Brian Sowers

12/17/2022

Site Reliability Engineering and SOAR

1. Explain in your own terms why a SRE would focus on the connections between the components within the system as much as focusing on the components themselves.

Software Reliability Engineering (SRE) is “a discipline that incorporates aspects of software engineering and applies them to infrastructure and operations problems with a goal of creating scalable and highly reliable software systems” (Secure Business Operations Module 4, 19). Software and systems engineering are two important subject-matter within the SRE role, and SREs tend to be assigned to work with one or the other. However, knowledge in both these areas are necessary to make an effective SRE. Hence, a SRE will focus on the connections between the components within the system as much as focusing on the components themselves. “Understanding the interactions between each system element is critical to building or troubleshooting systems that scale. Decisions about how communications are passed between the elements can have extreme effects on the overall stability of the system” (Hixson and Beyer, 41). For SREs to adequately scale software systems, the components within the system need to work seamlessly to create a reliable system. Further, the components themselves need to work seamlessly within itself to ensure portability and adaptability when/if these individual components are integrated with others. A software engineer will approach a problem with a different framework of solutions than a software engineer will. Given the purpose of the SRE role, the different problem-solving approaches prove invaluable to the SRE. Google, understanding SRE's value, takes advantage of these problem-solving frameworks sooner rather than naturally letting the two approaches combine later. "At the apex of the Silicon Valley job ladders, the SE and SWE jobs merge back together, since the largest and most complicated software problems cross so many disciplines and technologies that the leaders of such projects need to understand how all of their components fit together" (Hixson and Beyer, 42). If these nuances in the software system are not understood, small issues can snowball into larger ones. Since systems are increasingly complex and highly interconnected, an issue in one area can impact multiple related components.

2. Consider Quality Assurance. Where would you expect to include Regulatory Standards Compliance when Diagramming future applications or solutions subsystems?

SOAR

In the energy sector, I would expect regulatory standard compliance with the North American Electric Reliability Corporation (NERC), as they have become "increasingly concerned about cyber threats" (Smith, 377) from malicious actors and cyber hackers. Since the US Federal Energy Regulatory Commission (FERC), the independent regulator that supervises NERC, has ordered NERC to expand cyber threat incident reporting by transmission operators and owners of power plants (Smith, 377), I would expect NERC to enforce regulation on incident response and reporting. This would be important when diagramming a new solution such as a SOAR platform that manages incident response, incident investigation, and report making, so that my organization remains compliant with NERC.

1. Automation. Explain two governing criteria when deciding upon candidates for security automation.

The two governing criteria while deciding upon candidates for automation are

1) How long the task takes and
2) How often the task must be performed (The State of SOAR Report 2018, 16).

When considering these questions for candidacy, it is important to consider which tasks would be best served by automation. If the tasks are lengthy, of low severity or importance, must be performed frequently, and have repeatable iterative steps, then that task is an excellent candidate for automation. If the task is circumstantial, contextual, occurs infrequently, and requires a degree of risk management, then that task is best served by human decision-making.

2. Orchestration. Evaluate how process update frequency impacts playbook design. What future playbook design elements would you implement in order to reduce the impact of frequent updates?

Considering security analysts suffer from alert fatigue, are pressed for time, and do not usually update their IR processes, I would use a security orchestration, automation and response (SOAR) platform. Consider this statistic: “50% of respondents either didn’t update IR processes at all or updated them infrequently” (The State of SOAR Report 2018, 20). This lack of update suggests that these updates need to be updated manually, which takes time that security analysts do not have. When updating processes, security analysts need to identify gaps in processes that need to be resolved. It is better to automate this step. “SOAR platforms will not only improve process speed through automation, but also enable the iterative improvement of processes through proper metric capturing and visibility of process gaps and potential improvements” (The State of SOAR Report 2018, 20). Demisto, a SOAR platform, “enables security teams to ingest alerts across sources and execute standardized, automatable playbooks and features machine learning capabilities that enable more efficient security operations by providing personalized insights” (Secure Business Operations Module 4, 40). These automations, machine learning capabilities, and personal insights will reduce the process update workload for security analysts so that they may better allocate their time elsewhere.

Works Cited

Beyer, Betsey and David Hixson. “The Systems Engineering Side of Site Reliability Engineering.” *SYSADMIN.* http://panacademy.net/CourseFiles/sbo/Systems_Engineering_Site_Reliability_Engineering.pdf. Accessed: 17 December 2022.

“Secure Business Operations Module 4”, https://s3.amazonaws.com/assets.paloaltonetworksacademy.net/sbo/Business_Operations_Module_4.pdf. Accessed: 17 December 2022.

Smith, Don. “Enhancing cybersecurity in the energy sector: a critical priority.” *Journal of Energy & Natural Resources Law.* http://panacademy.net/CourseFiles/sbo/Enhancing_Cybersecurity_Energy_Sector.pdf. Accessed: 17 December 2022.

“The State of SOAR Report 2018.” *Demisto,* http://panacademy.net/CourseFiles/sbo/SOAR_Report_2018.pdf. Accessed: 17 December 2022.