

# Cloud Security Detection Engineering –Project Report

This report presents a fully refined, professionally rewritten documentation of the Log4j Exploit Detection and Azure Virtual Machine Availability Monitoring project. The goal is to demonstrate hands-on security engineering capability, SIEM detection logic implementation, cloud monitoring, and automation-driven incident response workflows within Microsoft Azure.

## Executive Summary

This project delivers two core cloud security capabilities:

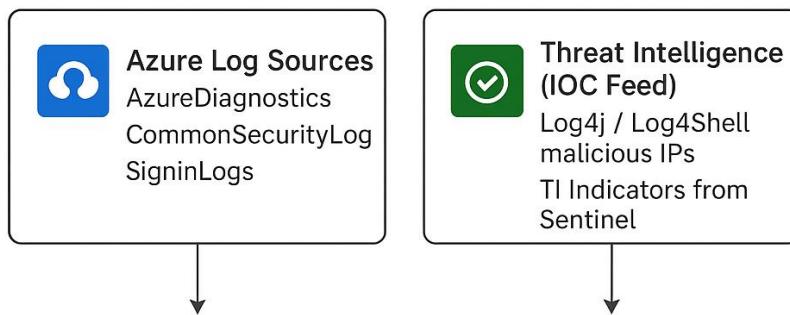
- Proactive detection of Log4j (Log4Shell) exploitation attempts using Microsoft Sentinel
- Real-time monitoring of Azure VM availability using Azure Monitor and Action Groups

Through the deployment of analytics rules, threat intelligence correlation, automation workflows, and alerting pipelines, this implementation showcases operational security engineering principles, practical SIEM usage, and cloud observability best practices.

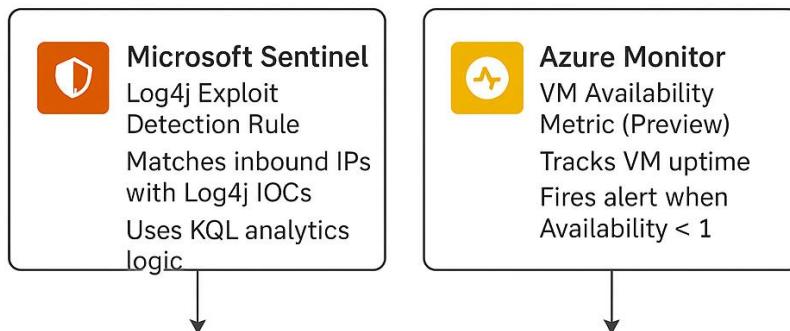
## Cloud Detection & Monitoring Architecture

The following diagram illustrates the end-to-end flow of data ingestion, threat detection, monitoring, automated responses, and incident generation across Microsoft Sentinel and Azure Monitor.

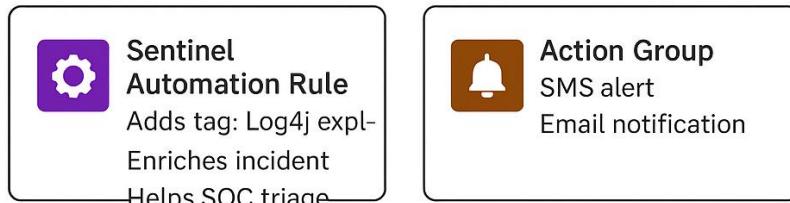
# Cloud Detection & Monitoring Flow



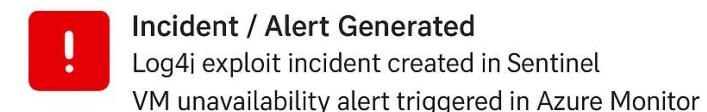
## Detection & Monitoring Logic



## Automated Response



## Final Output



# Part 1 — Log4j Exploit Detection Using Microsoft Sentinel

## Objective

Detect potential Log4j exploitation attempts by operationalizing the Log4j Vulnerability Detection solution within Microsoft Sentinel and enabling an analytics rule that correlates inbound IP activity with known Log4Shell-related threat intelligence indicators.

## Tools & Technologies

- Microsoft Sentinel
- Azure Log Sources (AzureDiagnostics, SigninLogs, CommonSecurityLog)
- Threat Intelligence Indicators (Log4j IOC Feed)
- Scheduled Analytics Rules
- KQL (Kusto Query Language)
- Sentinel Automation Rules

## Implementation Summary

1. Deployed the Log4j Vulnerability Detection solution via Microsoft Sentinel Content Hub.
2. Located and activated the 'Log4j vulnerability exploit aka Log4Shell IP IOC' analytics rule template.
3. Customized rule parameters, added a timestamp field, and enhanced alert naming for clarity.
4. Created an automation rule that tags incidents with 'Log4J exploit' to support structured SOC triage.

## Implementation Steps:

Activity #	Steps
<b>Activity 1:</b> Install the <i>Log4j Vulnerability Detection</i> solution from the Content hub.	<ol style="list-style-type: none"><li>1. Sign in to the Azure portal with your login credentials.</li><li>2. In the global search box, search for and select <b>Microsoft Sentinel</b>.</li></ol>

3. Select the desired Microsoft Sentinel workspace.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with 'Microsoft Azure' and an 'Upgrade' button. A search bar contains the text 'Microsoft Sentinel'. To the right of the search bar are icons for 'Copilot', 'Copilot help', 'Settings', 'Help & support', and a user profile. The main content area has a sidebar on the left with 'Azure services' and 'Resources' sections. The 'Resources' section includes 'Recent' and 'Favorite' tabs, and a 'Name' search input. The main pane displays search results for 'Services (42)'. The 'All' tab is selected, showing items like 'Microsoft Sentinel', 'Microsoft Entra ID', and 'Microsoft Entra authentication methods'. Below these are sections for 'Marketplace' (listing 'Microsoft Sentinel Training Lab Solution', 'PostgreSQL', 'Azure Storage solution for Sentinel', and 'Microsoft Project solution for Sentinel') and 'Documentation' (listing 'Continue searching in Microsoft Entra ID'). On the right side of the main pane, there are cards for 'Foundry', 'Kubernetes services', 'Virtual machines', and a 'More services' button. A vertical scroll bar is visible on the right edge of the main content area.

The screenshot shows the Microsoft Azure Microsoft Sentinel page. At the top, there's a navigation bar with 'Microsoft Azure', 'Upgrade', a search bar ('Search resources, services, and docs (G+)'), 'Copilot', and user information ('princerichard547@gmail.com'). Below the navigation is the 'Home > Microsoft Sentinel' breadcrumb. The main content area has a title 'Microsoft Sentinel' with a 'Discover key trends in resource metrics' button. It also includes buttons for 'Query top 5 resources in the list' and 'Are any resources impacted by outages'. Below this are buttons for 'Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', 'View incidents', and 'Add to service group'. A message indicates 'You are viewing a new version of Browse experience. Click here to access the old experience.' There are filter options: 'Filter for any field...', 'Subscription equals all', 'Resource Group equals all', 'Location equals all', and '+ Add filter'. The main table lists one item: 'Name' (SentinelWorkspace), 'Resource Group' (sentinel-rg), 'Location' (East US), 'Subscription' (Azure subscription 1), and 'Directory' (Default Directory). The table has columns for Name, Resource Group, Location, Subscription, and Directory. At the bottom, it says 'Showing 1 - 1 of 1. Display count: auto'.

4. On the **Microsoft Sentinel** page, under **Content management**, select **Content hub**.  
5. On the **Content hub** page, click on **Go to defender portal**  
6. Search and select the **Log4j Vulnerability Detection** solution.  
7. On the **Log4j Vulnerability Detection** wizard that appears, select **Install**.

Microsoft Azure   [Upgrade](#)   [Search resources, services, and docs \(G+\)](#)

Copilot   [Copilot](#)   [Copilot](#)   [Copilot](#)   [Copilot](#)   [Copilot](#)   [Copilot](#)   [Copilot](#)   [Copilot](#)   [Copilot](#)

princerichard547@gmail.com   DEFAULT DIRECTORY (PRINCERIC...)

