

# Behavioral Detection of WinRM-Based Remote Access, Detection Strategy DET0477

Archived: 2026-04-05 18:01:33 UTC

## Analytics

- [Windows](#)

### AN1313

Adversaries using WinRM to remotely execute commands, launch child processes, or access WMI. The detection chain includes service use, network activity, remote session logon, and process creation within a short temporal window.

#### Log Sources

#### Mutable Elements

Field	Description
TimeWindow	Defines max time between remote shell creation and child process execution (e.g., 60 seconds)
UserContext	Scope to unexpected remote user logons (non-admins, service accounts)
CommandLineAnomalyScore	Score for suspicious command usage via WinRM (e.g., encoded PowerShell)
KnownAdminHosts	List of trusted systems allowed to use WinRM legitimately

---

Source: <https://attack.mitre.org/detectionstrategies/DET0477#AN1313>