Automate Continuous Endpoint Security Testing with Microsoft® and AttackIQ®

Microsoft

AttackIQ® automates the evaluation of Microsoft® Defender Advanced Threat Protection (ATP) against the tactic categories as outlined by MITRE ATT&CK™. Within each category are individual techniques that are explained in more detail in our guide, How To Get Started Testing with the MITRE ATT&CK Framework.

Benefits:

Together, Microsoft and AttackIQ provide continuous visibility and control over the security of your endpoints. AttackIQ integrates with and automates ongoing testing of Microsoft Defender ATP to ensure it is deployed correctly and configured optimally.

1. **Assess your current prevention, detection, and response capabilities**
2. **Prove the benefits of using Microsoft Defender ATP**
3. **Continuously demonstrate that Microsoft Defender ATP is protecting your organization as intended**

On page 2, **Table 1** outlines the capabilities of Microsoft Defender ATP that can be tested with a predefined template in the AttackIQ Platform, which includes a subset of the MITRE ATT&CK Framework tactics and techniques.

The AttackIQ platform has automated the use of the MITRE ATT&CK framework, the most authoritative, comprehensive, and complete set of up-to-date attack techniques and supporting tactics in the world. MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world data. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

About Microsoft Defender ATP

Microsoft Defender Advanced Threat Protection (ATP) is a unified endpoint security platform for preventative protection, post-breach detection, automated investigation, and response.

Microsoft Defender ATP includes risk-based Threat & Vulnerability Management to discover, prioritize and automate mitigation of vulnerabilities and security misconfiguration. The platform also provides security admins tools to surgically reduce the attack surface without limiting user's productivity. Its behavioral based and cloud-powered threat & malware protection prevents sophisticated and never-seen-before threats from impacting devices. Deep optics into the operating system, including memory and kernel, help to detect 0-days, advanced attacks, and data breaches. Microsoft Defender ATP accelerates remediation by automatically investigating alerts and remediating threats – allowing security teams to go from alert to remediation in minutes - at scale. Finally, Microsoft Defender ATP comes with a managed hunting service, which provides critical threat monitoring, expert level analysis, and support for Security Operations Centers.

Microsoft Defender ATP is a complete solution providing security teams across the organization with threat protection, detection and response, deep and wide optics, and the needed tools to better protect the organization.

TABLE 1: Capabilities of Microsoft Defender ATP that can be tested with a predefined template in the AttackIQ Platform.

Highlighted Microsoft Defender ATP Defensive capability	Description	MITRE ATT&CK Tactics and Techniques
Identify and block potentially malicious software	Restrict and prevent an attacker from executing binaries when any given user logs into the compromised system	Persistence Lateral Movement T1037
Prevent debuggers from running escalated privileges	Keep attackers from exploiting a previously compromised system.	Persistence Privilege Escalation T1015 T1183
Block code injection	Prevent arbitrary monitoring programs from running malicious executables in any process or subprocess	Defense Evasion Persistence T1059 T1064 T1183
Limit modifications of system settings	Stop attackers from bypassing system settings to obtain restricted access	Defense Evasion Execution T1059 T1064 T1196
Prevent registry key modifications	Limit key registry changes to keep attackers from executing unknown applications	Privilege Escalation Persistence T1059 T1064 T1182
Identify and block potentially malicious software from being executed	Limit access to associated file types within a given registry key	Persistence T1042 T1059 T1064
Detect hidden malicious code replication	Prevent modification of files associated with the NTFS alternate stream	Defense Evasion T1096

CONTACT ATTACKIQ

U.S. Headquarters

9276 Scranton Road, Suite 100

San Diego, CA 92121

+1 (888) 588-9116

microsoft-alliance@attackiq.com

About AttackIQ

AttackIQ, a leader in the emerging market of continuous security validation, built the industry's first platform that enables red and blue teams to test and measure the effectiveness of their security controls and staff. An open platform, AttackIQ™ supports the MITRE ATT&CK Matrix, a curated knowledge base and model for cyber adversary behavior used for planning security improvements and verifying that defenses work as expected. AttackIQ's platform is trusted by leading companies around the world. For more information visit www.attackiq.com. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.

© 2019 AttackIQ, Inc. All rights reserved. AttackIQ® is a registered trademark of AttackIQ, Inc. Microsoft® Defender ATP is a registered trademark of Microsoft Corporation in the United States and/or other countries. MITRE ATT&CK™ (and MITRE ATTACK™) are trademarks of The Mitre Corporation.