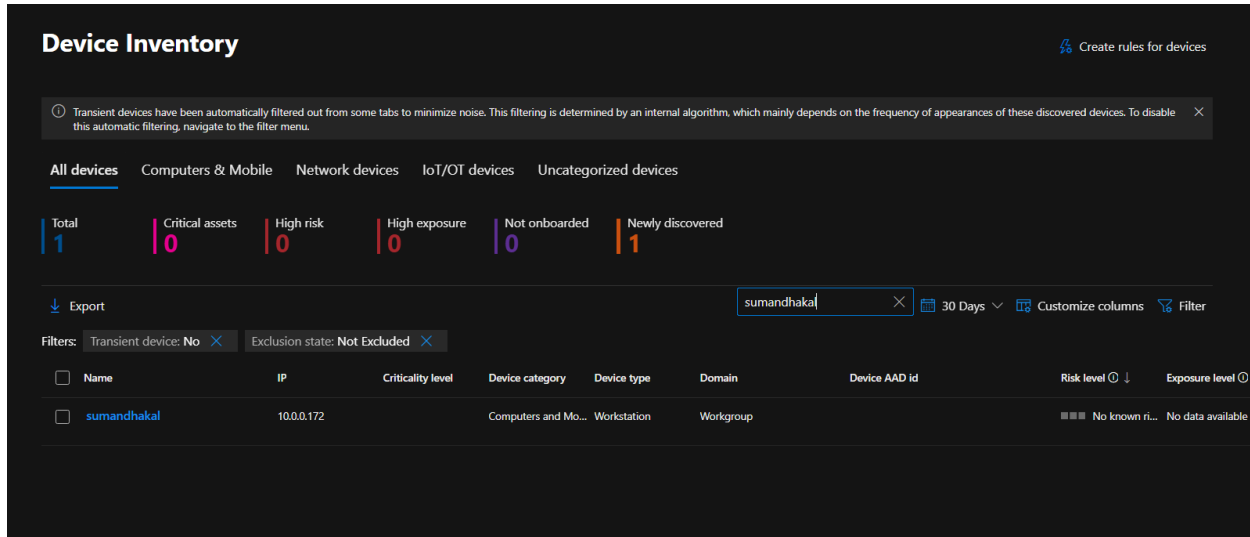


## Scenario 1: Virtual Machine Brute Force Detection

For this Lab I have created a Virtual Machine using Microsoft Azure. This Virtual Machine has been Onboarded to Microsoft Defender for Endpoint (MDE).



Virtual Machine Device Name as shown in screenshot: sumandhakal

IP Address: 10.0.0.172

Explanation:

When entities (local or remote users, usually) attempt to log into a virtual machine, a log will be created on the local machine and then forwarded to Microsoft Defender for Endpoint under the DeviceLogonEvents table. These logs are then forwarded to the Log Analytics Workspace being used by Microsoft Sentinel, our SIEM. Within Sentinel, we will define an alert to trigger when the same entity fails to log into the same VM a given number of times within a certain time period. (i.e. 10 failed logons or more per 5 hours).

### Part 1: Create Alert Rule (Brute Force Attempt Detection)

Design a Sentinel Scheduled Query Rule within Log Analytics that will discover when the same remote IP address has failed to log in to the same local host (Azure VM) 10 times or more within the last 5 hours.

Using the DeviceLogonEvents table, this query has been created:

```
DeviceLogonEvents
| where TimeGenerated >= ago(5h)
| where ActionType has "LogonFailed"
```

```
| summarize NumberOfFailures = count() by RemoteIP, ActionType, DeviceName
| where NumberOfFailures >= 50
```

New Query 1\* ... +

Run Time range: Set in query Show: 1000 results

```
1 DeviceLogonEvents
2 | where TimeGenerated > ago(5h)
3 | where ActionType has "LogonFailed"
4 | summarize NumberOfFailure = count() by RemoteIP, ActionType, DeviceName
5 | where NumberOfFailure >= 50
```

Results Chart

RemoteIP	ActionType	DeviceName	NumberOfFailure
> 63.250.59.176	LogonFailed	leon-test-mde	56
> 186.10.23.226	LogonFailed	josh-vm-student	100

And this query has been created:

```
DeviceLogonEvents
| where ActionType == "LogonFailed" and Timestamp > ago(5h)
| summarize EventCount = count() by RemoteIP, DeviceName
| where EventCount >= 50
| order by EventCount desc
```

Log Analytics workspace

New Query 1\* ... +

Run Time range: Set in query Show: 1000 results

```
6
7 DeviceLogonEvents
8 | where ActionType == "LogonFailed" and Timestamp > ago(5h)
9 | summarize EventCount = count() by RemoteIP, DeviceName
10 | where EventCount >= 50
11 | order by EventCount desc
12
```

Results Chart

RemoteIP	DeviceName	EventCount
> 186.10.23.226	josh-vm-student	100
> 63.250.59.176	leon-test-mde	56

Now I created the Schedule Query Rule in: Sentinel → Analytics → Schedule Query Rule.