Home > Microsoft Sentinel

## Microsoft Sentinel | Content hub

Selected workspace: 'sentinelworkspace'

Search  X

Threat intelligence

MITRE ATT&CK (Preview)

SOC optimization

Content management

Content hub

Repositories

Community

Configuration

Workspace manager (Preview)

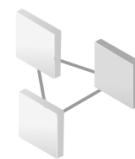
Data connectors

Analytics

Add or remove favorites by pressing Ctrl + Shift + F

This page has been moved to the Defender portal for the optimal, unified SecOps experience

[Click here to go to the Defender portal](#)



Microsoft Azure   [Upgrade](#)    Search resources, services, and docs (G+/)

Copilot         princerichard547@gmail.com  
DEFAULT DIRECTORY (PRINCERIC...)

Home >  
**Log4j Vulnerability Detection**  

Microsoft Sentinel, Microsoft Corporation

 **Log4j Vulnerability Detection**  Add to Favorites

Microsoft Sentinel, Microsoft Corporation | Azure Application  
★ 3.5 (2 ratings)

Subscription Plan  
Azure subscription 1 Log4j Vulnerability Detection 

[Overview](#) [Plans](#) [Usage Information + Support](#) [Ratings + Reviews](#)

Offered under [Microsoft Standard Contract](#).

Note: Please refer to the following before installing the solution:

- Review the solution [Release Notes](#)



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

Copilot ? ? ? ? ? ? ? ? ? ? ?

princerichard547@gmail.com DEFAULT DIRECTORY (PRINCERIC...)

Home > Log4j Vulnerability Detection >

## Create Log4j Vulnerability Detection

14. Microsoft Defender XDR

**Workbooks:** 2, **Analytic Rules:** 4, **Hunting Queries:** 10, **Watchlists:** 1, **Playbooks:** 1

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

**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 \* ⓘ Sentinel-RG Create new

**Instance details**

Workspace \* ⓘ SentinelWorkspace

Previous Next Review + create Give feedback

Home >



Deployment

Search

Delete

Cancel

Redeploy

Download

Refresh



Inputs

Outputs

Template

## Your deployment is complete

Deployment name : azuresentinel.azure-sentinel-so... Start time : 11/22/2025, 9:46:07 PM  
Subscription : Azure subscription 1 Correlation ID : 27f4d2b9-a6ed-4b1f-b74c-318...  
Resource group : Sentinel-RG

> Deployment details

▽ Next steps

Go to resource group

Give feedback

Tell us about your experience with deployment

Add or remove favorites by pressing Ctrl+Shift+F



Cost management

Get notified to stay within your budget and prevent unexpected charges on your bill.

[Set up cost alerts >](#)



Microsoft Defender for Cloud

Secure your apps and infrastructure

[Go to Microsoft Defender for Cloud >](#)

Free Microsoft tutorials

[Start learning today >](#)

Work with an expert

The screenshot shows the Microsoft Azure Resource Group Overview page for a resource group named "Sentinel-RG". The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings (Deployments, Security, Deployment stacks, Policies, Properties), and a note about adding or removing favorites. The main content area displays the "Essentials" section with tabs for Resources and Recommendations. Under Resources, there is a table listing two items:

	Name ↑	Type	Location
<input type="checkbox"/>	SecurityInsights(sentinelworkspace)	... Solution	East US
<input type="checkbox"/>	SentinelWorkspace	... Log Analytics workspace	East US

Filtering options include "Type equals all" and "Location equals all". A "JSON View" link is located in the top right corner.

#### Activity 2:

Navigate to the *Log4j vulnerability exploit aka Log4Shell IP IOC* scheduled analytics rule from the Rule templates tab.

1. On the **Microsoft Sentinel** page, under **Configuration**, select **Analytics**.
2. On the **Analytics** page, select the **Rule templates** tab.
3. In the search box, enter **log4j**.
4. From the filtered list of templates displayed, select **Log4j vulnerability exploit aka Log4Shell IP IOC**.

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

Copilot

princerichard547@gmail.com DEFAULT DIRECTORY (PRINCERIC...)

Home > Microsoft Sentinel | Overview

Selected workspace: 'sentinelworkspace'

Search Refresh

- SOC optimization
- Content management
  - Content hub
  - Repositories
  - Community
- Configuration
  - Workspace manager (Preview)
  - Data connectors
    - Analytics
    - Summary rules
    - Watchlist
    - Automation

Add or remove favorites by pressing Ctrl+Shift+F

# Get your SIEM and XDR in one place

Onboard your workspace to the Defender portal to gain the advantage of a unified SecOps platform with embedded Security Copilot.

Learn more

Incidents (0)  
Last 24 hours

The screenshot shows the Microsoft Sentinel Overview page. On the left, there's a navigation sidebar with various options like SOC optimization, Content management, Configuration, and Analytics. The 'Analytics' option is highlighted with a red box. The main area features a large banner with the text 'Get your SIEM and XDR in one place' and 'Onboard your workspace to the Defender portal to gain the advantage of a unified SecOps platform with embedded Security Copilot.' Below the banner, there's a section for 'Incidents (0)' with a note 'Last 24 hours'.

Microsoft Defender | Default Directory

Search

Refresh Guides & Feedback All workspaces

## Analytics

Manage all your rules in one place

Now you can manage all your rules on one page, providing a centralized and streamlined approach to rule management. This enhancement not only simplifies your workflow but also ensures that you can easily access, modify, and oversee all your rules in one convenient location.

Go to unified rules page

0 Active rules

More content at Content hub

Rules by severity

High (0) Medium (0) Low (0) Informational (0)

LEARN MORE About analytics rules

Active rules Rule templates Anomalies

Create Analytics workbooks Rule runs (Preview) Enable Disable Delete ...

Search by ID, name, tactic or technique Add filter

Severity	Name	Rule type	Status	Tactics	Techniques	Sub
----------	------	-----------	--------	---------	------------	-----

# Microsoft Defender | Default Directory

Search

Add filter

Severity	Name	Rule type	Data sources	Tactics	Techniques	Sub techniques
High	Log4j vulnerability	Scheduled	Microsoft... +7	Command	T1071	
High	User agent search	Scheduled	+4	Initial Access	T1190	
High	Vulnerable Machine	Scheduled		Ini +1	T1190 +1	
High	Azure WAF matches	Scheduled	Azure Web Appli...	Initial Access	T1190	

< Previous Page 1 of 1 Next > Showing 1 to 4 of 4 results.

Severity Content Source Rule Type

Description  
Identifies a match across various data feeds for IP IOCs related to the Log4j vulnerability exploit aka Log4Shell described in CVE-2021-44228. References:  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-44228>

Data sources

- Microsoft 365 (formerly, Office 365)
- Cisco ASA/FTD via AMA
- CommonSecurityLog --
- Microsoft Entra ID
- SignInLogs --
- Azure Activity
- AzureActivity --
- Amazon Web Services
- AWSCloudTrail --

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

**Activity 3:**

Create a rule logic for *Log4j vulnerability exploit aka Log4Shell IP IOC* and configure settings.

1. On the **Analytics** page, on the **Log4j vulnerability exploit aka Log4Shell IP IOC** wizard that appears on the right, select **Create rule**.

