# Cybersecurity Capstone Netcat Project Presentation for 10ALYTICS-DC

JUDE CHIDUBEM ANYAEGBU

- **Title**: Strengthening Security Monitoring at 10ALYTICS-DC
- **Subtitle**: Detecting Unauthorized Netcat Processes with Wazuh
- **Details**:

**Presented by:** Jude Chidubem Anyaegbu

**Date:** June 18, 2025

Capstone Netcat Project for 10ALYTICS-DC

# PROJECT PROCEDURE

# Project Overview

This project addresses critical security gaps at 10ALYTICS-DC by leveraging Wazuh's capabilities to monitor and respond to unauthorized Netcat usage, a common tool for data exfiltration and backdoors."

## Content:

- **Problem:** Threat intelligence reports increased attempts to exploit systems via unauthorized tools, particularly Netcat.
- **Goal:** Enhance security monitoring using Wazuh to detect and block malicious processes in real-time.

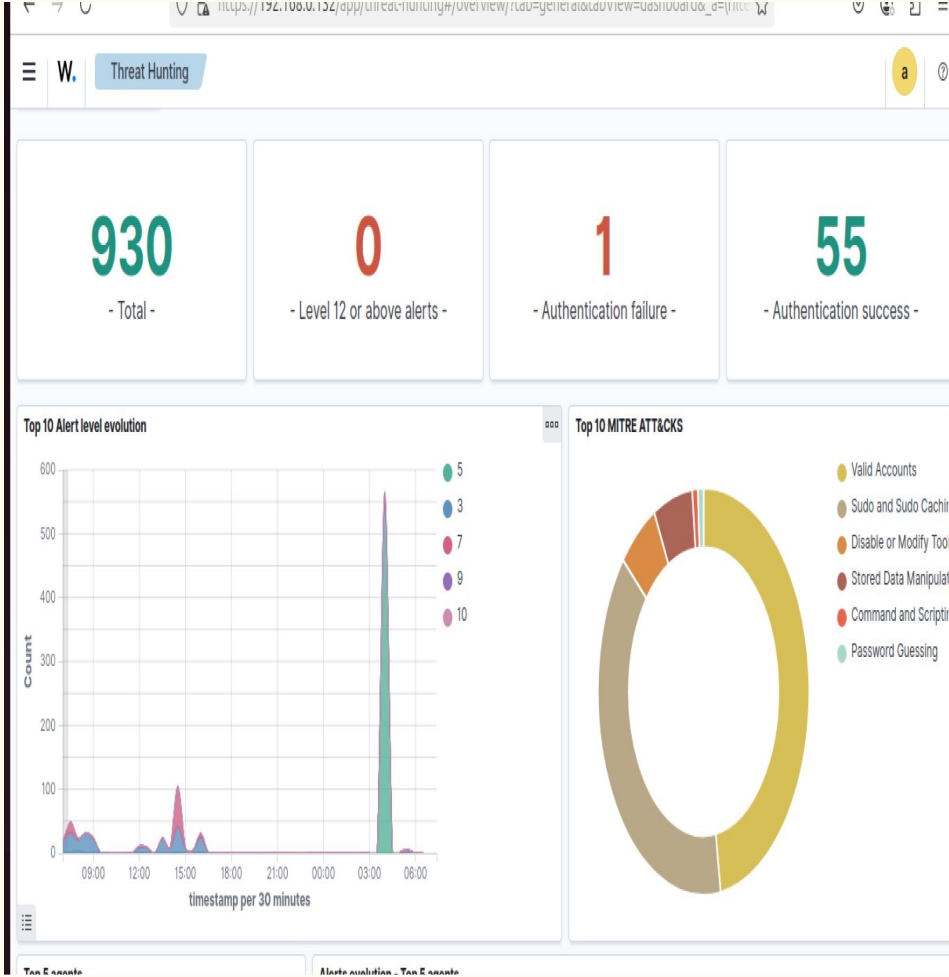
# Materials

The project was carried out with virtual machine tools listed

- Laptop
- Ubuntu VM
- Kali VM
- Wazuh VM
- Slack App
- Netcat VM

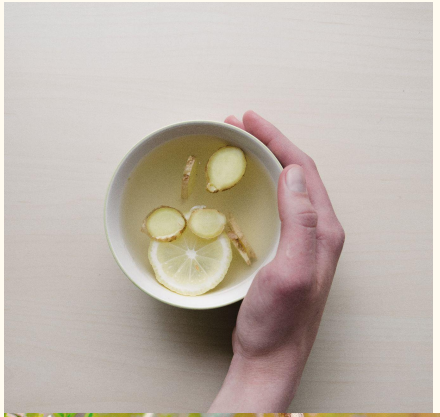
# Objectives

- Detect unauthorized Netcat processes, especially in listening mode.
- Generate real-time security alerts for suspicious activity.
- Implement active response to terminate malicious processes.
- Document findings and provide mitigation strategies.



