Persistent

Practitioner Point Of View

Beyond Alphabet Soup

Case for Attack-Chaining Vulnerability Management

After two decades as a CISO, I have watched our industry do one thing with extraordinary consistency: when a new threat emerges, we invent a new acronym, build a new point product and declare victory — until the next breach proves otherwise.

Dilip Panjwani
Cybersecurity Practice Head

Two decades of CISO experience watching our industry rename the same problems. Here is why Claude Mythos changes the question entirely — and what security leaders must ask next.

We now operate in a world crowded with CTEM, CNAPP, CIEM, DSPM, SIEM, SOAR, RBVM — each solving a slice of a problem that, at its core, has never been fragmented to begin with. Adversaries do not respect our taxonomy. They chain. They pivot. They synthesize. And for years, our defenses did not.

The Security Acronym Landscape

CTEM
Continuous Threat Exposure Management

CWASP
Cloud Workload Application Security Posture

CNAPP
Cloud-Native Application Protection Platform

CIEM
Cloud Infra. Entitlement Management

SIEM
Security Info. and Event Management

SOAR
Security Orchestration, Automation & Response

DSPM
Data Security Posture Management

RBVM
Risk-Based Vulnerability Management

ABVM
Attack-Based Vulnerability Management

When AI Collapses Alphabet Soup

AI now gives us something our tools never could: The ability to collapse this sprawl into a single coherent intelligence layer. A security misconfiguration connects to a threat alert and a compliance gap — and the system generates a Terraform template to remediate it. All the security data is synthesized, correlated and rendered into a board-ready narrative. Not three dashboards and a pivot table. One answer. I have spent the better part of two decades fighting for that synthesis manually — through governance frameworks, integration projects and brutal tuning of SIEM correlation rules. The idea that an AI platform can now do that coherently is not incremental. It is architectural.

> The practitioner in me does not celebrate the technology. It celebrates the outcome: Security teams spending time on decisions, not data reconciliation.

Dilip Panjwani
Cybersecurity Practice Head

What Claude Mythos Actually Did to Vulnerability Management

Then came Anthropic's Claude Mythos Preview. And it shifted the conversation in a way that warrants direct attention from every security leader.

Mythos did not simply find vulnerabilities faster. It expedited the discovery and chaining of vulnerabilities by elevating observations that would previously have been processed through Common Vulnerability Scoring System (CVSS) scores and RBVM principles into something far more dangerous in the wrong hands and far more powerful in the right ones: Context-aware attack chains. CVSS gives a vulnerability a number. RBVM adds business context to prioritize it. Both still assume a relatively static, linear view of risk. What Mythos demonstrated is that an AI system can now reason across the full attack graph by identifying how a CVE-9.8 in an edge system that the scanner de-prioritized because it sits behind a WAF can be chained with a mis-configured IAM role and an exposed S3 bucket to produce a critical breach path. That is not a score. That is a narrative. And narratives are how breaches actually happen.

RBVM was Never Enough. ABVM is What We Actually Need?

The distinction between Risk-Based and Attack-Chaining Vulnerability Management is not semantic. It is strategic.

Dimension	RBVM	ABVM
Core Logic	Prioritize by CVSS + asset criticality + exploitability	Map real attack paths, prioritize by blast radius of chains
Threat Model	Vulnerability-centric, each CVE evaluated in relative isolation	Adversary-centric, models attacker lateral movement and chaining
Output	Prioritized patch list	Mitigation strategy mapped to actual breach scenarios
AI Role	Scoring acceleration, de-duplication	Attack graph generation, automated chain discovery
Board Narrative	We patched 87% of criticals this quarter	We closed the three attack paths that could have led to crown jewel exfiltration

Boards do not fund patch percentages — they fund business resilience. ABVM speaks their language, because it speaks in outcomes, not metrics.

Four Questions Every Security Leader Must Now Answer

01 Find or Fortify?

Will we continue to invest primarily in finding vulnerabilities — scanning, testing, detection — or shift investment upstream into secure coding and secure deployment? DevSecOps and CI / CD guardrails represent a fundamentally different ROI model: Prevent the vulnerability class from ever reaching production. The answer is not binary, but the budget allocation signals strategic intent.

02 RBVM or ABVM — or both?

Risk-Based Vulnerability Management is not obsolete. It is incomplete. As AI-powered attack-chaining becomes a capability available to nation-states and organized crime alike, defenders who rely only on CVSS scores are fighting the last war. ABVM should augment RBVM — not replace it — and the integration point is the AI layer that can reason across both.

