Atos integrated with Microsoft

Transforming security operations for sovereignty and innovation

A guide to SOC transformation and managed extended detection and response

Microsoft

Why read this guide?

Cybersecurity is no longer a back-office function. It's a board-level priority. Threats are faster, more sophisticated, and more relentless than ever before. Geopolitical shifts are getting harder to predict. Regulators are demanding more stringent data management, and limitations on where data can reside. But legacy platforms and traditional approaches can't keep pace.

The risks of failing to respond extend beyond technology – customers are unforgiving in the face of any loss of service; regulators are issuing larger fines for non-compliance, and the overall cost of a breach is spiraling.

This guide shows how Atos and Microsoft help transform the Security Operations Center (SOC) with an AI-driven security operations model that protects your business, reduces risk, and enables safe innovation. AI-driven security operations support and augment security analysts to reduce risk and enable safe innovation. Data sovereignty and protection assure compliance with both current regulations and those coming in related to AI and Agentic AI, with Managed Extended Detection and Response (MXDR). Modernize and reduce risk while supporting innovation at scale and speed.

What you'll find inside:

- Why a SOC transformation and MXDR are critical for today's digital enterprise
- How Atos and Microsoft combine global expertise with cutting-edge technology
- What an AI-driven SOC with MXDR looks like, and why it matters to your business
- Practical steps to integrate, scale, and maximize ROI
- Proof points and success stories from real-world deployments

Cyber threats don't wait. Neither should your defenses.

Threats move faster, environments are increasingly distributed, and internal teams struggle to scale. At the same time, organizations must maintain control over sensitive data and ensure security operations align with regulatory and sovereignty expectations.

SOC transformation with MXDR ensures organizations are protected as risks evolve and technologies change. A MXDR service must be always-on, AI-enabled and connected across the entire digital estate, without compromising governance or oversight.

What do we mean by SOC transformation?

SOC transformation is the shift from reactive, tool-heavy security operations to an integrated, intelligence-driven model. It combines people, processes, and technology to deliver continuous visibility, faster detection and response, and consistent governance across the entire digital estate.

This is where SOC transformation comes into play. To meet all these requirements now and in the future, as well as overcome challenges such as the lack of IT security skilled resource, your SOC must transform. It must become automated, AI-enabled, cloud-native, and able to provide visibility, control, and response across the entire digital estate, while consistently enforcing governance. And it must support and augment skilled analysts so they can quickly address more complex issues and risks.

The approach to transformation must be methodical to reduce risk and capture requirements exactly; minimizing risk, speeding deployment, and delivering a SOC that protects and enables — so your organization can adapt and thrive. This requires considered and detailed assessments, careful road mapping, modernization and integration, and the right mix of expertise and technologies to support each organization's unique needs.

What is Managed Extended Detection and Response (MXDR)?

Atos MXDR is delivered through the combined strength of Atos security operations expertise and the Microsoft integrated security platform, and provides:

- **Reduce cost and complexity** with tool consolidation and reduced operational overhead
- **Free up internal resources** to focus on strategic initiatives while Atos handles 24x7 security operations
- **Meet sovereignty requirements** with analysts operating from sovereign facilities, ensuring data remains under full customer control
- **Continuous monitoring** across endpoints, cloud, and network environments
- **Advanced threat detection** powered by AI and global threat intelligence
- **Rapid, coordinated response** to contain and remediate incidents before they escalate
- **Endpoint policy management** ensuring security configurations remain compliant and optimized
- **Proactive threat hunting**
- **Bespoke playbook development** and automation to accelerate detection and response
- **Cyber Security Incident Response Team** (CSIRT) for major incident management

Together, Atos MXDR integrated with Microsoft helps you:

- **Increase resilience with proactive defense** powered by advanced threat detection with advanced AI-capabilities, Machine Learning (ML), and automation
- **Atos enables organizations to maximize their Microsoft investment through optimized,** consolidated solutions integrated with Microsoft, driving greater efficiency and improved return on investment (ROI)
- **Develop a tailored-fit solution from Industry specific offerings and our modular, tier-based approach.** This ensures you get solutions that work for your state of maturity, with protection based on your environments and regulation

Your licensing. Our operations.

With Atos MXDR, you bring the Microsoft licensing; we bring the operations, optimization, tuning, threat hunting and automation. Not to mention 20+ years of Microsoft experience and the highest levels of cybersecurity and expertise.

