist', 'Automation', and 'Settings'. The top navigation bar includes 'Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel' and a search bar. The bottom status bar shows '17°C Cloudy' and the date '2021/11/23'.



The screenshot shows the Microsoft Sentinel 'Data connectors' page with the 'Azure Activity' connector selected. The search bar now contains 'Azure Activity'. The table lists the 'Azure Activity' connector by Microsoft. On the right side, a details panel for 'Azure Activity' is open. It shows the status as 'Not connected', the provider as 'Microsoft', and the last log received as 'Last Log Received'. The description states: 'Azure Activity Log is a subscription log that provides insight into subscription-level events that occur in Azure, including events from Azure Resource Manager operational data, service health events, write operations taken on the resources in your subscription, and the status of activities performed in Azure.' Below the description, it shows 'Last data received' as '...'. The 'Related content' section displays '4 Workbooks', '2 Queries', and '16 Analytics rules templates'. At the bottom of the details panel, there is a button labeled 'Open connector page'. The rest of the page layout, including the sidebar and top navigation, remains the same as in the previous screenshot.

Home - Microsoft Azure x Azure Activity - Microsoft Azure x +

https://portal.azure.com/?quickstart=True#blade/Microsoft_Azure_Security_Insights/MainMenuBlade/1/subscriptionId/e987c85c-2802-427d-a463-0bb4ab93940e/r...

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel > Azure Activity

Azure Activity

Not connected Status Microsoft Provider Last Log Received

Description
Azure Activity Log is a subscription log that provides insight into subscription-level events that occur in Azure, including events from Azure Resource Manager operational data, service health events, write operations taken on the resources in your subscription, and the status of activities performed in Azure.

Last data received
--

Related content
4 Workbooks 2 Queries 16 Analytics rules templates

Data received
100
80
60
40
[Go to log analytics](#)

Instructions Next steps

Prerequisites

To integrate with Azure Activity make sure you have:

- ✓ **Workspace:** read and write permissions are required.
- ❗ **Policy:** owner role assigned for each policy assignment scope.
- ❗ **Subscription:** owner role permission on the relevant subscription

Configuration

❗ This connector has been updated to use the diagnostics settings back-end pipeline, which provides increased functionality and better consistency with resource logs. Connectors using this pipeline can also be governed at scale by Azure Policy. Learn more about the new Azure Activity connector. Follow the instructions below to upgrade your connector to the diagnostics settings pipeline.

17°C Cloudy 11:24 2021/11/23

Home - Microsoft Azure x Configure Azure Activity logs to x +

https://portal.azure.com/?quickstart=True#blade/Microsoft_Azure_Security_Insights/MainMenuBlade/1/subscriptionId/e987c85c-2802-427d-a463-0bb4ab93940e/r...

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel > Azure Activity > Configure Azure Activity logs to stream to specified Log Analytics workspace

Configure Azure Activity logs to stream to specified Log Analytics workspace

Assign policy

Basics Parameters Remediation Non-compliance messages Review + create

Scope [Learn more about setting the scope *](#)

Exclusions
Optionally select resources to exclude from the policy assignment.

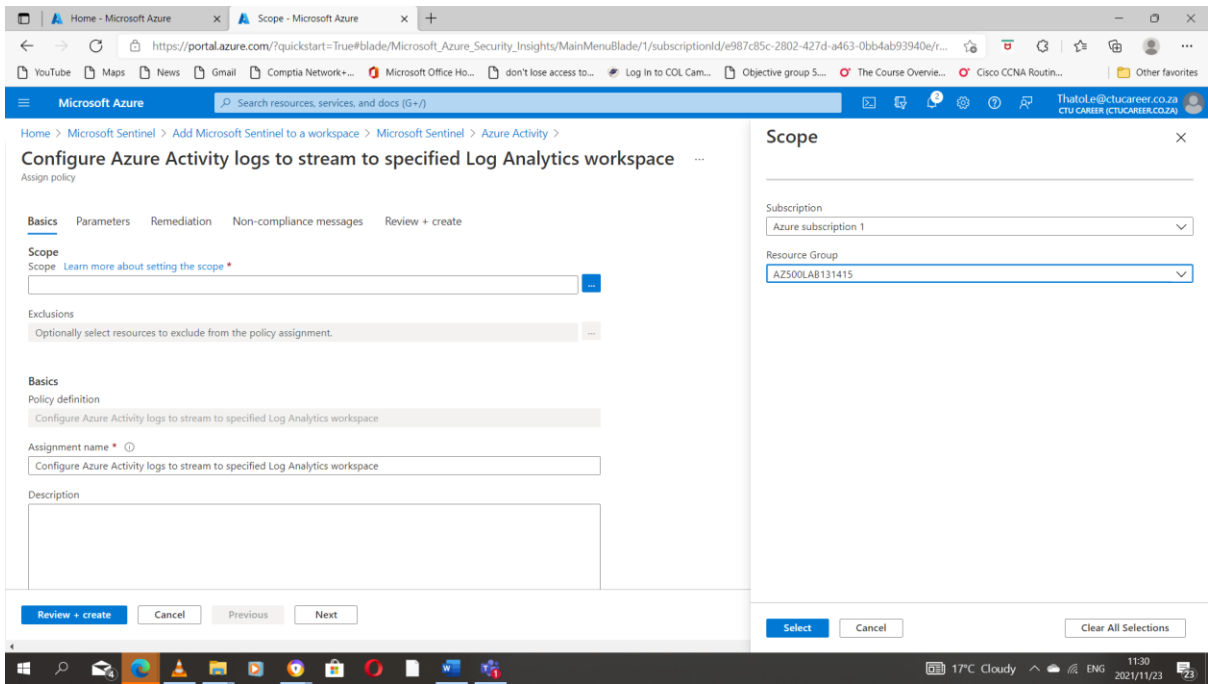
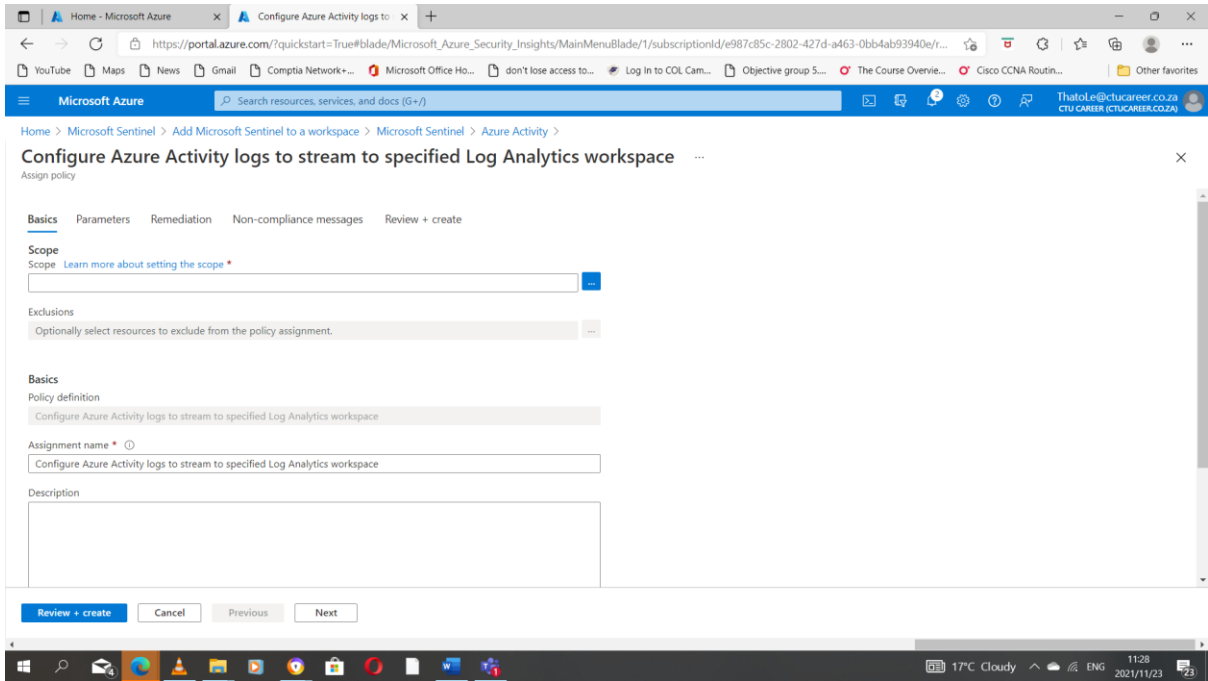
Basics
Policy definition
Configure Azure Activity logs to stream to specified Log Analytics workspace

