SmokeMont Methodology

A lightweight operator workflow for authorized planning, validation, observation, and evidence collection.

PLAN | VALIDATE | OBSERVE | COLLECT

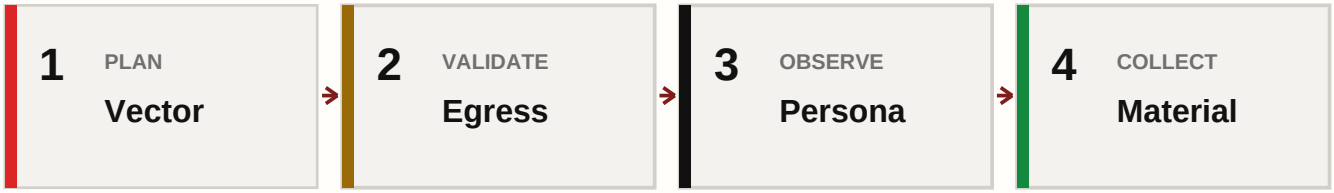
Whitepaper | Authorized security operations | 2026

WHITEPAPER

SmokeMont Methodology

SmokeMont Methodology is a lightweight operator workflow for authorized security work. It ties together planning, validation, observation, and evidence collection so that field activity can be scoped, reviewed, exported, and explained without installing agents or changing host configuration.

The methodology is intentionally practical. It is designed for red teams, blue teams, purple teams, incident responders, consultants, and security operations groups that need a repeatable way to document what was authorized, what was tested, what was observed, and what evidence was produced.



The loop is simple: plan with Vector, validate with Egress, observe with Persona, collect with Material, then feed lessons back into the next plan.

Why This Exists

- Operators need fast tools, but leadership and defenders need clear context.
- Validation without planning can create ambiguity about authority and scope.
- Observation without reporting can become anecdotal.
- Collection without boundaries can become invasive or operationally risky.
- SmokeMont connects these activities into one evidence-oriented workflow.

OPERATING MODEL

Four Phases

1. Plan

Vector

Define authorization, scope, assumptions, validation steps, detection hypotheses, risks, stop conditions, communication path, and readiness before activity begins.

2. Validate

Egress

Run approved benign outbound checks from a Windows endpoint to document which network paths work, fail, or require review.

3. Observe

Persona

Review how an endpoint appears through local posture, network identity, public egress context, and profile-fit reporting.

4. Collect

Material

Gather read-only incident-response material from Windows or macOS endpoints when authorized triage requires local evidence.

Feedback Loop

The fourth phase does not end the workflow. Reports, gaps, unresolved risks, and lessons learned should feed into the next Vector runbook. SmokeMont treats each engagement as an input into better scope, better controls, and better evidence handling.

CONTROL SURFACE

Operating Principles

SmokeMont tools are small by design, but the methodology is broader than the binaries. It defines how the tools should be used, what context should surround them, and what evidence should come out of the work.

Principle	Expectation
Authorization first	Every activity maps to scope, approver, window, stop contact, and communication channel.
Explicit operator action	Tools run only when an operator starts them. No hidden background workflow is assumed.
Conservative execution	Collect or validate only what is needed for the task and avoid unnecessary host impact.
Evidence-driven output	Reports preserve context, timestamps, selected mode, results, and interpretation.
Clear boundaries	Planning and observation are distinguished from remediation, bypass, or host change.

Governance Questions

1. What is authorized, and by whom?
2. Which systems, accounts, networks, and time windows are in scope?
3. What signals should defenders or operators expect to see?
4. What conditions require the operator to pause or stop?
5. Who receives the technical evidence and the executive summary?

TOOL MAPPING

Where Each App Fits

Vector - Planning And Readiness

Vector captures authorization context, runbook details, assumptions, validation steps, detection hypotheses, risk owners, stop conditions, notes, and readiness state. It is the first step because it makes the planned activity reviewable before anything happens.

Egress - Path Validation

Egress validates approved outbound paths using controlled benign checks. It helps answer whether DNS, HTTPS, WebSocket, UDP/443, HTTP/2, HTTP/3-style UDP/443, or SSH-over-443 paths behave as expected from the endpoint.

Persona - Endpoint Appearance

Persona helps operators understand how a system appears from local configuration, public egress identity, and profile-fit context. It does not spoof or mutate identity; it creates a shared evidence trail about appearance and posture.

Material - Read-Only Triage

Material gathers local incident-response material from Windows or macOS endpoints when triage is authorized. It does not remediate, quarantine, terminate processes, delete files, or modify host configuration.

ADOPTION

Recommended Rollout

Teams can adopt the methodology without changing their full operating model. Start with one authorized use case and make the evidence chain explicit.

1. Create a Vector runbook for one approved exercise or response workflow.
2. Name the approver, window, stop contact, communication channel, and expected signals.
3. Use Egress only when the runbook calls for outbound path validation.
4. Use Persona only when the runbook calls for endpoint appearance review.
5. Use Material only when authorized response or triage requires local read-only evidence.
6. Export reports and attach them to the engagement, ticket, or case record.
7. Convert gaps and lessons learned into the next Vector plan.

Success Criteria

- The operator can explain the purpose of each tool run.
- The report identifies scope, timing, context, and output.
- Stop conditions are visible before activity begins.
- Defenders know what signals should be observed.
- Leadership can separate authorized observations from recommendations.

BOUNDARIES

Safety And Publication Notes

The SmokeMont Methodology is intended for authorized security operations only. It does not grant permission to test systems, bypass controls, collect data, or perform response actions. Operators remain responsible for written authorization, scope control, privacy boundaries, and local policy.

What The Methodology Does

- Provides a shared language for planning, validation, observation, and evidence collection.
- Encourages explicit authorization and stop conditions.
- Promotes exportable reporting and repeatable review.
- Keeps tool activity tied to operator intent and documented scope.

What The Methodology Does Not Do

- It does not replace legal, compliance, or engagement authorization.
- It does not authorize offensive activity by itself.
- It does not require agents, persistence, or background service installation.
- It does not require remediation or host configuration changes.

SmokeMont creates native tools for authorized operators. The methodology helps teams use those tools with context, restraint, and a reviewable evidence trail.