NodeRisk

DATASHEET

Managed Detection & Response

Why NodeRisk

NodeRisk's **Managed Detection & Response (MDR)** service combines cutting-edge threat detection technology, premium intelligence sources, and SIEM/SOAR integration to deliver unparalleled protection. We validate and enhance each alert, ensuring high-quality insights. Our use of SIEM and SOAR tools automates routine tasks and enriches incident data, empowering our team to focus on threats that matter most

Service Overview

NodeRisk's MDR provides 24/7 monitoring, threat detection, and response through a layered approach, leveraging SIEM for centralized logging and analysis and SOAR to automate and streamline workflows. This integration enables us to reduce response times and enhance threat visibility, ensuring a robust defense against advanced threats.

Key Areas of Focus

- **Advanced Threat Detection:** Behavioral analytics, threat intelligence, and machine learning to identify known and unknown threats.
- **Automated & Rapid Response:** SOAR-driven playbooks that facilitate immediate containment and mitigation of high-priority incidents.
- **Threat Intelligence Integration**: Up-to-date intelligence feeds to inform detection and response, enhancing the accuracy and relevance of insights.

Deliverables

- **Executive Summary Reports:** Condensed insights and summary of actions for executive stakeholders.
- **Detailed Incident Reports**: Comprehensive breakdowns of detected threats, including remediation steps and threat intelligence context.
- **Customized Response Playbooks:** SOAR-driven, tailored response plans based on observed threats and security goals.
- **Real-Time Alerts & Notifications:** Immediate notifications on critical incidents, backed by SIEM and SOAR enrichment.
- **Threat Intelligence & Trend Analysis:** Periodic reports on evolving threat patterns, offering insights for proactive defense.

Methodology

NodeRisk's approach integrates SIEM and SOAR solutions for an optimized, efficient, and scalable response framework.

1. **24/7 Continuous Monitoring:** Real-time monitoring across networks, endpoints, and cloud environments through centralized SIEM logging and analysis.
2. **Automated Playbooks & Response:** SOAR-driven workflows automate alert handling, validation, and escalation, allowing rapid containment of verified threats.
3. **Expert Analysis & Threat Validation:** Our team validates high-priority alerts, focusing on high-impact incidents while SOAR handles routine tasks.
4. **Incident Response & Containment:** Manual and automated response actions are employed for precise containment, minimizing disruption and risk.

For more info visit: https://noderisk.com/contact