Driving Adversarial Exposure Validation Across CTEM Stages

AttackIQ's comprehensive approach to Continuous Threat Exposure Management (CTEM) empowers organizations to continuously validate exposure and enhance their security posture by combining threat intelligence, attack surface discovery, and breach and attack simulation. Here's how AttackIQ delivers comprehensive value across the CTEM lifecycle, ensuring tailored benefits for your security organization.

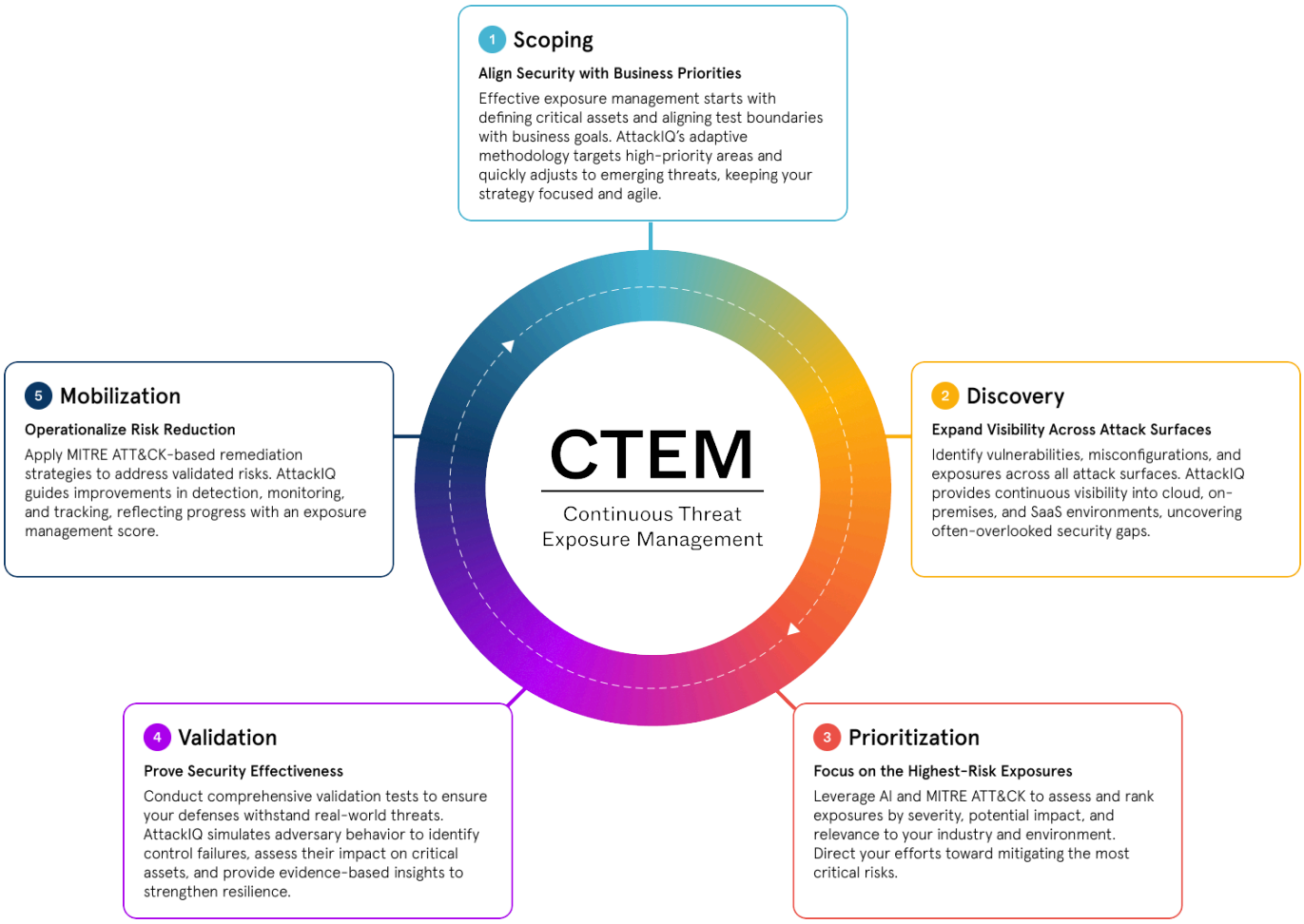
Gartner's insights reinforce this. They predict that:

"By 2026 organizations that prioritize their security investments based on a continuous exposure management program will be three times less likely to suffer a breach."

