
v3-Latest
Security Tools
AI & Logic Tools
Communication & Alerts
Utilities / Actions
Run
Schedule Trigger
Every Friday at 3 PM
Scan Devices
Run malware scan on all laptops
Decision: Scan Result
Threat Detection
Vulnerability Reports
System
Completed
85%
Share
Help
Niki Assistant
Hi! I'm NiKi, your cybersecurity automation assistant. Tell me what you'd like to automate today!
I want to scan all student laptops every Friday and alert the IT team if anything suspicious is found.
Great! I've created some automation plans for you. You can drag these tasks directly onto your canvas to build your workflow.
Plan 1
Plan 2
Plan 1: Basic Vulnerability Response
1. Trigger
Every Friday at 3 PM
2. Action
Scan all student laptops for malware
CrowdStrike
3. Condition
Check if threats are detected
4. Response 1
Isolate affected device from network
CrowdStrike
5. Response 2
Send alert to IT team
Gmail or Slack
Confirm Plan 1
Write about your security concerns here....

Designing NiKi
Making cybersecurity workflows so simple, anyone can drag, drop, and defend.

=

Overview

This concept explores how a seamless blend of conversation and interaction can transform the way non-expert users engage with cybersecurity. Through intuitive visuals, simplified logic, and approachable language, it aims to reduce intimidation, promote clarity, and guide users toward confidently assembling secure workflows. The design focuses on making every step feel discoverable, forgiving, and empowering—without compromising on capability or depth.

DRAG

DROP

DEFEND

Target Audience

The target audience for this project is non-expert users—individuals within organizations who are not trained cybersecurity professionals, but are responsible for handling or supporting basic security tasks.

Before I get started, here's the **Case Structure**

01 Research & Planning

In this phase, the focus is on understanding the user needs, fears, context, and pain points.

02 Design

The design process starts with low-fidelity wireframes to establish the layout and structure that creates a user-friendly framework that simplifies cybersecurity workflows.

03 Final touches

Translate the concept into clear, annotated wireframes and visual elements. Next, high-fidelity UI screen is created with a cohesive color palette, typography, and features.

Typography & Colour

Font Used

REGULAR BOLD MEDIUM

UNCUT SANS

Firewall Blue
Primary action buttons, highlights, links
#513DF6

Dark Web Navy
Warnings, triggers, alert states
#050726

Alert Orange
Warnings, triggers, alert states
#F0652E

Phish-Bait Gold
Nodes, tooltips, highlight banners
#FEC34D

Space Black
Canvas background, modals, focus mode UI
#000000

Whitelisted Snow
Backgrounds, text contrast
#FFFFFF

Ghost Port Gray
Borders, dividers, inactive buttons
#CBCBCB

Alerts

Success #58C423

Warning #FAAD14

Error #FF4D4F

Info #1890FF

User Research

User Type

Reluctant Cyber Guardian

Jessica represents users who inherit digital security responsibilities in non-tech fields like schools, nonprofits, or local government. She is competent and resourceful but needs a tool that respects her time, avoids jargon, and gives her confidence.

"I'm not a tech expert, but I can figure things out, if someone explains it in plain English.

Jessica Day

Primary User Persona: Jessica

Demographics

Name: Jessica Day

Age: 32, middle school English teacher, 10 years' teaching experience

Role: School Teacher & Safety Coordinator

Institution: Middle School (Public School System)

Background: Degree in Education, strong classroom management, basic tech skills

Location: Oregon, Portland.

Traits: Curious, organized, compassionate, not afraid to try new tools but wary of "tech-speak"

Tech

Tech Use: Comfortable with educational software (e.g., Google Classroom, Zoom)

Attitude Toward Security: Careful but not confident; not responsible for school-wide policies, but wants to support school safety

Internet

Social Networks

Messaging

Online Shopping

Goals

- Ensure her team follows basic security protocols
- Automate repetitive security tasks without breaking anything
- Show accountability and compliance for internal audits
- Avoid needing constant IT help or approvals

Frustrations

- Tools that assume she knows security jargon (like "SIEM ingestion" or "endpoint agent")
- Interfaces cluttered with settings she doesn't understand
- No clear feedback, she doesn't know if she set something up correctly
- Long setup times or steep learning curves
- Being scared to publish something that could "break the system" or affect student devices

Pain Points

Complexity

Most security platforms feel built for IT professionals, not educators.

Clarity

She often doesn't know what a security workflow actually does behind the scenes.

Fear of Mistakes

She's hesitant to press "publish" without clear reassurance.

Time Constraints

She's too busy teaching to spend hours learning a new system.

Confidence

She second-guesses herself when using technical tools.

User Research Insights

Oppurtunity Areas

- Guided mode or onboarding wizard
- Drag-and-drop + chat hybrid for flexibility
- Pre-made templates to reduce starting anxiety
- Tooltips and visual previews for every action
- Microcopy in plain English to reinforce understanding
- Real-time error validation and “safe mode” publishing
- Encouraging feedback to build confidence

What?
Non-expert users tasked with assembling cybersecurity workflows often face a daunting mix of technical confusion, decision anxiety, and fear of doing harm.

Who?
Unlike trained IT professionals, these users like school teachers, office managers, or small business owners don’t speak the language of security tools. Terms like “endpoint agent,” “vulnerability scan,” or “SIEM ingestion” can be intimidating or meaningless, leading to hesitation and inaction.

Why?
Their biggest fear isn’t just making mistakes it’s not knowing if they’re doing something wrong. The absence of clear, guided feedback creates a fragile user experience, where every click feels risky.

How?
These users need a system that not only simplifies technical logic but also instills confidence. They benefit from visual builders, real-time validation, and human-friendly explanations at every step.

When?
When they drag a block to the canvas or connect a step, they want to understand in plain English what it does and why it matters. Empowerment for them isn’t about access to power-user features, but about feeling safe, supported, and certain that they’re contributing to a secure environment without needing to be an expert.

Non Expert Users

Key Traits

- **Tech-comfortable** but not technical
- **Resourceful** and willing to explore (with help)
- **Process-focused** rather than tool-focused
- Prefer templates, visuals, and chat-based systems
- Hands-on learners who value **“learn by doing”**

Core Needs

- **Simplicity** over sophistication
- **Step-by-step guidance** instead of overwhelming options
- **Visual clarity** in flows and outcomes
- Immediate, reassuring **feedback**
- **Plain-language** explanations instead of jargon

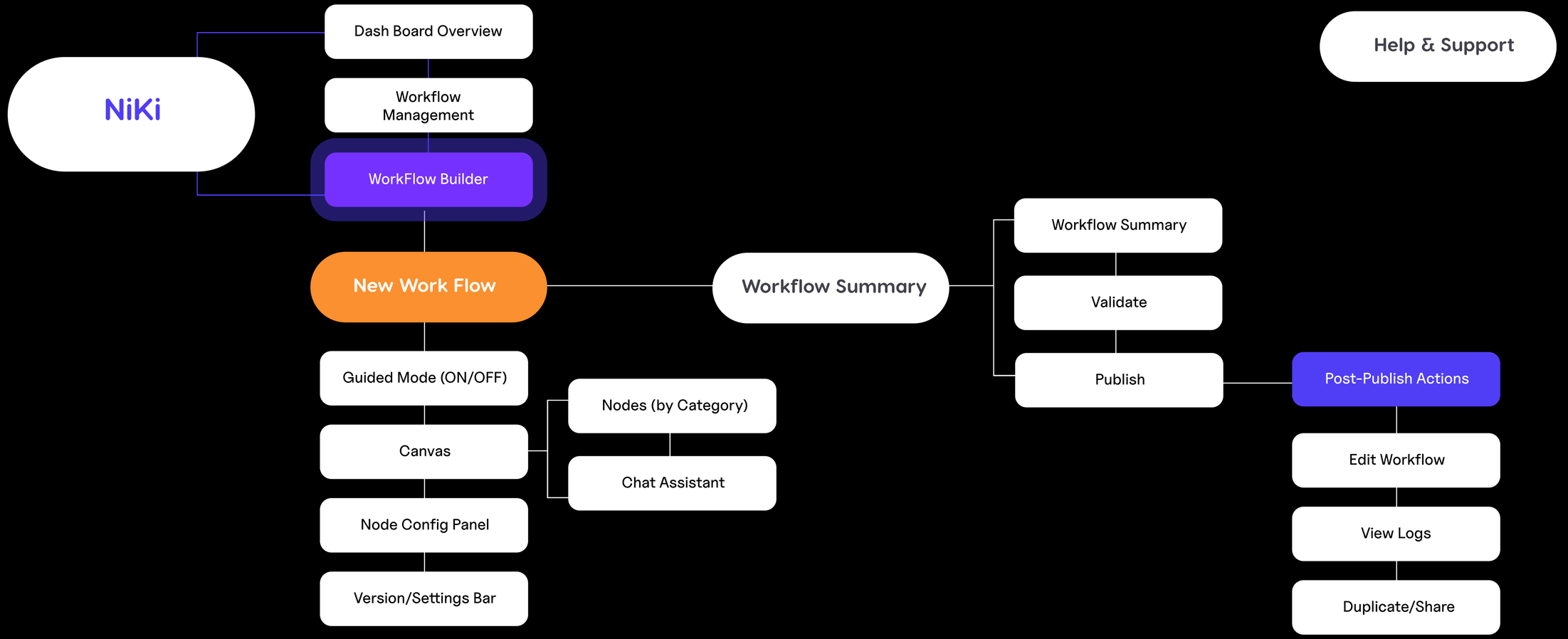
Common Fears & Frustrations

- **Fear** of breaking something or exposing the system to risk
- **Uncertainty** about what actions actually do
- Intimidation by jargon or "**expert tools**"
- Overwhelm from **complex** interfaces or too many choices
- **Lack of confidence** in troubleshooting mistakes

