Secure Software Operation Methodologies: Using Automated Tools for Optimal Design and Integration

Sean Carroll

Villanova University

"This paper or presentation is my own work. Any assistance I received in its preparation is acknowledged within the paper or presentation, in accordance with academic practice. If I used data, ideas, words, diagrams, pictures, or other information from any source, I have cited the sources fully and completely in footnotes and bibliography entries. This includes sources that I have quoted or paraphrased. Furthermore, I certify that this paper or presentation was prepared by me specifically for this class and has not been submitted, in whole or in part, to any other class in this University or elsewhere, or used for any purpose other than satisfying the requirements of this class, except that I am allowed to submit the paper or presentation to a professional publication, peer reviewed journal, or professional conference. In adding my name following the word 'Signature', I intend that this certification will have the same authority and authenticity as a document executed with my hand-written signature.
Signature Sean Carroll"

Abstract

This paper explores current automation tools implemented into secure software operation. The articles analyzed focus on the issues encountered with such methodologies when implemented. The current role of the information technology sector within a company is one that is changing rapidly and increasing in demand. The increased risk and complexity of software mandates that secures software practices and information technology groups are expanded. With this expansion, the integration of security operation centers (SOCs) and their expansion with automated tools is seen as a common approach to address the issues of secure software operation throughout its development lifecycle. The development of an optimal secure software operation methodology is one that integrates information technology, SOC, automation tools, and communication with business interests to ensure effectiveness.

Secure Software Operation Methodologies: Using Automated Tools for Optimal Design and Integration

The difficulty in outlining a secure software operation methodology is that general methodologies cannot simply meet optimal integration. The implementations of such optimal secure software operation practices are very business-specific, as the goals and tools to automate such optimization will vary depending on the needs and functions of the business discussed. Fortunately, the requirements and approach to design of such a methodology is similar, as the challenges of finding automation tools that assist in operation is a common challenge.

Literature Review

The use of Security Information and Event Management (SIEM) software is often treated as a synonymous with the design of a secure software operation methodology. Because such software provides many different security functions to a SOC, the difference between the two concepts is often misunderstood. Although a SIEM software solution could potentially perform many of the tasks needed by a SOC, it does not successfully encompass and solve the task of creating a methodology needed in the above-mentioned case. Nabil, in his 2017 research article titled, "SIEM Selection Criteria for an Efficient Contextual Security," outlines such flaws in current SIEM solutions. Nabil's research discusses the importance of deciding on the optimal tool to fit a certain organization's environment. OSIMM AlienVault, Elk Elastic, and Logpoint are three current SIEM solutions that are compared among technical and functional criteria. Nabil's research shows that the tools vary widely in categories of integration, reporting, documentation. However, Nabil asserts in his research that each SIEM solution shows difficulty in analyzing the overall risks facing a company, and that the overall analysis is limited due to the limited data collected. John's 2017 research on the "State of the Art Analysis of Defense

Techniques Against Advanced Persistent Threats" takes into consideration that a hybrid system that implements full coverage of secure software operation is optimal in pursuance of an optimal methodology. John's article lists a comparison of industrial solutions in his second table, where six features are addressed: network flow analysis, NIDS, threat intelligence, automatic correlation, deep package analysis, and sandboxing. John discovered in this analysis that the integration of THOR, TrendMicro DeepSecurity, Kaspersky SOC, and Symantec Endpoint Apt Protection would cover all industrial features, however such an implementation is unrealistic in terms of cost. It is clear that a balance between cost and secure operations must be considered when designing a secure software operation methodology for a specific environment.

Discussion

The current platform designed by Feng in his 2017 research shows the issues of implementing a rule-based system for flagging and mitigating threats to a system. SIEM functions upon a correlation concept to generate the risk levels of threats that are currently seen through analysis of systems logs. It is clear that a secure methodology would improve upon the current system. It should be noted that machine learning analysis of such correlation concepts, where neural networking was used, saw a marked improvement on threat detection in Feng's research. Bhatt's 2014 article on "The Operational Role of Security Information and Event Management Systems" contributes to this idea of machine learning. Bhatt mentioned that there is a certain point at which IBM's machine learning system will become overpowering in such a way that security advisors cannot deduce decisions based on automated analysis. With such SIEM systems that John deduced from his research, it appears that an optimal level of automated analysis is needed for developing a secure software operation methodology. A further balance is seen when it is written, "Communicating the right kind and amount of information between

enterprise operations and the SOC in an automated way is essential" (Bhat, 2017). It is often with automation that roles are still needed in guiding optimal progress. Communication between parties will often still necessitate qualified individuals to monitor and guide automated tools towards optimal operation practices.

Conclusion

A hybridization of automated tools must be selected in such a fashion that addresses the needs and demands of a specific work environment. It is clear that in terms of communication, the connection between IT, SOC, business management, must be optimized to achieve an optimized methodology for secure software operation. The automation of practices using tools requires the guidance of trained individuals, in order for an operation methodology to reach desired goals throughout phases of the development lifecycle. Mitigating threats and patching vulnerabilities can be optimized using automation tools and SIEM software solutions. Developing a secure software operation methodology requires qualified individuals to select solutions that optimizes both the implementation of automated tools and the communication between collaborating departments.

References

Bhatt, S. (2014). The Operational Role of Security Information and Event Management Systems. IEEE Security & Privacy, 12(5), pp. 35-41. doi:10.1109/MSP.2014.103

Feng, C. (2017). A user-centric machine learning framework for cyber security operations center. 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 173-175. doi:10.1109/ISI.2017.8004902

John, T.J. (2017). State of the Art Analysis of Defense Techniques against Advanced Persistent Threats. Seminar Future Internet SS2017 of Technische Universität München. https://doi.org/10.2313/net-2017-09-1_09

Nabil, M. (2017). SIEM Selection Criteria for an Efficient Contextual Security. *2017 International Symposium on Networks, Computers and Communications (ISNCC),* pp. 1-6. doi:10.1109/ISNCC.2017.8072035