Adversary Playbooks

Angela Milova

Palo Alto - Secure the Future 2023

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

Organizations seeking assistance may encounter several challenges that demand thoughtful consideration. Firstly, the ever-evolving landscape of Tactics, Techniques, and Procedures (TTPs) poses a significant hurdle. Threat actors continuously adapt their strategies, rendering adversary playbooks quickly outdated (Applebaum, Johnson, Limiero, et al., 2018). Recognizing this, organizations must establish a dynamic framework that undergoes regular updates, ensuring it remains a timely resource in threat intelligence sharing. The second challenge revolves around the integration of new technologies. While machine learning and AI hold promise in cybersecurity and threat intelligence, their implementation introduces complexities. Organizations must carefully manage the scope of information accessible to AI, considering potential risks and ensuring responsible sharing practices. The evolution of AI itself introduces the potential for adversaries to enhance their tactics, requiring adversary playbooks to offer guidance on navigating this dynamic landscape (Elluru, Howell, Garris, n.d). Global regulatory changes, including the emergence of new cybersecurity and data protection laws, present another challenge. As these regulations evolve globally, adversary playbooks must anticipate and adapt to these shifts. This challenge extends to preparing playbooks on a global scale to meet diverse regulatory requirements. Additionally, the involvement of nation-state actors introduces a unique set of challenges. Many countries leverage nation-state actors for cyberattacks, possessing substantial cyber knowledge but often withholding information (Buchanan, 2016). Navigating these challenges necessitates a comprehensive and globally aware approach to adversary playbook development and maintenance.

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

An Adversary Playbook is a critical document tailored to assist organizations in understanding and responding effectively to the dynamic landscape of cyber threats. It plays an important role in offering diverse strategies and procedures for various attack scenarios and threat actors. A central focus of the playbook lies in furnishing comprehensive information about threat actors, making it imperative to incorporate a core element known as Adversary Profiles (Cyber Threat Alliance, n.d). This section serves as a repository for profiles of known threat actors or groups, encompassing all their aliases to provide a consolidated reference. By offering insights into their behaviors, motives, and historical activities, this core element gives essential context to anticipating and responding to attacks. Another fundamental component of the Adversary Playbook revolves around Tactics, Techniques, and Procedures (TTPs). Detailed descriptions of these tactics equip the security team to respond adeptly to evolving threat behaviors (Applebaum, Johnson, Limiero, et al., 2018). Equally crucial is the inclusion of a section dedicated to Indicators of Compromise (IOCs) (Parmar, Domingo, 2019). Platforms like VirusTotal have proven invaluable, enabling organizations to identify malicious URLs, IP addresses, hashes, and more. Beyond on how and why of threat actor attacks, the playbook assumes a proactive role in risk mitigation. This involves providing valuable recommendations through diverse channels, including dedicated sections for resources, Incident Response Procedures, and, significantly, lessons learned from past attacks (Pamment, Falkheimer, Isaksson, n.d). This multifaceted approach ensures that the playbook serves as a repository of knowledge and a strategic guide for helping an organization's cybersecurity defenses.

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

Utilizing a comprehensive playbook as a strategic approach to defending against threat actor attacks offers diverse methods for responding to these evolving threats. However, it introduces complexities along the way. The comprehensive playbook provides a wide spectrum of cyber threats with the primary goal of improving the efficiency of response times. Its design emphasizes flexibility and adaptability, recognizing that information about threat actors constantly evolves with their changing tactics and techniques (Applebaum, Johnson, Limiero, et al., 2018). By incorporating details about specific attacks, the comprehensive playbook equips the security team with defense strategies for successfully protecting against these threats. Despite its strengths, a comprehensive playbook brings such challenges. Not all threat actors and Tactics, Techniques, and Procedures (TTPs) may universally apply to organizations using them. Understanding the specific audience becomes paramount for these playbooks to serve the unique needs of organizations effectively. Given the dynamic nature of the threat landscape, maintaining a comprehensive playbook demands significant resources, necessitating ongoing updates and coordination across various teams. Threat actors continually evolve, requiring increased team efforts to keep the comprehensive playbook up to date (Stevens, Votipka, Dykstra, et al., 2022). This dynamic landscape underscores the advantage of a more narrowly focused playbook, which requires fewer resources and allows for faster updates. Some comprehensive playbooks provide detailed technical information about attacks. However, as attacks become more complex, the information within these playbooks must keep up the pace (*Understanding playbooks in cyber security*. n.d). This brings the need for continuous training for teams involved in maintaining

comprehensive playbooks and, likewise, for organizations to ensure their security teams receive ongoing training. The ever-changing nature of cyber threats reinforces the importance of adapting strategies, refining playbooks, and investing in the continual development of cybersecurity expertise.

References:

Adversary playbooks - Cyber Threat Alliance. (n.d.-a)

Applebaum, A., Johnson, S., Limiero, M., & Smith, M. (2018, June). Playbook oriented cyber response. In *2018 National Cyber Summit (NCS)* (pp. 8-15). IEEE.

Buchanan, B. (2016). The cybersecurity dilemma: Hacking, trust, and fear between nations. Oxford University Press

Elluru, R., Howell, C., & Garris, M. National Security Addition to the National Institute of Standards and Technology Artificial Intelligence Risk Management Framework Playbook.

Pamment, J., Falkheimer, J., & Isaksson, E. Understanding the adversarial playbook.

Parmar, M., & Domingo, A. (2019, November). On the Use of Cyber Threat Intelligence (CTI) in Support of Developing the Commander's Understanding of the Adversary. In *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)* (pp. 1-6). IEEE.

Stevens, R., Votipka, D., Dykstra, J., Tomlinson, F., Quartararo, E., Ahern, C., & Mazurek, M. L. (2022, April). How ready is your ready? assessing the usability of incident response playbook frameworks. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (pp. 1-18).

Understanding playbooks in cyber security. What is a playbook in cyber security? (n.d.).