Automated SSH Brute Force Detection: Cloud SOC Monitoring with Microsoft Sentinel

Overview

This project implements an automated SSH brute force attack detection system using Microsoft Sentinel in Azure. It collects Linux VM authentication logs via Syslog, analyses them with KQL queries to identify suspicious login patterns, and triggers Logic App playbooks for real-time email alerts. The solution maps to MITRE ATT&CK T1110 (Brute Force) and demonstrates end-to-end SOC workflows from log ingestion to response. Designed for cloud security teams, it highlights SIEM analytics, automation, and threat simulation using tools like Hydra for testing.

Workflow

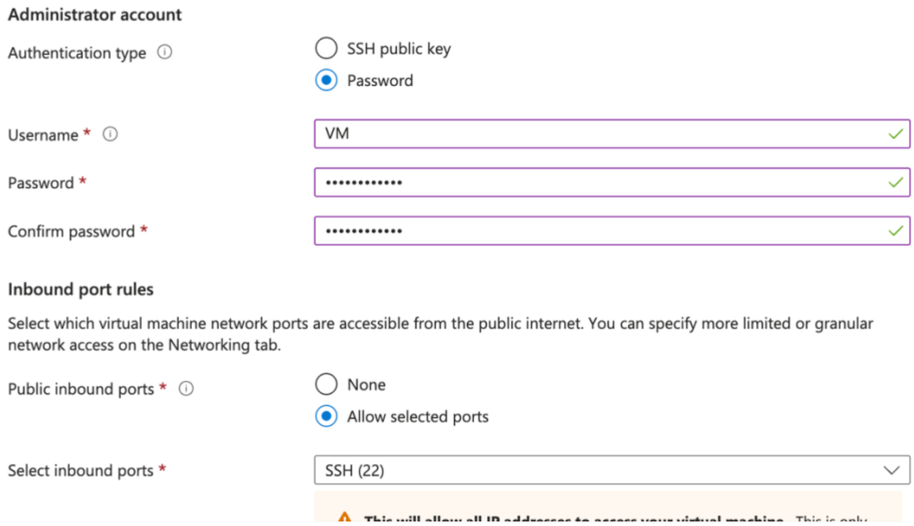
1. Linux VM generates SSH authentication logs.
2. Syslog forwards logs to Microsoft Sentinel.
3. Data Collection Rule (DCR) processes and stores logs.
4. KQL Analytical Rule detects brute force patterns.
5. Logic App Playbook triggers email alerts and/or mitigation actions.

Environment Setup

- Platform: Microsoft Sentinel (Azure Cloud SIEM)
- Log Source: Linux VM running SSH (sshd) on port 22
- Logging Method: Syslog with Data Collection Rule (DCR) for authpriv and auth logs
- Tools: Azure Sentinel, KQL, Logic Apps, Hydra (for testing)

VM Setup

This screenshot shows the authentication configuration for an Azure Linux Virtual Machine (VM) during setup. Instead of using the more secure SSH public key (RSA) authentication, this VM was configured with password-based authentication.



Administrator account

Authentication type ⓘ ○ SSH public key ● Password

Username * ⓘ VM ✓

Password * •••••••••••• ✓

Confirm password * •••••••••••• ✓

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

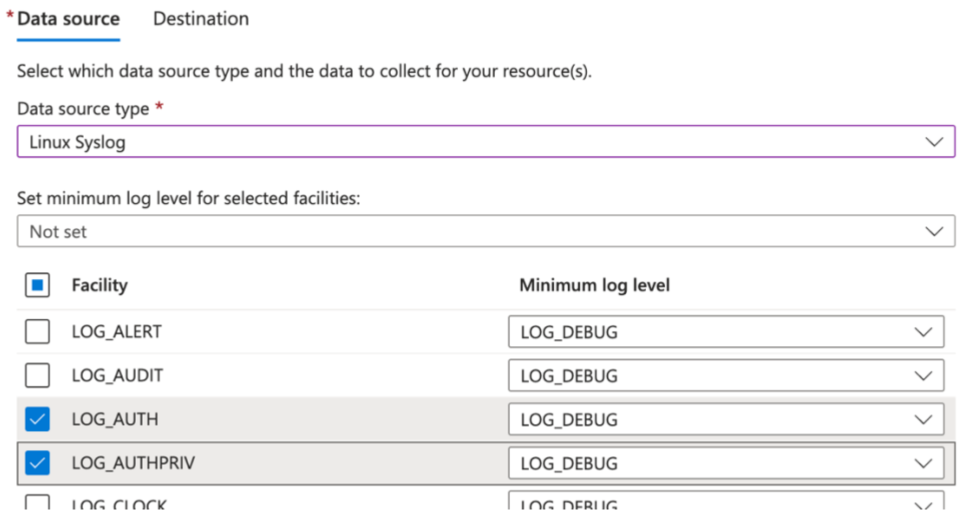
Public inbound ports * ⓘ ○ None ● Allow selected ports

