CARVER Live - Use Case Scenarios and Integration Guide

A practical guide for applying the CARVER target analysis and vulnerability assessment method with PESTELS and a 5x5 risk matrix across Cybersecurity, Humanitarian Aid, and Socioeconomic and Geopolitical assessments. This guide includes suggested indicators and data sources, scoring tips, and live monitoring patterns that align with the CARVER Live app.

Table of contents

---

1) Purpose and audience

This guide helps assessors, supervisors, and CSOs operationalize CARVER with PESTELS and a 5x5 matrix. It focuses on repeatable scoring, indicator alignment, and supervision oversight so assessments are consistent, auditable, and easy to brief.

2) Common workflow pattern

1. Establish context with PESTELS - define scope, constraints, and assumptions.
2. Build a DBT - describe realistic adversary capabilities and intent for the mission area.
3. Register assets - physical, digital, or programmatic units to be scored.
4. Score CARVER - use a 1 to 5 or 1 to 10 scale. High means worse. For Recuperability, high means low resilience per the standard used in the app.
5. Compute Pa, Likelihood, and Impact - Pa is the normalized CARVER sum. Likelihood is the average of A, V, Rz. Impact is the average of C, E, R.
6. Place on the 5x5 matrix - visualize concentration of risk and identify clusters.
7. Prioritize - sort by Pa, Total, or L×I and select top actions.
8. Mitigate and re-score - record controls, re-score, and verify risk reduction.
9. Monitor - connect a data feed that pushes relevant indicators and incidents.

3) Data sources and indicators

Use authoritative, regularly updated sources. Below are common categories and examples. Select a small, stable basket per project and document how each indicator influences a CARVER factor.

- Conflict and insecurity: ACLED, Insecurity Insight incident feeds, Armed Conflict datasets by region.
- Governance and fragility: V-Dem, Fragile States Index, World Governance Indicators, Freedom House, Bertelsmann Transformation Index.
- Humanitarian context: ReliefWeb, OCHA products, INFORM Severity Index, IOM DTM, WHO and UNICEF sector reports.
- Socioeconomic and macro: World Bank and IMF open data, HDI and GINI, trade and inflation series.
- Cybersecurity: CISA advisories and KEV catalog, MS-ISAC alerts, NVD CVE database, vendor advisories, MITRE ATT&CK knowledge base.
- Crime and trafficking: national police bulletins, UNODC reporting, port and customs notices.
- Infrastructure and environment: OpenStreetMap, USGS or national equivalents, EIA energy stats, meteorological services.

Document the exact dataset names, date ranges, and update cadence in your project folder or README for transparency.

4) Use case A - Cybersecurity

Objective: Prioritize digital and cyber-physical assets for hardening across enterprise IT and OT.

Typical assets: Identity provider, payment gateway, public web portal, SOC tooling, SCADA control server, PLC network segment, remote substation firewall, backup and recovery environment, SaaS tenant, executive devices.

Threat modeling inputs:

- DBT elements: likely actors, intent, capability, dwell time, targeting patterns.
- TTP references: MITRE ATT&CK tactics and techniques relevant to your environment.
- Vulnerability landscape: NVD CVEs affecting your stack, CISA KEV items, vendor advisories.

Scoring guidance:

- C - Criticality: map to business service tiers or safety impact for OT.
- A - Accessibility: external exposure, misconfigurations, remote access, supply chain connectivity.
- R - Recuperability: tested recovery time objectives, backup integrity, cyber insurance support. High score means slow or hard to recover.
- V - Vulnerability: patch latency, compensating controls, exploit maturity.
- E - Effect: scope of outage or safety impact for OT.
- Rz - Recognizability: public DNS footprint, OSINT, predictable naming, exposed banners.

Monitoring signals for the feed:

- New CVEs for key products, KEV additions, vendor critical advisories.

- IDS or EDR alerts that match DBT patterns.
- Failed backup verification or DR test failures.
- BGP, DNS, or WAF anomalies tied to public assets.

Example JSON signal:

```
{
  "type": "cve",
  "product": "VendorX Gateway 3.2",
  "cvss": 9.8,
  "kev": true,
  "note": "Public exploit released. Expedite patch on exposed gateways."
}
```

Action pattern:

1. Sort by Pa to find the most attractive digital targets.
2. Cross-check 5x5 placements. Items at L 4 to 5 and I 4 to 5 get top priority.
3. Apply mitigations and re-score. Track recovery improvements in R and see Impact drop.

5) Use case B - Humanitarian Aid Operations

Objective: Protect aid workers, beneficiaries, and critical aid flows while preserving access and neutrality.

Typical assets: Field offices, mobile clinics, cold chain hubs, warehouses, convoy routes and choke points, bridges, river crossings, distribution points, telecom nodes, coordination centers.

Threat modeling inputs:

- DBT elements: criminal groups, opportunistic theft, extortion, checkpoints, UXO or IED contamination, civil unrest.
- Context: ACLED event density near routes, OCHA access constraints, IOM DTM displacement flows, weather and seasonal hazards.

Scoring guidance:

- C - Criticality: lives saved, essential program outputs, cold chain viability.
- A - Accessibility: route complexity, curfew windows, checkpoint frequency.
- R - Recuperability: availability of alternate routes, mobile storage, surge staffing. High score means poor resilience.
- V - Vulnerability: perimeter conditions, lighting, locks, escorts, convoy SOPs.
- E - Effect: interruption of distributions, disease risk, reputational harm, community tensions.
- Rz - Recognizability: predictable schedules, branded vehicles, open posting of delivery times.

