

# Pondurance as an Extension of a Large Retail Supercenter SOC



## CASE STUDY

### THE CHALLENGE

Decision-makers at a large regional supercenter were considering the expansion of their security operations center (SOC) to provide cybersecurity support for a fresh grocery affiliate. They began a cost benefit analysis for expanding their own internal operations versus outsourcing additional cybersecurity support, explored a variety of options from several cybersecurity providers, and talked with Pondurance as part of the discovery process. Pondurance had a working relationship with both the supercenter and the grocer, having provided virtual chief information security officer (vCISO) support, cybersecurity advisory, and Payment Card Industry (PCI) compliance assistance in the past.

### OUR SOLUTION

Working side by side with the supercenter, the Pondurance team provided the cost benefit analysis for holistically outsourcing the security operations for the grocer. This move alleviated the need for the supercenter to take on a new responsibility and provided a tailored approach that allowed for alignment with the supercenter SOC and provided the visibility and oversight the grocer desired. Pondurance was able to customize a solution that fit the needs of the supercenter and the grocer in an efficient manner like no other provider could. The Pondurance SOC became a true extension of the supercenter's SOC, providing endpoint detection and response management, aggregation of network system logs, threat hunting and other specialized services, reducing overall costs for the grocer while providing a greater level of security.

### THE RESULT

With the successful management of the grocer SOC, the supercenter extended the relationship with Pondurance to cover additional areas of need. The supercenter did not have 24/7/365 SOC resources, so Pondurance supported the supercenter SOC outside of business hours. As the Pondurance team became more integrated into the supercenter SOC team, the Pondurance team took more of the tier 1 and tier 2 work, allowing the supercenter SOC resources to focus on higher value, higher priority business initiatives. In addition, as the relationship grew, the supercenter SOC was able to work more efficiently by consolidating tools and resources with the Pondurance SOC. Now, as a true extension of the supercenter SOC, the Pondurance SOC scales up and down during high activity time periods and scales across areas of specialty, giving the supercenter SOC complete access to threat hunters, SOC analysts, digital forensics and incident response specialists, and the collective threat intelligence of the Pondurance SOC.

### THE BENEFITS OF PONDURANCE MDR

- Stop security incidents through 24/7 detection and response
- Maximize internal resources and security investments
- Improve compliance through reporting
- Increase visibility into alerts that require action
- Rapidly accelerate security program maturity
- Lower total cost of ownership

### ABOUT PONDURANCE

Pondurance delivers world-class MDR services to industries facing pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements, and digital transformation. Our advanced platform with our experienced team of analysts continuously hunts, investigates, validates, and contains threats so your team can focus on what matters most.

**For more information, call 1-888-385-1702  
or email us at [info@pondurance.com](mailto:info@pondurance.com).**

**[pondurance.com](https://pondurance.com)**

Copyright © 2022 Pondurance

