

v3.4-SEC-004 – Threat Response & Automated Containment

Document Title	Threat Response & Automated Containment
Version	v3.4
Document ID	v3.4-SEC-004
Date	2025-03-22
Author	Take Back Your Data – Threat Response Unit
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the automated threat detection and response logic of MaxOneOpen. It ensures that malicious behavior, policy violations, or systemic drift are detected and neutralized in real time without exposing sensitive assets.

2. Threat Response Workflow

- Trigger → Verify → Contain → Log → Notify
- Each step is cryptographically signed
- Forks must implement full detection-to-containment path

3. Response Scenarios

Scenario	Trigger	Response	Fallback
Prompt Injection	Pattern deviation / unexpected output	Twin suspend + reroute	Fallback twin
Memory Leak	Quota overuse + undeclared storage	Immediate kill + log hash	None
Identity Spoofing	Signature mismatch	Hard stop + incident log	Blocked identity
Behavioral Drift	Anomaly detection spike	Contain + force verify	Escalation to Control

4. Containment Mechanisms

- Container isolation at runtime
- Control-triggered execution freeze
- Memory sealing and deallocation
- Notarization of final state before destroy
- Signed pulse to mesh controllers (optional)

5. Escalation Logic

- If no local resolution is possible:
 - Twin is suspended
 - Control Layer is informed with signed report

- Execution chain is paused
- No fallback may bypass containment trigger

6. Certification Relevance

All MaxOneOpen forks and deployments must demonstrate functioning, automated containment logic. Forks must document and validate each response type and escalation mechanism.