SecDSM Tool Talk

Spider Chart

Agenda

➔   Background
➔   Uses/Examples
➔   Thoughts/Questions

Before we begin…..

Thx to sponsors, organizers, etc.

Request of the group - speakers/presentations pls!

- Iowa is full of InfoSec talent
- We all know people who would be good speakers
- Pair-up

Background

Sometimes, we are selling things people don't want to buy.

Sometimes, we are explaining complex things to people in puffy chairs and we don't have a whiteboard or crayons available.

Sometimes, we have *1* opportunity to communicate and gain support with key leadership and/or stakeholders
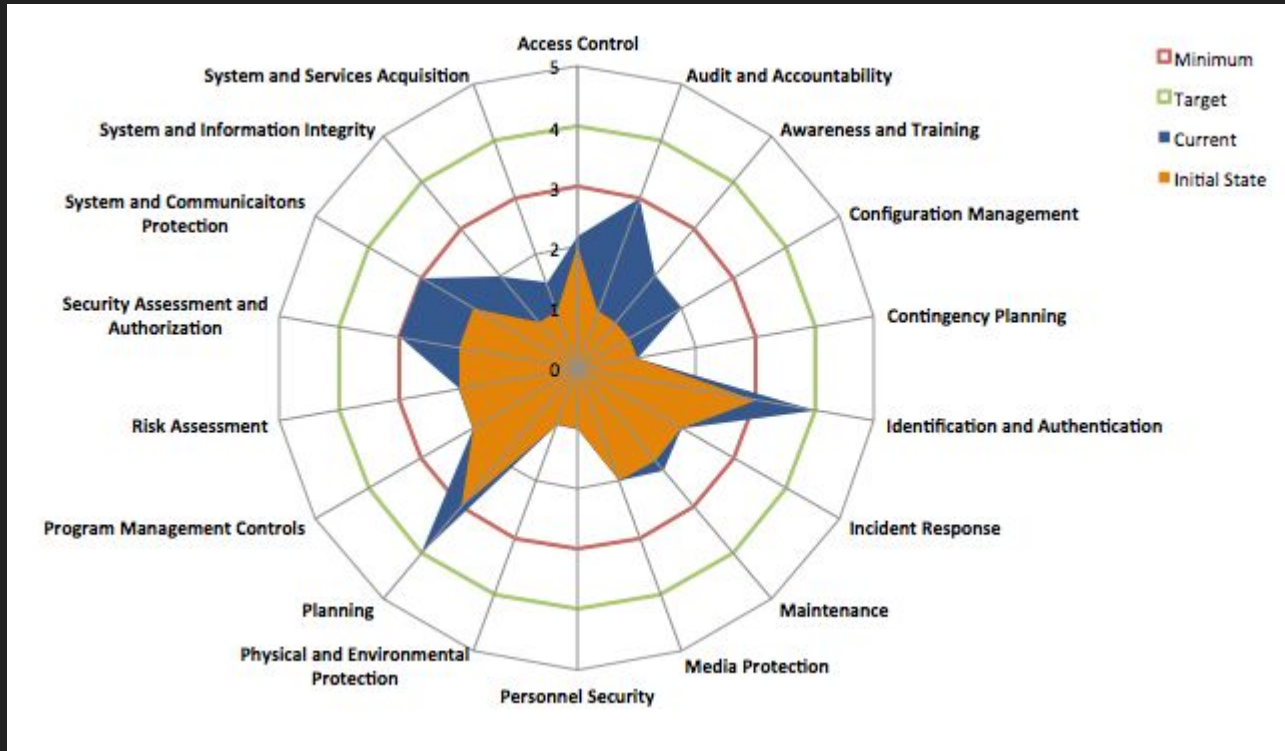
This story starts in Denmark...

One chart to show where to invest in InfoSec

Recipe:

- ● We need colors
- ● We need simple ratings (0-5)
- ● We need to show past and current states
- ● We need to show targets

Spider Chart (sample data)

Excel Chart - nothing special

Detailed tab - collection of controls as columns with 0-5 ratings

Ratings based on COBIT maturity model

Aggregate tab - before and after table which generates chart and targets/guard rails

Thoughts

- Can easily get cluttered - don't add more than 20 controls or use too much text
- Regression (moving backwards) - can be shown but needs thought
- Control families are averaged - individual outliers may be missed; families with different numbers of controls may need consideration
- Trending over time can be shown but will require more data and gradients - this is an exercise left to the reader
- This is the start of your story - give your audience time to read the chart and ask questions before you move forward. This chart can sell itself - let it and be well prepared for questions.
- .xlsx shell with sample data to be posted - have fun

Bonus Slides

NetFlix has an outstanding open source collection of tools - Sketchy is one of them

What is Sketchy?

Sketchy is a task based API for taking screenshots and scraping text from websites.

What is it used for?

When a phishing email or other alert requires investigation, how do you safely collect this information especially from an unknown web address?

- Use a browser - YOLO?
- wget/curl - because reading HTML and obfuscated JS is such fun
  - Vulnerabilities - wget RCE (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4971))
- How do you scale this, how do you automate?

Just show me screenshots

Final thoughts

https://github.com/Netflix/sketchy

A docker container is available for quick, non-production testing

This is built to scale - recipe is very Ubuntu specific

Can demo later if there is interest - bigtime thx to NetFlix team for this and other great solutions