Managed Detection and Response Services

Comprehensive, multi-vector defense for cyber threats

Atos

Use managed detection and response (MDR) to attain significant expertise to help drive detection and response, become proactive rather than reactive, and choose what the security team will focus on."

FORRESTER®

"Use MDR services to add remotely delivered modern 24/7 security operations center functions in a turnkey approach when there are no existing internal capabilities, or when the organization needs to accelerate or augment existing capabilities."

Gartner®

MDR to combat today's sophisticated cyber threats

Atos Managed Detection and Response (MDR) goes beyond the limited capabilities of traditional Managed Security Service Providers (MSSPs) and other MDR vendors that use disparate technologies. We combine the power of Artificial Intelligence (AI), big data analytics, high-density computing (BullSequana S) and EDGE computing on a single platform for a streamlined service. Clients receive deeper detection and full-spectrum response at speed and scale. The cloud-native service or "MDR in a box" is delivered through our 15 Security Operations Centers (SOCs) strategically placed across the globe, considering data sovereignty and can be deployed on public, hybrid & multi-cloud, or on-premises environments.

The Atos MDR service is built on three core components:

Multi-vector threat visibility

When it comes to cybersecurity, if you are blind on-premises, you are blind everywhere. This is why AIsaac®, the Atos Artificial Intelligence platform for cyber analytics and hybrid SecOps, brings superior threat visibility across threat vectors:

- As a native eXtended detection and response platform, AIsaac collects telemetry from your cloud, SaaS, endpoints, servers, security devices, and users. Giving you complete visibility of your environment on a single, integrated AI platform that can also leverage your existing investments in security technologies.
- We enhance the telemetry further with signals from the IT stack. AIsaac ingests logs, alerts, flows, vulnerabilities, configuration changes and more to uncover targeted, zero-day attacks in your environment.
- Atos brings purpose-built technology from leading partners for superior visibility on OT and IoT cyber threats. These signals are integrated into AIsaac to provide cohesive defense and central monitoring.

How this helped an MDR customer: In under three days of deploying MDR at a global chemical manufacturing company, AIsaac uncovered hidden, persistent threats that the existing SIEM, EPP, and other security tools could not identify.

Anticipate, monitor and hunt threats

The rich telemetry from AIsaac's event captures and your existing technology stacks are used in three different ways to uncover both known threats and covert, unknown attacks:

- AIsaac sifts through 200+ threat intel sources and contextualizes it to your network and IT services to predict attacks. Our SOCs then remediate related vulnerabilities and fortify your defenses to keep you protected.
- Attackers use known TTPs before inventing to evade your security controls. AIsaac uses 1000+ rules and signatures to identify known threats and attack patterns. The big data SIEM ensures lower false positives, so our analysts can intervene early.
- Unique AI models (75+) provide round-the-clock automated threat hunting, helping our hunters' efforts in uncovering cover attack behavior and advanced threats. Our threat hunters structure hunts around the cyber kill chain or the MITRE ATT&CK framework.

How this helped an MDR customer: Our machine learning models detected malware beaconing and lateral movement in a large financial institution within two days of deployment. The MDR team identified that the attackers used stealth malware to evade detection and were in the network for more than a year.

Auto containment and full-service response

Reducing threat detection time is pointless without a corresponding reduction in response time. Atos uses a combination of technology and security expertise to reduce the meantime to respond (MTTR). We achieve this by:

- Triaging the alerts to focus on the most relevant threats and accelerating decision making with AIsaac's threat visualization to identify attack chain, blast radius, and potential impact to assets.
- Containing threats at both the endpoint and network-level using AIsaac's continuously updated threat containment playbook. AIsaac can stop lateral movement, disrupt attacker command and control, terminate data exfiltration, and more.
- Investigate incidents using AIsaac and a host of other forensic tools to identify attacker TTPs and formulate a meticulous incident response to evict attackers and keep them out. The AIsaac SOAR module helps the IR team orchestrate response faster and provides unlimited support.