Gartner, "How to Manage Cybersecurity Threats, Not Episodes", August 21, 2023

At the heart of CTEM is Adversarial Exposure Validation (AEV)—the combination of adversary emulation, automated pentesting, and security control validation with breach and attack simulation. AttackIQ's platform takes this a step further by integrating attack surface discovery, vulnerability intelligence, and threat intelligence, enabling organizations to focus on actionable insights instead of noise. This approach delivers a consistent, real-time view of your most significant risks, empowering security teams to make faster, more informed decisions to protect critical assets. Furthermore, adopting a CTEM strategy can reduce risk by up to 30%.

AttackIQ's Adversarial Exposure Validation Platform supports every phase of CTEM by combining attack surface discovery, vulnerability intelligence, and adversary validation. This integrated approach delivers a continuous, data-driven defense against evolving threats.



1. Scoping: *Immediate Testing of Your Scoped Area*

Start your CTEM journey by defining focused test areas and high-risk assets that align with your organization's priorities. AttackIQ enables CISOs, SOC Analysts, and IT Administrators to act decisively with a clear understanding of where to concentrate efforts.

- **Define Focus Areas:** Identify critical boundaries and areas where testing will be most impactful.
- **Adapt to Evolving Threats:** Adjust scoping dynamically as new risks emerge.
- **Prioritize Assets:** Determine areas of focus based on asset criticality.

AttackIQ's scoping methodology is guided by precision and purpose, ensuring that testing efforts are both targeted and effective. For CISOs, this provides a strategic overview to inform broader security decisions. Security Managers gain clarity on which areas demand immediate attention, while Security Engineers receive actionable guidance to prepare for testing.

2. Discovery: *Findings at Your Fingertips*

Discovery capabilities seamlessly uncover devices, misconfigurations, and vulnerabilities. AttackIQ's adversary-informed approach continuously shows actionable intelligence that will inform validation tests.

- Discover devices and users across your environment.
- Identify vulnerabilities and misconfigurations that pose a threat.
- Access detailed insights into device configurations and software inventories.

AttackIQ internal, external and integration-sourced discoveries empower Security Managers to visualize critical gaps, Security Engineers to proactively address misconfigurations, and CISOs to make data-backed strategic validation and mobilization decisions. Real-world adversary behaviors inform these insights, ensuring organizations stay ahead of threats.

3. Prioritization: *Ready-to-Run Tests Tailored for You*

Leverage AttackIQ to continuously obtain prioritized, high-impact tests aligned with your organization's attack surface. This stage transforms discovery insights into targeted actions in the form of validation tests.

- Execute prioritized tests based on discovery findings and scoped devices.
- Address critical findings first to validate exposure where it matters most.
- Expand testing recommendations dynamically as scoping expands.

AttackIQ's prioritized tests help CISOs focus on impactful exposure reduction, while Security Managers prioritize security controls to validate based on alignment with critical findings. Security Engineers benefit from early visibility on where to act first.

4. Validation: *Adversary-Validated Exposures*

Confirm your defenses' effectiveness and resilience against discovered gaps and misconfigurations. By simulating real-world adversary tactics, organizations gain evidence-backed confidence in their security posture. Validation is critical to prove that security controls are prepared to withstand attacks.

- Gain confidence in your defenses by knowing which specific TTPs (Tactics, Techniques, and Procedures) are detected or prevented.
- Understand critical exposures and their impact on your security, allowing you to gauge risk.
- Measure your overall posture scoring, providing a clear, easy-to-understand benchmark of your resilience.

For CISOs, this stage provides test-backed evidence to showcase security effectiveness. Security Managers can validate and fine-tune detection rules, while Security Engineers identify where defense layers demand immediate attention to increase resilience. AttackIQ's adversary-informed simulations ensure realistic and actionable insights.

5. Mobilization: *Actionable Remediation Guidance*

Turn insights into action with AttackIQ's mitigations, offering detailed guidance tailored to your validated exposures. Each validated exposure includes a set of strategies designed to help you prevent and detect TTPs your controls did not withstand in the validation phase.

- Access mitigation strategies mapped to exposures and security controls.
- Leverage detection rules to strengthen monitoring and response.

AttackIQ aligns remediation actions with strategic goals for CISOs, while Security Managers receive tailored recommendations to improve detection and monitoring. Security Engineers gain clear, actionable steps to reduce the number of exposures. By combining automation and adversary-informed insights, AttackIQ ensures efficiency and precision.

Empowering Your Security Team to Lead with Confidence

AttackIQ's methodology to CTEM addresses your unique concerns. CISOs can answer critical strategic questions like, "Am I better today than I was yesterday?" and "Where is my risk?" Security Managers are empowered with insights into where to prioritize testing efforts. Security Engineers receive actionable, detailed guidance to execute tests and implement remediations seamlessly.

By bridging these perspectives, AttackIQ ensures alignment across roles, enabling organizations to continuously validate their defenses and drive meaningful security improvements in an ever-changing threat landscape.

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.