



PhalanxAI Security

Sentinel Agent Drift Scanner Report

Scan ID: 07aff414-621c-4bee-a58a-ba9b2369a49c

Mode: local-only

Generated: 2026-08-12T18:37:04Z

35 findings -- exactly what an attacker goes looking for first.

12 of them are CRITICAL or HIGH severity. Every day these sit unfixed is a day something can walk through them.

PhalanxAI's 2-Week AI Security Readiness Audit turns this into a prioritized remediation roadmap and an exec presentation that actually gets action -- not another PDF that sits in a folder.

[Inquire about your audit call ->](#)

SAMPLE

Insured & Bonded

Professional Liability (E&O), General Liability, Cyber Liability. Certificate of Insurance available on request.

Executive Summary

Severity	Count
● CRITICAL	0
● HIGH	12
● MEDIUM	1
● ADVISORY	22
Total	35

By Category	Count
Security Holes	9
Agent Execution Scope	26

Findings

Security Holes

● [HIGH] SDS-TOKEN_LEAK-001 -- TOKEN_LEAK

Resource: test/test_report.cpp:12

Summary: Hardcoded AWS Access Key ID found outside a proper secrets store

Evidence: AWS Access Key ID: AKIAIOSFODNN7EXAMPLE

● [HIGH] SDS-TOKEN_LEAK-002 -- TOKEN_LEAK

Resource: test/test_report.cpp:13

Summary: Hardcoded AWS Access Key ID found outside a proper secrets store

Evidence: AWS Access Key ID: AKIAIOSFODNN7EXAMPLE

● [HIGH] SDS-TOKEN_LEAK-003 -- TOKEN_LEAK

Resource: test/test_report.cpp:19

Summary: Hardcoded GitHub Token found outside a proper secrets store

Evidence: GitHub Token: ghp_*****wxyz

● [HIGH] SDS-TOKEN_LEAK-004 -- TOKEN_LEAK

Resource: test/test_token_leak.cpp:25

Summary: Hardcoded AWS Access Key ID found outside a proper secrets store

Evidence: AWS Access Key ID: AKIAIOSFODNN7EXAMPLE

● [HIGH] SDS-TOKEN_LEAK-005 -- TOKEN_LEAK

Resource: test/test_token_leak.cpp:27

Summary: Hardcoded GitHub Token found outside a proper secrets store

Evidence: GitHub Token: ghp_*****yz12

● [HIGH] SDS-TOKEN_LEAK-006 -- TOKEN_LEAK

Resource: test/test_token_leak.cpp:28

Summary: Hardcoded Private Key found outside a proper secrets store

Evidence: Private Key: -----**

● [HIGH] SDS-TOKEN_LEAK-007 -- TOKEN_LEAK

Resource: test/test_token_leak.cpp:39

Summary: Hardcoded AWS Access Key ID found outside a proper secrets store

Evidence: AWS Access Key ID: AKIA SHOULD NEVER APPEAR

● [HIGH] SDS-TOKEN_LEAK-008 -- TOKEN_LEAK

Resource: test/test_token_leak.cpp:58

Summary: Hardcoded AWS Access Key ID found outside a proper secrets store

Evidence: AWS Access Key ID: AKIAIOSFODNN7EXAMPLE

● [MEDIUM] SDS-AUDIT_TAMPER-001 -- AUDIT_TAMPER

Resource: test/test_audit_tamper.cpp:25

Summary: Agent decision-log write with no hash-chaining reference nearby -- log entries aren't tamper-evident

Agent Execution Scope

Insured & Bonded

Professional Liability (E&O), General Liability, Cyber Liability. Certificate of Insurance available on request.

