Rule – Discovery activity

Overview

This detection focuses on identifying account discovery activity performed via **PowerShell** or **cmd.exe**.
The base rule (92031) comes from the **Sysmon configuration (SwiftOnSecurity)** and triggers when commands such as `net.exe`, `net1.exe`, or `net users` are executed.

Enhancement Objective

Add additional matching for the `whoami` command to broaden coverage of discovery-related behavior under MITRE techniques **T1087 (Account Discovery)** and **T1033 (System Owner/User Discovery)**.

Correlation Rule (ID 900400)

To reduce noise and improve detection accuracy, a correlation rules was developed:

- `Confirmed discovery: PS discovery + PS-spawned + discovery executed (≤90s, same host)`

Correlation Rule (ID 900400)

- `Confirmed discovery: PS evidence + whoami (≤120s)`

This rules chains together:

- 92213 – PowerShell discovery event
- 92033 – PowerShell-spawned discovery activity
- 92031 – Discovery activity executed

If all three occur within **90 seconds** on the same host, 900400 fires as a high-confidence detection of active discovery behavior.

Logic Summary

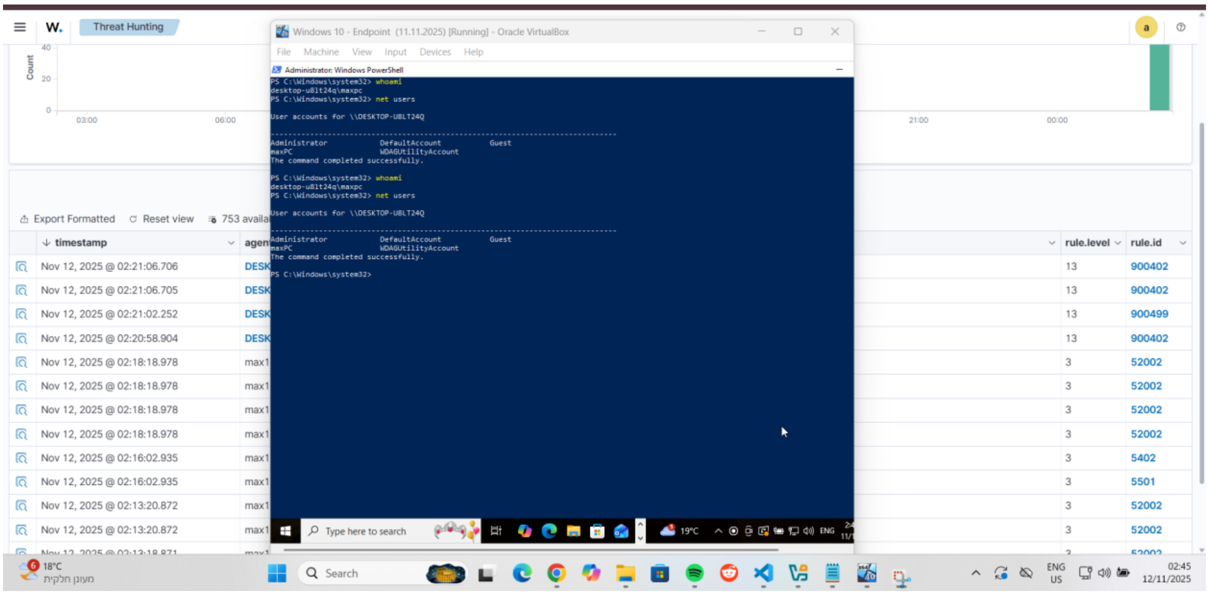
- Event source: Sysmon Operational Channel
- Trigger: Execution of account or user discovery commands (`net.exe`, `net1.exe`, `whoami`, etc.)
- Correlation window: 90 seconds
- Objective: Identify potential attack chains while suppressing isolated false positives from benign administrative activity.

- - For tests run those commands:

  - net users
  - whoami
  Or
  - powershell -c “whoami”
  - powershell -c "net user"

