## Case report for multiple alerts

ID 1024 | ID 1003

| ID | Alert rule | Description | Incident type | Severity level | Date and time detected |
|---|---|---|---|---|---|
| 1024 | Network drive disconnected from a local drive | A network drive was disconnected from a local drive. Normally, this is not a cause for concern, but investigate further to determine if it is malicious. | Execution | Medium | Dec 1st 2025 at 19:50 |

Alert details

datasource: sysmon

timestamp: 12/01/2025 11:47:44.544

event.code: 1

host.name: win-3450

process.name: net.exe

process.pid: 8004

process.parent.pid: 3728

process.parent.name: powershell.exe

process.command_line: "C:\Windows\system32\net.exe" use Z: /delete

process.working_directory: C:\Users\michael.ascot\downloads\

event.action: Process Create (rule: ProcessCreate)

## Incident report

Incident classification

(●) True positive ( ) False positive

Case report

Please write a detailed report on the steps taken to analyse and contain this incident, including all relevant information and the rationale for its closure.

When
**Time of activity:** 12/01/2025
Time: 11:47:44.

Who
**List of Affected Entities:**
- host.name: win-3450
- process.working_directory: C:\Users\michael.ascot\downloads\ -> michael.ascot

What:
**Reason for Classifying as True Positive:**
- PowerShell spawning net.exe can be an attacker's initial move.
- The process was executed through PowerShell instead of the GUI
- This can be a possible lateral movement
- This can be a possible data exfiltration

Why:

Does this alert require escalation?

(●) Yes ( ) No

**Complete IR:**

When
Time of activity: 12/01/2025
Time: 11:47:44.

Who
List of Affected Entities:
- host.name: win-3450
- process.working_directory: C:\Users\michael.ascot\downloads\ -> michael.ascot
What:
Reason for Classifying as True Positive:
- PowerShell spawning net.exe can be an attacker's initial move.
- The process was executed through PowerShell instead of the GUI
- This can be a possible lateral movement
- This can be a possible data exfiltration

Why:
Reason for Escalating the Alert:
- michael.ascot's access and activity needs to be reviewed:
- is he performing a system maintenance?
- is he transferring or sanitizing a drive?
- when are the previous and future maintenance schedule?

How:
Recommended Remediation Actions:
- Communicate with michael.asco ASAP to check his activities
- Check the system's health - monitor for changes, data, DLP, and other alerts and service.

List of Attack Indicators:
- unusual operation process - Used PowerShell
- Removed drive