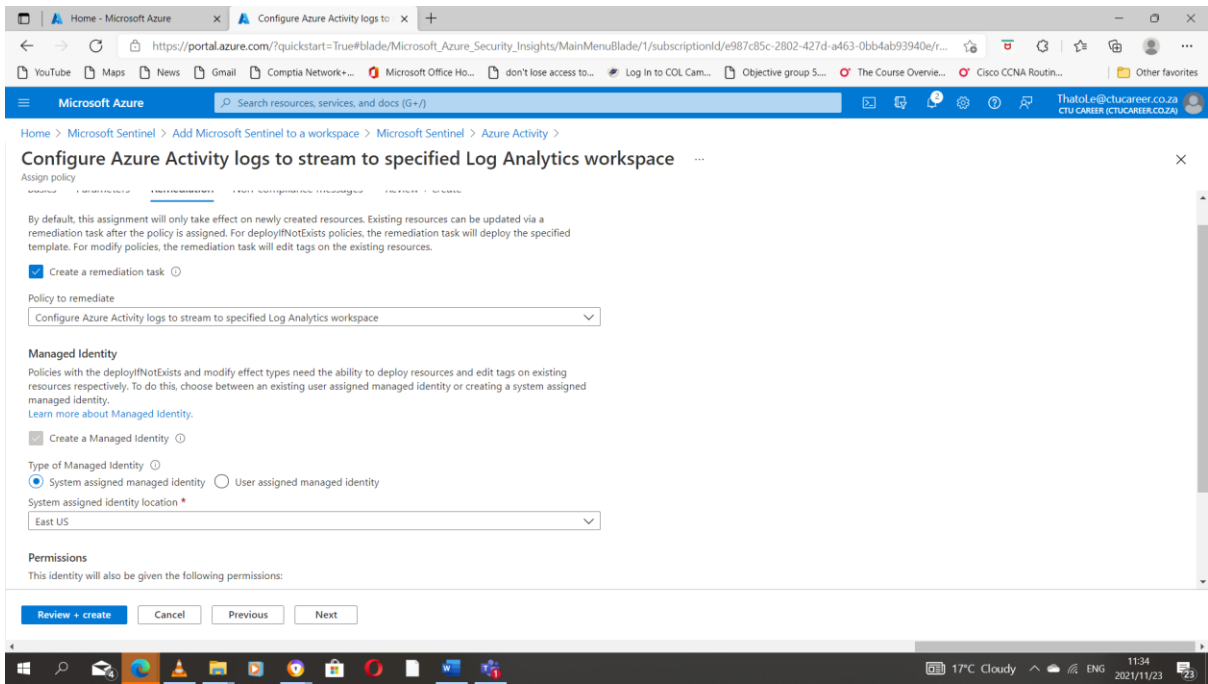
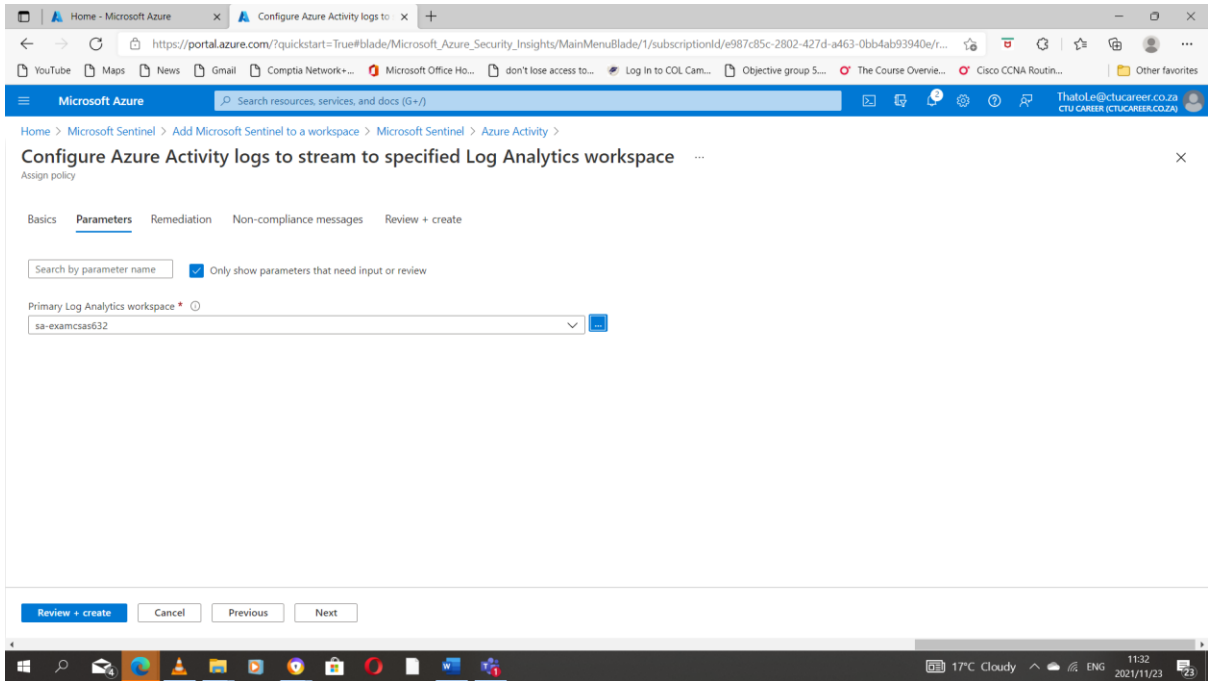
Assignment name *
Configure Azure Activity logs to stream to specified Log Analytics workspace

Description

[Review + create](#) [Cancel](#) [Previous](#) [Next](#)

17°C Cloudy 11:26 2021/11/23





Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel > Azure Activity > Configure Azure Activity logs to stream to specified Log Analytics workspace

Assign policy

Basics Parameters Remediation Non-compliance messages **Review + create**

Basics

Scope	Azure subscription 1/AZ500LAB131415
Exclusions	--
Policy definition	Configure Azure Activity logs to stream to specified Log Analytics workspa...
Assignment name	Configure Azure Activity logs to stream to specified Log Analytics workspa...
Description	--
Policy enforcement	Enabled
Assigned by	Thato Legoale

Parameters

logAnalytics	/subscriptions/e987c85c-2802-427d-a463-0bb4ab93940e/resourcegroups...
--------------	---

Remediation

Create managed identity	Yes
System assigned identity location	eastus
Create a remediation task	Yes

Non-compliance messages

Create Cancel Previous Next

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel > Azure Activity

Azure Activity

Not connected Status Microsoft Provider Last Log Received

Description
Azure Activity Log is a subscription log that provides insight into subscription-level events that occur in Azure, including events from Azure Resource Manager operational data, service health events, write operations taken on the resources in your subscription, and the status of activities performed in Azure.

Last data received
--

Related content
4 Workbooks 2 Queries 16 Analytics rules templates

Data received
100
80
60
40
[Go to log analytics](#)

Instructions Next steps

You don't have subscriptions using the legacy method, please move to [Disconnect All](#)

2. Connect your subscriptions through diagnostic settings new pipeline
This connector uses Azure Policy to apply a single Azure Subscription Log scope.
Follow the instructions below to create and apply a policy to all current this resource type.

Launch the Azure Policy Assignment wizard and follow the steps.

1. In the **Basics** tab, click the button with the three dots under **Sc...**
2. In the **Parameters** tab, choose your Microsoft Sentinel workspace as "True" all the log and metric types you want to ingest.
3. To apply the policy on your existing resources, select the **Remed...**

[Launch Azure Policy Assignment wizard >](#)

Notifications

More events in the activity log → Dismiss all ↓

- Creating policy assignment succeeded**
Creating policy assignment 'Configure Azure Activity logs to stream to specified Log Analytics workspace' in 'Azure subscription 1/AZ500LAB131415' was successful. Please note that the assignment takes around 30 minutes to take effect.
a few seconds ago
- Successfully added Microsoft Sentinel**
Successfully added Microsoft Sentinel to workspace 'sa-examcas632', it might take a few minutes for your workspace to appear in Microsoft Sentinel workspaces list
28 minutes ago
- Deployment succeeded**
Deployment 'sa-examcas632' to resource group 'AZ500LAB131415' was successful.
[Go to resource group](#) [Pin to dashboard](#)
30 minutes ago
- Optimize your cloud workloads with personalized recommendations**
With your Azure account, you get free, personalized recommendations to help you optimize your cloud workloads. Start with Azure Advisor recommendations—based on an analysis of your Azure usage—to improve cost-efficiency, security, reliability, performance, and operational excellence. [Learn more](#)

Azure Activity

Not connected Status | Microsoft Provider | Last Log Received

Description
Azure Activity Log is a subscription log that provides insight into subscription-level events that occur in Azure, including events from Azure Resource Manager operational data, service health events, write operations taken on the resources in your subscription, and the status of activities performed in Azure.

Last data received
--

Related content
4 Workbooks | 2 Queries | 16 Analytics rules templates

Data received
100
80
60
40
[Go to log analytics](#)

Instructions | Next steps

You don't have subscriptions using the legacy method, please move to [Disconnect All](#)

2. **Connect your subscriptions through diagnostic settings new pipeline**
This connector uses Azure Policy to apply a single Azure Subscription ID scope.
Follow the instructions below to create and apply a policy to all current this resource type.

Launch the **Azure Policy Assignment wizard** and follow the steps.

1. In the **Basics** tab, click the button with the three dots under **Scope**.
2. In the **Parameters** tab, choose your Microsoft Sentinel workspace as "True" all the log and metric types you want to ingest.
3. To apply the policy on your existing resources, select the **Remediation** option.

[Launch Azure Policy Assignment wizard](#)

Notifications

More events in the activity log → | [Dismiss all](#)

- ✓ **Remediation task creation succeeded**
Creating remediation task '54c58277-a996-40bc-bb74-d85b2f670014' was successful.
a few seconds ago
- ✓ **Role Assignments creation succeeded**
All role assignments were created successfully.
a few seconds ago
- ✓ **Creating policy assignment succeeded**
Creating policy assignment 'Configure Azure Activity logs to stream to specified Log Analytics workspace' in 'Azure subscription 1/AZ500LAB131415' was successful. Please note that the assignment takes around 30 minutes to take effect.
a few seconds ago
- ✓ **Successfully added Microsoft Sentinel**
Successfully added Microsoft Sentinel to workspace 'sa-examcsas632', it might take a few minutes for your workspace to appear in Microsoft Sentinel workspaces list
28 minutes ago
- ✓ **Deployment succeeded**
Deployment 'sa-examcsas632' to resource group 'AZ500LAB131415' was successful.

Task 3: Create a rule that uses the Azure Activity data connector.

Microsoft Sentinel | Analytics

Selected workspace: 'sa-examcsas632'

Search (Ctrl+F) | Create | Refresh | Analytics efficiency workbook (Preview) | Enable | Disable | Delete | Import | Export | Guides & Feedback

40 Active rules

Rules by severity: High (1) | Medium (0) | Low (0) | Informational (39)

Active rules | Rule templates

Search | Severity: All | Rule Type: All | Status: All | Tactics: All

Severity	Name	Rule type	Status	Tactics
High	Advanced Multistage Attack Detection	Fusion	Enabled	
Informational	(Preview) Anomalous Account Creation	Anomaly	Enabled	
Informational	(Preview) Anomalous Azure AD sign-in sessions	Anomaly	Enabled	
Informational	(Preview) Anomalous Code Execution	Anomaly	Enabled	
Informational	(Preview) Anomalous local account creation	Anomaly	Enabled	
Informational	(Preview) Anomalous scanning activity	Anomaly	Enabled	
Informational	(Preview) Anomalous Sign In	Anomaly	Enabled	

< Previous | Page 1 of 1 | Next >

No analytics rules selected
Select an analytics rule to view more details

Home - Microsoft Azure x Microsoft Sentinel - Microsoft A: x

https://portal.azure.com/?quickstart=True#blade/Microsoft_Azure_Security_Insights/MainMenuBlade/4/subscriptionId/e987c85c-2802-427d-a463-0bb4ab93940e/r...

