

Incident Response in SIEM Microsoft Sentinel Using NIST 800-61

In this project I observed potential brute force attacks against Windows VM, this VM a part of the Security group created in Azure that was intentionally weakened by having weak login, inbound rules open to all traffic and firewalls turned off. Within the project I applied custom analytics rules that are query based that will be used to trigger potential alerts, this will then generate incidents within sentinel leading to performing the proper incident response procedures using NIST 800-61 Preparation, Detection and Analysis, Containment, Eradication and recovery, Post Incident Activity.

Preparation:

Initiated by having already ingested logs in Log analytics workspace and Sentinel then configure rules for alerts.

- Implemented this query that logs the alert when multiple failed logins which are likely brute force attempts. Here the query shows if there are 10 failed logins within a 1 hour period alert would be logged.

| Logs ☆ ...



- Configured query rule **Detection & Analysis:**
 - setting severity, status, Owner
 - View full details
 - Observe Activity Log

- Observe Entities and Incident timelines etc
- Determine true positive

Home > Microsoft Sentinel > Microsoft Sentinel | Analytics >

Analytics rule wizard - Create a new scheduled rule

General Set rule logic Incident settings Automated response Review and create

Create an analytics rule that will run on your data to detect threats.

Analytics rule details

Name *
TEST: Brute Force Winodws

Description

Tactics and techniques
2 selected

Severity
Medium

Status
Enabled Disabled

Next: Set rule logic >

- Setting rule logic

Home > Microsoft Sentinel > Microsoft Sentinel | Analytics >

Analytics rule wizard - Create a new scheduled rule

General **Set rule logic** Incident settings Automated response Review and 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.

⚠ One or more entity mappings have been defined under the new version of Entity Mappings. These will not appear in the query code. Any entity mappings defined in the query code will be disregarded.

```
SecurityEvent
| where EventID == 4625
| where TimeGenerated > ago(60m)
| summarize FailureCount = count() by AttackerIP = IPAddress, EventID, Activity, DestinationHostName = Computer
| where FailureCount >= 10
```

[View query results >](#)

Please match the numeric format

Alert enrichment

Entity mappings

- Waited to trigger incident on intentionally weakened VM's host with the rules that have been set

13 Active rules

Rules by severity: High (7) Medium (6) Low (0) Informational (0)

Active rules Rule templates Anomalies

Search by ID, name, tactic or technique Add filter

Severity	Name	Rule type	Status	Tactics	Techniques	Source name	Last Modified
High	CUSTOM: Possible Privilege Escalation (Global Admin Role Assignment)	Scheduled	Enabled	Privilege Esc...	T1548 + 3	Custom Content	3/15/2023, 8:34:22 AM
High	CUSTOM: Possible Privilege Escalation (Azure Key Vault Critical Credential Retrieva...	Scheduled	Enabled	Privilege Esc...		Custom Content	3/15/2023, 8:34:22 AM
Medium	CUSTOM: Possible Lateral Movement (Excessive Password Resets)	Scheduled	Enabled		T1555 + 1	Custom Content	3/15/2023, 8:34:22 AM
High	CUSTOM: Malware Detected	Scheduled	Enabled			Custom Content	3/15/2023, 8:34:22 AM
High	CUSTOM: Brute Force SUCCESS - Windows	Scheduled	Enabled		T1110	Custom Content	3/15/2023, 8:34:22 AM
High	CUSTOM: Brute Force SUCCESS - Linux Syslog	Scheduled	Enabled	Credential A...	T1110	Custom Content	3/15/2023, 8:34:22 AM
High	CUSTOM: Brute Force SUCCESS - Azure Active Directory	Scheduled	Enabled			Custom Content	3/15/2023, 8:34:22 AM
Medium	CUSTOM: Brute Force ATTEMPT - Windows	Scheduled	Enabled	Credential A...	T1110	Custom Content	3/15/2023, 8:34:22 AM
Medium	CUSTOM: Brute Force ATTEMPT - MS SQL Server	Scheduled	Enabled	Credential A...	T1110	Custom Content	3/15/2023, 8:34:22 AM
Medium	CUSTOM: Brute Force ATTEMPT - Linux Syslog	Scheduled	Enabled	Credential A...	T1110	Custom Content	3/15/2023, 8:34:22 AM
Medium	CUSTOM: Brute Force ATTEMPT - Azure Key Vault	Scheduled	Enabled	Credential A...	T1110	Custom Content	3/15/2023, 8:34:22 AM

Incident response **Containment** was done by stopping VM.

Eradication of incident by resetting password:

linux-vm | Reset password

Virtual machine

Search Update

Insights Alerts Metrics Diagnostic settings Logs Connection monitor (classic) Workbooks

Automation Tasks (preview) Export template

Help Resource health Boot diagnostics Performance diagnostics VM Inspector (Preview)

Reset password

The VM agent is either unavailable, or not installed, which may prevent VMAccess from running.

This uses the VMAccessForLinux extension to reset the credentials of an existing user or create a new user with sudo privileges, and reset the SSH configuration. [Learn more](#)

Mode

Reset password

Reset SSH public key

Reset configuration only

Username *

labuser

Password *

Password must have 3 of the following: 1 lower case character, 1 upper case character, 1 number, and 1 special character.

The value must be between 12 and 72 characters long.

Confirm password *

Successfully stopped virtual machine

Successfully stopped the virtual machine 'linux-vm'.

Recovery and Post Event Activity

- Determine the origin of the attack and determine if the targets are against anything else.
- Remediated incident by Resetting password of the host and enabling 2 multi factor authentication.
 - Locked down group where the host was present
- Assess potential impact of incident.