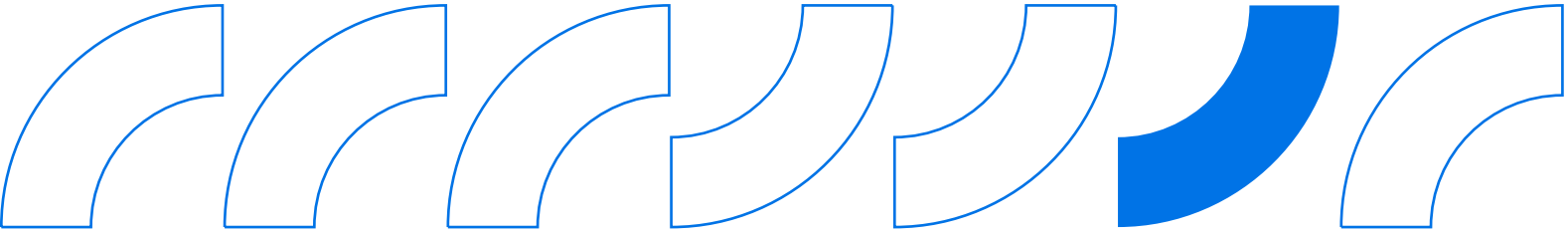
Atos Managed Detection and Response services

Modern Managed Detection Response (MDR) has shifted from purely responsive service to more proactive prevention. In the Mythos era, the window for human speed remediation continues to shrink. MDR must detect and respond faster, smarter and more effectively than ever before. Modern MDR is about speed, proactivity and prioritization.

Atos MDR is built for that outcome.

It brings together always-on operational accountability, deep domain expertise, and globally scaled cyber defense to move organizations from reactive security to confident, end-to-end resilience. With unified visibility across the enterprise, flexible operating models aligned to your reality and intelligence-driven response underpinned by dedicated research and global Security Operations Center (SOC) excellence, Atos becomes more than a service provider, it becomes a strategic partner in safeguarding business continuity and trust.



Why enterprises need next-generation MDR today

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

Threats move faster than teams can respond

AI-driven attacks demand minute-level detection and response to protect business operations and critical assets.

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.

Compliance requires proof, not just intent

Organizations need evidence-based reporting that stands up to audits and regulatory scrutiny.

Cyber skills and capacity remain constrained

Limited in-house expertise makes 24/7 access to experienced analysts essential to sustain operations.

Existing security investments are underutilized

Enterprises need solutions that integrate with current tools and teams to maximize value without added complexity.

Customized delivery model: Aligned to your operating reality

Organizations adopt MDR from very different starting points. Some need a fully managed outcome, others want to extend existing investments, while many prefer to retain partial control. Atos MDR is structured across five distinct models to reduce disruption, preserve existing value, and optimize cost efficiency, ensuring the service adapts to your environment, not the other way around.

Best-fit Security Platforms

End-to-end service

Need a complete MDR capability without building or managing it internally?

This model provides a fully outcome-based service delivered on Atos-owned platforms, eliminating upfront tooling investments and operational setup.

Best fit for: Organizations seeking a fast, low-complexity path to mature security operations.

Managed Microsoft XDR

Already invested in Microsoft E3 or E5 and want to maximize its value?

This model builds MDR directly on existing Microsoft capabilities, avoiding duplicate spend while enhancing detection and response outcomes.

Best fit for: Enterprises looking to optimize current investments without introducing additional platforms.

Flexible technology agnostic MDR

Need MDR that works with your existing or preferred tools?

Designed to integrate across platforms such as Google SecOps, Microsoft Sentinel, Splunk, Elastic, Trend Micro, and others, preserving existing investments while enabling consistent operations.

Best fit for: Organizations seeking flexibility and freedom to evolve their technology stack over time.

Best-fit Engagement models

Full outcome-based MDR service

Looking for clear accountability without managing multiple moving parts?

A fully packaged MDR service delivering end-to-end security outcomes under a single operating model, reducing coordination overhead.

Best fit for: Organizations prioritizing simplicity, consistency, and measurable outcomes.

Co-management

Want to retain control over key security functions while scaling expertise?

This model enables shared responsibility, allowing internal teams to stay in control of critical areas while augmenting with external expertise where needed.

