

FACULTY OF INFORMATION

AND

COMMUNICATION TECHNOLOGY

DEPARTMENT OF INFORMATION TECHNOLOGY

**PROJECT REPORT**

**COURSE:** [ COMMUNICATION NETWORKS ]

**SUBJECT CODE:** IDC30BC

**PROJECT NAME:** High Availability Network Upgrade for WireSpeed Systems

**SUBMISSION DATE:** **10 SEPTEMBER 2021**

**PROJECT CO-ORDINATOR:** MR. Z. Mapundu

**STUDENT DETAILS:**

**SURNAME & INITIALS: MONYELA ML**

**STUDENT NUMBER : 216771877**

# INTRODUCTION

I was fulltime intern at WireSpeed Systems doing Cybersecurity internship. The geographical location for my workplace 87 Gordon Road, Northcliff, Gauteng, 2195. I was with the company from 01 March 2021 to 31 August 2021.

# BACKGROUND THE NATURE OF THE WORK PERFORMED BY MY SECTION/DEPARTMENT

Wire Speed systems is an Information Communication Technology (ICT) company that offers Next Generation Cybersecurity Solutions to private and public clientele. Wire Speed Systems offer Managed Security Services, Cybersecurity Professional Services, Outsourcing, Hardware & Software Supplies and Cybersecurity Training.

# THE DEPARTMENT OBJECTIVES

Wire Speed Systems has successfully worked with various clients in the ICT industry offering robust Security Solutions and deploying complex, state of the art next-generation Firewalls, EDR, NAC, SIEM, MDM & XDR solutions. We have managed to cultivate this through our commitment to our projects and high professionalism within our team. The Team boasts of vast experience & expertise.

Wire Speed systems focuses on both perimeter-based networks as well as perimeter less networks and the following five areas are key:

* Design, implementation, integration, maintenance, and support of Security Solutions.
* IT Security assessment, Audits and Penetration Testing.
* Security Incident Monitoring, Response & Breach response.
* Cybersecurity Forensics and Investigations.
* IT Security Governance and Compliance

# THE NATURE OF MY WORK AREA

The nature of my work area as an information security analyst is based on protecting a company’s sensitive and mission-critical data, staying one-step ahead of cyber attackers.

# A STATEMENT OF MY WORK DUTIES

My duties are to work as part of the team to monitor security access and performing both internal and external security audits.

**PERSONAL ROLE AT WORKPLACE**

# TECHNICAL DETAILS OF MY WORK

Most of the work we do, if not all the work, is very team based and very practical. My work involved Monitoring security access and investigate a violation when one occurs, security reaches and other cyber security incidents. By implementing and maintaining computer and information security systems. I monitor network to detect and suspicious or hostile activities and take measurements such as installing firewalls, to defend against malicious attacks on the systems.

# HOW I HAVE APPLIED MY KNOWLEDGE AND SKILLS

Having a prior extensive background on Cyber security and networking helped me a lot because I didn’t slow down my team trying to learn the basics, I understood what was required of when it come to do the job that I am allocated to do and being able to understand the documentation. Even if the commands were slightly different having prior knowledge acquired from Communication networks III A as well as Communication networks III B really played a huge role in my grasping the work quickly. I was well prepared by TUT that I also have good analytical and problem solving skills to access network security. I have applied my theoretical knowledge and gained experience and knowledge of new things each and every single day. I now know how it feels like to be working with the actual network security than working with the simulation programs we used at campus during our academic years.

# THE SPECIFIC DUTIES DELEGATED TO ME AND HOW I ACCOMPLISHED THEM

I was conducting periodic network monitoring and intrusion detection analysis to determine if there have been any attracts on the system. I analyse network traffic to identify anomalies and test the information security controls for weakness if malicious activity has been detected in the system. I take mitigating actions to contain the activity and minimize damage.

I also facilitate forensics analysis to determine the source of the threat. I design and implement new safe guards to protect the system. I work with my team to implement new safe guards, whether it is in the form of software, hardware or new operating procedures.

To summarise this I can say my job is to protect the network from threats and bugs that could attack the system and from the existing damages. Most importantly, I must make sure that the networking systems can bounce back or with stand any type of attack.

# HOW I WORKED WITH THE OTHER TEAM MEMBERS

Working in a team requires communication skills and because the nature of our work really encourage and expects, I have learned to be vocal and communicative. I have grown as a professional bases and still understand them. My team is very open and we all learn from each other, the learning process is lifelong and out team reflect such. We use common language or language that everyone is in the team can hear and understand and we are happy to share ideas, brainstorm together, ask for feedback and be contradicted.