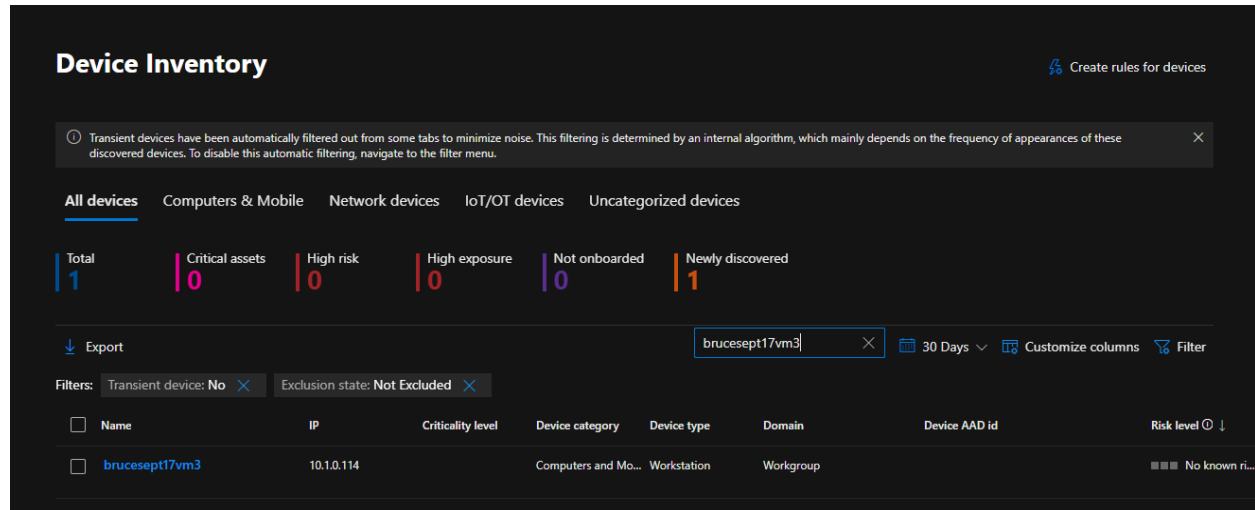


Scenario 1: Virtual Machine Brute Force Detection 9/17/2025

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: brucesept17vm3

IP Address: 10.1.0.114

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 KQL query editor interface. The query is as follows:

```
3 | summarize EventCount = count() by RemoteIP, DeviceName  
4 | where EventCount >= 10  
5 | order by EventCount  
6  
7 DeviceLogonEvents  
8 | where TimeGenerated >= ago(5h)  
9 | where ActionType has "LogonFailed"  
10 | summarize NumberOfFailures = count() by RemoteIP, ActionType, DeviceName  
11 | where NumberOfFailures >= 50
```

The results are displayed in a table with the following columns: RemoteIP, ActionType, DeviceName, and NumberOfFailures. The table contains 5 rows of data.

RemoteIP	ActionType	DeviceName	NumberOfFailures
> 115.140.161.61	LogonFailed	linux-target-1.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net	61
> 175.193.11.32	LogonFailed	lnx.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net	100
> 45.140.17.102	LogonFailed	gd-win-11-vm-md	80
> 20.80.241.91	LogonFailed	lnx.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net	101
> 103.110.181.18	LogonFailed	blless-win10	113

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
```

New Query 1* ... x +

Save

Share

...

Queries hub

Run

Time range: Set in query

Show: 1000 results

KQL mode