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel

Microsoft Sentinel | Analytics

Selected workspace: 'sa-examcsas632'

Search (Ctrl+/)

+ Create Refresh Analytics efficiency workbook (Preview) Enable Disable Delete Import Export Guides & Feedback

40 Active rules

Rules by severity: High (1) Medium (0) Low (0) Informational (39)

Active rules Rule templates

Search Severity: All Rule Type: All Tactics: All More (1)

Severity	Name	Rule type	Data sources	Tactics
High	TEARDROP memory-only dropper	Scheduled	Microsoft 365 Defend...	
High	Exchange SSRF Autosdiscover Proxy...	Scheduled	Azure Monitor (IIS)	Initial Access
High	Alsld Password Guessing	Scheduled	Alsld for Active Direct...	Credential Access
High	User login from different countries ...	Scheduled		Initial Access
High	Authentication Methods Changed f...	Scheduled	Azure Active Directory	Persistence
High	SUNBURST and SUPERNOVA back...	Scheduled		
High	Solorigate Named Pipe	Scheduled	Security Events ... +1	
High	Azure VM Run Command operatio...	Scheduled	Azure Activity	

< Previous Page 1 of 0 Next >

Antivirus Expired
Your Black Friday Discount Is Live
Enable Virus Protection Now
TotalAV
Open

17°C Cloudy 11:56 2021/11/23

Home - Microsoft Azure x Microsoft Sentinel - Microsoft A: x

https://portal.azure.com/?quickstart=True#blade/Microsoft_Azure_Security_Insights/MainMenuBlade/4/subscriptionId/e987c85c-2802-427d-a463-0bb4ab93940e/r...

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel

Microsoft Sentinel | Analytics

Selected workspace: 'sa-examcsas632'

Search (Ctrl+/)

+ Create Refresh Analytics efficiency workbook (Preview) Enable Disable Delete Import Export Guides & Feedback

40 Active rules

Rules by severity: High (1) Medium (0) Low (0) Informational (39)

Active rules Rule templates

Search Suspicious number of resource creation o... Severity: All Rule Type: All Tactics: All More (1)

Severity	Name	Rule type	Data sources	Tactics
Medium	Suspicious number of resource creati...	Scheduled	Azure Activity	Impact

< Previous Page 1 of 1 Next >

Suspicious number of resource creation or deploy...

Medium Severity Scheduled Rule Type

Impact

Rule query

```
let s2operationNames = dynamic(
["microsoft.compute/virtualMachines/write", "microsoft.resources/deployments/write"]);
let starttime = 7d;
let endtime = 1d;
```

Note:

- You haven't used this template yet; You can use it to create analytics rules.
- One or more data sources used by this rule is missing. This might limit the functionality of the rule.

Create rule

17°C Cloudy 11:58 2021/11/23

Home - Microsoft Azure x Analytics rule wizard - Create new rule from template x +

https://portal.azure.com/?quickstart=TRUE#blade/Microsoft_Azure_Security_Insights/MainMenuBlade/4/subscriptionId/e987c85c-2802-427d-a463-0bb4ab93940e/r...

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel >

Analytics rule wizard - Create new rule from template

Suspicious number of resource creation or deployment activities

General Set rule logic Incident settings (Preview) Automated response Review and create

Create an analytics rule that will run on your data to detect threats.

Analytics rule details

Name *
Suspicious number of resource creation or deployment activities

Description
Indicates when an anomalous number of VM creations or deployment activities occur in Azure via the AzureActivity log. The anomaly detection identifies activities that have occurred both since the start

Tactics
Impact

Severity
Medium

Status
Enabled Disabled

Next: Set rule logic >

17°C Cloudy 11:59 2021/11/23

Home - Microsoft Azure x Analytics rule wizard - Create new rule from template x +

https://portal.azure.com/?quickstart=TRUE#blade/Microsoft_Azure_Security_Insights/MainMenuBlade/4/subscriptionId/e987c85c-2802-427d-a463-0bb4ab93940e/r...

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel >

Analytics rule wizard - Create new rule from template

Suspicious number of resource creation or deployment activities

General Set rule logic Incident settings (Preview) Automated response Review and create

Define the logic for your new analytics rule.

Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

One or more entity mappings have been defined under the new version of Entity Mappings. These will not appear in the query code. Any entity mappings defined in the query code will be disregarded.

```
let sOperationNames = dynamic(["microsoft.compute/virtualMachines/write", "microsoft.resources/deployments/write"]);
let starttime = 7d;
let endtime = 1d;
AzureActivity
| where TimeGenerated between (startofday(ago(starttime)) .. startofday(ago(endtime)))
```

View query results >

Alert enrichment (Preview)

Entity mapping

Map up to five entities recognized by Microsoft Sentinel from the appropriate fields available in your query results. This enables Microsoft Sentinel to re-normalize and re-classify the data in these fields for further analysis.

Results simulation

This chart shows the results of the last 50 evaluations of the defined analytics rule. Click a point on the chart to display the raw events for that point in time.

Test with current data

Define a valid analytics rule configuration and click 'Test with current data' to test your rule with current data in your workspace.

Previous Next: Incident settings (Preview) >

17°C Cloudy 11:59 2021/11/23

Home > Microsoft Sentinel > Analytics rule wizard - Create new rule from template

Suspicious number of resource creation or deployment activities

General Set rule logic **Incident settings (Preview)** Automated response Review and create

Incident settings
 Microsoft Sentinel alerts can be grouped together into an incident that should be looked into. You can set whether the alerts that are triggered by this analytics rule should generate incidents.

Create incidents from alerts triggered by this analytics rule
 Enabled Disabled

Alert grouping
 Set how the alerts that are triggered by this analytics rule, are grouped into incidents. Grouping alerts into incidents provides the context you need to respond and reduces the noise from single alerts.

Group related alerts, triggered by this analytics rule, into incidents
 Enabled Disabled

Limit the group to alerts created within the selected time frame
 5 Hours

Group alerts triggered by this analytics rule into a single incident by
 Grouping alerts into a single incident if all the entities match (recommended)
 Resolving all alerts referenced by this rule into a single incident

Previous **Next: Automated response >**

Next: Automated response >

17°C Cloudy 12:01 2021/11/23

Home > Microsoft Sentinel > Analytics rule wizard - Create new rule from template

Suspicious number of resource creation or deployment activities

General Set rule logic Incident settings (Preview) **Automated response** Review and create

Alert automation
 Select a playbook to run when a new alert is generated from this analytics rule. The playbook will receive the alert as its input. Only playbooks configured with the alert trigger can be selected.

0 selected

Name	Status
No playbooks selected	

Incident automation (preview)
 View all automation rules that will be triggered by this analytics rule and create new automation rules. The automation rule will receive the incident as its input, as will any playbooks called by the automation rule. Only playbooks configured with the incident trigger can be called by automation rules.

+ Add new

Previous **Next: Review >**

17°C Cloudy 12:02 2021/11/23

Home - Microsoft Azure x Analytics rule wizard - Create new rule x

https://portal.azure.com/?quickstart=TRUE#blade/Microsoft_Azure_Security_Insights/MainMenuBlade/4/subscriptionId/e987c85c-2802-427d-a463-0bb4ab93940e/r...

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel >

Analytics rule wizard - Create new rule from template

Suspicious number of resource creation or deployment activities

Validation passed.

General Set rule logic Incident settings (Preview) Automated response **Review and create**

Analytics rule details

Name Suspicious number of resource creation or deployment activities

Description Indicates when an anomalous number of VM creations or deployment activities occur in Azure via the AzureActivity log. The anomaly detection identifies activities that have occurred both since the start of the day 1 day ago and the start of the day 7 days ago. The start of the day is considered 12am UTC time.

Tactics **Impact**

Severity **Medium**

Status **Enabled**

Analytics rule settings

Rule query

```
let szOperationNames = dynamic(["microsoft.compute/virtualMachines/write", "microsoft.resources/deployments/write"]);
let starttime = 7d;
let endtime = 1d;
AzureActivity
| where TimeGenerated between (startofday(ago(starttime)) .. startofday(ago(endtime)))
```

Previous Create

17°C Cloudy 12:03 2021/11/23

Home - Microsoft Azure x Microsoft Sentinel - Microsoft A x

https://portal.azure.com/?quickstart=TRUE#blade/Microsoft_Azure_Security_Insights/MainMenuBlade/4/subscriptionId/e987c85c-2802-427d-a463-0bb4ab93940e/r...

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel

Microsoft Sentinel | Analytics

Selected workspace: sa-examcas632

Analytics rule saved
Analytics rule 'Suspicious number of resource creation or deployment activities' saved successfully

40 Active rules

Rules by severity: High (1) Medium (0) Low (0) Informational (39)

Active rules Rule templates

Search

Severity: All Rule Type: All Status: All Tactics: All

Severity	Name	Rule type	Status	Tactics
High	Advanced Multistage Attack Detection	Fusion	Enabled	
Informational	(Preview) Anomalous Account Creation	Anomaly	Enabled	
Informational	(Preview) Anomalous Azure AD sign-in sessions	Anomaly	Enabled	
Informational	(Preview) Anomalous Code Execution	Anomaly	Enabled	
Informational	(Preview) Anomalous local account creation	Anomaly	Enabled	
Informational	(Preview) Anomalous scanning activity	Anomaly	Enabled	
Informational	(Preview) Anomalous Sign In	Anomaly	Enabled	

No analytics rules selected
Select an analytics rule to view more details

17°C Cloudy 12:03 2021/11/23

Task 4: Create a playbook

The screenshot shows the Microsoft Azure portal interface for creating a custom deployment. The browser address bar displays `https://portal.azure.com/?quickstart=True#create/Microsoft.Template`. The page title is "Custom deployment" with a subtitle "Deploy from a custom template".

Navigation options include "Select a template", "Basics", and "Review + create". A brief description states: "Automate deploying resources with Azure Resource Manager templates in a single, coordinated operation. Create or select a template below to get started. Learn more about template deployment".

There is a link to "Build your own template in the editor". Under "Common templates", several options are listed: "Create a Linux virtual machine", "Create a Windows virtual machine", "Create a web app", "Create a SQL database", and "Azure landing zone".

The "Start with a quickstart template or template spec" section has two radio buttons: "Quickstart template" (selected) and "Template spec". Below this is a dropdown menu for "Quickstart template (disclaimer)".

The Windows taskbar at the bottom shows the system tray with a temperature of 17°C, cloud status, and the date/time: 12:11 on 2021/11/23.

The screenshot shows the "Edit template" page in the Microsoft Azure portal. The browser address bar displays `https://portal.azure.com/?quickstart=True#create/Microsoft.Template`. The page title is "Edit template" with a subtitle "Edit your Azure Resource Manager template".