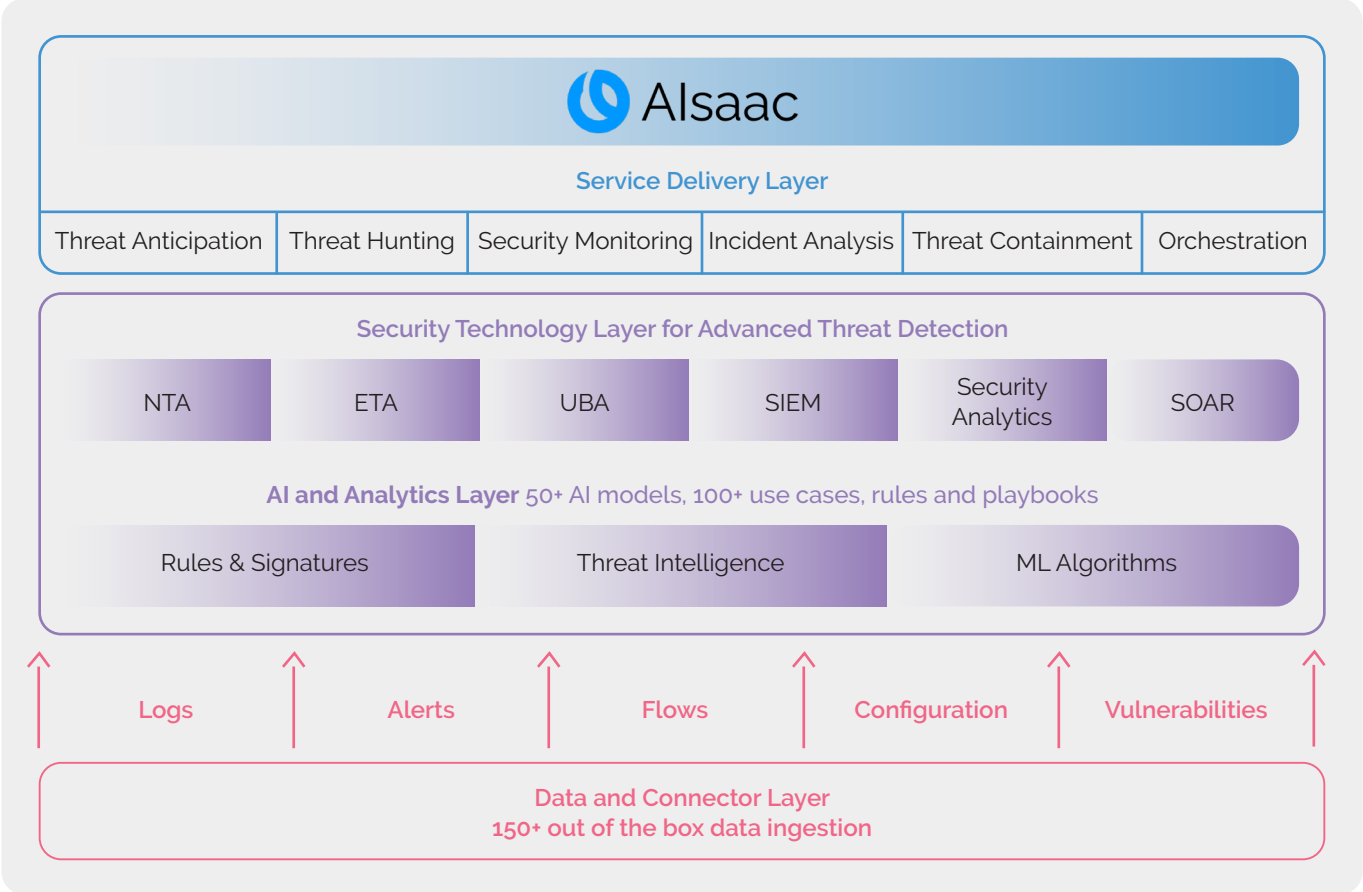
How this helped an MDR customer: Swift incident response requires validating substantial amounts of data related to the alert. Our MDR service brought machine-driven analysis to reduce the time to validate alerts by over 80%, revolutionizing response for the customer.

