ATTACKIQ

Defense Optimization

Prove detections work. Measure speed. Improve continuously.

Security teams spend heavily on EDR, SIEM, and cloud controls—yet still struggle with blind spots, noisy alerts, and detections that decay over time.

AttackIQ Defense Optimization helps you prove, measure, and improve how your security stack logs, detects, and prevents real attacker behavior.

It unifies validation outcomes, maps them to MITRE ATT&CK, and adds Mean Time to Detect (MTTD) analytics so you can see both coverage and detection speed across your security stack in one place.

Defense Optimization Challenges

Alert Fatigue & Noise
Too many alerts, too little confidence—analysts waste time chasing false positives while true gaps hide in the noise.

Detection Decay Over Time
Rules and detections age out as environments change, leaving "configured" coverage that no longer works in practice.

Unknown Coverage Across Tools
Teams can't easily answer: Which techniques are covered? Where are the gaps? Which control is responsible?

Slow Detection & Pipeline Delays
Even when detections exist, they may be too slow. Without MTTD visibility, teams can't pinpoint where time is being lost.

HIGHLIGHTS

Find Your Gaps

See what was missed vs. logged, detected, or prevented—by control, device, and test scenario.

Prove Detections Work

Validate which rules actually fire on real attacker behavior, not just what's configured.

Accelerate Detection Engineering with AI

Generate and translate detection rules faster, then re-test to confirm improvement.

Measure Detection Speed (MTTD)

Spot slow detections and pipeline delays with MTTD insights and trends over time.

Automate CTI Integration

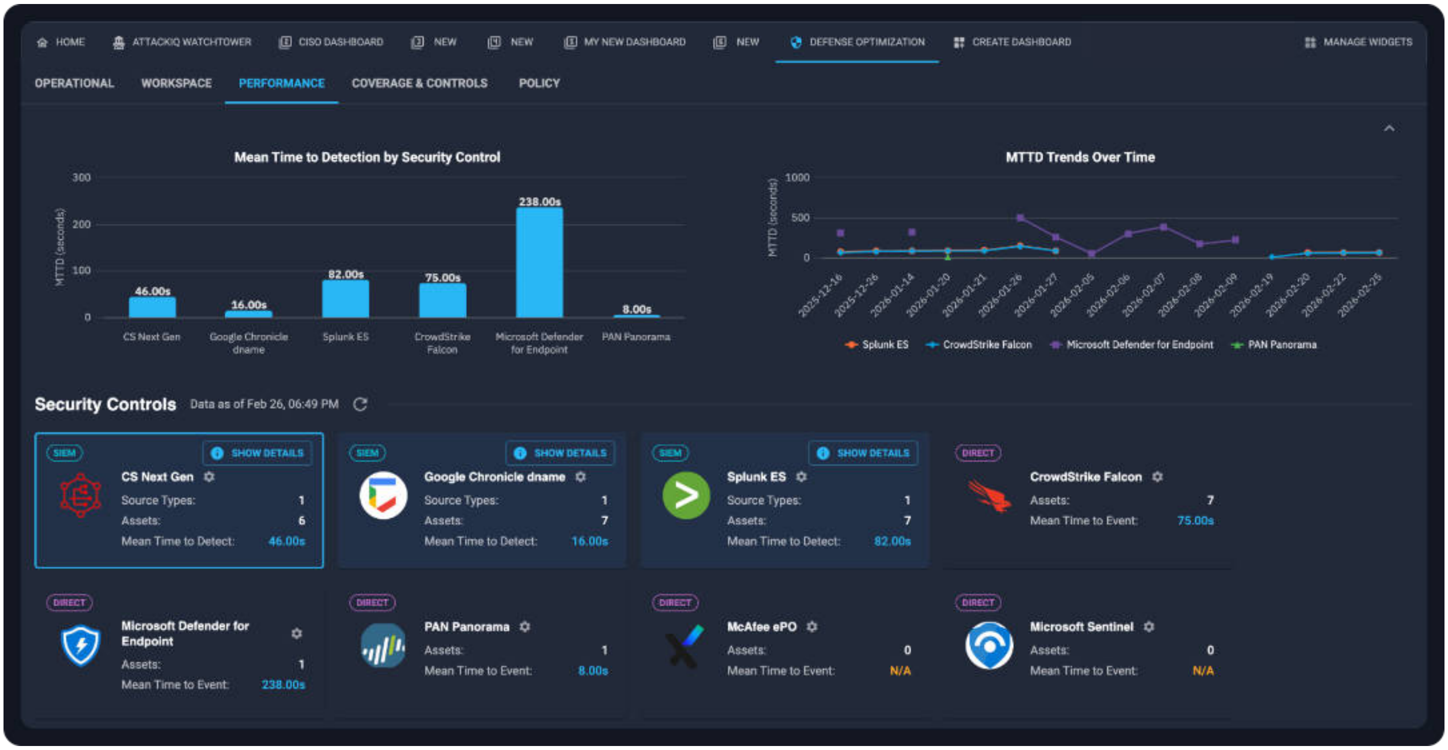
Translate threat reports into threat-informed validation and security coverage analysis automatically.

Analyze Defenses Through Custom Lenses

Filter MITRE ATT&CK coverage and outcomes by threat intelligence, techniques, assessments, or business entities you care about-so teams see what matters for specific security missions.

AttackIQ Defense Optimization turns validation into measurable SOC improvement.

Defense Optimization brings your detection and control validation views into one place—so teams can run a continuous loop to validate attacks, observe outcomes, measure performance, and improve detections and policies. Instead of pivoting between tools and reports, you get unified visibility into what was prevented, detected, logged, or missed. MTTD and trend analytics reveal which controls are strongest, slowest, or degrading over time.



Security Controls Data as of Feb 26, 06:49 PM

SIEM
CS Next Gen
Source Types: 1
Assets: 6
Mean Time to Detect: 46.00s

SIEM
Google Chronicle dname
Source Types: 1
Assets: 7
Mean Time to Detect: 16.00s

SIEM
Splunk ES
Source Types: 1
Assets: 7
Mean Time to Detect: 82.00s

DIRECT
CrowdStrike Falcon
Assets: 7
Mean Time to Event: 75.00s

DIRECT
Microsoft Defender for Endpoint
Assets: 1
Mean Time to Event: 238.00s

DIRECT
PAN Panorama
Assets: 1
Mean Time to Event: 8.00s

DIRECT
McAfee ePO
Assets: 0
Mean Time to Event: N/A

DIRECT
Microsoft Sentinel
Assets: 0
Mean Time to Event: N/A

Maximize detection effectiveness, minimize alert fatigue—and prove your SOC is getting faster over time. **Schedule a demo.**

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.