E-commerce giant dramatically reduces mean time to detect and respond to threats

A giant e-commerce organization suffered advanced targeted attacks throughout their global network and selected Atos AI-Driven Managed Detection and Response service to accelerate their threat investigation and remediation 24x7x365.

Trusted partner for your **Digital Journey**

Atos

At a glance

Industry
E-Commerce

Location
North America based, Global operations

Challenge
The company was suffering advanced, targeted cyber-attacks, including nonsignature- based threats in their network, and complex attacks in their broader environment.

Solution
Atos deployed their full AI-driven Managed Detection and Response (MDR) program with 24x7x365 security monitoring throughout the company's entire network. The company's new security program included multi-vector big-data security analytics and comprehensive response services.

Results

By partnering with Atos, this E-Commerce company:

- Detected new attacks and complex malware at each stage of the attack chain.
- Accelerated and expanded their ability to identify attacker information, asset impact, and attack spread. Automated their network and endpoint response.
- Greatly accelerated their alert validation, incident analysis, and threat containment.
- Reduced incident analysis effort by 50%.

"We thought we were doing a good job investing in our security. Yet, the security technologies which we had deployed within our network were not performing well enough. Our internal security teams remained overwhelmed, serious threats were penetrating our network, and we weren't responding fast enough to prevent significant harm."

CISO, E-commerce

A North America-based E-Commerce organization with global operations chose Atos AI-driven MDR program to improve the ROI of their existing security approaches, and for comprehensive protection against next-generation threats.

Overview

This giant E-Commerce company ran operations across the globe. They had invested significantly in security solutions that were not performing, and their internal security teams were stretched too thin to investigate and respond to threats in a timely manner. They had begun to receive an increased volume of advanced, targeted threats, and required Atos assistance in both detecting and responding to these threats.

Challenge

This North America-based E-Commerce giant operated globally through a massive internal network. The company faced a number of challenges protecting their network.

First, they were unable to derive satisfactory ROI from their existing security technology. Second, their network regularly experienced a slew of next-generation threats - including advanced targeted threats and complex threats emerging from their general environment. Finally, the company detected that they already suffered non-signature ("unknown") threats within their network. The company had already invested substantially in security technologies but these siloed technologies were not effectively monitoring their entire network with the speed and accuracy necessary to stay ahead of attackers, and their total security posture lacked, Alerts required hours to validate, and both incident analysis and threat containment required days to perform. Overall, the company's internal security team were overwhelmed and unable to keep pace with the escalating volume of threats that they received (and which were breaching their existing defenses).

Solution

The global E-Commerce giant chose Atos AI-Driven Managed Detection and Response (MDR) service to perform 24x7x365 security monitoring, rapid incident investigation, and near real-time incident response. The service provided this company, for the first time, with multi-channel big data security analytics and a coordinated response platform - powered by **AIsaac.** The program utilized a unique combination of AI-driven machine learning models and human intelligence from Atos global team of cyber security experts to accelerate and increase the accuracy of the company's detection, incident analysis, and incident response.

This new program initially empowered the company with high-speed automated alert validation. The program utilized automated alert validation and machine learning to leverage, and derive significantly greater value from the alerts produced by the security technologies the customer had already invested in. These services allowed the company to quickly filter out "noise" in their threat data, significantly lower their volume of false positives, and only detect real attacks that would require additional attention and response from their internal security team.

To do so, Atos's **AIsaac** advanced machine learning algorithms worked on alerts, proxy, Netflow, and DNS data to detect new and unknown attacks and malware at every stage of the cyber kill chain. This incident analysis automation did more than filter out false positives. It also gave this company a much broader, deeper, and more accurate picture of the real attacks they suffered—allowing them to quickly determine information on the threat actor, the full spread of the attack, and the attack's impact on the company's assets. Once an attack was identified and investigated, Atos service deployed comprehensive, coordinated incident response and containment that accelerated network and endpoint response.

Results

This E-Commerce company created - CISO, E-commerce substantial improvement to their security posture. After deploying the Atos AI-driven MDR program, the company experienced an immediate acceleration of its critical security activities. They were suddenly able to validate alerts in seconds (instead of hours), perform incident analysis, and threat containment in minutes instead of days. At the same time, they improved their security performance and were able to reduce the resources required to protect their organization. They also reduced effort from internal security teams by 50% on key activities, and were able to discontinue their usage of a traditional SIEM for log collection, resulting in significant cost reduction in their overall security technology investment. These resource and effort reductions freed their manpower and budget to focus on more strategic initiatives.

Most important: by partnering with Atos, this company was able to solve their most pressing challenges that lead them to seek additional defense support. They enhanced their threat detection capabilities for the nextgeneration threats that had been plaguing them, including advanced malware, ATA, data exfiltration, and emerging environmental attacks - while also mitigating the existing unknown, non-signature-based threats they had discovered within their network.

"Atos did more than just fill the gaps in our existing security posture. They became a true partner in our defense, in a way that our previous security vendors (in particular the SIEM we contracted) did not. It's not surprising that we ended up deciding to use Atos to replace a number of our previous vendors, and to offer us truly comprehensive next-generation security all under one cost-effective program."

CISO, E-commerce

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 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-201126-AR-MDR-CS-GIANT-ECOMMERCE-ORGANIZATION-EN-V1