# Methodology

1. Deploy Wazuh manager and agents on Linux servers.
2. Configure process monitoring for Netcat detection.
3. Create custom Wazuh rules for alerting.
4. Set up active response to terminate unauthorized processes.
5. Archive results and document findings.



# ACTIVE STEP

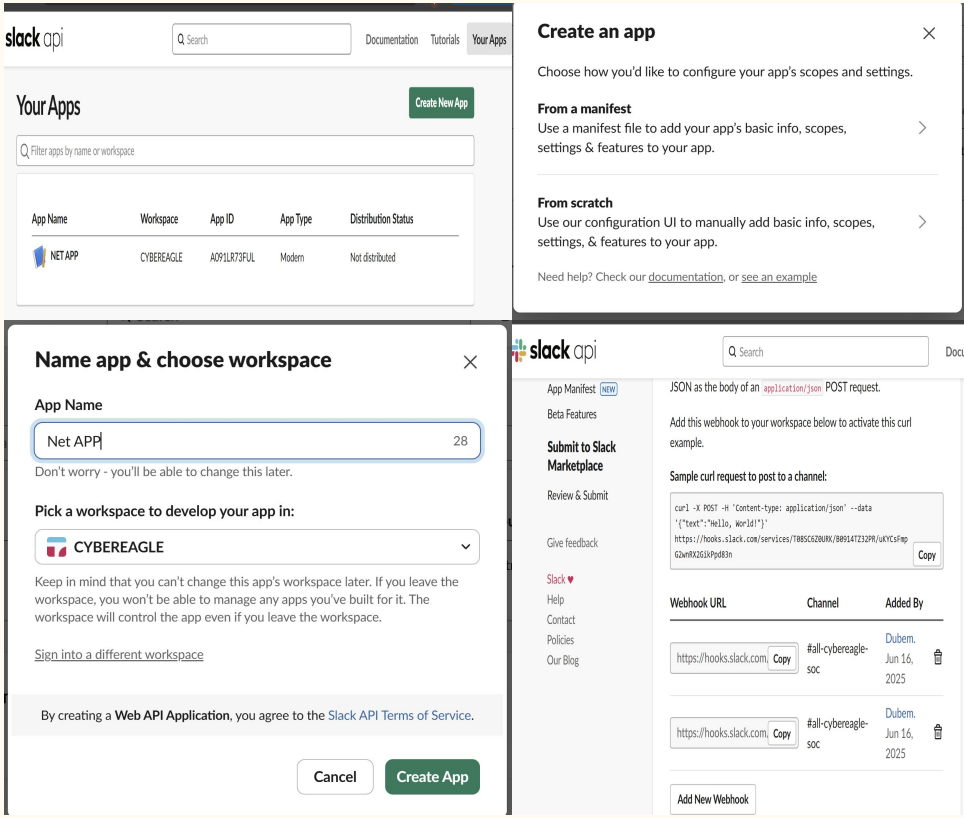
SET UP WAZUH :

- Start wazuh manager, dashboard, and Indexer, with {sudo systmctl start wazuh- ...}
- Run wazuh-manager status {sudo systmctl status wazuh-manager}
- Run {ifconfig} to confirm my ip address
- Integrate my slack app on wazuh  for real time monitoring by running {sudo nano /var/ossec/etc/ossec.conf} this action came after creating app in in slack platform
- I create Netcatcat rule after set up my wazuh agent in ubuntu {sudo nano /var/ossec/etc/rules/local_rules.xml}

