Test and Validate Your Detection Pipeline with Microsoft® and AttackIQ®

The industry-leading Breach and Attack Simulation (BAS) capabilities of the AttackIQ® platform provide Microsoft Azure Sentinel users with essential tooling to improve the effectiveness of their detection and investigation pipeline.

Benefits:

By emulating adversary according to the Tactics and Techniques cataloged in the MITRE ATT&CK Framework, analysts can conduct an end-to-end test of their detection pipeline, validate their alert rules, and practice investigations on benign suspicious events. AttackIQ® Assessments provide a structured and repeatable method to:

- Confirm that events are detected and/ or prevented by deployed security technologies.
- Confirm that detection and prevention messages are properly forwarded to Azure Sentinel
- Test built-in and custom queries and alert rules.
- Exercise the actions defined in Azure Sentinel Playbooks.

The AttackIQ platform helps demonstrate the depth and breadth of visibility achieved with Azure Sentinel through simple and intuitive configuration of source types, as well as attribution of detections that clearly indicate the origin of the event and the collection of the event by Azure Sentinel. The integrated solution gives analysts and incident responders confidence that their preventive, detective, and corrective controls are optimally configured and operating reliably.

About Microsoft Azure Sentinel

Microsoft Azure Sentinel is SIEM reinvented for the modern world, allowing you to see and stop threats before they cause harm. By combining the cloud and large-scale intelligence from decades of Microsoft security experience, threat detection and response become smarter and faster while eliminating security infrastructure setup and maintenance. Azure Sentinel provides a bird's-eye view across the enterprise, elastically scaling to meet security demands without increasing IT costs.

Microsoft Azure Sentinel is designed to:

- Collect data at cloud scale—across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.
- Detect previously undiscovered threats and minimize false positives using analytics and unrivaled threat intelligence from Microsoft.
- Investigate threats and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.
- Respond to incidents rapidly with built-in Playbooks that provide orchestration and automation based on Microsoft Azure Logic Apps.

Whether they are business applications, other security products, or homegrown, Microsoft Azure Sentinel integrates with existing tools. It also reduces noise and helps teams focus on finding real threats quickly using machine learning models trained on trillions of daily signals while allowing them to optimize for their own needs with tailored detections, machine learning models, and threat intelligence.

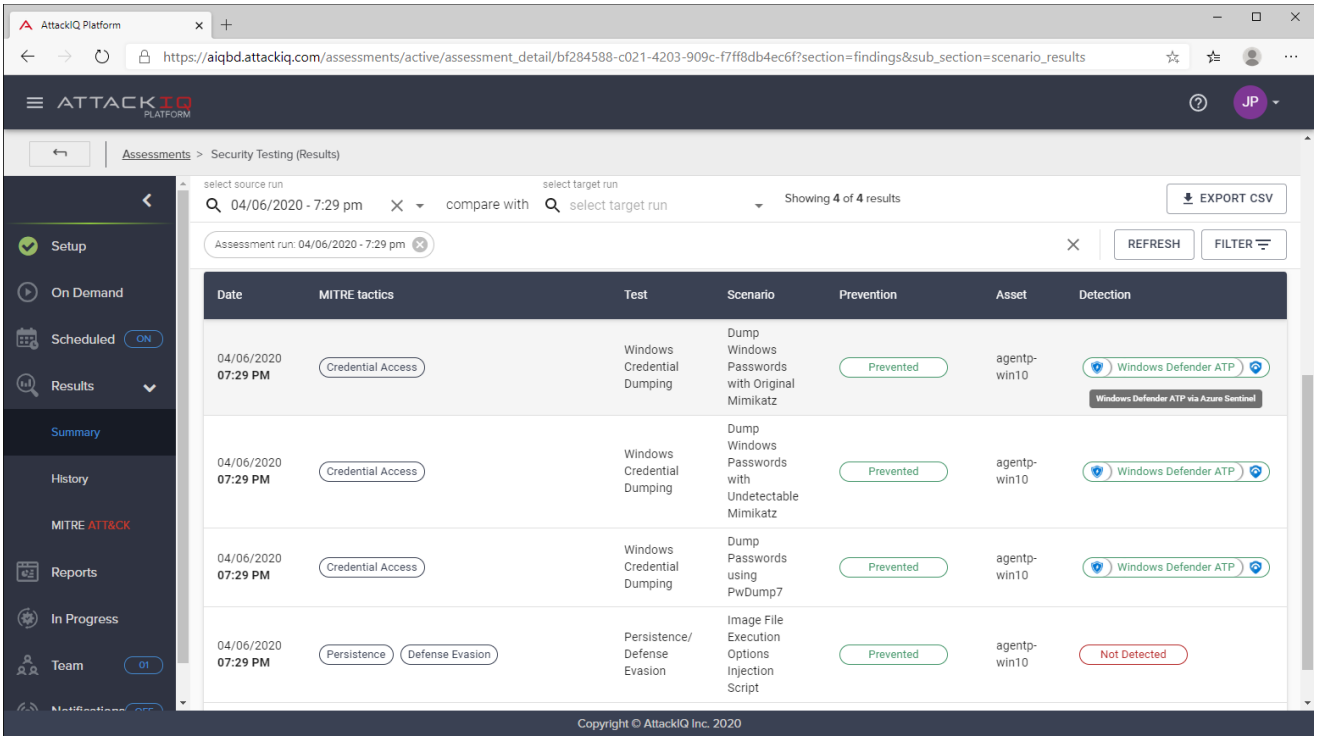

FIGURE 1: Detection results for Microsoft Defender ATP retrieved via Azure Sentinel

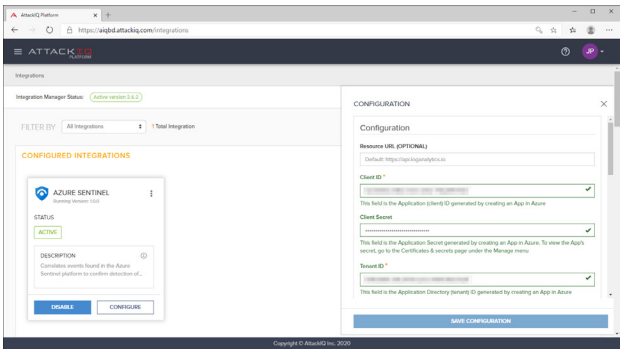

FIGURE 2: Azure Sentinel configuration

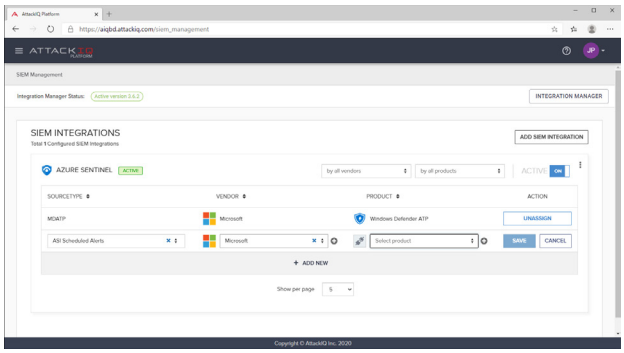

FIGURE 3: Source type selection

CONTACT ATTACKIQ

U.S. Headquarters

2901 Tasman Drive, Suite 112

Santa Clara, CA 94045

+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.