SIEM & analytics

Search, correlate and hunt across sensor data, entirely offline

Rhombus deploys the security information and event management (SIEM) platform your analysts prefer: Elastic in Security Onion, SOF-ELK, Malcolm or Splunk Enterprise. Search and dashboards work fully offline.

01 · WHY IT MATTERS

- Alerts matter only when an analyst can search the history behind them.
- Teams work faster on the analysis platform they were trained on.
- Evidence from a sensitive network should be analyzed where it was collected.

02 · HOW IT WORKS ON RHOMBUS

- Security Onion keeps its Zeek and Suricata data in Elasticsearch, searchable in Kibana.
- A clustered Elastic stack, SOF-ELK or Malcolm deploy from the console catalog, chosen to match the team's workflow.
- With the clustered Elastic stack, MixMode data gets prebuilt triage and hunting dashboards.
- The clustered Elastic stack, SOF-ELK and Malcolm run on images hardened to the DISA STIG (Security Technical Implementation Guide) in FIPS mode, scanned after each build.
- Splunk Enterprise can also run on the kit, licensed separately and configured before delivery by our Splunk Core Certified Consultants.

FIG · 01 FROM DEPLOYMENT TO RESULTS

01	02	03	04
Deploy the sensors and your chosen analytics platform; Splunk Enterprise arrives configured.	Run kit validation and review each platform's STIG scan.	Open the triage dashboards and hunt from alert to session.	Upload packet capture (PCAP) files to Malcolm for session-level review.

03 · DEFENSE & GOVERNMENT

- Defensive cyber operations (DCO) teams correlating network alerts during a mission.
- Incident response and hunt-forward teams reviewing captured PCAP on site.
- Analyst training on the same platforms used in the field.

04 · COMMERCIAL & ENTERPRISE

- Enterprise incident response teams that need an isolated analysis environment for a breach.
- Banks and financial services keeping investigation data inside a controlled enclave.
- Managed security service providers (MSSPs) standing up per-engagement analytics.

05 · OUTCOMES

- Network alerts, protocol logs and anomalies share one searchable history.
- MixMode data in one Kibana, on kits with the clustered Elastic stack.
- The clustered Elastic stack, SOF-ELK and Malcolm each get a STIG scan score after every build.

06 · CONSIDERATIONS

- Security Onion covers most kits; a clustered Elastic stack adds scale for larger retention or data volume.
- Elastic runs free or paid. We recommend paid for single sign-on, advanced alerting and AI features on the kit's GPU and local models.
- Malcolm reviews uploaded packet captures; live capture can be enabled when the mission needs it.

INTEGRATED TOOLS

Elastic · SOF-ELK · Malcolm · Splunk Enterprise COMMERCIAL

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