Centrilogic

Enhancing ISP security in a strict regulatory environment.

By providing a tailored, cost-effective solution, Centrilogic supported a dynamic internet service provider in implementing a new Security Operations Center.

PARTNER SUPPORT

In business for almost 30 years, Imagine is a Dublin-based high-speed broadband internet service provider (ISP) serving more than a million homes and businesses. Recently, Imagine was tasked by its parent company and by Irish and EU regulators to implement a Security Operations Center (SOC) and adopt stringent new protocols for information security in its service infrastructure.

"We were on the path towards compliance with national and EU regulatory requirements to have an SOC in place. We were looking for sourcing options, and when we saw Centrilogic's proposal of SOC as a service, we knew that Centrilogic was the ideal partner, and we wasted no time in implementing the solution."

Mike Stacey, CTIO, Imagine Communications Group

Imagine already ensures strict compliance with privacy regulations under the European Union's General Data Protection Regulation (GDPR), focusing on resiliency and continuity in the design of its network. The company does not tolerate downtime. An SOC requires 24/7 monitoring and support, and the regulatory landscape in Europe can change quickly and often. Imagine recognized that its IT department required partner support on meeting milestones in their aggressive implementation timeline.
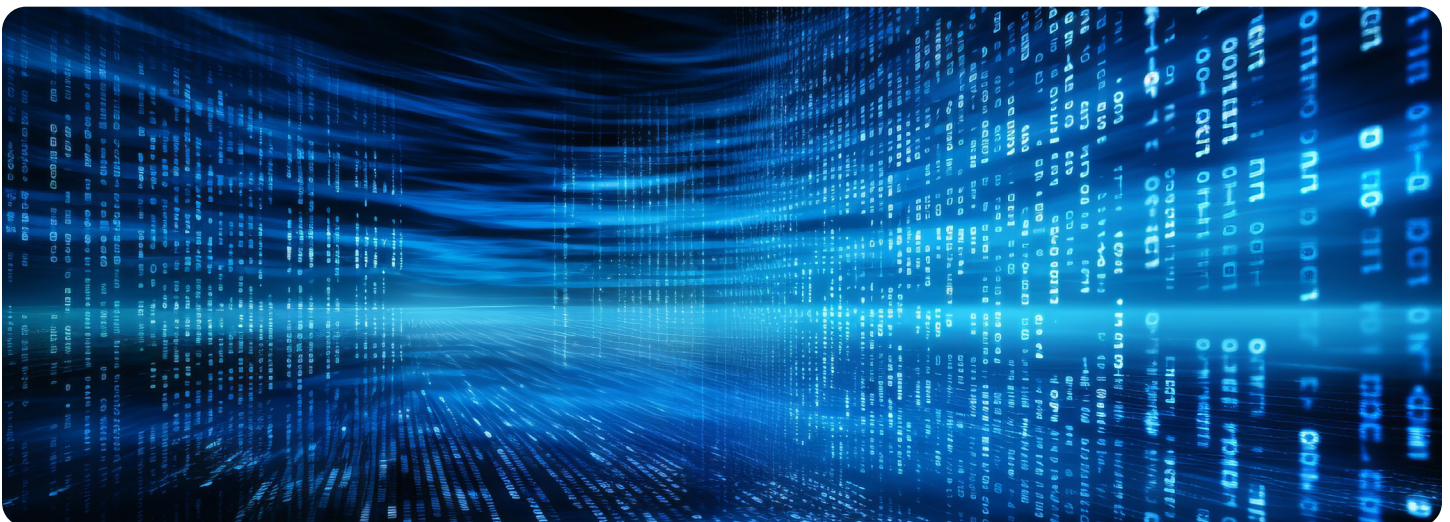
THE PROCESS

Following careful consultation to gain an understanding of Imagine's business realities and needs, Centrilogic developed a custom solution and supplied two appliances to be integrated into Imagine's network. One is in Imagine's office environment. The other is within a secure data center in its production environment. These appliances provide vulnerability scanning and SIEM (Security Information and Event Management), where log files from various network elements are analyzed to detect signs of vulnerability or attack.

Through these appliances and the active Managed Detection Response (MDR), Imagine's systems are protected against potential issues such as out-of-date software, open ports, or unauthorized access from cybercriminals and other nefarious actors. The system generates reports that are delivered to the Centrilogic Portal, which acts as an interface between the SOC and Imagine's IT department to alert it of any suspicious activity. The IT department then escalates the reports to the appropriate level so that corrective action can be taken immediately.

"We set up the solution so that issues are actioned quickly, according to Imagine's risk appetite, instead of sending multiple reports about low-risk activity. It's about not exposing the client team to a lot of unnecessary pressure."

Serge Maric, Director of Customer Success, Centrilogic

A WORKING RELATIONSHIP THAT WORKS

A component of Centrilogic's offering is vulnerability scanning and detection through monitoring of Imagine's network traffic. On a quarterly basis, Centrilogic finetunes the parameters of the SOC according to traffic patterns, internal requirements from Imagine, and any external regulatory requirements that may arise or evolve over time.

In addition, bi-weekly meetings between Imagine's IT department and Centrilogic's Client Success team ensure that there is a rapid and focused response to any threat intelligence arising from patterns observed across Imagine's network.

"Part of what made this arrangement so attractive to Imagine is the OpEx model where we pay for the solution on a monthly basis, rather than all upfront. And the whole process is invisible to our customers. All they see is reliable internet service from a provider with a more secure network."

Mike Stacey, CTIO, Imagine Communications Group

The Outcomes

In partnership with Centrilogic, Imagine has gone from having no SOC in place to having total visibility and coverage of all servers and devices (routers, computers, etc.) on its network. Now, thousands of end points are covered, monitored, and protected by the Centrilogic SOC-as-a-service solution. Beyond achieving regulatory compliance, Imagine has realized significant collateral benefits from implementing Centrilogic's solution, including:

- Minimized or eliminated potential outages and downtime for clients
- Significantly reduced possibility of cyberattack on Imagine's systems
- Added security measures with no disruption of service

CONTINUING SUPPORT

Imagine's experience of working with Centrilogic has been a positive, productive collaboration from start to finish. Centrilogic was able to implement the tailored solution with minimal disruption of Imagine's day-to-day operations, leaving the company free to focus on its mandate of delivering excellent service to its customers. The Imagine team is 100% confident that Centrilogic has delivered the best possible solution with modern technology and critical elements of the cybersecurity framework. As part of continued effort to increase the level of protection even further, Centrilogic will support Imagine with NIST audit requirements, advanced threat detection and security analytics; seamlessly connecting platforms, intelligence, and experts to address vulnerabilities and compliance risks.

The Imagine engagement illustrates Centrilogic's ability to understand and address a customer's need, help them respond to internal and regulatory pressures, and implement robust security measures through an SOC as a service. And all of this is done in a seamless changeover, invisible to Imagine's customers.

> "For Imagine, this is a model we're used to. Our size meant we had to outsource the solution. With Centrilogic, it's predictable, consistent, and responsive."

Mike Stacey, CTIO, Imagine Communications Group

ARE YOU READY TO REALIZE YOUR DIGITAL POTENTIAL?

Start with Centrilogic today.
centrilogic.com/contact-us

Imagine is a Centrilogic customer by way of the company's acquisition of WatServ in December, 2022. WatServ is now Centrilogc.