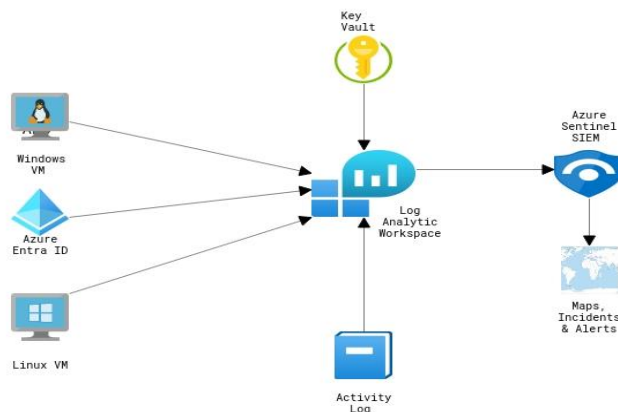


Report: Threat Detection and Monitoring with Sentinel

1. Introduction

With an emphasis on malware activity and brute force attacks, this assignment describes the deployment and efficiency of Azure Sentinel in identifying cybersecurity threats. The objective of this assignment was to evaluate Azure Sentinel's ability to collect endpoint logs, apply analytics rules, and identify potential security threats, such as repeated failed login attempts and malware activities.

These findings underscore the real-world applicability of Azure Sentinel in identifying and mitigating cybersecurity threats.



System Architecture

2. Key Objectives

- Set up Azure Sentinel to monitor both Windows and Linux endpoints.
- Identify brute force attacks by analysing repeated failed login attempts.
- Detect malware activities
- Automate incident generation for quick response.

3. Environment Setup

3.1 Azure Sentinel Configuration

- **Workspace Creation:** A new Log Analytics workspace was set up for Azure Sentinel

3.2 Data Connector Setup

Windows End Point: The Log Analytics Agent was installed on Windows endpoints to forward security logs to sentinel on Windows end point.


```
PS C:\Users\cyberlab> Get-Service -Name HealthService

Status      Name      DisplayName
-----
Running     HealthService  Microsoft Monitoring Agent

PS C:\Users\cyberlab>
```

```
PS C:\Users\cyberlab> wecutil qc
The service startup mode will be changed to Delay-Start. Would you like to proceed ( Y- yes or N- no)?Y
Windows Event Collector service was configured successfully.
PS C:\Users\cyberlab>
```

Screenshots showing the status of Azure Monitoring Agent(AMA)

Logs 

Cybersec-lab-analytics

```
1 Heartbeat
2 where OSType == 'Windows'
3 where Category == 'Azure Monitor Agent'
4 summarize ang_max(TimeGenerated, *) by SourceComputerId
5 sort by Computer
6 render table
```

Results Chart

SourceComputerId	TimeGenerated [UTC]	TenantId	SourceSystem	MG	ManagementG
8014c11a-4403-4316-812b-df69ac9de4d5	3/11/2025, 5:20:14.108 AM	fb90b8c-6ffe-4788-9d82-5132295dcee	OpsManager	00000000-0000-0000-0000-000000000001	AOI-fb90b8c-4
SourceComputerId	8014c11a-4403-4316-812b-df69ac9de4d5				
TimeGenerated [UTC]	2025-03-11T05:20:14.108568Z				
TenantId	fb90b8c-6ffe-4788-9d82-5132295dcee				
SourceSystem	OpsManager				
MG	00000000-0000-0000-0000-000000000001				

KQL query for showing status of AMA

Linux End point

Installed Syslog via AMA on the Linux machine.

created a Data Collection Rule and ran the provided script on the Linux machine to install AMA forwarder.

Syslog via AMA

Syslog via AMA

Connected Status **Microsoft Provider** 6 Minutes Ago Last Log Received

Description
Syslog is an event logging protocol that is common to Linux. Applications will send messages that may be stored on the local machine or delivered to a Syslog collector. When the Agent for Linux is installed, it configures the local Syslog daemon to forward messages to the agent. The agent then sends the message to the workspace.

