ATTACKIQ MISSION CONTROL

Seamlessly Orchestrate BAS Across Distributed Teams

AttackIQ Mission Control enhances AttackIQ Enterprise deployments within large organizations, streamlining security testing workflows.

Continuous Security Validation for the Extended Organization

As the use of the BAS platforms by large organizations expands over time, centralized missions and policies that are often designed to bring continuous improvement can be challenging to implement across distributed security teams with varying levels of technical expertise.

As a result, rolling out testing programs can be slower than desired. When BAS products identify security gaps, it's important for organizations to quickly assess the impact, fix the issues, and confirm improvements. Delays in finding and fixing security gaps leaves organizations exposed, consumes additional resources, and reduces the return-on-investment security teams get from their testing programs.

Introducing AttackIQ Mission Control

AttackIQ's Mission Control addresses these challenges directly by enabling BAS security administrators to seamlessly orchestrate testing across their distributed teams. It provides the enterprise organization a streamlined service delivery framework that facilitates teams with role-based insights and analytics designed to accelerate testing workflows while ensuring uniformity of mission across various business units, geographic locations, and departments. This enables them to concentrate on the work that matters to them, with insights tailored to their unique roles.

HIGHLIGHTS

Leverage the Benefits of BAS Faster

AttackIQ technology is now easily extensible across widely distributed corporate or government organizational structures. Regardless of your experience and skill level, you can more rapidly leverage the benefits of continuous security validation within your business unit, field office, or department.

Comprehensive Analytics and Reporting

Mission Control provides comprehensive analytics and reporting that shares insight into test point coverage and success. This includes detailed metrics into security control performance with actionable mitigation guidance to close gaps quickly and improve performance and an overall security score to help guide continuous improvement.

MITRE ATT&CK Aligned

AttackIQ Mission Control is part of AttackIQ Enterprise. AttackIQ Enterprise brings complete product alignment with MITRE ATT&CK. MITRE ATT&CK help provides results that are actionable, in a clearly understood universal language that are aligned with industry best practices. MITRE ATT&CK is used by more cybersecurity practitioners than any other framework in the world to model the mindset and activities of cyber threat actors.

Introducing AttackIQ Mission Control (cont.)

Users get detailed analytics that show coverage and success by MITRE ATT&CK tactic, techniques, prevention rates, and simplified scores designed to make progress tracking intuitive. Once remediations have been made in their environment they can rerun their assessments to validate improvement tests and review the scores for improvement. The highly simplified and focused environment allows for faster user adoption and more rapid response to the reported callouts from the continuous security validation program.

How Mission Control Works
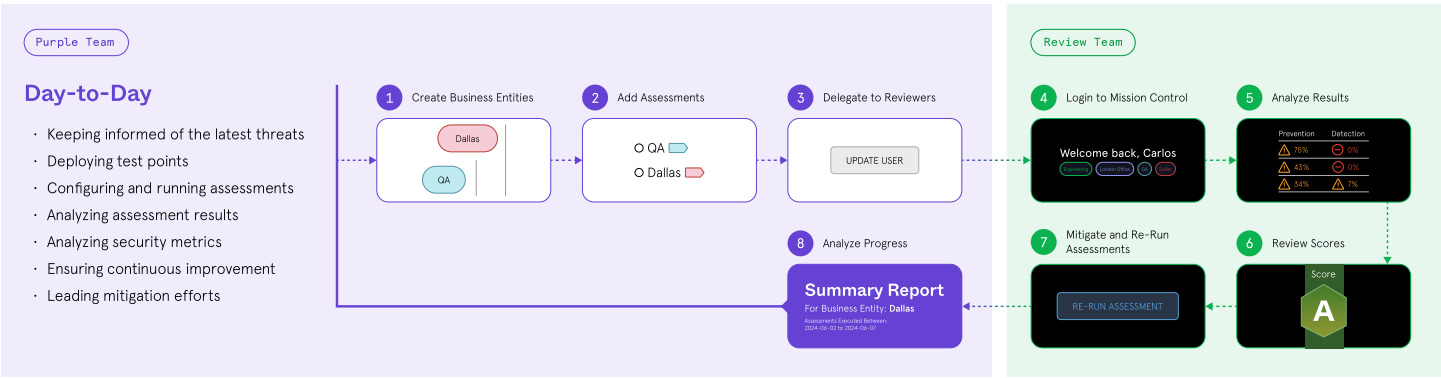
Mission Control Detection and Prevention Scoring Dashboard

Intuitive performance metrics by tactic, with a simplified scoring system designed to provide immediate insights into your businesses' security gaps

The Value of AttackIQ Mission Control

AttackIQ's Mission Control enables distributed teams to seamlessly orchestrate testing missions across their workforces, while simultaneously lowering the bar for less technical team members with simplified workflows. Within the Mission Control interface, security administrators can customize and manage testing for their departments, business units, or geographic office locations at the click of a button. Members of security teams assigned to these entities can then concentrate on the assessments assigned to their role. Once security gaps are identified and remediated, teams can easily rerun assessments and track performance.
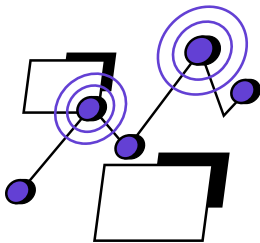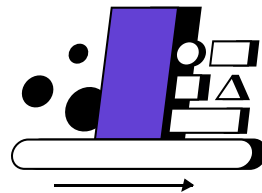
Up-Level Your Teams

Role-based insights and dedicated workspaces lower the bar for less skilled users to conduct testing.
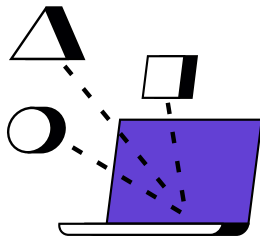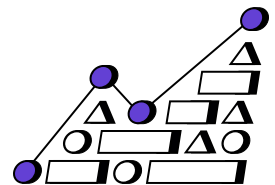
Actionable Data

Reviewers gain valuable insights from comprehensive analytics to guide ongoing security improvements.

Simplified Administration

Ensure mission alignment by enabling managers to create and assign testing objectives to team members easily.

Improved Efficiency

Streamlined workflows empower users to swiftly address and focus on their assigned security issues, leading to better ROI.