Get Persistent Defense with DeepSeas MDR+

Managed Detection & Response from DeepSeas

DeepSeas MDR delivers comprehensive, 24x7 threat detection and response by integrating with your existing security tools and building resilient, human-led business processes into your cyber program.

Overview

Managed Detection & Response (MDR) from DeepSeas delivers superior protection against all attack types, immediately expanding your visibility into the threat landscape while significantly lowering the average time to detect an intrusion from what is often months to mere minutes. We offer the next generation of advanced cyber defense managed services by providing 24x7 threat detection and analysis, white-glove response support to threats, advanced log management, and anomaly identification. We promote personal working relationships between our team and your organization and collaborate to meet your strategic cybersecurity objectives.
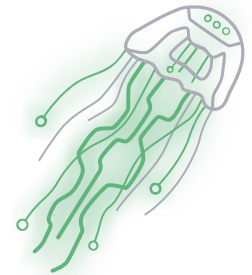
Why DeepSeas MDR+

Reduce business risk by protecting your digital assets, intellectual property, and day-to-day operations from cyber attacks.

Expand visibility across the attack surface to identify bad actors, their behaviors, and their motives for targeting your business.

Rapidly increase your cyber-ROI by rationalizing tools, building repeatable processes, and limiting hiring and retention burdens.

Generate measurable outcomes that can be tracked, benchmarked, and easily communicated to your Board of Directors.

Benefit from flexible engagement models, ranging from remote and dedicated to hybrid, ensuring the right level of support for your program.

DeepSeas MDR Offerings

MDR for endpoint from DeepSeas offers 24×7 detection, analysis, and response to validated threats generated from the endpoint security tool(s) deployed within your environment and supplemented by proactive hunting and continuous technical threat intelligence updates.

MDR for network from DeepSeas offers 24×7 detection, analysis, and response to validated threats generated from out-of-band, full-packet capture intrusion detection systems (IDS) deployed within your environment to enable behavioral and analytic-based monitoring of inbound, outbound, and lateral network traffic.

MDR for email from DeepSeas offers continuous monitoring of user-reported suspected phishing and business email compromise attacks. Suspicious emails are isolated and aggregated in a separate, controlled cloud environment and forwarded to the DeepSeas Cyber Defense Platform for human analysis, triage, and disposition.

MDR for SIEM from DeepSeas offers 24×7 event analysis and supervised response to machine data generated by one or more system event log aggregation servers installed on your network. DeepSeas will deploy a core set of alerting rules and analytics to enable increased contextualization of the machine data.

MDR for Operational Technology (OT) from DeepSeas offers 24×7 threat detection, analysis, and response to potential threats found within your manufacturing, industrial and/or other OT environment(s). Threats are detected and verified by DeepSeas cyber defense analysts who review alerts from passive OT threat detection tools.

Dive Deeper