The screenshot shows the Microsoft Defender Analytics interface. A search bar at the top contains the query "Log4j". Below the search bar is a table with columns: Severity, Name, Rule type, Data sources, Tactics, Techniques, and Sub techni. There are four rows in the table, each representing a different Log4j-related alert or rule. To the right of the table is a sidebar with sections for Severity, Content Source, and Rule Type. Under "Severity", it says "Identifies a match across various data feeds for IP IOCs related to the Log4j vulnerability exploit aka Log4Shell described in CVE-2021-44228. References: https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-44228". Under "Data sources", it lists Microsoft 365 (formerly, Office 365), Cisco ASA/FTD via AMA, CommonSecurityLog, Microsoft Entra ID, SigninLogs, Azure Activity, AzureActivity, Amazon Web Services, and AWSCloudTrail. At the bottom right of the main pane, there is a note: "You haven't used this template yet; You can use it to create analytics rules." followed by a bulleted list: "One or more data sources used by this rule is missing. This might limit the functionality of the rule." A large blue "Create rule" button is highlighted with a red box.

2. On the **Analytics rule wizard – Create a new Scheduled rule** page, on the **General** tab, leave the settings as default, and select **Next: Set rule logic**.

Microsoft Defender | Default Directory

Analytics > Analytics rule wizard

## Analytics rule wizard - Create a new Scheduled rule

Log4j vulnerability exploit aka Log4Shell IP IOC

General

**Set rule logic**

Incident settings

Automated response

Review + create

Search

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.

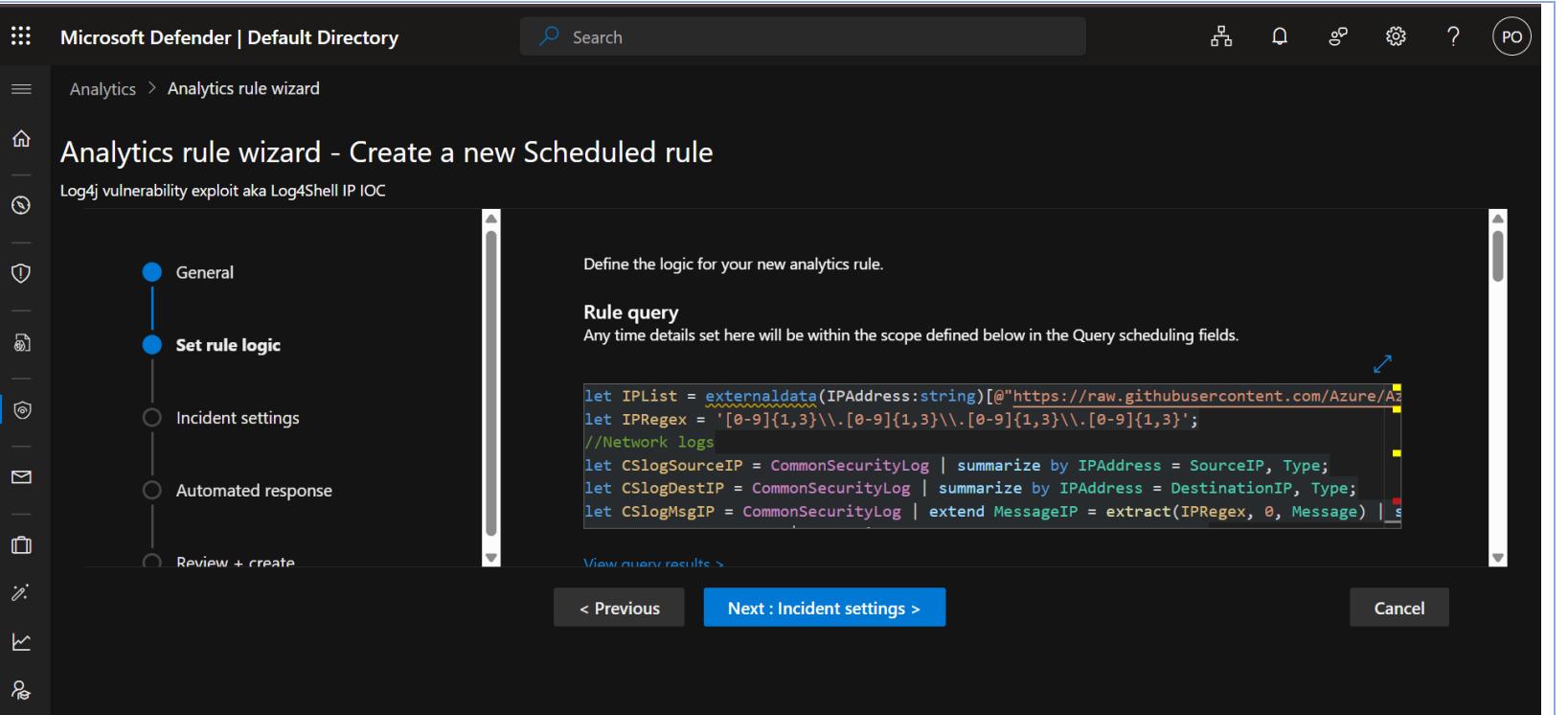
```
let IPList = externaldata(IPAddress:string)[@"https://raw.githubusercontent.com/Azure/Az...  
let IPRegex = '[0-9]{1,3}\\.[0-9]{1,3}\\.[0-9]{1,3}\\.[0-9]{1,3}';  
//Network logs  
let CSlogSourceIP = CommonSecurityLog | summarize by IPAddress = SourceIP, Type;  
let CSlogDestIP = CommonSecurityLog | summarize by IPAddress = DestinationIP, Type;  
let CSlogMsgIP = CommonSecurityLog | extend MessageIP = extract(IPRegex, 0, Message) | s...
```

< Previous

Next : Incident settings >

Cancel

3. On the **Set rule logic** tab, review the query as it appears under the **Rule query** section.



The screenshot shows the Microsoft Defender Analytics rule wizard interface. The title bar reads "Microsoft Defender | Default Directory". The left sidebar has a tree view with "Analytics" selected, and the breadcrumb navigation shows "Analytics > Analytics rule wizard". The main content area is titled "Analytics rule wizard - Create a new Scheduled rule" and has a subtitle "Log4j vulnerability exploit aka Log4Shell IP IOC". On the left, a vertical navigation pane lists steps: "General" (selected), "Set rule logic" (selected), "Incident settings", "Automated response", and "Review + create". The right side contains configuration fields: "Alert Name Format" set to "Log4j vulnerability exploit aka Log4Shell IP IOC from {{timestamp}}", "Alert Description Format" with the example "Example: Alert from {{ProviderName}} generated at {{TimeGenerated}}", and a "Add new property override" button. At the bottom are "Next : Incident settings >" and "Cancel" buttons.

- |  |                                                                                                                                                                                                                                                                                                          |
|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <ol style="list-style-type: none"><li>4. Then, in the <b>Custom details</b> section, in the <b>Key</b> field, enter <b>timestamp</b> to add the timestamp of each occurrence to the alert.</li><li>5. From the <b>Value</b> dropdown list, select <b>timestamp</b>.</li></ol>                            |
|  | <ol style="list-style-type: none"><li>6. In the <b>Alert details</b> section, in the <b>Alert Name Format</b> box, enter <b>Log4j vulnerability exploit aka Log4Shell IP IOC from {{timestamp}}</b>.</li><li>7. Leave the other settings as default and select <b>Next: Incident settings</b>.</li></ol> |
|  | <ol style="list-style-type: none"><li>8. Review the remaining settings on the <b>Incident settings</b> tab, leave it as default, and select <b>Next: Automated response</b>.</li></ol>                                                                                                                   |
|  | <ol style="list-style-type: none"><li>9. On the <b>Automated response</b> tab, in the <b>Automation rules</b> section, select <b>Add new</b> to create a new automation rule for this analytics rule.</li></ol>                                                                                          |

10. On the **Create new automation rule** wizard that appears, in the **Automation rule name** box, enter **Log4J vulnerability exploit detection**.
11. Then, from the **Actions** dropdown list, select **Add tags**.

The screenshot shows the 'Create new automation rule' interface in Microsoft Defender. In the 'Conditions' section, there is a single condition: 'If Analytic rule name Contains Value: Current rule'. In the 'Actions' section, under 'Add tags', a tag named 'Log4J exploit' is selected. A modal window titled 'Add tag' is open, showing the tag 'Log4J exploit' and buttons for 'Apply' and 'Cancel'. Below the actions, there is a 'Time' field with a calendar icon.