Select inbound ports * SSH (22)

⚠ This will allow all IP addresses to access your virtual machine. This is only

DCR Syslog

The screenshot shows the configuration of Syslog data collection in Azure Monitor, specifically tuned to capture authentication-related events from Linux systems for security monitoring.



*Data source   Destination

Select which data source type and the data to collect for your resource(s).

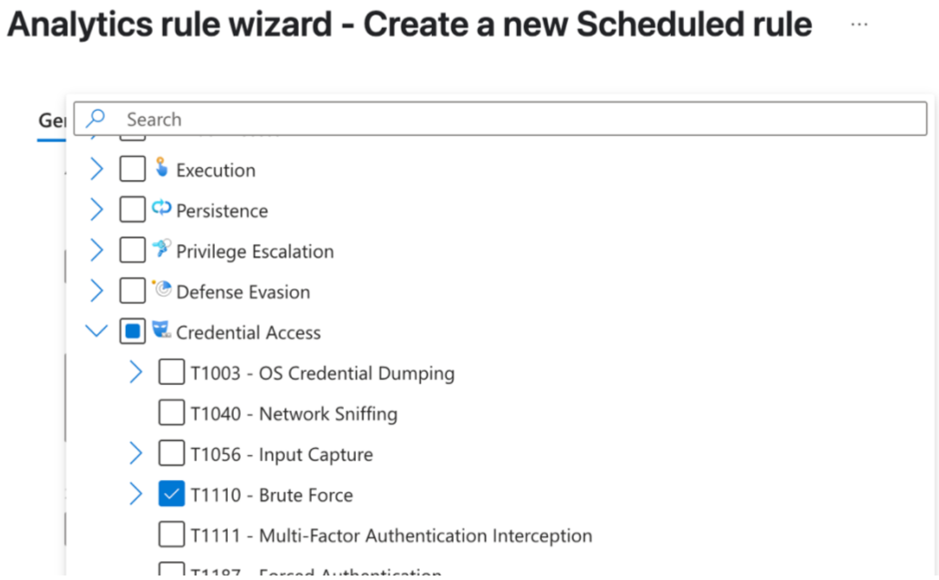
Data source type *
Linux Syslog

Set minimum log level for selected facilities:
Not set

■ Facility	Minimum log level
□ LOG_ALERT	LOG_DEBUG
□ LOG_AUDIT	LOG_DEBUG
☑ LOG_AUTH	LOG_DEBUG
☑ LOG_AUTHPRIV	LOG_DEBUG
□ LOG_CLOCK	LOG_DEBUG

MITRE ATT&CK Mapping with Analytics Rule Wizard Configuration

This image shows the Microsoft Sentinel Analytics Rule Wizard being configured to create a detection rule specifically focused on MITRE ATT&CK Tactic T1110 (Brute Force Attacks).