# CONTINUE ACTIVE STEP

## SLACK APP SET UP

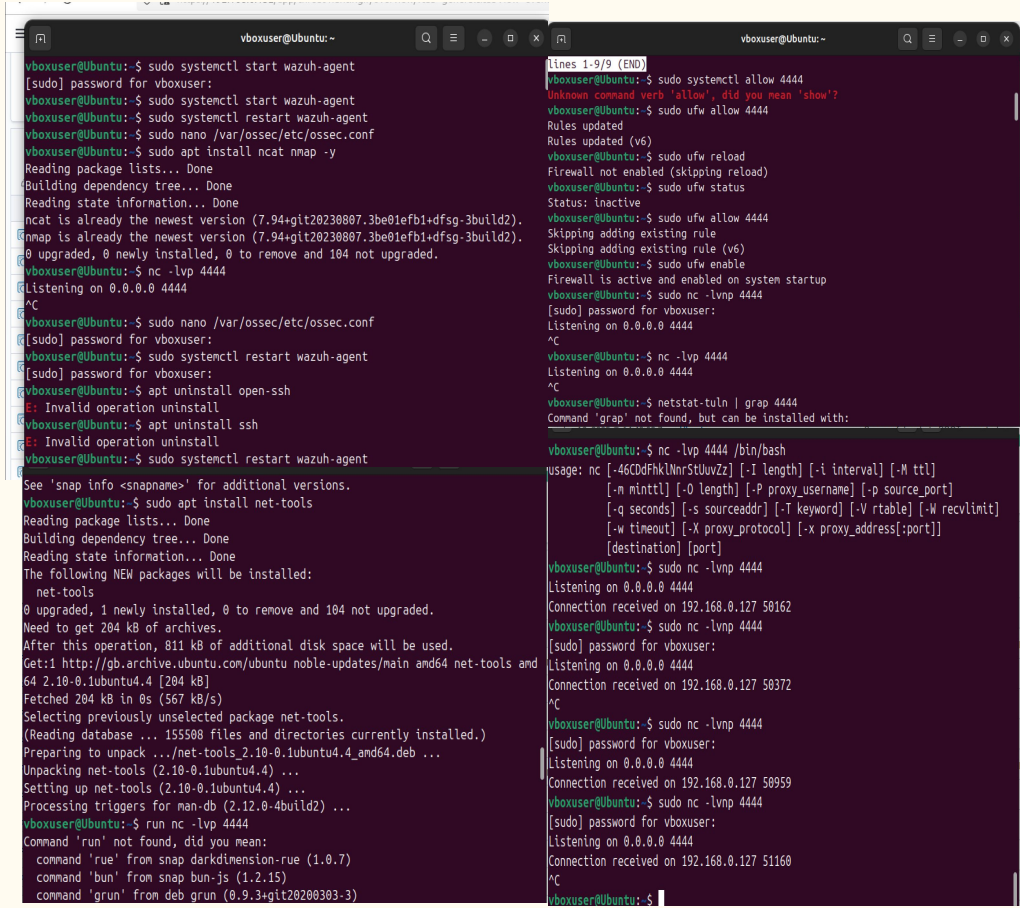
- I login to https://api.slack.com/app
- I click create a new app {from scratch}
- I selected a slack channels {cyber eagle}
- I was taken to app {besic information},
- I selected {incoming webhook} on the side bar.
- I copy webhook url of {all cyber eagle}.



