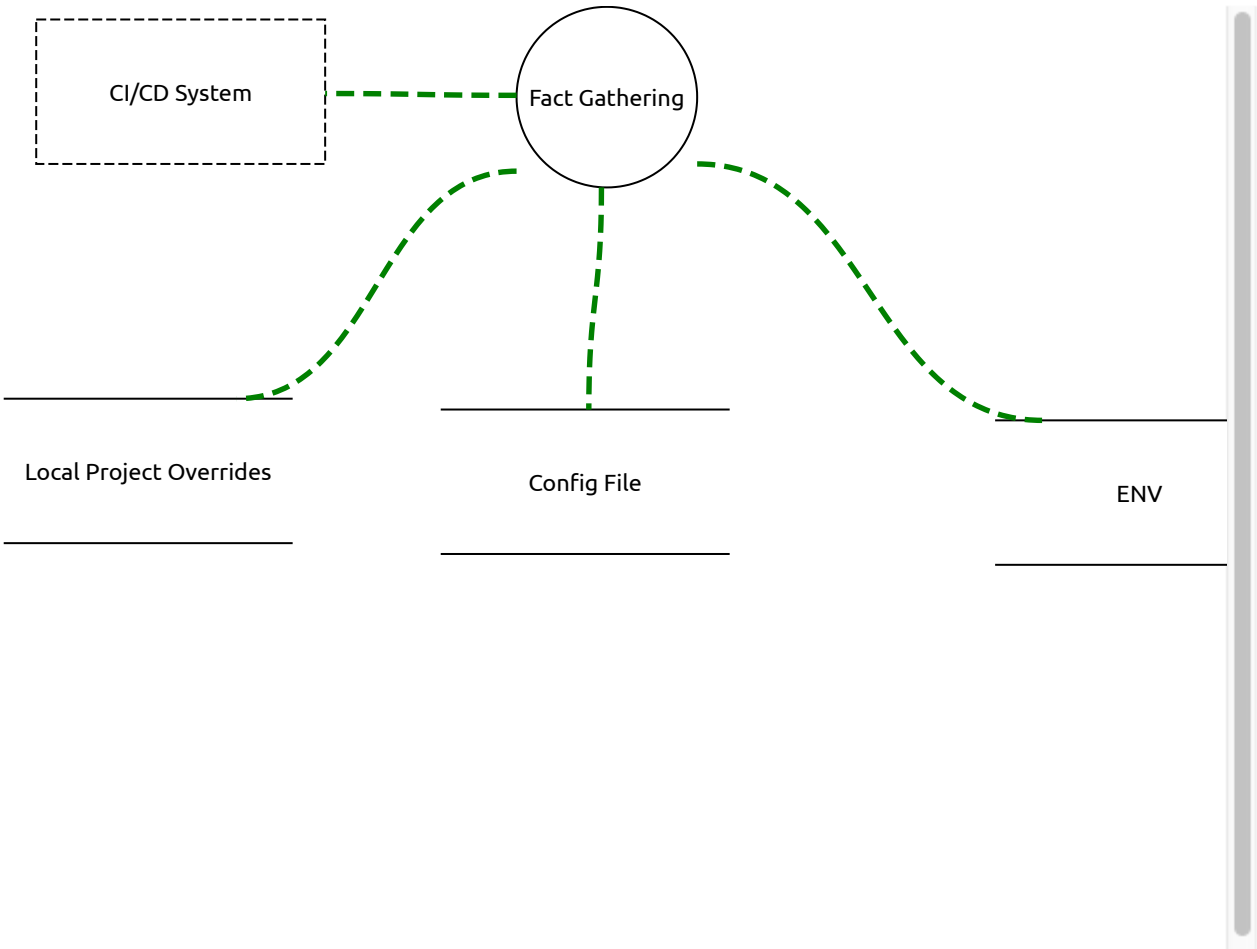
Threat model report for Peril CLI Tool

Owner:
erich.smith
Reviewer:
adam.williams
Contributors:

High level system description

CLI tool for analyzing project risk

Fact Discovery



Fact Gathering (Process)

Description:
Gather facts prior to performing checks

ID: potential display of sensitive values

Information disclosure, Mitigated, Medium Severity

Description:
Sensitive values discovered at fact-gathering time may later leak if displayed via log or stack trace.

Mitigation:
Application code redacts sensitive facts from configuration before display.

ENV (Data Store)

Description:
Process ENV

Information Disclosure Threat

Information disclosure, Mitigated, Medium Severity

Description:
Sensitive credentials are expected to be passed in from ENV. These may leak out via logs, stack-traces, etc.

Mitigation:
Application redacts sensitive values before debug logging.

Config File (Data Store)

Description:
Config values may be optionally specified in config file

No threats listed.

Local Project Overrides (Data Store)

Description:
Authorized users (typically security team) may sign tokens that override risk values or force-accept risk.

Copy/Pasted overrides may be inserted into project repos.

Repudiation, Mitigated, High Severity

Description:

A previous, valid override token may be copy/pasted into another project repo, in an attempt to re-use the override.