Analytics Rule Settings:

- Enable the Rule
- Set Mitre ATT&CK Framework Categories based on the query
- Run query every 4 hours
- Lookup data for last 5 hours (can define in query) •
- Stop running query after alert is generated == Yes
- Configure Entity Mappings for the Remote IP and DeviceName
- Automatically create an Incident if the rule is triggered • Group all alerts into a single Incident per 24 hours
- Stop running query after alert is generated (24 hours)

This is the Rule script:

DeviceLogonEvents

```
| where TimeGenerated >= ago(5h)
| where ActionType has "LogonFailed"
| summarize NumberOfFailures = count() by RemoteIP, ActionType, DeviceName
| where NumberOfFailures >= 30
```

Relevant MITRE ATT&CK Techniques:

T1110 – Brute Force

Sub-technique: T1110.001 – Password Guessing

Repeated failed login attempts from the same remote IP address fit this exactly. (Optional, depending on interpretation)

T1078 – Valid Accounts

If successful logins are later seen from the same IP after failures, it may indicate stolen/guessed credentials.

How it would be written in the rule:

MITRE ATT&CK Mapping:

T1110 – Brute Force (T1110.001 – Password Guessing)

Possible related: T1078 – Valid Accounts

---

## **Part 2: Trigger Alert to Create Incident**

Generated Alert:

**Microsoft Sentinel | Incidents**

Selected workspace: law-cyber-range

Search

Create incident (Preview) Refresh Last 24 hours Actions Delete Security efficiency workbook Columns Guides & Feedback

General

Threat management

**Incidents**

Workbooks

Hunting

Notebooks

Entity behavior

Threat intelligence

MITRE ATT&CK (Preview)

SOC optimization

Content management

Content hub

Repositories

Community

Configuration

594 Open Incidents 593 New Incidents 1 Active Incidents

Open incidents by severity

High (58) Medium (456) Low (25) Informational (55)

Search by ID, title, tags, owner or product

Severity: All Status: 2 selected More (3)

Auto-refresh incidents

Severity	Incident number	Title	Alerts	Incident provider name
Informational	227999	Test - Unusual Sign-in (Off H...	1	Azure Sentinel
Medium	227998	sumandhakal- Brute force att...	1	Azure Sentinel
Low	227997	Detect Azure VM Guest Agen...	1	Azure Sentinel
Medium	227983	AnalyticsRule_JB_ImpossibleT...	2	Azure Sentinel
High	227996	SL_Suspicious Execution of O...	1	Azure Sentinel
Informational	227995	Test - Unusual Sign-in (Off H...	1	Azure Sentinel
Medium	227994	Ossie-Create Alert Rule (Pote...	1	Azure Sentinel

< Previous 1 - 50 Next >

sumandhakal- Brute force attack detection

Incident number 227998

Unassigned New Medium

Alert product names

- Microsoft Sentinel

Evidence

6 Events 1 Alerts 0 Bookmarks

Last update time: 11/12/25, 14:15 Creation time: 11/12/25, 14:15

Entities (10)

- leon-test-mde
- irene-test-vm...
- matt-mde-vm

View full details Actions

sumandhakal- Brute force attack detection

Incident number 227998

Refresh Delete incident Logs Tasks Activity log

This is the new, improved incident page - Now generally available. You can use the toggle to switch back. New experience

Medium Severity New Status Unassigned Owner

Workspace name: law-cyber-range

Description: --

Alert product names: Microsoft Sentinel

Evidence: 6 Events 1 Alerts 0 Bookmarks

Last update time: 12/11/2025, 2:15:26 PM Creation time: 12/11/2025, 2:15:26 PM

Entities (10): 92.63.197.9, 186.10.23.226

Investigate

Overview Entities

Incident timeline

11 Dec 09:10:18 sumandhakal- Brute...

Entities

- 92.63.197.9 IP
- 186.10.23.226 IP
- 185.156.73.173 IP

Similar incidents

Severity	Incident number	Title	Last update time
Medium	227990	SL_Brute Force External Network ...	11/12/2025, 13:48

Top insights

Last 24 hours before the first alert

IP address remote connections

12/10/2025, 2:15:20 PM - 12/11/2025, 2:15:20 P...

