Chad Ballay

CYBR 450-342N

12/10/2020

**Week 3 Milestone**

**Title**

Enterprise Secret Storage: Selling and Adopting

**Bibliography**

Forsgren, N., Humble, J., & Kim, G. (2018). Accelerate : the science behind DevOps : Building and Scaling High Performing Technology Organizations. Portland: IT Revolution.

*Chapter 6 contains most of the relevant material. Covers shifting security to the left of the software delivery lifecycle. Later chapters reference continuous delivery gains but not sure how to fit that in.*

Hashicorp. (2020). Unlocking the Cloud Operating Model: Security. Retrieved from Hashicorp: https://www.datocms-assets.com/2885/1597082390-vault-com-security-whitepaper-v2-digital.pdf

*They’ve done the hard work of explaining the how and why secret management is needed. I will use this mainly to introduce the framework they use of Adoption, Operationalizing, and Scaling. My focus is on the first two but all three are relevant*

Kovacs, E. (2017, 01 09). "Truffle Hog" Tool Detects Secret Key Leaks on GitHub. Retrieved from Security Week: https://www.securityweek.com/truffle-hog-tool-detects-secret-key-leaks-github

*Specific example of one mechanism to start using for building metrics on if things are bad and if things are getting better. Iffy on specifics but using a digestible article that covers the highpoints.*

Marlow, P. (2019). Finding Secrets in Source Code the DevOps Way. Retrieved from SANS Reading Room: https://www.sans.org/reading-room/whitepapers/securecode/finding-secrets-source-code-devops-38985

*Referencing as a case study on implementing code scanning. Will be using to argue the need to focus on building metrics to drive adoption rates.*

Surowiecki, J. (2005). The Wisdom of Crowds. New York: Anchor Books.

*Part of my case is that we should move fast by adopting best practices already in existence and that where we are out of alignment with the industry that we should shift to get into alignment. Rather than walk through why secret management is needed, why Vault was chosen, or why DevSecOps practices will have to be adopted I’m going to use this to make the case for me.*

Wiggins, A. (2017). Retrieved from The Twelve Factor App: https://12factor.net/

*References to coding best practices. Secrets and configs often overlap so will use the config factor to show the awareness that this needs to be removed out of the source code.*