12. Select **Add tag**.
13. Enter **Log4J exploit** in the text box and select **OK**.
14. Next, select **Apply**.
15. Then, select **Next: Review and create**.

Microsoft Defender | Default Directory

Analytics > Analytics rule wizard

## Analytics rule wizard - Create a new Scheduled rule

Log4j vulnerability exploit aka Log4Shell IP IOC

General

Set rule logic

Incident settings

**Automated response**

Review + create

Automation rules

View all automation rules that may be triggered by this analytics rule and create new automation rules.

+ Add new

Order	Automation rule name	Trigger	Action
1	Log4J vulnerability exploit detection	Incident created	Add tags

< Previous      Next : Review + create >      Cancel

The screenshot shows the Microsoft Defender Analytics rule wizard interface. The left sidebar has a navigation menu with icons for Home, Analytics, Threats, Incidents, Automation, and more. The main area title is 'Analytics rule wizard - Create a new Scheduled rule' for 'Log4j vulnerability exploit aka Log4Shell IP IOC'. A vertical progress bar on the left indicates the current step: 'General', 'Set rule logic', 'Incident settings', 'Automated response' (which is bolded), and 'Review + create'. The right side displays the 'Automation rules' section, which lists one rule: 'Log4J vulnerability exploit detection' (Order 1), triggered by 'Incident created', and performing the action 'Add tags'. Navigation buttons at the bottom include '< Previous', 'Next : Review + create >', and 'Cancel'.

16. Review all the settings for your new analytics rule on the **Review and create** tab and select **Save**.

Microsoft Defender | Default Directory

Analytics > Analytics rule wizard

Validation passed.

## Analytics rule wizard - Create a new Scheduled rule

Log4j vulnerability exploit aka Log4Shell IP IOC

General Set rule logic Incident settings Automated response Review + create

Analytics rule details

Name: Log4j vulnerability exploit aka Log4Shell IP IOC

Description: Identifies a match across various data feeds for IP IOCs related to the Log4j vulnerability exploit aka Log4Shell described in CVE-2021-44228. References: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-44228>

MITRE ATT&CK: Command And Control (1)

Severity: High

Status: Enabled

Analytics rule settings

Rule query: `let IPList = externaldata(IPAddress:string)`

< Previous Save Cancel

The screenshot shows the Microsoft Defender Default Directory interface. The top navigation bar includes a search bar, a gear icon, and a user profile icon labeled 'PO'. A banner at the top states: 'now you can manage all your rules on one page, providing a centralized and streamlined approach to rule management. This enhancement not only simplifies your workflow but also ensures that you can easily access, modify, and oversee all your rules in one convenient location.' Below the banner is a blue button labeled 'Go to unified rules page'.

The main area displays 'Active rules' (1) and a 'Content hub' button. A 'Rules by severity' chart shows 1 High rule, 0 Medium, 0 Low, and 0 Informational rules. To the right, there's a 'LEARN MORE' link for 'About analytics rules'.

The 'Active rules' section includes tabs for 'Active rules', 'Rule templates', and 'Anomalies'. It features a toolbar with 'Create', 'Analytics workbooks', 'Rule runs (Preview)', 'Enable', 'Disable', 'Delete', 'Import', 'Export', and 'Columns' options. A search bar and a 'Add filter' button are also present.

The table below lists the single active rule:

Severity	Name	Rule type	Status	Tactics	Techniques	Sub techniques	Source name	Last modified
High	Log4j vulnerability	Scheduled	Enabled	Command And Control	T1071		Apache Log4j Vu...	22/11/2025, 22:3...

## Outcome

The analytics rule now provides continuous detection of known malicious Log4Shell-related IP interactions. Automated tagging enhances SOC workflow efficiency, improves triage speed, and aligns incidents under a standardized taxonomy.

## Part 2 — Azure VM Availability Monitoring

### Objective

Enable near real-time alerting for virtual machine downtime by leveraging Azure Monitor's VM Availability metric and Action Groups for escalation notifications.

### Tools & Technologies

- Azure Monitor
- VM Availability Metric (Preview)
- Azure Metrics Explorer
- Action Groups (SMS/Email)
- Azure Alerting Engine

### Implementation Summary

1. Configured Azure Monitor metrics scope for VM IPO-VM.
2. Selected the 'VM Availability Metric (Preview)' to monitor uptime (1 = available, 0 = unavailable).
3. Created an alert rule that fires when availability falls below 1 within a 1-minute evaluation window.
4. Configured an Action Group with SMS/email notifications for immediate response.

### Implementation Steps:

Activity #	Steps
<b>Activity 1:</b> Set the scope in metrics explorer for a subscription or resource group with the VM to monitor.	<ol style="list-style-type: none"><li>1. Sign in to the Azure portal with your login credentials.</li><li>2. In the global search box, search for and select <b>Monitor</b>.</li></ol>

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with icons for Copilot, Home, Monitor, Settings, and Help. The main search bar contains the text "Monitor". Below the search bar, the "Azure services" section includes a "Create a resource" button and a "Monitor" icon. The "Resources" section shows "Recent" and "Favorite" items, with "Recent" currently selected, displaying "SentinelWorkspace", "SecurityInsights(sentinelworkspace)", and "Sentinel-RG". The "Navigate" section has a "See more" link. On the right side, a search results panel titled "Services (19)" is open, showing items under "All" and "More (5)". The "All" section includes "Monitor", "Azure Monitor workspaces", "Azure Monitor pipelines (preview)", and "Azure Monitor Private Link Scopes". The "Microsoft Entra ID" section lists "Azure Monitor System", "Metrics Monitor API", "Azure Monitor Control Service", and "Azure Monitor Restricted", all categorized as "Service Principal". Below this is a "Marketplace" section with a "Continue searching in Microsoft Entra ID" link. The "Last Viewed" section shows three items last viewed 6 hours ago. A footer at the bottom of the search panel says "Searching all subscriptions." and "Give feedback".

	<ol style="list-style-type: none"><li>3. Select <b>Metrics</b> from the <b>Monitor</b> menu.</li><li>4. On the <b>Metrics</b> page, choose <b>Select a scope</b>.</li><li>5. In the <b>Select a scope wizard</b> that appears, select a subscription or resource group with the VM to monitor.</li><li>6. In the <b>Refine scope</b> section, from the <b>Resource type dropdown list</b>, select <b>Virtual machines</b>.</li><li>7. Then, select the desired <b>Location</b>.</li><li>8. Select <b>Apply</b> to set the scope in metrics explorer.</li></ol>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Microsoft Azure   [Upgrade](#)      [Copilot](#)

princerichard547@gmail.com  
DEFAULT DIRECTORY (PRINCERICHARD547)

Home > Monitor | Overview

... Summarize these Monitor services in a table Catch me up on my alerts Run an anomaly investigation into my resource

The Log Analytics agents, used by VM Insights, won't be supported as of August 31, 2024. Plan to migrate to VM Insights on Azure Monitor agent prior to this date. →

[Overview](#)   [Tutorials](#)

**Insights**  
Use curated monitoring views for specific Azure resources. [View all insights](#)

**Application insights**  
Monitor your app's availability, performance, errors, and usage.  
[View](#)   [More](#)

**Container Insights**  
Gain visibility into the performance and health of your controllers, nodes, and containers.  
[View](#)   [More](#)

**VM Insights**  
Monitor the health, performance, and dependencies of your VMs and VM scale sets.  
[View](#)   [More](#)

**Network Insights**  
View the health and metrics for all deployed network resources.

Add or remove favorites by pressing **Ctrl+Shift+F**

Microsoft Azure    Upgrade    Search resources, services, and docs (G+)    Copilot    Home > Monitor

## Monitor | Metrics

Microsoft

Can I get alerted based on live metrics?   What metrics do people commonly use to track this kind of resource?   What metrics are available for this resource?

