Mapping to MITRE ATT&CK

Reading

45m

Status | Incomplete

Introduction

As you learned in the previous reading, the MITRE ATT&CK framework gives a clear understanding of online attack techniques and tactics by shining light on the behaviors of attackers and describing such behaviors using a framework that is easy to navigate and understand. It showcases how attackers work, from high-level tactics to specific procedures.

Security professionals can improve their security controls by learning from the actions of attackers after real-world security incidents. Mapping ATT&CK against security incident reports is a useful way to extract valuable intelligence that you can use to improve the security of your organization. The ATT&CK mappings have the potential to serve as a bedrock resource, enabling businesses and defenders to get insight into their impacts on adversarial behaviors and make decisions based on this knowledge.

After identifying techniques and tactics as a result of ATT&CK mappings across an organization, it is recommended that the organization conduct a thorough assessment of each stage of an attack, establish understanding across core areas of the environment, and determine where improvements can be made to security controls or where gaps can be filled in security postures.

Reading

1. Cybersecurity and Infrastructure Security Agency (CISA) has developed a best practices guide to map MITRE ATT&CK against incidents. This guide provides detailed step-by-step instructions to best map adversary behavior to the MITRE ATT&CK framework. Focus on each best practice given in this guide and reflect how you may adopt it for your specific requirements: Best Practices for MITRE ATT&CK Mapping
2. Once you have attributed a set of behaviours to a specific type of attack(s), next you need to map them to specific mitigations. The MITRE Framework makes this easy, review the following page and click on a few of these mitigations to see all of the attacks that can be prevented by that mitigation. MITRE ATT&CK Mitigation List
3. Alternatively, you can always search a specific attack and at the bottom of it's description you will see a list of mitigations you can use to defend against it, here is brute forcing for as an example. MITRE ATT&CK brute force

Throughout your career and this course you will be asked to identify risks/vulnerabilities and recommend mitigations for them. Rather than trying to come up with them from memory, you can search specific attacks in the MITRE Framework and get a list of mitigations for each attack type, along with a ready to use description.

Note

> Understanding MITRE ATT&CK mapping helps you understand how to work with the ATT&CK Navigator tool. Later in the course, you will use this tool to highlight and practice with the differing views of mapping.

Conclusion

Now that you know about the MITRE ATT&CK framework and how to map incidents to it, it's time to jump to a knowledge check on the Cyber Kill Chain Model, Diamond Model, and MITRE ATT&CK in the next activity.

✓ Mark Completed

Previous
MITRE ATT&CK Framework

Next
Models & Frameworks Exercise

How well did this activity help you to understand the content?

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W07D5

Fri Aug 9

- Outline & Notes (1)
- Lectures (1)
- Work (5)
  - 5 hrs
  - Using Strategic Intelligence on Carbanak Report
  - Diamond Model for Intrusion Analysis
  - MITRE ATT&CK Framework
  - Mapping to MITRE ATT&CK
  - Models & Frameworks Exercise
- Other (1)

W07D5 Schedule »