Delivering SOC transformation

SOCs need to evolve away from siloed tools and manual workflows to cloud-native, intelligence-driven platforms designed to operate as part of the wider business, not alongside it.

They must also support strong governance, data residency, and operational control.

Atos and Microsoft for SOC transformation

SOC transformation that goes beyond technology to empower your business

Atos and Microsoft align security solution expertise with deep understanding of regulations, business operations, and applications. We work with our customers to provide services such as policy management on the endpoints, playbook and automation development, and support from our Cyber Security Incident Response team (CSIRT).

Services such as Digital Forensics and Digital Experience Management add layers of insight and ensure targeted responses, so neither security nor user experience (UX) is compromised as new innovation is adopted and the organization responds to change.

Our range of services, combined with Atos's wider capabilities in Cloud, Infrastructure, and Digital Workplaces, ensures SCO transformation is aligned to business needs including sovereignty requirements and their unique attack surfaces and risk profiles.

We deliver:

01.
Unified visibility with Atos, integrated with Microsoft

Atos delivers integrated security visibility across endpoint and cloud signals within the Microsoft estate through solutions integrated with Microsoft Sentinel and Microsoft Defender XDR. This shared visibility is transformed into prioritized, actionable insight—reducing tool sprawl and eliminating blind spots.

02.
AI-assisted detection and investigation

Atos accelerates detection and investigation by leveraging security capabilities integrated with Microsoft that use behavioral analytics and AI. Atos analysts apply this intelligence to speed triage and response, enabling earlier, more confident decision-making and reduced operational risk.

03.
Human expertise where it matters most

Atos goes beyond alert handling. Analysts validate threats in business context, assess impact, and apply response playbooks aligned to each customer's environment and risk appetite. The result is precision and relevance, not alert noise.

04.
Proactive threat hunting and continuous improvement

Atos threat hunters proactively search for indicators of compromise and emerging threats. The service includes continuous tuning of detection rules, custom use case development, and ongoing playbook optimization to evolve with your environment.

05.
Sovereign SOC with security-cleared analysts

Atos operates a SOC with security-cleared personnel authorized to work on government and critical national infrastructure projects. Analysts manage endpoint policy configuration, ensuring security controls remain compliant and optimized. This ensures operations meet the highest standards for data sovereignty, regulatory compliance, and national security requirements.

06.
End-to-end SOC lifecycle management

Atos provides end-to-end security services across onboarding, tuning, monitoring, incident response, reporting, governance, and continuous improvement, using a cloud-native security foundation integrated with Microsoft technologies. This ensures the SOC evolves as organizational needs change.

07.
Continuous efficiency through AI and automation

Atos continuously applies efficiency improvements through AI and automation adoption. As the service matures, customers benefit from enhanced automation, refined detection logic, and optimized workflows — delivering increasing value over time without additional effort.

Did you know?

Atos offers a sovereign SOC with security cleared personnel that are cleared to work on government and critical national infrastructure (CNI) projects.

MXDR SOC transformation with Atos

SOC transformation shouldn't feel abstract or overly technical. It should be clear, tangible, and easy to understand – especially for business leaders who need confidence, not complexity. This section lays out exactly what customers get when they choose Atos integrated with Microsoft for managed extended detection and response (MXDR).

A clear, comprehensive, business-ready scope

24x7 monitoring and detection

Continuous monitoring is delivered across Microsoft Defender XDR and Microsoft Sentinel, covering endpoints, cloud workloads, and network infrastructure. Security analysts are based in sovereign facilities, ensuring compliance with national security and critical infrastructure requirements. Endpoint policy management is included to maintain compliant and optimized security configurations across the estate.

Incident response and containment

Rapid response to security incidents through automated playbooks and expert analyst validation. Atos CSIRT provides major incident management, coordinating response activities and ensuring business continuity during significant security events.

Threat hunting and intelligence

Proactive threat hunting is delivered using threat intelligence integrated with Microsoft alongside Atos cyber threat intelligence feeds. Security analysts search for indicators of advanced threats that may evade automated detection controls.

Playbook development and automation

Bespoke security playbook development and continuous automation optimization. Atos works with customers to develop custom automated response workflows that accelerate containment while maintaining governance and approval requirements.

Continuous tuning and optimization

Ongoing refinement of detection rules, reduction of false positives, and development of custom use cases aligned to each customer's environment. Monthly service briefings provide visibility into security posture, threats detected, and optimization recommendations.

