

Introduction

Madiba Hudson-Quansah

CONTENTS

CHAPTER 1

INTRODUCTION _____ PAGE 2 _____

Chapter 1

Introduction

Definition 1.0.1: Security

A state of being secure and free from danger or harm, i.e. the actions taken to make someone or something secure. Protection from adversaries (those who would do harm), intentionally or otherwise, is the goal of security.

Definition 1.0.2: Asset

Anything that has value to an organization and therefore requires protection.

Some examples of assets include:

- Sensitive data (e.g., personal information, financial records, intellectual property)
- Proprietary information (e.g., trade secrets, business strategies)
- Systems and networks (e.g., servers, databases, communication infrastructure)

Definition 1.0.3: Adversary

An individual, group, or entity that poses a threat to the security of an asset.

Some examples of adversaries include:

- Cybercriminals (e.g., hackers, malware authors)
- Hacktivists (e.g., politically motivated groups)
- Nation-state actors (e.g., government-sponsored hackers)
- Insider threats (e.g., disgruntled employees, contractors)

Approaches for security

- Prevention
- Detection
- Response
- Recovery and remediation
- Policy and Mechanism