Security Frameworks

Objectives

- Discuss the types of frameworks out there
- Discuss which one might work best in which cases
- Explain where to find them and how to use them

What Are Frameworks?

- Frameworks are standards that can be followed to enhance and validate your security posture or processes
- Frameworks are generally well tested and reviewed thoroughly by many people that are in the industry

How Frameworks Can Help

- Since frameworks are tested and vetted by many users and organizations over time, they are proven standards to abide by
- Think of frameworks as a map. The map tells you how to get to places, explains points of interest, and tell you how to avoid certain areas
- Frameworks will point you in different directions on how to comply with security
- Frameworks are sometimes also required to be followed because of industry standards
- Frameworks can also help you communicate effectively to executives in an enterprise setting

Types of Frameworks

- Industry Based Frameworks – Designed to be a broad set of rules and guidelines that allows you to protect certain industry based architectures
- General Frameworks – Designed to apply to almost any industry. These are the most widely adopted since in an enterprise we can pick and choose what we want to follow within the framework

NIST Frameworks - 1

- The National Institute for Standards and Technology (NIST) has many frameworks out there.
- These are special publications that have been a standard for many years.
- They are very easy to follow and have different levels depending on what type of compliance or rigor you need.

NIST Frameworks - 2

- NIST Cybersecurity Framework
  - Aimed at protecting critical infrastructure
  - One of the best frameworks to follow and easy to adopt
- NIST SP 800-53
  - Security and Privacy Controls for Federal Information Systems and Organizations
  - Broken down into security controls
  - Comprehensive
- NIST SP 800-171
  - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
  - Much easier to follow than 800-53

ISO 27001 and 27002 Frameworks

- The international Organization for Standardization
- Provides a comprehensive framework for security controls
- 27001 – Information security management systems
- 27002 – Code of practice for information security controls

- Easier to follow than some NIST publications, but last update was in 2013.

CIS Framework

- Center for Information Security
- Framework is Critical Security Controls (CSC)
- Designed to cover many different sectors of industry
- Power, Defense, Transportation, Finance, etc.
- CIS also has controls that you can put into some software to test if you are complying with the framework
- Lesser known and adopted

Industry Frameworks

- HITECH – Healthcare in the US
- PCIDSS – Worldwide credit card compliance
- DFARS – US military contracts

How do I choose?

- Choosing a frame is as simple as, what do you think you can follow?
- Some frameworks are hard to comply with
- Some frameworks are meant to be implemented fully
- CU chose NIST 800-53 years ago. It took us nearly 3 years to write ours. We chose the controls that we thought we could all follow
- Benefit of using NIST 800-53 is there are high, medium, and low categories.
- You don’t have to think up this stuff on your own! There is a map!