SOC Home Lab for Threat Detection and Incident Response using Microsoft Sentinel

Tony Philip

December 2025

Abstract

This report documents a home Security Operations Centre (SOC) lab built to simulate attacks, ingest telemetry into Microsoft Sentinel, detect malicious activity, and perform incident response. The lab demonstrates attack simulation (brute force, suspicious PowerShell), data ingestion using Azure Arc and Log Analytics, analytics rules in Sentinel, and investigation workflows. Relevant screenshots from the lab are included close to the descriptive text.

Contents

1 Executive Summary **2**

2 Architecture and Components **2**
2.1 High-level Architecture 2
2.2 Architecture Diagram 2

3 Tools & Technologies **3**

4 Lab Setup **3**
4.1 VMs and Agents 3
4.2 Log Collection 4

5 Attack Simulations **5**

6 Detection Rules and Analytics **5**

7 Alerts and Incidents **7**

8 Log Analysis and KQL **7**

9 Investigation Workflow **8**

10 Results & Outcomes **10**

11 Conclusion and Recommendations **10**

1 Executive Summary

This project builds an end-to-end SOC home lab using a Windows 10 victim machine and a Kali Linux attacker machine. Logs are ingested into an Azure Log Analytics workspace via Azure Arc; Microsoft Sentinel is used as the SIEM to create analytics rules, generate alerts, and manage incidents. The lab validates detection of brute-force attacks and suspicious PowerShell execution and illustrates the triage and investigation steps.

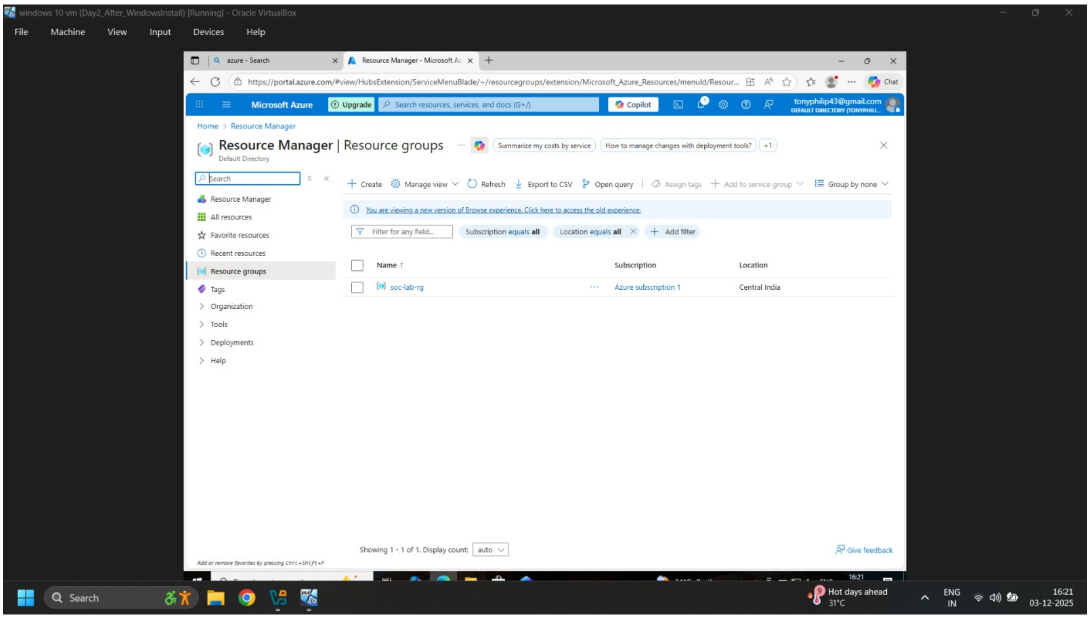
2 Architecture and Components

2.1 High-level Architecture

The lab architecture contains the following main components:

- **Windows 10 VM (Victim):** Host for Windows event logging, Sysmon and PowerShell telemetry.
- **Kali Linux VM (Attacker):** Used to run offensive tools (Hydra, Nmap) and simulate adversary activity.
- **Azure Arc Agent:** Onboard the Windows VM to Azure for log forwarding.
- **Log Analytics Workspace:** Central log store (”soclaws-workspace”).
- **Microsoft Sentinel:** SIEM for detection, analytics rules, alerts, and incidents.

2.2 Architecture Diagram



Resource Manager | Resource groups
Default Directory

You are viewing a new version of Browse experience. Click here to access the old experience.