Navigation options include "Add resource", "Quickstart template", "Load file", and "Download". On the left, there are sections for "Parameters (0)", "Variables (0)", and "Resources (0)".

The main area is a code editor showing the following JSON template structure:

```
1 {
2   "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
3   "contentVersion": "1.0.0.0",
4   "parameters": {},
5   "resources": []
6 }
```

At the bottom of the editor, there are "Save" and "Discard" buttons. The Windows taskbar at the bottom shows the system tray with a temperature of 17°C, cloud status, and the date/time: 12:13 on 2021/11/23.

Home - Microsoft Azure x Edit template - Microsoft Azure x +

https://portal.azure.com/?quickstart=True#create/Microsoft.Template

Microsoft Azure Search resources, services, and docs (G+)

Home > Custom deployment >

Edit template

Edit your Azure Resource Manager template

+ Add resource ↑ Quickstart template ↑ Load file ↓ Download

Upload Completed for changeincidentseverity.json
6.83 KIB | "Streaming upload"

```
1 {
2   "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
3   "contentVersion": "1.0.0.0",
4   "metadata": {
5     "comments": "This playbook will change Incident Severity based on specific username that is part of the Incident user entity.",
6     "author": "Yaniv Shasha"
7   },
8   "parameters": {
9     "playbookName": {
10      "defaultValue": "Change-Incident-Severity",
11      "type": "string"
12    },
13    "userName": {
14      "defaultValue": "<username>@<domain>",
15      "type": "string"
16    }
17  },
18  "variables": {
19    "azureSentinelConnectionName": "[concat('azuresentinel-', parameters('playbookName'))]"
20  },
21  "resources": [
22    {
23      "type": "Microsoft.Web/connections",
```

Save Discard

17°C Cloudy 12:14 2021/11/23

Home - Microsoft Azure x Custom deployment - Microsoft x +

https://portal.azure.com/?quickstart=True#create/Microsoft.Template

Microsoft Azure Search resources, services, and docs (G+)

Home >

Custom deployment

Deploy from a custom template

Select a template Basics Review + create

Template

Customized template 2 resources

Edit template Edit parameters Visualize

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription Azure subscription 1

Resource group Loading... Create new

Instance details

Region Loading...

Playbook Name Change-Incident-Severity

User Name <username>@<domain>

Review + create < Previous Next: Review + create >

17°C Cloudy 12:18 2021/11/23

Home - Microsoft Azure x Custom deployment - Microsoft x +

https://portal.azure.com/?quickstart=True#create/Microsoft.Template

Microsoft Azure Search resources, services, and docs (G+)

Home > Custom deployment ...

Deploy from a custom template

Select a template Basics Review + create

Template

Customized template 2 resources

Edit template Edit parameters Visualize

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription Azure subscription 1

Resource group AZ500LAB131415

Create new

Instance details

Region (US) East US

Playbook Name Change-Incident-Severity

User Name ThatoLe@ctucareer.co.za

Review + create < Previous Next: Review + create >

17°C Cloudy 12:20 2021/11/23

Home - Microsoft Azure x Custom deployment - Microsoft x +

https://portal.azure.com/?quickstart=True#create/Microsoft.Template

Microsoft Azure Search resources, services, and docs (G+)

Home > Custom deployment ...

Deploy from a custom template

Validation Passed

Select a template Basics Review + create

Summary

Customized template 2 resources

Terms

Azure Marketplace Terms Azure Marketplace

By clicking "Create," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated with the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the [Azure Marketplace Terms](#) for additional terms.

Deploying this template will create one or more Azure resources or Marketplace offerings. You acknowledge that you are responsible for reviewing the applicable pricing and legal terms associated with all resources and offerings deployed as part of this template. Prices and associated legal terms for any Marketplace offerings can be found in the [Azure Marketplace](#); both are subject to change at any time prior to deployment.

Create < Previous Next

17°C Cloudy 12:21 2021/11/23

Home - Microsoft Azure | Microsoft.Template-2021112312 | Overview

Deployment

Search (Ctrl+F) | Delete | Cancel | Redeploy | Refresh

We'd love your feedback! →

✓ Your deployment is complete

Deployment name: Microsoft.Template-20211123122125
 Subscription: Azure subscription 1
 Resource group: AZ500LAB131415

Start time: 11/23/2021, 12:21:49 PM
 Correlation ID: e7abc5c2-4dda-49ce-92ad-7aff002bd47a

Deployment details (Download)
 Next steps
 Go to resource group

Microsoft Defender for Cloud
 Secure your apps and infrastructure
 Go to Azure security center >

Free Microsoft tutorials
 Start learning today >

Work with an expert
 Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
 Find an Azure expert >

17°C Cloudy | 12:22 2021/11/23

Home - Microsoft Azure | Resource groups - Microsoft Azure | Overview

Subscription == all | Location == all | Add filter

Showing 1 to 1 of 1 records.

Name ↑	Subscription ↑	Location ↑
AZ500LAB131415	Azure subscription 1	East US

< Previous | Page 1 of 1 | Next >

17°C Cloudy | 12:23 2021/11/23

Home - Microsoft Azure > AZ500LAB131415 - Microsoft Azure

https://portal.azure.com/?quickstart=True#@ctucareer.co.za/resource/subscriptions/e987c85c-2802-427d-a463-0bb4ab93940e/resourceGroups/AZ500LAB131415/...

Microsoft Azure Search resources, services, and docs (G+)

Home > Resource groups > AZ500LAB131415

Resource group

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Deployments

Security

Policies

Properties

Locks

Cost Management

Cost analysis

Cost alerts (preview)

Budgets

Essentials

Subscription (Move) Azure subscription 1

Subscription ID e987c85c-2802-427d-a463-0bb4ab93940e

Location East US

Deployments 2 Succeeded

Tags (Edit) Click here to add tags

Resources Recommendations

Filter for any field...

Type == all X Location == all X Add filter

Showing 1 to 4 of 4 records. Show hidden types

No grouping List view

Name	Type	Location
azuresentinel-change-incident-severity	API Connection	East US
change-incident-severity	Logic app	East US
sa-examcsas632	Log Analytics workspace	East US
securityinsights(sa-examcsas632)	Solution	East US

Page 1 of 1

https://portal.azure.com/?quickstart=True#@ctucareer.co.za/resource/subscriptions/e987c85c-2802-427d-a463-0bb4ab93940e/resourceGroups/AZ500LAB131415/properties

17°C Cloudy 12:23 2021/11/23

Home - Microsoft Azure > Change-Incident-Severity - Microsoft Azure

https://portal.azure.com/?quickstart=True#@ctucareer.co.za/resource/subscriptions/e987c85c-2802-427d-a463-0bb4ab93940e/resourceGroups/AZ500LAB131415/...

Microsoft Azure Search resources, services, and docs (G+)

Home > Resource groups > AZ500LAB131415 > Change-Incident-Severity

Logic app

Run Trigger Refresh Edit Delete Disable Update Schema Clone Open in mobile Export Feedback

Introducing the new portable Logic Apps runtime that supports local development and debugging. Click to learn more. →

Essentials

Resource group (Move) : AZ500LAB131415

Location : East US

Subscription (Move) : Azure subscription 1

Subscription ID : e987c85c-2802-427d-a463-0bb4ab93940e

Definition : 1 trigger, 3 actions

Status : Enabled

Runs last 24 hours : 0 successful, 0 failed

Integration Account : ...

Get started Runs history Trigger history Metrics

All Start time earlier than Pick a date Pick a time

Specify the run identifier to open monitor view directly

Status	Start time	Identifier	Duration	Static Results
No runs				

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Development Tools

Logic app designer

Logic app code view

Versions

API connections

Quick start guides

Settings

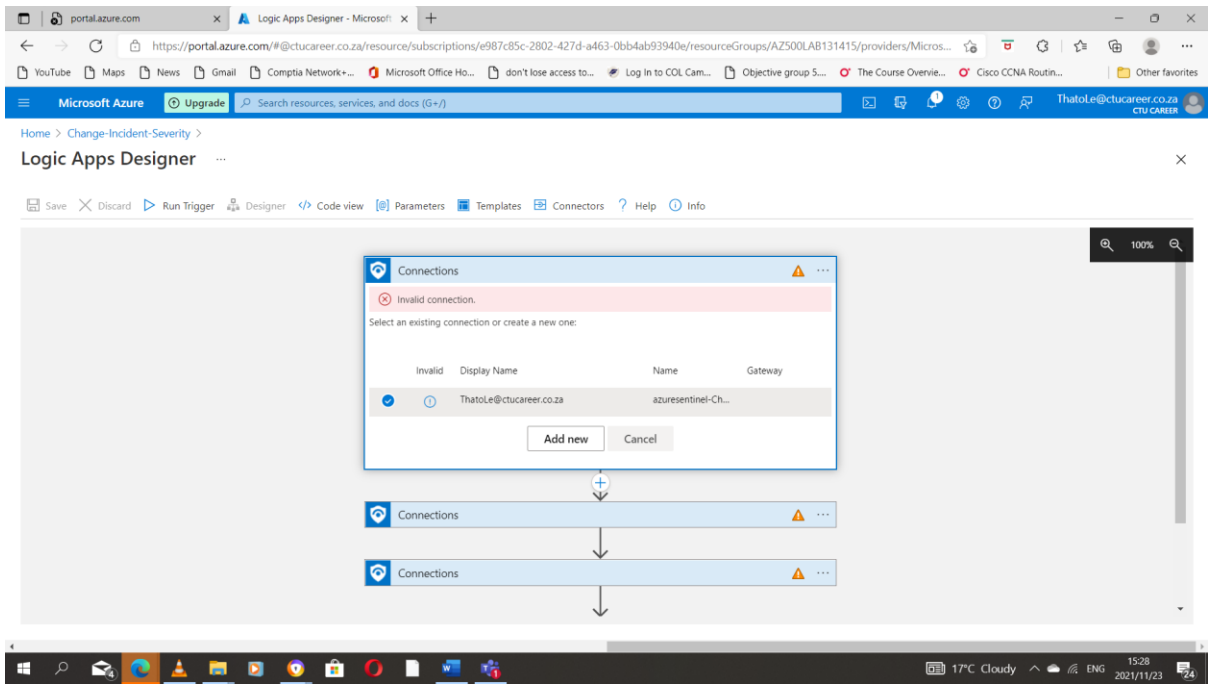
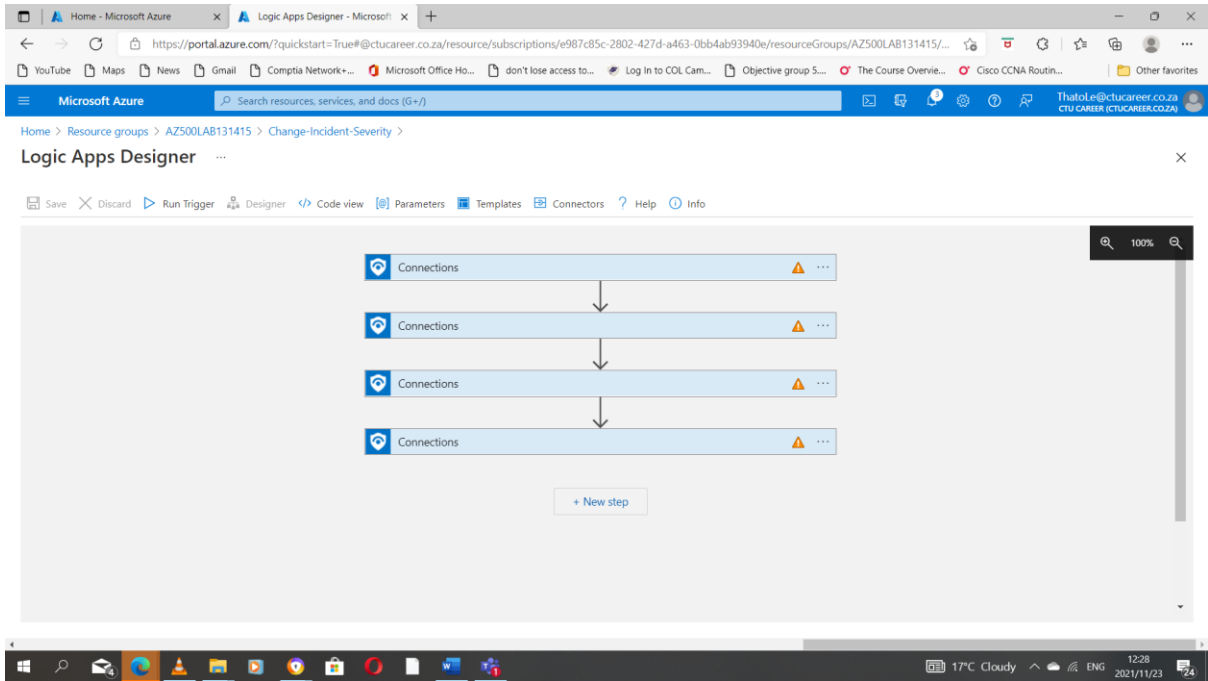
Workflow settings