+ New chart   Refresh   Share   Local Time: Last 24 hours (Automatic)

Search   Overview   Activity log   Alerts   Issues (preview)   Metrics   Logs   Change Analysis   Service health   Workbooks   Dashboards with Grafana (preview)   Insights   Managed Services

Chart Title  + Add metric   Add filter   Apply splitting   Line chart   Drill into Logs   New alert rule   Save to dashboard   ...

Scope   Metric Namespace   Metric   Aggregation  
+ Select a scope   Select namespace   Select metric   Select aggregation

100  
90  
80  
70  
60  
50  
40  
30  
20

Select a metric above to see data appear on this chart or learn more below:

- Filter + Split   Apply filters and splits to
- Plot multiple metrics   Create charts with multiple
- Build custom dashboards

Give Feed

This screenshot shows the Microsoft Azure Monitor Metrics blade. The left sidebar contains links for Overview, Activity log, Alerts, Issues (preview), Metrics (which is selected and highlighted in blue), Logs, Change Analysis, Service health, Workbooks, Dashboards with Grafana (preview), Insights, and Managed Services. The main area features a search bar, a chart title input, and buttons for adding a new chart, refreshing, sharing, and changing the local time. Below these are dropdown menus for Scope, Metric Namespace, Metric, and Aggregation. A vertical scale from 20 to 100 is visible on the left. At the bottom, there's a section titled 'Select a metric above to see data appear on this chart or learn more below:' with three cards: 'Filter + Split' (Apply filters and splits to), 'Plot multiple metrics' (Create charts with multiple), and 'Build custom dashboards'. A 'Give Feed' button is located at the bottom right.

Microsoft Azure   [Upgrade](#)      [Copilot](#)        

princerichard547@gmail.com  
DEFAULT DIRECTORY (PRINCERIC...)

Home > Monitor

## Monitor | Metrics

Search      

- Overview
- Activity log
- Alerts
- Issues (preview)
- Metrics**
- Logs
- Change Analysis
- Service health
- Workbooks
- Dashboards with Grafana (preview)
- > Insights
- > Managed Services

 New chart   

Chart Title 

 Add metric 

Scope  Azure subscription 1

 Sentinel-RG

Resource type   Location

Subscription   -

Resource group   -

**Why can't I select multiple resources?** Azure limits selections to one resource type and one location. Please refine your scope.

Refine scope

Resource type \*   Location \*

Virtual machines   West US 2

Selected scopes 1 scope

 Sentinel-RG   Resource group - 

 IPO-VM   Virtual machine   West US 2

**Apply**   **Cancel**   **Clear all selections**

The screenshot shows the Microsoft Azure Monitor Metrics interface. The left sidebar includes links for Overview, Activity log, Alerts, Issues (preview), Metrics (selected), Logs, Change Analysis, Service health, Workbooks, Dashboards with Grafana (preview), Insights, and Managed Services. The main area displays a chart titled "Avg VM Availability Metric (Preview)" for Azure subscription 1 in West US 2 region, filtered by ResourceId where ResourceGroupName = 'Sentinel-RG'. The chart shows a single data series with values ranging from 0.40 to 1.00. The chart has a legend indicating "1". The top navigation bar features "Microsoft Azure", "Upgrade", "Search resources, services, and docs (G+)", "Copilot", and user information "princerichard547@gmail.com DEFAULT DIRECTORY (PRINCERICHARD547)".

<b>Activity 2:</b> Create an alert rule and action group.	<ol style="list-style-type: none"><li>On the <b>Metrics</b> page, from the <b>Metric</b> dropdown list, select <b>VM Availability Metric (Preview)</b>.</li><li>Then, select <b>New alert rule</b> to create an alert rule.</li></ol>
--------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The screenshot shows the Microsoft Azure Monitor Metrics blade. On the left, there's a navigation menu with items like Overview, Activity log, Alerts, Issues (preview), Metrics (which is selected and highlighted in grey), Logs, Change Analysis, Service health, Workbooks, Dashboards with Grafana (preview), Insights, and Managed Services. A search bar and a refresh button are at the top. The main area displays a chart titled "Avg VM Availability Metric (Preview) for Azure subscription 1 in West US 2 region by ResourceId where ResourceGroupName = 'Sentinel-RG'". The chart shows a single data series with values ranging from 0.40 to 1.00. The chart controls include "Add metric", "Add filter", "Apply splitting", "Line chart", "Drill into Logs", "New alert rule" (which is highlighted with a red box), "Save to dashboard", and other settings. The time range is set to "Last 24 hours (Automatic - 15 minutes)".

3. On the **Create an alert rule** page, select the **Condition** tab.
4. In the **Alert logic** section, set the following values:

Setting	Value
Threshold	Static
Aggregation type	Average
Operator	Greater than
Unit	Count
Threshold value	1

**Note:** The alert logic specifies that an alert should fire whenever the average value of the availability metric falls below 1, indicating that the VM in the selected scope isn't functional.

The screenshot shows the 'Create an alert rule' wizard in the Microsoft Azure portal. The current step is 'Alert logic'. The configuration is as follows:

- Signal name:** VM Availability Metric (Preview)
- Threshold type:** Static
- Aggregation type:** Average
- Value is:** Less than
- Unit:** Count
- Threshold:** 1

A preview chart on the right shows a single data series for 'IPO-VM; Aggregate' over the last 6 hours. The Y-axis ranges from 0.5 to 1.0. The data points fluctuate between 0.9 and 1.0, with a sharp drop to approximately 0.5 at the end of the period, which triggers the alert.

At the bottom of the wizard, there are buttons for 'Review + create', 'Previous', and 'Next: Actions >'.

5. In the **When to evaluate** section, set the following values:

Setting	Value
Check every	1 minute
Loopback period	1 minute

**Note:** These values specify that the alert rule will check the log data every minute to identify issues with the specified VM.

6. Select **Next: Actions** to move to the **Actions** tab.

**Note:** The **Actions** tab allows you to add one or more action groups to the alert rule. Action groups define a set of actions to take when an alert is fired, such as sending an email or an SMS.

Microsoft Azure Upgrade Search resources, services, and docs (G+/-) Copilot 1 🔍 ⚙️ ⓘ 🔍 princerichard547@gmail.com DEFAULT DIRECTORY (PRINCERIC... X

Home > Monitor | Metrics >

## Create an alert rule

Split by dimensions

Use dimensions to monitor specific time series and provide context to the fired alert. [About monitoring multiple time series](#)

Dimension name	Operator	Dimension values	Include all future...
Select dimension	=	0 selected	<input type="checkbox"/>
Add custom value			

When to evaluate

Check every ⓘ 1 minute

Lookback period ⓘ 1 minute

+ Add condition

Review + create Previous Next: Actions >

PREVIEW time range: Over the last 6 hours TIME SERIES: IP-O-VM, Aggregate

VM Availability Metric (Preview) (Avg), ipo-vm | 0.91

11 PM Nov 23 1 AM 2 AM 3 AM UTC-08:00

7. On the **Actions** tab, select **Create action group**.

The screenshot shows the 'Create an alert rule' page in the Microsoft Azure portal. The 'Actions' tab is selected, indicated by a red box around the tab name. Below the tabs, a note states: 'An action group is a set of actions that can be applied to an alert rule.' A link to 'Learn more' is provided. Two buttons are available: '+ Select action groups' and '+ Create action group', with the latter also enclosed in a red box. A section titled 'Action group name' shows the message 'No action group selected yet'. To the right, a 'Contains actions' column is visible. At the bottom, there are navigation buttons: 'Review + create' (highlighted in blue), 'Previous', and 'Next: Details >'. The top navigation bar includes links for 'Home', 'Monitor | Metrics', and other Azure services like Copilot, along with user information.

**Note:** If you already have an action group, choose **Select action groups** to add an existing group to the alert rule instead of creating a new one.