Name ↑	Subscription	Location
soc-lab-rg	Azure subscription 1	Central India

Showing 1 - 1 of 1. Display count: auto

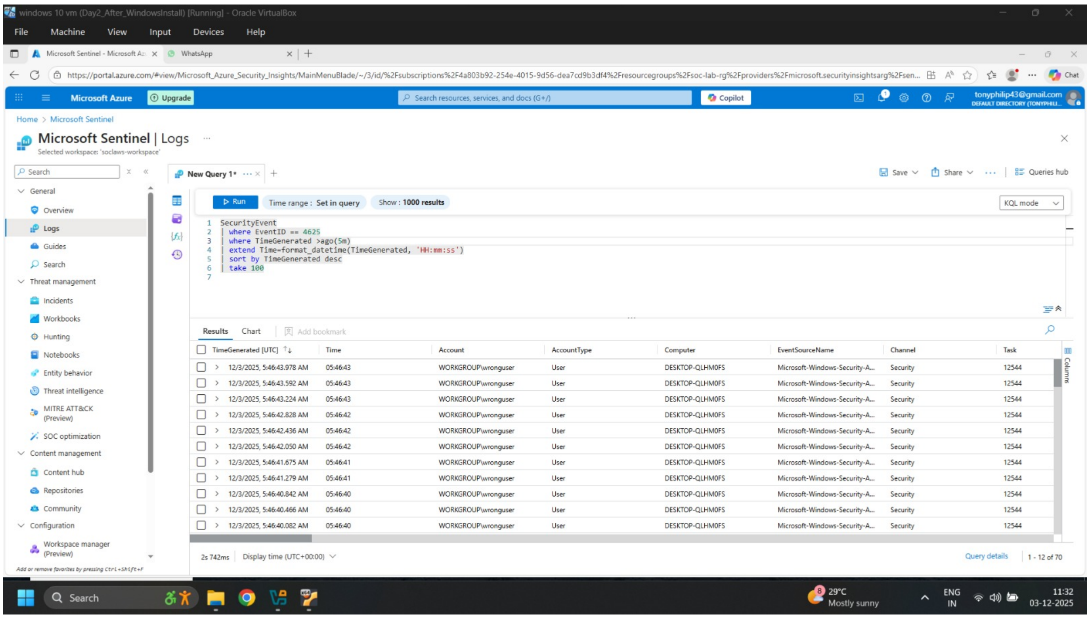
Add or remove favorites by pressing Ctrl+Shift+F

Figure 1: Azure Resource Manager showing the resource group (soc-lab-rg) and Log Analytics workspace.

3 Tools & Technologies

Key tools and technologies used in the lab:

- Microsoft Azure: Resource Manager, Azure Arc, Log Analytics, Sentinel.
- Microsoft Sentinel: Analytics rules, Incidents, Hunting, Workbooks.
- Sysmon and Windows Event Logging: Detailed endpoint telemetry.
- Kali Linux tools: Hydra (brute force), Nmap for reconnaissance.
- Kusto Query Language (KQL): Log queries and hunting.



```
SecurityEvent
| where EventID == 4625
| where TimeGenerated >ago(5m)
| extend Time=format_datetime(TimeGenerated, 'HH:mm:ss')
| sort by TimeGenerated desc
| take 100
```

TimeGenerated [UTC]	Time	Account	AccountType	Computer	EventSourceName	Channel	Task
12/3/2025, 5:46:43.978 AM	05:46:43	WORKGROUP\wronguser	User	DESKTOP-QLHM0FS	Microsoft-Windows-Security-A...	Security	12544
12/3/2025, 5:46:43.592 AM	05:46:43	WORKGROUP\wronguser	User	DESKTOP-QLHM0FS	Microsoft-Windows-Security-A...	Security	12544
12/3/2025, 5:46:43.224 AM	05:46:43	WORKGROUP\wronguser	User	DESKTOP-QLHM0FS	Microsoft-Windows-Security-A...	Security	12544
12/3/2025, 5:46:42.828 AM	05:46:42	WORKGROUP\wronguser	User	DESKTOP-QLHM0FS	Microsoft-Windows-Security-A...	Security	12544
12/3/2025, 5:46:42.436 AM	05:46:42	WORKGROUP\wronguser	User	DESKTOP-QLHM0FS	Microsoft-Windows-Security-A...	Security	12544
12/3/2025, 5:46:42.050 AM	05:46:42	WORKGROUP\wronguser	User	DESKTOP-QLHM0FS	Microsoft-Windows-Security-A...	Security	12544
12/3/2025, 5:46:41.675 AM	05:46:41	WORKGROUP\wronguser	User	DESKTOP-QLHM0FS	Microsoft-Windows-Security-A...	Security	12544
12/3/2025, 5:46:41.279 AM	05:46:41	WORKGROUP\wronguser	User	DESKTOP-QLHM0FS	Microsoft-Windows-Security-A...	Security	12544
12/3/2025, 5:46:40.842 AM	05:46:40	WORKGROUP\wronguser	User	DESKTOP-QLHM0FS	Microsoft-Windows-Security-A...	Security	12544
12/3/2025, 5:46:40.466 AM	05:46:40	WORKGROUP\wronguser	User	DESKTOP-QLHM0FS	Microsoft-Windows-Security-A...	Security	12544
12/3/2025, 5:46:40.082 AM	05:46:40	WORKGROUP\wronguser	User	DESKTOP-QLHM0FS	Microsoft-Windows-Security-A...	Security	12544