Learn more >

Last data received
3/10/2023, 12:44:39 PM

Content source
Syslog

Version
1.0.0

Author
Microsoft

Supported by
Microsoft Corporation | Email

Related content
0 Workbooks 2 Queries 7 Analytics rules templates

Aggregated data received
Go to log analytics

Prerequisites

To integrate with Syslog via AMA make sure you have:

- ✓ **Workspace data sources:** read and write permissions.
- ❗ To collect data from non-Azure VMs, they must have Azure Arc installed and enabled. [Learn more](#)

Configuration

Enable data collection rule

You can collect Syslog events from your local machine by installing the agent on it. You can also collect Syslog generated on a different source by running the installation script below.

Syslog logs are collected only from **Linux** agents. For device specific configuration refer to the documentation. [Learn more](#)

Refresh

Rule name Event filter type

DCR-cyber log_auth : LOG_DEBUG

+ Create data collection rule

To use your AMA installed machine as a collector for logs from other machines, run this script on your AMA installed machine:

```
sudo wget -O Forwarder_AMA_installer.py https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/DataConnectors/Syslog/Forwarder_AMA_installer.py
```

```
cyberlab@linux-VM:~$ sudo wget -O Forwarder_AMA_installer.py https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/DataConnectors/Syslog/Forwarder_AMA_installer.py&sudo python3 Forwarder_AMA_installer.py
--2025-03-10 02:56:08-- https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/DataConnectors/Syslog/Forwarder_AMA_installer.py
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.110.133, 185.199.111.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13604 (13K) [text/plain]
Saving to: 'Forwarder_AMA_installer.py'

Forwarder_AMA_installer.py 100%[=====>] 13.29K --.-KB/s in 0s

2025-03-10 02:56:08 (48.4 MB/s) - 'Forwarder_AMA_installer.py' saved [13604/13604]


Located rsyslog daemon running on the machine
Rsyslog.conf configuration was changed to fit required protocol - /etc/rsyslog.conf
Restarting rsyslog daemon.
sudo service rsyslog restart
Rsyslog daemon restarted successfully
Please note that the installation script opens port 514 to listen to incoming messages in both UDP and TCP protocols. To change this setting, refer to the Rsyslog configuration file located at '/etc/rsyslog.conf'.

Warning: please make sure your Syslog daemon configuration does not store unnecessary logs. This may cause a full disk on your machine, which will disrupt the function of the owa agent installed. For more information:
https://www.rsyslog.com/doc/master/configuration/actions.html
Installation completed successfully
cyberlab@linux-VM:~$
```

4. Analytics Rule Configuration

4.1 Scheduled Query Rules for Brute Force Detection

Windows Endpoint: The KQL query triggers an alert if more than 10 failed login attempts occur within 10 minutes.

 **Test: Brute-Force attempt on Windows**

High Severity

Custom Content Source

Enabled Status

Info

Insights

ID

de4f1eb7-0366-4ef7-8aca-5957cfa7ec3a

Description

To see if someone is trying to brute force

MITRE ATT&CK

Initial Access

Rule query

```
SecurityEvent
| where EventID == 4625
| where TimeGenerated > ago(60m)
| summarize FailureCount = count() by AttackerIP = IpAddress
| where FailureCount >= 10
```

Rule frequency

Run query every 5 minutes

Rule period

Last 5 hours data

Linux Endpoint: The KQL query triggers an alert if more than 10 failed ssh login attempts occur within 10 minutes.

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

Analytics rule wizard - Edit existing Scheduled rule ...

Test: Brute-Force attempt on Linux

General Set rule logic Incident settings Automated response Review + 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.



```
Syslog
| where ProcessName == "sshd"
| where SyslogMessage contains "Failed password"
| extend User = extract(@"Failed password for (\w+) from", 1, SyslogMessage) // Extracts the username
| summarize FailedAttempts = count() by User, Computer, bin(TimeGenerated, 10m)
| where FailedAttempts >= 10
```

[View query results >](#)

4.2 Scheduled Query Rules for Malware activity Detection

Windows Endpoint: The Rule detects windows event IDs 1116 and 1117 which are triggered when Windows Defender detects malware, potentially unwanted programs and when Windows Defender successfully removes or quarantines a detected threat respectively.