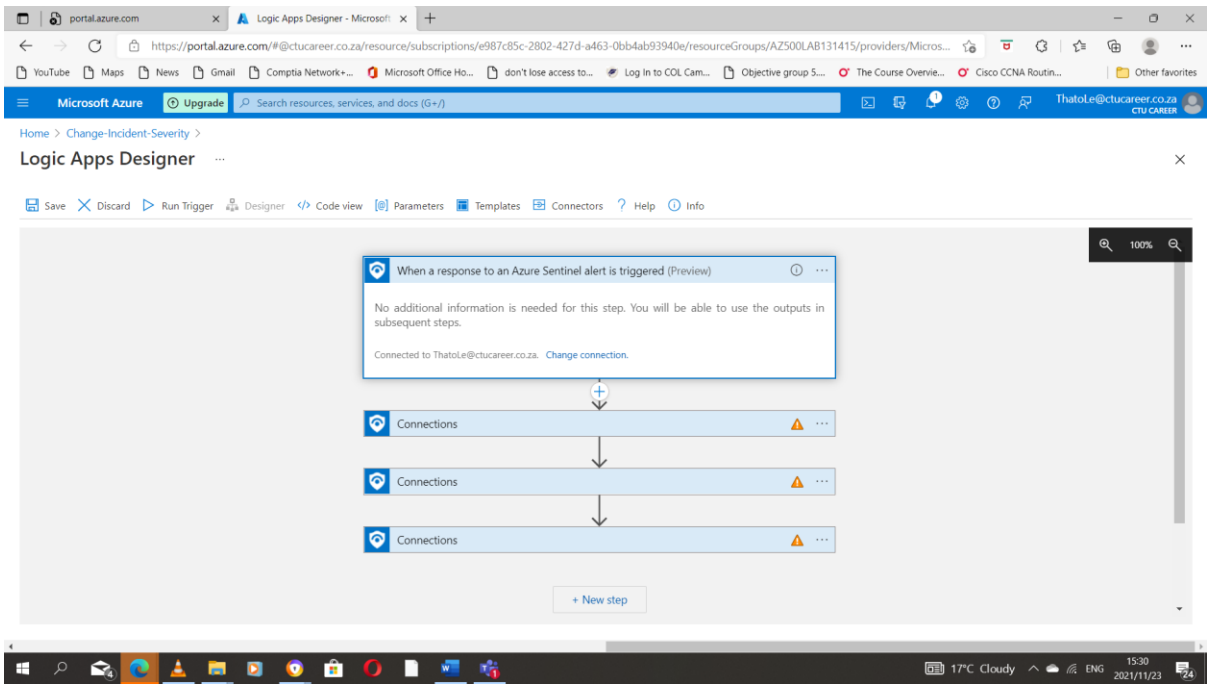
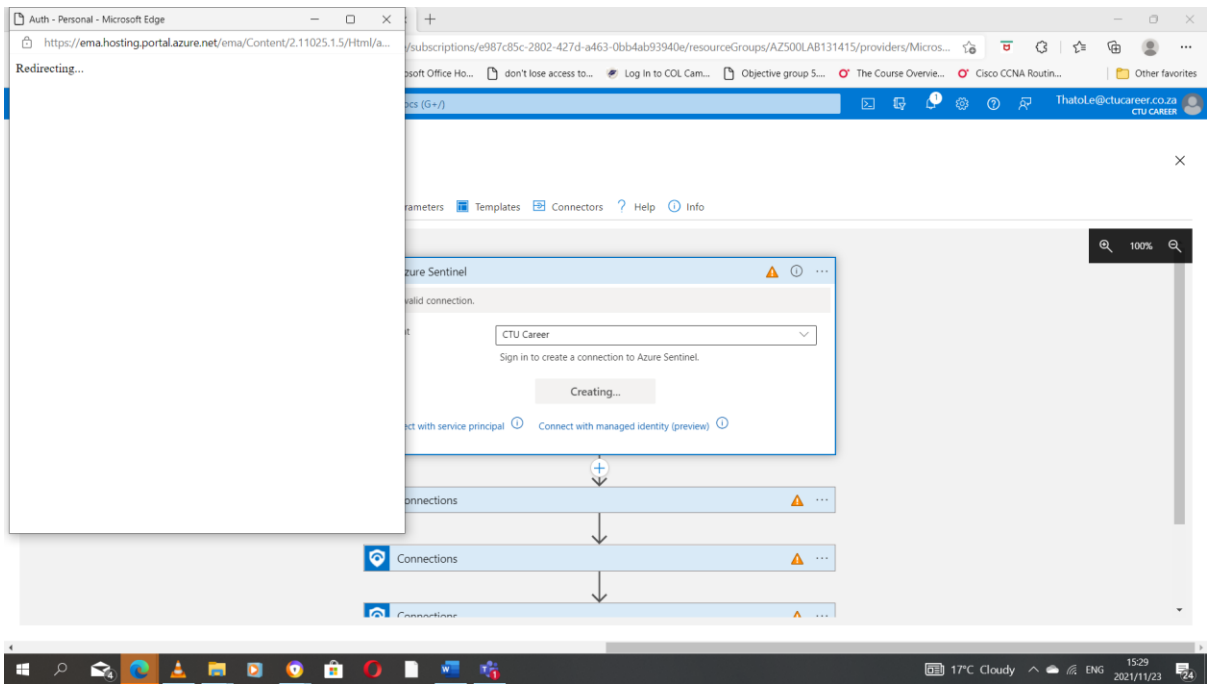
Authorization

Access keys

Identity

17°C Cloudy 12:28 2021/11/23





portal.azure.com x Logic Apps Designer - Microsoft x +

https://portal.azure.com/#@ctucareer.co.za/resource/subscriptions/e987c85c-2802-427d-a463-0bb4ab93940e/resourceGroups/AZ500LAB131415/providers/Micros...

Microsoft Azure Upgrade Search resources, services, and docs (G+)

Home > Change-Incident-Severity >

Logic Apps Designer

Save Discard Run Trigger Designer Code view Parameters Templates Connectors Help Info

Alert - Get incident (Preview)

- * Specify subscription id: Subscription ID x
- * Specify resource group: Resource group x
- * Specify workspace id: Workspace ID x
- * Specify alert id: System alert ID x

Connected to ThatoLe@ctucareer.co.za. Change connection.

Connections

Connections

+ New step

17°C Cloudy 15:32 2021/11/23

portal.azure.com x Logic Apps Designer - Microsoft x +

https://portal.azure.com/#@ctucareer.co.za/resource/subscriptions/e987c85c-2802-427d-a463-0bb4ab93940e/resourceGroups/AZ500LAB131415/providers/Micros...

Microsoft Azure Upgrade Search resources, services, and docs (G+)

Home > Change-Incident-Severity >

Logic Apps Designer

Save Discard Run Trigger Designer Code view Parameters Templates Connectors Help Info

Alert - Get accounts (Preview)

- * Entities list: Entities x

Connected to ThatoLe@ctucareer.co.za. Change connection.