What you don't get

Data movement outside your tenant, vendor lock-in to proprietary platforms, hidden costs for scaling, or offshore analyst teams. Atos MXDR keeps your data sovereign, your operations transparent, and your costs predictable.

As a Verified MXDR Partner and long-standing member of the Microsoft Intelligent Security Association, Atos combines global-scale intelligence with operational excellence to deliver enhanced detection, response, and resilience across environments integrated with Microsoft.

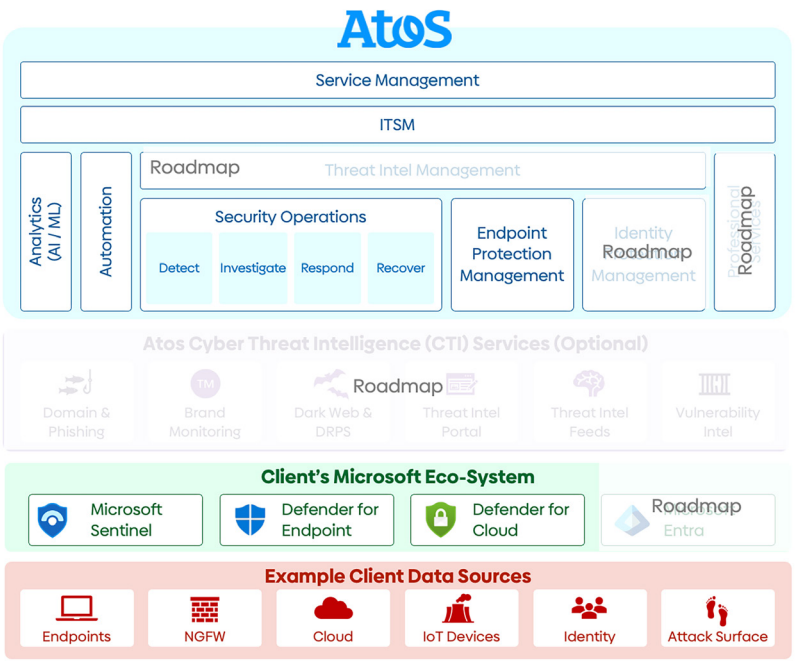
Category	What You Get
Monitoring	24/7 coverage with Sentinel
Detection	Defender XDR, AI models, behavioral analytics
Response	Verified incidents, containment, remediation
Intelligence	Integrated global intelligence and Atos industry insights
Compliance	Audit-ready dashboards & reporting
Governance	Monthly service reviews, continuous improvements

What are the Atos MXDR Sentinel Building Blocks?

Atos offers a holistic security solution built on four core security technologies integrated with Microsoft, including Microsoft Sentinel, Microsoft Defender for Endpoint, Microsoft Defender for Cloud (Defender for Servers), and Microsoft Entra.

Atos provides a comprehensive managed security service across all four technologies, whether you require a single technology or all four.

Clients can leverage an existing Microsoft agreement, which may already include some of these technologies, for example Defender for Endpoint as part of a Microsoft 365 E5 license.



From Detection to Decision: How Your MXDR service operates

A day in the life of your security operations, transformed by Atos and Microsoft.

01.
Security environments integrated with Microsoft are connected and prepared

Atos works with you to connect security environments integrated with Microsoft to support the service. Read-only access is enabled for security telemetry, with limited write permissions applied only for approved response actions. There is no access to business data, emails, or files. All actions are logged in the Microsoft Azure Activity Log to provide full transparency, and permissions can be revoked at any time.

Transformation services ensure the secure connection of security environments using Microsoft technologies to Atos SOC analysts through Microsoft Azure Lighthouse. Bespoke playbooks are defined to ensure governance and response align with regulatory and business requirements, including escalation where required. Security-relevant telemetry is enabled across agreed in-scope areas, which may include endpoints and cloud workloads.

Connections typically leverage:

- Microsoft Sentinel (SIEM)
- Microsoft Defender XDR (endpoint and cloud)
- Microsoft Azure logs, workloads, and telemetry

Your business context is documented, including:

- Critical systems and crown-jewel assets
- Escalation paths and operational constraints
- Industry and regulatory requirements

Fast time to value

Using cloud-native architecture and Atos onboarding accelerators, many customers can achieve operational readiness in weeks, depending on scope and existing maturity.

