Introduction

This is a work in progress site elaborating on the concept of Deliberate Defense and what people train themselves to do and build without excessive cost.

Eventually this will be published as a book online. In addition to this site, this material can be found in PDF form and in ePub

Until the site is finished there may be downtime, wonky formatting, or cause your computer to explode.

Dedication

This site is dedicated to the memory of Darlene M. Tester.

Last Modification

- 2022-04-21T23:30:42.264595Z
- MJD 59690.979655840245

Deliberate Defense

Over the years I have been asked for the same basic advice, how do I protect myself from attackers? Hopefully this mini-book on Deliberate Defense will help people make good decisions as we explore the various attack vectors.

What is my threat model?

Everyone has a different threat model. Some people have a laptop and mobile phone and that is their work environment. Others have a small data center at home. Others work remotely and have a multi-tier network. Each person is slightly different in what they need to consider.

Threat Model Considerations

The first question you should be asking yourself is "What am I protecting against?" or what is your threat agent?

- Ex-significant other
- Corrupt Politicians
- Organized Crime
- Farmer with a Backhoe
- Untargetted Malware

- Spear Phishing
- 419 Scammers
- Cyber Warfare
- Disgruntled Employee
- Corporate Espionage

Threat Objectives

What is it that the threat agent is attempting to accomplish or gain, what is their objective?

Tactics, Techniques, and Procedures

Every threat agent has a toolbox of tactics, techniques, and procedures. These are items that they have rehearsed, purchased, learned, or otherwise gained. In the case of a phone scammer, there is typically an urgency attack from a supposed authority.

Types of Security

Each one of is an archetype for a group of countermeasures with the goal of operational security through applying protective measures. The major categories are attributes grouped as:

- Physical Security (PHYSSEC),
- Human Security (HUMSEC),

- Communications Security (COMSEC),
- Social Security (SOCSEC).