MISSION FIRST CYBER · RHOMBUS

A datacenter. In a kit.

Mission-Ready, Portable, Air-Gapped Operations — Anywhere, Anytime.

Rhombus is a software-defined, infrastructure-as-code cyber operations platform: DFIR, threat hunting, deception, training, and the network underneath, on a single field- deployable kit. **Built once, deployed identically, runs fully disconnected.**



01 Software-Defined
Environment is code. Versioned, inspectable, auditable.

02 Hardware-Agnostic
NoSKUlock. Deployonthe hardware the mission requires.

03 Full-Spectrum
DFIR, hunt, deception, training, networking. One kit.

04 Offline-Native
Local mirrors. Pre-staged intel. Nothing phones home.

THE PROBLEM
The hardest networks to defend are the ones the SOC can't see: forward sites, air-gapped enclaves, OT environments.

THE APPROACH
Define the entire environment as code (image, provisioning, configuration) so the deployed kit is the tested kit.

THE OUTCOME
One platform. Many missions. Reproducible by construction: an accreditation and evidentiary asset, not a liability.

The hardware-first kit sells you a box.
Rhombus delivers the capability, as code, on any box.

HARDWARE

Configured to the **ceiling.**

Tuned to the mission. Rhombus is hardware-agnostic; the platform runs on the configuration the program selects.

CPU	Up to 128 Cores	256 Threads
MEMORY	Up to 2 TB	DDR5 ECC
STORAGE	Up to 1 PB	NVMe
GPU	Optional	AI / Accel
NETWORK	2× 10 GbE 4× 10/25 GbE	Copper · Onboard SFP+

CAPABILITY

One kit. **Any mission.**

Each capability ships pre-integrated, defined as code, on the same offline foundation. The brief for each: a separate whitepaper.

01 · DFIR

Forensics Without a Connection.

A full digital and mobile forensics practice: evidence acquisition, disk and mobile triage, malware analysis, defined as code and deployed disconnected. Malware stays isolated from evidence by architecture.

02 · HUNT

Hunting Without a Lifeline.

Signature-free behavioral detection paired with air-gapped malware classification. Surface the novel and the low-and-slow, then render a verdict on the unknown, locally, with no cloud submission.

03 · DECEPT

The Ground You Choose.

Active cyber deception at the edge. Decoys, lures, breadcrumbs, and AI-driven personas on an isolated segment. Any interaction is a high-fidelity signal, near-zero false positives by design.

04 · RANGE

Train the Way You Fight.

A full cyber range in the kit. Instrumented, repeatable scenarios deploy by the dozen: same platform, same tools, same architecture the team operates with for real. Reset in minutes.

05 · NETWORK

The Network Is Part of the Kit.

Enterprise-grade load balancing, WAF, DDoS protection, and application delivery, provisioned as code on the kit's own foundation. Routing and segmentation declared, not drawn.

06 · CORE

Datacenter in a Box.

Identity, DNS, DHCP, time, single sign-on, collaboration, and monitoring: the foundation every mission stack depends on. One command brings up the base; everything else enrolls into it.

Schedule a briefing: see Rhombus stand up a full mission stack, disconnected, in hours.

REQUEST A DEMO TODAY