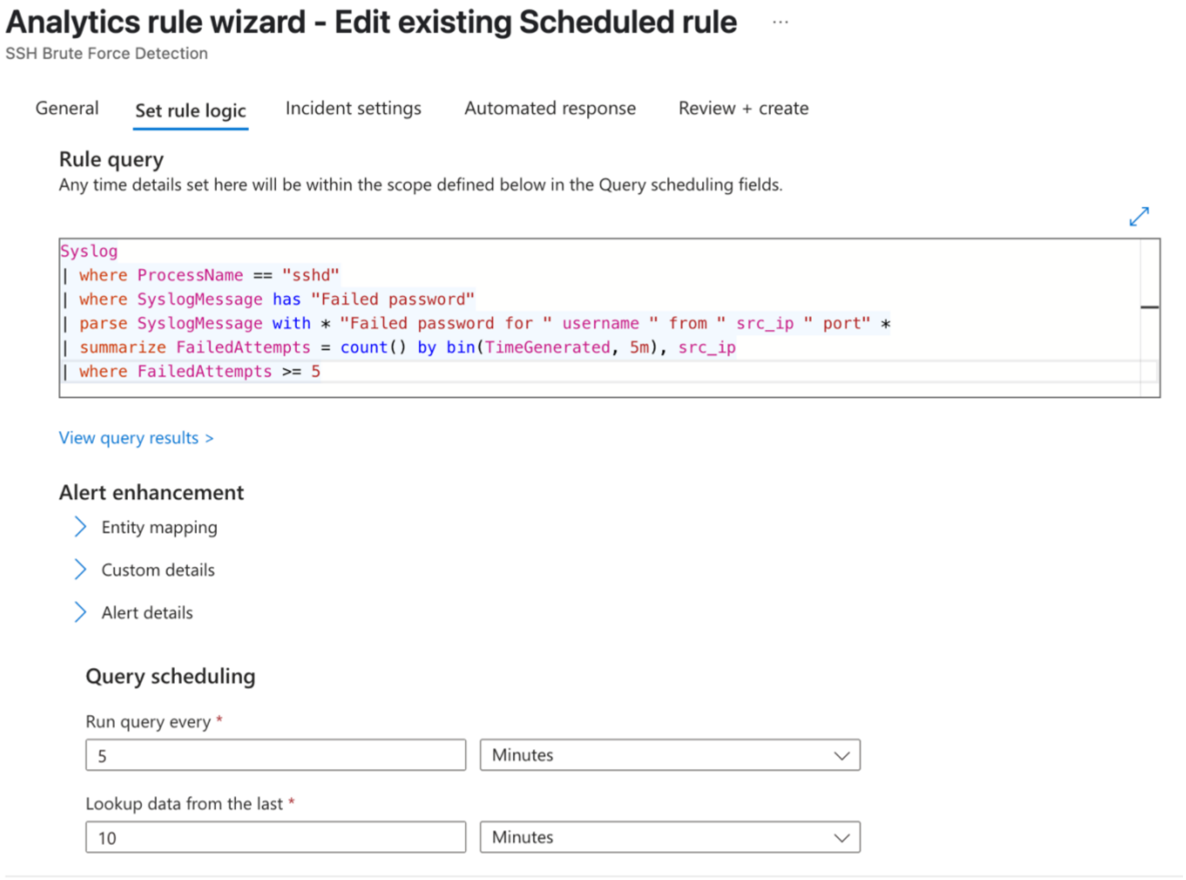
Analytics rule wizard - Create a new Scheduled rule ...

Search

- □ Execution
- □ Persistence
- □ Privilege Escalation
- □ Defense Evasion
- ■ Credential Access
  - □ T1003 - OS Credential Dumping
  - □ T1040 - Network Sniffing
  - □ T1056 - Input Capture
  - ☑ T1110 - Brute Force
  - □ T1111 - Multi-Factor Authentication Interception
  - □ T1187 - Forced Authentication

Setting Rule Logic

This screenshot shows the configuration of scheduled analytics rule in Microsoft Sentinel designed to detect SSH brute force attacks on Linux systems.



