Zeek - Support Operations Specialist - November 19, 2025

→ See Cover Letter Portfolio Website

My Core Mission

> **I'm excited about the Support Operations Specialist position because it directly addresses what drives me every day: eliminating friction that slows people down and building systems that lift everyone up.**

The best solutions come from people who experience the problems daily. As someone who's been in the support trenches for 6 years, I understand our pain points. But I also believe in collaborative problem-solving and sharing tools, teaching others, and building together.

I'm not trying to revolutionize everything overnight. I want to contribute steady, thoughtful improvements that make everyone's job easier, while learning from and supporting the excellent work the Support Ops Team has already established.

My Framework for Innovation:

1. **Identify the gap** - Spot where current systems fall short
2. **Prototype solutions** - Build working models, not theories
3. **Test thoroughly** - Validate with real scenarios before rollout
4. **Share for feedback** - Collaborate with leadership and team members
5. **Document everything** - Ensure knowledge transfers and scales

The result:

Systems that don't just solve today's problems, they prevent tomorrow's headaches.

For five years, I've been building these solutions between support tickets, staying late to refine automations, and training teammates when possible. This role would let me channel that energy into focused impact.

I'm drawn to three aspects:

- **Building at scale:** Moving from ad-hoc solutions to systematic infrastructure that serves our entire team.
- **Collaborative growth:** Learning from Zach's expertise while contributing my unique perspective.
- **Teaching as a multiplier:** Turning individual wins into team-wide capabilities through structured training and documentation.

Thank you for considering my application. I'm excited about the possibility of turning my passion for problem-solving into focused value for our entire team.

Best,
Zeek

Technical Training Examples

Spanish Support System Implementation

The Challenge: Zero Spanish support capacity with growing Spanish-speaking customer base

Solution: Built comprehensive AI-powered Spanish support system including custom GPT with terminology guardrails, complete process documentation, and live team training workflows.

Result: 100% team adoption, full Spanish support coverage without additional hiring

→ View complete Spanish Support AI System implementation

AI Productivity Systems for Support Team:

- → ChatGPT Productivity Training
- → Bug Report Automation GPT
- → Planning Center Support Chatbot
- → Video-to-Documentation Workflow

Calendar Specialist Training Portfolio

Comprehensive Training Program:

- → Training Sessions Archive
- → Custom Report Builder Training
- → AI Custom Report Builder Project

Result: Enabled team to handle "technically impossible" customer requests

Process Automation Opportunity

Identified Process: Bug Report Submission

Current Problem: Agents must leave Front, find the Asana form link in Notion, fill it out in a separate tab, then return to Front. The team reports feeling "slower" and frustrated by "multiple steps across multiple products."

Proposed Solution: Integrate a Front macro that collects bug report data and automatically creates Asana tasks via n8n webhook integration.

How It Works:

1. Agent clicks "Report Bug" macro in Front
2. Fills out form (bug summary, steps, links) without leaving Front
3. n8n webhook receives data and creates Asana task
4. Agent sees confirmation and continues helping customer

Trust & Safety LLM Prompt Engineering

Planning Center Trust & Safety Classifier — Three-Phase System

Why This Was Built in Three Phases

Running Trust & Safety analysis on every incoming ticket demands a design that balances speed, cost, and accuracy without overwhelming the LLM or generating false alarms. Splitting the classifier into three passes gives us the best trade-offs.

Speed: Most tickets are harmless. Phase 1 lets the model make a fast, cheap judgment about whether the message *might* be Trust & Safety–related. Only the small fraction of suspicious tickets move on to deeper analysis.

Cost Control: LLM usage scales with tokens. Instead of running a heavy, context-rich classifier on every message, the system uses:

- **Phase 1:** ultra-light, ultra-cheap pre-scan
- **Phase 2:** deeper Planning Center specific classification only for tickets flagged by Phase 1
- **Phase 3:** small, structured output to pass to automations or risk workflows

This architecture keeps your monthly LLM bill predictable.

