Cover story:

Welcome to ADVENTURES IN CYBERSECURITY: THE DEFENDER SERIES

Intro

I'm happy to say I'm done with Microsoft certifications (AZ104/AZ500/SC100) and as a result, I've put some effort into a blog series that hopefully will entertain you with some of the topics around cybersecurity. As a security consultant/architect I work with all the subjects I'll be discussing, so there will be use-case examples presented that help explain some of the topics in a real-world sense.

Red, Blue, Purple?

All the topics discussed are 'Blue Team' related, there will be little discussion around 'Red Team' topics like pen testing and exploiting vulnerabilities.

Who are these posts for?

These blog posts are intended for the following audiences:

Security Architects – several security frameworks are discussed.
Security Admins – there are labs for most of the posts in GitHub.
Security Auditors – every post is mapped to several compliance controls in a spreadsheet format that you're welcome to download and share.

Is there anything other than blog posts here?

Many of the posts are accompanied by a **lab** (in GitHub) with instructions for getting started with the presented topic and/or technology.

Each topic is mapped to relevant **compliance controls** (for our auditor friends). This table can be downloaded from GitHub **<here>**.

Fun You Say? Labs!

For "fun", there will be a backstory to accompany the labs:

"ZPM International: Architecting Security Defenses Against APT 42a"

Outro

I hope that the audience will provide feedback and expand on the topics presented.

The combination of posts, labs, and audit tools is intended as an easy getting-started path for some important security topics.

Thanks for your interest.