02.
Security signals flow into Microsoft Sentinel and are enriched with intelligence

Security signals from endpoints, identities, cloud resources, and networks are onboarded into Sentinel and enriched with:

- 65+ trillion daily threat signals from Microsoft
- Atos global SOC threat intelligence
- Behavioral analytics and AI models for anomaly detection
- Indicators of compromise (IOC) and indicators of attack (IOA)
- Atos industry-specific insights (FSI, public sector, healthcare, manufacturing)

This approach helps prioritize real threats over low-value noise.

03.
AI-assisted threat hunting and automated investigation accelerate analysis and triage

AI capabilities within the Microsoft security platform are used to support investigation and triage, helping to:

- Acquire global threat intel
- Correlate related alerts
- Summarize threats and incidents
- Map activity across endpoint, cloud, and network domains
- Recommend next investigative or response actions

These capabilities augment analysts, reducing manual effort and investigation time.

04.
Atos analysts validate threats and escalate only what matters

Atos security analysts apply human judgement to determine which incidents require action. Analysts:

- Validate alerts against known attacker behavior
- Analyze activity in business and operational context
- Eliminate false positives
- Assess impact and urgency
- Determine appropriate containment or escalation paths

Precision, not noise

Atos brings deep experience operating SOC services for regulated and sovereign environments, ensuring customers receive actionable, prioritized incidents rather than alert overload.

05.
Containment actions are executed through aligned and pre-agreed playbooks

Where appropriate, response actions may be executed through automated or analyst-driven playbooks, aligned to your risk appetite, policies, and regulatory requirements. Actions may include:

- Isolating affected endpoints in specific cases agreed in advance
- Quarantining suspicious files
- Blocking malicious IPs or domains

06.
Clear executive reporting and recommendations

Incidents and trends are translated into business-relevant insight, including:

- What happened and why it mattered
- Business impact and risk exposure
- Actions taken
- Recommendations to strengthen security posture

Reporting is designed to support executive decision-making, governance, and assurance.

07.
Operational SOC in weeks, not months, then continuous improvement

Thanks to native integrations with Microsoft technologies and Atos global onboarding accelerators, customers reach operational readiness quickly with:

- Active 24x7 monitoring by analysts
- Tuned detection rules customized to your environment
- Executive dashboards and reporting
- Agreed escalation paths and communication protocols
- CSIRT team on standby for major incident response
- Detection rule tuning and enhancement
- Playbook optimization
- Threat modeling updates
- Ongoing alignment with Microsoft platform updates and threat intelligence
- Regular reviews focused on resilience and maturity uplift

Your SOC becomes fully operational — fast, mature, and aligned to your business from day one.

Always Evolving

Atos' award-winning MDR Service (Intersec Cybersecurity Service/Product of the Year 2023) ensures your SOC never stands still. And as a Microsoft Verified MXDR Partner, Atos receives early insight into emerging threats and platform innovations from Microsoft.

Your role – what you retain and control

Clarity, confidence, and partnership. Built in from day one.

A MXDR SOC is not something that happens to you. It's something built with you.
Atos and Microsoft bring world-class technology and operational excellence, but your strategic insight, priorities, and governance shape how the service performs.

What you own. And why it matters

Atos MXDR is a managed service — but you remain firmly in control.

Here's what stays with you:

- **Strategic direction:** You define risk appetite, security policies, and business priorities. Atos operates within your governance framework.
- **Data ownership:** Your data remains in your Microsoft tenant. Atos accesses through delegated permissions via Azure Lighthouse — no data movement, full control retained.
- **Final decision authority:** You approve response playbooks, escalation paths, and major incident actions. Atos provides recommendations; you decide.
- **Licensing and infrastructure:** You own Microsoft licenses and cloud infrastructure. Atos optimizes and operates the security capabilities within your estate.
- **Business context:** You provide insight into critical systems, maintenance windows, and business operations. Atos aligns security operations accordingly.
- **Compliance accountability:** You remain accountable for regulatory compliance. Atos provides auditable, transparent operations that support your compliance requirements.

Why this matters:

You gain enterprise-grade security operations without surrendering control. Atos handles the operational burden — 24x7 monitoring, analysis, and response — while you maintain ownership, governance, and strategic direction.

Shared Responsibility Model (Atos, Microsoft, and You)

You	Atos	Microsoft
Strategy and governance	24/7 monitoring and response	Defender XDR/Sentinel
Business context	Triage, investigation, containment	AI models and global intel
Data ownership	Playbook execution	Cloud-native scalability
Risk appetite definition	Threat hunting, tuning	65+ trillion daily signals
Escalation approvals	Monthly service governance	Secure-by-design platform

How we integrate into your environment

Seamless onboarding. Zero disruption. Built around Microsoft environments.