03 Who owns the attack graph?

Traditional structures divide this across AppSec, InfraSec, CloudSec and Red Teams. Attack-chaining requires a unified view. Whether this sits in a platform like CyberBox™ or a bespoke integration, the accountability model must match the threat model. A siloed team cannot defend against a chained attack.

04 Is your board presentation telling the right story?

If the monthly risk report leads with patch counts and CVSS heatmaps, you are presenting the language of tools, not the language of risk. The AI synthesis capability Mythos exemplifies should ultimately feed a board narrative that maps to business impact — not security taxonomy.

Posture That Follows

Twenty years in this industry teaches you to be skeptical of hype and deliberate about signal. Mythos is signal. Not because Anthropic says so — but because the capability it demonstrated maps directly to how sophisticated adversaries have operated for years. We have been playing catch-up with manual threat modeling and red team exercises. AI-powered attack chaining means the gap between attacker capability and defender insight can, for the first time, meaningfully close. At Persistent, we are building this into how we deliver cybersecurity as a service — through CyberBox™ — because our clients deserve not just a patch queue but a breach narrative, and not just a compliance dashboard but an attack-path mitigation roadmap. The era of siloed point products is not ending because of AI. It ended because the threats outgrew the architecture. AI is simply giving us the means to build what we should have built a decade ago.The acronyms will keep coming. ABVM may well join the soup. But if it forces the industry to think in attack chains rather than CVE lists — even for one planning cycle — it will have earned its place.

About the Author

Dilip is a seasoned cybersecurity leader with over two decades of experience serving as CISO across major BFSI institutions, fintech organizations and global IT enterprises.

Across these roles, he has been responsible for securing high value financial systems, regulatory driven environments and large scale digital transformation programs. His work spans enterprise security architecture, threat management, data protection, cloud security and building cyber resilience for organizations operating in some of the most demanding risk landscapes.

Today, Dilip leads the cybersecurity practice and delivery function at Persistent, where he partners with CIOs, CISOs, CTOs and digital leaders to elevate their cybersecurity maturity, strengthen governance and build future ready security programs.

His unique blend of practitioner depth and advisory experience gives him a 360 degree view of the challenges enterprises face as they navigate emerging threats like cyber risk management, quantum risk, AI driven attacks and regulatory complexity.

Dilip is a trusted voice in the cybersecurity community and a leader who continues to shape how organizations think about security, resilience and digital trust.

Reference: Anthropic Claude Mythos Preview: https://red.anthropic.com/2026/mythos-preview/

Views are personal, not representative of Persistent official position.

Re(AI)magining™ the World

About Persistent

Persistent Systems (BSE: 533179 and NSE: PERSISTENT) is a global services and solutions company delivering AI-led, platform-driven Digital Engineering and Enterprise Modernization to businesses across industries. With over 27,500 employees located in 21 countries, the Company is committed to innovation and client success. Persistent offers a comprehensive suite of services, including software engineering, product development, data and analytics, CX transformation, cloud computing, and intelligent automation. The Company is part of the MSCI India Index and is included in key indices of the National Stock Exchange of India, including the Nifty Midcap 50, Nifty IT, and Nifty MidCap Liquid 15, as well as several on the BSE such as the S&P BSE 100 and S&P BSE SENSEX Next 50. Persistent is also a constituent of the Dow Jones Best-in-Class World Index. The Company has achieved carbon neutrality, reinforcing its commitment to sustainability and responsible business practices. Persistent has also been named one of America's Greatest Workplaces for Inclusion & Diversity 2025 by Newsweek and Plant A Insights Group. As a participant of the United Nations Global Compact, the Company is committed to aligning strategies and operations with universal principles on human rights, labor, environment, and anti-corruption, as well as take actions that advance societal goals. With 468% growth in brand value since 2020, Persistent is the fastest-growing IT services brand in 'Brand Finance India 100' 2025 Report.

USA
Persistent Systems, Inc.
2055 Laurelwood Road, Suite 210
Santa Clara, CA 95054
Tel: +1 (408) 216 7010
Fax: +1 (408) 451 9177
Email: info@persistent.com

India
Persistent Systems Limited
Bhageerath, 402
Senapati Bapat Road
Pune 411016
Tel: +91 (20) 6703 0000
Fax: +91 (20) 6703 0008

Persistent
Re(AI)magining the World

www.persistent.com