Monitoring signals for the feed:

- New incidents along planned routes or near sites.
- Flood or storm warnings affecting river crossings or bridges.
- Access negotiation updates from coordination bodies.
- Fuel and commodity price spikes that change threat incentives.

Example JSON signal:

```
{
  "type": "access",
  "route": "Corridor B",
  "status": "restricted",
  "source": "cluster-update",
  "note": "Two new checkpoints and a curfew extension add 90 minutes to
transit."
}
```

Action pattern:

1. Rank assets by L×I to surface near-term operational risk to life-saving activities.
2. Use CARVER details to craft targeted mitigations like schedule randomization, community liaison meetings, and alternate route staging.
3. Re-score after each change and show risk reduction to leadership and donors.

6) Use case C - Socioeconomic and Geopolitical Assessments

Objective: Support strategic planning and early warning for public policy, private investment, and civil society operations.

Typical assets: Border crossings, ports and free trade zones, major mines, energy nodes, food import terminals, critical highways and rail, sovereign functions like revenue collection IT, electoral logistics hubs, strategic programs and reforms.

Threat modeling inputs:

- DBT elements: political violence actors, protest organizers, cyber activists, illicit networks, external spoilers.
- Context: V-Dem governance shifts, FSI or INFORM changes, macro indicators like inflation and FX reserves, conflict proximity and trends.

Scoring guidance:

- C - Criticality: national or regional systemic importance, cross-border effects.
- A - Accessibility: public proximity, protest feasibility, labor actions, corruption gates.

- R - Recuperability: fiscal buffers, redundancy of corridors, emergency powers, reserve capacity. High score means slow or costly recovery.
- V - Vulnerability: bottleneck design, chokepoints, outdated systems, weak controls.
- E - Effect: cascading economic losses, social unrest, diplomatic fallout.
- Rz - Recognizability: symbolic value, media attention, ease of mobilization around the site.

Monitoring signals for the feed:

- Rapid changes in commodity prices or exchange rates.
- Protest calls or permits, union strike ballots, border advisories.
- Surge in incidents near strategic nodes, cross-border spillovers.

Action pattern:

1. Use PESTELS to frame scenario drivers then score CARVER for key nodes.
2. Map assets to provinces or corridors and visualize matrix concentrations by region.
3. Prepare contingency plans for high L×I nodes and track R changes as resilience projects land.

7) Mapping PESTELS context to CARVER factors

Use PESTELS to explain why a factor is trending. Example influences:

- Political: coup risk lifts E and R; protest cycles raise A and Rz at symbolic sites.
- Economic: inflation and fuel shortages raise V for convoy hijacking and raise E if supply chains are fragile.
- Social: intergroup tensions raise E and Rz at visible aid points; trust-building can reduce A.
- Technological: patch velocity and legacy systems affect V and R in cyber and ICS.
- Environmental: flood season raises A on certain approaches and raises R where detours are scarce.
- Legal: new regulations can reduce A and V if enforced; weak enforcement can raise both.
- Security: rising incident density or IED contamination raises A and E, lowers R where alternate routes are few.

State the causal link in notes next to each score so audits and handovers are simple.

8) Indicator to CARVER mapping reference

Map each indicator to one or more CARVER factors with a simple rule and a weight. Examples:

- ACLED weekly incidents within 10 km of an asset - raises A by +1 step when above the 80th percentile of past 12 weeks.
- CISA KEV entry matching your product - raises V by +1 until patched and verified.
- OCHA access constraint update for a corridor - raises A by +1 and R by +1 where no detour exists.
- V-Dem drop in rule of law percentile by 10 points year over year - raises E by +1 for assets needing judicial enforcement.
- FX reserve coverage below 2 months of imports - raises R by +1 for import dependent nodes.

Keep rules transparent and consistent. Revisit weights during after action reviews.

9) Live monitoring - JSON feed schemas

Use simple, typed events so the app can display them consistently. Suggested baseline schema:

```
{
  "updated": "2025-08-12T00:00:00Z",
  "signals": [
    {
      "type": "incident|intel|cve|access|weather|economic",
      "assetId": "optional-id",
      "severity": 1,
      "summary": "short text",
      "source": "string",
      "url": "optional-link"
    }
  ]
}
```

You can also store rolling indicator snapshots:

```
{
  "updated": "2025-08-12T00:00:00Z",
  "indicators": {
    "acled_proximity_high": ["Asset-12","Asset-44"],
    "kev_products": ["VendorX Gateway 3.2"],
    "fx_reserve_months": 1.8
  }
}
```

10) Risk tiers, reporting, and oversight

- Pa tiers example: 0.00 to 0.25 Low, 0.26 to 0.50 Moderate, 0.51 to 0.75 High, 0.76 to 1.00 Extreme.
- 5x5 interpretation: L 4 to 5 and I 4 to 5 are priority one. Combine with Pa where tie breaking is needed.
- Reporting cadence: weekly for active programs, monthly for strategic dashboards. Always re-score after material changes.
- Oversight: keep a short audit trail in the Notes field that cites which indicator moved which factor and why.

11) Ethical, legal, and safety notes

- Do No Harm and impartiality in humanitarian contexts.
- Respect legal constraints on data collection and privacy. Avoid collecting personally identifiable information unless required and authorized.

- For cyber, do not probe or scan systems without authorization. Use public advisories and internal telemetry that you are permitted to access.
- Treat sensitive feeds as confidential and secure them appropriately. Use private repos or endpoints for restricted data.

Tip: Start small. Pick 5 to 10 high value assets, define 5 to 8 indicator rules, and iterate. The goal is a stable, explainable system that supervisors and boards can trust.