Atos integrates directly into existing security stacks integrated with Microsoft, making onboarding fast, smooth, and controlled. Without interrupting your operations.

01.
Connect Microsoft security tools

Atos securely connects to your existing Microsoft services using native integrations:

- Microsoft Sentinel (SIEM)
- Microsoft Defender XDR (endpoint, cloud, SaaS)
- Microsoft Azure logs and workload telemetry

No rip and replace. No custom agents. No business disruption.

02.
Ingest and enrich your security signals

Signals from endpoints, cloud resources, and networks are onboarded into Sentinel and enriched with:

- 65+ trillion daily threat signals from Microsoft
- Atos global SOC insights
- Behavioral analytics and AI models

This delivers high-fidelity visibility from day one.

03.
Microsoft tooling integration for end-to-end protection

To strengthen your full security posture, Atos creates a unified, secure foundation across user, device, data, and workload.

04.
Automate response with tailored playbooks

Atos creates and configures automated and analyst driven bespoke playbooks for:

- Endpoint isolation
- Account containment
- Incident triage, investigation, and correlation
- Malware detection and remediation
- Cloud resource lockdown
- Email/phishing response

All aligned to your risk appetite, escalation rules, and regulatory requirements.

05.
Operational SOC in weeks, not months

Thanks to native integration with Microsoft technologies and Atos' global onboarding accelerators, customers reach operational readiness quickly, with:

- Active monitoring
- Tuned detection rules
- Executive dashboards
- Agreed escalation paths
- CIRT team on standby

The SOC becomes fully operational: fast, mature, and aligned to your business from day one.

Designed for Fast Time to Value

Atos and Microsoft SOCs onboard faster because everything is built on your existing tools, not bolted on.

This means quicker protection, predictable delivery, and earlier ROI.

Service tiers and options

Flexible, scalable SOC services to match your security maturity

Every organization is at a different stage in its security journey, and we meet you where you are. Atos offers clear, scalable service tiers, built on the same Microsoft native foundation — so you can adopt the right level of coverage and increase maturity over time.

Flexible service tiers

Atos Sovereign MXDR is delivered in flexible tiers aligned to Microsoft E3/E5 licensing and organizational maturity.

Essentials Tier

Organizations with Microsoft licensing establishing core MXDR capabilities or seeking to consolidate existing security tools.

What you get:

- 24x7 monitoring and response across Sentinel, Microsoft Defender for Endpoint, and Microsoft 365 Defender
- Automated incident triage and correlation for email, endpoint threats
- Core threat detection rules and playbooks aligned to common attack patterns
- Monthly service briefings with security metrics and threat trends
- Analysts operating from sovereign facilities

Business value: Immediate reduction in alert noise and faster incident response without hiring specialized security staff. Maximizes existing investment while establishing foundation for security maturity growth.

Enhanced Tier

Microsoft organizations requiring full-spectrum detection, advanced threat hunting, and comprehensive cloud security coverage.

What you get (includes Foundation capabilities plus):

- Microsoft Sentinel SIEM integration with unified threat visibility across hybrid and multi-cloud environments
- Proactive threat hunting and sector-specific risks
- Custom playbook development and advanced automation for complex incident response
- Cloud workload protection coverage across Azure, AWS, and Google Cloud via Microsoft Defender for Cloud
- Advanced use case development (e.g., insider threat, lateral movement, supply chain attacks)
- Quarterly business reviews assessing security maturity and optimization opportunities

Business value: Unlock the full potential of your investment — most organizations use less than 30% of available security capabilities. Atos activates underutilized features, delivering enterprise-grade SOC operations without additional licensing costs. Eligible for programs funded by Microsoft to accelerate adoption.

Tier flexibility and growth

Tiers are not locked. Organizations start where they are today and evolve as security maturity and requirements grow.

Start with Essential, establish baseline monitoring, then scale to Enhanced as cloud adoption and threat complexity increase.

Expand to Enhanced when ready to activate full capabilities and add proactive threat hunting.

Why this matters: You pay for the service tier that matches your current maturity and licensing, not for capabilities you cannot yet use. As your Microsoft estate grows, Atos grows with you — no renegotiation, no vendor lock-in, no service disruption.