8. On the **Create action group** page, on the **Basics** tab, in the **Project details** sections, select a **Subscription** and **Resource group** for the action group.
9. Next, select the region.
10. Then, in the **Instance details** section, enter the **Action group name** and the **Display name**.  
**Note:** The **Action group name** will appear on the Azure portal, and the **Display name** will appear in email and SMS notifications.
11. Select **Next: Notifications**.

The screenshot shows the 'Create action group' wizard in the Microsoft Azure portal. The top navigation bar includes 'Microsoft Azure', 'Upgrade', 'Search resources, services, and docs (G+)', 'Copilot', and user information 'princerichard547@gmail.com'. The main title is 'Create action group'.

**Project details**

Select a 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 \*: Sentinel-RG (highlighted with a purple border)

Create new

Region: Global

**Instance details**

Action group name \*: My Action Group 1 (highlighted with a green checkmark)

Display name \*: My Group (highlighted with a green checkmark)

The display name is limited to 12 characters

Buttons at the bottom: 'Review + create' (blue), 'Previous', and 'Next: Notifications >'.

- |  |                                                                                                                                                                                                                                                                                                                                          |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <ol style="list-style-type: none"><li>12. On the <b>Notifications</b> tab, from the <b>Notification type</b> dropdown list, select <b>Email/SMS message/Push/Voice</b>.</li><li>13. In the <b>Email/SMS message/Push/Voice</b> wizard that appears, select <b>SMS</b>, enter the mandatory details, and then select <b>OK</b>.</li></ol> |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Microsoft Azure Upgrade Search resources, services, and docs (G+/ Copilot     princerichard547@gmail.com DEFAULT DIRECTORY (PRINCERIC...)

Home > Monitor | Metrics > Create an alert rule >

## Create action group

Basics Notifications Actions Tags Review + create

Choose how to get notified when the action group is triggered. This step is optional.

Notification type 	Name 	Selected 
<input type="button" value="Email/SMS message..."/>	<input type="text"/>	
	<input type="text"/>	

**OK**

Email/SMS message/Push/Voice 

Add or edit Email/SMS message/Push/Voice action

Email  
Email 

SMS (Carrier charges may apply)  
Country code \* 1

Phone number \* 07052112344 

Message & data rates may apply. Message frequency varies. Reply HELP for more info. Reply STOP to cancel. Full Terms & Conditions can be found [here](#) and view our [Privacy Policy](#).

Azure mobile app notification  
Azure account email 

Voice  
Country code 1

Phone number 

**Note:** The selected notification type is displayed in the **Selected** field.

14. Then, in the **Name** box, specify the people to be notified when the alert is fired.
15. Select **Review + create**.

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

Copilot   [Copilot](#)   [Copilot](#)   [Copilot](#)   [Copilot](#)   [Copilot](#)   [Copilot](#)

princerichard547@gmail.com  
DEFAULT DIRECTORY (PRINCERIC...)

Home > Monitor | Metrics > Create an alert rule >

## Create action group

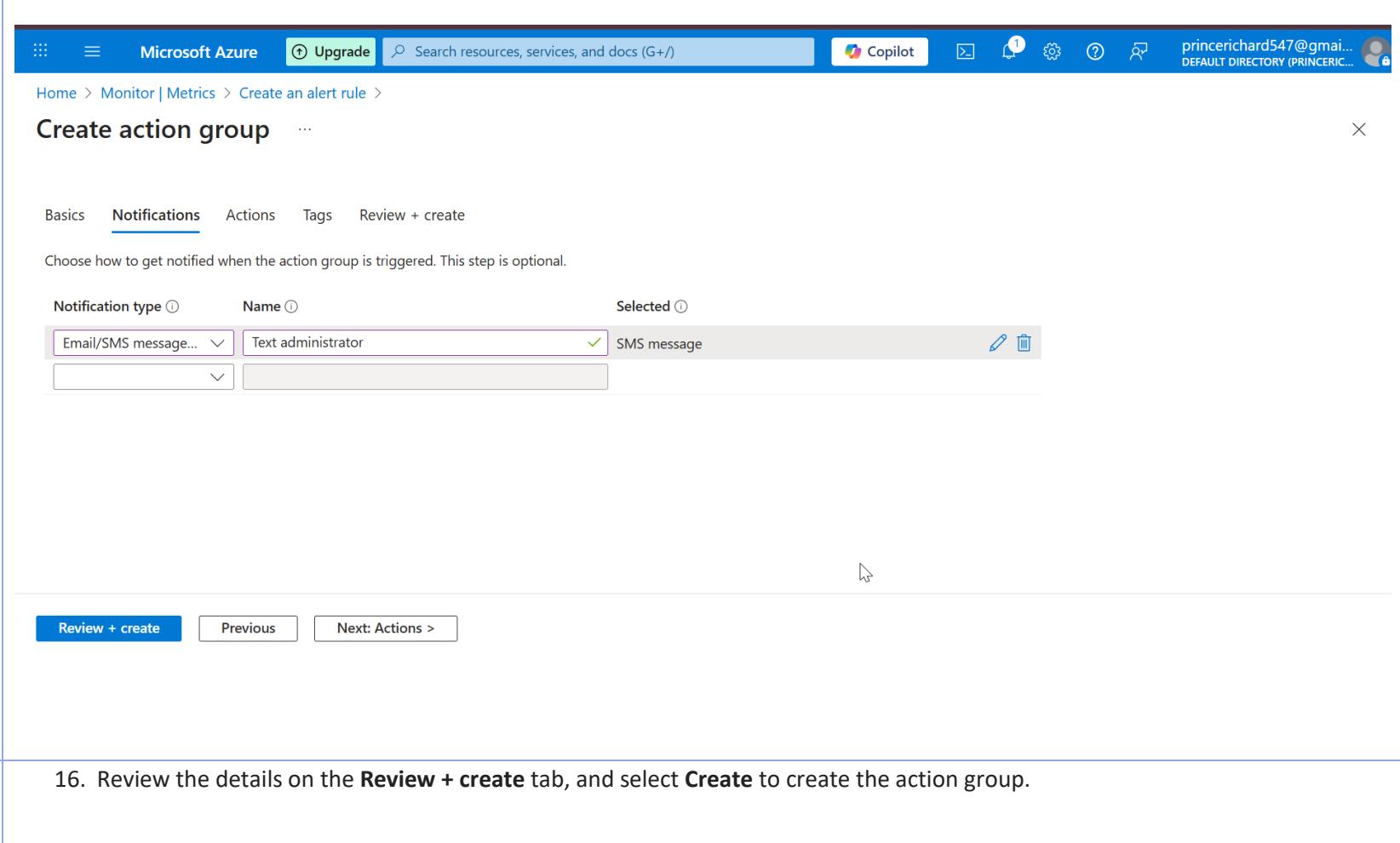
Basics   **Notifications**   Actions   Tags   Review + create

Choose how to get notified when the action group is triggered. This step is optional.

Notification type ⓘ	Name ⓘ	Selected ⓘ
Email/SMS message...	Text administrator	SMS message
		<a href="#">Edit</a> <a href="#">Delete</a>

Review + create   Previous   Next: Actions >

16. Review the details on the **Review + create** tab, and select **Create** to create the action group.



The screenshot shows the 'Create action group' review page in the Microsoft Azure portal. At the top, there's a navigation bar with 'Microsoft Azure', 'Upgrade', a search bar, 'Copilot', and user information. Below the navigation is a breadcrumb trail: 'Home > Monitor | Metrics > Create an alert rule'. The main title is 'Create action group'. A horizontal navigation bar below the title includes 'Basics', 'Notifications', 'Actions', 'Tags', and 'Review + create' (which is underlined, indicating it's the active tab). A note below the tabs says: 'This is a summary of your action group. Please review to ensure the information is correct and consider [Azure Monitoring Pricing](#) and the [Azure Privacy Statement](#)'. The 'Basics' section contains the following details:

Subscription	Azure subscription 1
Resource group	Sentinel-RG
Region	global
Action group name	My Action Group 1
Display name	My Group

The 'Notifications' section shows a single entry:

Notification type	Name	Selected
-------------------	------	----------

At the bottom of the page are two buttons: 'Create' (highlighted in blue) and 'Previous'.