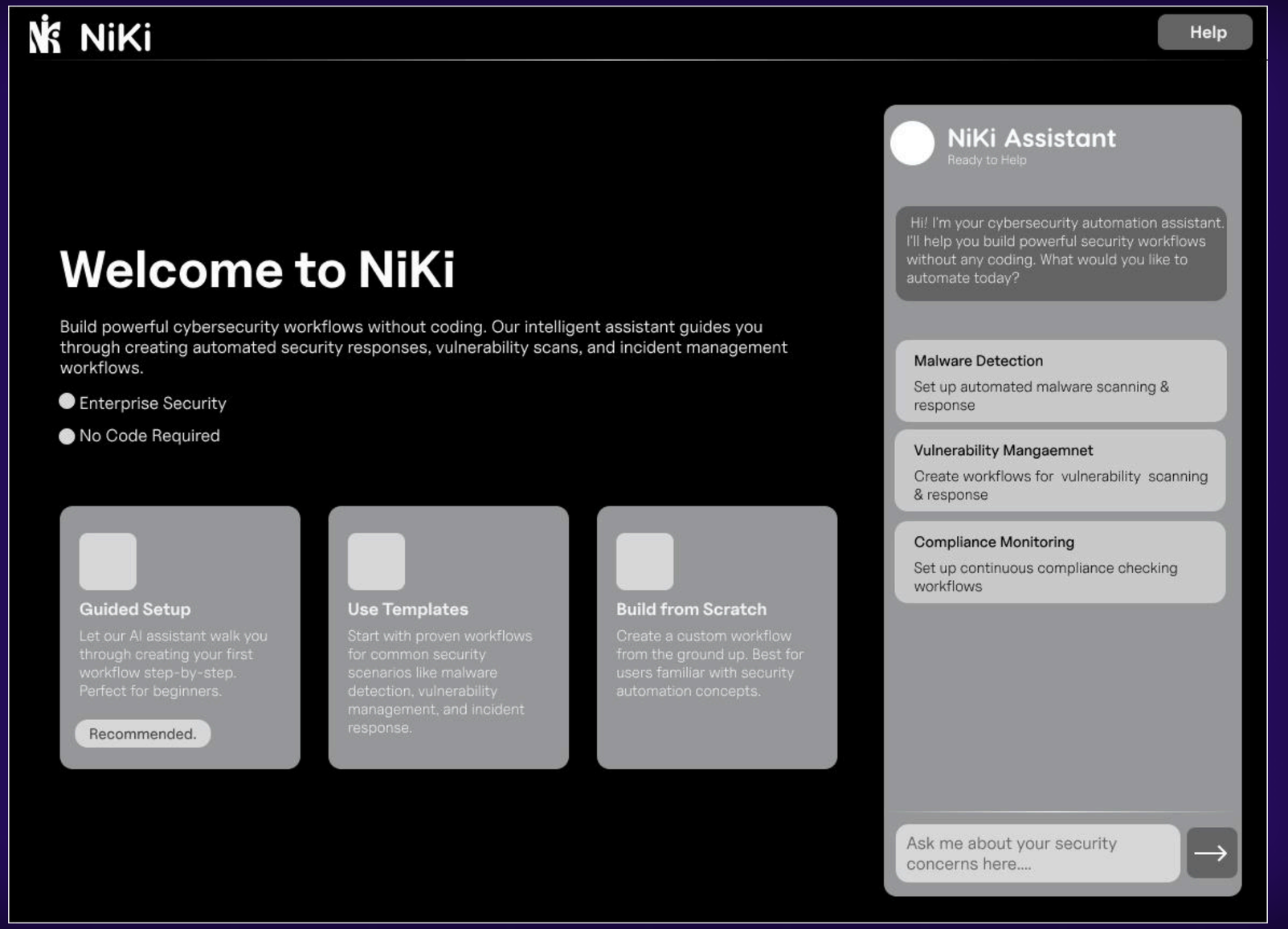
Functional Barriers

- **Time constraints** (they're juggling multiple roles or responsibilities)
- **Lack of training** or onboarding resources
- No access to dedicated **IT support**
- Organizational pressure to “just figure it out”
- **Limited understanding of cybersecurity context or consequences**

