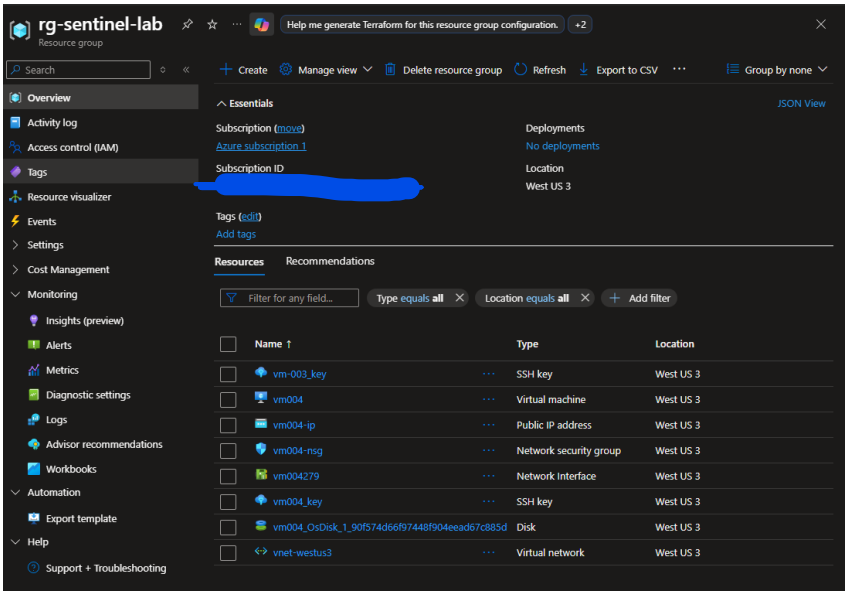
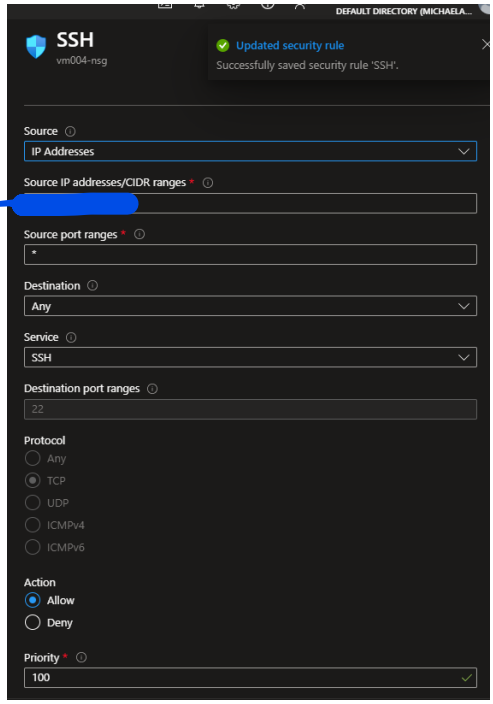
Azure - Microsoft Sentinel Lab

1. Creating Resource Group (rg-sentinel-lab) and VM (vm-004)

   - Deployed Ubuntu Server VM with SSH key authentication.

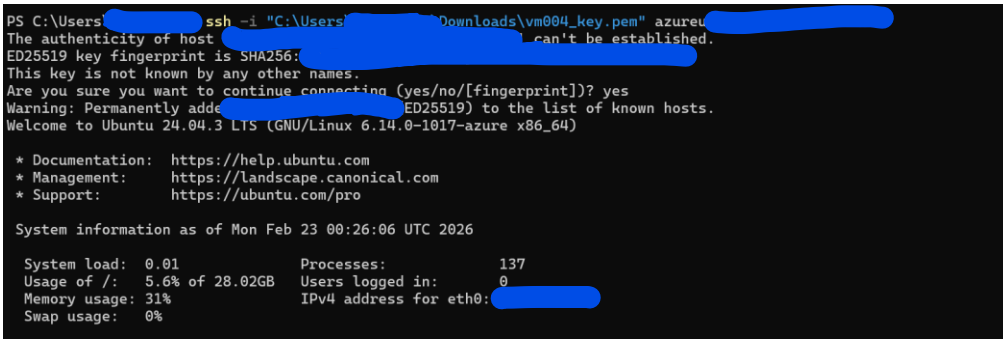


   - Configured NSG to allow SSH only from your IP.



