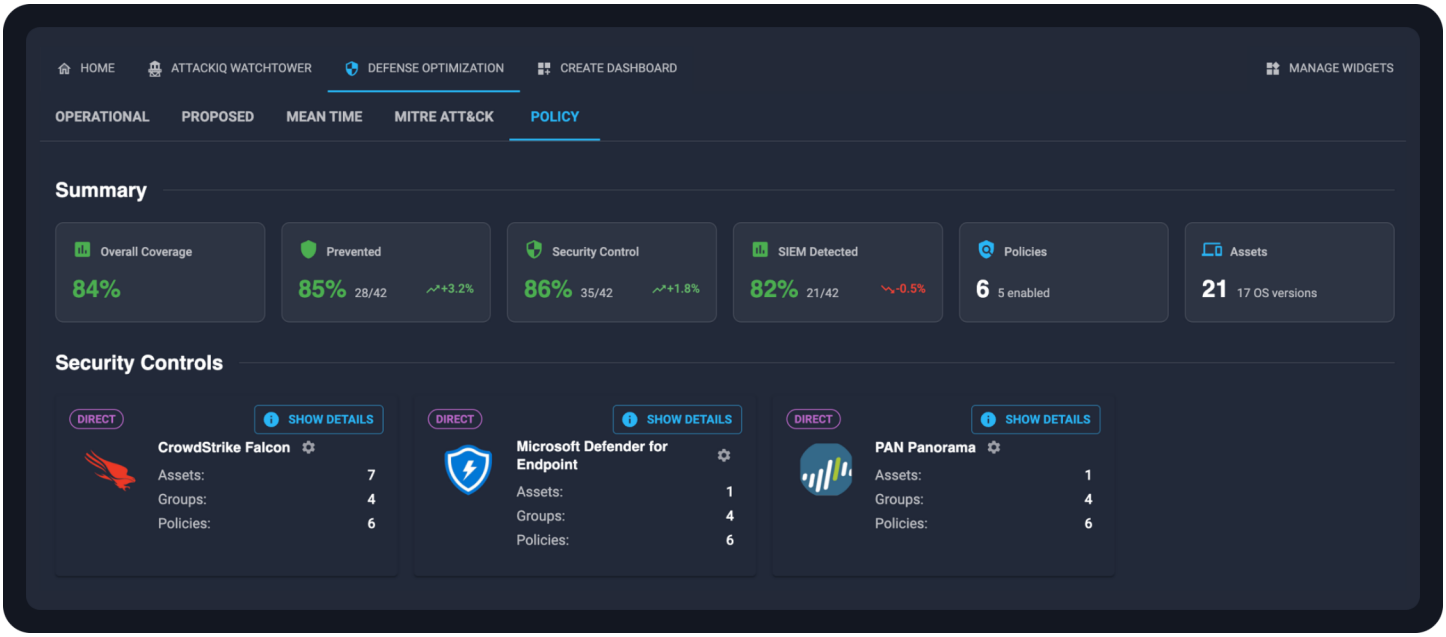
A SOC Optimization Service

Defense Optimization

SOCs are inundated with alerts, detections decay over time, and security controls drift—undermining security operations, increasing inefficiency, and driving analyst burnout. The Defense Optimization Service helps organizations manage and optimize security controls and detections as an ongoing practice, maximizing effectiveness while minimizing alert fatigue.



Cyber Defense Optimization, Continuously Validated

AttackIQ Professional Services partners with you to build a threat-informed detection management practice that improves detection coverage, quality, and effectiveness across the SOC.

Through the engagement, you will:

- Learn to evaluate and develop robust detections mapped to MITRE ATT&CK
- Implement detection rule management with KPIs that drive defense optimization
- Establish a continuous process for reducing the mean time to detect and false positives
- Increase SOC effectiveness by identifying coverage gaps and redundancies

Service Description

The Defense Optimization Service teaches a threat-informed defense approach to detection engineering and guides organizations in developing an optimized cyber defense.

AttackIQ Professional Services delivers advisory services tailored to the organization, beginning with training on threat-informed defense, detection engineering and management, as well as security control validation. Following training, the team takes a hands-on approach to building an enduring practice for managing detection rules and security control policy management within the AttackIQ platform.

Train: Foundational Knowledge Development

Training begins with a 3-hour workshop designed for security analysts and team leads with a goal of preparing the organization to implement a threat-informed defense approach to detection engineering.

Key topics include:

- Threat-informed defense and MITRE ATT&CK fundamentals
- Building robust detections with MITRE's Summiting the Pyramid methodology
- Mapping cyber threat intel, logs, and detections to MITRE ATT&CK
- Four-dimensional framework for detection management
- Establishing a continual process (team, KPIs, weekly cadence)

Target participants include team leads, managers, detection engineers, purple teams, and SOC analysts.

Establish: Visibility, Validation, & Measurement

Optimizing cyber defense starts with visibility. AttackIQ Professional Services works in partnership with the customer to configure AttackIQ integrations – creating visibility across security controls, detection rules, policies, and assets. With visibility established, customers are trained to apply their knowledge of threat-informed defense and detection engineering to validate and manage detections in the AttackIQ platform. AttackIQ Professional Services then guides customers in establishing metrics for program measurement.

Operate: Continuous Improvement

Enabled by AttackIQ Defense Optimization, customers practice managing and optimizing security controls and detections. Through ongoing consultation, AttackIQ Professional Services guides customers as they operate with a focus on continuous improvement. KPIs are refined as the program evolves into an enduring practice, maximizing cyber defense effectiveness.

Customer Outcomes

Upon completion of the Defense Optimization Service, you will have:

1. Upskilled your detection engineering team
2. Launched a continuous process for detection rule management
3. Identified and eliminated coverage gaps and redundancies
4. Implemented a set of KPIs that will drive defense optimization

Throughout the engagement, experienced advisors support your organization's ongoing defense optimization.

Professional Services Expertise

AttackIQ is a founding Research Partner in MITRE's Center for Threat-Informed Defense and an active leader in advancing threat-informed defense as a practice across the security community. In this role, AttackIQ contributes to MITRE's Summiting the Pyramid research program, which focuses on engineering cyber analytics to make adversary evasion more difficult.

AttackIQ Professional Services operators bring experience from government, intelligence, and commercial cybersecurity environments. The team applies proven implementation patterns and operational best practices, developed through years of customer engagement, to help organizations systematically advance their security operations.

Getting Started

To begin a Defense Optimization 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, the leading provider of Adversarial Exposure Validation (AEV) solutions, is trusted by top organizations worldwide to validate security controls in real time. By emulating real-world adversary behavior, AttackIQ closes the gap between knowing about a vulnerability and understanding its true risk. AttackIQ's AEV platform aligns with the Continuous Threat Exposure Management (CTEM) framework, enabling a structured, risk-based approach to ongoing security assessment and improvement.

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.