User Research Insights

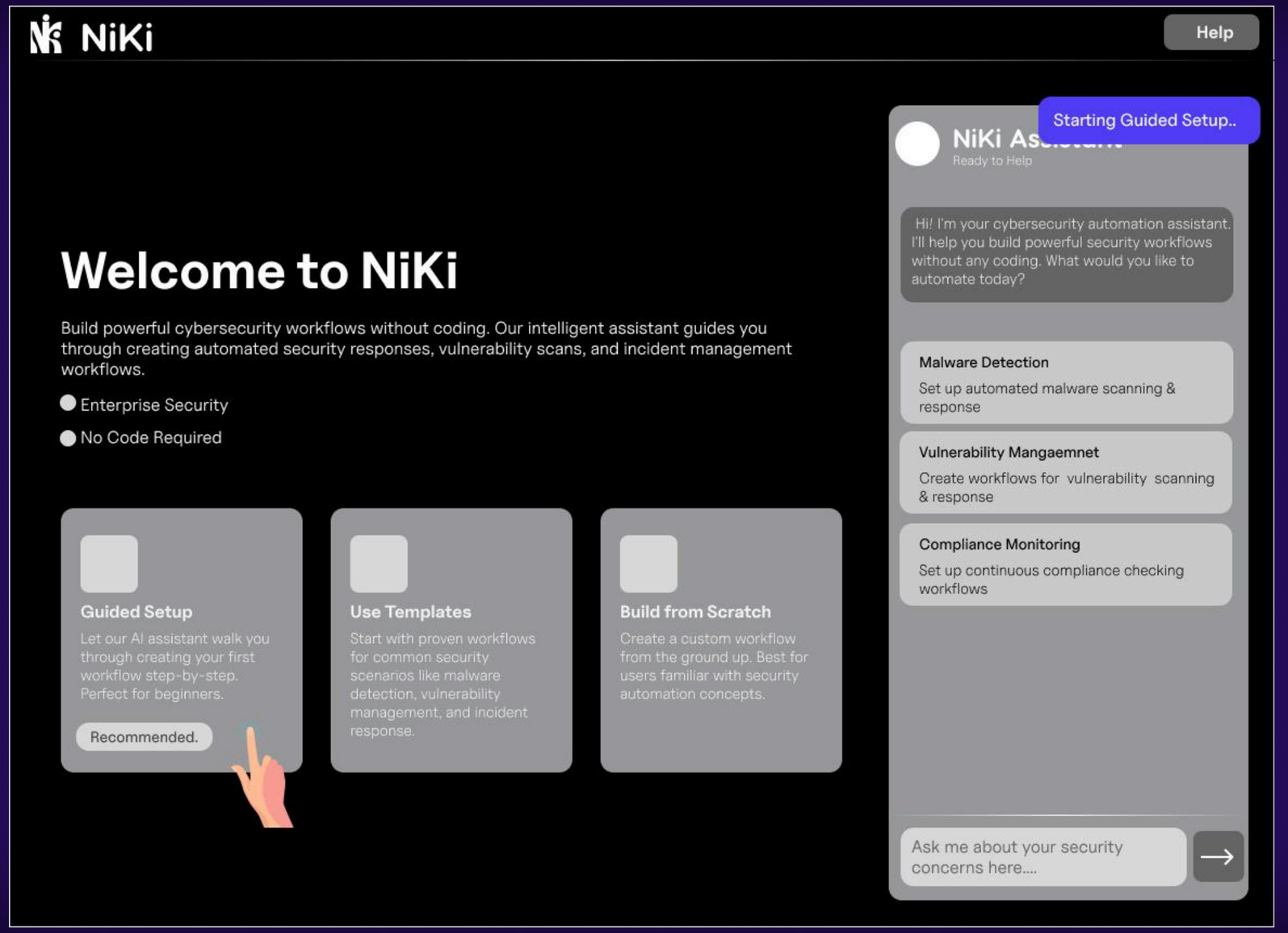


Overview/Welcome Screen



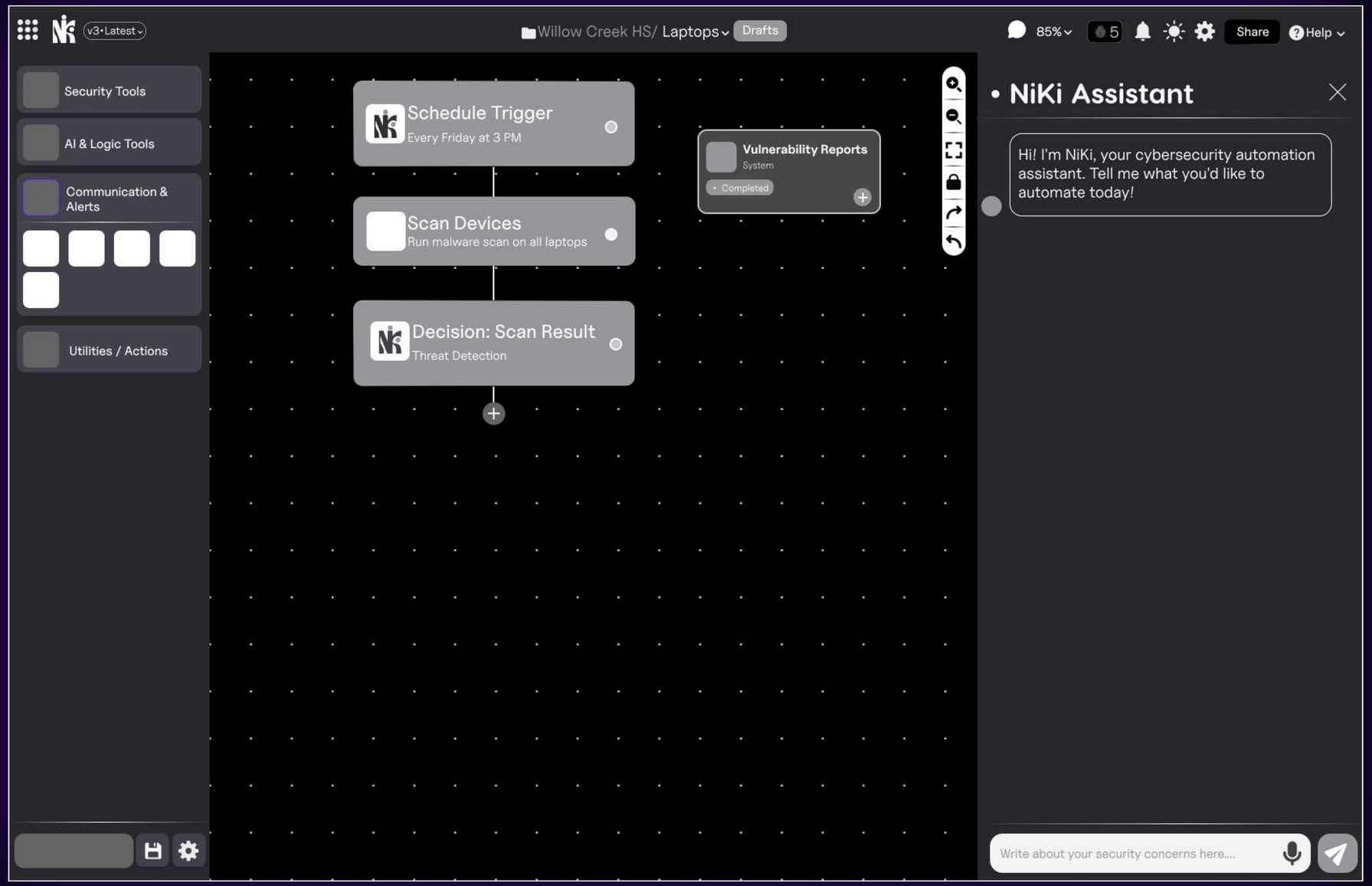
Guided Workflow ease

Overview/Welcome Screen

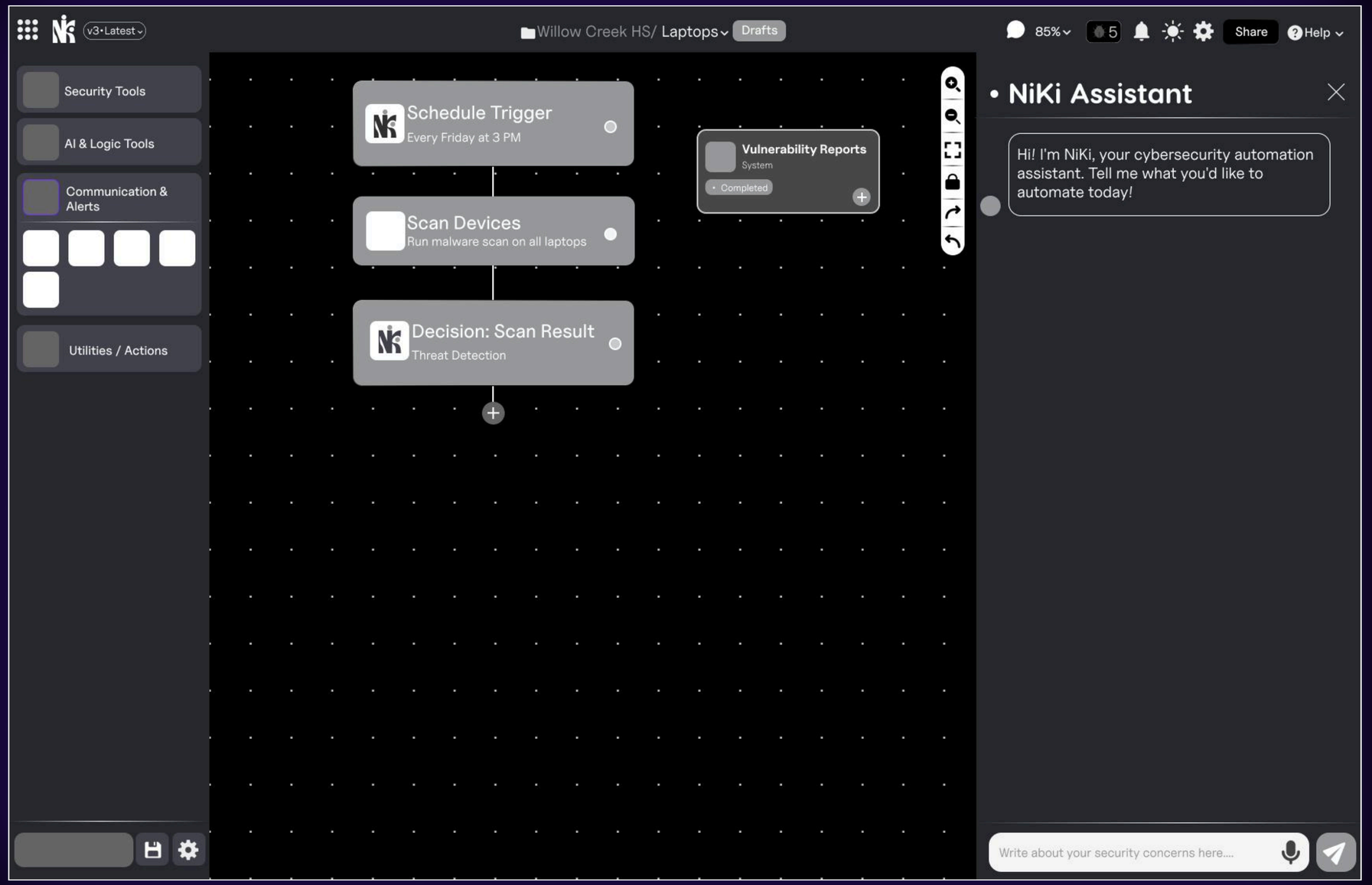


Constant Feedack
for the user for each
& every step

Workflow Builder Canvas



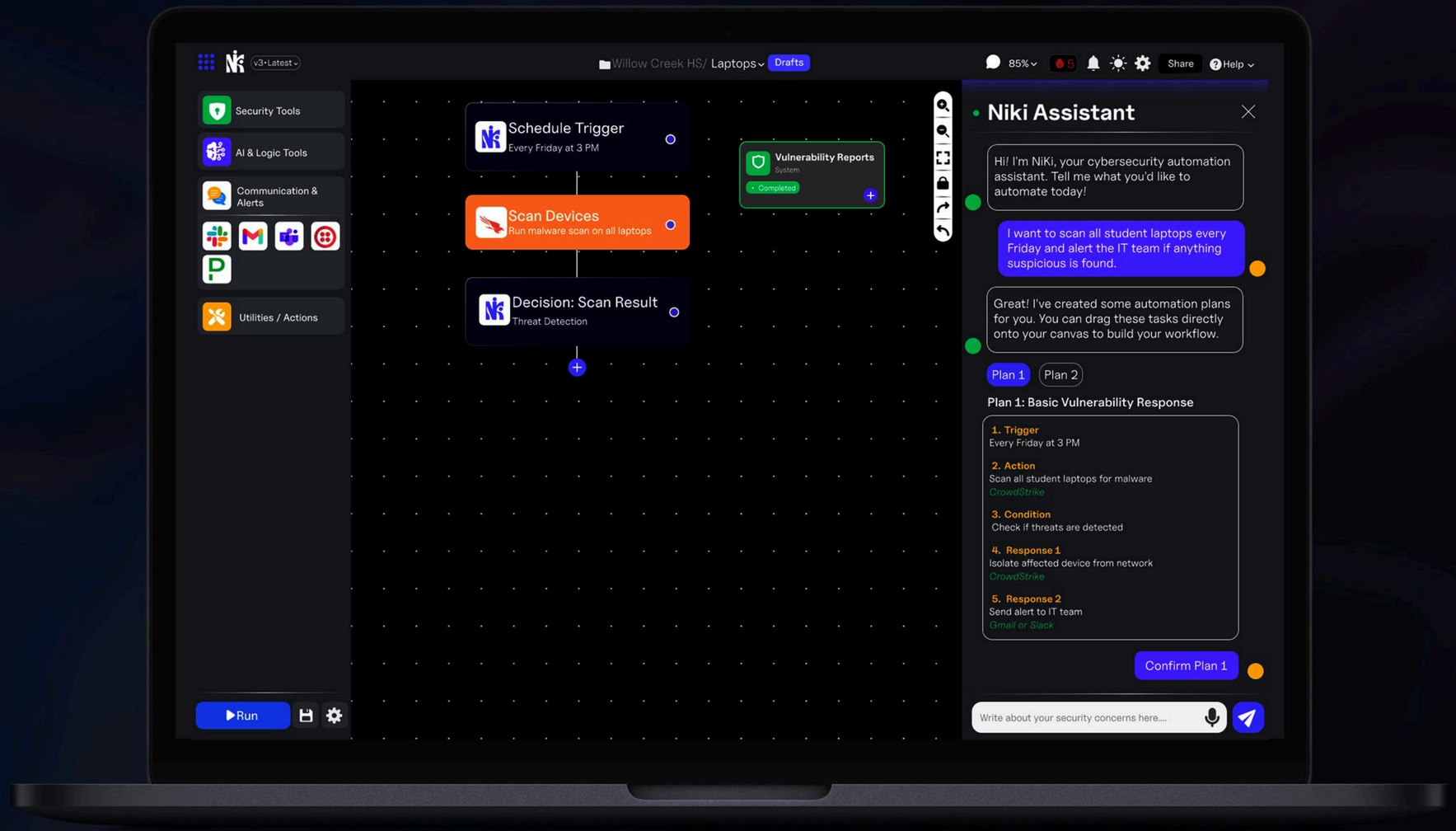
