Threat intelligence

Run curated threat intelligence without an internet connection

Rhombus runs a Malware Information Sharing Platform (MISP) fed from verified offline feed mirrors. Indicators flow to the network sensors and malware triage engine, and the kit's verdicts flow back.

01 · WHY IT MATTERS

- A platform that pulls from the internet stops working when the link drops.
- Intelligence helps only when it reaches the tools watching traffic and files.
- Stale indicators cause false alarms, so each needs a source, a handling marking and an age limit.

02 · HOW IT WORKS ON RHOMBUS

- MISP runs in containers with kit account sign-in. Its guest is hardened to the Defense Information Systems Agency Security Technical Implementation Guide (DISA STIG), in Federal Information Processing Standards (FIPS) mode.
- Feed mirrors are checked against published digests; content that fails is quarantined, never imported.
- Every hour, published detection indicators become Suricata rules and Zeek intel. A canary indicator proves the path.
- Rhombus reconnects MISP integrations after each rebuild, and kit validation checks feed freshness.

FIG · 01 FROM DEPLOYMENT TO RESULTS

01	02	03	04
Deploy the network forensics mission package from the console.	Sign in to MISP and review the loaded feeds.	Run kit validation to confirm feed freshness and the sensor export.	Hunt with the indicators; apply signed bundles to refresh feeds.

03 · DEFENSE & GOVERNMENT

- Defensive cyber operations (DCO) teams turn published indicators into sensor detections on a mission network.
- Hunt-forward teams keep their own malware verdicts as indicators, shared only within the organization.
- Training cohorts pivot from a sample hash to its MISP event during triage labs.

04 · COMMERCIAL & ENTERPRISE

- Banks can run isolated intelligence for segregated networks from vetted feeds.
- Incident response teams can carry a self-contained intelligence platform into a compromised environment.
- Critical infrastructure and operational technology (OT) sites can correlate traffic without an outbound connection.

05 · OUTCOMES

- Detection indicators reach Suricata and Zeek, and a canary indicator confirms the path.
- Security Onion can report indicators that fired back to MISP as sightings.
- Tampered feed files are quarantined on every refresh, and stale feeds fail kit validation.

06 · CONSIDERATIONS

- Each feed keeps its source's terms; restrictive feeds are off by default, and customer-keyed feeds need a connected kit.
- An air-gapped kit is as fresh as its last sustainment bundle. Rebuilding MISP discards its events, and factory reset skips MISP unless an operator includes it.
- Assemblyline sharing is included. Spectra Analyze and MixMode exchanges are optional and licensed separately.

INTEGRATED TOOLS

MISP · CISA KEV · CISA joint advisories · CIRCL OSINT · Offline feed mirrors · STIX import

Commercial products licensed separately · Trademarks of their owners; no endorsement implied