SALT

MITRE ATT&CK Framework for API Threats: Understanding Adversary Tactics

The MITRE ATT&CK framework offers a knowledge base on adversary tactics tailored to API threats. It helps organizations comprehend how attackers target APIs and provides a common language for sharing threat intelligence. Techniques like credential stuffing, API abuse, and data exfiltration enhance threat detection and response. By using MITRE ATT&CK, organizations can address potential API attacks and improve their security posture.

- Adversary Behavior:
  - Mapping of adversary tactics and techniques to API-specific threats.
  - Understanding of common attack patterns and methodologies.
  - Identification of potential attack vectors and vulnerabilities.
- Threat Intelligence:
  - Sharing of threat intelligence using a common language.
  - Collaboration with industry partners to enhance threat awareness.
  - Use of threat intelligence to improve security controls.
- API Specific Tactics:
  - Credential stuffing and brute-force attacks.
  - API abuse and exploitation of business logic flaws.
  - Data exfiltration and unauthorized access to sensitive data.

Why It Matters: he MITRE ATT&CK framework provides valuable insights into how attackers operate, enabling organizations to proactively defend against API-based threats. By understanding adversary tactics, organizations can improve their security posture and reduce their risk of attack.

Relevant Sections Referencing APIs:

- T1078: API credential theft and abuse.
- T1190: Exploiting public-facing APIs.

How Salt Security Helps: Salt Security helps organizations leverage the MITRE ATT&CK framework by providing threat detection that aligns with the framework's tactics and techniques. Threat intelligence and reporting capabilities help organizations understand and communicate the nature of threats, enhancing their overall security posture. Salt Security's data security capabilities provide context for understanding the impact of attacks by allowing you to view the data being targeted or exfiltrated in motion through APIs. Learn more about API Security and Compliance in our **White-paper.**