2s 742ms | Display time (UTC+00:00) | Query details | 1 - 12 of 70

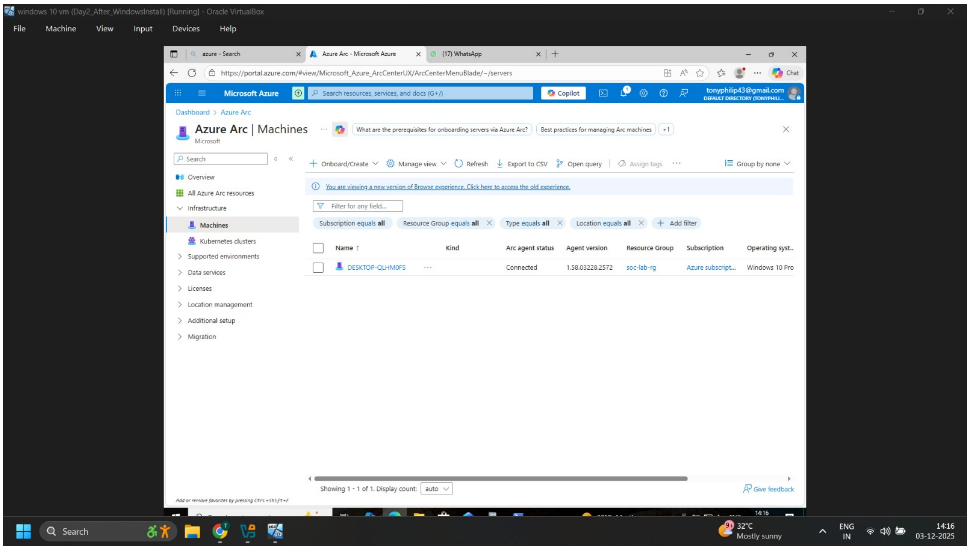
Figure 2: Microsoft Sentinel Logs view showing SecurityEvent queries (example query for EventID=4625 - failed logon).

4 Lab Setup

This section explains how the environment was prepared and connected to Azure Sentinel.

4.1 VMs and Agents

1. Deploy Windows 10 VM and Kali Linux VM in a host-only or NAT network to allow controlled attacks.
2. Onboard the Windows VM to Azure using the *Azure Arc* agent. Verify it appears in Azure Arc Machines. (Screenshot below.)



https://portal.azure.com/#view/Microsoft_Azure_ArcCenterUX/ArcCenterMenuBlade/~/servers

Azure Arc | Machines
Microsoft

You are viewing a new version of Browse experience. Click here to access the old experience.

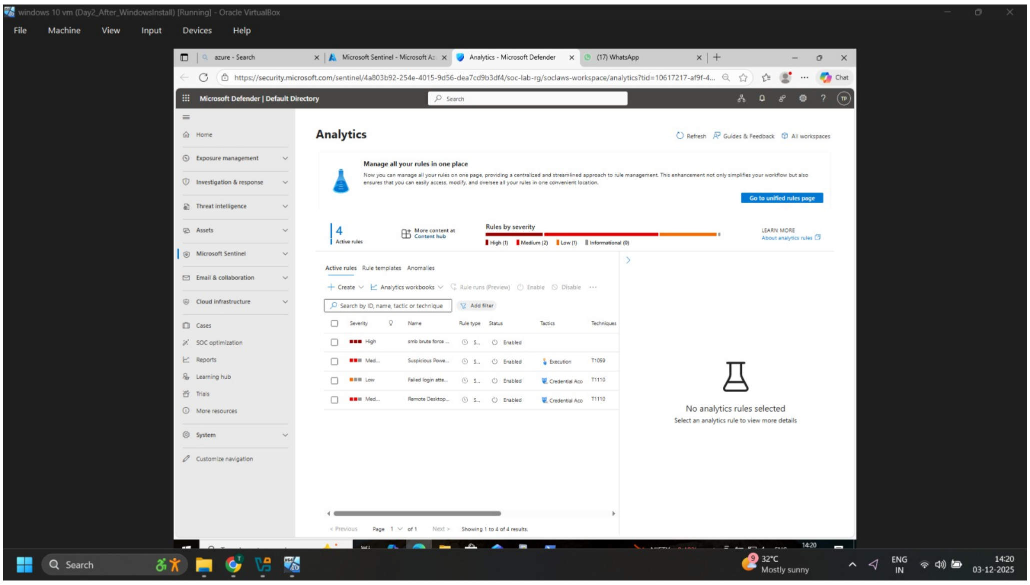
Name ↑	Kind	Arc agent status	Agent version	Resource Group	Subscription	Operating syst..
DESKTOP-QLHM0FS		Connected	1.58.03228.2572	soc-lab-rg	Azure subscript...	Windows 10 Pro

Showing 1 - 1 of 1. Display count: auto

Figure 3: Azure Arc Machines showing the onboarded Windows machine (Connected).

4.2 Log Collection

- Enabled Windows Security, System, Application and PowerShell logs.
- Installed and configured Sysmon for enhanced process and network telemetry.
- Forwarded logs to the Log Analytics workspace (soclaws-workspace). See workspace overview below.



https://security.microsoft.com/sentinel/4a803b92-254e-4015-9d56-dea7cd9b3df4/soc-lab-rg/soclaws-workspace/analytics?tid=10617217-af9f-4...

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.