One platform, many paths All tiers leverage the same unified Microsoft security stack.

You can scale coverage, automation, and response depth at any time — without reinvesting in tools or architecture.

Security that protects your business. And strengthens it.

A MXDR SOC must deliver more than threat detection.

It must reduce risk, support transformation, and demonstrate clear commercial value.

Atos MXDR, built on the Microsoft security platform, delivers measurable business outcomes while maintaining regulatory requirements.

Enterprise benefits

Organizations adopting Atos Sovereign MXDR achieve:

- **Stronger cyber resilience** with unified visibility and AI-driven detection across the Microsoft estate
- **Maximize Microsoft investment** by activating and optimizing Defender XDR and Sentinel capabilities already included in E3/E5 licensing
- **Reduce cost and complexity** through security tool consolidation and reduced operational overhead
- **Free up internal resources** to focus on strategic initiatives aligned to business objectives, while Atos handles 24x7 security operations
- **Meet sovereignty requirements** with analysts operating from sovereign facilities, ensuring data remains under full customer control
- **Accelerate threat response** with automated playbooks, continuous tuning, and expert analyst validation
- **Improve compliance posture** through auditable, transparent security operations aligned to regulatory frameworks
- **Scale with confidence** as the service adapts to new workloads, geographies, and evolving threat landscape
- **Leverage programs funded by Microsoft** to accelerate innovation, security maturity, and improve ROI on existing investments

Security that protects your business and strengthens innovation

Security should enable business agility, not constrain it. Atos Sovereign MXDR shifts security from a reactive cost center to a proactive business enabler.

Protection:

- **Reduce business risk:** Faster detection and response minimize exposure, reducing the likelihood of breaches, regulatory fines, and operational disruption.
- **Protect revenue streams:** Maintain business continuity during security events, preventing downtime that impacts customer service and revenue.
- **Safeguard reputation:** Demonstrate robust, auditable security operations to customers, partners, and regulators — building trust and confidence.
- **Meet regulatory obligations:** Compliance, sector-specific regulations, and sovereignty requirements through transparent, auditable operations.

Enablement:

- **Accelerate cloud adoption:** Security confidence enables faster migration to Microsoft Azure and Microsoft 365, knowing operations are monitored and protected.
- **Enable digital innovation:** Free internal teams to focus on strategic initiatives — new applications, services, and capabilities — while Atos handles security operations.
- **Support business growth:** Scale security operations seamlessly as you expand into new markets, regions, or services without hiring specialized security staff.
- **Improve decision-making:** Monthly security insights and threat briefings provide leadership with visibility into risk posture, informing strategic planning.
- **Leverage Microsoft investments:** Maximize ROI from existing Microsoft E3/E5 licenses by activating underutilized security capabilities with expert management.

Why this matters: Security becomes a competitive advantage. Organizations with strong security operations can move faster, innovate with confidence, and differentiate themselves in regulated markets where trust and compliance matter.

Why Atos MXDR integrated with Microsoft

- Avoid the cost and skills shortage associated with running a 24/7 SOC
- Leverage Microsoft's continuous innovation in AI, automation, and threat analytics
- Gain Atos's industry-specific operational maturity and governance experience
- Benefit from global threat intelligence
- Maintain full control of security strategy, data handling, and decision-making

Real results from real organizations, delivered by Atos and Microsoft integrations.

01. Strengthening resilience after a major cyber incident

Public sector managed SOC and CSIRT

After a significant cyber incident, a public sector organization needed to improve visibility, response speed, and operational resilience across its cloud environment. Atos established a managed SOC and CSIRT operating model integrated with Microsoft Sentinel, providing continuous monitoring, faster threat validation, and coordinated incident response. This enabled the organization to restore confidence, strengthen escalation processes, and support digital modernization while maintaining regulatory alignment and service continuity.