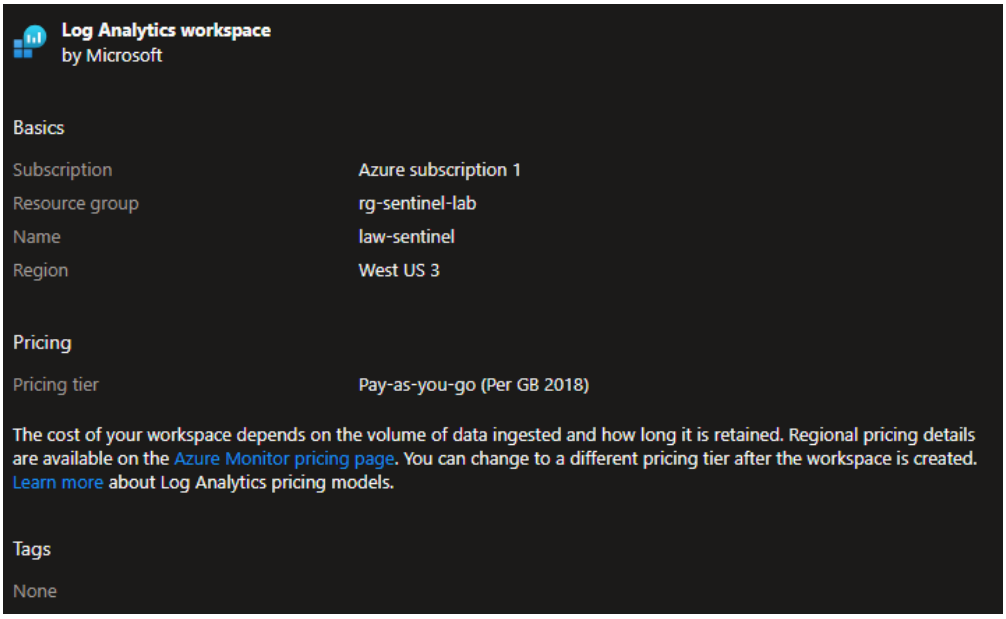
2. Connecting to VM server

- Used ssh azureuser@ with SSH key

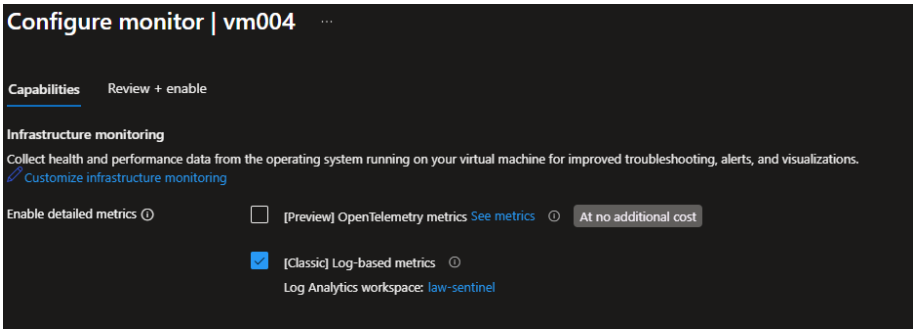


3. Create Log Analytics Workspace (law-sentinel)

- Created LAW in the same region as VM.



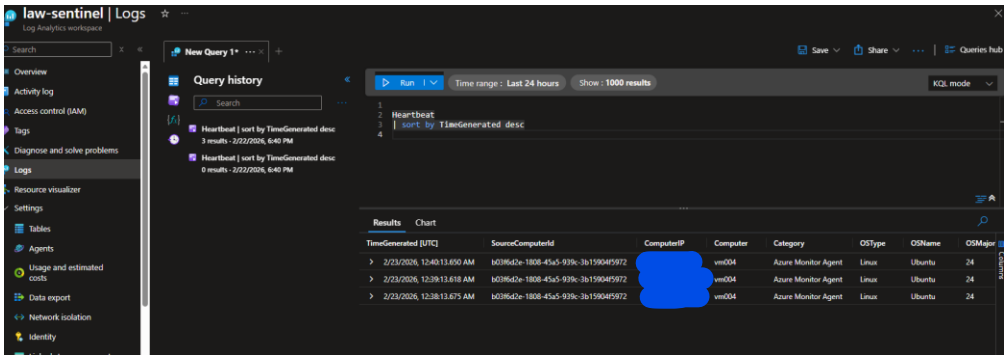
4. Install Azure Monitor Agent (AMA)
    a. - Onboarded VM from Monitor -> Virtual Machines.



