**Course Overview – Sound the Alarm: Detection and Response**
**Provider:** Coursera (Google Cybersecurity Certificate)
**Completion Date:** September 2025

**Overview**
This course focused on detection and response as part of the incident response lifecycle. I learned how to monitor and analyze network traffic, investigate alerts, and escalate incidents when needed. The course introduced packet sniffing, IDS and SIEM tools, and reinforced documentation practices used in SOC workflows. The goal was to practice identifying suspicious activity, documenting findings, and escalating tickets to the right level.

**Key Topics**

- Incident response process and team roles
- Network traffic monitoring with Wireshark and tcpdump
- Identifying suspicious packets and filtering captured data
- Investigating file hashes and evidence collection
- Documentation and triage during incident response
- Using IDS and SIEM tools for log and alert analysis

**Practical Applications**
Assignments included investigating a phishing attempt where a malicious attachment was downloaded and opened on a user machine. I created an alert ticket documenting the incident, noting inconsistencies in the sender's information, the malicious hash, and the presence of a suspicious executable. I spent significant time troubleshooting case sensitivity issues between the "Staff" and staff tables in pgAdmin during practice, which reinforced how important small details are in investigations. This course also introduced optional labs with Splunk and packet sniffers, which provided practice with filtering commands and analyzing logs.

**Personal Reflection**
This course strengthened my understanding of how SOC analysts detect, investigate, and respond to threats. Writing the alert ticket gave me confidence in documenting real incidents in a professional format, and I learned how to justify escalation clearly. While the course did not have the same depth of lab reports as others in the program, it still gave me valuable practice with incident handling and reinforced the importance of persistence when resolving issues.