Executive Summary — WCDN Outbreak Command Unit

The Wakanda Cyber Defense Network (WCDN) Outbreak Command Unit was established to simulate a full-scale Security Operations Center (SOC) environment designed to detect, analyze, triage, escalate, and respond to cyber outbreaks in a coordinated cloud-based defense system. As the Outbreak Triage Specialist, I played a critical role in evaluating alerts, determining urgency levels, initiating incident workflows, and coordinating with Threat Hunters, Analysts, and Command Ops during active security incidents.

This capstone simulated real-world SOC operations, leveraging AWS-native monitoring tools and structured incident-response frameworks to manage both technical findings and team communication during a multi-stage outbreak event. Throughout the project, our SOC team monitored a cloud range configured with GuardDuty, CloudTrail, VPC Flow Logs, and Security Hub findings mapped to MITRE ATT&CK; techniques. Each finding required structured triage, classification, and assignment based on impact, threat level, and required response speed.

My role centered on rapid intake and classification of alerts, ensuring that every incoming event was routed, documented, and prioritized correctly. This involved analyzing GuardDuty findings for indicators such as reconnaissance, unauthorized access attempts, credential misuse, or anomalous API activity. Alerts were mapped into severity tiers — Urgent, High, Medium, and Low — using our team's outbreak triage matrix. Each ticket was enriched with evidence, logs, and recommended next steps before being sent to the Threat Hunting or Containment teams.

Throughout the operation, the team executed coordinated workflows involving: • Detection & log correlation from AWS monitoring tools • Evidence gathering from GuardDuty, CloudTrail, and Flow Logs • Threat hunting on suspicious network behavior • Documentation of triaged incidents and escalation paths • Cross-functional communication during outbreaks • Incident containment recommendations and remediation paths

The project also required documenting multiple outbreak scenarios, including simulated exploitation, reconnaissance, privilege escalation attempts, and anomalous network traffic patterns. For each event, I completed the triage packet, validated the severity level, communicated the status to Command Ops, and provided clear recommendations for containment or further investigation.

By the conclusion of the capstone, the Outbreak Command Unit demonstrated a fully functional SOC workflow replicating real-world industry processes. This project showcased my ability to work under pressure, analyze multi-source security alerts, prioritize threats, and collaborate effectively with a broader cloud security team. It highlights readiness for roles in SOC Operations, Cloud Security, Threat Analysis, and Incident Response, serving as a cornerstone of the WCDN cybersecurity portfolio.