Future Improvements

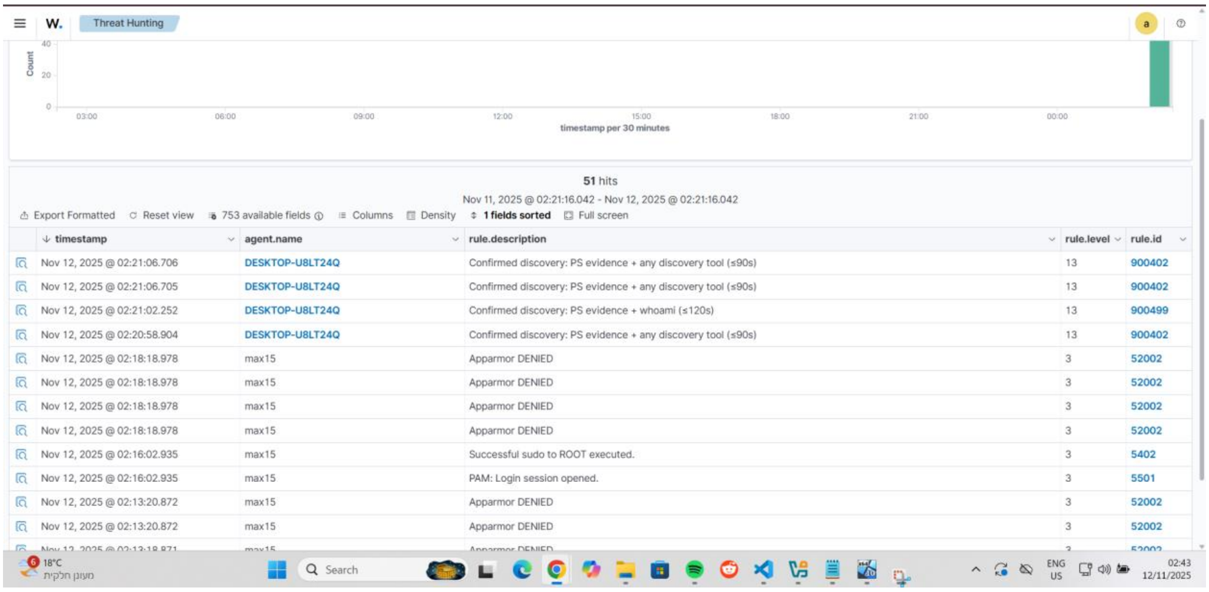
- Expand matching to include `dsquery`, `Get-ADUser`, and `Get-LocalUser` patterns.
- Introduce process tree validation (parent-child verification between PowerShell and discovery tools).
- Test detection coverage against simulated discovery scripts (e.g., via Atomic Red Team).



```
PS C:\Windows\system32> whoami
desktop-u8lt24q\maxpc
PS C:\Windows\system32> net users

User accounts for \\DESKTOP-U8LT24Q

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
maxPC                    WDAGUtilityAccount
The command completed successfully.

PS C:\Windows\system32> whoami
desktop-u8lt24q\maxpc
PS C:\Windows\system32> net users

User accounts for \\DESKTOP-U8LT24Q

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
maxPC                    WDAGUtilityAccount
The command completed successfully.

PS C:\Windows\system32>
```

Export Formatted   Reset view   753 availa

timestamp	agen	rule.level	rule.id
Nov 12, 2025 @ 02:21:06.706	DESK	13	900402
Nov 12, 2025 @ 02:21:06.705	DESK	13	900402
Nov 12, 2025 @ 02:21:02.252	DESK	13	900499
Nov 12, 2025 @ 02:20:58.904	DESK	13	900402
Nov 12, 2025 @ 02:18:18.978	max1	3	52002
Nov 12, 2025 @ 02:18:18.978	max1	3	52002
Nov 12, 2025 @ 02:18:18.978	max1	3	52002
Nov 12, 2025 @ 02:18:18.978	max1	3	52002
Nov 12, 2025 @ 02:16:02.935	max1	3	5402
Nov 12, 2025 @ 02:16:02.935	max1	3	5501
Nov 12, 2025 @ 02:13:20.872	max1	3	52002
Nov 12, 2025 @ 02:13:20.872	max1	3	52002
Nov 12, 2025 @ 02:13:18.871	max1	3	52002



51 hits

Nov 11, 2025 @ 02:21:16.042 - Nov 12, 2025 @ 02:21:16.042

Export Formatted   Reset view   753 available fields   Columns   Density   **1 fields sorted**   Full screen

timestamp	agent.name	rule.description	rule.level	rule.id
Nov 12, 2025 @ 02:21:06.706	DESKTOP-U8LT24Q	Confirmed discovery: PS evidence + any discovery tool (≤90s)	13	900402
Nov 12, 2025 @ 02:21:06.705	DESKTOP-U8LT24Q	Confirmed discovery: PS evidence + any discovery tool (≤90s)	13	900402
Nov 12, 2025 @ 02:21:02.252	DESKTOP-U8LT24Q	Confirmed discovery: PS evidence + whoami (≤120s)	13	900499
Nov 12, 2025 @ 02:20:58.904	DESKTOP-U8LT24Q	Confirmed discovery: PS evidence + any discovery tool (≤90s)	13	900402
Nov 12, 2025 @ 02:18:18.978	max15	Apparmor DENIED	3	52002
Nov 12, 2025 @ 02:18:18.978	max15	Apparmor DENIED	3	52002
Nov 12, 2025 @ 02:18:18.978	max15	Apparmor DENIED	3	52002
Nov 12, 2025 @ 02:18:18.978	max15	Apparmor DENIED	3	52002
Nov 12, 2025 @ 02:16:02.935	max15	Successful sudo to ROOT executed.	3	5402
Nov 12, 2025 @ 02:16:02.935	max15	PAM: Login session opened.	3	5501
Nov 12, 2025 @ 02:13:20.872	max15	Apparmor DENIED	3	52002
Nov 12, 2025 @ 02:13:20.872	max15	Apparmor DENIED	3	52002
Nov 12, 2025 @ 02:13:18.871	max15	Apparmor DENIED	3	52002