ATTACKIQ

AttackIQ Watchtower

AI-Powered Hyperlocal CTI Analyzer for AEV

AttackIQ Watchtower is an AI-powered cyber threat intelligence analyzer that transforms generic threat data into hyperlocal insights tailored to your environment. It automatically generates precise Adversarial Exposure Validation (AEV) recommendations to ensure your defenses are configured against the specific adversaries targeting your organization. Even organizations without a dedicated CTI team can now easily gain immediate access to enterprise-grade adversarial insights with testing emulations at a fraction of the cost.

AttackIQ Watchtower auto-generates testing scenarios based on real threat actor tactics, techniques, and procedures (TTPs), helping to ensure that defenses are resilient against the current threats. This highly proactive approach to hyperlocal threat analysis enables the validation of mitigating and compensating controls to know the level of cyber resilience to those identified threats. Hyperlocal means Watchtower's AI synthesizes threat intelligence that reflects real-world attacker behavior targeting your environment, not generic static reports or industry averages. Measurable and actionable security metrics show how prepared your organization is for those attacks. This proactive strategy enhances your overall security effectiveness.

"Security programs cannot afford to rely on static playbooks or once-a-year audits. AttackIQ Watchtower gives us a view of targeted pre-active adversary behavior, clear guidance on how to test our defenses, and confidence that our controls will hold when it counts. It's a more adaptive, evidence-based approach that helps security leaders shift from reactive checklists to operational readiness."

-Pete Luban, Field CISO, AttackIQ

HIGHLIGHTS

AI Threat Intelligence Agent
Continuously analyzes global threat data and distills it into hyperlocal insights, making enterprise-grade CTI accessible to any security team.

Hyperlocal Threat Visibility
Detect threats actively targeting your organization, not generic assumptions. Ideal for briefing executives on relevant adversaries.

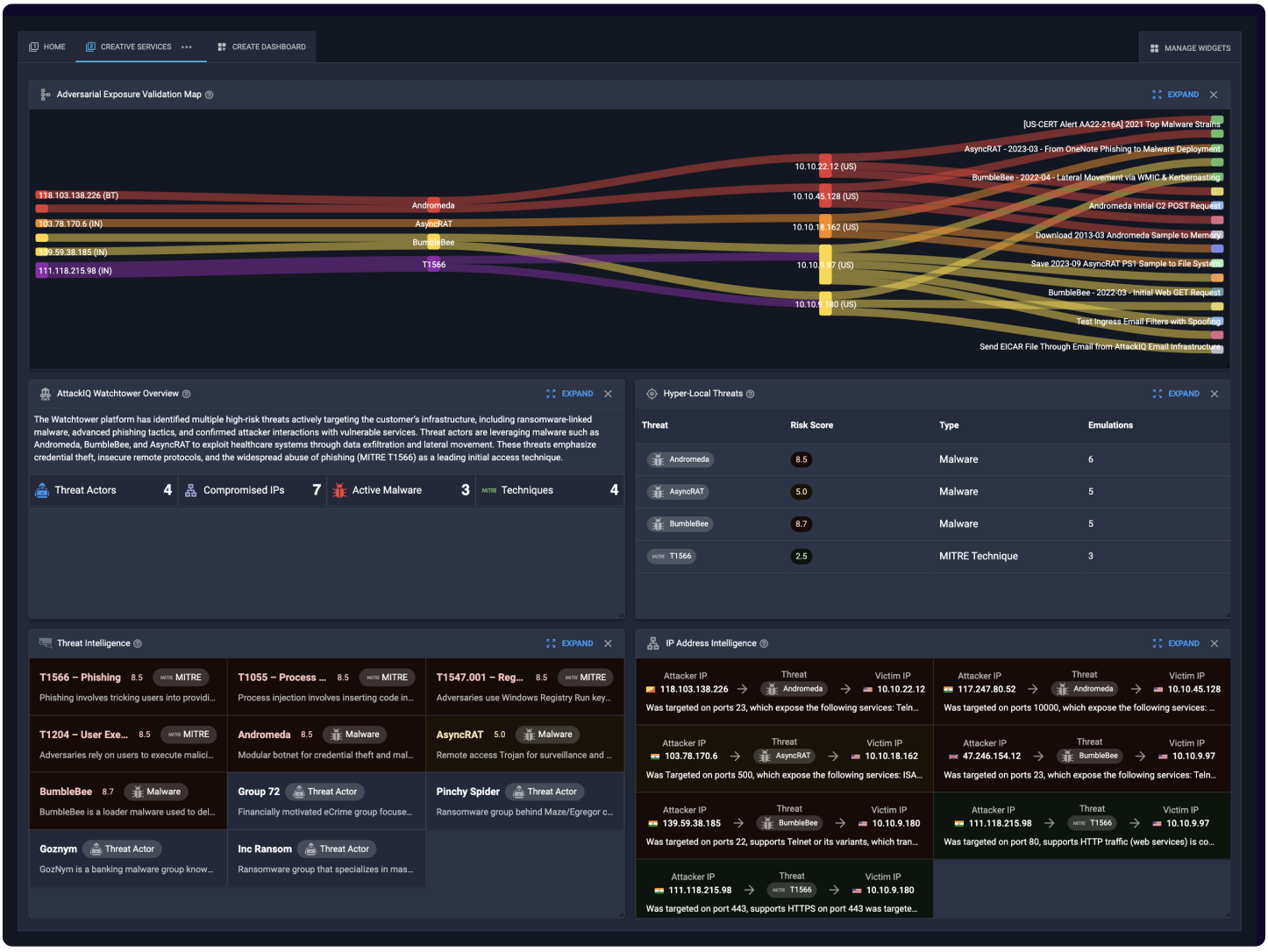
Adaptive Testing Without Manual Effort
Testing scenarios evolve automatically to match changing adversary behaviors and keep defenses current.