Analytics rule wizard - Edit existing Scheduled rule

SSH Brute Force Detection

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 has "Failed password"
| parse SyslogMessage with * "Failed password for " username " from " src_ip " port" *
| summarize FailedAttempts = count() by bin(TimeGenerated, 5m), src_ip
| where FailedAttempts >= 5
```

Alert enhancement

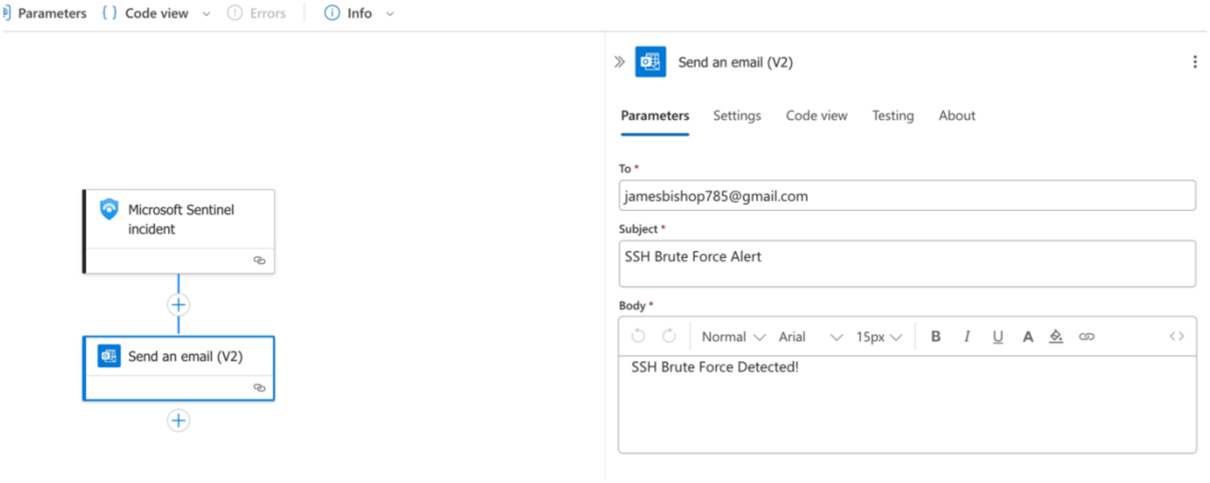
Query scheduling

Run query every *: 5 Minutes

Lookup data from the last *: 10 Minutes

Logic App Playbook

This screenshot shows the configuration of an automated email notification system in Microsoft Sentinel, designed to alert security teams about detected SSH brute force attacks.



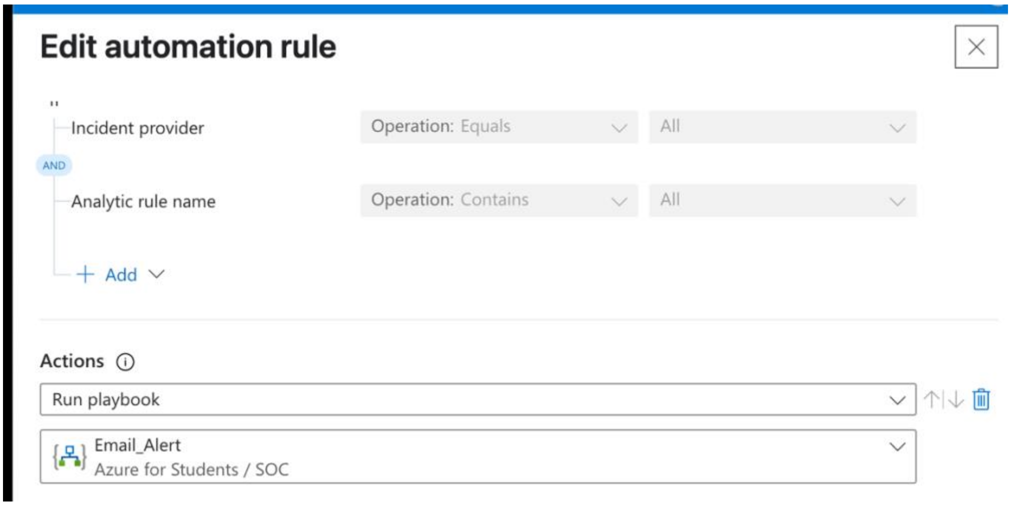
To *: jamesbishop785@gmail.com

Subject *: SSH Brute Force Alert

Body *: SSH Brute Force Detected!

Automation Rule

This screenshot shows the configuration of an Automation Rule in Microsoft Sentinel that links security incidents to response actions.



