A SOC Optimization Service

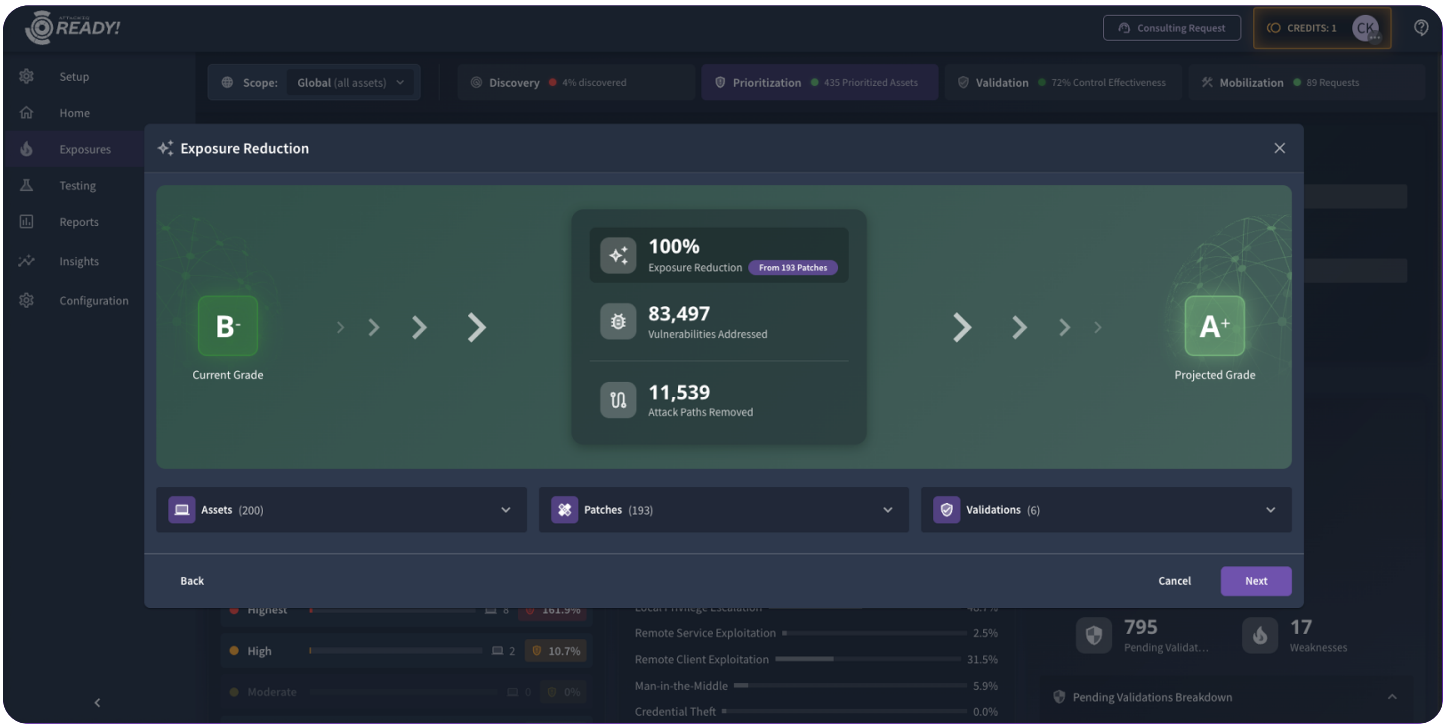
AttackIQ Vanguard

Co-Managed Continuous Security Validation

Security controls change. Detections degrade. Adversary techniques evolve. Without structured validation, security teams lack objective data on whether controls are working as intended.

Many organizations require continuous validation but lack the internal capacity to sustain dedicated adversary emulation and follow-through.

AttackIQ Vanguard provides ongoing, co-managed security validation to extend internal capability. This service combines structured adversary emulation, practitioner-led analysis, and remediation guidance to help organizations continuously assess and improve the effectiveness of their security controls as part of regular operations.



Strengthen Security Control Validation

AttackIQ Professional Services partners with your team to establish a sustained validation practice aligned to real-world adversary behavior and operational requirements.

Strengthen Security Control Validation (cont.)

Through the engagement, you will:

- Establish a repeatable validation cadence aligned to MITRE ATT&CK
- Measure detection and prevention effectiveness across environments
- Identify control gaps, misconfigurations, and redundancies
- Prioritize remediation based on observed performance data
- Integrate validation into SOC and security engineering workflows

A mature validation practice provides continuous insight into the effectiveness of controls and supports threat-informed security investment decisions.