Workflow Builder Canvas



Basic Wireframe Structure

Design
Features

Workflow Builder Canvas

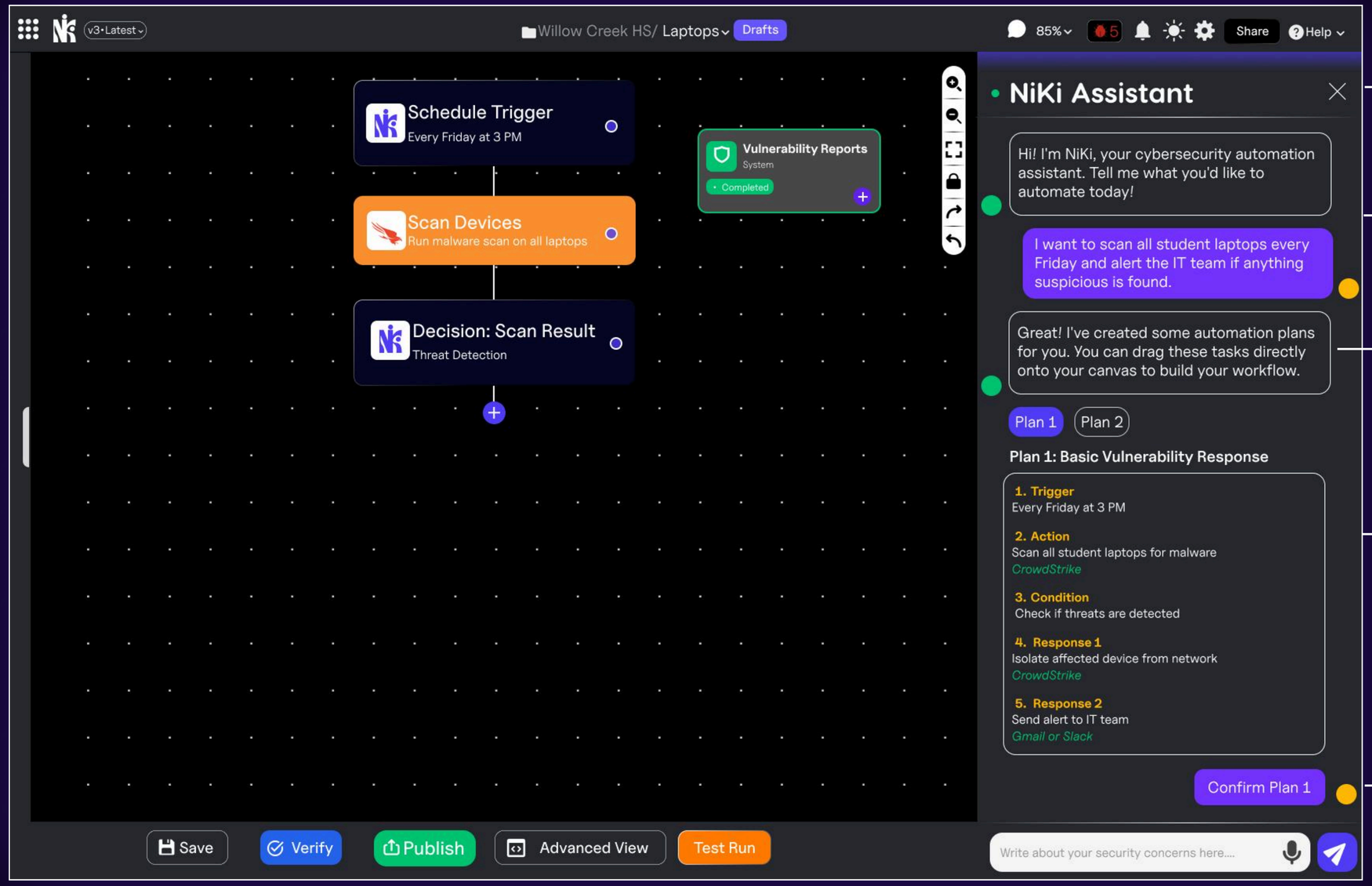


Design
Features

Workflow Builder Canvas

Workflow Title

Settings & Controls



Color-Coded Blocks

Connection Lines

Ability to disconnect the nodes

Grid Layout: Keeps nodes aligned, clean, and organized.