CONTINUE ACTIVE STEP

# UBUNTU SET UP

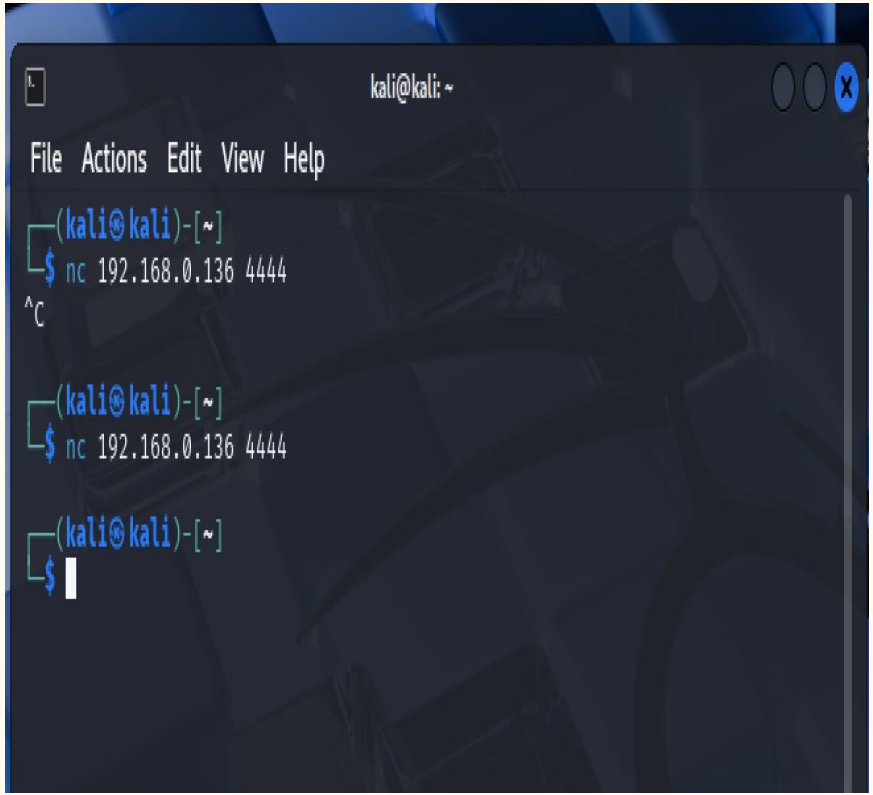
- I open ubuntu web browser to confirm my agent deployment
- I run the ubuntu terminal
- Restart my wazuh agent by {sudo systemctl restart wazuh agent}
- Install netcat { sudo apt install ncat nmap -y},
- {sudo apt install netcat-traditional} , {sudo ufw enable}, {sudo apt status ufw}
- I open up listening port in ubuntu by running { sudo nc -lvnp /bin/bash/}



# CONTINUE ACTIVE STEP

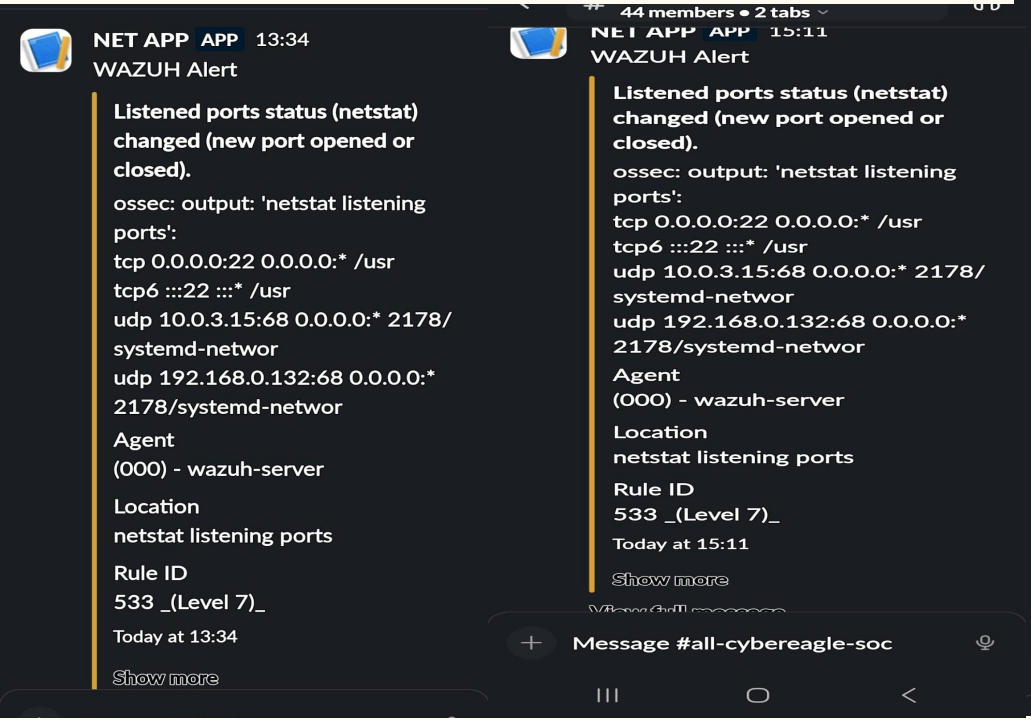
## KALI LINUX SETUP

- I open my kali linux
- I signup
- I goto terminal
- Run this command {nc ‘my ubuntu ip address’ 4444} to connect to the my ubuntu that is actively listening.



