

Company at a Glance

This organization is an Ireland-based company with 13 offices across Europe, the Americas, and Asia Pacific focused on accelerating business transformations for its broad base of global customers. For almost three decades, the company has specialized in international management consulting, software asset management, software development, cloud computing, and outsourcing, helping organizations across sectors and size exceed their business and technology goals.

Challenges

- Lacked 24x7 monitoring and staff to detect threats after hours
- Needed guidance and expertise to supplement internal team and reach security goals
- Struggled to continually train employees on social engineering threats

Results

- 24x7 monitoring, detection, and response managed by Arctic Wolf® Managed Detection and Response
- Regular meetings with the Arctic Wolf Security Teams to continually advance the company's security journey and strengthen its security posture
- Fully managed, continuous phishing and social engineering training delivered by Arctic Wolf Managed Security Awareness®

Technology and Expertise Combine to Keep Leading Software Management and Consulting Organization Secure

“The core of what Arctic Wolf brings to us is the confidence that our stuff is safe.”

– IT Infrastructure Manager

Continually improving their security posture is a top priority for the Ireland-based technology provider, a global leader in business transformation that works with organizations large and small across multiple continents. Their customers — and the security of the often valuable, private data kept within those customers' environments — is a critical goal for the trusted technology solutions and services provider. That's why the company not only recommends the best cybersecurity to those they work with but also ensures that they adhere to the same standards.

“You have to be very careful as some of the data we work with is extremely sensitive so the potential for a major incident can be quite high,” said the IT manager. “You have to put your best foot forward.”

After taking a formal National Information and Security (NIS) assessment three years ago, the IT department took their own advice and started to evaluate how they could fill a major security gap — a lack of 24x7 monitoring. After realizing that building an in-house security operations center (SOC) was too costly and limited in terms of needed personnel and resources, The company began conversations with Arctic Wolf, who offer not only 24x7 monitoring, detection, and response technology but also, a full suite of solutions designed to provide end-to-end cybersecurity coverage, all backed by human expertise and support.

“From the conversations with Arctic Wolf, what sold us was that sense of, ‘We want to understand your business, and we want to work with you,’” the IT manager said. “The Concierge Experience and that constant point of contact aligned with our values and way of working. That was the kicker for us.”



Around-The-Clock Support Creates Confidence

This company works across time zones with a disparate workforce responsible for building, deploying, and maintaining customers' data-rich environments, so having eyes-on-glass at all hours is essential to incident prevention.

Powered by the Aurora™ Platform, Arctic Wolf® Managed Detection and Response provides 24x7 monitoring, detection, and response across endpoint, network, identity, and cloud sources, offering broad visibility, seamless integrations, and rapid response to all manners of threats.

Crucially, Arctic Wolf's technology, backed by the Arctic Wolf Security Teams, is able to filter out the alerts that don't matter and swiftly act on the ones that do, whether it's 3 p.m. or 3 a.m.

For the IT team, that continuous support inspires confidence in the state of their security and allows the company's IT team to focus on proactive projects, knowing threats will be detected and stopped in their tracks.

"Where Arctic Wolf really comes in is those out-of-hours issues," the IT manager said. "We've had one or two incidents, such as a virus detected on a device at 11 p.m. on a Friday, and we were able to give quick permission to Arctic Wolf to isolate the device, so we can deal with it the morning. Being able to detect those is exactly what we bought the service for."

That accurate and decisive detection and response is possible because of Arctic Wolf's broad visibility and integrations into the organization's environment. The company utilizes Amazon Web Services (AWS) as well as Microsoft solutions in its digital operations. Data from these sources, as well as other sources across the company's environment is ingested, enriched, and analyzed by Arctic Wolf and made available to their internal teams, creating valuable, comprehensive telemetry. "Whatever we see, Arctic Wolf sees, and that's particularly important to us," the IT manager said. "If something happens during working hours, within two minutes of us seeing it, Arctic Wolf will reach out with a message. When it's out-of-hours that response is particularly important."

Detection and Response Backed by White-Glove Service

While the company was looking for a 24x7 monitoring service and third-party security operations center (SOC) originally, what was found with Arctic Wolf was a comprehensive operations-focused solution where every piece of technology is backed by human guidance and expertise.

The Arctic Wolf Concierge Experience fills the internal security skills gap and works to create real security outcomes by providing tailored guidance to enhance the organization's security programs alongside on-demand expertise to respond to and mitigate threats in the environment.

"The Concierge Experience was really appealing," the IT manager said. "Having someone that would be able to work with us and know our business and understand the particular challenges we had instead of a faceless service."

Part of that model is regularly scheduled meetings with the IT team to go over recent alerts, the current threat landscape, and, critically, plans to continually improve the security posture. For example, recently the IT team was conducting an audit of Microsoft Active Directory, which can be a high-risk application due to its credential storage. The Arctic Wolf Concierge Security Team was able to help them define specific goals and offer security hardening solutions.

"The Arctic Wolf team said, 'Yes, let's run some reports for you and go through what our findings are and give you some areas to target and work on,'" the IT manager said. "That was extremely helpful. It's those type of things where we were able to combine our internal improvement calendar with those add-on services that make Arctic Wolf more than a SOC."

In addition to helping secure the tech stack in their environment, Arctic Wolf also helps the organization reduce their human risk as their headcount grows.



Creating a Culture of Security Through Continuous Trainings

This company already operated internal security awareness training, which involves regular phishing simulations. But with a lean IT department and an evolving threat landscape, the team knew that supplementing it to better reduce human risk was paramount to their security goals.

Arctic Wolf Managed Security Awareness® offers fully managed security training with frequent microlearning lessons that are as engaging as they are informative. The training is launched by Arctic Wolf, not the IT team, and teaches users about common threats that match the risks their employees may face.

“Having something that was prepackaged for us and could be deployed at a single click was really impressive,” they said. “The number one feedback I get now is the how the Arctic Wolf training is great.”

That feedback is also reflected in the company’s phishing simulation testing. The volume of overall phishing simulations reported to IT has increased from 40% to 70% and the number of employees who fell for phishing and did not report it to IT dropped from 5% to 0.01%.

“The training results have been a real win for us. It’s really paying off,” said the IT manager.

Arctic Wolf Allows This Organization to Exceed Security Goals

The partnership with Arctic Wolf began three years ago with an assessment score. Three years later the company took the same assessment again, only to find the organization had achieved an internal “stretch goal” score, concretely improving their security posture.

The IT manager said that goal was only possible because of the continued support of Arctic Wolf, who help his team set short-term and medium-term goals, and create a culture where they are consistently working to improve.

“You always overestimate what you can do in one year and underestimate what you can do in three years, so hitting those short-term goals and the continuous planning is how we managed to achieve that stretch goal over three years,” they said.

He stated that the partnership has only been positive, and he hopes the next three years will be just as successful.

“It’s going really well,” they said. “No complaints.”

