Leader in oil and gas reduces attacker dwell time from 60 days to minutes

Beset by next-generation attacks, and challenged by politically-motivated regional threats, a leading global oil and gas conglomerate selected Atos's AI-Driven Managed Detection and Response (MDR) service to protect its critical infrastructure.

Trusted partner for your **Digital Journey**

Atos

At a glance

Industry
Oil and gas

Location
Middle East, with global operations and service delivery

Challenge
Their complex, huge, and increasinglydigitized production and service networks features 2,500 log sources suffering more than 10,000 security incidents. Their limited experience with IT security lead to damaging breaches.

Solution
They contracted Atos to provide 24x7x365 AI-Driven MDR security services. These services include network, endpoint, user behavior, and application threat analytics, as well as threat intelligence and expert incidence response.

Results
By partnering with Atos, this oil and gas company now:

- Reduced their threat remediation time 86% - from 15 days to 2 hours.
- Reduced their attacker and malware dwell time 97% : from 60 days to Minutes
- No longer worries about their security, and focuses on their complex business. Provided 24x7x365 security services in a cost-effective manner.

Overview

This oil and gas conglomerate is one of the world's largest Liquefied Natural Gas (LNG) producers and exporters in the world. They recently acquired advanced instrumentation and SCADA application filled with critical applications and databases. They sought a proven security partner to protect their new, valuable network.

Challenge

As one of their country's top revenue generators, this company received a high volume of advanced cyberattacks by rival nation-states. Apart from facing external attacks (such as DDoS), this company increasingly faced internal threats (such as data exfiltration). However, despite these growing threats, the company lacked experience in IT security, and knew developing their own SOC would be too costly.

Then, the company received their wake-up call. They were breached by the Shamoon malware. This breach wiped hard disk data on over 4,000 machines, and resulted in lost revenue and reputation. The company realized they needed to better detect threats early, and proactively resolve detected attacks. To achieve this, they sought a partner who could provide 24x7x365 security monitoring and incident response services. They ultimately selected Atos's AI-Driven Security services, and have since been able to effectively prevent themselves from their many incoming threats (including attacks from Shamoon2).

"Partnering with Atos was the best decision we could have made to improve our security. They immediately gave us non-stop security analytics, threat intelligence, and rapid-fire response. With Atos on our side, we now find threats in minutes instead of months, and clear them out of our networks in a couple hours instead of a couple of weeks. Most importantly, we no longer have to think about our cybersecurity, and can get back to focusing on the complex business challenges that drive the most value for our organization."
CISO,
Oil & Gas Company

Solution

Atos gave the company's next-generation infrastructure true next-generation defenses via their AI-Driven MDR service. This service upgraded the company's existing security operations with active threat detection, alert investigation, and response orchestration delivered from Atos's "always-on" global security centers staffed by one of the world's largest teams of cybersecurity experts.

By partnering with Atos, this company received access to their proprietary AI-driven Big Data security analytics platform—**AIsaac**. By leveraging this platform, the company can now prioritize, investigate, and mitigate alerts & incidents in near-real-time. **AIsaac** now gives this company the ability to proactively hunt for threats, through a robust suite of analytics:

Threat Anticipation

Atos's Threat Intel Team and the **AIsaac** platform continuously monitors over 200 sources of global and regional threat data to detect emerging attacks. Atos then determines which threats are most likely to attack a specific company, and proactively upgrades its defenses.

Endpoint Threat Analytics

EDR agents now continuously monitor and proactively hunt for both known and unknown threats at this company's endpoints. Once they detect suspicious behavior, **AIsaac** takes immediate action to prevent lateral progression.

Network Threat Analytics

Atos's highly-trained Threat Hunters deploy proprietary data science models and machine learning algorithms to continuously monitor the company's complex network for anomalies, APTs, and blended, targeted, and zero-day attacks.

User Behavior Analytics

AIsaac created a baseline for how this company's users operate. The platform now flags suspicious behavior (access of inappropriate assets, running unnecessary commands, etc.) and Atos's Threat Hunters initiate appropriate countermeasures.

Application Threat Analytics

Atos identified the company's highest-risk applications-including low-footprint applications that give attackers an attractive target to exploit-and now continuously monitor them for anomalies.
Once the platform uncovers a threat, Atos's SANS-certified incident responders and experts work hand-in-hand with the company's distributed security personnel to contain, mitigate, and recover from major incidents at a highly accelerated rate.

Results

After partnering with Atos, the company gained next-generation security to protect their next-generation infrastructure. By deploying Atos's AI-Driven platform and skilled staff of globally located cybersecurity staff, the company is now able to protect their "crown jewels"
and critical infrastructure with 24x7x365 security monitoring and response.

By deploying Atos's AI-Driven MDR service, this company has been able to dramatically increase the speed of their detection and response to threats. Previously this company suffered an attacker or malware dwell time of 60 days. Atos reduced the company's attacker dwell time to Minutes - a 97% reduction. Before contracting Atos, the company required 15 days
to remediate threats. With Atos protecting them, the company now remediates threats within 24 hours-an 86% faster response to threats.

Working with Atos, this company no longer suffers the "wake up call" breaches they used to. They are able to detect and remove advanced threats from their critical infrastructure well before those threats create real harm. And once an attack has been detected and removed, Atos's AI-Driven platform can now produce detailed investigations and attack chain recreations to understand the context, motive, and path of the attack-to continuously evolve the company's defenses, and prevent similar attacks from ever succeeding again.

"As a global energy provider based in the Middle East, our production and service networks are massive- and under constant attack. We receive over 10,000 security incidents to investigate every day. And on our own, we just didn't have the IT resources, or technology know-how-to stop the breaches we kept suffering."

CISO,
Oil & Gas Company

About Atos

Atos is a global leader in digital transformation with 110,000 employees in 73 countries and annual revenue of € 12 billion.

European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos|Syntel, and Unify. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information technology 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/careers

Atos Global Head Office
River Ouest, 80 quai Voltaire
95877 Bezons cedex – France
+33 1 73 26 00 00

Let's start a discussion together

For more information: **cybersecurity@atos.net**

CT-210607-AR-MDR-CS-LEADER-IN-OIL-AND-GAS-EN-V2