DeepSeas MDR for SIEM

Enrich and contextualize alerts.

Managed Detection & Response (MDR) for SIEM by DeepSeas provides comprehensive security oversight by harnessing advanced analytics to identify and neutralize cyber threats, delivering 24x7, expert-driven monitoring and response tailored to your unique environment. With DeepSeas MDR, SIEM rules are deployed and fine-tuned for enhanced contextualization of machine data utilizing Endpoint Detection and Response (EDR) and Network Detection and Response (NDR) technologies. These rules enrich alerts, with SIEM use cases serving as a primary source for threat detection.

What You Can Expect from DeepSeas MDR for SIEM

Specialized Threat Detection

DeepSeas specializes in detecting threats by leveraging the security tools you already have in place for alert review, proactive searches, and targeted threat hunting.

Detailed Threat Notification

The DeepSeas crew will provide detailed reports on validated threats, including nature, context, severity, and remediation steps, crafted by our expert cyber defense analysts.

Expert Threat Response

DeepSeas will provide you and appropriate teams in your organization with expert guidance and actions for threat resolution, all detailed in a jointly approved MDR runbook.

Curated Threat Intelligence

Threat detection and response effectiveness are enhanced by DeepSeas through tailored detection logic and analytics in your network.

Incident Response

Following threat detection, DeepSeas coordinates effective response strategies, including containment and eradication of threats, and advises on remediation actions.

In-depth Event Analysis

DeepSeas integrates and analyzes security data from across your network, identifying anomalies and potential threats through sophisticated correlation rules, enhancing visibility and insights.

DeepSeas MDR for SIEM Service Levels

Essential SIEM	Managed SIEM	SIEM Alert Management
Shared Service	Personalized Service	Co-managed service
DeepSeas Core Threat Detections Library	DeepSeas Core Threat Detections Library + Custom Use Cases	DeepSeas Core Threat Detections Library + Custom Use Cases
400 Days Log Storage & Search	Configurable Log Retention & Search	Configurable Log Retention & Search
24x7 Detection & Response	24 x 7 Detection & Response	24 x 7 Detection & Response
DeepSeas Managed SIEM Platform – powered by Devo	Customer Managed SIEM Platform – Devo, Splunk, or Microsoft Sentinel	DeepSeas Managed SIEM Platform – Devo, Splunk, or Microsoft Sentinel

Get a Single Virtual Command Center

DeepSeas VISION, our proprietary security operations platform, unites your entire security program and provides a single virtual command center to manage strategic security planning, ongoing attack surface and vulnerability management, and 24x7 defense from cyber threats. Only clients of DeepSeas have access to DeepSeas VISION, which increases visibility, maximizes utilization of security tools, and gives immediate uplift to detection and response capabilities while covering all attack surfaces, including Operational Technology (OT).

Get a quote for MDR from DeepSeas.