4
Active rules

Rules by severity
High (1) Medium (2) Low (1) Informational (0)

Severity	Name	Rule type	Status	Tactics	Techniques
High	smb brute force ...	S...	Enabled		
Med...	Suspicious Powe...	S...	Enabled	Execution	T1059
Low	Failed login atte...	S...	Enabled	Credential Acc	T1110
Med...	Remote Desktop...	S...	Enabled	Credential Acc	T1110

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

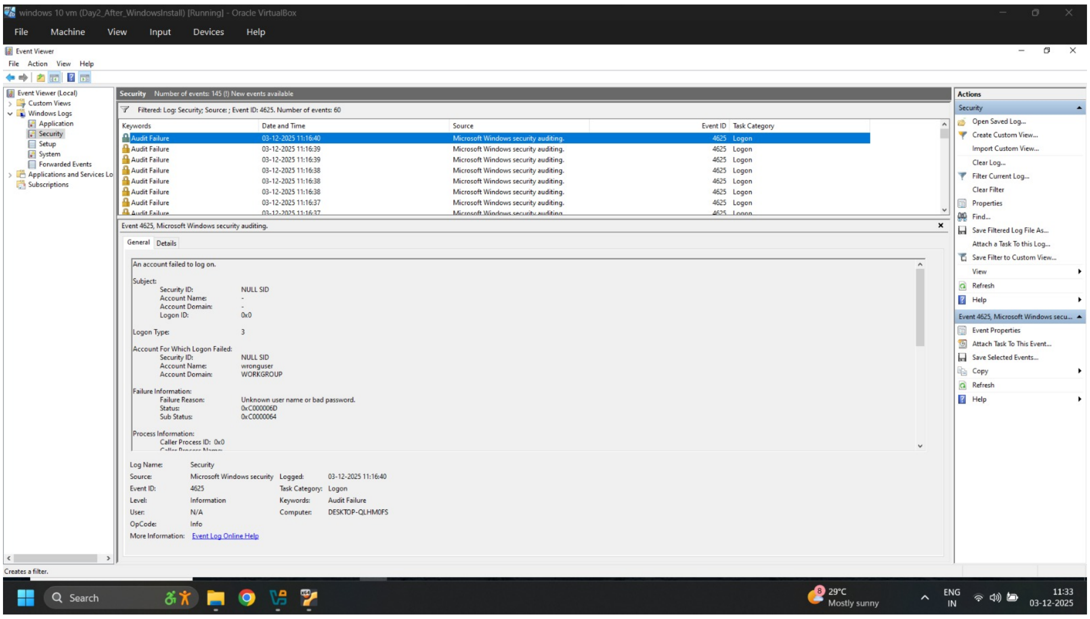
Showing 1 to 4 of 4 results.

Figure 4: Log Analytics workspace (soclaws-workspace) essential details and connectivity status.

5 Attack Simulations

We simulated multiple attacks from the Kali VM targeting the Windows VM. The two key scenarios used were:

1. **SMB / RDP Brute-force:** Multiple failed authentication attempts to a local account (EventID 4625) using Hydra.
2. **Suspicious PowerShell Execution:** Executing scripts and commands intended to mimic attacker post-exploitation behavior.



Security Number of events: 145 (!) New events available

Filtered: Log: Security; Source: ; Event ID: 4625. Number of events: 60

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	03-12-2025 11:16:40	Microsoft Windows security auditing.	4625	Logon
Audit Failure	03-12-2025 11:16:39	Microsoft Windows security auditing.	4625	Logon
Audit Failure	03-12-2025 11:16:39	Microsoft Windows security auditing.	4625	Logon
Audit Failure	03-12-2025 11:16:38	Microsoft Windows security auditing.	4625	Logon
Audit Failure	03-12-2025 11:16:38	Microsoft Windows security auditing.	4625	Logon
Audit Failure	03-12-2025 11:16:38	Microsoft Windows security auditing.	4625	Logon
Audit Failure	03-12-2025 11:16:37	Microsoft Windows security auditing.	4625	Logon
Audit Failure	03-12-2025 11:16:37	Microsoft Windows security auditing.	4625	Logon

Event 4625, Microsoft Windows security auditing.

```
An account failed to log on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           wronguser
        Account Domain:         WORKGROUP

Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xC000006D
        Sub Status:             0xC0000064

Process Information:
        Caller Process ID:  0x0
        Caller Process Name:
```

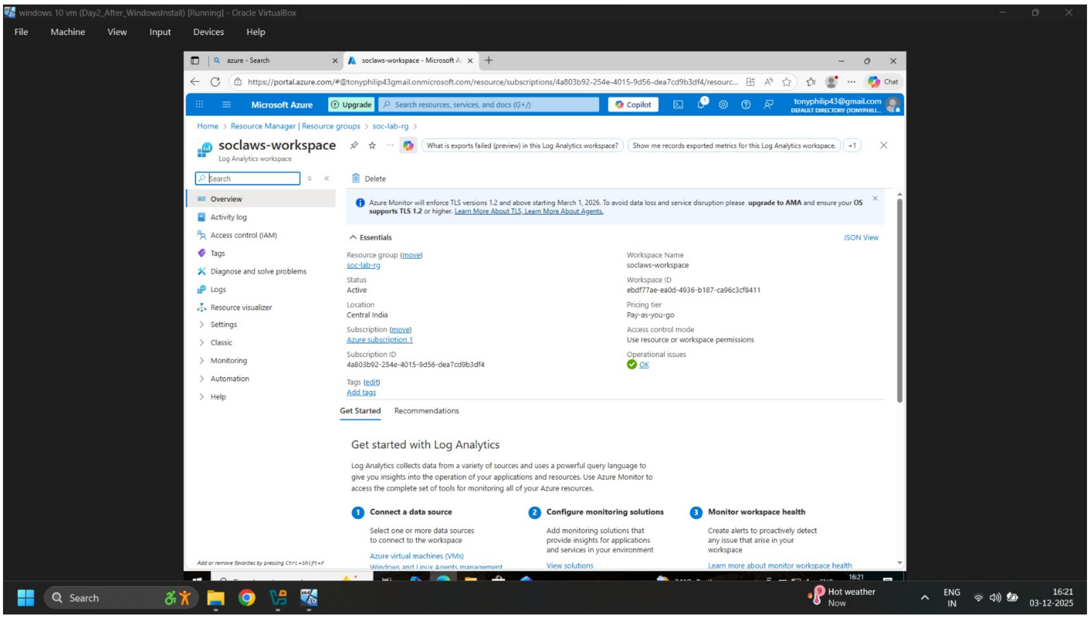
```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          03-12-2025 11:16:40
Event ID:          4625                         Task Category:   Logon
Level:             Information                  Keywords:        Audit Failure
User:              N/A                          Computer:        DESKTOP-QLHM0FS
OpCode:            Info
More Information:  Event Log Online Help
```

