Pacific Northwest
NATIONAL LABORATORY

PNNL-30242

Charting the unknown

A dive into the world of standards mapping

August 2020

Matthew J Mincey

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov

PNNL-30242

Charting the unknown

A dive into the world of standards mapping

August 2020

Matthew J Mincey

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Abstract

When you hear standards mapping what do you think about? For the Secure Software Central (SSC) project this means comparing our process to the National Institute of Standards and Technology's (NIST) security control catalog. So how is it done? The project completed this summer can be broken down into three simple phases. Phase one consists of mapping the SSC process to the NIST's security control catalog. While phase two entails mapping mitigations from a threat profile to NIST. Lastly phase three requires the creation of a knowledge base allowing for the reuse of controls across numerous projects.

This project presented a few different challenges: locating the correct control within the NIST catalog while correctly matching the proposed mitigations from the SSC team, accurately leveling the mitigation to the security level of the system, creating a toolbox to showcase a dataset of mitigations and standards to be used in current and future projects. each challenge allowed for opportunities in growth and understanding of how security controls can map to a governing set of standards. These standards maps are a crucial element to support the insights provided by the SSC team and allow the client to have confidence in the work being completed.

My internship has allowed me to set and achieve many goals such as coming to understand that the field of cybersecurity truly is the right place for me. I have also learned that it's ok to be wrong if you learn something from it. For significant accomplishments I have helped integrate standards mapping into the fabric of SSC. The field experience that I have gained such as interacting with the SSC team along with other senior staff and building a good rapport are crucial skills to. This time at PNNL has been an irreplaceable experience.

Acknowledgments

This work was supported in part by the U.S. Department of Energy, Office of Science, Office of Workforce Development for Teachers and Scientists (WDTS) under the Science Undergraduate Laboratory Internships Program (SULI)

Torri Simmons (Administrator)

Patrick O'Connell (Cyber Security engineer)

Chance Younkin (Cyber security engineer)

Acronyms and Abbreviations

CIS- Center for Internet Security

HIPPA- Health Insurance Portability and Accountability

ISO- International Organization for Standardization

NIST- National Institute of Standards and Technology

SSC - Secure Software Central

Contents

Abstract....3
Acknowledgments....4
Acronyms and Abbreviations....5
Contents....6
1.0 Introduction....7
2.0 Phases of the Process....8
2.1 Phase one: process mapping....8
2.2 Phase Two: mitigations mapping....8
2.3 Phase 3: toolbox creation....9
3.0 Conclusion....10
4.0 References....11

1.0 Introduction

In the world of risk assessment, one thing reigns supreme: assurance. Assurance is key between client and assessor. What is assurance in this case: assurance is the trust between an assessor and client that the services, such as mitigation recommendations and threat surveillance, etc. the assessor provides will benefit the system in a cost-effective way. One way to build trust in a risk assessment is by mapping it to industry-accepted standards. Standards mapping is when an assessor compares their process to standards set out by an authoritative body such as the National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO) and integrates the matching standard into their process.

Secure Software Central (SSC) at PNNL is interested in doing this. SSC provides services to provide threat-based software analysis (threat modeling), secure design, and secure code review. The focus of the project was to map SSC processes to an accredited set of standards, thus giving assurance of the quality of the work. Its second goal was to also map mitigations from a threat profile to NIST security control standards, thus creating a security baseline. That then spun into creating a multi-use standard-compliant toolbox. This project posed many challenges along the way and most without straightforward solutions; in one case it was like exploring an unknown world. Along with challenges were many lessons learned in both my line of work and my conduct. With a project of this size and scope, it's best to break it down into phases.

2.0 Phases of the Process

2.1 Phase one: process mapping

The project began with research into numerous standards from the Center for Internet Security (CIS), NIST, and ISO. Early on NIST proved to be the optimal starting point because it is the most well-known of the standard creating entities, and for its diversity in controls and enhancements. Most of the work in this phase was simple due to revision 4 of the NIST security Standards catalog being so comprehensive with its security control catalog and an included ISO standard map for that extra bit of assurance. This research led to one of the more intriguing parts of the project-- mapping our process to NIST. This portion was fascinating because of how focused our process was around a single standard. The part that became the core of our practices shared names and details with the standard and was also a big part of our work within SSC in general. Possibly the biggest challenge from this portion to me was figuring out what NIST security standard fit best to the SSC process as what became the main standard was not apparent during the first few iterations of the map. But thanks to a second perspective it made the most sense to group most steps in the process under that single standard. The most intriguing challenge from this project, in general, was the potential of expanding the process of SSC. The process is still relatively new, which means that new steps can be added easily with decent reasoning or entirely new areas of the process. The challenges of incorporating acts such as the Health Insurance Portability and Accountability Act (HIPAA) into our process for compliance reasons popped up after a review of the work done. This was a great idea for showing off an extra layer of compliance within our process. The acts that applied were already tied to NIST or vaguely touching on it and coming up with the reasoning that didn't sound redundant or flimsy would be a challenge. While this phase was the easiest out of the three, the next phase was the most challenging of them all.