Redundancy & Accuracy: Security work benefits from redundancy. Two independent classification checkpoints dramatically reduce:

- false positives (mislabeling normal support as T&S)
- false negatives (missing impersonation, data exposure, or scam attempts)

The model must say "YES" twice before a ticket is flagged as Trust & Safety. This protects both the team and the customer experience.

LLM Model: Haiku 4.5

- Haiku is engineered for high-volume classification, delivering extremely low latency and very low per-token cost, ideal for running on *every incoming ticket*.
- Claude models, including Haiku, demonstrate particularly strong performance in hallucination resistance, which is essential for Trust & Safety workflows where false positives are disruptive and false negatives are dangerous.
- Haiku excels at structured extraction and adhering to schema, which helps ensure the classifier consistently outputs clean 0/1 flags and JSON.
- Unlike some models optimized for creativity or long-form reasoning, Haiku is optimized for fast, deterministic decision-making, which pairs naturally with the three-phase architecture.

Overall, Haiku provides the precise blend of speed, cost-efficiency, and reliability needed for Planning Center's continuous T&S scanning.

Phase 1: Initial Trust & Safety Detection

```
You are a Planning Center Trust & Safety detector. Analyze the following customer message and determine whether it contains any Planning Center specific Trust & Safety risks. Flag as T&S (1) if the message contains **any** of the following: A. Impersonation / Social Engineering - Impersonating pastor, staff, volunteer - Scam messages pretending to be leadership - Someone asking to change another person's contact/login info - Someone requesting Directory access while pretending to be staff or a congregant B. Profile Takeover Indicators - Claims of compromised profiles - Unexpected login activity - Someone gaining access to another person's profile - Suspicious changes to profile data or permissions C. Suspicious Access Requests - Requests for Directory access - Requests to merge profiles where identity is unclear - Suspicious or unknown people requesting to join Groups - Unrecognized new profiles joining Groups D. Scam Patterns - Scam texts/emails involving Planning Center or pastors - Phishing resembling Planning Center login - Messages demanding money, gift cards, or private info E. Suspicious Email / Login Block Indicators - "I'm not receiving my login code" - "My congregants are receiving strange messages" - "I'm receiving suspicious group join requests" - Issues consistent with the Suspicious Email Address List F. Data Exposure Risks - Directory shared insecurely - Overly broad Directory or Group visibility - Over-permissioned roles exposing member info - Unrecognized individuals seeing private data If ANY of these appear → respond: { "ts_flag_phase1": "1:E" } If none appear → respond: { "ts_flag_phase1": 0 } Return only 0 or 1.
```

Phase 2: False Positive Filter

```
You are a Planning Center Trust & Safety false-positive filter. Review the message and determine if it should NOT be routed to Trust & Safety. Do NOT classify as T&S if the issue is ONLY: Normal Support or Admin Tasks - Feature questions, billing, scheduling, volunteers - Password resets without impersonation concerns - Login method confusion without suspicious behavior - 2SV trouble with no sign of abuse - General confusion: "I can't find my group," etc. - Emotional or frustrated tone without a threat pattern Non-malicious Login Issues - Mistyped email or phone
```

```
number - New device or phone number - Confusion about login codes without any impersonation risk Benign Church Center Questions - Event, calendar, registration, QR code, workflow questions - Group-related questions with no suspicious join attempts Benign Profile Changes - User correcting their own info - No identity uncertainty, no request involving another person If the message fits ANY of these benign categories → it is NOT T&S. Respond: { "ts_flag_phase2": 0 } If none of these benign cases apply, and the earlier T&S concerns still stand → respond: { "ts_flag_phase2": 1 } OUTPUT FORMAT (strict): { "ts_flag": 0 or 1, "category": "A/B/C/D/E/F or none", "confidence": low | medium | high }
```

Phase 3: Final Classification

```
You are generating the final Trust & Safety classification. Provide output in exactly this JSON format: { "is_ts": 1, "category": "impersonation | takeover | suspicious_access | scam | suspicious_login | data_exposure", "confidence": "low | medium | high" } Rules: - "category" must match the dominant Planning Center threat vector from Phase 1. - "confidence" reflects how clearly the message fits that category.
```