Global Marketing Communications Company Reduces Hour-Long Tasks to Minutes with Combined Power of the Devo Platform and Devo SOAR

DEVO

CASE STUDY

The global marketing communications company is able to reduce touchpoints by 75% to combat burnout and augment analysts.

SUMMARY

This media and advertising firm, headquartered in New York, New York, was founded in 1986. Today, it has over 2000 agencies that operate in 56 countries serving over 5,000 clients. The team was leveraging a legacy SIEM but found it could not keep up with the evolving threat landscape. By implementing The Devo Platform, the team 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, this firm 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. They were unhappy with this legacy tech stack and needed a more modern approach to their SOC to stay on top of evolving threats. The SOC needed a solution that would work for multiple teams globally, ingest data around the world, and improve visibility to reduce risk.

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

The client 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, the team 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. The Managing Director of Cyber Security Architecture, Implementation, and Response, 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, the team was looking for a tool that had integrated SOAR capabilities. They needed to automate routine playbooks and free up analyst time to focus on more sophisticated threats.

THE SOLUTION

After an extensive search, this leading media firm selected Devo as their SIEM and SOAR solution. The team was drawn to The Devo Platform for many reasons. Devo enables the team to ingest all necessary data, provide threat intelligence, and leverage AI across an integrated SIEM and SOAR solution. Additionally, they 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, the company can centralize its data and work as one team to defend its organization, despite its global presence. On the topic, the Director of Cyber 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. He 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, the customer can maximize its platform integrations and automate playbooks faster than the team had hoped. Devo SOAR was the only solution that allowed them to maximize their 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.” - Managing Director of Cyber
Security Architecture, Implementation, and Response

Devo SIEM and SOAR have allowed the team to address their challenges head-on to secure their organization and combat the evolving threat landscape. After implementing Devo, the team has found the partnership they were initially seeking in a new solution. The manager 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 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 team consolidated their workload to save time.

> *“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 us.”*
>
> ***- Managing Director Cyber Security Architecture, Implementation, and Response***

Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass. Learn more at **www.devo.com**.