Untrusted input for a security agent

2026-11-12T10:02:19Z run=r-3107 rule=untrusted-context-v2 tool=alert_close decision=blocked input_tag=outside_control tag_source=alert_connector

Agentic AI in Cybersecurity, Untrusted input for a security agent, edition 19 Nov 2026, https://agenticaiincybersecurity.com/evaluation-checklist/untrusted-input/. License CC BY 4.0.