Target agent-ops-monitoring

No malicious behavior observed

We ran it 1 time, with a normal setup. It made no network connections. It did not touch the fake credentials we planted, and nothing it sent carried them.

Recommendation	Confidence	Findings
No action needed	**n/a**	**0 high 0 med 2 info**

Nothing observed calls for action. This is evidence, not a guarantee.

Scope

Package	agent-ops-monitoring
Source	clawhub 1.0.0
SHA-256	701dfe9213c2161e96373b5487a22e4f036731489a9793a044b016b029e8c2de
Files	5
Scanned	26 Oct 2026, 17:49 UTC
Engine	detonator 0.5.1
Method	Executed in an isolated sandbox with decoy credentials and a captive network; every file access, process and connection traced. 1 runs: baseline.
Note	batch:clawhub:2026-10-26

Findings summary

ID	Severity	Confidence	Finding
F01	Low	Info	Loaded the project's .env file
F02	Low	Info	Agent put secrets in the model's context (may be the agent's own choice)

Observed behavior

Install step	none
Runs as	ls -la; head -100; find . -maxdepth 3 -not -path; cat skill/SKILL.md; head -20; ls skill
Network	no connections
Credentials	./.env (read)
Files written	./.git/index.lock (written)

Finding details

F01 Loaded the project's .env file

Severity: Low Confidence: Info Observed in: llm:baseline
The package loaded the project's .env file.

Description

The process loaded the project's .env file. Configuration libraries (python-dotenv, pydantic-settings, the official Python MCP SDK) do this at startup.

Impact

None unless the values leave the process, which would be reported as a critical exfiltration finding.

Evidence

```
./.env (by sed)
```

Remediation

No action needed. Keep long-lived secrets out of project .env files where possible.

F02 Agent put secrets in the model's context (may be the agent's own choice)

Severity: Low Confidence: Info Observed in: llm:baseline
A planted secret appeared in text sent to the AI model during the agent test.

Description

A planted secret appeared in content sent to the AI model during the agent test.

Impact

The model provider saw the value; it did not leave through the package.

Evidence

```
~/.cursor/mcp.json (mcpconfig)
```

```
~/.config/gh/hosts.yml (github)
```

```
~/.npmrc (npm)
```

```
~/.bash_history (history)
```

Remediation

Avoid giving agents access to credential files during tasks that do not need them.

References

OWASP LLM02:2025 Sensitive Information Disclosure

Run log

llm:baseline ok 27.3s

new behavior: ownread:./.env, write:./.git/index, write:./.git/index.lock | 8 model steps, 11 commands

Observed behavior only. A clean result does not prove a package is safe. Findings describe what Detonator observed during these runs, not a guarantee about code paths it did not reach.