

# Research Skills 3

## Task 10

Abdulaziz Alarfaj



## Step 1: Research Scenario Using AI to Generate Research Hypotheses

**Field:** Cybersecurity – Operational Technology (OT)

**Research Variables:**

**Independent Variable (IV):** Implementation of Zero Trust Architecture in OT networks

**Dependent Variable (DV):** Cybersecurity compliance rate and incident response effectiveness

**Objective:** To examine how the adoption of Zero Trust principles affects OT cybersecurity performance.

## Step 2: AI-Generated Research Hypotheses

Using **ChatGPT (GPT-5)**, the following hypotheses were generated:

**Hypothesis 1 (H1):**

The implementation of Zero Trust Architecture in OT networks is positively associated with increased cybersecurity compliance among employees.

**Hypothesis 2 (H2):**

Zero Trust Architecture adoption in OT networks reduces the average incident response time to detected cyber threats.

**Hypothesis 3 (H3):**

The combined effect of Zero Trust and network segmentation leads to higher resilience against ransomware and lateral movement attacks in OT systems.

## Step 3: AI Tool & Prompt Used

### AI Tool: ChatGPT (GPT-5) Prompt Used:

Generate three research hypotheses for a study in Operational Technology cybersecurity.

The study should examine the impact of adopting Zero Trust Architecture on (1) employee compliance with security policies, (2) incident response effectiveness, and (3) resilience against cyber threats. Make the hypotheses clear, testable, and aligned with quantitative research.

## Step 4: AI-Generated Exploratory Interview Questions

Using **ChatGPT (GPT-5)**, the following **5 exploratory interview questions** were generated:

1. Can you describe the main challenges your organization has faced in implementing Zero Trust principles within OT systems?
2. How does network segmentation impact day-to-day operations in your OT environment?
3. What strategies have been most effective in improving employee compliance with OT cybersecurity policies?
4. How does your team monitor and respond to cyber threats in OT networks, and what improvements would you suggest?
5. What lessons have you learned from past incidents that could inform future OT cybersecurity practices?