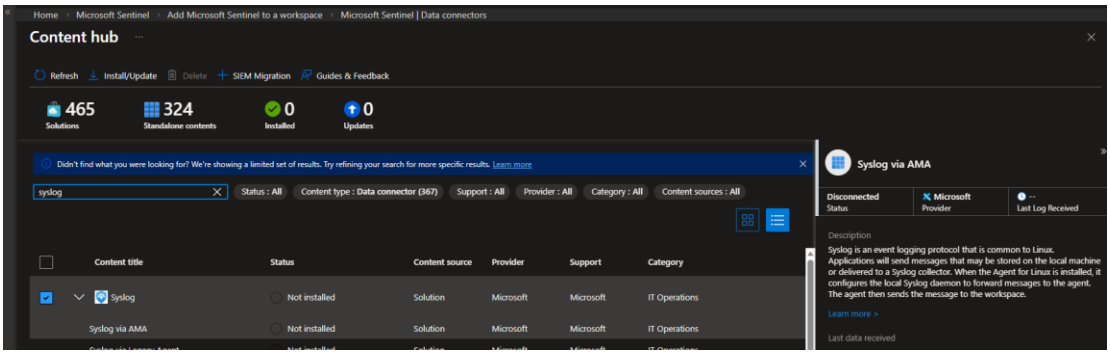
b. AMA is installed ✅

c. Confirmed LAW is working properly with VM via heartbeat

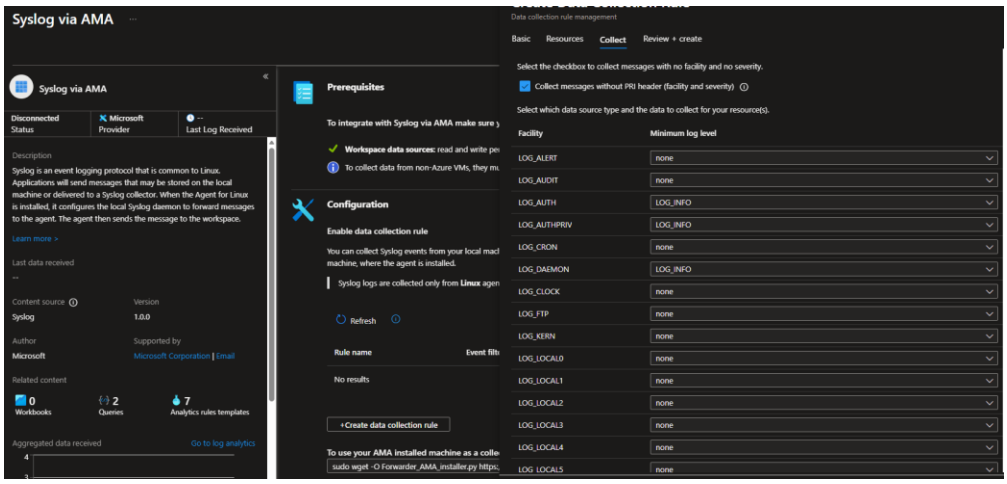
Query: Heartbeat | sort by TimeGenerated desc



