sentra

Building a Holistic Data Security Strategy

The MITRE ATT&CK Framework, DDR, and Protecting the Data that Matters

Introduction

Data Security Posture Management (DSPM) is playing a growing role in safeguarding sensitive information. It's a continuous process of assessing, improving, and monitoring an organization's security posture relating to its data assets. By proactively identifying and mitigating risks, DSPM empowers organizations to build stronger defenses against evolving cyber threats. Anyone who has suddenly discovered sensitive data in a new location or noticed a 3rd party with excessive access, understands the value of knowing where your data is and who has access to it at all times.

The accurate classification provided by DSPM is also enabling another security approach to finally reach its potential - **Data Detection and Response (DDR)**. DDR solutions are dependent on accurate data classification, and the inability to accurately classify structured and unstructured data leads to unacceptable false positive rates. Accurate classification is changing this.

This ebook delves into the world of data security elements of the MITRE ATT&CK Framework, aiming to equip enterprise data security professionals with the knowledge and strategies to effectively adopt data security tools that can assist in relevant areas of the framework.

Chapter 1

Understanding Data Security Posture Management (DSPM)

1.1 What is DSPM?

Data security posture management (DSPM) is a continuous and iterative process focused on assessing, improving, and monitoring an organization's security posture around its data assets. It involves:

- **Identifying and classifying data assets:** This includes understanding the location, type, sensitivity, and value of each data asset within the organization's network.
- **Assessing risks to data assets:** This entails deploying various technical and non-technical controls to safeguard data assets, such as firewalls, access controls, security awareness training, and data encryption.
- **Monitoring and improving the security posture:** Regularly reviewing the effectiveness of implemented controls, identifying new vulnerabilities, and adapting the security strategy as needed is essential for maintaining a robust security posture.

1.2 Benefits of DSPM

Effective DSPM offers numerous advantages for enterprises, including:

- **Reduced risk of data breaches:** By proactively identifying and mitigating vulnerabilities, organizations can significantly reduce the likelihood of data breaches and associated financial and reputational damage.

- **Improved compliance with data security regulations:** Many data security regulations mandate organizations to implement appropriate security controls to protect sensitive data. A comprehensive DSPM program facilitates compliance with these regulations.

- **Enhanced security posture:** Through ongoing assessment, improvement, and monitoring, DSPM strengthens an organization's overall security posture, making it less susceptible to cyberattacks.

- **Reduced costs:** Data breaches can incur significant financial costs, including remediation efforts, legal fees, and reputational damage. Proactive measures through DSPM can help minimize these costs.

1.3 Challenges of DSPM

While valuable, implementing and maintaining a comprehensive DSPM program comes with certain challenges:

- **Complexity:** DSPM encompasses various processes, methodologies, and tools, requiring a deep understanding of data security and information technology.

- **Keeping up with evolving threats:** The cyber threat landscape is constantly changing, requiring organizations to continuously update their security strategies and controls to stay ahead of emerging threats.

Chapter 2

Demystifying the MITRE ATT&CK Framework

2.1 What is the MITRE ATT&CK Framework?

The MITRE ATT&CK Framework is a globally recognized knowledge base of adversary tactics and techniques based on real-world observations. It serves as a comprehensive resource for understanding how attackers operate, allowing organizations to:

- **Identify potential attack vectors:** By understanding the tactics and techniques employed by adversaries, organizations can proactively identify areas within their network that might be vulnerable to attack.

- **Develop targeted defense strategies:** By aligning their security controls with the tactics and techniques outlined in the framework, organizations can prioritize their efforts and focus on mitigating the most relevant threats.

- **Improve threat detection and response:** The framework provides valuable insights into attacker behavior, enabling organizations to develop more effective detection and response capabilities.

2.2 Components of the MITRE ATT&CK Framework

The MITRE ATT&CK Framework is structured around three key components:

Tactics:	Techniques:	Procedures:
These represent the high-level goals pursued by adversaries during an attack, such as "initial access" or "persistence.	These represent the specific methods employed by adversaries to achieve their tactical objectives. Each tactic encompasses a range of techniques, providing a granular understanding of attacker behavior.	These are specific implementations of techniques, often involving a combination of tools and scripts. While not officially part of the core framework, procedures offer additional insights into attacker behavior but may vary depending on the attacker's specific tools and capabilities.