Merging security expertise and artificial intelligence

The AIsaac® platform

AIsaac, our proprietary AI platform, powers all our SOCs. AIsaac was developed from years of front-line security experience, allowing us to perform detection and orchestrate response in near-real-time at scale. Clients can choose between a cloud native or on-premises deployment of AIsaac MDR to address data sovereignty concerns. AIsaac enables our SOC in:

- Detecting complex attacks by leveraging advanced technologies, including Hortonworks Big Data platform, Atos OneCloud, edge, and next-gen ML algorithms.
- Creating centralized threat visibility through a single console that combines logs, alerts, flows, vulnerabilities, and configuration changes across all assets.
- Monitoring for 1,000+ rules and signatures and hunting with 50+ machine learning models and 500+ use cases.
- Anticipating attacks by correlating 200+ threat intelligence sources against your assets and proactively raising your defenses.
- Breaking silos by integrating SIEM, SOAR, CSPM, EDR, UBA, NTA and Security Analytics within a single cloud-delivered platform.



AIsaac – Functional Architecture

Flexible and adaptable MDR SOCs

Our SOCs do not deliver a cookie-cutter MDR service. They learn your environment, leverage global experience, deep industry expertise, and the AIsaac platform to offer bespoke, high-level cybersecurity — even as your needs change and your threat landscape continues to evolve. Our SOCs:

- Maintain situational awareness of your cyber from 15 global SOC locations that offer truly always-on, 24x7x365 threat detection and response.
- Break convention with specialized teams that take a collaborative approach, unlike other MDR providers using an L1, L2… system. Roles in our SOC include researchers, hunters, data scientists, analysts, SIEM specialists, forensic experts, incident responders, ethical hackers and more.
- Provide regulatory compliance for security monitoring and focus on threat detection and response use cases Integrate existing security investments in your environment by updating use cases and configuring them to our standards. AIsaac integrates with leading security technologies.
- Update and customize artificial intelligence models to your environment. Data scientists are part of the core Atos SOC team, so our AI models reflect the most current threat scenarios

What you get with Atos MDR service

Threat Intelligence: We protect you from emerging threats by maintaining a real-time threat intelligence library that consumes multiples feeds.

Security Monitoring: We provide deep detection by performing advanced security analytics on endpoints, user behavior, applications, and networks.

Threat Hunting: We proactively search for in-progress attacks that evaded initial detection using automated and manual threat hunting.

Auto-Containment: In real-time, we contain potential incidents to prevent the lateral spread and stop them from causing damage.

Incident Analysis: We thoroughly investigate and decode incidents to define all compromised assets and determine how to stop attacks at their root.

Incident Response: We remediate incidents to prevent harm, fully evict the attacker, and help you rapidly return to normal business operations.

The result: With our MDR services, you will gain a full-service, hands-free security posture that protects you from modern threats without expanding your internal team.

Atos MDR service features

- Support for hybrid, multi-cloud, on-premises, and SaaS
- 24x7x365 monitoring, detection, investigation, and response
- 15 SOCs combined with our AI-driven MDR platform
- Automated detection, blocking and containment of threats.
- Transparency on how we use Artificial Intelligence
- Out of the box AI and use cases for swift deployment
- Built-in SOAR capabilities for shorter investigation and response
- EDGE response for rapid incident remediation
- Incident response from trained CSIRT teams

Our Results

Atos MDR clients have seen the following results within weeks of deployment:

- 80% reduction in time to validate alerts
- 70% improvement in mean time to detect (MTTD)
- 75% reduction in false positives
- 80% improvement in mean time to respond (MTTR)

Bring Atos MDR services to your organization

Contact us to schedule a free demo today.
cybersecurity@atos.net

About Atos

Atos is a global leader in digital transformation with 105,000 employees and annual revenue of over € 11 billion.

European number one in cybersecurity, cloud and high performance computing, the Group provides tailored end-to-end solutions for all industries in 71 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos operates under the brands Atos and Atos|Syntel. Atos is a SE (Societas Europaea), listed on the Next 20 Paris Stock Index.

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

For more information: cybersecurity@atos.net

CT-210316-AR-BR-MDR