2.2 Phase Two: mitigations mapping

Then came the mitigations mapping where it was necessary to translate and match our mitigations to NIST standards. This was a far bigger challenge due to our mitigations running a gamut of scopes and controls. When looking through over a hundred controls and possibly hundreds of enhancements, it's a challenge to find which standard or standards encompasses each mitigation's parts. This was because some mitigations were multi-step processes unto themselves and the controls that fit the whole mitigation weren't even a part of a single-family one of the best examples of diversity in how the controls from the catalog map to SSC's mitigations is the mitigation tied to the threat of a key component crashes, halts, stops, or runs slowly; in all cases violating an availability metric. Whose mitigation deals with the configuration of an automatic recovery system. The mitigation is a combination of two different controls from different control families. The first from the System and Communications (SC) control family within the NIST security control catalog. NIST defines the control as follows "Failure in a known state addresses security concerns in accordance with the mission/business needs of organizations. Failure in a known secure state helps to prevent the loss of confidentiality, integrity, or availability of information." (Transformation Initiative, 2013) the second control for this mitigation comes from the System and information integrity (SI) control family. NIST defines this control as follows "Fail-safe procedures include, for example, alerting operator personnel and providing specific instructions on subsequent steps to take." (Transformation Initiative, 2013) The translation process became somewhat easier from that point on. However, one area was still a challenge due to its diverse range of mitigations, that is how the threat profile became something closer to a security baseline. A baseline in this context is something that is like a

cost-effective mitigation recommendation set. For example, recommending something like a high-tech security system to protect a common pencil cup, just doesn't make any financial sense. Whereas recommending locking your office door before leaving makes far more cost-effective sense. The baseline presented a unique challenge compared to the other phases. This challenge stemmed from the NIST standards we were mapping them to in the sense that not every standard fit in each baseline and some even require advanced controls. These challenges appeared in two distinct forms: the first being over half of the mapped standard being attributed to a high-security baseline, which did not even begin to fit the system for which the threat profile was developed. As was the case with a good thirty to forty-five percent of the controls had no baseline data. The second challenge was mapping web app mitigations. This was due to the 4th revision age at this point is 7 years old. It had a decent understanding of web apps for its time but never explicitly mentions them in any fashion. The process has expanded significantly and better defined in the years following in its 5th revision, making it much easier to find but still not in an entirely usable state due to it still being a draft and lack of presence.

2.3 Phase Three: toolbox creation

This idea then leads to what I considered to be the most confusing part of the project -- an all-purpose mitigation toolbox with the single-use translation becoming akin to a prototype. The challenge from this portion was figuring out how to generalize the tools. This is because each scenario is unique and not every tool can be applied universally no matter how general it may be. For example, UNIX tools are similar but different enough from the Windows or MAC tools that there are bound to be something that just doesn't work universally for each configuration. In this case, many of the mitigations were tailor-made for that profile with most only containing pieces that could be generalized but only a scant few that could be taken over as general mitigation. Another big challenge was potentially implementing more sets of standards into the toolbox. It was a challenge figuring out how to implement it due to their obtuse nature in comparison with the other standards mapped previously because of its main purpose being tied mostly to mitigations and attack vector descriptions which could work in the toolbox. We decided that for now, we would leave that be.

3.0 Conclusion

This project's scope ballooned in a way I believe no one was expecting but on the same token, it was truly for the best. Starting with the relatively straight forward task of standards mapping with the few challenges and many key lessons it provided. The biggest lessons I learned from phase one of the project are do not be afraid to ask for help from members of your group. Do not rush ahead. Reviewing your work is also a key part of the mapping process. Finally, don't be afraid to ask questions. You can't learn if you don't ask. Phase two was most certainly the most challenging due to the sheer amount of mitigations that needed to be mapped. The lesson learned from phase two was not to fear making mistakes or being wrong, just take the feedback and learn from your mistakes. Phase three lead to the generalization process of the tools at our disposal, which was somewhat mysterious in the beginning but became the second easiest part of the entire project overall and an intriguing endeavor. Phase three's biggest lessons were don't overthink things because that just causes unnecessary complications. The second biggest lesson was what may sound good on paper doesn't always translate well into practice. Personal lessons are not the only thing I've learned. This whole process has been about adapting; to a new environment that is teleworking -- adapting to online meetings, such as learning how to lead them and how to schedule them, adapting to working with others, and developing a good rapport with my coworkers. Looking at the SSC project in the long term this was a great direction to go for the sake of futureproofing and streamlining the standards mapping process, which will become key to future threat profiles and SSC ensuring assurance. It makes me proud and grateful to have been part and to be given such a great privilege to experience the development of PNNL's Cyber Security division.

4.0 References

Transformation Initiative, J., 2013. *Security and Privacy Controls for Federal Information Systems and Organizations*. 4th ed. [eBook] N/A: National Institute of Standards and Technology, pp.359, 390. Available at: <http://dx.doi.org/10.6028/NIST.SP.800-53r4> [Accessed 7 August 2020].