 **Malware detection** >>

High Severity	 Custom Content Source	 Enabled Status
---------------	---	--

Info Insights

ID1ae624bc-abad-4e94-aa60-42f67745f9d8

DescriptionTo detect malware on a windows machine!

Rule query

```
Event
| where EventLog == "Microsoft-Windows-Windows Defender/Operational"
| where EventID == "1116" or EventID == "1117"
```

Rule frequencyRun query every 5 hours

Rule periodLast 5 hours data

Rule thresholdTrigger alert if query returns more than 0 results

Event grouping

Linux End point: It triggers an alert when malware detection events are logged.

Malware detection on Linux End points

General Set rule logic Incident settings Automated response Review + 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.

```
Syslog
| where SyslogMessage contains "malware detected"
| summarize MalwareAlerts = count() by Computer, bin(TimeGenerated, 10m)
```

[View query results >](#)

5. Results

5.1 Simulated Brute Force Attack

Linux Machine

Logs were generated by trying multiple failed login attempts on Linux machines, which can be seen in /var/log/auth.log.

```
cyberlab@Linux-VM:~$ tail -f /var/log/auth.log
Mar 13 07:56:57 Linux-VM sshd[2092330]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=20.211.84.55 user=cyberlab
Mar 13 07:56:59 Linux-VM sshd[2092330]: Failed password for cyberlab from 20.211.84.55 port 56298 ssh2
Mar 13 07:57:06 Linux-VM sshd[2092330]: message repeated 2 times: [ Failed password for cyberlab from 20.211.84.55 port 56298 ssh2]
Mar 13 07:57:08 Linux-VM sshd[2092330]: Connection closed by authenticating user cyberlab 20.211.84.55 port 56298 [preauth]
Mar 13 07:57:08 Linux-VM sshd[2092330]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=20.211.84.55 user=cyberlab
Mar 13 07:57:36 Linux-VM sshd[2092390]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=20.211.84.55 user=cyberlab
Mar 13 07:57:39 Linux-VM sshd[2092390]: Failed password for cyberlab from 20.211.84.55 port 34156 ssh2
Mar 13 07:58:09 Linux-VM sshd[2092390]: message repeated 2 times: [ Failed password for cyberlab from 20.211.84.55 port 34156 ssh2]
Mar 13 07:58:10 Linux-VM sshd[2092390]: Connection closed by authenticating user cyberlab 20.211.84.55 port 34156 [preauth]
Mar 13 07:58:10 Linux-VM sshd[2092390]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=20.211.84.55 user=cyberlab
```

Windows machine

Failed logon events logged in the event viewer.

Security Number of events: 29,917 (1) New events available				
Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	3/13/2025 10:28:04 AM	Microsoft Windows securi...	4625	Logon
Audit Success	3/13/2025 10:27:46 AM	Microsoft Windows securi...	4688	Process Creation
Audit Success	3/13/2025 10:27:46 AM	Microsoft Windows securi...	4688	Process Creation
Audit Failure	3/13/2025 10:27:41 AM	Microsoft Windows securi...	4625	Logon
Audit Failure	3/13/2025 10:27:35 AM	Microsoft Windows securi...	4625	Logon
Audit Failure	3/13/2025 10:27:03 AM	Microsoft Windows securi...	4625	Logon