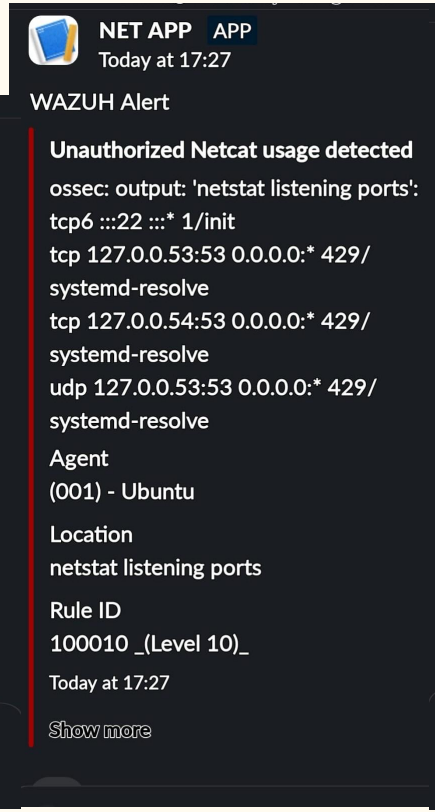
# EXPECTED RESULT

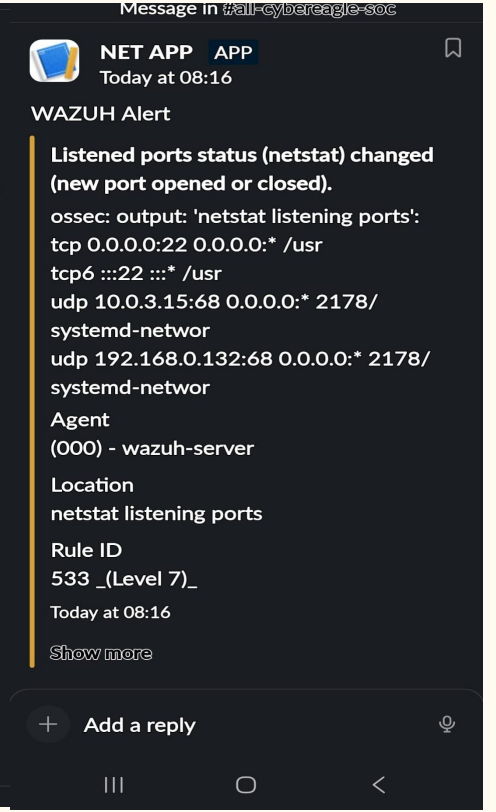
SOME OF THE SLACK MESSAGE RECEIVE.