Edit automation rule

Incident provider — Operation: Equals — All

AND

Analytic rule name — Operation: Contains — All

+ Add

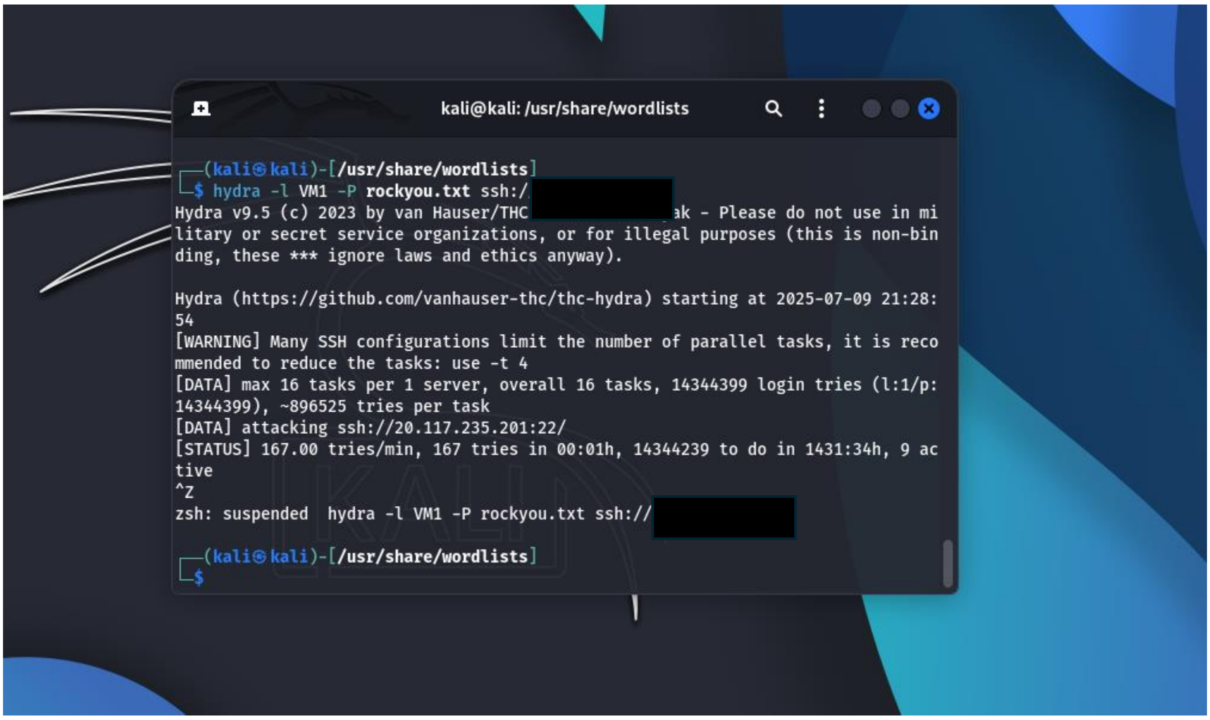
Actions

Run playbook

Email_Alert
Azure for Students / SOC

Brute-Force Attack

This screenshot captures an active SSH brute force attack simulation being conducted from Kali Linux using Hydra.



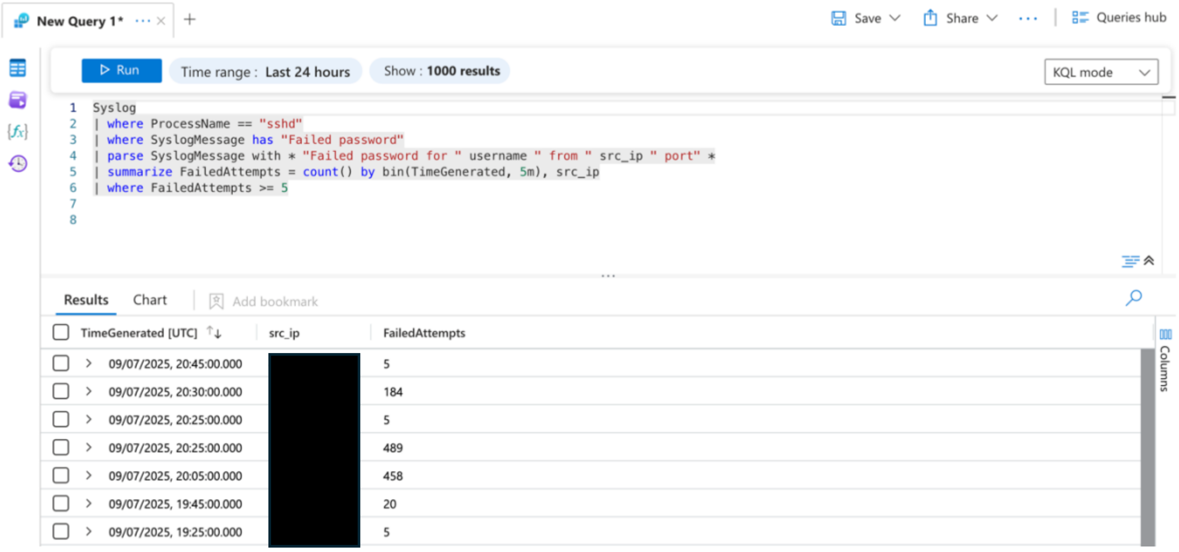
```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ hydra -l VM1 -P rockyou.txt ssh:/[redacted]
Hydra v9.5 (c) 2023 by van Hauser/THC [redacted]ak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-09 21:28:
54
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:
14344399), ~896525 tries per task
[DATA] attacking ssh://20.117.235.201:22/
[STATUS] 167.00 tries/min, 167 tries in 00:01h, 14344239 to do in 1431:34h, 9 ac
tive
^Z
zsh: suspended  hydra -l VM1 -P rockyou.txt ssh://[redacted]

