Continuous Guidance and Validation

A Smarter Workflow: Guide First, Then Validate.

🏁 Start Here: Proactive Guidance

Workflow:

Research → Guide → Implement

Keywords:

- ✓ Before Coding
- ✓ Building Context
- ✓ High First-Time Accuracy

✅ Finish Strong: Reactive Validation

Workflow:

... → Validate Once

Keywords:

- ✓ Final Check
- ✓ Catching Edge Cases

Layered Security Workflow

LAYER 1: ESSENTIAL PATTERNS (Proactive)
⚡ Instant awareness • 0 tokens • Always-on

▼

LAYER 2: SEMANTIC RESEARCH (Proactive)
🔍 Deep understanding • ~20k tokens • ~2 min

▼

LAYER 3: DOMAIN SPECIALISTS (Guidance & Validation)
👥 Expert guidance & validation • ~250k tokens • ~3 min

▼

LAYER 4: COMPREHENSIVE ANALYSIS (Reactive)
🎯 Final validation • ~200k tokens • ~4-5 min

📊 Decision Points

The LLM makes the optimal choice based on the task.

Simple Fix:	`L1 Only`
New Feature:	`L1 + L2 + L3`
Security Review:	`L1 + L3 or L4`
Critical System:	`All Layers`
Learning:	`L2 Primary`

The Validation Spectrum

Validation isn't one-size-fits-all. Match the tool to the task.

Targeted Validation

Use a **specialist agent** to check a specific piece of code against its domain rules. Fast, focused, and precise.

Use Case: "Is this new authentication function secure?"

Comprehensive Validation

Use the **comprehensive agent** to audit an entire feature or application against all security rules. Catches cross-domain issues.

Use Case: "Is our user profile system secure end-to-end?"

The Proactive Advantage

Shifting left on security delivers measurable results.

Higher Accuracy

Get it right the first time by building with full security context from the start.

Nearly 2x Faster

Eliminate rework and repetitive validation cycles. Ship secure features faster.

Token Savings

Proactive guidance is more efficient than repeated, expensive validation calls.

Better Coverage

Address security at a conceptual level, catching entire classes of vulnerabilities.

The Accelerator

Speed up both security guidance and validation.

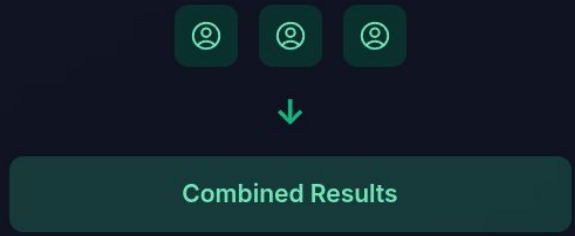
Sequential

Agents run one after another, creating a bottleneck.

7+ Minutes

Parallel

Multiple agents work simultaneously for maximum efficiency.



~3 Minutes

The Optimal Workflow

Connecting tools and process for proactive security.

1. RESEARCH

Semantic Search on OWASP/ASVS Corpus

2. IDENTIFY

Define Affected Security Domains

3. GUIDE

Use Specialist Claude Agents

4. IMPLEMENT

With Always-On CLAUDE.md Patterns

5. VALIDATE

Verify with Specialist Agents

6. TEST

Confirm with Security Test Scripts

7. DOCUMENT

Record Decisions & Compliance