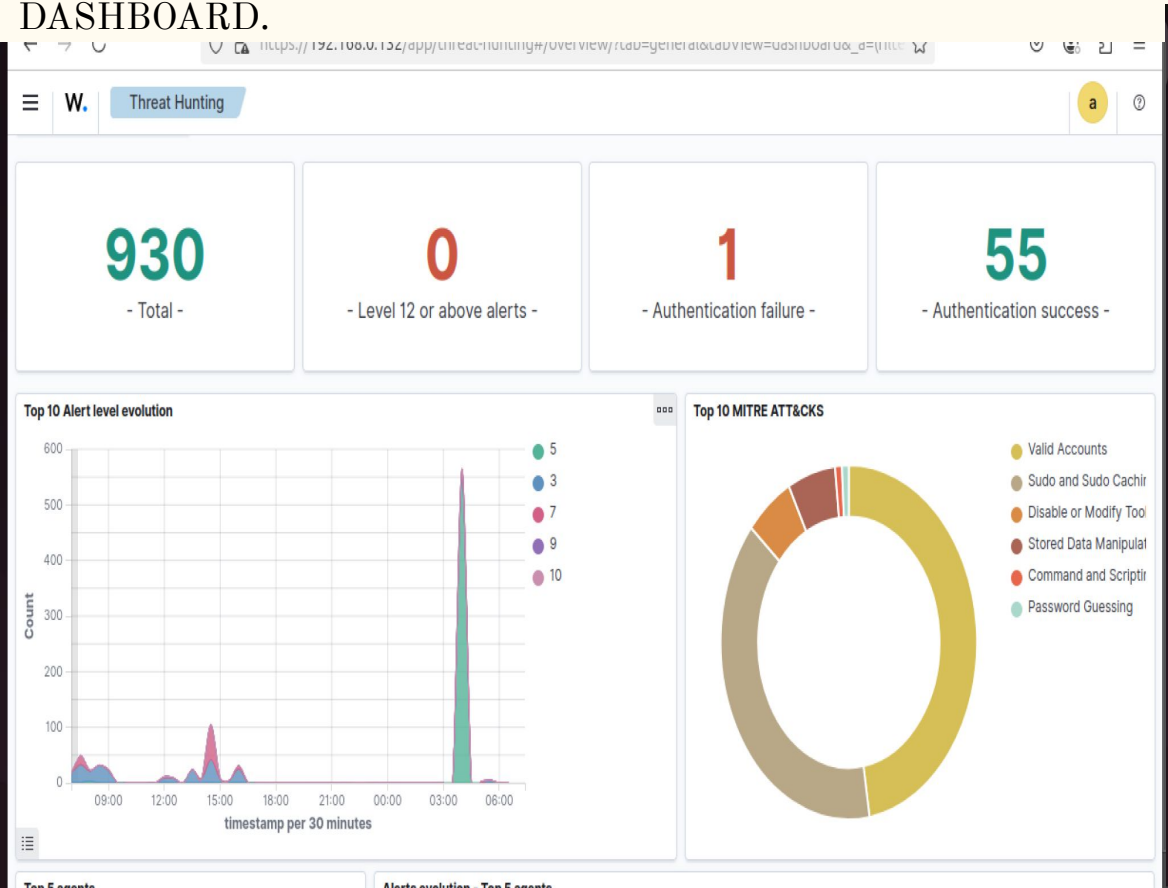


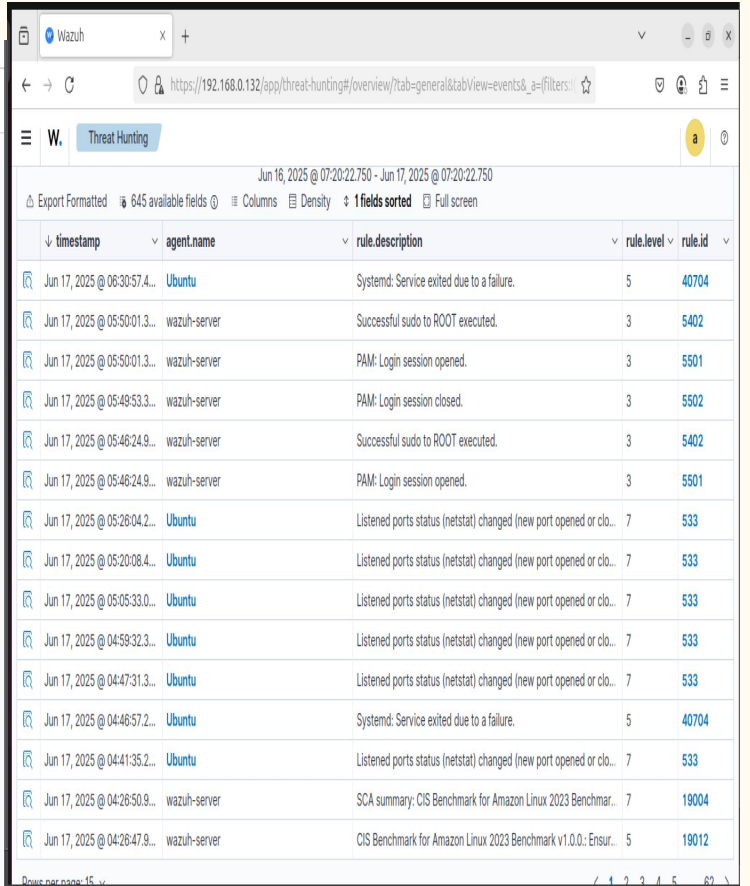


# EXPECTED RESULT

MY WAZUS THREAT HUNTING EVENT AND DASHBOARD.



# Mitigation Strategies

- **Restrict Netcat**: Remove from non-essential systems (apt-get remove netcat).
- **AppArmor/SELinux**: Restrict execution to authorized users.
- **Network Monitoring**: Add netstat monitoring in ossec.conf.
- **User Training**: Promote secure alternatives (e.g., tcpdump).
- **Incident Response**: Develop playbook for Netcat alerts.

# Conclusion

- Enhanced detection and response capabilities for 10ALYTICS-DC.
- Reduced risk of unauthorized access and data breaches.
- Blueprint for future security enhancements.
- Next Steps: Expand monitoring to other tools, integrate with SIEM.