US-based manufacturing giant reduces attacker dwell time from 91 days to minutes

Faced with next-generation threats after upgrading their IT infrastructure, a Fortune 1000 manufacturing company, chose Atos to provide next-generation cyber defense - Managed Detection and Response.

Trusted partner for your **Digital Journey**

Atos

At a glance

Industry
High-Tech Manufacturing

Location
U.S.-based, with global operations

Challenge
Their adoption of the cloud and EDR increased their network complexity and threat landscape, making them susceptible to sophisticated cyber threats.

Solution
They contracted Atos to provide 24/7 managed detection and response to continuously monitor their vulnerability points, hunt for threats within their network, and respond to incidents swiftly.

Results

- Prevents new malicious attacks via threat anticipation
- Monitors, hunts, and responds to threats across all networks, users, and endpoints
- Reduced attacker dwell time or MTTD from 91 days to minutes
- Improved remediation time or MTTR from 12 days to 2 hours

Overview

This high-tech manufacturer with 40+ global locations recently migrated to the cloud for log management, while deploying multiple next generation technologies (including EDR). This increased their vulnerability to sophisticated attacks. They sought a proven next-generation managed security provider to handle their complex security needs, and protect them from advanced cyber-threats 24/7.

Challenge

After upgrading their technology infrastructure, the customer opened themselves to an increasingly complex threat landscape. Building their own team to continuously monitor for threats would have been time-consuming and cost-prohibitive. Instead, they sought a managed detection and response provider who could protect their assets on the cloud, and provide 24/7 protection from threats immediately; at a fraction of the cost of developing internal security capabilities.

Specifically, the customer required 24/7 monitoring and response on all security alerts, full security integration with their new cloud log management solution, and Threat Hunting on their endpoint AMP, Netflow, and proxy data.

Ultimately, they selected SUMO for their Cloud log management, Cisco AMP for their EDR system, and Atos as their Managed Detection and Response partner to oversee and orchestrate their full security posture.

Solution

First, we deployed a classic MDR architecture in this client's cloud. These included collectors in client locations, with 24/7 monitoring, and full integrations with Cisco AMP and SUMO logic. We further focused on this client's security posture around comprehensive Threat Hunting and incident response from our global SOC.

Our Threat Hunting services combined our diverse threat hunting team with our streamlined AI platform - **AIsaac** to uncover threats and attack campaigns this client's traditional security monitoring mechanisms would likely miss. This service included:

Endpoint Detection and Response

We deployed deep analytics to continuously monitor their endpoints for compromises. We leveraged our machine learning algorithms to triage their alerts, investigate threat spread, and stop attacks. Our hunting experts verified these outputs to remove false positives, and to detect any additional attacks that may have bypassed other security controls.

User Behavior Analytics

We monitored their user and contextual data to analyze user behavior anomalies, insider threats, and fraud. Our machine learning algorithms and statistical models identified their threat actors and anomalies, and mapped them to the cyber kill chain. Our threat hunters deployed proprietary tools to detect even the slightest "bread crumb" of insider threat activity, and immediately informed and collaborated with the client's team to initiate appropriate counter measures.

Network Threat Analytics

Our threat hunting experts sifted out suspicious activities in the client's network and applications, to stop creative attackers who were not deterred by intrusion prevention. Our multi-source analytics continuously uncovered new threats in our client's networks, which our machine learning systems triaged, investigated, and quickly responded to.

Application Threat Analytics

We identified our client's high-risk applications to mitigate attacks. Our MDR teams looked beyond our client's highvalue business systems and entry points, and also tracked low-footprint applications which attackers see as attractive targets to exploit.

Results

After partnering with Atos, this client has upgraded to a next-generation security posture. They have brought advanced (and rare) threat hunting skills, expertise, and insight into their defense. They leverage a leading-edge analytics program that processes multiple forms of analytics to produce actionable outcomes. They are now capable of uncovering difficult-to-detect (and increasingly subtle) internal threats. And they receive all of the above through a collaborative approach that tailors their new security posture to their custom threat profile, which gives their existing internal teams the guidance required to move from investigation to remediation.

This client now receives 24/7 monitoring and response coverage across their networks, users and endpoints (and across their data centers and cloud). We perform daily Threat Hunting on their network, user, and endpoint data, and they discover threats in devices without AMP via our information security telemetry module. In addition, they are now preventing breaches from new variants of malware with our threat anticipation service.

In short: this client no longer waits for threats to show their hand. They actively hunt their increasingly complex technology infrastructure to uncover threats in every stage of an attack.

"Recently, we went all-in with cloud and EDR adoption. On the one hand, as a high-tech manufacturer, this dramatically improved our business processes, efficiency, and capabilities. On the other hand, this digitization also dramatically increased the complexity and vulnerability of our networks— far more than we could continue to defend on our own."

CIO,
Oil and Gas Company

"We knew we needed a proven next-generation managed security firm, and after looking through the competition, it quickly became clear Atos was the only partner who could handle our network's complexity 24/7. From 'day one' they gave us 24/7 monitoring and response that integrated perfectly into our new Cloud solutions and next-generation infrastructure. By partnering with Atos we've cut our threat dwell time to next-to-nothing and remediate threats within a single day (before it took us a couple of weeks, on average)."

CIO,
Oil and 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-201126-AR-MDR-CS-US-BASED-MFG-GIANT-EN-V1