Omnicom automates routine playbooks and reduces hour-long tasks to minutes with the combined power of the Devo Platform and Devo SOAR

CASE STUDY

The Omnicom team is able to reduce touchpoints by 75% to combat burnout and augment analysts.

SUMMARY

Omnicom Group is a media and advertising firm headquartered in New York, New York. The firm was founded in 1986 and has over 2000 agencies that operate in 56 countries serving over 5,000 clients. Omnicom was using AlienVault but found it could not keep up with the evolving threat landscape. By implementing The Devo Platform, Omnicom now has an end-to-end solution that combines behavior analytics, SOAR, and artificial intelligence to detect modern hackers before security incidents arise.

THE CHALLENGE

With such a wide range of clients, Omnicom faces the challenge of working across regions with different regulations and security requirements. The team was previously using a variety of tools for their SIEM, including AlienVault. They were unhappy with this legacy tech stack and needed a more modern approach to their SOC to reduce risk and better protect their clients. Omnicom needed a solution that would work for multiple teams globally, ingest data around the world, and improve visibility to reduce risk.

Omnicom Group

INDUSTRY

- Media and Advertising

ENVIRONMENT

- 2000 agencies across 56 countries
- 5,000 clients across 70 countries
- Multiple teams working within multiple systems

SECURITY CHALLENGES

- Lack of visibility across teams
- Manually scripting playbooks
- Evolving threat landscape

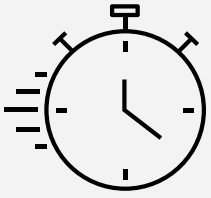
SOLUTION

- The Devo Platform and Devo SOAR

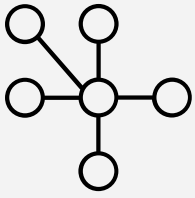
KEY BENEFITS

- Access to a true partnership
- Ability to ingest all named sources
- Single pane of glass
- Ability to automate playbooks
- Advanced threat intelligence

Omnicom leverages a risk-based approach within its security team. They use cyber intel to prioritize and effectively manage risk within their environment. As the threat landscape began to shift and the risk of security incidents



Hour-long tasks reduce to minutes



Reduced touchpoint by 75%

increased, Omnicom started looking for a next-generation SIEM that had capabilities beyond traditional logging. The team sought a single platform that could proactively identify and remediate events using leading-edge technology. Gladman Dibi, Managing Director of Cyber Security Architecture, Implementation, and Response at Omnicom, explained:

> *"The threat landscape is ever-changing. Threat actors are now using tools that normally would be approved or acceptable within our environments. We needed a tool that would allow us to detect those types of changes in the environment, and we began looking for a platform that could scale and provide the flexibility to meet our needs."*

Additionally, Omnicom was looking for a tool that had integrated SOAR capabilities. The team needed to automate routine playbooks and free up analyst time to focus on more sophisticated threats.

THE SOLUTION

After an extensive search, Omnicom selected Devo as their SIEM and SOAR solution. The team was drawn to The Devo Platform for many reasons. Devo enables Omnicom to ingest all necessary data, provide threat intelligence, and leverage AI across an integrated SIEM and SOAR solution. Additionally, Omnicom liked that Devo integrates well with the MITRE framework, via the MITRE ATT&CK Adviser, thus enabling them to continuously audit and improve their security posture. With these unique features of the Devo Platform, Omnicom can centralize its data and work as one team to defend its organization, despite its global presence. On the topic, Gladman shared:

"The greatest value of Devo is that it allows us to combine data from multiple countries around the world. From there, we can make decisions globally about the risk that impacts our company in a way that we were unable to in the past. Our SOC is much more efficient with Devo."

One of their most prominent goals was to implement an integrated SOAR solution that would save the team time and allow them to focus on the most complex threats. Gladman noted that with Devo, they instantly realized time savings. He further explained:

"Most notably what would take us hours to resolve an efficient case we can now do in literally minutes. Devo has given us the ability to work with our users more efficiently and resolve incidents faster. What used to take 20 touchpoints to resolve a case, we can now execute in 5-6 steps with Devo."

With the combined power of the Devo Platform and Devo SOAR, Omnicom can maximize its platform integrations and automate playbooks faster than the team had hoped. Devo SOAR was the only solution that allowed Omnicom to maximize its investment. One of their primary use cases with Devo SOAR is built around phishing attempts.

"With Devo, when we receive a phishing attempt, we can automate the remediation and the password reset, and we can talk to the user directly without having to wait. With Devo SOAR we're now able to ensure that we have consistency in our response." - Gladman Dibi, Managing Director of Cyber Security Architecture, Implementation, and Response at Omnicom.

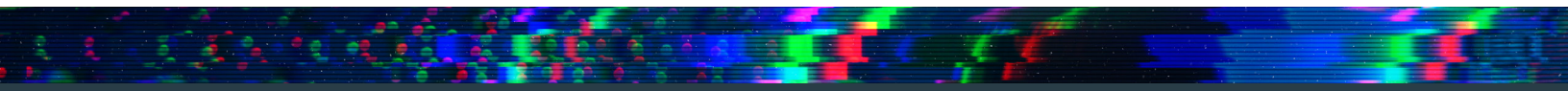
Devo SIEM and SOAR have allowed the Omnicom team to address their challenges head-on to secure their organization and combat the evolving threat landscape. After implementing Devo, the Omnicom team has been able to find the partnership they were initially seeking in a new solution. Gladman reported:

"I have found that the Devo team is very approachable and they're very inquisitive and apt to learn about not only our business but also how they can help us move faster in the security space. Devo has proven to be a true partner to our organization."

THE RESULT

The Omnicom team has realized an instant ROI. Through Devo SOAR, they have been able to automate routine tasks and reduce analyst touchpoints by 75%, thus saving time and increasing consistency. With this time savings, the team now proactively responds to threats to provide the most secure experience for their clientele. With the combined power of The Devo Platform and Devo SOAR, the Omnicom team consolidated their workload to save time and gain access to a true partnership.

> *"What I love about Devo are the people and how hard they work with our people to make sure that we have the best solution and the best product for Omnicom"*
>
> ***- Gladman Dibi, Managing Director Cyber Security Architecture, Implementation, and Response at Omnicom***



Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native security analytics platform that combines the power of people and intelligent automation to confidently defend expanding attack surfaces. An ally in keeping your organization secure, Devo augments security teams with AI — enabling you to continuously scale SOC efficiency, increase the speed of threat detection and response, and gain greater clarity to empower bold action, minimize risk, and maximize outcomes. Learn more at **www.devo.com**.