Red Canary MDR operationalizes Microsoft Defender, 24x7

Ansys relies on Red Canary MDR to detect and respond to threats across its Microsoft environment.

BUSINESS SNAPSHOT

Ansys is a leader in engineering simulation that helps the world's most innovative companies deliver radically better products to their customers. If you've ever seen a rocket launch, flown on an airplane, driven a car, used a computer, or put on wearable technology, chances are you've used a product where Ansys software played a critical role in its creation.

THE MISSION

Add 24x7 security coverage that delivers value from the Microsoft Defender suite

Ansys has an experienced, high-performing security team. They sought to maintain eyes-on-glass security coverage after business hours that met their high standards.

They also wanted to supercharge the value they received from Microsoft's security tools. Ansys is a Microsoft E5 license holder that uses Microsoft Defender for Endpoint, Microsoft Defender for Cloud Apps, Office 365, and other Microsoft tools that come with their E5 license. They wanted to derive even more security value from those investments.

THE CHALLENGE

Scaling Ansys' quality of defense to 24x7 coverage posed a few problems to Dave Coughanour, their VP of Cybersecurity. First, the cost of adding enough team members to deliver 24x7 coverage was prohibitively expensive. And second, even if Ansys did decide to staff its SOC 24x7, a markedly bigger team would just amplify the existing challenges he faced of finding and retaining staff with the necessary expertise.

Ansys needed a partner it could trust to deliver quality detection and response across the breadth of its Microsoft tools and environment.

THE SOLUTION

Red Canary impressed Ansys with its deep and comprehensive integration with the Microsoft Defender suite. Red Canary's platform processes telemetry and alerts from Ansys' Microsoft security tools, and its detection engineers investigate that data thoroughly. Red Canary's ability to distill signal from noise across the Microsoft Defender tools helps streamline Ansys' existing security operations program by reducing alert fatigue and allowing the team to focus on what really matters.

> "One of the ways that Red Canary helps is that it cuts down on alert fatigue. Red Canary acts as a filter for us: they bubble up the most pressing things to the top, and it's very easy to collaborate with them within their portal. We get the most pressing alerts passed to our response team, and they get actioned first."

Red Canary's focus on fast response stood out to Ansys. Dave knew that when attacks occur it is imperative to respond quickly and precisely. The extensive experience of Red Canary's Incident Handling team, combined with the Red Canary platform's automated response capabilities, gave Ansys confidence.

> "With such a small window of response time, you need to have not just good detection but automated responses that you build very easily with Red Canary's playbooks."

And lastly, Dave appreciated Red Canary's ability to translate learnings from one customer's environment into protection for all of its customers. When Red Canary encounters a new threat, it rapidly builds detectors and applies them across all customer environments. Combine that with Microsoft's visibility across its hundreds of thousands of customers, and Ansys knew it would benefit from Red Canary and Microsoft's joint partnership.

> "We have the advantage of a global community with Red Canary and Microsoft. Our partnership gives us maximum visibility into cyber threat trends and remediations."

Red Canary met Ansys' criteria for a 24x7 security partner that could deliver value from their Microsoft security tools.

But at the end of the day, the decision to partner with Red Canary came down to trust. Dave knew that his team would be working very closely with whichever MDR partner they chose, so just strong resumes and quality technology wouldn't cut it. His team's partner needed to be collegial, respectful, and perform at the highest level in the most stressful situations. Red Canary met the mark.

> "
>
> Cybersecurity is all about trust. You need to trust the people that are handling your most sensitive data; you need to trust their work ethic, their professionalism, and their ability to execute, typically in a time of crisis. We've worked with many of the members of the Red Canary team for years now, and we know that when it's "go time", they're not going to panic. They're going to execute in a very disciplined manner. That's what you need on a response team."

Supercharge Microsoft Defender with Red Canary

Learn how Red Canary leverages your Microsoft tools for 24/7 security coverage

→ **MDR FOR MICROSOFT**