5.2 Simulated Malware Activity

Linux Machine

The malware simulation tool EICAR test file was used to generate malware detection logs on Windows and Linux endpoints. The screenshot below shows the results of file scanning by Clamscan.

```
cyberlab@Linux-VM:~$ wget -O eicar.com.txt https://secure.eicar.org/eicar.com.txt
--2025-03-13 08:28:56-- https://secure.eicar.org/eicar.com.txt
Resolving secure.eicar.org (secure.eicar.org)... 89.238.73.97, 2a00:1828:1000:2497::2
Connecting to secure.eicar.org (secure.eicar.org)|89.238.73.97|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 68 [text/plain]
Saving to: 'eicar.com.txt'

eicar.com.txt                                100%[=====]

2025-03-13 08:28:57 (69.6 MB/s) - 'eicar.com.txt' saved [68/68]

cyberlab@Linux-VM:~$ ls
Forwarder_AMA_installer.py  eicar.txt          'index.html?wpdmdl=8842'
eicar.com.txt              'index.html?LinkId=828603'  omsagent-1.19.0-0.universal.x64.sh
cyberlab@Linux-VM:~$ clamscan eicar.com.txt
/home/cyberlab/eicar.com.txt: Win.Test.EICAR_HDB-1 FOUND

----- SCAN SUMMARY -----
Known viruses: 8704696
Engine version: 0.103.12
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 26.258 sec (0 m 26 s)
Start Date: 2025:03:13 08:29:11
End Date: 2025:03:13 08:29:37
cyberlab@Linux-VM:~$ cat eicar.comsudo nano /etc/clamav/clamd.conf
```

Windows Machine

The below screenshot shows the event IDs 1116 and 1117 generated by Microsoft Defender on Windows machines.

Icon	Level	Date and Time	Source	Event ID	Category
Warning	Warning	3/10/2025 5:05:18 AM	Windows Defender	1116	None
Warning	Warning	2/28/2025 1:40:46 PM	Windows Defender	1116	None
Warning	Warning	2/28/2025 1:42:12 PM	Windows Defender	1116	None
Information	Information	2/28/2025 1:40:51 PM	Windows Defender	1117	None
Information	Information	3/10/2025 5:05:23 AM	Windows Defender	1117	None
Information	Information	2/28/2025 1:42:17 PM	Windows Defender	1117	None
Information	Information	2/27/2025 7:55:26 AM	Windows Defender	1150	None
Information	Information	3/4/2025 2:55:33 AM	Windows Defender	1150	None

Event 1116, Windows Defender

General

Details

Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
For more information please see the following:
<https://go.microsoft.com/fwlink/?linkid=37020&name=Virus:DOS/EICAR&threatid=2147760934&enterprise=0>

Log Name:

Microsoft-Windows-Windows Defender/Operational

Source:

Windows Defender

Logged:

3/10/2025 5:05:18 AM

Event ID:

1116

Task Category:

None

Level:

Warning

Keywords:

Icon:

CVSTFM

Computer:

Windows-VM

5.3 Incidents logged by Sentinel

Incident management interface showing a list of incidents and details for incident number 8.

Open incidents by severity: High (8), Medium (0), Low (0), Informational (0)

Incident details for Incident number 8:

- Owner:** Unassigned
- Status:** New
- Severity:** High
- Description:** To detect malware on a windows machine!
- Alert product names:** Microsoft Sentinel
- Evidence:** 4 Events, 1 Alerts, 0 Bookmarks

Severity	Incident number	Title	Alerts	Incident
High	7	Test: Brute-Force att...	19	Azure
High	8	Malware detection	1	Azure
High	6	Test: Brute-Force att...	19	Azure
High	5	Test: Brute-Force att...	7	Azure
High	4	Test: Brute-Force att...	5	Azure

Brute force and Malware Incidents logged in Sentinel.

Cybersec-lab-analytics | Logs

Log Analytics workspace

log m

New Query 1* ... x +

Syslog Time range: Last 24 hours

Show: 1000 results Add

Facility	HostName	SeverityLevel	SyslogMessage
auth	Linux-VM	info	Invalid user flink from 68.183.102.75 port 35538
auth	Linux-VM	info	Invalid user uftp from 68.183.102.75 port 35530
auth	Linux-VM	info	Connection closed by invalid user default 68.183.102.75 p
auth	Linux-VM	info	Connection closed by invalid user tomcat 68.183.102.75 p
auth	Linux-VM	info	Invalid user oracle from 68.183.102.75 port 35514
auth	Linux-VM	info	Failed password for invalid user www from 68.183.102.75
auth	Linux-VM	info	Connection closed by invalid user gitlab 68.183.102.75 pc
auth	Linux-VM	info	Connection closed by authenticating user root 68.183.102
auth	Linux-VM	info	Failed password for invalid user admin from 68.183.102.7
auth	Linux-VM	info	Failed password for root from 68.183.102.75 port 35458 s
auth	Linux-VM	info	Invalid user es from 68.183.102.75 port 35502