Figure 5: Windows Event Viewer showing repeated Event ID 4625 (Audit Failure — failed logon). This correlates to brute-force attempts.

6 Detection Rules and Analytics

Using Microsoft Sentinel, analytics rules were created or enabled to detect suspicious activity. Example rules used in the lab:

- SMB brute force detection (High severity)
- Suspicious PowerShell execution (Medium severity)
- Failed login attempts aggregation (Low/Medium severity)
- Remote Desktop brute force (Medium severity)


windows 10 vm (Day2_After_WindowsInstall) [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
azure - Search
soclaws-workspace - Microsoft A
https://portal.azure.com/#@tonyphilip43gmail.onmicrosoft.com/resource/subscriptions/4a803b92-254e-4015-9d56-dea7cd9b3df4/resourc...
Chat
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
tonyphilip43@gmail.com
DEFAULT DIRECTORY (TONYPHILI...
Home > Resource Manager | Resource groups > soc-lab-rg >
What is exports failed (preview) in this Log Analytics workspace?
Show me records exported metrics for this Log Analytics workspace.
+1
Search
Delete
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Resource visualizer
Settings
Classic
Monitoring
Automation
Help
Add or remove favorites by pressing Ctrl+Shift+F
Essentials
JSON View
Get Started
Recommendations
Search
Hot weather
Now
ENG
IN
16:21
03-12-2025

soclaws-workspace
Log Analytics workspace

Azure Monitor will enforce TLS versions 1.2 and above starting March 1, 2026. To avoid data loss and service disruption please **upgrade to AMA** and ensure your OS **supports TLS 1.2** or higher. Learn More About TLS, Learn More About Agents.

Resource group (move)
soc-lab-rg

Status
Active

Location
Central India

Subscription (move)
Azure subscription 1

Subscription ID
4a803b92-254e-4015-9d56-dea7cd9b3df4

Tags (edit)
Add tags

Workspace Name
soclaws-workspace

Workspace ID
ebdf77ae-ea0d-4936-b187-ca96c3cf8411

Pricing tier
Pay-as-you-go

Access control mode
Use resource or workspace permissions

Operational issues
OK

Get started with Log Analytics

Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources. Use Azure Monitor to access the complete set of tools for monitoring all of your Azure resources.

1 **Connect a data source**

Select one or more data sources to connect to the workspace

Azure virtual machines (VMs)

Windows and Linux Agents management

2 **Configure monitoring solutions**

Add monitoring solutions that provide insights for applications and services in your environment

View solutions

3 **Monitor workspace health**

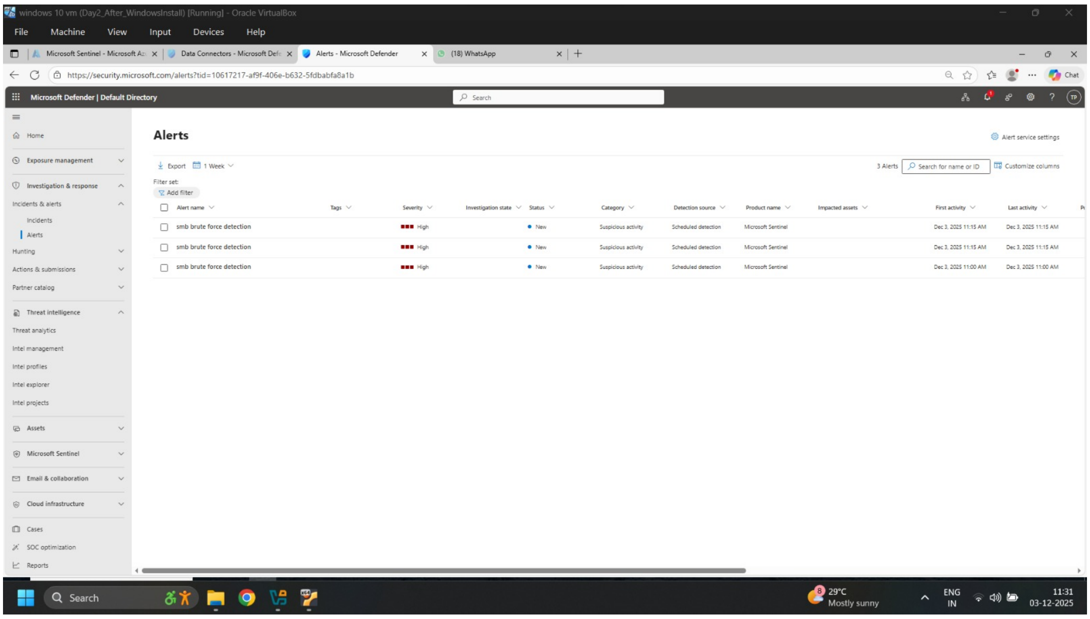
Create alerts to proactively detect any issue that arise in your workspace

Learn more about monitor workspace health

Figure 6: Microsoft Defender / Sentinel Analytics rules dashboard showing active rules and severity.

