# Incident Detection and Response

December 20, 2023

## Introduction

Part of the job we do as security analyst is monitoring and analyzing alerts, and responding to security incidents. In this project, I will be filling in for Jacqui, a colleague at Yoyodyne's satellite office in Kalamazoo who is on vacation.

### The Scenario

From: jacqui@kz.yoyodyne
To: you@hq.yoyodyne
Subject: hope this helps!
I found a network diagram for you. A couple years old, but mostly up-to-date!
I jotted down some notes on the usual incident handling processes, at least here in the KZ office.
I launched a honeypot earlier this week. I meant to exclude it from the alerts, but what are the chances that any bad actors would have found it already?
Sorry I did not have time to put together more info! Good luck!
-j

Here is the project outline:

## Outline

- Analyze Alerts from the Intrusion Detection System using Sguil.
- Live Packet Capture with tcpdump
- Read and Analyze Packet Captures with wireshark
- Create a Snort rule
- Use Splunk to Collect and Analyze Data
- Use Incident Response playbooks to Determine the Next Steps