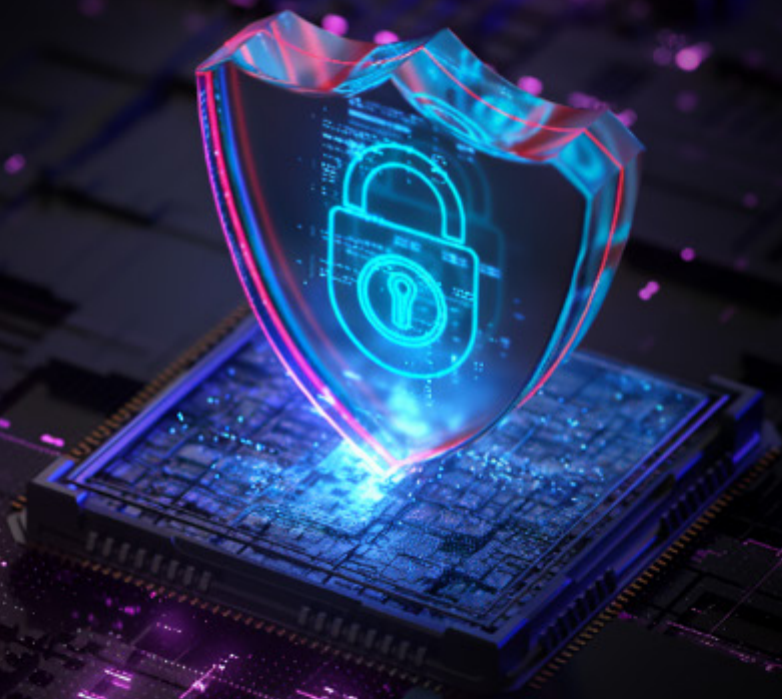


CTEM service for Frontier AI era



Atos |  tenable®

Atos Continuous Threat Exposure Management (CTEM) services

The release of Claude Frontier AI era Preview exposed an uncomfortable truth: the time between vulnerability discovery and exploitation has collapsed. What once took weeks now happens in hours, sometimes minutes. In the Frontier AI era, the window for human-speed remediation continues to shrink, making traditional reactive defense obsolete. Modern CTEM must detect, prioritize, and respond faster and smarter than ever before.

Atos CTEM is built for that outcome. Powered by the Atos-Tenable Vulnerability Operations Center (VOC), it brings together AI-driven exposure management and globally scaled cyber defense to move organizations from reactive patching to proactive risk reduction. With unified visibility across the enterprise and intelligence-driven prioritization, Atos becomes more than a service provider; it becomes a strategic partner in safeguarding business continuity.



Why enterprises need next-generation CTEM today

Security leaders are facing a simple reality: risk is rising faster than response capacity. Next-gen CTEM is critical because it addresses the gaps that most organizations can't close internally:

- **Threats move faster than teams can respond** AI-driven attacks and autonomous models like Frontier AI automate the scale and speed of exploits, demanding machine-speed defense.
- **Vulnerability volume is overwhelming** With an order-of-magnitude increase in vulnerabilities, relying on raw CVSS scores is no longer viable; prioritizing based on real risk is essential.
- **The attack surface is too broad to manage in silos** Enterprises must secure IT, cloud, identity, network, and OT/IoT, requiring unified visibility, not fragmented tools.
- **Shadow AI introduces unseen risks** Unsanctioned AI tools and excessive permissions create invisible entry points and complex, multi-agent attack chains.

The "Frontier AI-Ready" Architecture: Aligned to Your Operating Reality

To stay ahead of AI-accelerated threats, Atos and Tenable integrate VOC capabilities into a comprehensive framework that adapts to your environment:

Prepare Through our joint VOC and CTEM capabilities, we continuously map your entire attack surface across IT, cloud, identity, OT, and AI. By prioritizing exposure based on real risk, we ensure that the routes leading to your critical assets are closed early.

Respond Our Managed Detection & Response (MDR) delivers intelligence-led detection and proactive threat hunting. We don't wait for alerts; AI accelerates correlation, investigation, and triage through our AI Virtual SOC Analyst to reduce the time attackers can operate undetected.

Adapt We utilize regular Breach & Attack Simulation (BAS) to keep detections and response playbooks aligned with reality—not assumptions.

Why Atos & Tenable?

A structured, end-to-end approach that ensures consistent coverage, coordinated execution, and measurable risk reduction:

- **Vulnerability Operations Center (VOC)** Makes exposure management highly operational and affordable, asking "what will actually be used against us?" rather than just "what is vulnerable?".
- **Tenable Hexa AI** Automates the heavy lifting of asset discovery, tagging, and triage to remove triage bottlenecks and keep pace with vulnerability volume.
- **Vulnerability Priority Rating (VPR)** Uses machine learning to analyze the actual threat landscape, narrowing down thousands of vulnerabilities to the ~1.6% that pose an immediate risk.
- **Attack Path Analysis via ExposureAI** Generative AI summarizes complex attack paths in natural language and proactively hunts for legacy vulnerabilities that human reviews might miss.
- **Global Cybersecurity Leader** Supported by 6,500+ security experts and 17 global Security Operations Centers (SOCs) delivering vendor-agnostic operations.



Case study: Securing a global event at scale

Challenges Delivering cybersecurity for one of the world's largest global events required uncompromised resilience across a highly visible, mission-critical ecosystem. Operations had to adapt in real-time to evolving threats while integrating a complex, multi-vendor environment under strict compliance requirements.

Atos solution



Centralized platform combining Atos's expertise and partner technologies.



46 security technologies integrated into a unified Security Information and Event Management (SIEM) environment.



52 billion logs analyzed with 24/7 monitoring and response by global SOC teams.

Business benefits



22 million alerts triaged from 42 billion events.



Zero business impact reported, ensuring uninterrupted operations throughout Paris 2024.



17,000 incidents investigated and resolved by experts.

About Atos Group

Atos Group is a global leader in digital transformation with c. 56,000 employees and annual revenue of c. €7.2 billion (at the go-forward perimeter), operating in 54 countries under two brands - Atos for services and Eviden for products and systems. European number one in cybersecurity and a leader in cloud, Atos Group is committed to a secure and decarbonized future and provides tailored AI-powered, end-to-end solutions for all industries. Atos Group is listed on Euronext Paris.

About Eviden

Eviden is the Atos Group brand focused on cybersecurity products, mission-critical systems and vision AI. A trusted partner to public and private sector organizations, Eviden deploys advanced analytics capabilities and helps ensure the robustness, continuity and resilience of its customers' operations. Leveraging more than 2,200 experts and 720 patents, Eviden helps protect people, data and critical infrastructures worldwide, at the convergence of intelligence, sovereignty and trust.

Find out more about us

atos.net

atos.net/career

Let's start a discussion together



Atos Group is a registered trademark of Atos Group. © Atos Group. Confidential information owned by Atos Group, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos Group.