7 Alerts and Incidents

When the analytics rules triggered, Sentinel generated alerts and grouped them into incidents for investigation. Below are screenshots from the Alerts and Incidents pages.

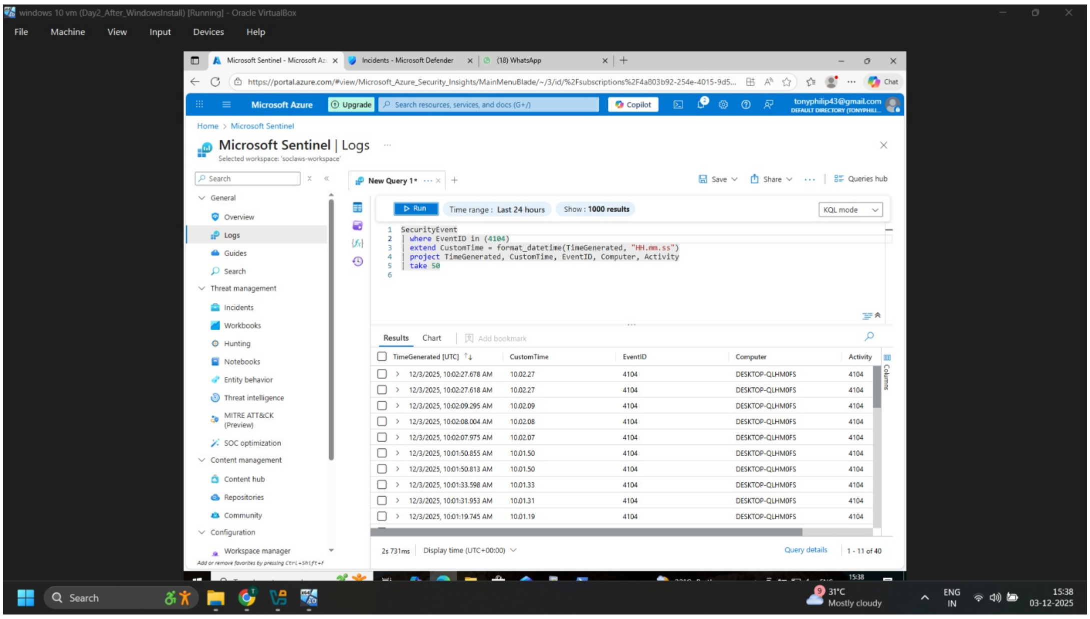


Alerts

3 Alerts

Alert name	Tags	Severity	Investigation state	Status	Category	Detection source	Product name	Impacted assets	First activity	Last activity
smb brute force detection		High		New	Suspicious activity	Scheduled detection	Microsoft Sentinel		Dec 3, 2025 11:15 AM	Dec 3, 2025 11:15 AM
smb brute force detection		High		New	Suspicious activity	Scheduled detection	Microsoft Sentinel		Dec 3, 2025 11:15 AM	Dec 3, 2025 11:15 AM
smb brute force detection		High		New	Suspicious activity	Scheduled detection	Microsoft Sentinel		Dec 3, 2025 11:00 AM	Dec 3, 2025 11:00 AM

Figure 7: Alerts list showing several ”smb brute force detection” alerts created by scheduled analytics rules.



Microsoft Sentinel | Logs

Time range : Last 24 hours Show : 1000 results KQL mode

```
SecurityEvent
| where EventID in (4104)
| extend CustomTime = format_datetime(TimeGenerated, "HH.mm.ss")
| project TimeGenerated, CustomTime, EventID, Computer, Activity
| take 50
```

TimeGenerated [UTC]	CustomTime	EventID	Computer	Activity
12/3/2025, 10:02:27.678 AM	10.02.27	4104	DESKTOP-QLHM0FS	4104
12/3/2025, 10:02:27.618 AM	10.02.27	4104	DESKTOP-QLHM0FS	4104
12/3/2025, 10:02:09.295 AM	10.02.09	4104	DESKTOP-QLHM0FS	4104
12/3/2025, 10:02:08.004 AM	10.02.08	4104	DESKTOP-QLHM0FS	4104
12/3/2025, 10:02:07.975 AM	10.02.07	4104	DESKTOP-QLHM0FS	4104
12/3/2025, 10:01:50.855 AM	10.01.50	4104	DESKTOP-QLHM0FS	4104
12/3/2025, 10:01:50.813 AM	10.01.50	4104	DESKTOP-QLHM0FS	4104
12/3/2025, 10:01:33.598 AM	10.01.33	4104	DESKTOP-QLHM0FS	4104
12/3/2025, 10:01:31.953 AM	10.01.31	4104	DESKTOP-QLHM0FS	4104
12/3/2025, 10:01:19.745 AM	10.01.19	4104	DESKTOP-QLHM0FS	4104

