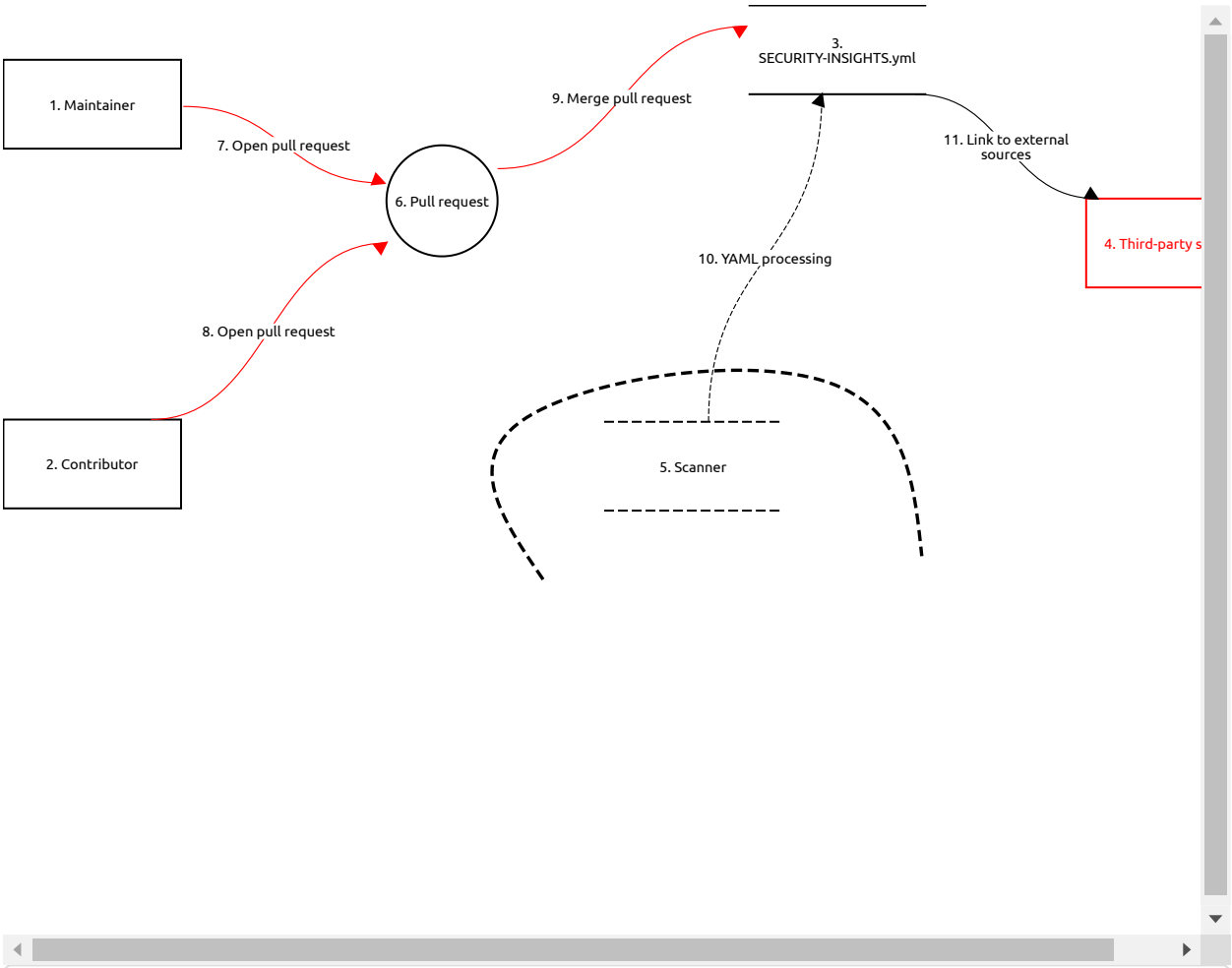
Threat model report for SECURITY-INSIGHTS Threat Model

Owner:
Luigi Gubello
Reviewer:
Contributors:

High level system description

A threat model for the project SECURITY-INSIGHTS to evidence the related risks.

SECURITY-INSIGHTS Threat Model



1. Maintainer (External Actor)

Description:
Official maintainer of the open source project

No threats listed.

2. Contributor (External Actor)

Description:
External contributor to the open source project

No threats listed.

4. Third-party sources (External Actor)

Description:
(e.g. URLs, documents, third-party tools mentioned in the SECURITY-INSIGHTS.yml)

Supply-chain

Spoofing, Open, High Priority

Description:
Attackers can obtain the control of a third-party sources (e.g. website domain, server, etc) linked in the SECURITY-INSIGHTS.yml.

Mitigation:
Maintainers could self-host the evidence to reduce risks.

6. Pull request (Process)

Description:

No threats listed.

7. Open pull request (Data Flow)

Description:
The user opens a pull request to edit/update/implement SECURITY-INSIGHTS.yml

False information in the SECURITY-INSIGHTS.yml

Repudiation, Open, High Priority

Description:
Maintainers could upload false information in the SECURITY-INSIGHTS.yml just to obtain a high score from the scanners or other services which use SECURITY-INSIGHTS to evaluate the project.

Mitigation:
Scanners could introduce some additional checks (e.g. check if URLs return 200 OK status) and a weighted score to reduce the risks. In addition, the open-source community can read the file and report false information (or just information without clear evidence).

Private information sharing

Information disclosure, Open, High Priority

Description:
A maintainer shares mistakenly private critical information (e.g. security audit containing unpatched vulnerabilities).

Mitigation:

8. Open pull request (Data Flow)

Description:
The user opens a pull request to edit/update/implement SECURITY-INSIGHTS.yml

Malicious pull-request

Tampering, Open, Medium Priority

Description:
A malicious contributor could introduce false or malicious information (e.g. malicious URLs) to obtain a particular advantage.

Mitigation:
The contributors' PRs to SECURITY-INSIGHTS.yml should be carefully reviewed and approved by the maintainers. In addition, the maintainers could decide to not accept direct contributions to the SECURITY-INSIGHTS.yml.

9. Merge pull request (Data Flow)

Description:

Missing pull-request review or lacks in the review process

Tampering, Open, Medium Priority

Description:
Missing PR review or lack in the review process can lead to the tampering of SECURITY-INSIGHTS.yml by adding false information.

Mitigation:
THE PR should be formally reviewed and approved by another maintainer.

3. SECURITY-INSIGHTS.yml (Data Store)

Description:

No threats listed.

11. Link to external sources (Data Flow)

Description:
SECURITY-INSIGHTS.yml links to external sources

No threats listed.

5. Scanner (out of scope Data Store)

Description:
A tool that processes the SECURITY-INSIGHTS.yml

Out of scope reason:
Vulnerabilities or malicious behaviors in the scanner are not directly related to SECURITY-INSIGHTS.yml

10. YAML processing (out of scope Data Flow)

Description:
The scanner ingests and processes the SECURITY-INSIGHTS.yml

Out of scope reason:
The scanner's security is not directly related to SECURITY-INSIGHTS.yml