Automated Isolation of Vulnerable Workloads

Aiden Johnson | HPC-SYS, The Pennsylvania State University B.S. Computer Science;
Mentor: Thomas Mackell | HPC-SYS

The Problem

From Risk Detection to Network Containment

StackRox/RHACS identifies vulnerable workloads, but manual response is slow and inconsistent. Immediate isolation can also disrupt services before owners have time to remediate. Without automated containment, safely supporting user-provided container environments remains difficult in shared infrastructure.

Project Objective

Automated, Risk-Based Workload Isolation

Build a system that:

- Detects high-risk workloads.
- Applies configurable remediation windows.
- Generates Kubernetes NetworkPolicies.
- Supports manual and automatic isolation.
- Preserves audit and recovery information.

> "All organizations should have clear, executable cyber incident response plans and strategies…to prevent an incident from growing and causing greater harm."
> - CISA

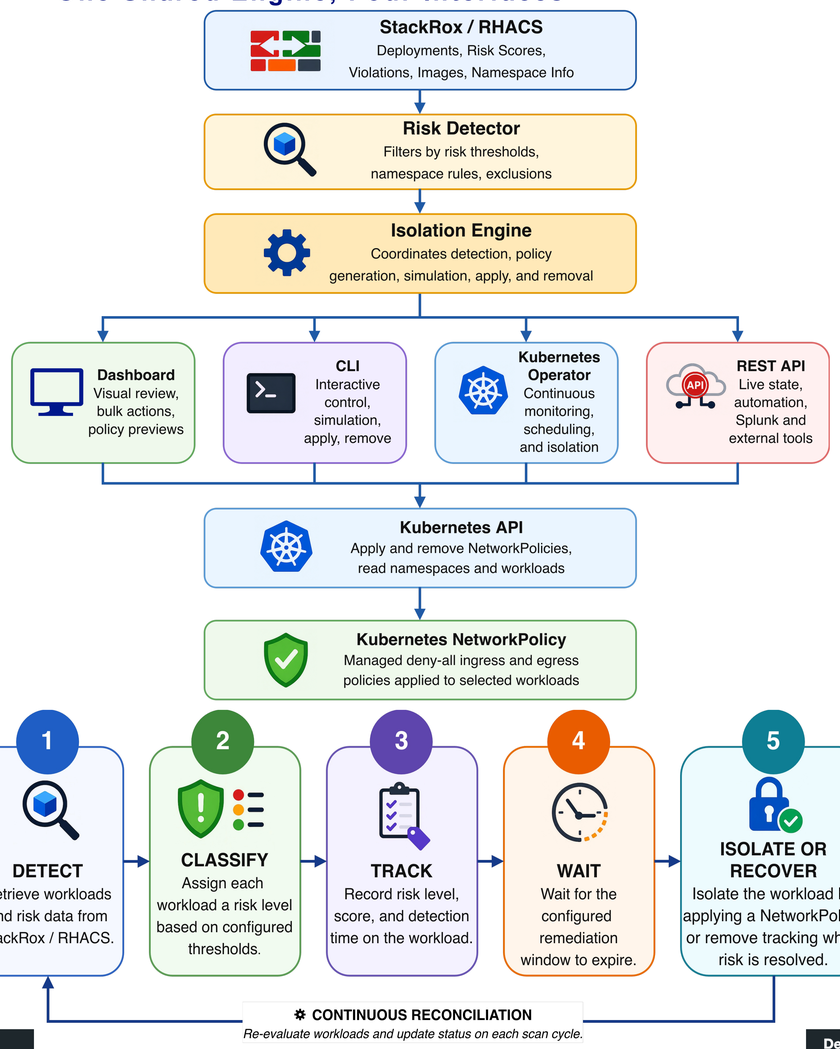
Safety and Recovery

Controlled Changes with Explicit Rollback

- Protected namespaces are excluded.
- Policies can be previewed or simulated.
- Isolation can be removed.
- Workloads can opt out of automatic re-isolation.