2s 731ms Display time (UTC+00:00) 1 - 11 of 40

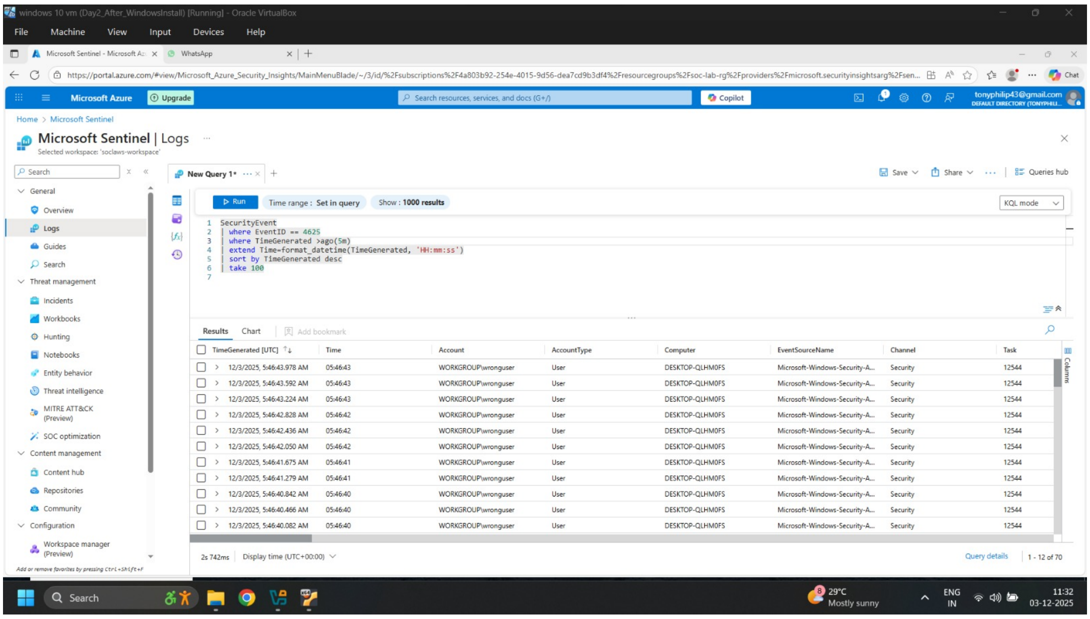
Figure 8: Incidents view in Microsoft Sentinel aggregating related alerts into incidents for triage and response.

8 Log Analysis and KQL

Kusto Query Language (KQL) was used for log exploration, validation, and hunting. Example queries used include:

```
SecurityEvent
| where EventID == 4625
| where TimeGenerated > ago(5m)
| extend Time=format_datetime(TimeGenerated,’HH:mm:ss’)
| sort by TimeGenerated desc
| take 100
```

The query results confirmed repeated failed logons from the test account (wronguser) which matched the attacker activity. Screenshot of KQL query results is shown below.


windows 10 vm (Day2_After_WindowsInstall) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Microsoft Sentinel - Microsoft Az
WhatsApp
https://portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/3/id/%2Fsubscriptions%2F4a803b92-254e-4015-9d56-dea7cd9b3df4%2Fresourcegroups%2Fsoc-lab-rg%2Fproviders%2Fmicrosoft.securityinsightsarg%2Fsen...
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
tonyphilip43@gmail.com
DEFAULT DIRECTORY (TONYPHILI...
Home > Microsoft Sentinel
Microsoft Sentinel | Logs
Selected workspace: 'soclaws-workspace'
Search
General
Overview
Logs
Guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
SOC optimization
Content management
Content hub
Repositories
Community
Configuration
Workspace manager (Preview)
New Query 1*
Save
Share
Queries hub
Run
Time range : Set in query
Show : 1000 results
KQL mode
Results
Chart
Add bookmark
Columns
2s 742ms
Display time (UTC+00:00)
Query details
1 - 12 of 70
Search
29°C
Mostly sunny
ENG
IN
11:32
03-12-2025

```
SecurityEvent
| where EventID == 4625
| where TimeGenerated >ago(5m)
| extend Time=format_datetime(TimeGenerated, 'HH:mm:ss')
| sort by TimeGenerated desc
| take 100
```