Failed login attempts in Linux forwarded from Syslog

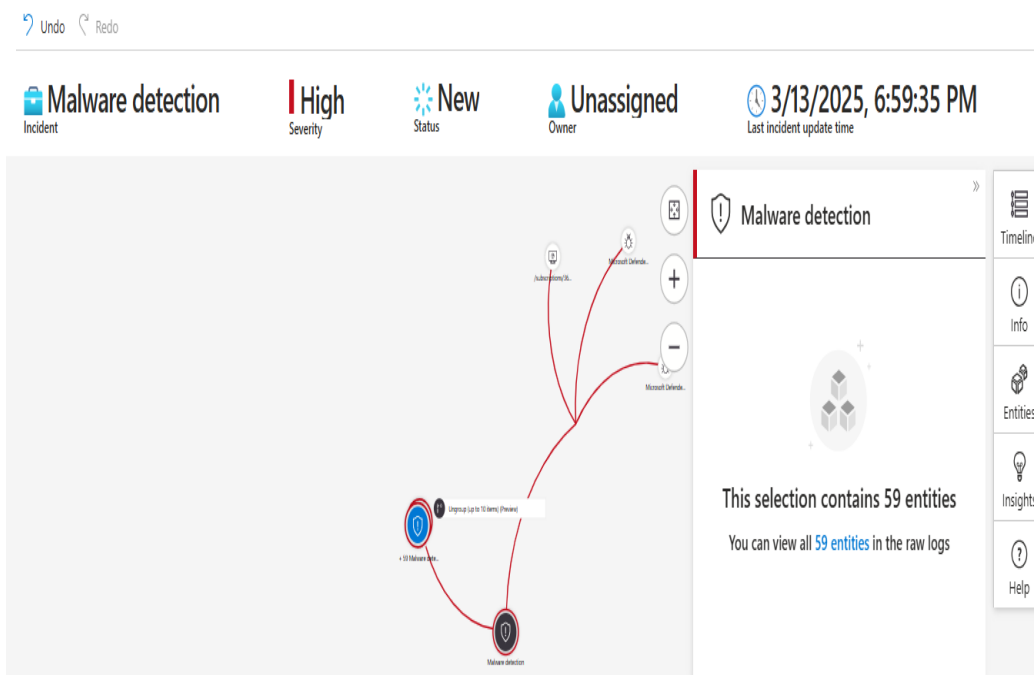
Cybersec-lab-analytics

User Query Time range: Custom Show: 30000 results Add

Simple mode

TimeGenerated [UTC]	Source	EventLog	Computer	EventLevel	EventLevelNam
> 3/13/2025, 3:57:11.672 AM	Microsoft-Windows-Windows Defender	Microsoft-Windows-Windows Defender/Operational	Windows-VM	4	Information
> 3/13/2025, 3:57:06.798 AM	Microsoft-Windows-Windows Defender	Microsoft-Windows-Windows Defender/Operational	Windows-VM	3	Warning