Best fit for: Enterprises with established SOC capabilities looking to extend capacity without disruption.

How Atos MDR works

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

Onboarding
Assess business risks and critical systems, identify relevant data sources, and prioritize use cases aligned to the client's threat landscape - ensuring security efforts are focused where they matter most.

AI-assisted operations
24/7 monitoring and investigation led by Atos experts, augmented by Virtual SOC Analyst and ActiveHunt to improve speed, accuracy, and depth of detection and analysis.

Response
Timely, expert-driven containment actions, combining automation with analyst-led decisions executed in close coordination with client teams to minimize business impact.

Continuous optimization
Security coverage is continuously refined through detection engineering and threat intelligence to keep defenses aligned with evolving threats and attack patterns.

Accountability
Clear, measurable detection and response outcomes, providing transparency, auditability, and ongoing validation of security effectiveness.

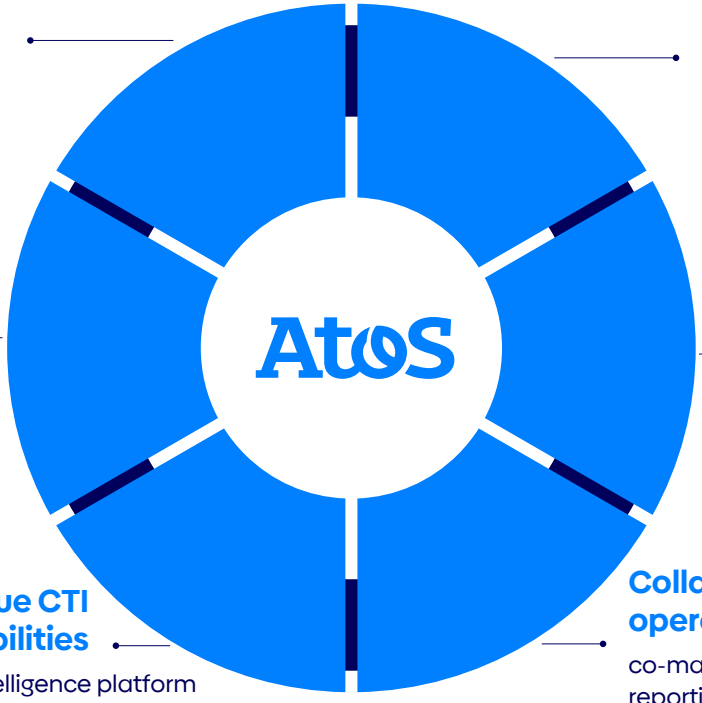
Why Atos?

Vendor-agnostic operations
on the customer's SIEM/ XDR (Microsoft SecOps, Google Chronicle, Splunk/Elastic, others) — no forced re-platform

Responsible AI: Virtual SOC Analyst
+ AI-assisted triage, correlation, and case building across our SOC operations

Unique CTI capabilities
A shared Threat Intelligence platform across **17 Atos SOCs**, enabling rapid detection engineering to keeps pace with emerging threats.

Strategic partnership with Google Threat Intelligence



Threat Research Center
adversary research, dark-web monitoring,
OSINT actionable detections

Strategic Microsoft Partnership
to maximize the value of client' E3 and E5 license investments through enhanced security and operational outcomes

Collaborative operating model
co-managed SOC, outcome-based reporting,
executive briefings,
continual coverage improvements and end-to-end lifecycle: seamless Digital forensics and incident response (DFIR) engagement

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. At the same time, operations had to adapt in real-time to evolving threats while integrating a complex, multi-vendor environment under strict compliance requirements.

Atos solution

Centralized MDR platform combining Atos's expertise, Alsaac, 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	17,000 incidents investigated and resolved by experts	Zero business impact reported, ensuring uninterrupted operations throughout the event

About Atos

Atos Group is a global leader in digital transformation with c. 72,000 employees and annual revenue of c. € 10 billion, operating in 68 countries under two brands — Atos for services and Eviden for products. European number one in cybersecurity, cloud and high-performance computing, Atos Group is committed to a secure and decarbonized future and provides tailored AI-powered, end-to-end solutions for all industries. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
atos.net
atos.net/career

Let's start a discussion together

000000 - INITIALS DESIGNER + INITIALS BP