

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).

The screenshot shows the Microsoft Defender for Endpoint Device Inventory interface. At the top, there's a header bar with a 'Create rules for devices' button. Below it is a summary bar with counts for Total (1), Critical assets (0), High risk (0), High exposure (0), Not onboarded (0), and Newly discovered (1). A search bar contains the name 'sumandhaka'. The main table lists one device: 'sumandhaka' with IP 10.0.0.172, categorized as a 'Computers and Mo...' Workstation in a 'Workgroup' domain. The 'Risk level' is shown as 'No known ri...' and 'Exposure level' as 'No data available'.

Virtual Machine Device Name as shown in screenshot: sumandhaka

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
```

The screenshot shows a Log Analytics workspace interface. At the top, there's a navigation bar with icons for Home, Dashboards, Metrics, Logs, Metrics + Logs, and Metrics + Insights. Below the navigation is a search bar with placeholder text "Search logs and metrics". Underneath the search bar is a "New Query" button followed by a dropdown menu and a plus sign for creating new queries.

The main area displays a query editor with the following code:

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

Below the code, there are two tabs: "Results" (which is selected) and "Chart". The "Results" tab shows a table with the following data:

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

The screenshot shows a Log Analytics workspace interface, similar to the first one. It features a navigation bar, a search bar, and a "New Query" button.

The main area displays a query editor with the following code:

```
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
```

Below the code, there are two tabs: "Results" (selected) and "Chart". The "Results" tab shows a table with the following data:

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'

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

> General
v 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 na...
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

Add or remove favorites by pressing Ctrl + Shift + F

Home > Microsoft Sentinel | Incidents >

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.

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
185.156.73.173

Investigate

Overview Entities

Incident timeline

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

Entities

Search Type: All

- 92.63.197.9 IP
- 186.10.23.226 IP
- 185.156.73.173 IP

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 IP
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...
92.63.197.9

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.

Medium Severity Active Status Owner 6a9089dbd31c710096231c910a3d3fd76696d40c1c3da6987912487b5e7e082e

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

Entities

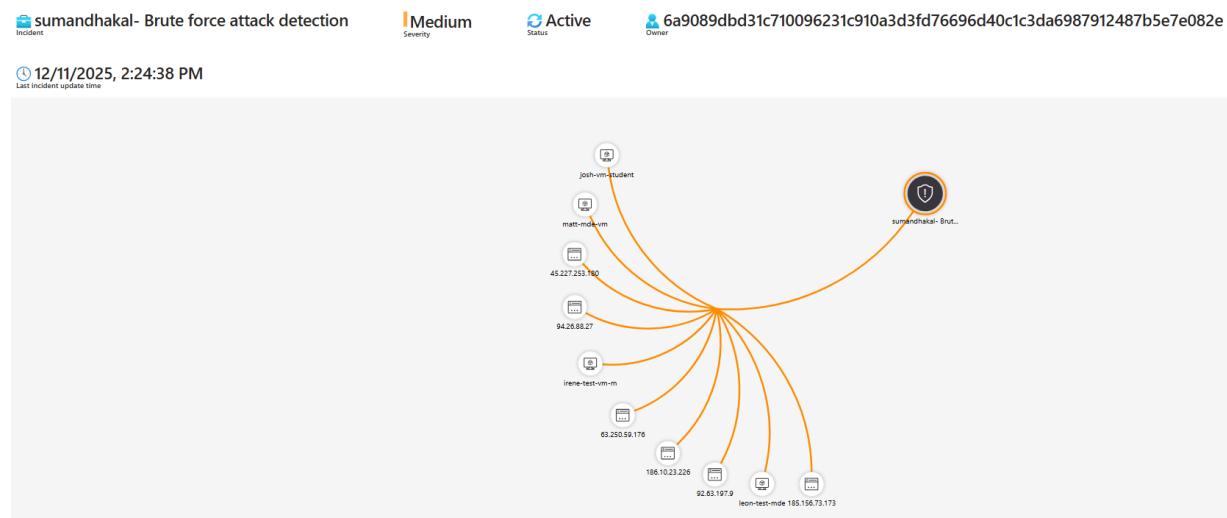
Top insights

IP address remote connections

IP address remote connections

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

Observations of the different entity mappings and notes:



LAW-Cyber-Range | Logs

Log Analytics workspace

New Query 1*