```

9 | where ActionType has "LogonFailed"
10 | summarize NumberOfFailures = count() by RemoteIP, ActionType, DeviceName
11 | where NumberOfFailures >= 50
12
13 DeviceLogonEvents
14 | where ActionType == "LogonFailed" and Timestamp > ago(5h)
15 | summarize EventCount = count() by RemoteIP, DeviceName
16 | where EventCount >= 50
17 | order by EventCount desc
18

```

Results Chart

RemoteIP	DeviceName	EventCount
> 103.110.181.18	blless-win10	113
> 20.80.241.91	lnx.p2zfvso05mlezjev3ck4vqd3...	101
> 175.193.11.32	lnx.p2zfvso05mlezjev3ck4vqd3...	100
> 45.140.17.102	gd-win-11-vm-md	77
> 115.140.161.61	linux-target-1.p2zfvso05mlezje...	61

1s 153ms

Display time (UTC+00:00)

Query details

1 - 5 of 5

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
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules

558 Open incidents 557 New incidents 1 Active incidents

Open incidents by severity
High (92) Medium (424) Low (0) Informational (42)

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...	Alert product na...
Medium	181466	SL_Brute Force Ext...	1	Azure Sentinel	Microsoft Sentir
Medium	181465	Powershellencoded	1	Azure Sentinel	Microsoft Sentir
Informational	181464	Test - Unusual Sign...	1	Azure Sentinel	Microsoft Sentir
Medium	181463	Rogue - Potential I...	1	Azure Sentinel	Microsoft Sentir
Medium	181462	Ossie- Create Alert ...	1	Azure Sentinel	Microsoft Sentir
Medium	181461	bruce Virtual Machi...	1	Azure Sentinel	Microsoft Sentir
Medium	181460	Powershellencoded	1	Azure Sentinel	Microsoft Sentir
High	181380	SL[UNIX] Suspiciou...	4	Azure Sentinel	Microsoft Sentir

Previous 1 - 50 Next

bruce Virtual Machine Brute Force Detection
Incident number 181461

Unassigned Owner New Status Medium Severity

Description
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

Alert product names
Microsoft Sentinel

Evidence
9 Events 1 Alerts 0 Bookmarks

Last update time 09/17/25, 08:45 PM Creation time 09/17/25, 08:45 PM

Entities (15)
View full details Actions

bruce Virtual Machine Brute Force Detection
Incident number 181461

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
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

Alert product names
Microsoft Sentinel

Evidence
9 Events 1 Alerts 0 Bookmarks

Last update time 9/17/2025, 8:45:16 PM Creation time 9/17/2025, 8:45:16 PM

Entities (15)
linux-target-1 20.80.241.91

Investigate

Overview Entities

Incident timeline
Sep 17 15:40:07 bruce Virtual Machine ...

Entities
linux-target-1 Host
20.80.241.91 IP
115.140.161.61 IP

Top insights
Last 24 hours before the first alert
Windows sign-in activity
9/16/2025, 8:45:08 PM - 9/17/2025, 8:45:08 PM
linux-target-1
Title Signin Co... User Count
Successful 0 0
Failed 0 0
Sign-ins over time

Similar incidents
Severity Incident number Title Last update time Status
Medium 181462 Ossie- Create Alert Rule (Brute F... 9/17/2025, 08:46 PM Ne