● **[HIGH] SDS-UNBOUNDED_LOOP-001 -- UNBOUNDED_LOOP**

Resource: test/test_prompt_injection.cpp:26

Summary: LLM API call with no max_tokens-equivalent parameter or token-budget check nearby

● **[HIGH] SDS-UNBOUNDED_LOOP-002 -- UNBOUNDED_LOOP**

Resource: test/test_prompt_injection.cpp:32

Summary: LLM API call with no max_tokens-equivalent parameter or token-budget check nearby

● **[HIGH] SDS-UNBOUNDED_LOOP-003 -- UNBOUNDED_LOOP**

Resource: test/test_unbounded_loop.cpp:23

Summary: Retry loop with no bounded retry count or backoff ceiling nearby

● **[HIGH] SDS-UNBOUNDED_LOOP-004 -- UNBOUNDED_LOOP**

Resource: test/test_unbounded_loop.cpp:51

Summary: LLM API call with no max_tokens-equivalent parameter or token-budget check nearby

● **[ADVISORY] SDS-UNGATED_STATE_CHANGE-001 -- UNGATED_STATE_CHANGE**

Resource: test/test_prompt_injection.cpp:16

Summary: State-changing call 'remove_all()' found with no policy-check or HITL-confirmation reference nearby -- review needed, not a confirmed vulnerability

● **[ADVISORY] SDS-UNGATED_STATE_CHANGE-002 -- UNGATED_STATE_CHANGE**

Resource: test/test_prompt_injection.cpp:41

Summary: State-changing call 'remove_all()' found with no policy-check or HITL-confirmation reference nearby -- review needed, not a confirmed vulnerability

● **[ADVISORY] SDS-UNGATED_STATE_CHANGE-003 -- UNGATED_STATE_CHANGE**

Resource: test/test_over_privilege.cpp:16

Summary: State-changing call 'remove_all()' found with no policy-check or HITL-confirmation reference nearby -- review needed, not a confirmed vulnerability

● **[ADVISORY] SDS-UNGATED_STATE_CHANGE-004 -- UNGATED_STATE_CHANGE**

Resource: test/test_over_privilege.cpp:61

Summary: State-changing call 'remove_all()' found with no policy-check or HITL-confirmation reference nearby -- review needed, not a confirmed vulnerability

● **[ADVISORY] SDS-UNGATED_STATE_CHANGE-005 -- UNGATED_STATE_CHANGE**

Resource: test/test_audit_tamper.cpp:16

Summary: State-changing call 'remove_all()' found with no policy-check or HITL-confirmation reference nearby -- review needed, not a confirmed vulnerability

● **[ADVISORY] SDS-UNGATED_STATE_CHANGE-006 -- UNGATED_STATE_CHANGE**

Resource: test/test_audit_tamper.cpp:34

Summary: State-changing call 'remove_all()' found with no policy-check or HITL-confirmation reference nearby -- review needed, not a confirmed vulnerability

● **[ADVISORY] SDS-UNGATED_STATE_CHANGE-007 -- UNGATED_STATE_CHANGE**

Resource: test/test_identity_isolation.cpp:17

Summary: State-changing call 'remove_all()' found with no policy-check or HITL-confirmation reference nearby -- review needed, not a confirmed vulnerability



Professional Liability (E&O), General Liability, Cyber Liability. Certificate of Insurance available on request.

