

AUTOMATE **Advanced** 30 MIN · UPDATED 2026-09-30

Run a security script analysis before deployment.

Use Security Copilot to evaluate a script for safety issues before it ships to production.

MICROSOFT 365

Teams

WORKS WITH

Security Copilot

Business Outcome

Fewer security incidents caused by scripts that weren't reviewed for risky behavior before deployment.

Workflow Steps

Step 1: Submit the script with its intended context

Security Copilot

Give Security Copilot the script along with what it's meant to do and where it will run (a scheduled task, a login script, a deployment pipeline) — the same command can be benign or risky depending on context.

Step 2: Ask for a specific risk breakdown

Security Copilot

Have it evaluate the script for concrete risk categories – unrestricted network calls, credential handling, privilege escalation, destructive file operations – rather than a general "looks fine" verdict.

PROMPT

Review this PowerShell script intended to run as a scheduled maintenance task on domain-joined machines. Flag any command that makes an outbound network call, handles credentials, or could escalate privileges, and explain the specific risk for each.

Step 3: Have a security engineer review every flag

Teams

Post the flagged behaviors and Security Copilot's stated reasoning to the reviewing engineer in Teams, with the script attached.

Have them confirm each flag against the script's actual intended use (a credential handling flag might be completely necessary for this specific maintenance task) rather than reflexively stripping out anything flagged.

Step 4: Re-run after every material change

Security Copilot

Any time the script changes meaningfully, re-run the analysis – a script that passed review last month may have picked up new risky behavior since.

✓ Check the work

- Manually inspect every flagged line to confirm the described risk is accurate, not a false positive from pattern matching.
- Confirm the analysis actually covered the full script, not just a truncated portion.
- Don't treat a "clean" result as a substitute for a human security review on any script with elevated privileges.



Expected Outcome

A specific list of flagged risky behaviors in the script, or a clean result, before it's approved for deployment.

Want help rolling this out across your team? [Go to Liminals.Tech](#) ■