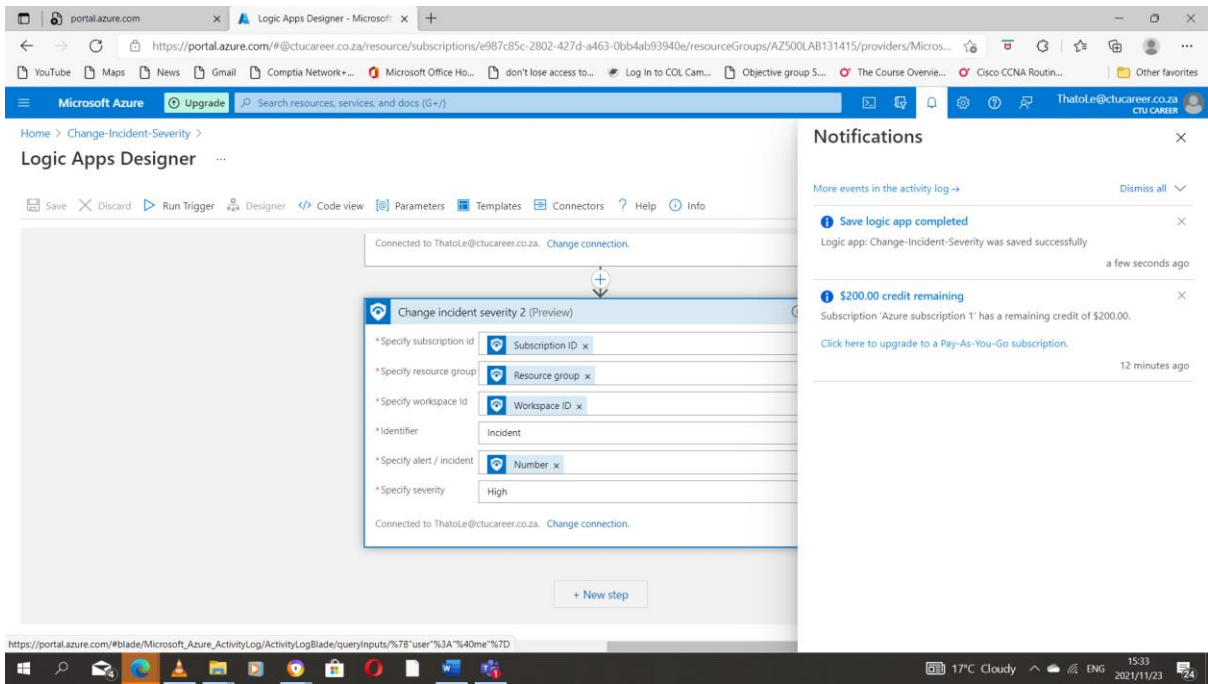
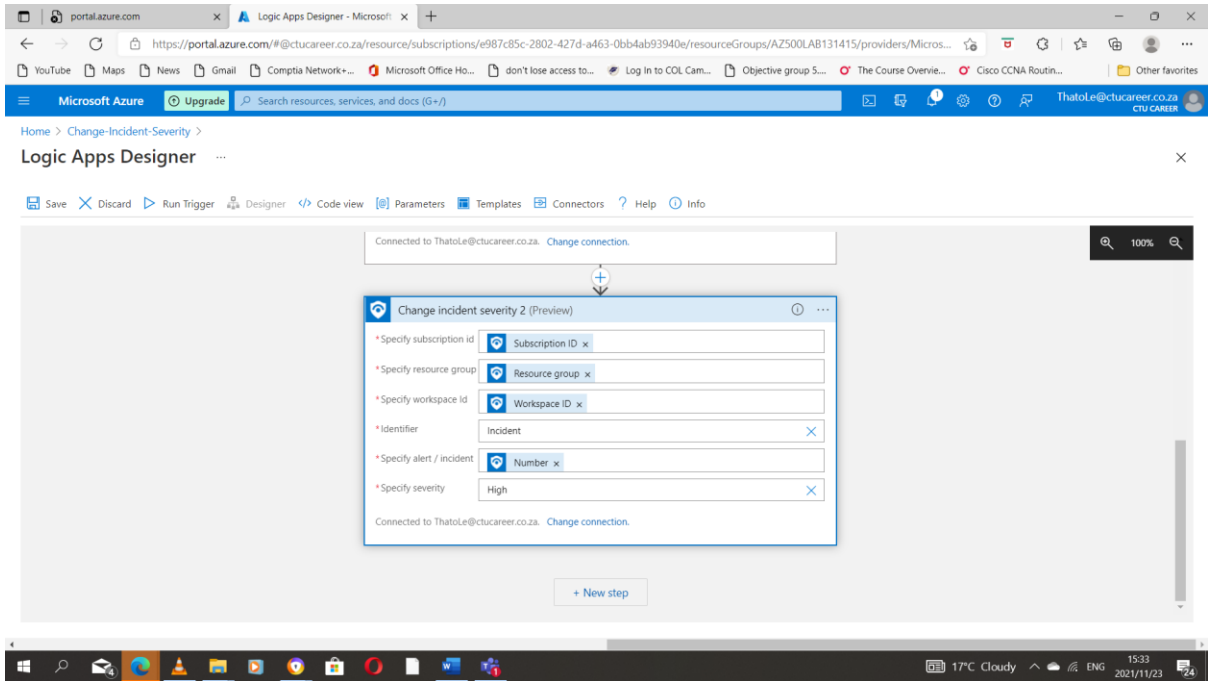
Change incident severity 2 (Preview)

- * Specify subscription id: Subscription ID x
- * Specify resource group: Resource group x
- * Specify workspace id: Workspace ID x
- * Identifier: Incident x
- * Specify alert / incident: Number x
- * Specify severity: High x

Specify severity

Connected to ThatoLe@ctucareer.co.za. Change connection.

17°C Cloudy 15:32 2021/11/23



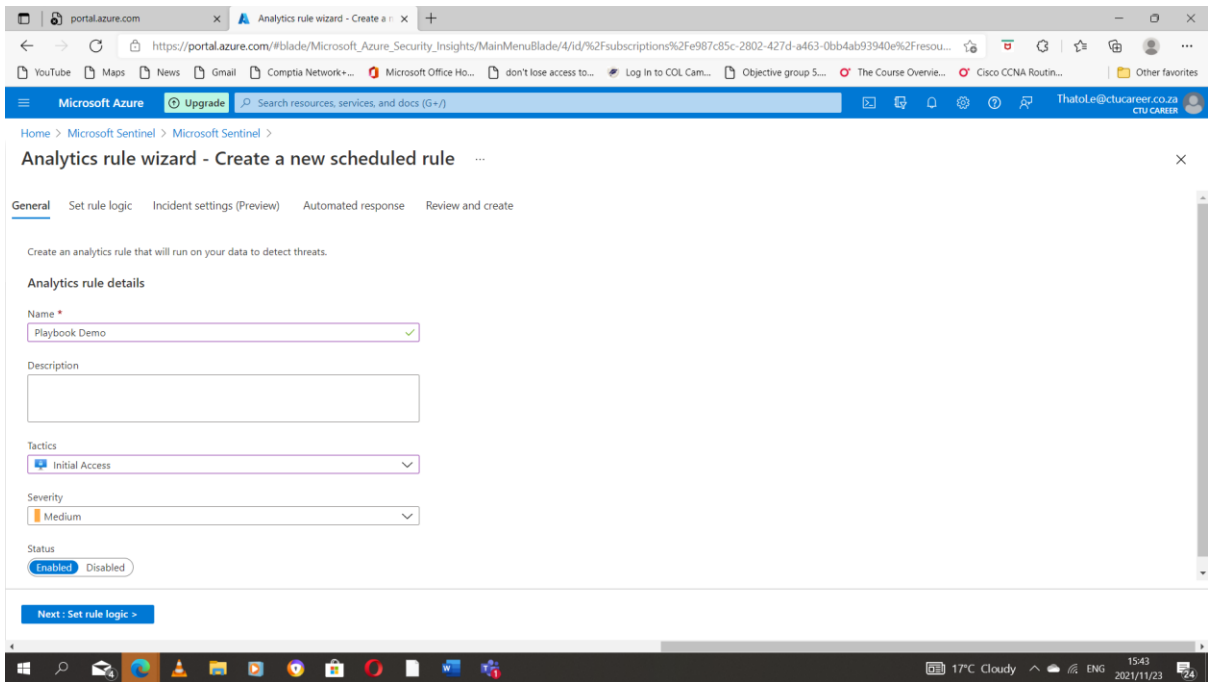
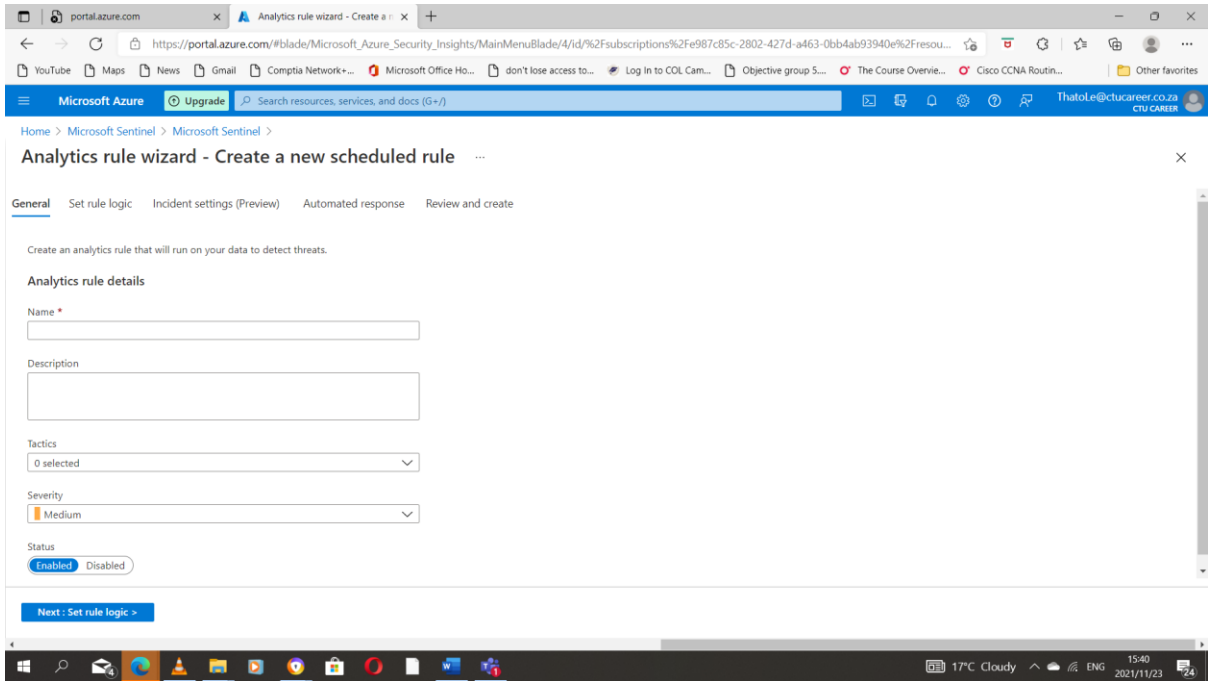
Task 5 Create a custom alert and configure a playbook as an automated response

The screenshot shows the Microsoft Sentinel console interface. At the top, there are navigation options like 'Home', 'Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', 'View incidents', and 'Feedback'. Below this is a search bar and filter options: 'Subscription == all', 'Resource group == all', and 'Location == all'. A table displays one record for a resource named 'sa-examcsas632' with details for resource group, location, subscription, and directory.

