

Detection of Serverless, Detection Strategy DET0829

Archived: 2026-04-05 18:19:55 UTC

AN1961

Once adversaries leverage serverless functions as infrastructure (ex: for command and control), it may be possible to look for unique characteristics associated with adversary software, if known.^[1] Much of this activity will take place outside the visibility of the target organization, making detection of this behavior difficult. Detection efforts may be focused on related stages of the adversary lifecycle.

Log Sources

Data Component	Name	Channel
Response Content (DC0104)	Internet Scan	None

Source: <https://attack.mitre.org/detectionstrategies/DET0829#AN1961>