17. Then, navigate to the **Create an alert rule** page.

18. On the **Details** tab, configure the settings:

Setting	Description
Subscription	Select the desired subscription.
Resource group	Select the desired resource group.
Severity	Select a desired severity.
Alert rule name	VM unavailability
Alert rule description	Enter an optional description for the alert rule.

19. Then, select **Review + create**.

Microsoft Azure [Upgrade](#)  Search resources, services, and docs (G+/-) Copilot princerichard547@gmail.com DEFAULT DIRECTORY (PRINCERIC...)

Home > Monitor | Metrics >

## Create an alert rule

Actions

An action group is a set of actions that can be applied to an alert rule. [Learn more](#)

+ Select action groups + Create action group

Action group name	Contains actions
My Action Group 1	1 SMS message

[Review + create](#) [Previous](#) [Next: Details >](#)

Microsoft Azure Upgrade Search resources, services, and docs (G+/-) Copilot 2 ? ? ? ? princerichard547@gmail.com DEFAULT DIRECTORY (PRINCERIC...)

Home > Monitor | Metrics

## Create an alert rule

Project details

Select the subscription and resource group in which to save the alert rule.

Subscription \* ⓘ Azure subscription 1

Resource group \* ⓘ Sentinel-RG Create new

Alert rule details

Severity \* ⓘ 3 - Informational

Alert rule name \* ⓘ VM unavailability

Alert rule description ⓘ

Advanced options

Review + create Previous Next: Tags >

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

Copilot   [Copilot](#)   [Copilot](#)   [Copilot](#)   [Copilot](#)   [Copilot](#)   [Copilot](#)   [Copilot](#)   [Copilot](#)

princerichard547@gmail.com  
DEFAULT DIRECTORY (PRINCERIC...)

Home > Monitor | Metrics >

## Create an alert rule

Project details

Select the subscription and resource group in which to save the alert rule.

Subscription \* [Azure subscription 1](#)

Resource group \* [Sentinel-RG](#)   [Create new](#)

Alert rule details

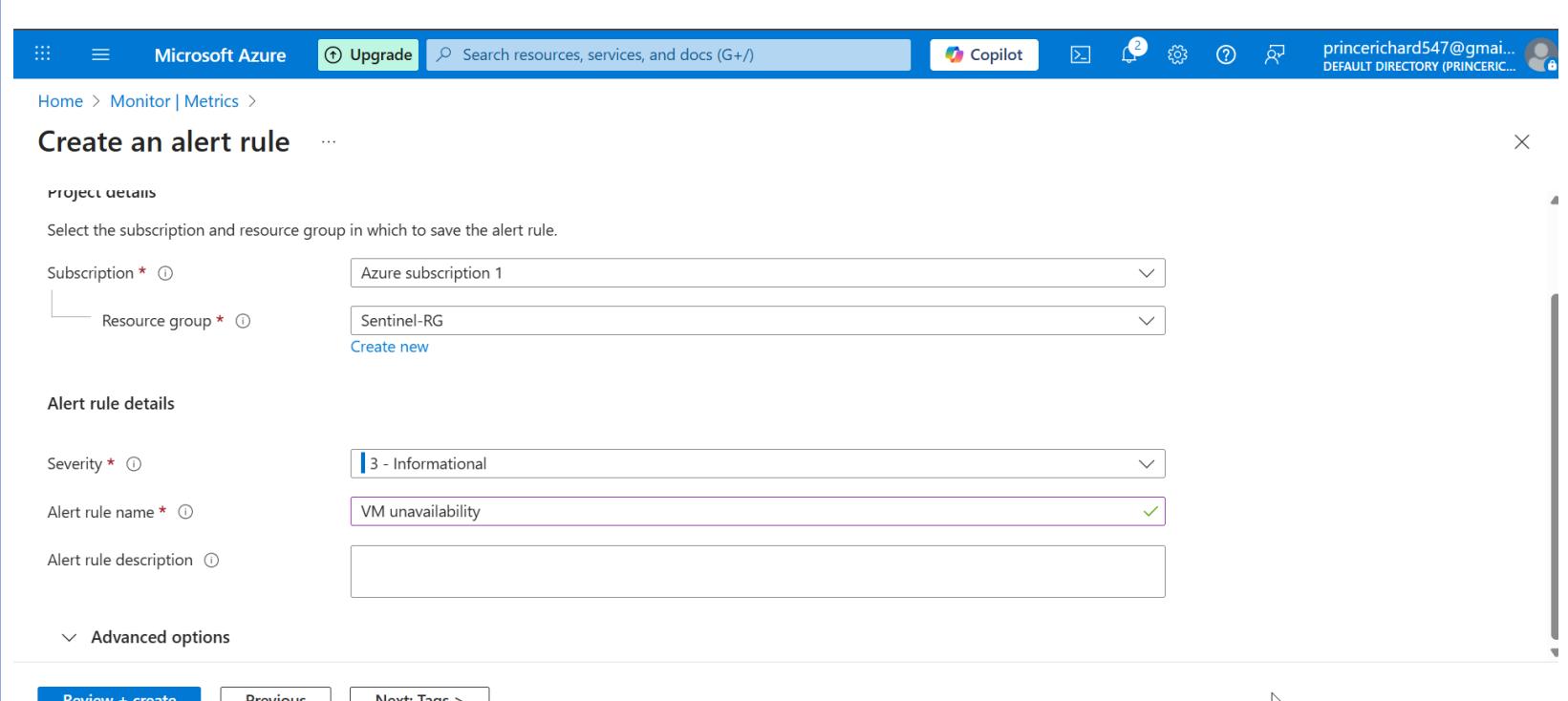
Severity \* [3 - Informational](#)

Alert rule name \* [VM unavailability](#)

Alert rule description [\(1\)](#)

Advanced options

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



20. On the **Review + create** tab, select **Create** to create the alert rule.

Microsoft Azure   [Upgrade](#)    Search resources, services, and docs (G+/)

Copilot                             
princerichard547@gmail.com  
DEFAULT DIRECTORY (PRINCERIC...)

Home > Monitor | Metrics >

## Create an alert rule

Scope

Scope level  Subscription

Resource  Azure subscription 1 >  Sentinel-RG >  All virtual machines (West US 2)

Condition

Signal name	VmAvailabilityMetric
Operator	Less than
Aggregation type	Average
Threshold value	1
Lookback period	1 minute
Check every	1 minute

Actions

Action group name  Contain actions 

[Create](#)   [Previous](#)

The screenshot shows the Microsoft Azure portal interface for creating an alert rule. At the top, there's a navigation bar with 'Microsoft Azure', 'Upgrade', a search bar ('Search resources, services, and docs (G+/)'), and various icons for Copilot, notifications, settings, and help. The user is signed in as 'princerichard547@gmail.com'.

The main title is 'Create an alert rule'. Below it, there are two action groups: 'My Action Group 1' and '1 SMS message'. The 'Details' section is expanded, showing 'Project details' and 'Alert rule details'.

**Project details:**

- Subscription: Azure subscription 1
- Resource group: Sentinel-RG
- Region: global

**Alert rule details:**

- Alert rule name: VM unavailability
- Alert rule description: (empty)
- Severity: 3 - Informational
- Enable upon creation:
- Automatically resolve alerts:

At the bottom, there are 'Create' and 'Previous' buttons.

21. To view the alert rule, navigate to the **Monitor** homepage, and select **Alerts** from the menu.  
22. Then, select **Alert rules**.