These alerts were generated immediately after creating and launching this detection rule. 9 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

Home > Microsoft Sentinel

Microsoft Sentinel | Incidents

Selected workspace: 'law-cyber-range'

Search

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

558 Open incidents 556 New incidents 2 Active incidents

Open incidents by severity: High (92) Medium (424) Low (0) Informational (42)

Search by ID, title, tags, owner or product

Severity: All Status: 2 selected

Auto-refresh incidents

Severity	Incident number	Title	Alerts	Incident provider na...	Alert product nam...
Medium	181466	SL_Brute Force Ext...	1	Azure Sentinel	Microsoft Sentir
Medium	181465	Powershellencod...	1	Azure Sentinel	Microsoft Sentir
Informational	181464	Test - Unusual Sign...	1	Azure Sentinel	Microsoft Sentir
Medium	181463	Rogue - Potential I...	1	Azure Sentinel	Microsoft Sentir
Medium	181462	Ossie- Create Alert ...	1	Azure Sentinel	Microsoft Sentir
Medium	181461	bruce Virtual Machi...	1	Azure Sentinel	Microsoft Sentir
Medium	181460	Powershellencod...	1	Azure Sentinel	Microsoft Sentir
High	181380	SL[LINUX] Suspiciou...	4	Azure Sentinel	Microsoft Sentir

bruce Virtual Machine Brute Force Detection

Incident number 181461

Owner: d9a7b5983... Status: Active Severity: Medium

Description: 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

Alert product names: Microsoft Sentinel

Evidence: 9 Events 1 Alerts 0 Bookmarks

Last update time: 09/17/25, 09:10 PM Creation time: 09/17/25, 08:45 PM

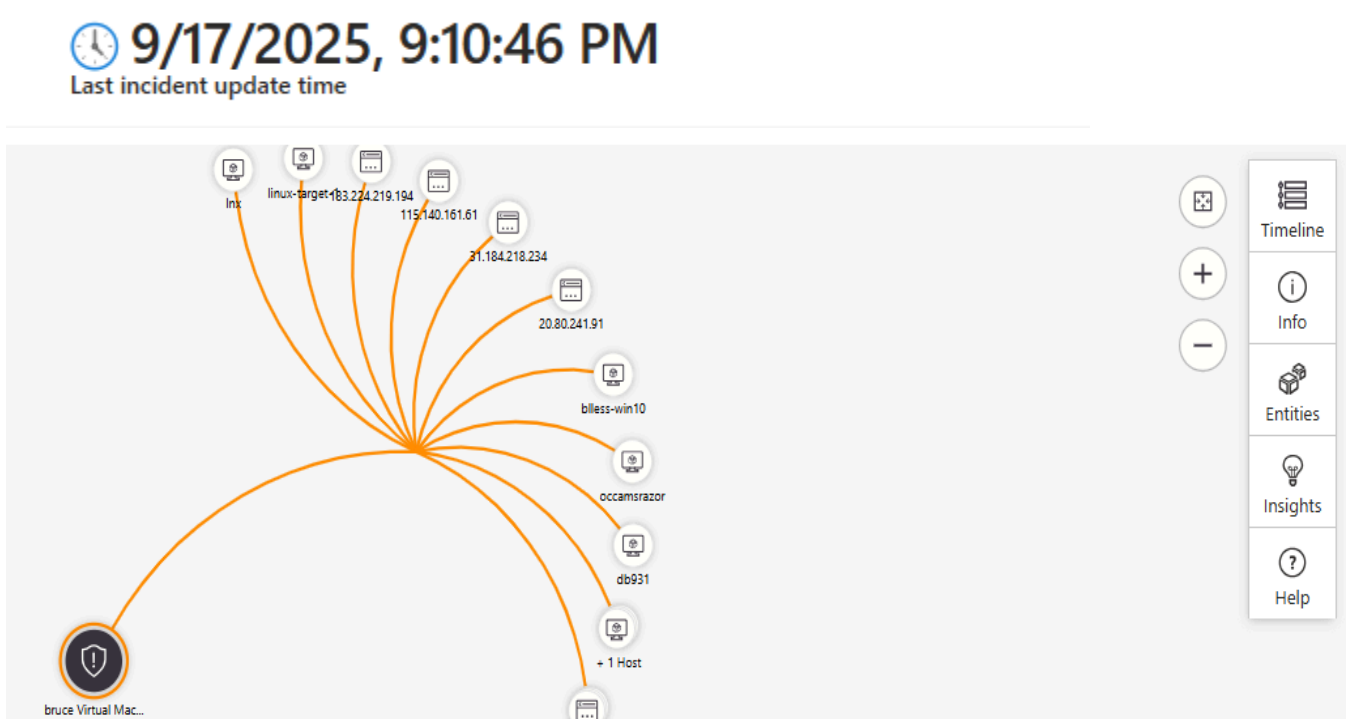
Entities (15)

View full details Actions

Investigate the Incident by Actions → Investigate

Gather relevant evidence and assess impact.

Observations of the different entity mappings and notes:



115.140.161.61

LogonFailed linux-target-1.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net61

103.110.181.18

LogonFailed blless-win10189

78.157.215.250

LogonFailed linux-target-1.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net99

178.16.53.22

LogonFailed db93172

5.188.118.202

LogonFailed blless-win1036

183.224.219.194

LogonFailed vm-lab-am.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net52

78.134.102.204

LogonFailed vm-lab-am.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net45

31.184.218.234

LogonFailed occamsrazor95

This evidence shows the 4 remote IP addresses that are attempting to Brute Force their way into the Virtual Machine that I have created "brucesept17vm3" along with the Virtual Machines that run alongside this one on the Cyber Range System.

These IP Addresses are:

occamsrazor95 [31.184.218.234]

blless-win1036 [5.188.118.202]

db93172 [178.16.53.22]

Blless-win10189 [103.110.181.18]

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 = "brucesept17vm3";  
let SuspectIP = "5.188.118.202";  
DeviceLogonEvents  
| where ActionType == "LogonSuccess"  
| where DeviceName == TargetDevice and RemoteIP == SuspectIP  
| order by TimeGenerated desc
```