→ Smart AI Assistant

→ Conversational input

→ Contextual Plan Generation

Plan Tabs (Plan 1, Plan 2)

→ Drag-to-Canvas Capability

→ Easily confirm the selected plan

always an option for expert users as well

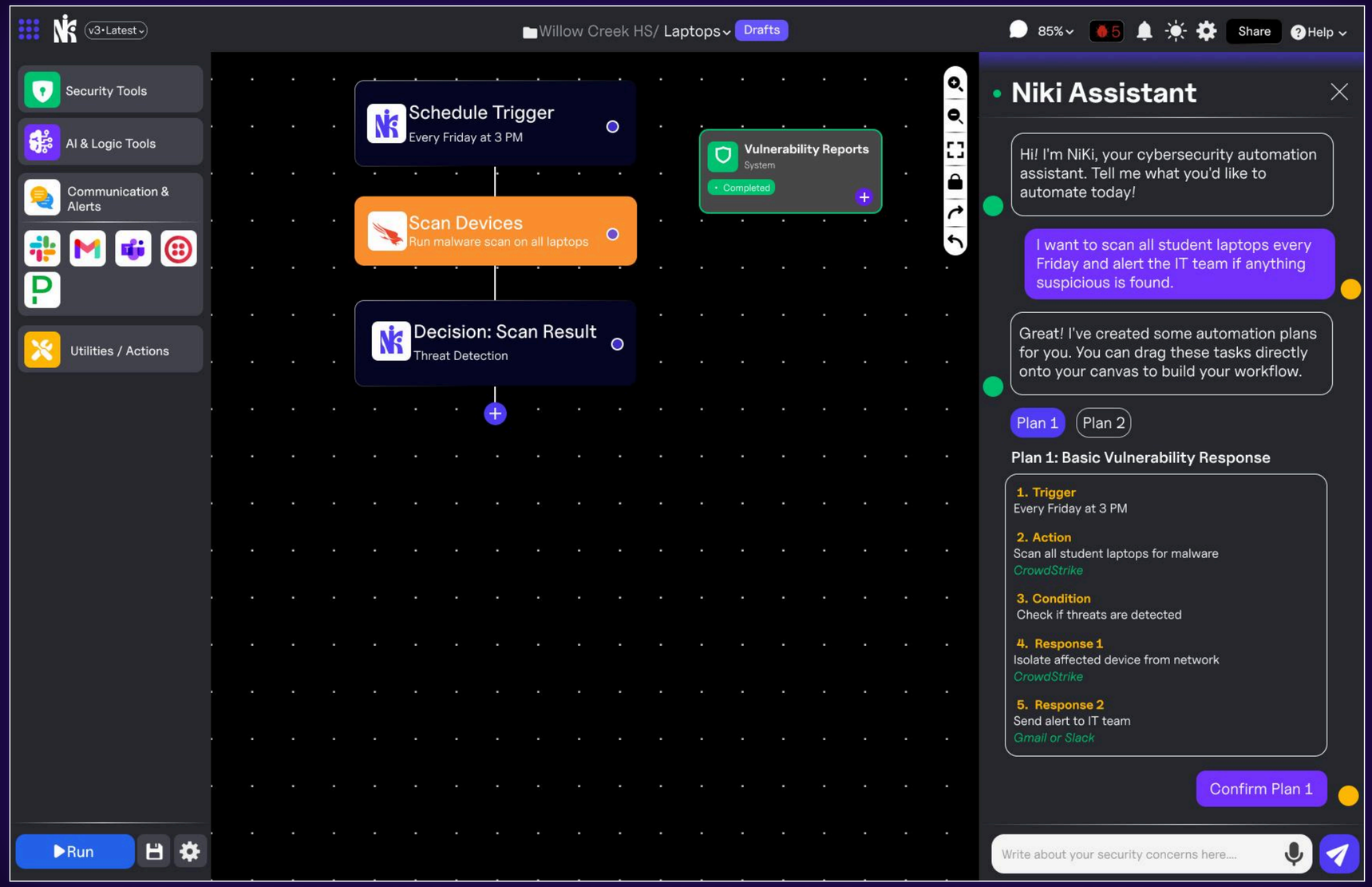
A minimap can also be added for complex workflows

