Pondurance Services

SERVICES CATALOG

Strategic and Operational Leadership

VIRTUAL CHIEF INFORMATION SECURITY OFFICER (VCISO)

With decades of experience in security consulting and advisory services, Pondurance delivers a vCISO service that applies expertise where it is needed most. Our team of seasoned security consultants aligns with a wide array of key administrative, operational, and security program competencies to help organizations that are not in the position to bring in a full-time CISO to achieve their short- and long-term goals.

24/7 Managed Detection and Response

MDR FOR LOGS (MANAGED SIEM)

Pondurance Managed Detection and Response (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.

MDR FOR NETWORK

Pondurance MDR for networks delivers a 24/7 detection and response solution that analyzes your network traffic to uncover threats and drive rapid mitigation. Powered by a dynamic technology platform and elite SOCs, we provide full visibility into your data and round-the-clock access to Pondurance experts for help with any issue, any time.

MDR FOR ENDPOINT

Pondurance MDR for endpoints delivers a 24/7 detection and response solution with full management of some of the best endpoint security technology in the business.

Pondurance partners with industry-leading endpoint security tools from SentinelOne, CrowdStrike, and Microsoft Defender to offer fully managed licenses including implementation, policy management, remote isolation, and remediation. If you already license these products, there is no additional charge for licensing. If you prefer a different endpoint detection and response (EDR) solution, we can ingest alerts from other EDR tools you may use to deliver comprehensive visibility and detection on your endpoints as your trusted partner.

MDR FOR CLOUD

Part of our MDR for logs service, Pondurance MDR for cloud delivers a 24/7 detection and response solution that analyzes your cloud telemetry to uncover threats and drive rapid mitigation, powered by best-in-class technology and elite SOCs.

Breach Response

INCIDENT RESPONSE (IR) SERVICES

When every minute counts, you need specialized cybersecurity experts to help you respond to a compromise, minimize losses, and prevent future incidents. Pondurance delivers digital forensics and incident response (DFIR) services with an experienced team capable of assisting your organization and legal team every step of the way. This includes containing the incident, determining exposure through forensic analysis, and providing confidence to continue normal business operations.

IR RETAINER

Our proactive service offering collects key company information to facilitate IR services and technical details about your network infrastructure to enable fast deployment should a cyber incident occur. We deliver an IR plan and conduct tabletop exercises to test the plan. We develop the plan to integrate with any of your internal response plans, insurance policies, and legal team, and we establish service level agreements based on your objectives.

FORENSICS DISCOVERY AND ANALYSIS

Cybersecurity and forensic experts manage and review each investigation to validate findings and assist with providing clear and concise written reports or oral testimony. Forensic and malware specialists apply deep technical forensics skills, ensuring the proper handling of digital evidence to aid in the investigation and prevent disruptions. E-discovery specialists have the ability to collect your data from various sources and programmatically analyze it for protected or other sensitive information.

POST-REMEDIATION VULNERABILITY SCANNING

To help improve ongoing cyber resilience, Pondurance can identify, categorize, and prioritize vulnerabilities, as well as recommend actionable insight to mitigate potential threats. Our team of highly experienced security operation experts examines components within your environment that pose potential threats. They utilize manual tests to reduce false positives and identify threats that are not easily discovered through automated processes.

LITIGATION SUPPORT AND INVESTIGATIVE SERVICES

With our investigative services and comprehensive litigation support, we are with you through the entire life cycle of the incident. Our forensic specialists focus on your unique requirements to collect and analyze data, determine if protected information has been compromised, and support your legal team to assist them in providing you legal strategies and decisions. With Pondurance as your IR team, you get the independent, expert investigative services (e-discovery, IP theft, and cyber incidents) needed to fuel your legal action plans alongside your business recovery plan.

Discover and Manage Vulnerabilities

PENETRATION TESTING

Pondurance performs comprehensive discovery and enumeration procedures to target pertinent internal address ranges and establish a baseline of services to manually test for common configuration issues and vulnerabilities.

We review and validate all identified vulnerabilities to remove false positives. Human-driven manual testing procedures are executed to identify flaws not easily identified with automated tools. Penetration Testing is performed against identified vulnerabilities to evaluate the effectiveness of security controls. We perform detailed security analysis and vulnerability scanning using a comprehensive suite of tools.

VULNERABILITY MANAGEMENT PROGRAM (VMP)

With experience in midmarket and enterprise organizations, Pondurance VMP provides a managed service to continually identify, categorize, and prioritize vulnerabilities, as well as recommend actionable insight to mitigate potential threats. Our team of highly experienced security operation experts examines components within your environment that pose potential threats. They utilize manual tests to reduce false positives and identify threats that are not easily discovered through automated processes. Our program includes weekly threat reports, specialized threat and vulnerability inventory assessment and scanning, comprehensive monthly external and quarterly internal vulnerability scanning, and annual penetration testing.

Assess Systems and Controls

TABLETOP EXERCISE

Tabletop exercises are truly one of the best, most cost-effective ways to assess and prepare your organization's cyber resilience planning without having to experience an actual disaster. This is your opportunity to perform this critical exercise and prepare for a crisis before you're in the midst of the crisis itself.