**Microsoft Azure** [Upgrade](#)  [Copilot](#) (3) [princerichard547@gmail.com](#) [DEFAULT DIRECTORY \(PRINCERIC...\)](#)

Home > Monitor

## Monitor | Alerts

Microsoft

[View as timeline \(preview\)](#) [Create](#) [Alert rules](#) [Action groups](#) [Alert processing rules](#) [Prometheus rule groups](#)

Subscription : **b4356883-deda-4c0e-b502-319053c33546** [Add filter](#) [More \(3\)](#)

**Overview** [Activity log](#) [Alerts](#) [Issues \(preview\)](#) [Metrics](#) [Logs](#) [Change Analysis](#) [Service health](#) [Workbooks](#) [Dashboards with Grafana \(preview\)](#) [Insights](#) [Managed Services](#)

Total alerts: **0** Critical: **0** Error: **0** Warning: **0** Informational: **0** Verbose: **0**

Name ↑↓ Severity ↑↓ Affected resource ↑↓ Alert condition ↑↓ User response ↑↓ Fire time ↑↓

Add or remove favorites by pressing **Ctrl+Shift+F**

23. On the **Alert rules** page, view the alert rule created.



Microsoft Azure   [Upgrade](#)      [Copilot](#)          [princerichard547@gmail.com](#)   [DEFAULT DIRECTORY \(PRINCERIC...\)](#)

Home > Monitor | Alerts >

## Alert rules

[Create](#) | [Columns](#) [Refresh](#) [Export to CSV](#) [Open query](#) |  [Delete](#)

  [Subscription : Azure subscription 1](#)   [Target scope : all](#)   [Target resource type : all](#)   [+ Add tag filter](#)   [More \(3\)](#)   [No grouping](#)

Name ↑↓	Condition	Severity ↑↓	Target scope	Target resource type	Signal type ↑↓	Status ↑↓
<a href="#">VM unavailability</a>	VmAvailabilityMetric < 1	3 - Informational	All virtual machines in 'Se...' Virtual machine	Virtual machine	Metrics	Enabled

Showing 1 - 1 of 1 results.   [Give feedback](#)

24. To view the action group, navigate to the **Monitor** homepage, and select **Alerts** from the menu.  
25. Then, select **Action groups**.

Microsoft Azure     Upgrade     Search resources, services, and docs (G+)     Copilot     3     Settings     Help     princerichard547@gmail.com     DEFAULT DIRECTORY (PRINCERIC...)

Home > Monitor

## Monitor | Alerts

Microsoft

Search     View as timeline (preview)     Create     Alert rules     Action groups (highlighted with red box)     Alert processing rules     Prometheus rule groups     ...

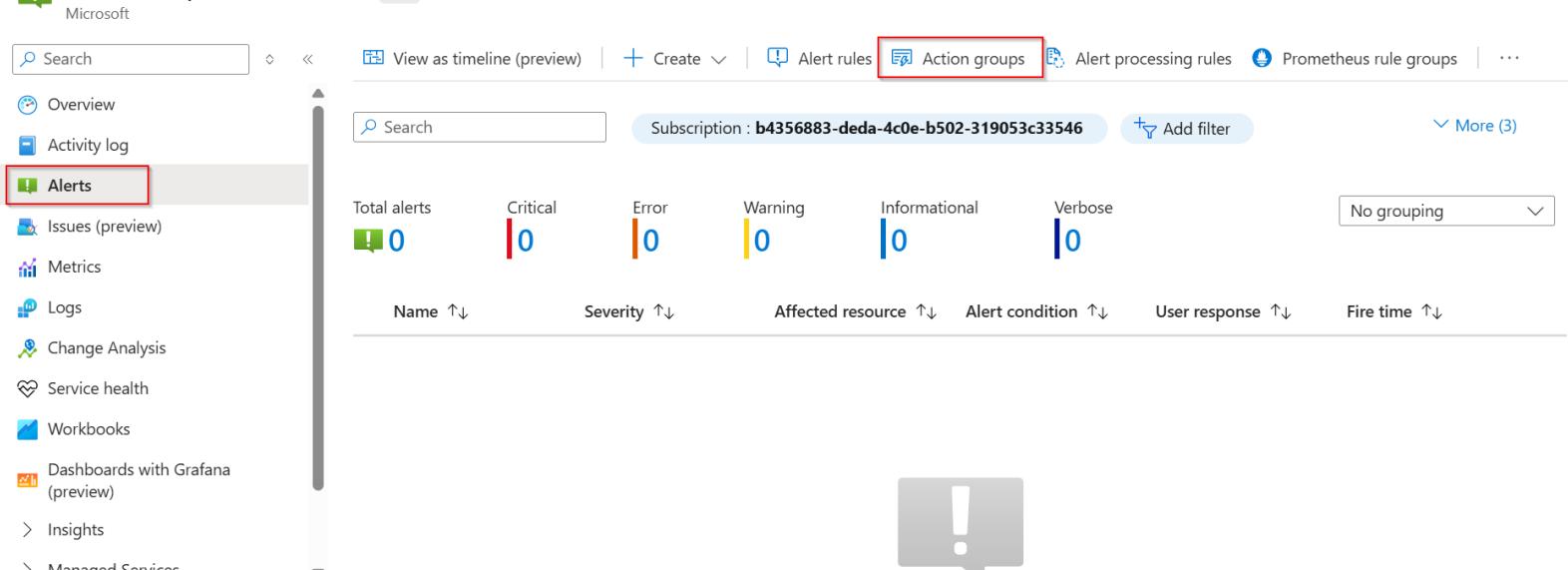
Subscription : b4356883-deda-4c0e-b502-319053c33546     Add filter     More (3)

Search     Total alerts     Critical     Error     Warning     Informational     Verbose     No grouping

Overview     Activity log     Alerts (highlighted with red box)     Issues (preview)     Metrics     Logs     Change Analysis     Service health     Workbooks     Dashboards with Grafana (preview)     Insights     Managed Services

Add or remove favorites by pressing *Ctrl+Shift+F*

26. On the **Action groups** page, view the action group created.



The screenshot shows the Microsoft Azure Monitor Alerts interface. At the top, there's a navigation bar with 'Microsoft Azure', 'Upgrade', a search bar, and user information. Below it, the title 'Alert rules' is displayed with a back arrow. A toolbar below the title includes 'Create', 'Columns', 'Refresh', 'Export to CSV', 'Open query', 'Delete', 'Enable', and 'Disable' buttons. There are also 'Search', 'Subscription: Azure subscription 1', 'Target scope: all', 'Target resource type: all', 'Add tag filter', 'More (3)', and 'No grouping' filters. The main table lists one alert rule:

Name ↑↓	Condition	Severity ↑↓	Target scope	Target resource type	Signal type ↑↓	Status ↑↓
<input type="checkbox"/> VM unavailability	VmAvailabilityMetric < 1	3 - Informational	All virtual machines in 'Se...' Virtual machine	Metrics	<input checked="" type="checkbox"/>	Enabled

At the bottom left, it says 'Showing 1 - 1 of 1 results.' and at the bottom right, there's a 'Give feedback' link.

## Outcome

The monitoring pipeline ensures rapid awareness of VM outages, improving service reliability, reducing response time, and enhancing operational resilience.

## Skills Demonstrated

- SIEM Configuration & Operations
- Cloud Security Monitoring
- Threat Detection Engineering
- Scheduled Analytics Rule Development

- Threat Intelligence Integration
- KQL Reading & Interpretation
- Automation Workflow Configuration
- Cloud Reliability Engineering
- Alerting & Incident Response
- Technical Reporting & Documentation

## Conclusion

This project successfully integrates threat detection, cloud observability, and automated response capabilities within Microsoft Azure. By combining Sentinel analytics with Azure Monitor alerting pipelines, it demonstrates practical SOC-ready expertise, the ability to engineer detections aligned with real-world threats, and the operational mindset required for security engineering and cloud monitoring roles.