Service Description

The AttackIQ Vanguard service delivers structured, co-managed adversary emulation and control validation tailored to your environment.

AttackIQ Professional Services advisors design testing plans, execute assessments, analyze results, and guide remediation efforts. The service integrates with existing SOC, detection engineering, and security operations processes to create an ongoing validation program.

Establish: Validation Strategy & Baseline

Effective validation begins with structure and alignment.

AttackIQ Professional Services works with your team to:

- Define scope and validation objectives
- Align testing priorities to relevant adversary behaviors
- Configure assessments within the AttackIQ platform
- Establish baseline performance metrics
- Define roles, responsibilities, and reporting cadence

This phase creates a foundation for measurable, repeatable validation.

Continued on next page.

Validate: Adversary Emulation & Control Testing

AttackIQ Vanguard executes adversary emulations aligned to MITRE ATT&CK to assess real-world control effectiveness.

Activities may include:

- Prioritized adversary technique testing
- Detection validation across EDR, SIEM, NDR, and cloud controls
- Preventive control effectiveness testing
- Cross-environment validation (endpoint, network, cloud)
- Emerging threat assessments

Results provide objective evidence of which controls detect, prevent, or fail to detect specific techniques.

Operate: Continuous Improvement & Remediation Guidance

Security validation is most effective when integrated into ongoing operations.

AttackIQ Professional Services supports your team by:

- Analyzing validation results to identify gaps and weaknesses
- Recommending prioritized remediation actions
- Guiding detection tuning and policy refinement
- Tracking performance trends over time
- Refining KPIs to support continuous improvement

Over time, when validation becomes embedded in standard operating procedures, it helps strengthen detection and prevention capabilities across the program.

Continued on next page.

Engagement Cadence Options

AttackIQ Vanguard is delivered based on a validation-based cadence with an advisory posture. Engagement model selection should align with operational maturity, risk profile, and internal staffing capacity.

All engagement options include MITRE ATT&CK–aligned adversary emulations, structured reporting, and co-managed advisory support.

	Vanguard Enterprise	Vanguard Premier
Assessment Frequency	Monthly validation cycle	Weekly or recurring validation aligned to operational needs
Assessment Scope	Co-managed adversary emulations with expanded coverage	High-frequency and customized adversary emulations
Detection & Control Analysis	Coverage analysis with trend tracking and KPI refinement	Continuous performance monitoring across environments
Remediation Guidance	Ongoing remediation and detection tuning support	Embedded advisory with architectural and deployment guidance
Customization Level	Prioritized scenarios aligned to operational risk	Fully customized, topology-specific, and cross-environment testing
Best Fit	Integrating validation into SOC operations	Mature programs requiring continuous validation and advisory depth

Continued on next page.

Customer Outcomes

Upon engaging with AttackIQ Vanguard, your organization will have:

1. Continuous visibility into security control effectiveness
2. Measurable detection and prevention performance data
3. Identified and prioritized security control gaps
4. A defined validation cadence aligned to threat activity
5. Improved operational confidence in cybersecurity readiness

Throughout the engagement, experienced advisors support your organization's continued development of a sustainable validation practice.

Professional Services Expertise

AttackIQ is a founding Research Partner in MITRE's Center for Threat-Informed Defense and an active contributor to threat-informed security practices.

AttackIQ Professional Services operators bring experience from government, intelligence, and enterprise cybersecurity environments. The team applies established adversary emulation methodologies and operational best practices developed through extensive customer engagements.

Getting Started

To begin an AttackIQ Vanguard engagement, contact your AttackIQ account team.

ATTACKIQ

U.S. Headquarters
171 Main Street Suite 656
Los Altos, CA 94022
+1 (888) 588-9116
info@attackiq.com

About AttackIQ

AttackIQ is the industry's leading Continuous Threat Exposure Management (CTEM) platform, enabling organizations to measure true exposure, prioritize risk, and disrupt real-world attack paths. By moving beyond static vulnerability data, AttackIQ operationalizes CTEM by continuously validating exposures against real adversary behavior and defensive controls. The platform connects vulnerabilities, configurations, identities, and detections into adversary-validated attack paths—quantifying the likelihood of attacker movement and impact. This evidence-based approach empowers security leaders to focus on what matters most, optimize defensive investments, and strengthen resilience through threat-informed, AI-driven security operations.

The company is committed to supporting its MSSP partners with a Flexible Preactive Partner Program that provides turn-key solutions, empowering them to elevate client security. AttackIQ is passionate about giving back to the cybersecurity community through its free award-winning AttackIQ Academy and founding research partnership with MITRE Center for Threat-Informed Defense.