92.63.197.9

Direction	IPAddress	Remote I
Top In	92.63.197.9	10.1.0.15
All	92.63.197.9	3 IPs

See All connections >

IP address remote connections

12/10/2025, 2:15:20 PM - 12/11/2025, 2:15:20 P...

These alerts were generated immediately after creating and launching this detection rule. 6 total events at this time

### **Part 3: Work Incident**

Now this incident is worked to completion and will be closed out, in accordance with the NIST 800-61: Incident Response Lifecycle.

Detection and Analysis Steps:

Identify and validate the incident.

Observe the incident and assign it to yourself, set the status to Active

sumandhakal- Brute force attack detection

Incident number 227998

Refresh

Delete incident

Logs

Tasks

Activity log

This is the new, improved incident page - Now generally available. You can use the toggle to switch back.

New experience

Medium

Severity

Active

Status

6a9089dbd31c710096231c910a3d3fd76696d40c1c3da6987912487b5e7e082e

Owner

Analytics rule

sumandhakal- Brute force attack detection

Incident Team

Tags

+

Incident link

https://portal.azure.com/#asset/Microsoft\_Azure\_Security\_Insig...

Last comment

(Total: 0)

Write a comment...

Investigate

Overview

Entities

Incident timeline

11 Dec 09:10:18 sumandhakal- Brute...

Entities

92.63.197.9 IP

186.10.23.226 IP

185.156.73.173 IP

Similar incidents

Severity Incident number Title Last update time

Medium 227990 SL\_Brute Force External Network ... 11/12/2025, 13:48

Top insights

Last 24 hours before the first alert

IP address remote connections

Direction IPAddress Remote I

Top In 92.63.197.9 10.1.0.15

All 92.63.197.9 3 IPs

IP address remote connections

Investigate the Incident by Actions → Investigate Gather relevant evidence and assess impact.

Observations of the different entity mappings and notes:

sumandhakal- Brute force attack detection

Incident

Medium

Severity

Active

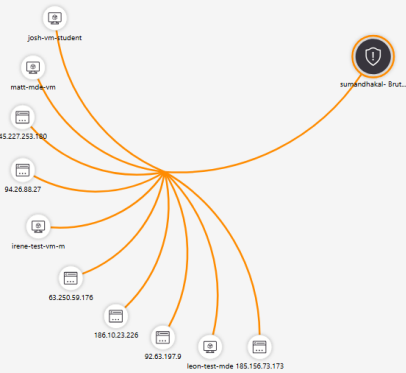
Status

6a9089dbd31c710096231c910a3d3fd76696d40c1c3da6987912487b5e7e082e

Owner

12/11/2025, 2:24:38 PM

Last incident update time



LAW-Cyber-Range | Logs

Log Analytics workspace

Search

New Query 1\*

Time range : Set in query

Show : 1000 results

KQL mode

1 DeviceLogonEvents

2 > | where TimeGenerated >= ago(5h) ...

3 | where ActionType has "LogonFailed"

4 | summarize NumberOffailures = count() by RemoteIP, ActionType, DeviceName

5 | where NumberOffailures >= 30

6

7

8

9

10

Results

Chart

RemoteIP	ActionType	DeviceName	NumberOffailures
> 63.250.59.176	LogonFailed	leon-test-mde	48
> 45.227.253.180	LogonFailed	irene-test-vm-m	40
> 186.10.23.226	LogonFailed	josh-vm-student	100
> 185.156.73.173	LogonFailed	matt-mde-vm	30
> 92.63.197.9	LogonFailed	matt-mde-vm	35
> 45.136.68.88	LogonFailed	windows-target-1	79

This evidence shows the 6 remote IP addresses that are attempting to Brute Force their way into the Virtual Machine that run alongside this one on the Cyber Range System