- **[ADVISORY] SDS-UNGATED_STATE_CHANGE-008 -- UNGATED_STATE_CHANGE**
Resource: test/test_identity_isolation.cpp:79
Summary: State-changing call 'remove_all()' found with no policy-check or HITL-confirmation reference nearby -- review needed, not a confirmed vulnerability
- **[ADVISORY] SDS-UNGATED_STATE_CHANGE-009 -- UNGATED_STATE_CHANGE**
Resource: test/test_yaml_credentials.cpp:38
Summary: State-changing call 'remove()' found with no policy-check or HITL-confirmation reference nearby -- review needed, not a confirmed vulnerability
- **[ADVISORY] SDS-UNGATED_STATE_CHANGE-010 -- UNGATED_STATE_CHANGE**
Resource: test/test_yaml_credentials.cpp:45
Summary: State-changing call 'remove()' found with no policy-check or HITL-confirmation reference nearby -- review needed, not a confirmed vulnerability
- **[ADVISORY] SDS-UNGATED_STATE_CHANGE-011 -- UNGATED_STATE_CHANGE**
Resource: test/test_yaml_credentials.cpp:54
Summary: State-changing call 'remove()' found with no policy-check or HITL-confirmation reference nearby -- review needed, not a confirmed vulnerability
- **[ADVISORY] SDS-UNGATED_STATE_CHANGE-012 -- UNGATED_STATE_CHANGE**
Resource: test/test_yaml_credentials.cpp:74
Summary: State-changing call 'remove()' found with no policy-check or HITL-confirmation reference nearby -- review needed, not a confirmed vulnerability
- **[ADVISORY] SDS-UNGATED_STATE_CHANGE-013 -- UNGATED_STATE_CHANGE**
Resource: test/test_ungated_state_change.cpp:16
Summary: State-changing call 'remove_all()' found with no policy-check or HITL-confirmation reference nearby -- review needed, not a confirmed vulnerability
- **[ADVISORY] SDS-UNGATED_STATE_CHANGE-014 -- UNGATED_STATE_CHANGE**
Resource: test/test_ungated_state_change.cpp:29
Summary: State-changing call 'chargeCustom()' found with no policy-check or HITL-confirmation reference nearby -- review needed, not a confirmed vulnerability
- **[ADVISORY] SDS-UNGATED_STATE_CHANGE-015 -- UNGATED_STATE_CHANGE**
Resource: test/test_ungated_state_change.cpp:41
Summary: State-changing call 'deleteUser()' found with no policy-check or HITL-confirmation reference nearby -- review needed, not a confirmed vulnerability
- **[ADVISORY] SDS-UNGATED_STATE_CHANGE-016 -- UNGATED_STATE_CHANGE**
Resource: test/test_ungated_state_change.cpp:43
Summary: State-changing call 'remove()' found with no policy-check or HITL-confirmation reference nearby -- review needed, not a confirmed vulnerability
- **[ADVISORY] SDS-UNGATED_STATE_CHANGE-017 -- UNGATED_STATE_CHANGE**
Resource: test/test_ungated_state_change.cpp:53
Summary: State-changing call 'remove_all()' found with no policy-check or HITL-confirmation reference nearby -- review needed, not a confirmed vulnerability



Professional Liability (E&O), General Liability, Cyber Liability. Certificate of Insurance available on request.

● [ADVISORY] SDS-UNGATED_STATE_CHANGE-018 -- UNGATED_STATE_CHANGE

Resource: test/test_ungated_state_change.cpp:62

Summary: State-changing call 'remove(' found with no policy-check or HITL-confirmation reference nearby -- review needed, not a confirmed vulnerability

● [ADVISORY] SDS-UNGATED_STATE_CHANGE-019 -- UNGATED_STATE_CHANGE

Resource: test/test_unbounded_loop.cpp:16

Summary: State-changing call 'remove_all(' found with no policy-check or HITL-confirmation reference nearby -- review needed, not a confirmed vulnerability

● [ADVISORY] SDS-UNGATED_STATE_CHANGE-020 -- UNGATED_STATE_CHANGE

Resource: test/test_unbounded_loop.cpp:71

Summary: State-changing call 'remove_all(' found with no policy-check or HITL-confirmation reference nearby -- review needed, not a confirmed vulnerability

● [ADVISORY] SDS-UNGATED_STATE_CHANGE-021 -- UNGATED_STATE_CHANGE

Resource: test/test_token_leak.cpp:19

Summary: State-changing call 'remove_all(' found with no policy-check or HITL-confirmation reference nearby -- review needed, not a confirmed vulnerability

● [ADVISORY] SDS-UNGATED_STATE_CHANGE-022 -- UNGATED_STATE_CHANGE

Resource: test/test_token_leak.cpp:71

Summary: State-changing call 'remove_all(' found with no policy-check or HITL-confirmation reference nearby -- review needed, not a confirmed vulnerability

SAMPLE



Professional Liability (E&O), General Liability, Cyber Liability. Certificate of Insurance available on request.