2.3 Benefits of Utilizing the MITRE ATT&CK Framework

Integrating the MITRE ATT&CK Framework into an organization's security strategy offers numerous benefits:

- **Threat-informed defense:** The framework provides a common language for discussing cyber threats, facilitating communication and collaboration between different security teams within an organization.

- **Benchmarking and threat intelligence sharing:** The framework allows organizations to compare their security posture against the tactics and techniques used by known threat actors, enabling them to leverage threat intelligence shared by the broader security community.

Chapter 3

The MITRE ATT&CK Framework and DDR

3.1 How DSPM & DDR Add a Layer of Protection against Adversaries

- **Gain a deeper understanding of potential attack vectors:** By aligning identified vulnerabilities with the tactics and techniques employed by adversaries, organizations can gain a clearer picture of how their specific data assets might be targeted. A DSPM featuring a Data Detection and Response (DDR) capability would be able to find suspicious or malicious applications and actors

- **Prioritize security efforts:** DDR allows organizations to prioritize their security efforts by focusing on data that's at highest risk of exposure.

- **Develop more effective security controls:** With a clear understanding of potential attack vectors, organizations can implement more targeted and effective security controls to mitigate identified risks.

3.2 Mapping Process

Using DSPM, DDR and the MITRE ATT&CK Framework for a Holistic Data Security approach involves a number of steps:

- **Identify vulnerabilities through data security assessments:** Conduct comprehensive assessments of your organization's security posture to identify vulnerabilities and gaps in your security controls. Analyze vulnerabilities for potential attacker exploitation. Evaluate each identified vulnerability and assess how it could be exploited by adversaries based on the tactics and techniques outlined in the MITRE ATT&CK Framework.

- **Map vulnerabilities to relevant tactics and techniques:** Utilize the MITRE ATT&CK Matrix to identify the specific tactics and techniques that align with the identified vulnerabilities. This mapping exercise helps you understand how attackers might leverage these vulnerabilities to achieve their objectives.

- **Understand the implications of the mappings:** Analyze the mapped tactics and techniques to comprehend the potential consequences of a successful attack scenario. This understanding is crucial for prioritizing your security efforts. This is again where a DDR capability is able to assist by looking at malicious applications or actors and then enriching the most sensitive data that is vulnerable to exfiltration

- **Prioritize vulnerabilities based on risk:** Consider factors like the likelihood of an attack, the potential impact of a successful attack, and the ease of exploitation when prioritizing vulnerabilities for remediation.

Chapter 4

Leveraging Combined Insights for Actionable Defense

A Holistic Approach to Data Security

Integrate these insights into your organization's overall security program for a holistic approach. This includes:

- **Threat intelligence sharing:** Regularly share and update threat intelligence based on your DDR findings and MITRE ATT&CK mappings with other security teams within your organization. This collaborative approach fosters a more comprehensive understanding of the threat landscape and facilitates coordinated defense efforts.

- **Security awareness and training:** Educate employees about cyber threats and best practices aligned with the tactics and techniques identified through the mapping process. This empowers employees to play a vital role in the organization's cybersecurity posture by recognizing and reporting suspicious activity.

- **Incident response planning and testing:** Leverage the insights from your mappings to inform your incident response plan and procedures. Regularly test your incident response capabilities to ensure you are prepared to effectively respond to and remediate security incidents.

- **Incident response planning and testing:** Leverage the insights from your mappings to inform your incident response plan and procedures. Regularly test your incident response capabilities to ensure you are prepared to effectively respond to and remediate security incidents.

Conclusion

In today's dynamic threat landscape, a comprehensive and data-driven approach to cybersecurity is essential. By factoring Data Detection and Response (DDR) into your MITRE ATT&CK Framework strategies, organizations can gain a deeper understanding of their vulnerabilities, potential attack vectors, and the tactics employed by adversaries.

This integrated approach empowers organizations to develop more targeted and effective security strategies, ultimately enhancing their overall security posture and safeguarding their valuable data assets.

sentra