02. Reducing audit risk and improving threat response in banking

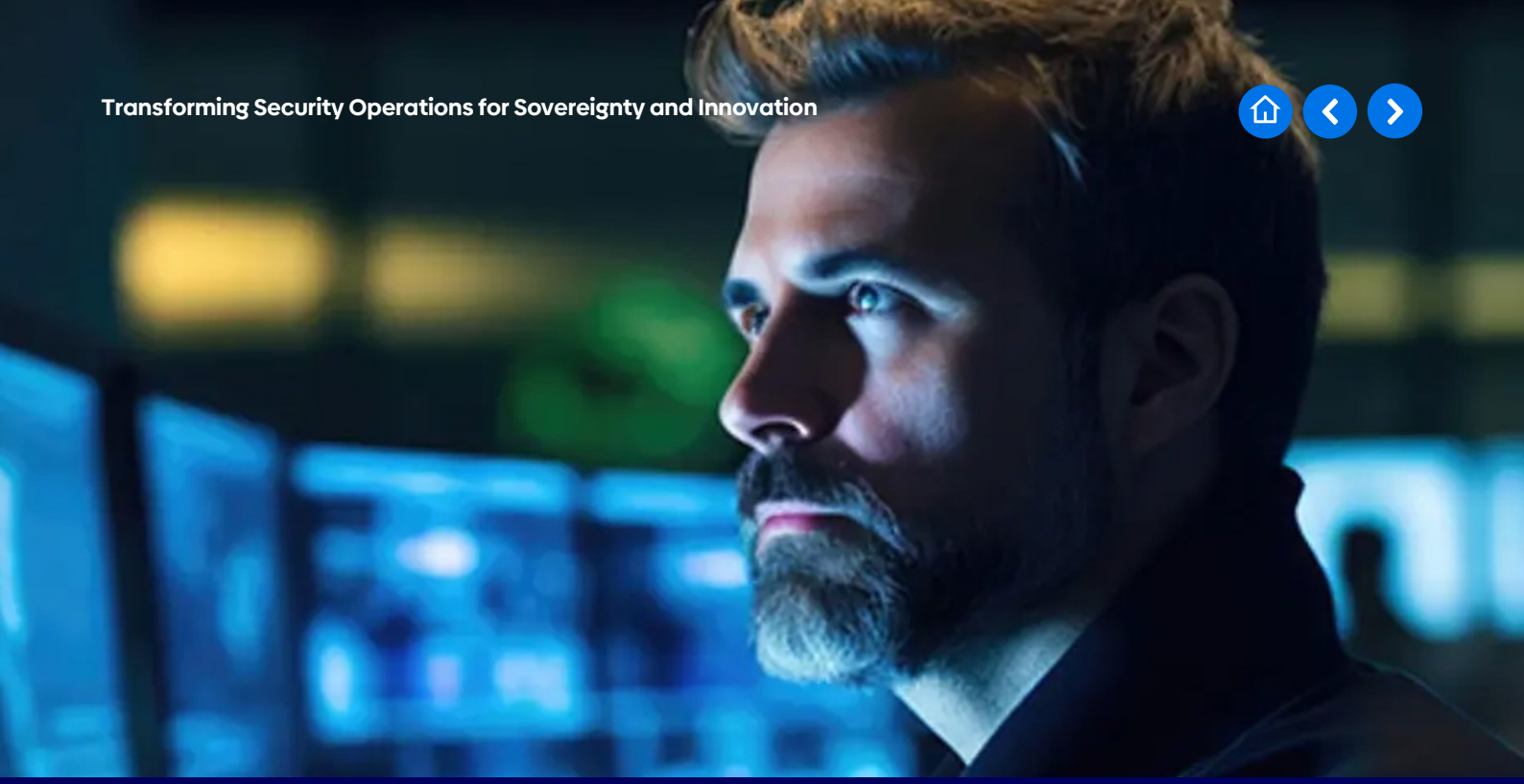
Managed SOC for a regulated financial environment

Following an audit-driven review, a banking organization sought to strengthen security monitoring and response across the Microsoft 365 environment. Through managed SOC services, Atos delivered continuous detection, analyst-led validation, and timely response to email and other threats. The result was a stronger security posture, reduced operational risk, and improved protection of sensitive information, without disrupting day-to-day banking operations.

03. Accelerating SOC readiness and validating security maturity

Proof of value for managed detection and response

A financial institution looking to modernize its security operations engaged Atos to assess and validate its threat detection capabilities. Through a structured SOC readiness and proof-of-value engagement, Atos helped the organization identify gaps, test detection and response workflows, and understand how managed SOC services could enhance its operating model. This gave security and business leaders clear insight into risk, maturity, and next steps, enabling a confident transition to ongoing managed detection and response.