Malware activity events 1116 and 1117 forwarded from Defender on Windows VM



Infographic diagram depicting malware detection

5.4 Malicious Activities Identified During Monitoring

Detection of Suspicious IP Addresses

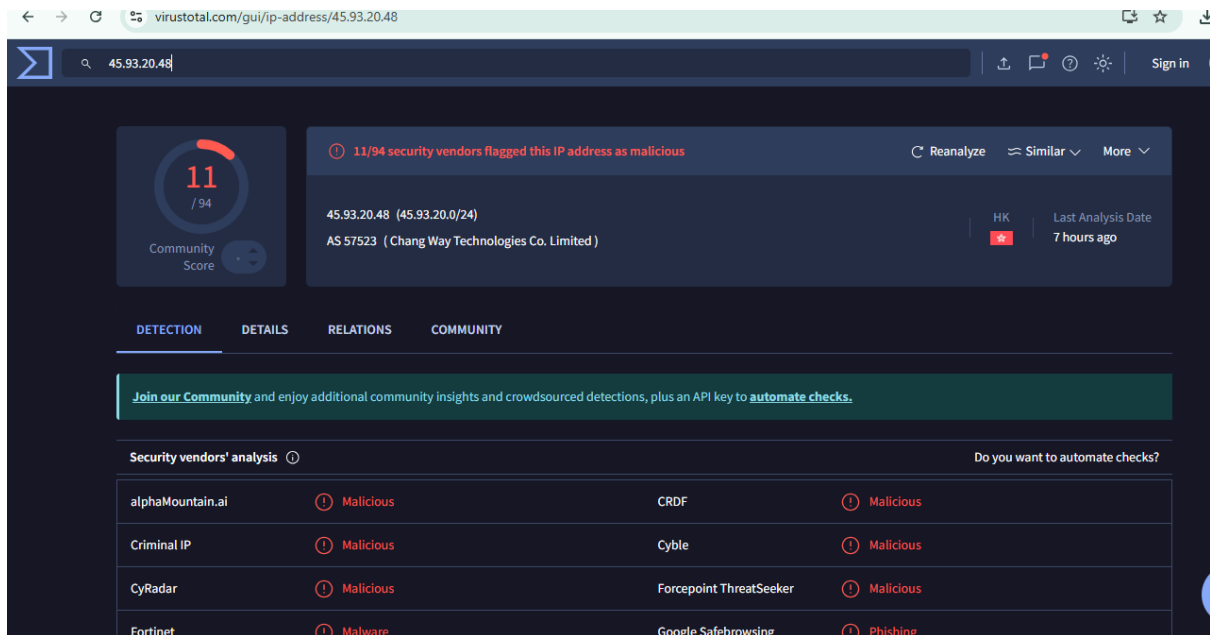
- During the monitoring phase, multiple source IP addresses involved in brute-force attempts were logged and analysed using VirusTotal. The analysis confirmed that these IPs were associated with known malicious actors.

Verification Process

- Further cross-referencing revealed links between these IP addresses, botnet activities, and large-scale brute-force campaigns.

Mitigation Actions

- To contain the threat, the identified IPs were promptly blocked at the firewall level. Additionally, alerts were escalated to the Security Operations Center (SOC) team for in-depth investigation and further response.



6. Key Insights

- Azure Sentinel's built-in analytics effectively detect brute force attacks and malware across multiple platforms.
- Integrating data ingestion from various endpoints enhances security visibility and threat detection.
- Automating response actions boosts operational efficiency and strengthens incident response.

7. Conclusion

The implementation of Azure Sentinel demonstrated its effectiveness in detecting and responding to cybersecurity threats, particularly brute force attacks and malware activities. By collecting and analysing endpoint logs, applying analytics rules, and identifying security threats, Azure Sentinel proved to be a valuable tool for proactive threat detection and mitigation. These findings highlight its real-world applicability in enhancing security operations, reinforcing its role as a critical component in modern cybersecurity defence strategies.

8. Next Steps

- Expand data integration to include more endpoints for better visibility.
- Refine analytics rules to improve detection accuracy and reduce false positives.
- Automate response actions using playbooks to enhance operational efficiency.
- Continuously monitor and tune detection and response mechanisms.
- Conduct penetration testing to evaluate security effectiveness.

- Improve reporting and dashboards for better insights.

9. References

- Microsoft Azure Sentinel Documentation: <https://learn.microsoft.com/en-us/azure/sentinel/>
- CloudSkew for Architecture diagrams: <https://www.cloudskew.com/>