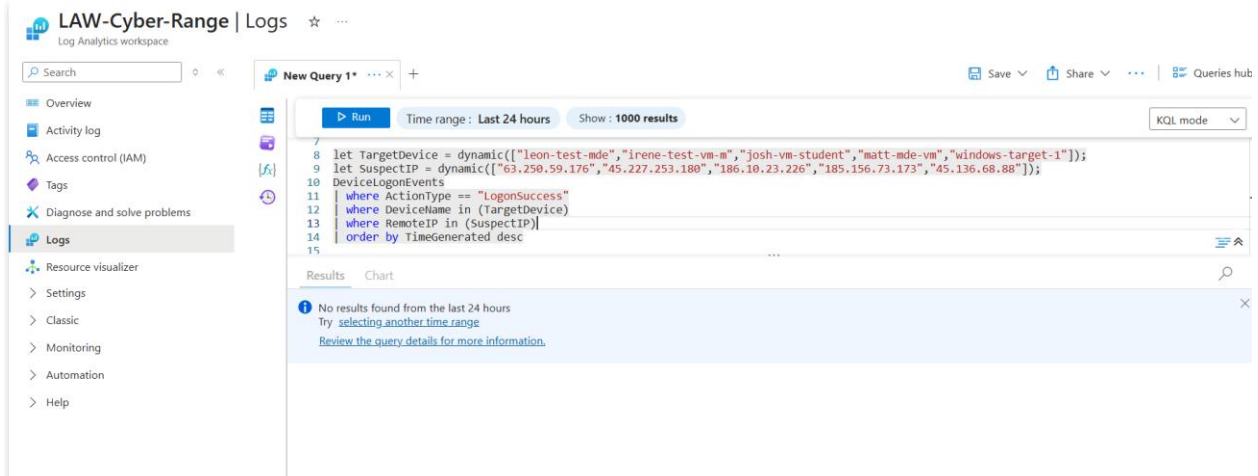
## Containment, Eradication, and Recovery Steps:

- **Checked to make sure none of the IP addresses attempting to brute force the machine actually logged in.**

Ran this script to verify that there were no "LogonSuccess" in the ActionType from this suspicious IP Address: 5.188.118.202

```
let TargetDevice = dynamic(["leon-test-mde","irene-test-vm-m","josh-vm-student","matt-mde-vm","windows-target-1"]);
let SuspectIP =
dynamic(["63.250.59.176","45.227.253.180","186.10.23.226","185.156.73.173","45.136.68.88"]);
DeviceLogonEvents
| where ActionType == "LogonSuccess"
| where DeviceName in (TargetDevice)
| where RemoteIP in (SuspectIP)
| order by TimeGenerated desc
```

This was the return:



No results found from the last 24 hours  
Try selecting another time range

There were no "LogonSuccess" in the ActionType from these suspicious IP Addresses,

---

**Isolated affected systems/Virtual Machines to prevent further damage.**

**This can be done with Defender for Endpoint.  
Conducted Anti-Virus and Anti-Malware scans.**

---

For future prevention, there will be created or updated Network Security Group (NSG) rules attached to your Virtual Machine to prevent any traffic except your local PC from reaching the VM.

NSG was locked down to prevent RDP attempts from the public internet.  
Corporate policy was proposed to require this for all VMs going forward. (this can be done with Azure Policy)

Brute Force was not successful, so no threats related to this incident.

## Summary:

This detection rule monitors the DeviceLogonEvents table in Microsoft Sentinel for brute force activity against Azure VMs. It triggers when the same remote IP fails to log in 30 or more times within a 5-hour window. In this scenario, the rule identified multiple external IPs attempting repeated logons against the VM in the Cyber Range System. No successful logons were observed from the suspicious IPs. Containment and recovery steps included verifying no credential compromise, isolating the VM, and applying stricter NSG rules to block RDP from the internet.

## MITRE ATT&CK Mapping:

T1110 – Brute Force (T1110.001 – Password Guessing)

Possible related: T1078 – Valid Accounts (if success occurs after failures)

Closed out the Status.

The screenshot shows the Microsoft Sentinel incident page for an incident titled "sumandhakal- Brute force attack detection" with incident number 227998. The status is "Closed" and the severity is "Medium". The page is divided into several sections: "Overview", "Entities", "Incident timeline", "Entities", "Top insights", and "Similar incidents".

**Incident timeline:** Shows a single event on 11 Dec 09:10:18 with the title "sumandhakal- Brute...".

**Entities:** Lists three entities: "185.156.73.173 IP", "92.63.197.9 IP", and "irene-test-vm-m".

**Top insights:** Shows "IP address remote connections" for the last 24 hours before the first alert. It lists connections from "185.156.73.173" to "10.1.0.15" and "185.156.73.173" to "3 IPs".

**Similar incidents:** Shows a table of similar incidents:

Severity	Incident number	Title	Last update time
Medium	228021	mm-failed-login-rule	11/12/2025, 14:58

This has been classified as a "True Positi