Network security monitoring

Watch the mission network from day one, fully disconnected

Rhombus deploys a network security monitoring stack from the console: Security Onion with Zeek, Suricata and full packet capture (PCAP), plus optional commercial sensors. Installers and rule content come from the kit, so monitoring needs no internet connection.

01 · WHY IT MATTERS

- Defenders on a forward network need evidence on day one, not after an integration project.
- Protocol logs, signature alerts and packets from one feed take an analyst from alert to evidence.
- A disconnected site needs updated content and a sensor it can rebuild to a known-good baseline.

02 · HOW IT WORKS ON RHOMBUS

- Security Onion runs Zeek, Suricata and packet capture on traffic from a switch mirror (SPAN) port or network tap (TAP).
- Optional MixMode sensors watch the same feed, and a dashboard shows each receiving it.
- The console deploys the sensors as a mission package and sizes capture retention.
- Signed update bundles refresh the kit's offline mirror. Factory reset can rebuild Security Onion and MixMode to their delivered baseline.

FIG · 01 FROM DEPLOYMENT TO RESULTS

01	02	03	04
Connect the monitored network's SPAN or TAP to the kit.	Deploy the network forensics mission package from the console.	Run kit validation to confirm the sensors are healthy.	Hunt in Security Onion and route high-severity alerts to team chat.

03 · DEFENSE & GOVERNMENT

- Defensive cyber operations (DCO) teams baselining an unfamiliar network on arrival.
- Hunt-forward and incident response missions that need packet-level evidence offline.
- Training ranges that score emulated attacks against the detections they trigger.

04 · COMMERCIAL & ENTERPRISE

- Banks and financial services needing a self-contained kit for branch or data-center incident response.
- Critical infrastructure and operational technology (OT) sites where monitoring must stay passive and on premises.
- Managed security service providers (MSSPs) bringing a repeatable sensor stack to each engagement.

05 · OUTCOMES

- Zeek logs, Suricata alerts and captured packets are searchable in Security Onion.
- High-severity detections can be posted to team chat, each linked back to the hunt view.
- Kit validation produces a sensor health report to export and file.

06 · CONSIDERATIONS

- MixMode is optional and licensed separately. Its image is hardened to the Defense Information Systems Agency Security Technical Implementation Guide (DISA STIG), in Federal Information Processing Standards (FIPS) mode.
- Security Onion installs from its vendor appliance image. Rebuilding it discards captured data, so export evidence first.
- Sensors see only what the SPAN or TAP delivers. Encrypted sessions yield metadata and behavior, not payload.

INTEGRATED TOOLS

Security Onion | Zeek | Suricata | Full PCAP | MixMode COMMERCIAL

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