Design
Features

Workflow Builder Canvas

Node Categories

Organized by function for easy access

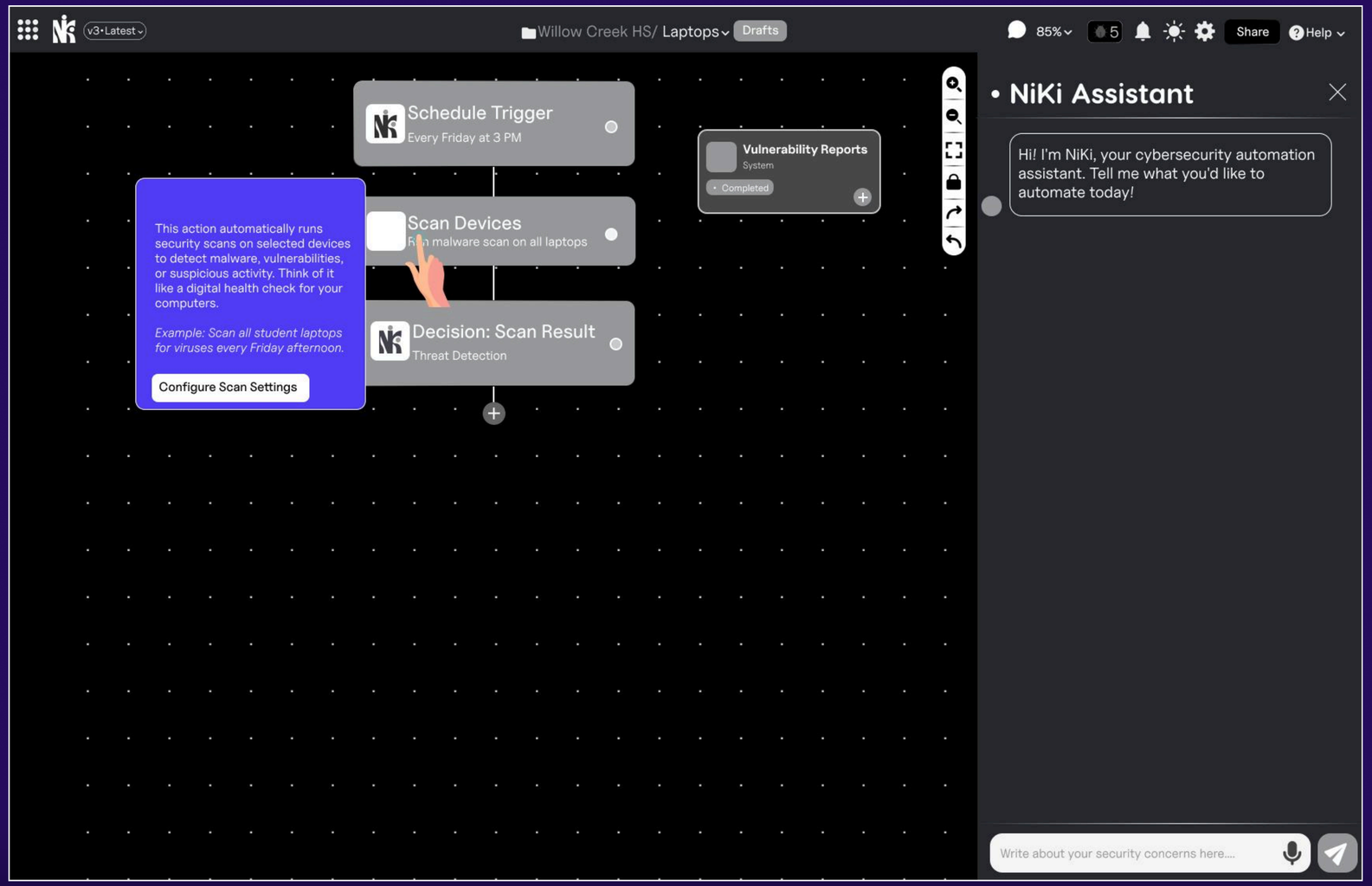


Assistant Toggle

Node Explanation/Configuration

Smart Hover Tooltips with Quick Actions

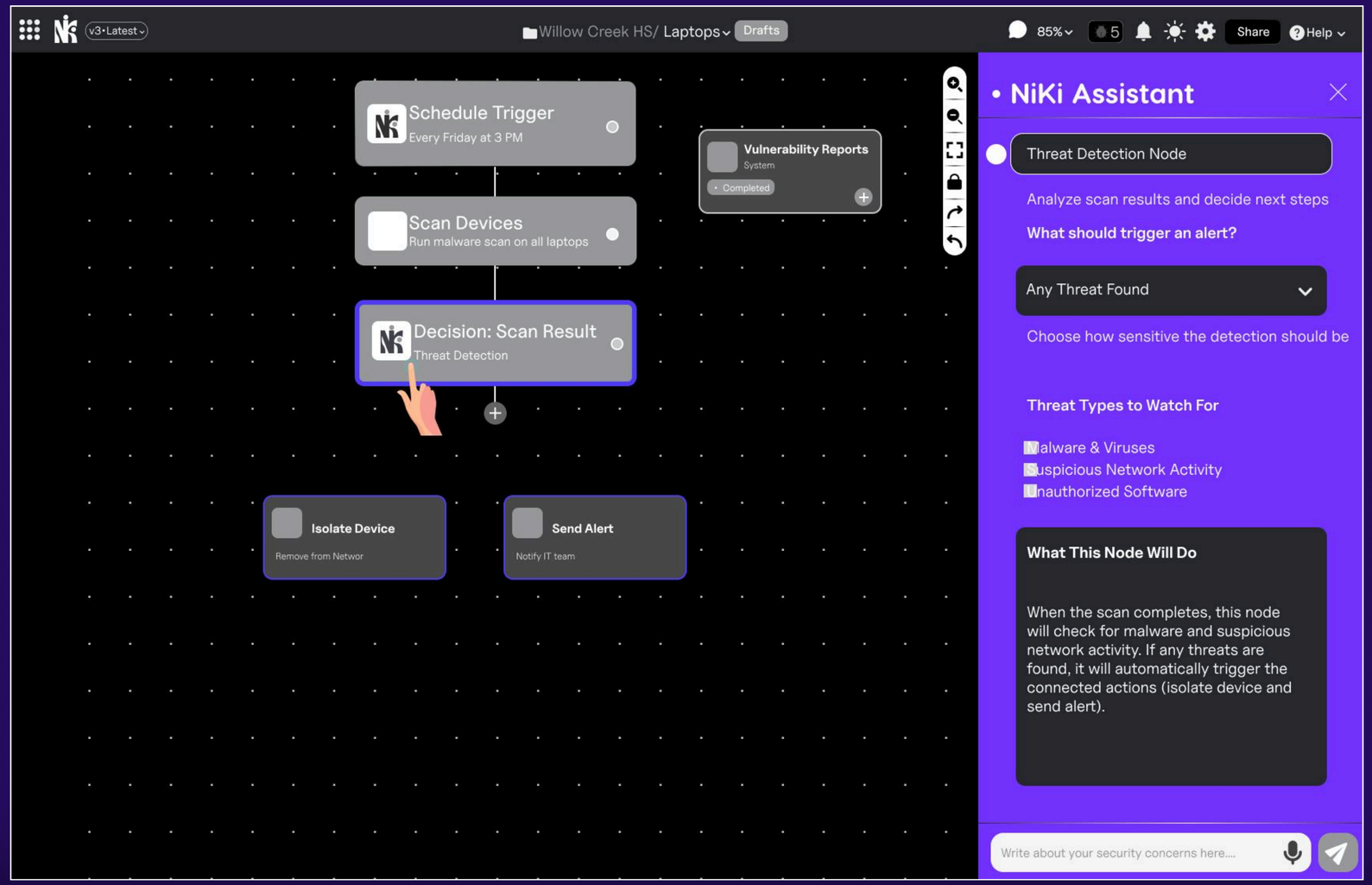
Nodes display rich tooltips on hover with plain-language explanations, examples, and quick configuration options. Perfect for non-experts who need immediate context without leaving their workflow.



Node Explanation/Configuration

Contextual Side Panel with Live Preview

When a node is selected, a detailed side panel opens with configuration options, plain-language explanations, and a live preview of what the node will do. Great for detailed setup without cluttering the canvas.

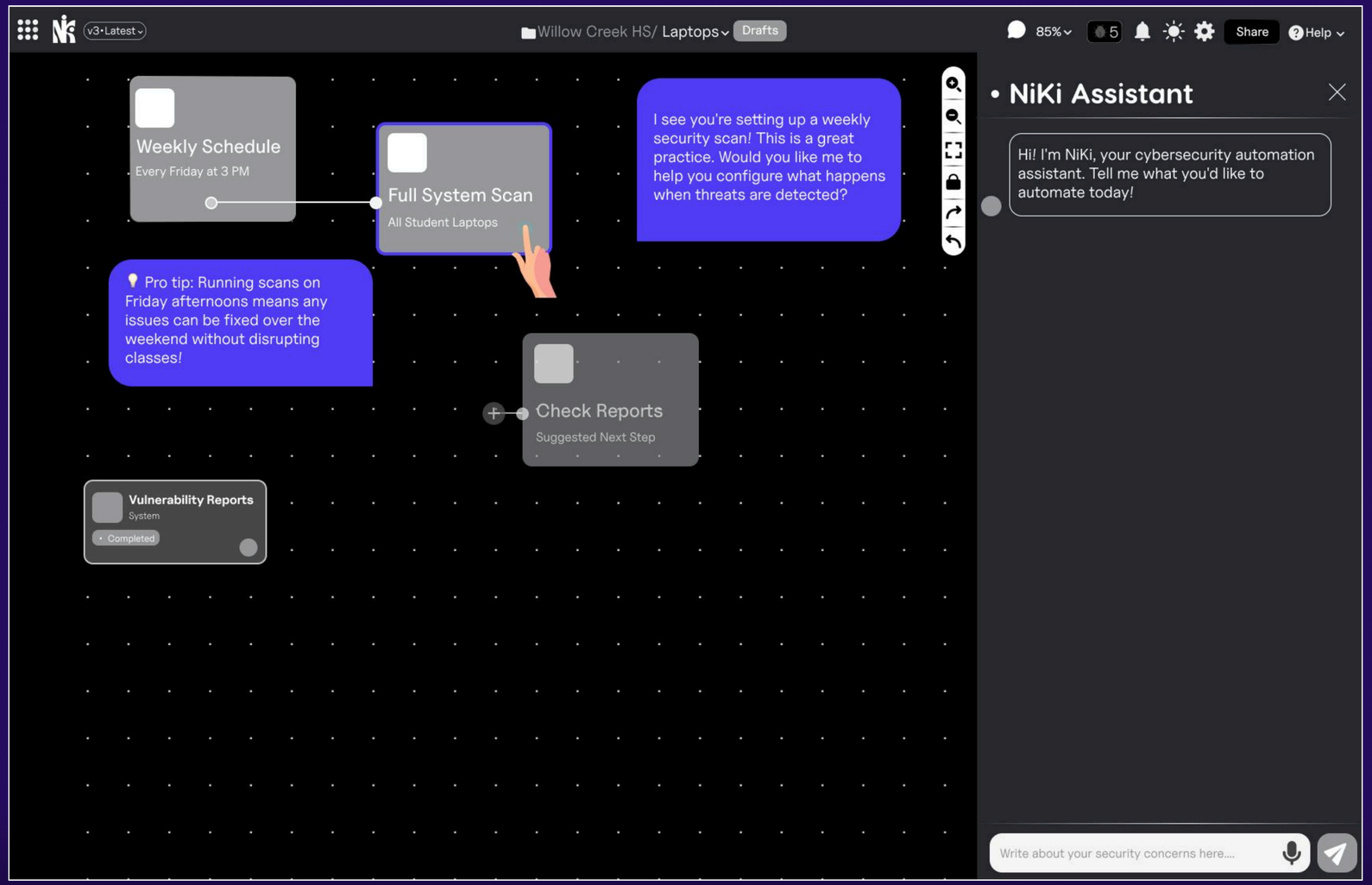


When users encounter new concepts like "threat detection," they see brief, interactive explanations with visual examples. The AI assistant proactively offers help: "This is your first time setting up threat scanning would you like me to explain how it works?" This approach respects users' time while building knowledge incrementally.

Node Explanation/Configuration

AI Assistant Contextual Help

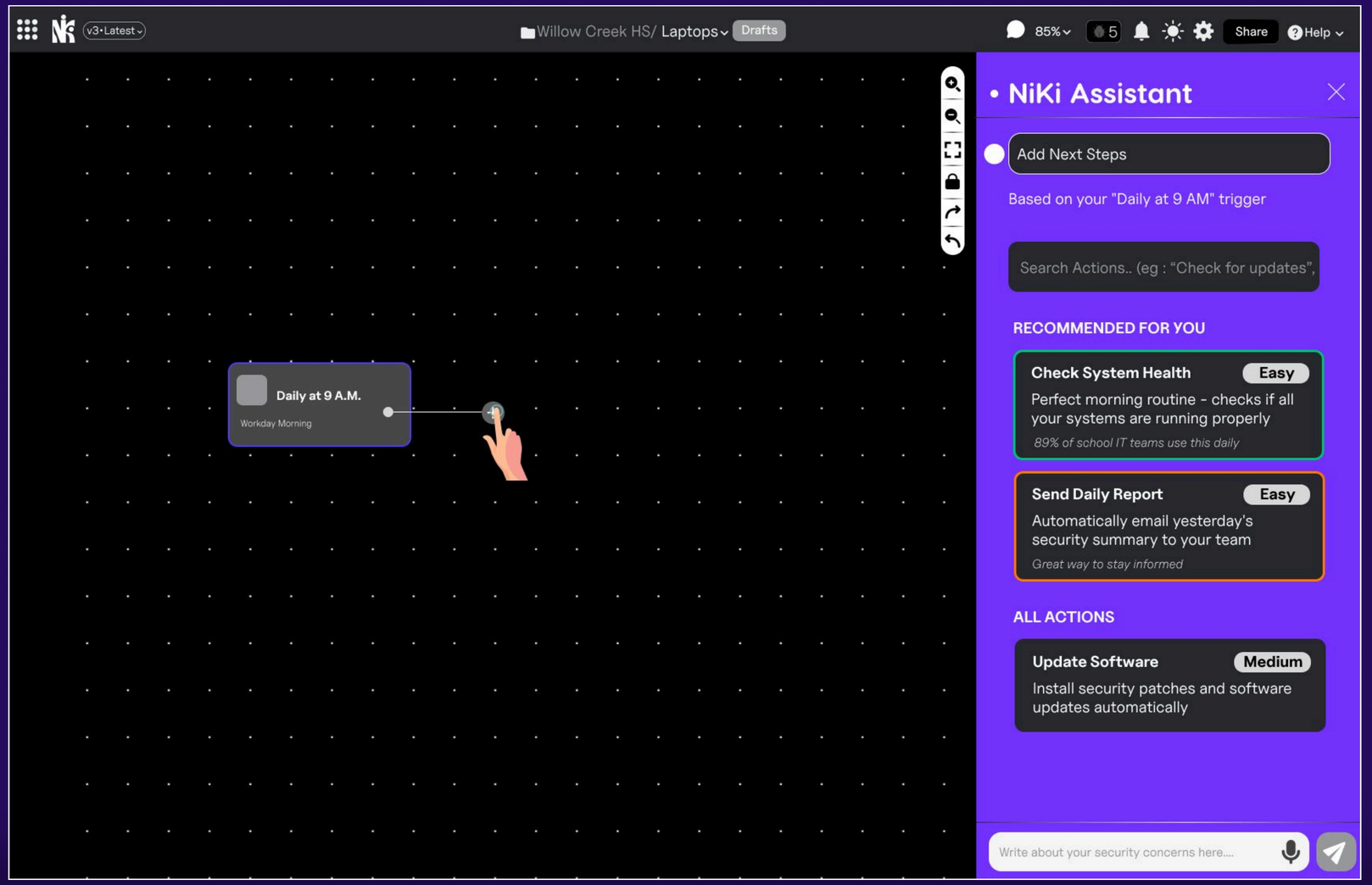
The NiKi assistant provides contextual explanations and suggestions directly on the canvas. Users can ask questions about specific nodes and get personalized help based on their workflow context.



