Detection of Command-Line Interface, Detection Strategy DET0760

Archived: 2026-04-05 17:15:28 UTC

On Windows and Unix systems monitor executed commands and arguments that may use shell commands for execution. Shells may be common on administrator, developer, or power user systems depending on job function.

On network device and embedded system CLIs consider reviewing command history if unauthorized or suspicious commands were used to modify device configuration.
Monitor logs from installed applications (e.g., historian logs) for unexpected commands or abuse of system features.
Monitor for processes spawning from known command shell applications (e.g., PowerShell, Bash). Benign activity will need to be allow-listed. This information can be useful in gaining additional insight to adversaries' actions through how they use native processes or custom tools.