Exposure-Focused Defense
Proactively identify overlooked vulnerabilities and close gaps before attackers exploit them—strengthening your defensive posture.

Unique Actionable Intelligence
Use AI to automatically generate tailored detection scenarios and YARA/SNORT rules without manual effort.

Executive-Ready Outcomes
Prove control effectiveness against real-world threats through targeted testing with clear, actionable metrics for leadership.

AttackIQ Watchtower



AttackIQ Watchtower captures actual attacker activities targeting your organization, then automatically analyzes these threats to prescribe specific adversary emulation scenarios based on threat actor TTPs. This dynamic approach ensures organizations can identify and close defense gaps before adversaries exploit them, especially against emerging threats, overlooked vulnerabilities, or unexpected attack vectors. Security teams gain actionable insights, intelligently prioritize efforts, and significantly reduce threat intelligence overload while maintaining resilient defenses against sophisticated, real-world adversaries with measurable outcomes.

Benefits

AttackIQ offers a range of compelling benefits that significantly enhance your organization's security posture and drive a true Security Operations Center (SOC) transformation. One key advantage is reduced alert fatigue and enhanced CTI efficiency, which is foundational to a more effective SOC. Watchtower rapidly and precisely directs threat intelligence teams toward the most critical and timely threats, cutting through the overwhelming noise often associated with threat data. This allows CTI resources to focus on what truly matters, leading to more effective threat hunting and response, and fundamentally changing how your SOC operates.

Beyond driving SOC efficiency, AttackIQ provides:

Measurable Security Outcomes

The platform generates clear, executive-ready metrics that demonstrate the effectiveness of threat detection and blocking capabilities, as well as ongoing defensive improvements. This quantifiable data is invaluable for communicating your security posture to leadership and proving return on investment (ROI).

Enhanced Customer ROI

The platform clearly demonstrates the measurable effectiveness of your security controls, enabling targeted investments, improved resource allocation, and higher customer satisfaction.

Automated, Continuous Testing at Scale

Security testing can be scaled without manual effort, providing continuous validation of your defenses, aligned with real-world attacker behavior. This automation is a cornerstone of an efficient and modern SOC.

AI-Driven Threat Detection

AttackIQ automatically identifies emerging threats with unprecedented speed and precision. This helps to ensure that are always ahead of adversaries and boosts the proactive capabilities of your transformed SOC.

Compelling Executive-Level Outcomes

AttackIQ delivers concise, executive-ready evidence illustrating its strategic value. This clearly shows threats detected, mitigated, and proactively defended against. This ultimately leads to increased adoption and revenue growth.

How AttackIQ Watchtower Works

AttackIQ Watchtower operates through a streamlined three-step process, leveraging hyperlocal threat intelligence to provide AEV recommendations when you are actively targeted by cyber threat actors.

The process is as follows:

Step 1 – Configuration

Customers declare their Classless Inter-Domain Routing (CIDRs) for monitoring. Each customer is allocated a specified number of CIDRs to add to AttackIQ Watchtower, which are then evaluated for hyperlocal cyber security threats. This ensures monitoring is tailored to your organization's specific network segments. Watchtower also supports Bring Your Own CTI. By leveraging an existing threat inteligence provider, the findings will match the taxonomy already in use inside of your organization and will reflect the customization of the existing CTI feeds. Watchtower will deduplicate and normalize multiple CTI feeds, providing actionable insights.