5. Create Microsoft Sentinel: Syslog Data Collection Rule (DCR)

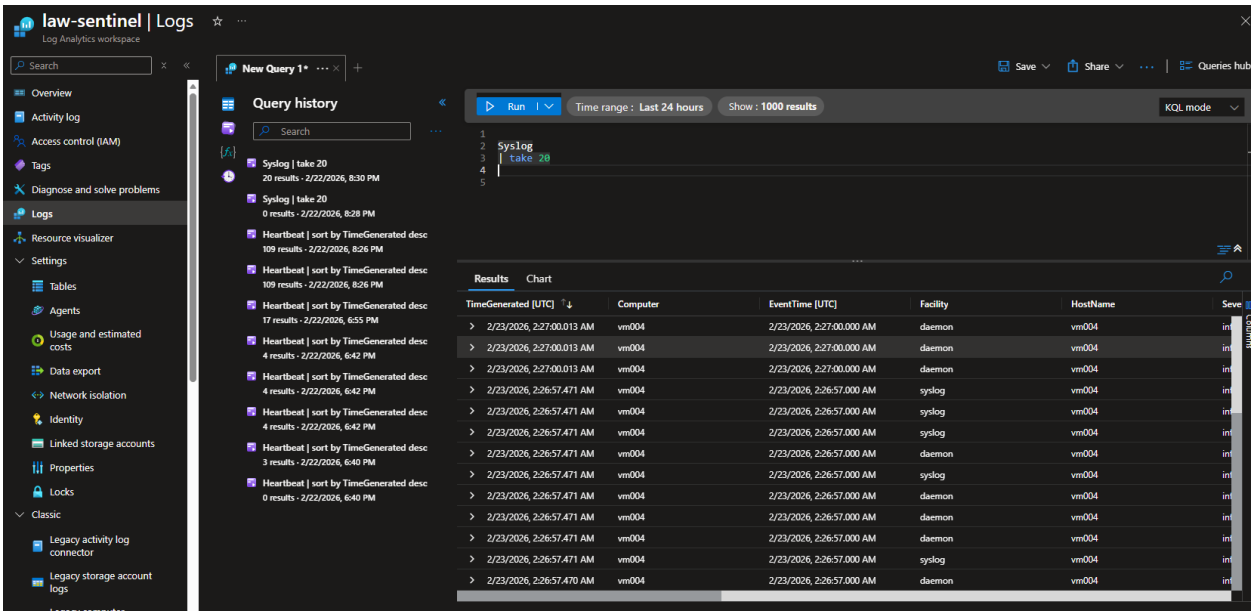


a. - Enabled syslog facilities: auth, authpriv, daemon, syslog.



- Destination: law-sentinel.

-Query test syslog integration: Syslog | take 20

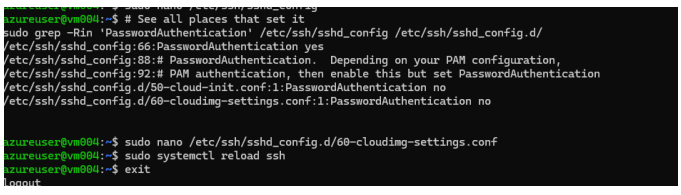


b. - Associated VM to DCR

6. Enable PasswordAuthentication on VM

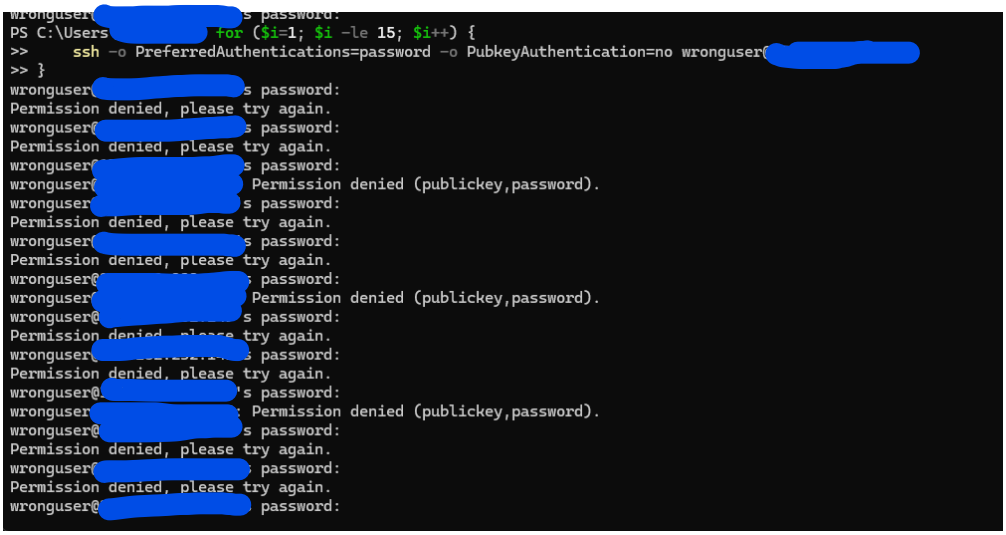
a. - Edited /etc/ssh/sshd_config and /etc/ssh/sshd_config.d/60-cloudimg-settings.conf.