System Architecture

One Shared Engine, Four Interfaces



NetworkPolicy Additivity

Kubernetes NetworkPolicies are additive, so the isolation engine must account for existing allow policies:

- **Isolation labeling:** marks isolated pods without triggering a rollout.
- **Default policy updates:** uses `NotIn` selectors so baseline OpenShift policies exclude isolated pods.
- **Conflict analysis:** evaluates overlapping namespace, pod, and service-mesh policies.
- **Failure checks:** reviews host networking, pod capabilities, CNI behavior, and DNS paths.

Results

End-to-End Isolation Platform

- Connected StackRox risk data to Kubernetes containment.
- Added manual and automated isolation workflows.
- Preserved workload state with labels and annotations.
- Integrated dashboard, CLI, operator, API, and Splunk.

Future Work

Expanding Scale, Policy Options, and Analytics

- Event-driven detection.
- Multi-cluster support.
- Owner notifications.
- Configurable isolation levels.
- Risk-trend analysis.

Conclusion

A Repeatable Path from Detection to Containment

The system converts StackRox/RHACS findings into controlled Kubernetes actions. High-risk workloads are detected, tracked, given time to remediate, and isolated when necessary while preserving safeguards, auditability, and recovery paths. Together, these capabilities provide a safer path toward supporting user-provided container environments in shared infrastructure.

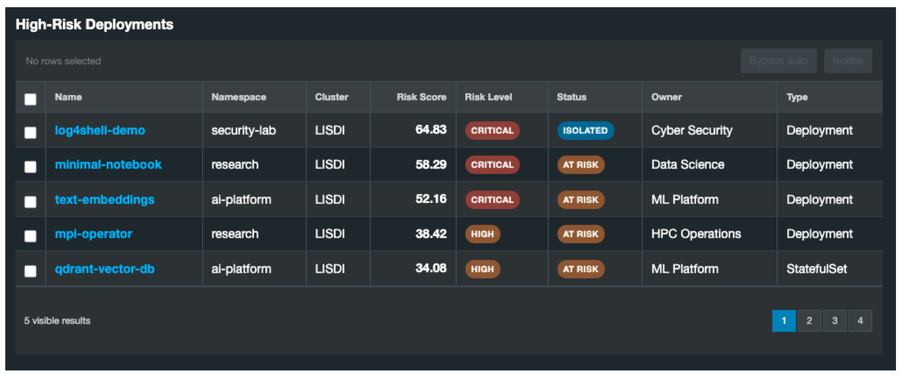


Figure 1. High-risk workload overview in the Splunk dashboard.

Higher Risk, Shorter Remediation Window

Risk level	Score	Default wait
Critical	Greater than 40	15 days
High	30–40	21 days
Medium	10–30	45 days

Standard Kubernetes NetworkPolicies

The system creates workload-specific policies that deny both ingress and egress traffic to matching pods.

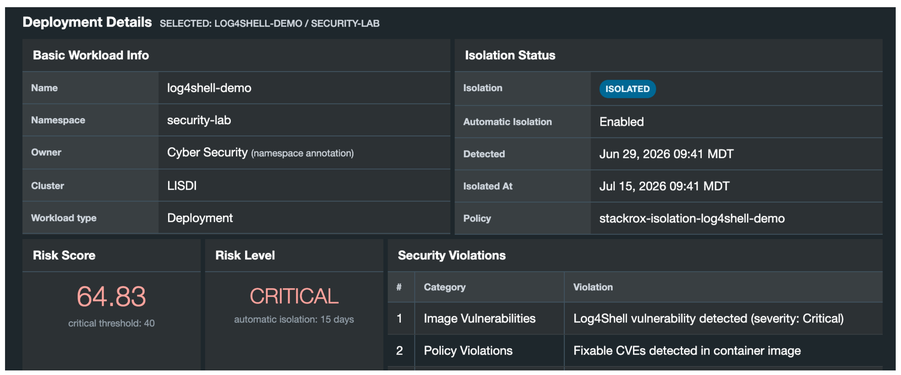


Figure 2. Selected workload details in the Splunk dashboard.

Managed by Triad National Security, LLC, for the U.S. Department of Energy's NNSA.
LA-UR-26-26606