Brian Sowers

08/11/2022

Adversary Playbooks

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

Two challenges present when considering a specific adversary playbook is it if matches the needs and context of the organization. The CART (Completeness, Accuracy, Relevance, Timeliness) model is a model to help differentiate between playbooks. I believe timeliness and relevance are the two biggest challenges in the future because without these, the playbook selected is arguably worse than having no playbook at all. For example, consider a playbook that is not relevant to the organization whatsoever. The man hours monitoring the playbook and the additional data waste resources that could be utilized elsewhere. Timeliness is also important when considering a playbook that does not produce results quickly. Potentially, a malicious actor can infiltrate your network and take sensitive information before your playbook does anything to prevent that.

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

The core elements found in a typical adversary playbook includes a technical profile, typical plays, and recommended actions for end-users. An adversary playbook for cybersecurity providers those for an end-user with the addition of technical indicators (Secure Business Systems Operations Module 2, 61). The technical profile describes the “ the specific adversary, a

generic adversary type, or the generic effect an adversary wants to achieve, along with the tools and tactics, techniques, and procedures (TTPs) typically associated with the adversary or effect" (Adversary Playbooks, 4). The typical plays "demonstrates how the adversary typically employs those observables, capabilities, and TTPs in certain exemplar scenarios, through a collection of attack techniques defined by MITRE's Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) model and laid out according to the Kill Chain structure" (Adversary Playbooks, 4). The recommended actions "describes the defensive actions and mitigations that will have the greatest impact and return on investment, based on the profile and typical plays described in the first two elements" (Adversary Playbooks, 4). Lastly, the technical indicators "provide a compilation of the technical indicators used to build the playbook in a shareable format via Structure Threat Information Expression (STIX)4, which are also included in the CTA Platform prior to public release" (Adversary Playbooks, 4).

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

A comprehensive playbook has both pros and cons and is up to the organization to differentiate between the two and select the most appropriate one. For instance, a comprehensive playbook may act on an attack you may have not considered and will help to protect your organization against previously unconsidered threats. On the other hand, a comprehensive playbook may alert and recommend actions to end-users and cybersecurity providers that may have little relevance to the organization in question, thus resulting in information overload. Both results happen due to a lack of context in which the adversary playbook is operating in. It is best that an adversary playbook is tailored to the organization using it, so that it is used most effectively and produces relevant results for both the end-user and cybersecurity provider.

Works Cited

"Adverary Playbooks: An Approach to Disrupting Malicious Actors and Activity." *Cyber Threat Alliance*.http://panacademy.net/CourseFiles/sbo/CTA_Adversary_Playbook_Principles.pdf. Accessed: 08 November 2022.

"Secure Business Operations Module 2, https://s3.amazonaws.com/assets.paloaltonetworksacademy.net/sbo/Business_Operations_Module_1.pdf. Accessed: 08 November 2022.