i. Set passwordauthenication on so we can test brute force

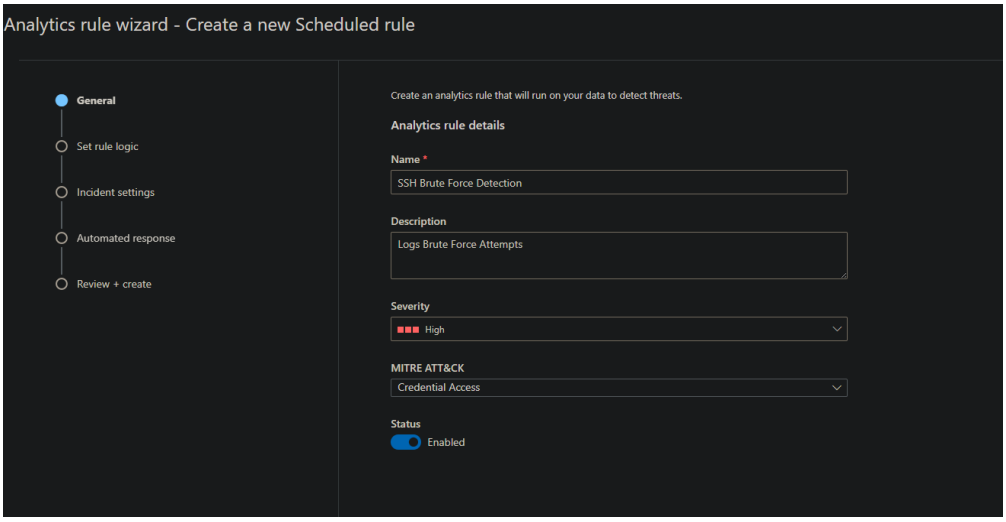


b. - Set PasswordAuthentication yes, restarted SSH.

7. Run brute-force simulation from local machine
    a. - Used PowerShell loop to generate failed SSH password attempts.



8. Build Sentinel Analytic Rule (SSH Brute Force Detection)
    a. - Created Scheduled Query Rule in Defender portal.

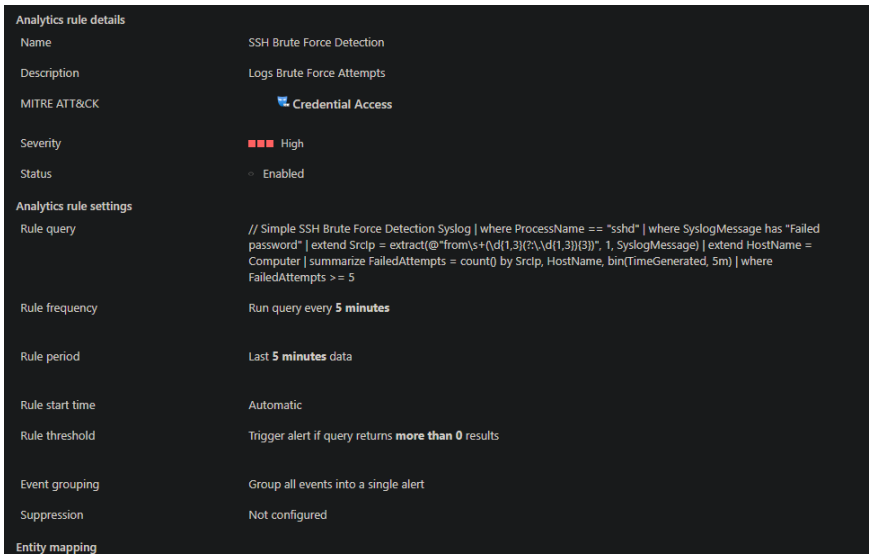


    b. - Added KQL to detect >5 failures in 5 minutes.
    c. - Entity mapping: SourceIP -> IP entity, HostName -> Host entity.

    d. - Enabled alert grouping.

Simple SSH Brute Force Detection Rule:

```
Syslog
| where ProcessName == "sshd"
| where SyslogMessage has "Failed password"
| extend SrcIp = extract(@"from\s+(\d{1,3}(?:\.\d{1,3}){3})", 1, SyslogMessage)
| extend HostName = Computer
| summarize FailedAttempts = count() by SrcIp, HostName, bin(TimeGenerated, 5m)
| where FailedAttempts >= 5
```



