Managed Detection and Response (MDR) for Logs

PONDURANCE

Personal. Proactive. Around-the-clock.

Your business works hard to achieve its mission and avoid costly interruptions, but your team likely struggles to meet detection and response goals. This includes monitoring your environments 24/7, responding quickly to threats, and complying with log storage requirements. To keep your business up and running, you need complete visibility and response across your infrastructure, powered by the ability to quickly separate real threats from noise and false positives. Your resources simply aren't growing as fast as the threats are.

Pondurance MDR for Logs delivers a 24/7 detection and response solution that analyzes your logs to uncover threats and drive rapid mitigation, powered by best-in-class technology and elite security operations centers (SOCs). We provide a managed SIEM service with forensic capabilities by aggregating and correlating log data generated by your critical assets, applications, and security controls — both on-premises and in the cloud.

THE PONDURANCE DIFFERENCE

24/7, U.S.-based SOCs

Skilled threat hunters

360-degree full visibility across networks, logs, endpoints, and cloud environments

Rapid response and close collaboration

Integration with your existing infrastructure and controls

Custom service packages designed for your desired business outcomes

PARTNER WITH OUR SECURITY EXPERTS

To start, we install cross-platform log forwarders to collect and forward logs from our extensive library of supported sources. Everything from physical or virtual server infrastructure, network infrastructure logs, and third-party applications is correlated to give you a complete picture of the actions taking place in your environments.

Meanwhile, the Pondurance SOC conducts rigorous 24/7 alert triage and threat hunting using your log data to identify and mitigate new threats. Our SOC only notifies you of validated threats - say goodbye to all those false positives. These notifications along with our findings and remediation recommendations are delivered with the Scope platform. If further investigation is required, you can view all your log data and work with our SOC analysts at anytime.

KEY FEATURES

- Pondurance's proprietary Dynamic Defense Model enables rapid threat identification, prioritization, response, and continuous improvement.
- All your data, dashboards, analyses, alerts, and communications with the Pondurance SOC are at your fingertips in our Scope platform.
- Scalable, modern log platform built to meet the needs of your business now and evolve as your log volume and velocity requirements increase.

*"Pondurance immediately proved their value and earned our trust due to their immense expertise and guidance throughout the entire process." — **Steve Long,** President and CEO of Hancock Health*

SEE A DEMO

pondurance.com