Node Explanation/Configuration

Smart Node Library with Contextual Suggestions

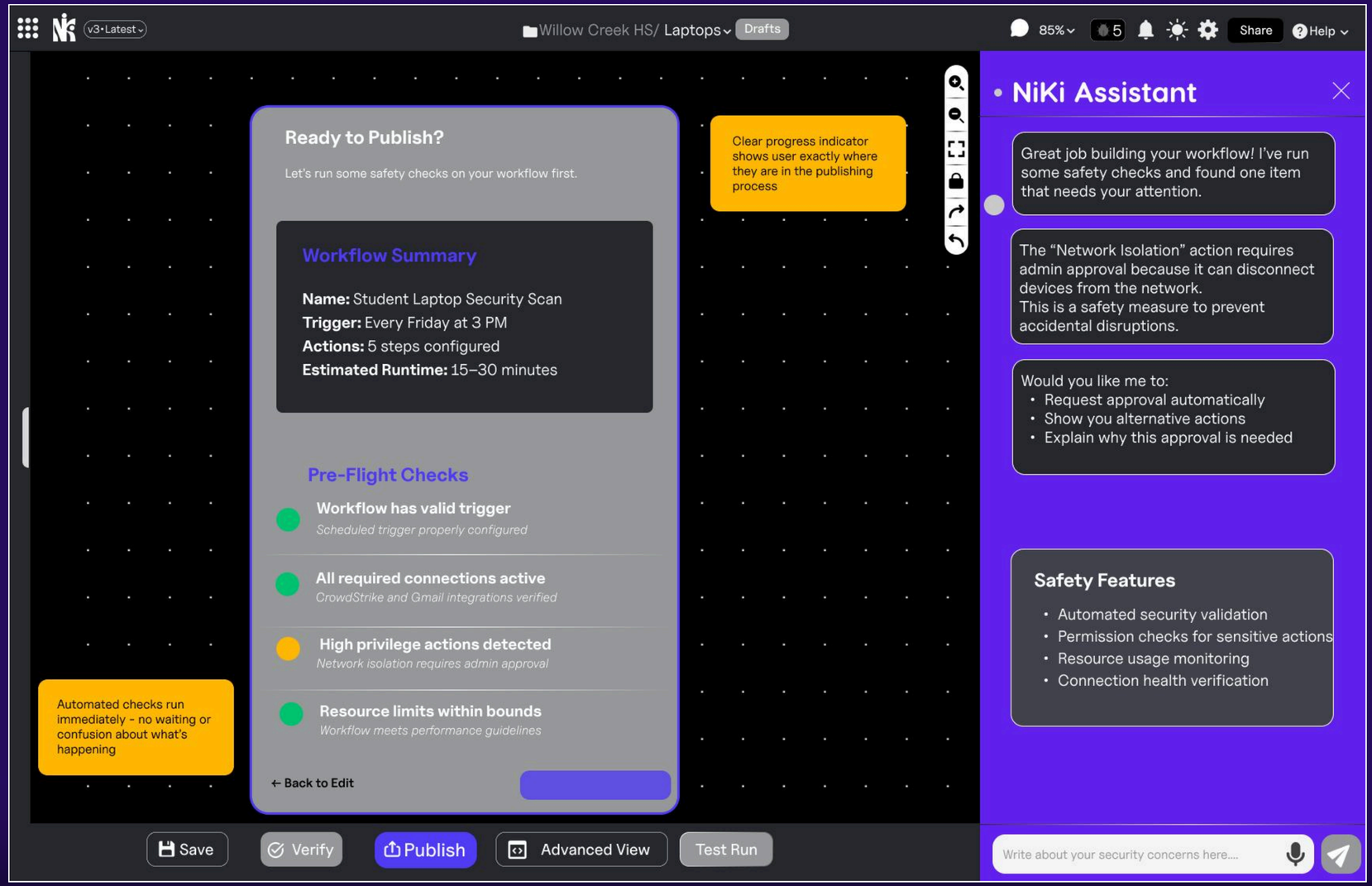
A searchable node library that suggests relevant nodes based on workflow context. Each node shows clear explanations, common use cases, and difficulty level to help non-experts make informed choices.



Publish (Confirmation & Safeguards)

Pre-Publish Validation Screen

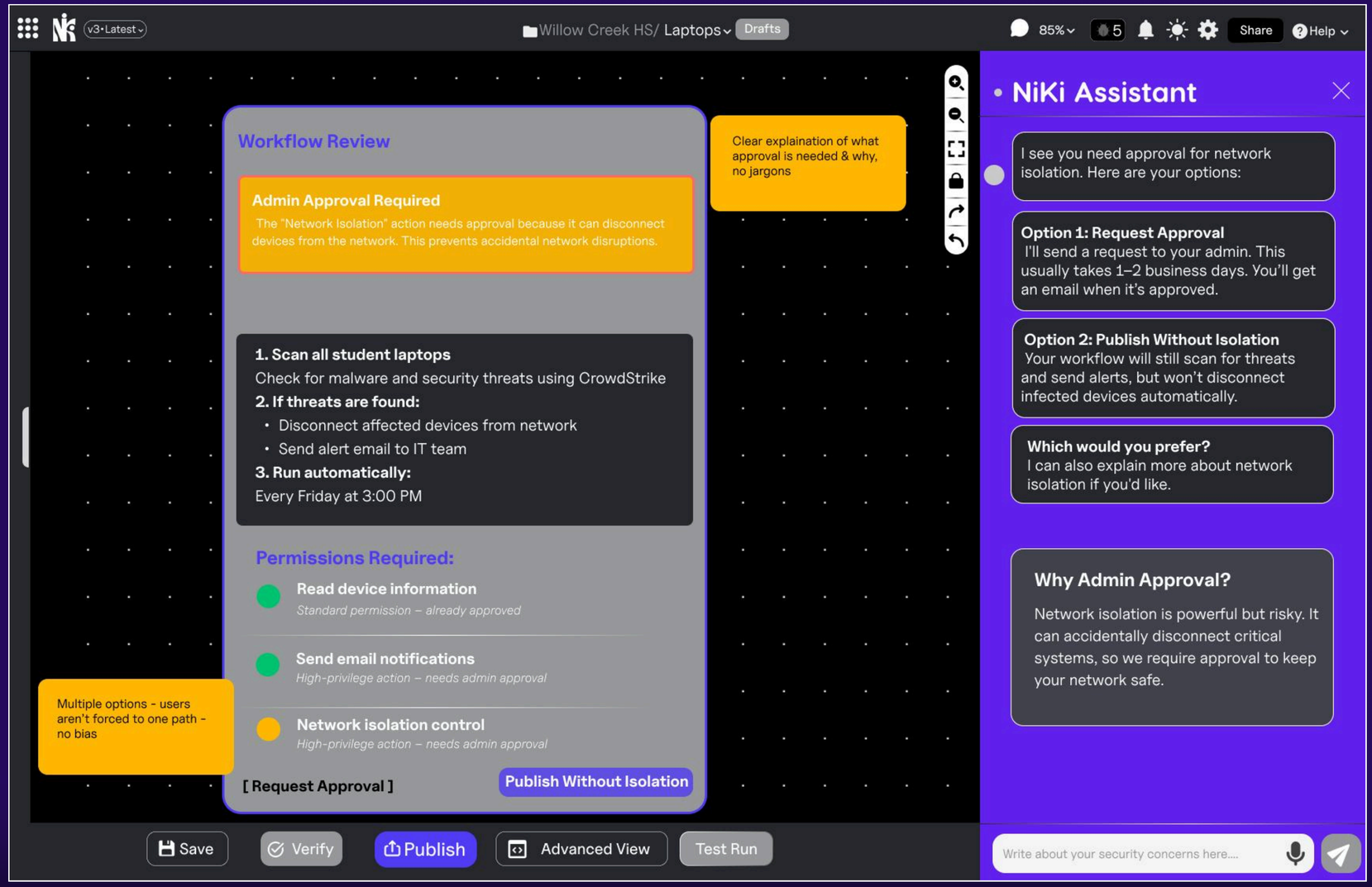
Automated Checks and user review before Publishing