We take our experiences across hundreds of events and observations to provide you with a best practices IR plan with an integrated playbook. Pondurance will walk through any questions you and your team may have and suggest options that would make your organization more prepared for an actual threat.

SECURITY INCIDENT RESPONSE PLANNING

Pondurance can help your organization review and develop security incident response plans to ensure that your procedures are comprehensive, actionable, and robust. Our methodology ensures that you have IR plans that cover preparation of management and organizational resources; establishment of organizational posture for monitoring events and recognizing, identifying, and detecting incidents; predefined processes and procedures for containment and eradication; and established procedures to facilitate recovery, communication with stakeholders, and documentation of key learnings.

APPLICATION AND SYSTEMS ARCHITECTURE REVIEWS

Pondurance performs detailed application security analysis and vulnerability scanning using a comprehensive suite of tools. The testing encompasses the various tiers of the application architecture to provide a deep assessment of critical applications. Areas of testing include, but are not limited to, OWASP Top 10 and verification and manual testing.

STATIC CODE REVIEW

Pondurance will analyze your application source code, byte code, and binaries for coding and design conditions that are indicative of security vulnerabilities. Our Static Application Security Testing services analyze an application from the "inside out" in a non-running state via information gathering and isolation and automated methods verification and manual review.

RED TEAM EXERCISE

Pondurance can help validate both digital and physical security to ensure that your organization has a clear understanding of risk. Whether the engagement begins with spear-phishing an employee or attempting to enter facilities, we'll first discuss all scenarios with you during a rules of engagement meeting. This discussion ensures that your expectations will be met and our techniques are approved.

Program Assessment

CYBER RISK ASSESSMENTS POWERED BY MYCYBERSCORECARD

Pondurance Cyber Risk Assessments powered by MyCyberScorecard is an all-in-one solution that delivers streamlined and efficient cybersecurity assessments that align with regulatory standards and compliance requirements. Our cyber risk experts, using the MyCyberScorecard platform, partner with you to analyze and visualize potential cybersecurity gaps and make key remediation recommendations.

PCI ASSESSMENT (CERTIFIED QUALIFIED SECURITY ASSESSOR)

Pondurance offers a focused review of your IT systems environment to identify areas of risk and maturity as they relate to Payment Card Industry Data Security Standard (PCI DSS) compliance. At the conclusion of the assessment, Pondurance either conducts a self-assessment questionnaire or delivers a report on compliance accompanied by an attestation of compliance. If your organization is out of compliance, we offer a tailored, prioritized approach to helping you get in compliance quickly.

Program Assessment

HIPAA ASSESSMENT

Pondurance offers a focused review of your IT systems environment to identify areas of risk and maturity as they relate to the HIPAA security rule. At the conclusion of the assessment, Pondurance delivers an executive summary along with detailed findings, risk ratings, and recommendations, using the National Institute of Standards and Technology (NIST) maturity levels rating system for each control requirement. This ensures you have a comprehensive foundation to develop a plan of action milestones.

The Pondurance HIPAA security rule compliance assessment is conducted by our team of security experts, partnering directly with you to guide you through the process. A team of Pondurance experts embeds with your multidisciplinary teams, analyzes your current HIPAA compliance posture, and outlines a set of desired outcomes for proper handling of electronic protected health information with categorized references to how they can be achieved.

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

We are a CMMC registered provider organization with registered practitioners on our team. We have the experience and skills to work effectively with your organization to help you achieve CMMC 2.0 compliance and better understand the gaps in your processes, capabilities, and practices across the CMMC domains. Members of our skilled compliance advisory services team will conduct a readiness assessment aligned with your desired CMMC 2.0 maturity level. This identifies any deficiencies across all relevant CMMC domains and related processes, capabilities, and practices, along with remediation recommendations. As part of the remediation effort, we can augment your capabilities with staffing.

NIST-CSF CYBER RISK ASSESSMENT

Pondurance offers a focused review of your IT systems environment to identify baseline risk and maturity as they relate to the security practices recommended by NIST with its cybersecurity framework (CSF). At the conclusion of the assessment, Pondurance delivers an executive summary along with detailed findings, risk ratings, and recommendations available through our MyCyberScorecard platform for each control requirement. This ensures you have a comprehensive foundation to develop a plan of action milestones. The Pondurance NIST-CSF Cyber Risk Assessment is conducted by our team of security experts, partnering directly with you to guide you through the process. The framework core, designed to be intuitive and act as a communication layer between multidisciplinary teams, outlines a set of desired cybersecurity outcomes with categorized references to how they can be achieved.

BUSINESS CONTINUITY PLANNING AND REVIEW

Business impact analysis, business continuity planning, and disaster recovery plan integration are advisory practices that focus on business and information technology integration.

VENDOR RISK MANAGEMENT ADVISORY

The vendor risk management program develops a repeatable process to evaluate supply chain and third-party vendor risk prior to purchase or implementation to help ensure applications and vendors are providing an appropriate level of compliance and security for any organization's needs.

Training

AWARENESS TRAINING

In addition to being a KnowBe4 reseller, Pondurance can create and deliver custom awareness training leveraging vCISO resources.

CUSTOM SECURITY TRAINING

Develop training tailored to your organization's specific needs and gaps.