Brian Sowers

12/04/2023

Site Reliability Engineering and SOAR

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

A Site Reliability Engineer (SRE) places equal focus on the connections between system components as on the components themselves because understanding these interactions is crucial for building or troubleshooting scalable systems. This holistic view ensures that communication and data flow between different parts of the system are optimized, which directly impacts the system's overall stability and performance. By focusing on how these elements interact, an SRE can identify potential bottlenecks, inefficiencies, or points of failure that might not be apparent when considering each component in isolation. This approach aligns with the principle that "Understanding the interactions between each system element is critical to building or troubleshooting systems that scale" (Hixson and Beyer, 41). It reflects the interconnected nature of modern technological systems, where the functionality and reliability of the whole system can be heavily influenced by how well its individual parts communicate and work together. In essence, an SRE's role extends beyond the realm of individual components to the broader architecture, ensuring that the system operates efficiently as a cohesive unit.

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

When considering Quality Assurance (QA) for future application or solution subsystems, incorporating Regulatory Standards Compliance is essential at strategic points of the development lifecycle. The integration of compliance should be holistic, proactive and promote technological advancement. For example, to achieve Know Your Customer (KYC) utility on blockchain, "the auditability and transparency enabled by the underlying blockchain technology should be integrated with compliance processes while adhering to all cybersecurity compliance requirements and emerging standards" (Building the Digital Bank of the Future, 13). This quote underscores the importance of embedding compliance within the core architectural and design phases of application development. When diagramming subsystems, compliance should be included at the initial design stage, ensuring that the foundational blueprint adheres to regulatory standards. This approach should be maintained throughout the development process, with continuous checks and balances at key milestones. By integrating compliance at these critical moments, it becomes an inherent part of the QA process, rather than an external addition. This method not only aligns with regulatory requirements but also fosters a culture of compliance and quality from the outset, increasing the feasibility of a well-built and compliant final product.

3. Security Orchestration, Automation, and Response (SOAR)

- **Automation. Explain two governing criteria when deciding upon candidates for security automation.** The first of two criteria when deciding upon a candidate for security automation is the duration and frequency of resolving a security alert. The 2018 SOAR Report conducted a study in which the response for the number of alerts that occur per week was 174956 and the number of days to resolve an alert was 4.34 (SOAR Report 2018, 17). This criterion emphasizes the efficiency of automating tasks that are both time-intensive and frequently occurring, thereby reducing the workload on security teams and

speeding up response times. The second criterion concerns the definition and structure of the tasks. For successful automation, it's crucial that "the tasks which the automation system takes over must be properly defined, preferably with sequential workflows" (SOAR Report 2018, 18). This means that tasks suited for automation should have clear, step-by-step processes that can be easily translated into automated workflows. Tasks with well-defined structures are easier to program into an automation system and this leads to more effective and error-free automation.

- **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?** Process update frequency is crucial in playbook design for security operations, impacting their effectiveness and relevance. Jane Goh from Palo Alto Networks emphasizes the necessity for playbooks to be "simple and intuitive" yet "primed for automation," (Security Orchestration Use Case) highlighting the need for ease of use and adaptability in the face of frequent updates. This balance ensures that playbooks remain effective against evolving threats. The SOAR report in 2018 conducted a study and found that "over 50% of respondents either didn’t update incident response processes at all or updated them infrequently." This lack of regular updates can lead to outdated playbooks, reducing their effectiveness in responding to new security incidents. To reduce the impact of frequent updates in future playbook designs, integrating modular components and AI-driven adaptability is key. Modular design allows for independent updates of different sections, while AI and machine learning enable dynamic adaptation

to new threats. These features ensure that playbooks stay current and effective, aligning with the evolving cybersecurity landscape.

Work Cited

"Building the Digital Bank of the Future: The Emerging Role of Quality Assurance." Everest Global, 2018, https://panacademy.net/CourseFiles/sbo/Everest_Group_Quality_Orchestration.pdf. Accessed 4 Dec. 2023.

Goh, Jane. "Security Orchestration Use Case: Automating IOC Enrichment." Palo Alto Networks, 09 Oct. 2018, https://www.paloaltonetworks.com/blog/security-operations/security-orchestration-use-case-automating-ioc-enrichment/. Accessed 5 Dec. 2023.

Hixson, David, and Betsy Beyer. The Systems Engineering Side of Site Reliability Engineering. Sysadmin, 2018, https://panacademy.net/CourseFiles/sbo/Systems_Engineering_Site_Reliability_Engineering.pdf. Accessed 4 Dec. 2023.

VIB. "The State of SOAR Report, 2018." Sponsored by Demisto, 2018, https://panacademy.net/CourseFiles/sbo/SOAR_Report_2018.pdf. Accessed 5 Dec. 2023.