Name	Resource group	Location	Subscription	Directory
sa-examcsas632	az500lab131415	East US	Azure subscription 1	CTU Career

The screenshot shows the Microsoft Sentinel Analytics console. It features a search bar, navigation options, and a 'Rules by severity' bar. A table lists active rules with columns for severity, name, rule type, status, and tactics. A sidebar on the left contains navigation options like 'Incidents', 'Workbooks', and 'Settings'.

Severity	Name	Rule type	Status	Tactics
High	Advanced Multistage Attack Detection	Fusion	Enabled	
Medium	Suspicious number of resource creation or depl...	Scheduled	Enabled	
Informational	(Preview) Anomalous Account Creation	Anomaly	Enabled	
Informational	(Preview) Anomalous Azure AD sign-in sessions	Anomaly	Enabled	
Informational	(Preview) Anomalous Code Execution	Anomaly	Enabled	
Informational	(Preview) Anomalous local account creation	Anomaly	Enabled	
Informational	(Preview) Anomalous username activity	Anomaly	Enabled	



portal.azure.com x Analytics rule wizard - Create a new scheduled rule

https://portal.azure.com/#blade/Microsoft_Azure_Security_Insights/MainMenuBlade/4/id/%2Fsubscriptions%2F987c85c-2802-427d-a463-0bb4ab93940e%2Fresou...

Microsoft Azure Upgrade Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Microsoft Sentinel > Analytics rule wizard - Create a new scheduled rule

General **Set rule logic** Incident settings (Preview) Automated response Review and create

Define the logic for your new analytics rule.

Rule query
Any time details set here will be within the scope defined below in the Query scheduling fields.

```
AzureActivity
| where ResourceProviderValue == "Microsoft.Security"
| where OperationNameValue == "Microsoft.Security/locations/jitnetworkAccessPolicies/delete"
```

View query results >

Alert enrichment (Preview)

- Entity mapping
- Custom details
- Alert details

Previous **Next : Incident settings (Preview) >**

Results simulation
This chart shows the results of the last 50 evaluations of the defined analytics rule. Click a point on the chart to display the raw events for that point in time.

Test with current data

Define a valid analytics rule configuration and click 'Test with current data' to test your rule with current data in your workspace.

17°C Cloudy 15:45 2021/11/23

portal.azure.com x Analytics rule wizard - Create a new scheduled rule

https://portal.azure.com/#blade/Microsoft_Azure_Security_Insights/MainMenuBlade/4/id/%2Fsubscriptions%2F987c85c-2802-427d-a463-0bb4ab93940e%2Fresou...

Microsoft Azure Upgrade Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Microsoft Sentinel > Analytics rule wizard - Create a new scheduled rule

Entity mapping

- Custom details
- Alert details

Query scheduling

Run query every *
5 Minutes

Lookup data from the last *
5 Hours

Alert threshold

Generate alert when number of query results
is greater than 0

Event grouping

Configure how rule query results are grouped into alerts

Previous **Next : Incident settings (Preview) >**

current data in your workspace.

17°C Cloudy 15:46 2021/11/23

portal.azure.com x Analytics rule wizard - Create a new scheduled rule

https://portal.azure.com/#blade/Microsoft_Azure_Security_Insights/MainMenuBlade/4/id/%2Fsubscriptions%2F987c85c-2802-427d-a463-0bb4ab93940e%2Fresou...

Microsoft Azure Upgrade Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Microsoft Sentinel

Analytics rule wizard - Create a new scheduled rule

General Set rule logic **Incident settings (Preview)** Automated response Review and create

Incident settings

Microsoft Sentinel alerts can be grouped together into an incident that should be looked into. You can set whether the alerts that are triggered by this analytics rule should generate incidents.

Create incidents from alerts triggered by this analytics rule

Enabled Disabled

Alert grouping

Set how the alerts that are triggered by this analytics rule, are grouped into incidents. Grouping alerts into incidents provides the context you need to respond and reduces the noise from single alerts.

Group related alerts, triggered by this analytics rule, into incidents

Enabled Disabled

Limit the group to alerts created within the selected time frame

5 Hours

Group alerts triggered by this analytics rule into a single incident by

Grouping alerts into a single incident if all the entities match (recommended)

Generate all alerts triggered by this rule into a single incident

Previous Next: Automated response >

17°C Cloudy 15:47 2021/11/23

portal.azure.com x Analytics rule wizard - Create a new scheduled rule

https://portal.azure.com/#blade/Microsoft_Azure_Security_Insights/MainMenuBlade/4/id/%2Fsubscriptions%2F987c85c-2802-427d-a463-0bb4ab93940e%2Fresou...

Microsoft Azure Upgrade Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Microsoft Sentinel

Analytics rule wizard - Create a new scheduled rule

General Set rule logic Incident settings (Preview) **Automated response** Review and create

Alert automation

Select a playbook to run when a new alert is generated from this analytics rule. The playbook will receive the alert as its input. Only playbooks configured with the alert trigger can be selected.

Change-Incident-Severity

Name	Status
Change-Incident-Severity	Enabled

Incident automation (preview)

View all automation rules that will be triggered by this analytics rule and create new automation rules. The automation rule will receive the incident as its input, as will any playbooks called by the automation rule. Only playbooks configured with the incident trigger can be called by automation rules.

+ Add new

Previous Next: Review >

17°C Cloudy 15:51 2021/11/23

The screenshot shows the Microsoft Sentinel Analytics dashboard. At the top, there's a navigation bar with 'Home > Microsoft Sentinel > Analytics'. Below that, a search bar and a '42 Active rules' indicator are visible. A 'Rules by severity' chart shows 1 High, 2 Medium, 0 Low, and 39 Informational rules. The main area displays a table of active rules:

Severity	Name	Rule type	Status	Tactics
High	Advanced Multistage Attack Detection	Fusion	Enabled	
Medium	Playbook Demo	Scheduled	Enabled	
Medium	Suspicious number of resource creation or depl...	Scheduled	Enabled	
Informational	(Preview) Anomalous Account Creation	Anomaly	Enabled	
Informational	(Preview) Anomalous Azure AD sign-in sessions	Anomaly	Enabled	
Informational	(Preview) Anomalous Code Execution	Anomaly	Enabled	
Informational	(Preview) Anomalous local account creation	Anomaly	Enabled	

A notification at the top right says 'Analytics rule saved' and 'Analytics rule 'Playbook Demo' saved successfully'. A sidebar on the left contains navigation options like Incidents, Workbooks, Hunting, Notebooks, etc.

Task 6: Invoke an incident and review the associated actions.

Can't access the security centre due to the subscription I am using

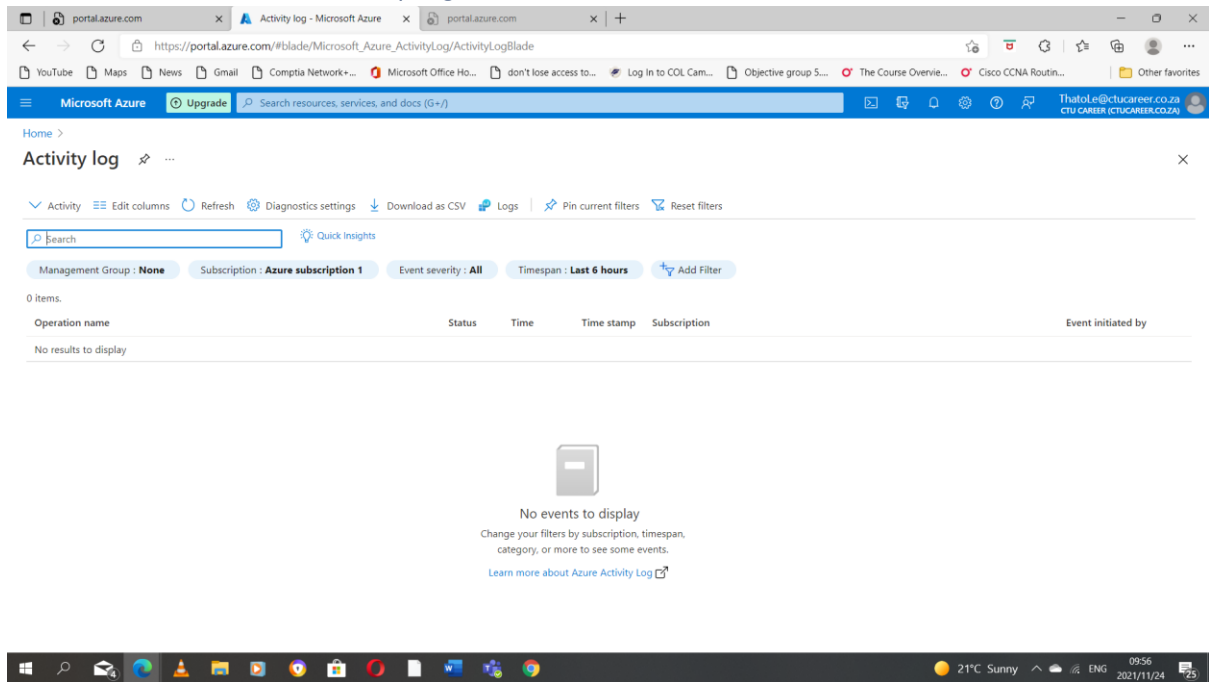
The screenshot shows an error message in the Azure portal: 'You do not have access'. Below the message is a 'Summary' box with the following details:

Property	Value
Session ID	1c36ec37bf64930bc7b9ca0c0d5c4ff
Resource ID	Not available
Extension	Microsoft_AAD_IAM
Content	SecurityMenuBlade
Error code	401