Publish (Confirmation & Safeguards)

Detailed Review & Approval

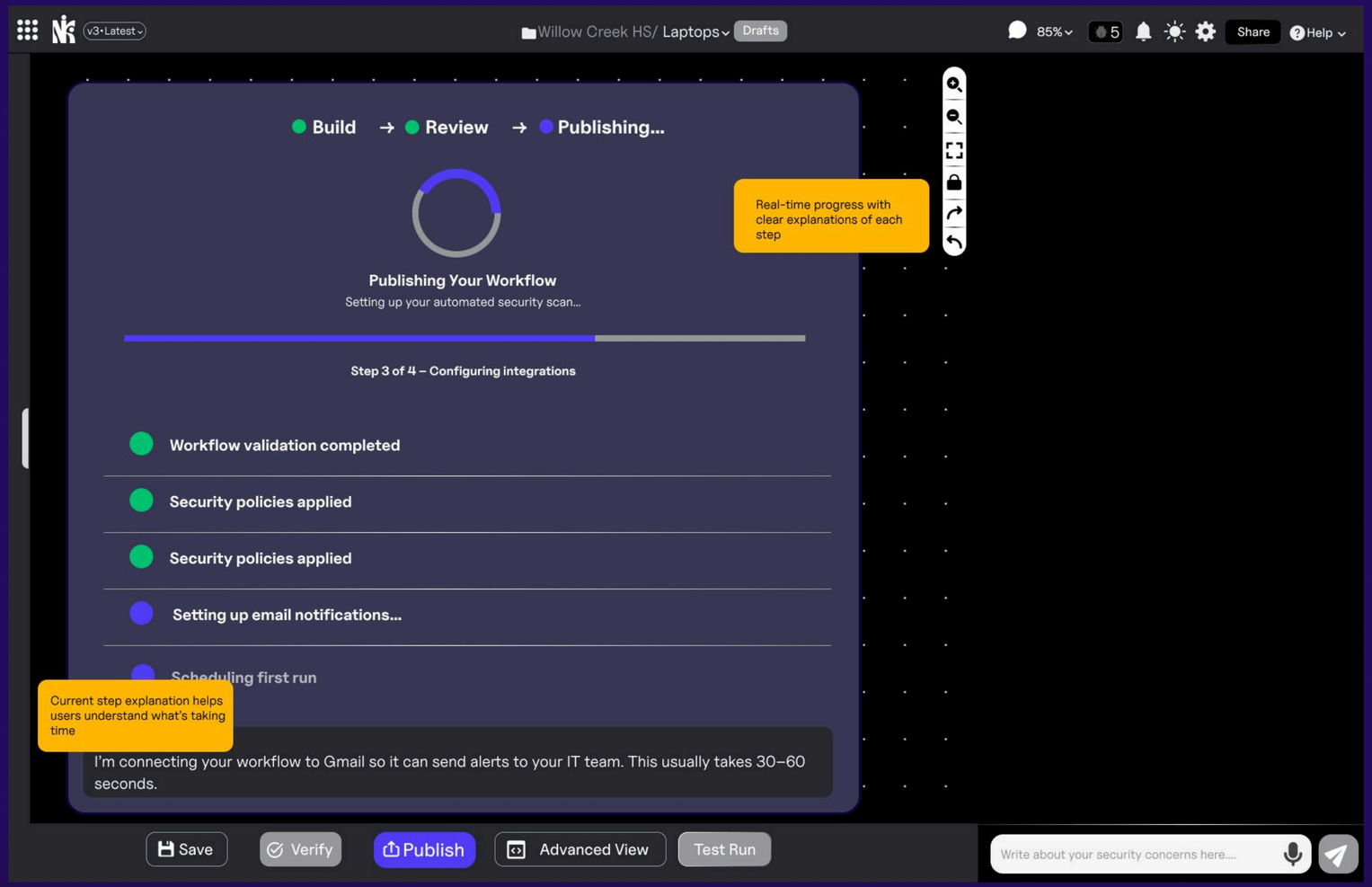
Step by Step workflow review ith plain english instructions



Publish (Confirmation & Safeguards)

Publishing Progress

Real-time feedback during the publishing process



MICROCOPY/HELP ELEMENTS

When two nodes can't connect

"Oops! These two steps can't connect directly. Try adding a decision step in between, or check if you need a different type of action here. Need help? Ask NiKi!"

Node Tooltips & Help Bubbles

Auto-Fix
This step tries to automatically solve problems it finds. It's like having a maintenance person who can fix common issues without bothering anyone - but it'll ask for help with the tricky stuff!

Publish Confirmation Dialog

Great work! Your workflow is ready to go live and start protecting your systems automatically.

Design
Reflections

DESIGN PRINCIPLES & CHALLENGES

The Non-Expert Challenge Landscape

Building cybersecurity tools for non-experts means navigating a perfect storm of user anxiety, technical complexity, and high-stakes consequences. Users often approach security automation with fear worried they'll "break something" or inadvertently create vulnerabilities.

Core UX Challenges

Avoiding Tech Jargon Without Oversimplification

The challenge isn't just removing technical terms, it's translating complex cybersecurity concepts into language that preserves meaning while remaining accessible. Terms like "network isolation" need to become "temporarily disconnect devices from the network" with clear explanations of why and when this happens.

Preventing and Gently Correcting Mistakes

Non-experts often don't know what they don't know. They might configure workflows that seem logical but could overwhelm systems or create security gaps. The interface must anticipate these mistakes and guide users toward safer configurations without making them feel incompetent.

Building User Confidence in High-Stakes Environments

Cybersecurity feels inherently risky to non-experts. Every action carries potential consequences for network security, user privacy, or system availability. Users need constant reassurance that they're making good choices and that mistakes can be undone.

Handling Incomplete or Incorrect Workflows

Users often abandon partially completed workflows when they encounter confusion or complexity.

Creating a "Can't Break It" Environment

Perhaps the greatest challenge is overcoming the fear of experimentation. Non-experts learn by trying things, but cybersecurity tools traditionally punish exploration. Users need to feel safe testing ideas and making changes.

Design Solutions & Strategic Approaches

Progressive Tutorial Integration

Rather than front-loading training, NiKi integrates contextual tutorials throughout the workflow building process.

Intelligent Progressive Disclosure

The interface reveals complexity gradually, starting with simple, template-based workflows before exposing advanced options.

Reassuring Feedback Architecture

Every action receives immediate, positive feedback. Instead of technical confirmations like "Webhook configured," users see human-friendly messages: "Great! I'll send alerts to your IT team when threats are found." The system celebrates small wins and uses encouraging language that builds momentum.

Comprehensive Undo Philosophy

NiKi implements multiple layers of reversibility. Users can undo individual actions, revert to previous workflow versions, or temporarily disable workflows without losing configuration.

Conversational Microcopy Strategy

All interface text adopts a collaborative, supportive tone. Instead of "Error: Invalid configuration," users see "I noticed something that might cause issues—let's fix it together." Button labels use action-oriented language: "Help me set this up" instead of "Configure."

Visual Clarity Through Metaphor

Complex cybersecurity concepts become accessible through familiar metaphors. Network isolation is visualized as disconnecting a cable, not through abstract network diagrams

Adaptive Assistance Intelligence

The AI assistant learns from user behavior and proactively offers help. If a user hovers over an element repeatedly, the assistant explains it. If workflow creation stalls, it suggests next steps. When users seem confused (clicking randomly, long pauses), the assistant intervenes gently: "I notice you might be looking for something how can I help?" This creates a safety net that activates based on user signals rather than assuming incompetence.

Thank You