

# Detection Strategy for Exfiltration to Code Repository, Detection Strategy DET0318

Archived: 2026-04-05 16:28:04 UTC

## AN0895

Processes such as PowerShell, Git, or curl initiating outbound HTTPS POST requests to known code repository APIs (e.g., github.com, gitlab.com) immediately following large file reads. Defender view: correlation between file access of sensitive directories (e.g., Documents, Finance) and abnormal data uploads to repository domains.

### Log Sources

### Mutable Elements

Field	Description
MonitoredDomains	List of external code repository domains to monitor (github.com, gitlab.com, bitbucket.org).
ExfilVolumeThreshold	Threshold for outbound data volume per session to flag suspicious uploads.

## AN0896

Processes like git, curl, or python scripts executing commands that package files (tar, gzip) followed by HTTPS uploads to code repository endpoints. Defender view: detect unusual git push activity or scripted HTTPS requests outside normal developer work hours.

### Log Sources

### Mutable Elements

Field	Description
WorkHours	Baseline normal developer activity periods to reduce false positives.
RepoDomainList	Known allowed internal or external repository domains.

## AN0897

Office or scripting applications initiating unusual HTTPS traffic to code repository APIs with high outbound-to-inbound ratios. Defender perspective: monitor for sensitive file access in combination with network connections to github.com, gitlab.com, or bitbucket.org.

**Log Sources**

**Mutable Elements**

<b>Field</b>	<b>Description</b>
MonitoredApplications	Applications not expected to upload large data sets to repos (Word, Excel, Preview).

**AN0898**

ESXi host processes (vmx, hostd) initiating HTTPS sessions toward external code repositories. Defender perspective: detect datastore reads followed by outbound web traffic inconsistent with administrative baselines.

**Log Sources**

**Mutable Elements**

<b>Field</b>	<b>Description</b>
DatastoreTransferThreshold	Amount of data moved from datastore to external services before raising alert.

---

Source: <https://attack.mitre.org/detectionstrategies/DET0318#AN0897>