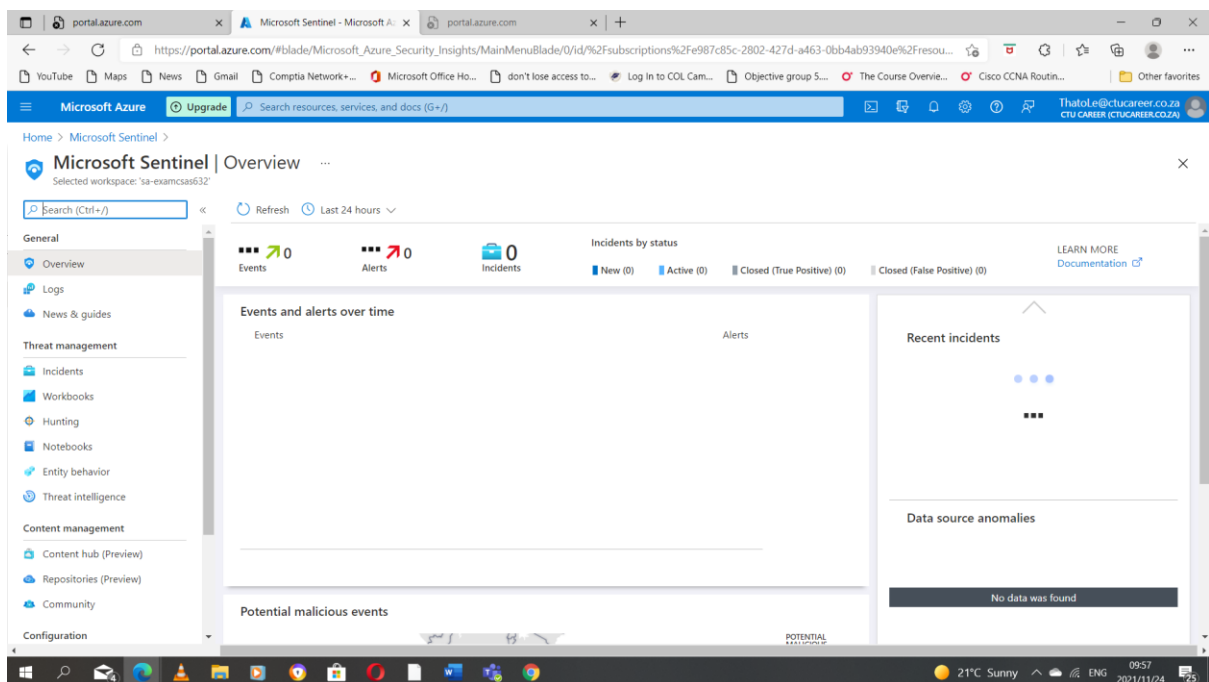
The error message also includes the text: 'User has no admin roles. Current directory do not allow non admin users to access portal'. The top of the page shows the user is logged in as 'ThatoLe@ctucareer.co.za'.

2. On the Security Center | Azure Defender blade, click Just-in-time vm access section.
Due to I can't access the security centre the assignment will not be full when it comes to entering and working with security center.

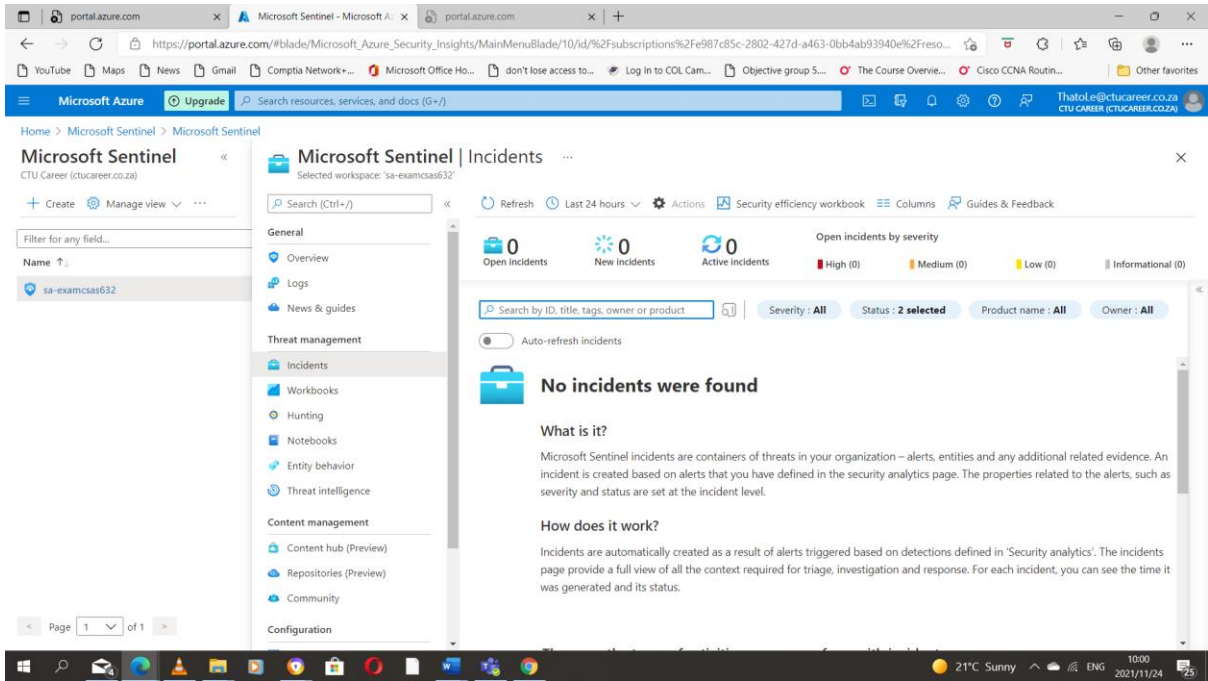
4. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Activity log** and press the **Enter** key.



The screenshot shows the Azure portal's Activity Log page. The search bar at the top contains the text "Activity log". Below the search bar, there are filters for Management Group (None), Subscription (Azure subscription 1), Event severity (All), and Timespan (Last 6 hours). The main content area displays a table with columns for Operation name, Status, Time, Time stamp, Subscription, and Event initiated by. The table is currently empty, with the text "No results to display" below it. A message in the center states "No events to display" and suggests changing filters to see some events. The Windows taskbar at the bottom shows the time as 09:56 on 2021/11/24.

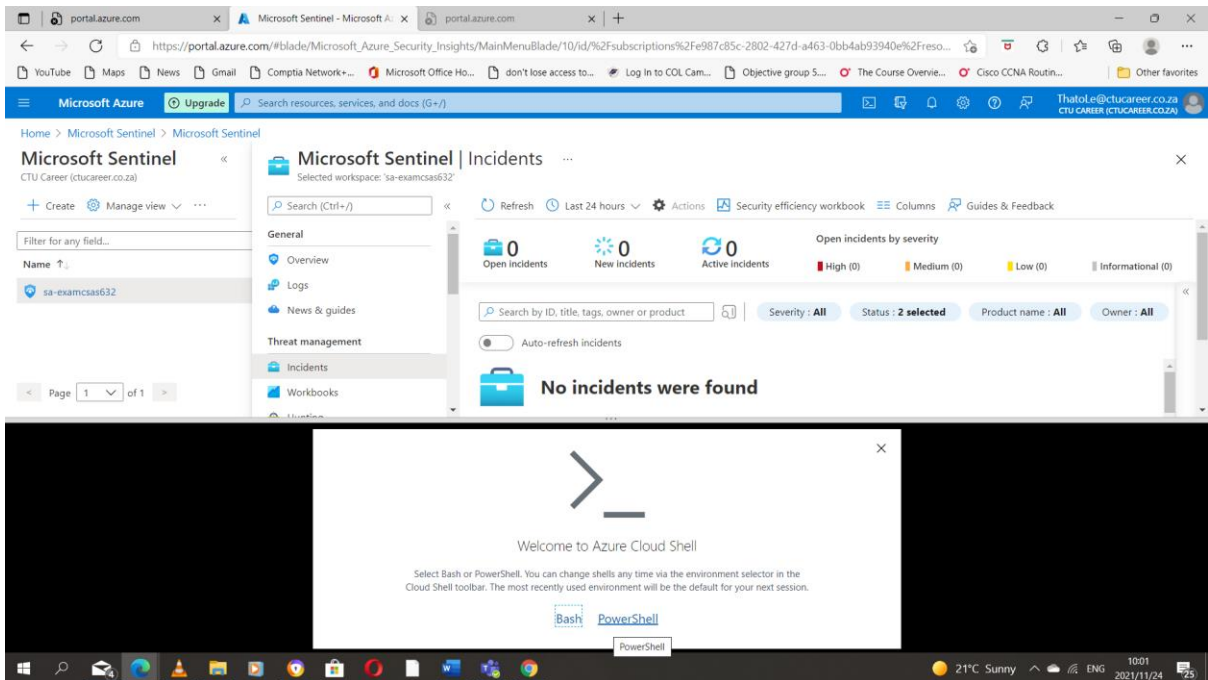


The screenshot shows the Microsoft Sentinel Overview page in the Azure portal. The page title is "Microsoft Sentinel | Overview" and the selected workspace is "sa-examcsas632". The left sidebar contains navigation options such as Overview, Logs, News & guides, Threat management, Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence, Content management, Content hub (Preview), Repositories (Preview), and Community. The main content area displays a dashboard with several sections: "Events and alerts over time" with sub-sections for Events and Alerts; "Incidents by status" showing counts for New (0), Active (0), Closed (True Positive) (0), and Closed (False Positive) (0); "Recent incidents" with a "Learn More" link; "Data source anomalies" showing "No data was found"; and "Potential malicious events". The Windows taskbar at the bottom shows the time as 09:57 on 2021/11/24.



Conclusion

The following it is to clean-up though the powershell might not open due to the dummy account



Microsoft Azure Upgrade Search resources, services, and docs (G+r) ThatoLe@ctucareer.co.za CTU CAREER (CTUCAREER.CO.ZA)

Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel

CTU Career (ctucareer.co.za)

+ Create Manage view ...

Filter for any field...

Name ↑

- sa-examcsas632

Page 1 of 1

Microsoft Sentinel | Incidents

Selected workspace: 'sa-examcsas632'

Search (Ctrl+/) Refresh Last 24 hours Actions Security efficiency workbook Columns Guides & Feedback

General

- Overview
- Logs
- News & guides

Threat management

- Incidents
- Workbooks

Open incidents by severity

Open incidents	New incidents	Active incidents	High (0)	Medium (0)	Low (0)	Informational (0)
----------------	---------------	------------------	----------	------------	---------	-------------------

Search by ID, title, tags, owner or product

Severity: All Status: 2 selected Product name: All Owner: All

Auto-refresh incidents

No incidents were found

You have no storage mounted

Azure Cloud Shell requires an Azure file share to persist files. [Learn more](#)

This will create a new storage account for you and this will incur a small monthly cost. [View pricing](#)

* Subscription

Azure subscription 1 [Show advanced settings](#)

Cloud Shell terminal dialog

Create storage Close

21°C Sunny 10:03 2021/11/24