This was the return:

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

LAW-Cyber-Range | Logs ☆ ...
Log Analytics workspace

Search

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Resource visualizer
Settings
Tables
Agents
Usage and estimated costs
Data export
Network isolation
Identity
Linked storage accounts
Properties

New Query 1* ... x +

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

```
16 | where EventCount >= 50
17 | order by EventCount desc
18
19 let TargetDevice = "brucesept17vm3";
20 let SuspectIP = "5.188.118.202";
21 DeviceLogonEvents
22 | where ActionType == "LogonSuccess"
23 | where DeviceName == TargetDevice and RemoteIP == SuspectIP
24 | order by TimeGenerated desc
25
```

Results Chart

No results found from the last 24 hours
Try [selecting another time range](#)

1s 39ms Query details

From this suspicious IP Address: 103.110.181.18

```
let TargetDevice = "brucesept17vm3";
let SuspectIP = "103.110.181.18";
DeviceLogonEvents
| where ActionType == "LogonSuccess"
| where DeviceName == TargetDevice and RemoteIP == SuspectIP
| order by TimeGenerated desc
```

This was the return:

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

The screenshot shows the LAW-Cyber-Range Log Analytics workspace. On the left is a navigation pane with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Logs (selected), Resource visualizer, Settings, Tables, Agents, Usage and estimated costs, Data export, Network isolation, Identity, Linked storage accounts, and Properties. The main area displays a 'New Query 1*' editor with a KQL query. The query is as follows:

```
16 | where EventCount >= 50
17 | order by EventCount desc
18
19 let TargetDevice = "brucesept17vm3";
20 let SuspectIP = "103.110.181.18";
21 DeviceLogonEvents
22 | where ActionType == "LogonSuccess"
23 | where DeviceName == TargetDevice and RemoteIP == SuspectIP
24 | order by TimeGenerated desc
25
```

The query is set to run for the 'Last 24 hours' and show '1000 results'. Below the query editor, the 'Results' tab is active, displaying a message: 'No results found from the last 24 hours. Try selecting another time range'. The status bar at the bottom indicates '6s 905ms' and a 'Query details' link.

From this suspicious IP Address: 178.16.53.22

```
let TargetDevice = "brucesept17vm3";
let SuspectIP = "178.16.53.22";
DeviceLogonEvents
| where ActionType == "LogonSuccess"
| where DeviceName == TargetDevice and RemoteIP == SuspectIP
| order by TimeGenerated desc
```

This was the return:

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

LAW-Cyber-Range | Logs ☆ ...