Credentials

- More than 20 years of collaboration, supported by 30+ co-sell-ready solutions
- Microsoft Solutions Partner for Security and Azure Expert Managed Services Provider
- Advanced specializations in cloud security, threat protection, and identity and access management
- Verified Microsoft MXDR Partner and member of the Microsoft Intelligent Security Association (MISA)
- 17+ Security Operations Centers and 6,500+ cyber experts delivering global intelligence with sovereign capability
- Award-winning MXDR services recognized for excellence in detection, response, and SOC transformation
- Proven sovereign delivery across government, defense, public sector, and CNI
- Sovereign-grade hosting capabilities, including HSM (high spec manufacturing)
- Multiple industry awards, including Best Cybersecurity Project in Europe (2025) and Intersec Cybersecurity Service/Product of the Year (2023)
- Microsoft Solutions Partner for Security

Recognized. Trusted. Proven.

Atos is positioned as a Leader in the Gartner® Magic Quadrant™ for Managed Security Services, Worldwide, and a Leader in Outsourced Digital Workplace Services nine years running.

Clear answers to the questions every organization asks.

Security leaders often raise the same concerns with regards to SOC transformation and managed services. These FAQs tackle the big ones head-on — with reassurance grounded in the strength of the Atos and Microsoft partnership.

Q: Do I lose control if we move to MXDR?

No. You stay firmly in control. You retain ownership of governance, licensing, data, strategy, and final decision-making. Atos operates your SOC according to your rules, your approved playbooks, and your escalation paths. Your data remains in your tenant — only the operational burden shifts to Atos.

Q: How fast do you respond?

Response times are governed by clear SLAs covering detection, triage, containment, and escalation. With AI-assisted triage and Atos's 24/7 analyst coverage from sovereign facilities, response is dramatically faster than typical in-house teams.

Q: What if Microsoft security tools are already in use?

Then you're already halfway there. Atos takes your existing investment and transforms it into a fully managed, expertly tuned, context-aware SOC — without additional tooling or platform complexity.

Q: Can the service scale as we grow?

Absolutely. Cloud-native security technologies from Microsoft are built to scale horizontally. Atos ensures detection rules, analytics, governance, and automation scale alongside business growth, including new workloads, geographies, and regulatory needs. The service is delivered in flexible tiers that grow with your organization.

Q: How much automation is included?

Significant automation is built into the service through Microsoft Sentinel and Microsoft Defender XDR automated playbooks. Atos develops bespoke playbooks tailored to your environment, continuously optimizing automated investigation and response workflows to accelerate containment while maintaining governance controls.

Q: What does Atos do to proactively protect our organization?

Atos provides proactive threat hunting, searching for indicators of advanced threats that may evade automated detection. Threat hunters analyze emerging attack patterns, validate potential compromises, and provide actionable recommendations to strengthen your security posture before incidents occur.

Q: What does success look like after 90 days?

Most customers see stabilized alert volumes, automated playbooks driving faster response, refined use cases and custom detection rules, improved MTTD/MTTR, and clear, actionable executive reporting. By day 90, the service becomes your SOC — tuned to your business, your risks, and your priorities.

Q: What if we have specialized compliance or sovereignty requirements?

Atos is a global leader in regulated, sovereign, and high-assurance environments. The Sovereign MXDR service is delivered by analysts from sovereign facilities, with sovereign hosting capabilities and deep compliance expertise. This is one of the partnership's strongest differentiators.

Confidence Built In

The SOC is built on a cutting edge security platform from Microsoft and delivered by one of the world's most experienced cybersecurity organizations.

That means stronger protection, clearer governance, and zero compromise.

Turn security from a challenge into a competitive advantage.

You've seen what SOC transformation with MXDR can deliver — reduced risk, lower cost, stronger compliance, improved ROI, and a foundation for safe innovation.

Now it's time to take the next step.

Ready to transform your security operations?

01. Book a SOC Readiness Assessment

Understand your current security maturity, coverage gaps, and priority improvement areas.

02. Define an Onboarding and Integration Approach

Gain clarity on how Atos can integrate with security environments integrated with Microsoft, including indicative timelines, in-scope data sources, governance, and operating model.

03. Launch a Pilot or Proof of Value

Validate the impact of Atos and Microsoft in your own environment using agreed success measures and operational KPIs.

04. Explore ROI Modelling

Assess how tooling consolidation, automation and managed detection can reduce operational effort, improve resilience, and strengthen return on existing Microsoft investments.

Your Security. Accelerated.

With Atos solutions integrated with Microsoft, organizations modernize their security faster, reduce operational strain, improve compliance, and achieve enterprise-grade resilience — while retaining full control and ownership.

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.