Brian Sowers

11/09/2023

Adversary Playbooks

1. Identify two or more future challenges that should be addressed when selecting a specific Adversary Playbook.

"Adversary Playbooks are a compilation of adversarial acts that are collected, organized and shared by the Cyber Threat Alliance" based upon the CART model to improve the reliability of attack prevention efforts (Secure Business Systems Operations Module 2, 62). The CART model, emphasizing Completeness, Accuracy, Relevance, and Timeliness, allows cybersecurity professionals to better secure their organization. However, these playbooks are not standalone self-sustaining solutions. One challenge in selecting a playbook to provide a solution to the dynamic nature of cyber threats is the demand for continuous playbook updates to counter evolving tactics from malicious actors. Without these adequate updates, organizations will struggle with staying ahead of emerging risks in cybersecurity's highly evolving environment. Another critical challenge occurs from the diversity of cyber threats and varying adversary sophistication levels. If the selected playbook is too specific in sophistication, it may limit its application in varied threat scenarios, while being too general may fail to provide actionable insights for specific challenges. Careful consideration of industry sector, threat landscape, and adversary sophistication is crucial for crafting effective playbooks.

2. Describe the Core Elements that would be found in a typical Adversary Playbook.

The core elements of a typical Adversary Playbook include a "Technical Profile" describing the specific adversary, associated tools, tactics, techniques, and procedures (TTPs); "Typical Plays" illustrating how adversaries employ observables and TTPs in portrayed scenarios; "Recommended Actions" detailing defensive measures based on the adversary's profile and typical plays; and "Technical Indicators," compiling shareable technical indicators via the Structure Threat Information Expression (STIX). "Adversary Playbooks should, at a minimum, describe the tools adversaries often employ; the tactics, techniques, and procedures they frequently use; and the typical ways adversaries employ those tools to achieve their goals" (Adversary Playbooks, 2). TTPs are always evolving, however, as “APT actors, by their nature, attempt intrusion after intrusion, adjusting their operations based on the success or failure of each attempt” (STIX Whitepaper, 5). These core elements provide a structured and comprehensive framework for the development and use of Adversary Playbooks in the cybersecurity domain.

3. Compare and contrast the practices of using a comprehensive playbook to defend against a wide range or scope of attacks.

Various practices exist in the deployment of a playbook since an organization may focus on different principles a playbook is founded on. For example, the principles of "Not let the perfect be the enemy of the good" and CART offer complementary yet distinct approaches when implementing a comprehensive playbook for defending against a broad scope of cyber threats (Adversary Playbooks, 4). "Not let the perfect be the enemy of the good" emphasizes acknowledging the inevitable incompleteness of an Adversary Playbook and encourages a proactive stance in seeking additional data through regular updates. This latter principle aligns with CART's completeness aspect, emphasizing the need to provide sufficient detail for an

effective response. However, CART introduces additional dimensions, including accuracy, relevance, and timeliness, underscoring the importance of ensuring data quality that enables the right actions and addresses threats pertinent to the target audience's business operations. While both principles advocate adaptability, "Not let the perfect be the enemy of the good" primarily focuses on acknowledging gaps, whereas CART provides a more structured framework, incorporating multiple elements to enhance the overall quality and effectiveness of the playbook.

Works Cited

"Adversary Playbooks: An Approach to Disrupting Malicious Actors and Activity." *Cyber Threat Alliance*.http://panacademy.net/CourseFiles/sbo/CTA_Adversary_Playboo k_Princip les.pdf. Accessed: 10 November 2023.

Barnum, Sean. "Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression." *MITRE*. https://panacademy.net/CourseFiles/sbo/Structured_T hreat_Information.pdf. Accessed: 10 November 2023.

"Secure Business Operations Module 2, https://s3.amazonaws.com/assets.paloaltonetwor ksacademy.net/sbo/Business_Operations_Module_1.pdf. Accessed: 10 November 2023.