SOC Incident Reports Portfolio

IR-001: Brute Force Login Attempt

Severity: Medium

Summary: Multiple failed authentication attempts were detected from a single IP address targeting a Windows virtual machine.

Timeline:
- Multiple failed login attempts observed
- Sentinel analytics rule triggered
- SOC investigation initiated

Findings:
- Repeated Event ID 4625 detected
- Single source IP targeting one account
- No successful authentication observed

MITRE ATT&CK;: T1110 – Brute Force

Impact: No confirmed account compromise.

Response Actions:
- Recommend blocking source IP
- Enforce account lockout policies
- Continue monitoring affected account

IR-002: Privilege Escalation Event

Severity: High

Summary: A logon event where special administrative privileges were assigned to a user account was detected.

Timeline:
- Admin logon detected
- Event ID 4672 logged
- Alert generated and reviewed

Findings:
- User account received elevated privileges
- No evidence of lateral movement
- Activity confirmed as administrative access

MITRE ATT&CK;: T1068 – Privilege Escalation

Impact: Potential risk of unauthorized system control.

Response Actions:
- Validate legitimacy of admin access
- Review group memberships
- Monitor for follow-on activity

IR-003: Network Reconnaissance Activity

Severity: Medium

Summary: Multiple network connection attempts from a single source IP were detected targeting an Azure virtual machine.

Timeline:
- Repeated connection attempts logged
- NSG Flow Logs captured activity
- Sentinel alert triggered

Findings:
- High volume of connection attempts
- Multiple ports targeted
- Pattern consistent with scanning

MITRE ATT&CK;: T1046 – Network Service Scanning

Impact: Pre-attack discovery activity identified.

Response Actions:
- Recommend blocking source IP at NSG
- Review exposed services
- Increase monitoring sensitivity