Step 2 – Generation of Recommendations

Once network traffic metadata is collected from the specified IP ranges, they are passed to AI-based AttackIQ Virtual Advisor (AVA). AVA matches these flows against extensive CTI collected daily from leading threat-intelligence sources or from your own CTI if configured. Based upon this comparison, AEV recommendations are generated, and each assigned an importance level (High, Medium, or Low, on a scale of 1-10). AVA generates a weekly report summarizing prioritized recommendations and observed threat activity, providing a clear overview of identified exposures.

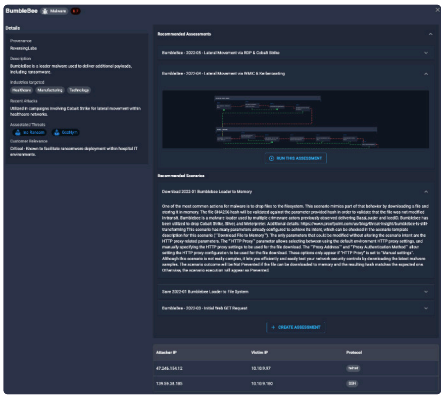
Step 3 – User Interface Integration

Findings and recommendations from AttackIQ Watchtower are seamlessly integrated into the AttackIQ User Interface. This integration offers comprehensive visibility into identified threats and provides actionable insights. These insights enable security teams to quickly understand their exposure and prioritize remediation efforts effectively. The dashboard includes a "What's New" section, lists of threat actors, adversary cards with emulation options, a hyperlocal threat explorer visualizing threats and mitigations, and criticality rankings to prioritize actions.

Why Watchtower

AI-Driven Threat Intelligence and Automated Testing

AttackIQ Watchtower delivers automated, scalable, and adaptive security testing with unmatched speed and accuracy, all powered by advanced AI. It leverages AttackIQ's unique strengths in generative AI, a deep library of AEV emulations, and the ability to generate and validate YARA and SNORT signatures. This ensures your organization continuously identifies and tests against rapidly evolving threat actor behaviors, receiving high-value, proprietary detection capabilities and content.



This proactive approach significantly boosts your ROI. Watchtower automatically pinpoints defensive gaps, validates controls against active threats, and streamlines threat prioritization. By clearly demonstrating security effectiveness and measurable outcomes to executives, it helps you articulate the tangible value of your security program and secure future investments.

Impact for Enterprises, MSSPs, and Partners

AttackIQ Watchtower delivers significant value across diverse organizational structures, from large enterprises to managed security service providers (MSSPs) and partners, by empowering them with advanced security validation capabilities.

For Enterprises

AttackIQ Watchtower provides a unified approach to fully automated agentic CTI analysis and security validation, enabling consistent practices and elevating security maturity across distributed business units. Through the AttackIQ Command Center, enterprises can precisely tailor validation scenarios to team requirements, compare results across units for optimized posture, and streamline organization-wide compliance reporting, ensuring a robust and consistent security framework.

For MSSPs

AttackIQ Watchtower provides a powerful yet economical pre-active hyperlocal CTI analysis to every customer. When integrated with AttackIQ Command Center it enables MSSPs to centrally manage multiple client deployments, offer flexible tiered services, and efficiently scale their validation business and services business. MSSPs can enhance their portfolio by offering new high-value security services.

For Partners

AttackIQ Watchtower helps to facilitate extremely economical CTI analysis capabilities for organizations on tight budgets. It provides actionable insights into adversaries targeting their organization at a fraction of the cost of traditional detection engineering and CTI solutions.

Conclusion

AttackIQ Watchtower fundamentally improves security by observing real attacker behaviors, providing actional insights and recommendations, while leveraging AI to automatically build testing scenarios based on observed threat actor TTPs. This helps to ensure that defenses are continuously resilient against current threats, reducing alert fatigue, and enhancing overall security effectiveness. Watchtower helps you stay ahead of adversaries.

AttackIQ Watchtower drives a true SOC transformation, delivering measurable security outcomes, AI-driven threat detection, and automated, continuous testing at scale. This powerful combination results in enhanced customer ROI and compelling outcomes across enterprises, MSSPs, and partners, clearly demonstrating the strategic value of the AttackIQ platform.

Ready to see AttackIQ in action?

- **Request a Demo:** attackiq.com/demo
- **Start Your Free Trial:** attackiq.com/free

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.