HORIZON3.ai

~~TRUST~~ BUT VERIFY

WHITE PAPER

Building an Overwatch Service with NodeZero Tripwires™: A Strategic Guide for MSSPs

MSSP Overwatch Services

Building an Overwatch Service with NodeZero Tripwires™: A Strategic Guide for MSSPs

Managed Security Service Providers (MSSPs) often look for innovative ways to enhance their service portfolios. Leveraging **NodeZero Tripwires™**, MSSPs can create an advanced **"Overwatch Service"** to proactively detect threats, improve incident response (IR) capabilities, and unlock new revenue streams. This guide outlines how MSSPs can strategically build, market, and operationalize an Overwatch Service to strengthen client security and drive business growth.

The Role of NodeZero Tripwires in an Overwatch Service

NodeZero Tripwires strategically deploys decoys – such as fake files and fake credentials – along proven attack paths in an environment during autonomous pentests performed by the NodeZero platform. This approach ensures that the tripwires are placed where it matters most to an organization.

This approach reduces the complexity of traditional deception solutions, allowing MSSPs to focus on delivering actionable insights without the burden of managing extensive setups of traditional honeytoken approaches.

An Overwatch Service powered by NodeZero Tripwires offers a proactive layer of defense, ensuring swift detection and response to critical threats, while enabling MSSPs to differentiate their offerings in the cybersecurity market.

NodeZero Tripwires Strategic Features

Automated Deployment: Seamlessly integrated with NodeZero's autonomous pentesting, tripwires are automatically deployed in high-risk areas without the need for manual intervention.

Real-Time Alerts: Receive immediate alerts in the NodeZero Tripwires notification center, with detailed information on the nature of the access attempt, location, and potential threat to help investigations.

Low False-Positive Rate: High-quality signal ensures that alerts are meaningful and actionable, minimizing the occurrence of false positives.

Versatile Tripwire Types: Deploys a variety of tripwires to detect unauthorized access attempts across different attack vectors. Types include AWS API Key, mysqldump, and Windows Suspicious Process Monitor.

Easy-to-Use Management Console: Centralized dashboard for managing all deployed tripwires and viewing alert histories. