

# Modernizing Security Operations

How SOAR Helps Enable the Next-Generation SOC  
for One of the World's Largest MSSPs



COMPANY

Atos

LOCATION

Bezons, France  
Irving, Texas

DESCRIPTION

Multinational information technology service and consulting company

WEBSITE

atos.net

## Challenges

As a provider of managed security services – which is just one component of a digital services business spanning 73 countries and 120,000 employees – Atos has a large and diverse customer base.

Within its cybersecurity services division, that means having to cope with myriad security tools initiating countless alerts requiring at least some degree of investigation. Specifically, the MSSP arm of Atos is responsible for managing some 125 million security events per hour and securing 3.2 million endpoints across its 14 global security operations centers (SOCs).

But trying to address all those events, from initial detection through triage and resolution, can often include too many manual steps and the inability to deliver the necessary context to ensure the right decisions are made about each case.

In addition, such a process would run counter to Atos' stated mission of enabling business reinvention, providing a secure environment and ensuring operational excellence.



### MULTIPLE TOOLSETS

Integrating a disparate ecosystem of SOC tools across customer environments can be a blow to efficiency.



### MANUAL EFFORTS

Solely relying on SIEM technology in the SOC limited analysts in the scope of automation they could perform.



### KNOWLEDGE CAPTURE

So-called tribal knowledge can easily be lost within SOCs that fail to document repeatable and consistent processes shareable across the team.

**“Just by putting a tool doesn't give any value unless you actually have a 'prescriptive SOC' behind it that is addressing the output of those tools and knows how to deal with those in a correlated and orchestrated fashion ... and the Siemplify (Security Operations) Platform helps us get there.”**

– Eric Taylor, CTO of cyber security for North America, Atos



# Modernizing Security Operations

How SOAR Helps Enable the Next-Generation SOC for One of the World's Largest MSSPs

## Solutions

To help it cope with these hurdles and ensure its processes are mapped to the entire attack “kill chain,” Atos adopted the Siemplify Security Operations Platform, which combines security orchestration, automation, and response (SOAR) with end-to-end security operations management.

Now the service provider is able to ingest threat data and bring it all together into standardized, automated playbooks that execute response actions across customer environments, independent of the disparate tools they all may be running. These workflows drastically reduce the time spent gathering data, switching between consoles and applying threat intelligence to understand each individual alert.

The ‘case wall’ feature of the Siemplify SOAR platform has benefits that go far beyond an individual incident. The platform is designed to document and maintain which case decisions were made for customers, which controls were applied and what helped analysts make that determination. This not only provides full transparency for Atos’ customers, but it also serves as a single source of truth for the SOC, automatically capturing and documenting case activity for analysts in one centralized place.




**“This efficiency of savings (that SOAR provides) turns into better defensive mechanisms for customers.”**

-Eric Taylor, CTO of cyber security for North America, Atos



## Wins

Since the adoption of the Siemplify Security Operations Platform, Atos is able to extend the capabilities of SIEM to also effectively investigate and respond to threats while also supporting its “prescriptive SOC” model of dramatically improving detection and response times through automation that uses data to learn from past threats to interpret and prevent future attacks before they strike.

|   |   |  |
|---|---|--|
|    |    |    |
| <b>Faster Response</b>  | <b>Greater Context</b>  | <b>Demonstrated Value</b>  |
| Automation from SOAR enables Atos to reduce time-consuming tasks, offload lower-priority and repetitive tasks and improve the learning curve for analysts by connecting the dots quicker. | Analysts automatically have access to the full context and threat intelligence related to each alert for better and faster decision making. | Atos leverages integrated reporting in the platform to convey better visibility, as well as the ROI of SOAR, to its client base. |