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$
```

Brute Force Logs

This screenshot shows the results of a Kusto Query Language (KQL) investigation in Microsoft Sentinel, revealing active SSH brute force attacks against the Linux VM.

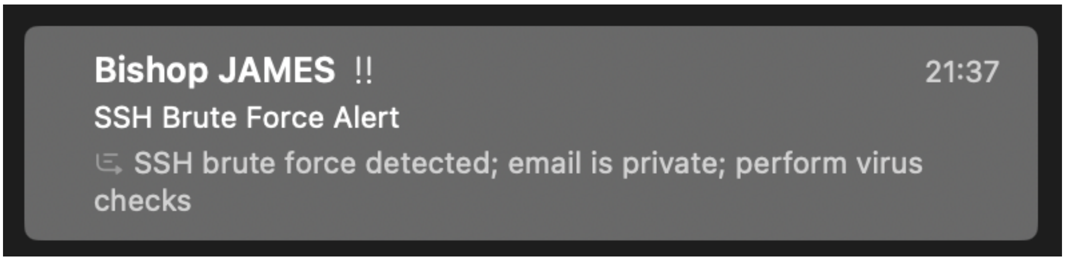


```
Syslog
| where ProcessName == "sshd"
| where SyslogMessage has "Failed password"
| parse SyslogMessage with * "Failed password for " username " from " src_ip " port" *
| summarize FailedAttempts = count() by bin(TimeGenerated, 5m), src_ip
| where FailedAttempts >= 5
```

TimeGenerated [UTC]	src_ip	FailedAttempts
09/07/2025, 20:45:00.000	[redacted]	5
09/07/2025, 20:30:00.000	[redacted]	184
09/07/2025, 20:25:00.000	[redacted]	5
09/07/2025, 20:25:00.000	[redacted]	489
09/07/2025, 20:05:00.000	[redacted]	458
09/07/2025, 19:45:00.000	[redacted]	20
09/07/2025, 19:25:00.000	[redacted]	5

Notification

This screenshot shows an email alert generated by Microsoft Sentinel's Logic App playbook, notifying me about a detected SSH brute force attack.



Bishop JAMES !! 21:37

SSH Brute Force Alert

SSH brute force detected; email is private; perform virus checks

Skills Applied

- Cloud Security (Azure Sentinel, Linux VM)
- SIEM Analytics (KQL query writing)
- SOC Automation (Logic Apps, playbooks)
- Threat Simulation (Hydra, MITRE ATT&CK T1110)