```
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
```

Save Share Qu KQL mode

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

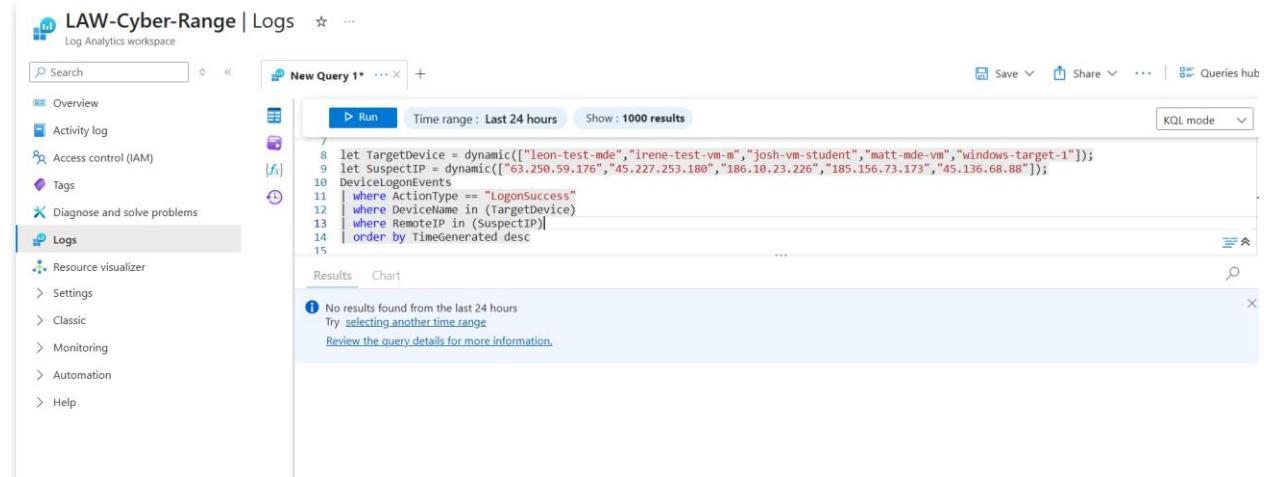
Containment, Eradication, and Recovery Steps:

- 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:



The screenshot shows the Microsoft Log Analytics workspace interface. On the left, there's a navigation sidebar with various logs and monitoring options. The main area displays a KQL query in the 'New Query' editor. The query is as follows:

```
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
```

The results pane below shows a message: "No results found from the last 24 hours. Try selecting another time range. Review the query details for more information." This indicates that the query did not find any logon successes for the specified IP addresses over the last 24 hours.

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:

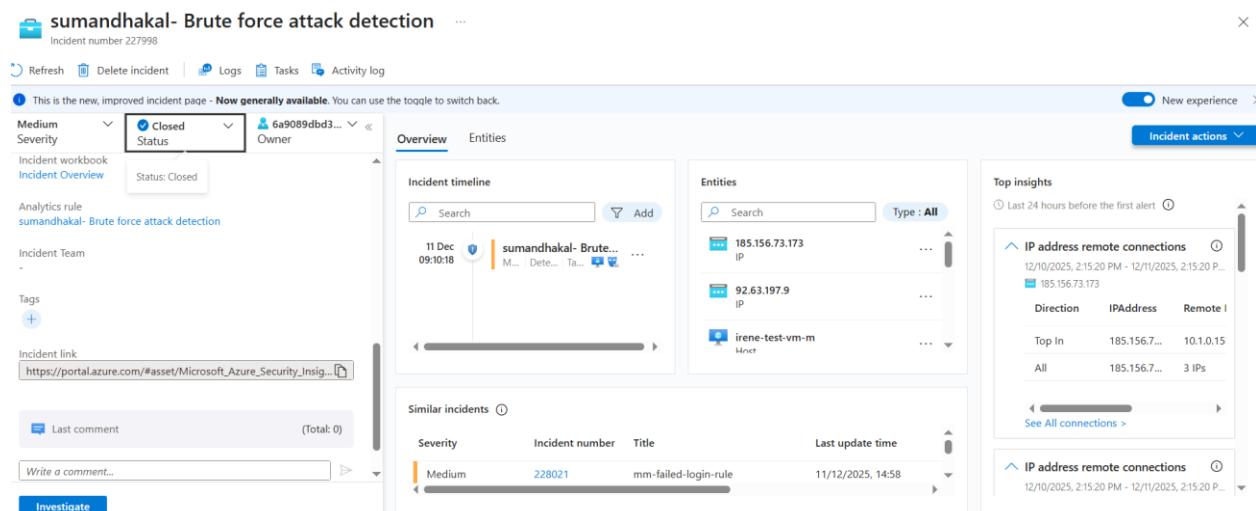
This detection rule monitors the DeviceLogonEvents table in Microsoft Sentinel for brute force activity against Azure VMs. It triggers when the same remote IP fails to log in 30 or more times within a 5-hour window. In this scenario, the rule identified multiple external IPs attempting repeated logons 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". The status is set to "Closed". The page includes sections for Overview, Entities, and Top insights. The Overview section shows the incident timeline with a single event on 11 Dec 09:10:18. The Entities section lists three entities: 185.156.73.173, 92.63.197.9, and irene-test-vm-m. The Top insights section shows two entries under "IP address remote connections": one for 185.156.73.173 with "Top In" and "All" directions, and another for 185.156.73.173 with "3 IPs".

This has been classified as a “True Positive”