1) 10/9/2025-10/10/2025

CUSTOM: Brute Force ATTEMPT - Linux Syslog
Incident ID 1784

141 different IP addresses are associated with this medium severity incident against the system "linux-vm" (all failed)

Inspected IP's for correlations and searched for any high-severity incidents involving these IP's - none found.

This type of brute force traffic should not be reaching the VM in the first place.

Closing out incident as true positive, and will start the process for hardening NSGs.

2) 10/9/2025-10/10/2025

Credential access incident on one endpoint
Incident ID 1811

- 10 IP addresses associated with this incident against the system "windows-vm".
- 1 High-severity alert triggered - "CUSTOM: Brute Force SUCCESS - Windows"
    - IP Address: 223.100.22.69
    - Account: NT AUTHORITY\ANONYMOUS LOGON
- A number of other alerts include "CUSTOM: Brute Force ATTEMPT - Windows" and "CUSTOM: Brute Force ATTEMPT - MS SQL Server"

Inspected actions from 223.100.22.69. It was concluded that this alert was a false positive created by a service account. See explanation: https://www.inversecos.com/2020/04/successful-4624-anonymous-logons-to.html).

After the false "success", the attacker continued attempts at brute force (all failed).

Though the high-severity alert was a false positive, this type of brute force traffic should not be reaching the VM in the first place.

Closing out incident as false positive, but will start the process for hardening NSGs.

3) 10/1/2025-10/3/2025

Multi-stage incident involving Privilege escalation & Credential access on one endpoint
Incident ID 1271

Multiple high-severity alerts:

1. **CUSTOM: Brute Force SUCCESS - Azure Active Directory**
   - 1.1. IP address 20.53.16.140 involved in brute force success into the account: attacker@rez1922001gmail.onmicrosoft.com
   - 1.2. The same IP was also involved in multiple brute force attempts on the MS SQL Server that resides within "windows-vm" (all failed).
   - 1.3. Upon the initial incident alert, user account was temporarily removed from all roles/groups to prevent any further unauthorized access. Viewed account's activity in last 30 days, no malicious actions detected (no PII/PHI accessed). The compromised account's password was reset, followed by returning it to initial roles/groups. SQL server's password was reset and its associated IP address was changed. Closed out as true positive.
2. **CUSTOM: Possible Privilege Escalation (Azure Key Vault Critical Credential Retrieval or Update) + CUSTOM: Windows Host Firewall Tampering**
   - 2.1. Same IP viewed critical credentials several times
     - 2.1.1. Name: Rezwan Islam
     - 2.1.2. User principal name: rez1922001_gmail.com#ext#@rez1922001gmail.onmicrosoft.com
   - 2.2. Not only did this user view the critical credentials multiple times, they also are involved in several other incidents including excessive password resets and windows host firewall tampering.
   - 2.3. After calling the above user, they confirmed that they were just doing their normal duties; corroborated with their manager. Closing out for false positive.
3. **CUSTOM: Malware Detected**
   - 3.1. 6 alerts of this type were generated against "windows-vm". This device is also associated with several other alerts.
   - 3.2. Called the user and their supervisor, confirmed that they were running tests with EICAR files (defender deleted the files automatically). Closing out as false positive.

4) 10/3/2025-10/4/2025

CUSTOM: Possible Lateral Movement (Excessive Password Resets) involving one user
Incident ID 1700

IP address 40.123.53.159 involved in excessive password resets for the following account:

- Name: Rezwan Islam
- User principal name: rez1922001_gmail.com#ext#@rez1922001gmail.onmicrosoft.com

User's password was reset immediately. Inspected all other activity from the threat actor, no incidents/suspicious activity found. Closing out as true positive.

5) 10/8/2025

CUSTOM: Malware Detected
Incident ID 1783

6 alerts of this type were generated against "windows-vm". This device is also associated with several other alerts.

Called the user and their supervisor, confirmed that they were running tests with EICAR files (defender deleted the files automatically). Closing out as false positive.