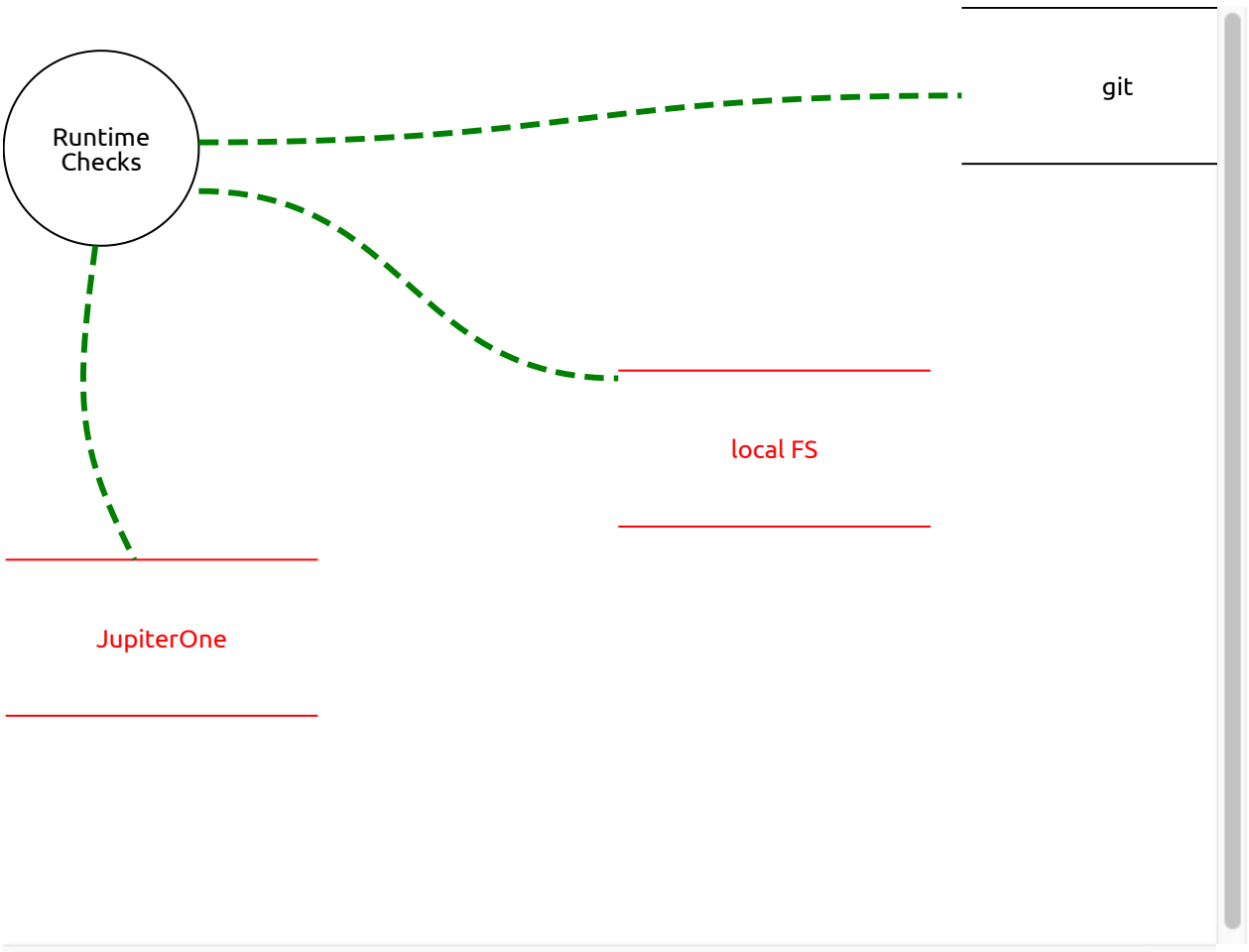
Mitigation:
Mitigated by run-time code at check-time. (See other diagram)

CI/CD System (out of scope External Actor)

Description:
Invoker of peril CLI

Out of scope reason:
CI/CD security is handled CSP, or Vendor and ultimately responsibility of Peril user.

Checks



Runtime Checks (Process)

Activated Desktop Report Controller

Description:

Post fact-gathering checks that gather risk elements.

Malicious repo commiters can copy/paste override tokens

Spoofing, Mitigated, Medium Severity

Description:
Commiters can attempt to spoof valid, signed override tokens by copy/pasting from another repository.

Mitigation:
Signed token payloads include project/repo name, and this is verified at runtime.

git (Data Store)

Description:
introspect the local repo via `git` commands

Malicious commits could impersonate someone other than commit authors.

Repudiation, Mitigated, Medium Severity

Description:
It is possible to craft git commits with arbitrary author name/email values.

Mitigation:
GPG signing is supported and encouraged by peril.

local FS (Data Store)

Description:

It is possible to inject fake scan data into repo fs.

Tampering, Mitigated, Medium Severity

Description:
A malicious repo author could commit fake scan data to a path with Peril auto-discovers and treats as genuine.

Mitigation:
Transfer. It is expected that the caller of peril has run sideband security scanning, such as ShiftLeft/scan, in a CI/CD step prior to invoking peril.

Malicious JSON DoS threat

Denial of service, Open, Low Severity

Description:
It is possible for malicous repo committers to commit very large JSON files that cause the parser to behave poorly.

Mitigation:

JupiterOne (Data Store)

Description:
Query J1 for relevant risk elements.

Tampering of graph data threat

Tampering, Open, Medium Severity

Description:
It is possible for users of the J1 system to tamper with graph data in an attempt to modify Peril risk results.

Mitigation:

DoS threat

Denial of service, Mitigated, Low Severity

Description:
If JupiterOne is behaving poorly, or down, this could cause peril to block, effectively DoSing CI.

Mitigation:
Retry logic in code has sensible timeouts.