Log Analytics workspace

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Logs

Resource visualizer

Settings

Tables

Agents

Usage and estimated costs

Data export

Network isolation

Identity

Linked storage accounts

Properties

Add or remove favorites by pressing Ctrl+Shift+F

New Query 1 * ... +

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

```
16 | where EventCount >= 50
17 | order by EventCount desc
18
19 let TargetDevice = "brucesept17vm3";
20 let SuspectIP = "178.16.53.22";
21 DeviceLogonEvents
22 | where ActionType == "LogonSuccess"
23 | where DeviceName == TargetDevice and RemoteIP == SuspectIP
24 | order by TimeGenerated desc
25
```

Results Chart

No results found from the last 24 hours
Try [selecting another time range](#)

3s 262ms Query details

And from this suspicious IP Address: 31.184.218.234

```
let TargetDevice = "brucesept17vm3";
let SuspectIP = "31.184.218.234";
DeviceLogonEvents
| where ActionType == "LogonSuccess"
| where DeviceName == TargetDevice and RemoteIP == SuspectIP
| order by TimeGenerated desc
```

This was the return:

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

The screenshot shows the 'LAW-Cyber-Range | Logs' interface in the Log Analytics workspace. A sidebar on the left contains navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Logs (selected), Resource visualizer, Settings, Tables, Agents, Usage and estimated costs, Data export, Network isolation, Identity, Linked storage accounts, and Properties. The main area displays a 'New Query 1*' editor with a KQL query. The query is set to a time range of 'Last 24 hours' and shows '1000 results'. The query text is as follows:

```
16 | where EventCount >= 50
17 | order by EventCount desc
18
19 let TargetDevice = "brucesept17vm3";
20 let SuspectIP = "31.184.218.234";
21 DeviceLogonEvents
22 | where ActionType == "LogonSuccess"
23 | where DeviceName == TargetDevice and RemoteIP == SuspectIP
24 | order by TimeGenerated desc
25
```

Below the query editor, the 'Results' tab shows a message: 'No results found from the last 24 hours. Try [selecting another time range](#).' The status bar at the bottom indicates '1s 638ms' and a 'Query details' link.

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 brucesept17vm3. 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 "bruce Virtual Machine Brute Force Detection" with incident number 181461. The page is in the "Overview" tab. The incident is classified as "Medium" severity and "Closed" status. The workspace name is "law-cyber-range". The description states: "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". The alert product names include "Microsoft Sentinel". The reason for closing is "TruePositive - Suspicious activity". The evidence section shows 9 events, 1 alert, and 0 bookmarks. The incident timeline shows a single event on Sep 17 at 15:40:07. The entities section lists "linux-target-1" (Host), "115.140.161.61" (IP), and "db931" (Host). The top insights section shows "Windows sign-in activity" for the period 9/16/2025, 8:45:08 PM - 9/17/2025, 8:45:08 PM, with a table showing 0 successful and 0 failed sign-ins. The similar incidents section shows a table with one incident: "Ossie- Create Alert Rule (Brute F..." with severity "Medium", incident number "181462", and last update time "9/17/2025, 08:46 PM".

Home > Microsoft Sentinel | Incidents >

bruce Virtual Machine Brute Force Detection ...
Incident number 181461

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 Closed Status d9a7b59833... Owner

Workspace name
law-cyber-range

Description
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

Alert product names
• Microsoft Sentinel

Reason for closing
TruePositive - Suspicious activity
Even though multiple attempts were made Brute Force was not successful, so no threats related to this incident.

Evidence
9 Events 1 Alerts 0 Bookmarks

Last update time 9/17/2025, 8:45:08 PM Creation time 9/17/2025, 8:45:08 PM

Investigate

Overview Entities

Incident timeline
Sep 17 15:40:07 bruce Virtual Machine ...

Entities
linux-target-1 Host
115.140.161.61 IP
db931 Host

Top insights
Last 24 hours before the first alert
Windows sign-in activity
9/16/2025, 8:45:08 PM - 9/17/2025, 8:45:08 PM
linux-target-1
Title Signin Co... User Count
Successful 0 0
Failed 0 0
Sign-ins over time

Similar incidents
Severity Incident number Title Last update time Str
Medium 181462 Ossie- Create Alert Rule (Brute F... 9/17/2025, 08:46 PM Ne

This has been classified as a "True Positive."