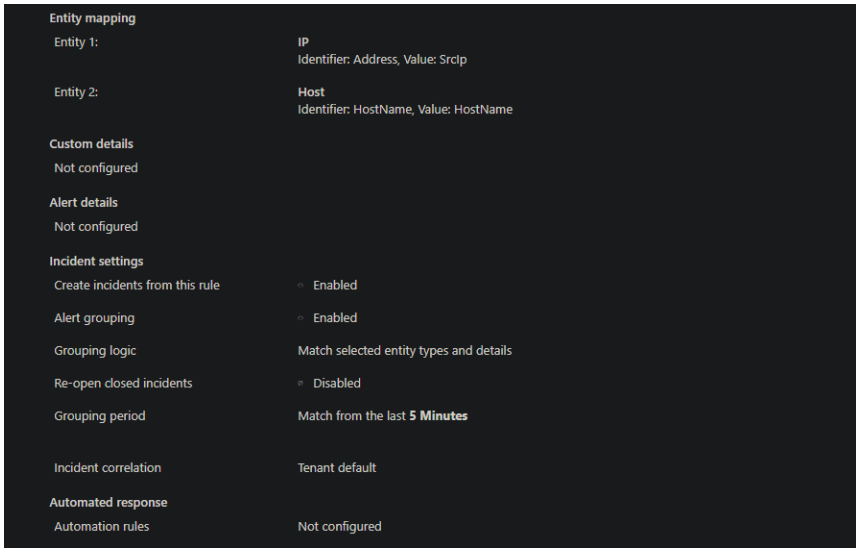
Analytics rule details

Name	SSH Brute Force Detection
Description	Logs Brute Force Attempts
MITRE ATT&CK	Credential Access
Severity	High
Status	Enabled

Analytics rule settings

Rule query	// Simple SSH Brute Force Detection Syslog | where ProcessName == "sshd" | where SyslogMessage has "Failed password" | extend SrcIp = extract(@"from\s+(\d{1,3}(?:\.\d{1,3}){3})", 1, SyslogMessage) | extend HostName = Computer | summarize FailedAttempts = count() by SrcIp, HostName, bin(TimeGenerated, 5m) | where FailedAttempts >= 5
Rule frequency	Run query every **5 minutes**
Rule period	Last **5 minutes** data
Rule start time	Automatic
Rule threshold	Trigger alert if query returns **more than 0** results
Event grouping	Group all events into a single alert
Suppression	Not configured

Entity mapping



Entity mapping

Entity 1:	**IP** Identifier: Address, Value: SrcIp
Entity 2:	**Host** Identifier: HostName, Value: HostName

Custom details

Not configured

Alert details

Not configured

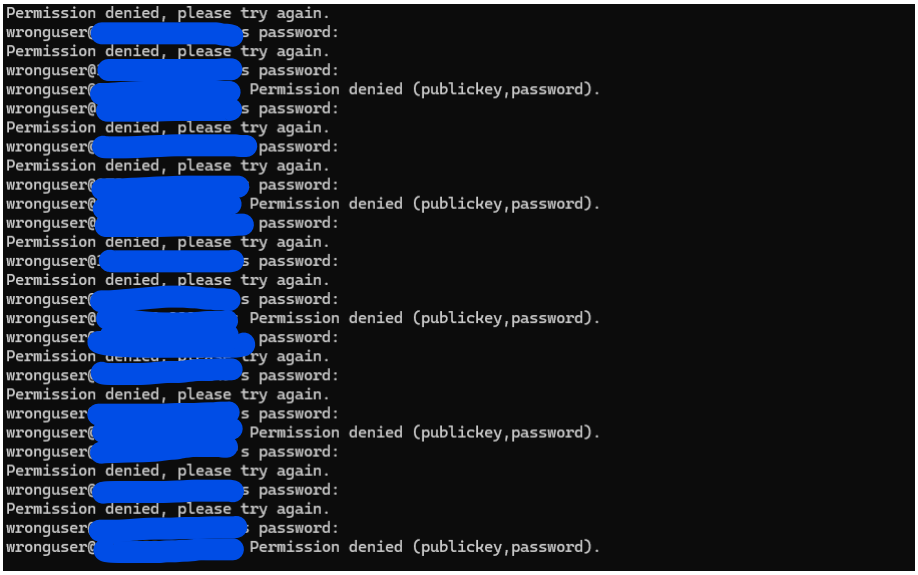
Incident settings

Create incidents from this rule	Enabled
Alert grouping	Enabled
Grouping logic	Match selected entity types and details
Re-open closed incidents	Disabled
Grouping period	Match from the last **5 Minutes**
Incident correlation	Tenant default

Automated response

Automation rules	Not configured

9. Validate Incident Creation
    i. - Verified incidents in Microsoft Defender -> Incidents.
        1. Brute forced



    ii. - Confirmed high-severity brute-force detection triggered