TimeGenerated [UTC]	Time	Account	AccountType	Computer	EventSourceName	Channel	Task
12/3/2025, 5:46:43.978 AM	05:46:43	WORKGROUP\wronguser	User	DESKTOP-QLHMOFS	Microsoft-Windows-Security-A...	Security	12544
12/3/2025, 5:46:43.592 AM	05:46:43	WORKGROUP\wronguser	User	DESKTOP-QLHMOFS	Microsoft-Windows-Security-A...	Security	12544
12/3/2025, 5:46:43.224 AM	05:46:43	WORKGROUP\wronguser	User	DESKTOP-QLHMOFS	Microsoft-Windows-Security-A...	Security	12544
12/3/2025, 5:46:42.828 AM	05:46:42	WORKGROUP\wronguser	User	DESKTOP-QLHMOFS	Microsoft-Windows-Security-A...	Security	12544
12/3/2025, 5:46:42.436 AM	05:46:42	WORKGROUP\wronguser	User	DESKTOP-QLHMOFS	Microsoft-Windows-Security-A...	Security	12544
12/3/2025, 5:46:42.050 AM	05:46:42	WORKGROUP\wronguser	User	DESKTOP-QLHMOFS	Microsoft-Windows-Security-A...	Security	12544
12/3/2025, 5:46:41.675 AM	05:46:41	WORKGROUP\wronguser	User	DESKTOP-QLHMOFS	Microsoft-Windows-Security-A...	Security	12544
12/3/2025, 5:46:41.279 AM	05:46:41	WORKGROUP\wronguser	User	DESKTOP-QLHMOFS	Microsoft-Windows-Security-A...	Security	12544
12/3/2025, 5:46:40.842 AM	05:46:40	WORKGROUP\wronguser	User	DESKTOP-QLHMOFS	Microsoft-Windows-Security-A...	Security	12544
12/3/2025, 5:46:40.466 AM	05:46:40	WORKGROUP\wronguser	User	DESKTOP-QLHMOFS	Microsoft-Windows-Security-A...	Security	12544
12/3/2025, 5:46:40.082 AM	05:46:40	WORKGROUP\wronguser	User	DESKTOP-QLHMOFS	Microsoft-Windows-Security-A...	Security	12544

Figure 9: KQL query results listing multiple EventID 4625 entries with the account ”wronguser” and corresponding timestamps.

9 Investigation Workflow

When an incident is created, the typical SOC workflow followed in this lab was:

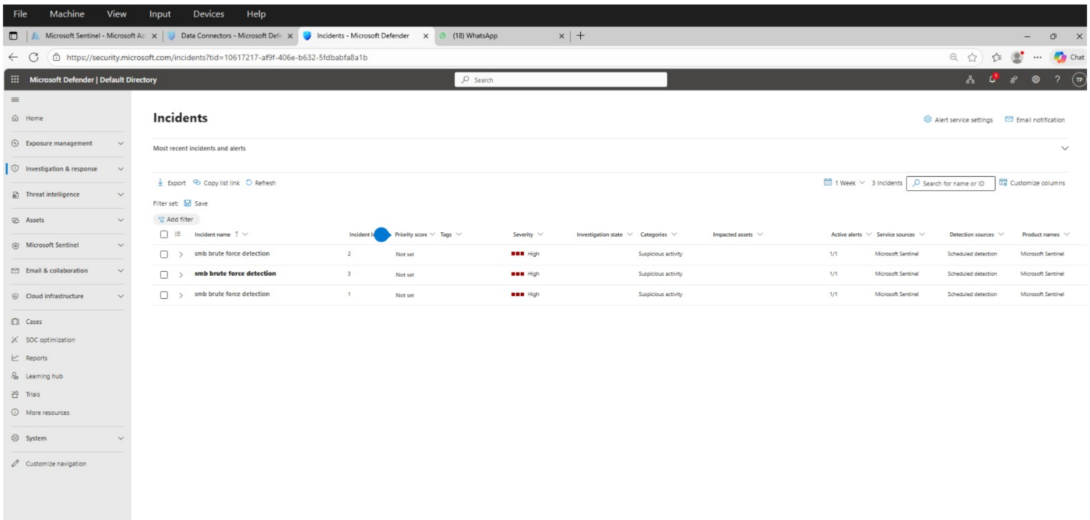
1. Triage: Confirm whether alerts are true positives (check logs, context).

2. Enrichment: Lookup related entities (IP addresses, hostnames, user accounts).

3. Containment: Isolate the affected host if necessary.

4. Remediation: Reset credentials, block attacker IPs, remove malicious binaries.

5. Post-Incident: Document timeline, root cause, and recommendations.



Incidents

Most recent incidents and alerts

3 Incidents

	Incident name	Incident I	Priority score	Tags	Severity	Investigation state	Categories	Impacted assets	Active alerts	Service sources	Detection sources	Product names
□	smb brute force detection	2	Not set		■■■ High		Suspicious activity		1/1	Microsoft Sentinel	Scheduled detection	Microsoft Sentinel
□	**smb brute force detection**	3	Not set		■■■ High		Suspicious activity		1/1	Microsoft Sentinel	Scheduled detection	Microsoft Sentinel
□	smb brute force detection	1	Not set		■■■ High		Suspicious activity		1/1	Microsoft Sentinel	Scheduled detection	Microsoft Sentinel

Figure 10: Additional Sentinel logs view with EventID 4104 entries (PowerShell logging) captured for analysis.

10 Results & Outcomes

The lab successfully:

- Detected simulated SMB/RDP brute-force attempts via analytics rules.
- Captured Windows event logs and PowerShell telemetry into Log Analytics.
- Generated alerts and grouped related signals into incidents for investigation.
- Demonstrated the end-to-end SOC workflow (detect, triage, investigate, remediate).

11 Conclusion and Recommendations

This SOC home lab proves that with proper instrumentation (Sysmon, PowerShell logging, Azure Arc) and tuned analytics in Microsoft Sentinel, an administrator can detect common attack patterns and carry out incident response processes.

Recommendations:

- Harden endpoint configurations (disable unnecessary services, enforce strong passwords).
- Enable advanced logging (Sysmon, PowerShell Script Block Logging) for richer telemetry.
- Tune analytics rules to reduce false positives and add suppression windows where appropriate.
- Maintain playbooks for common incidents to speed up response.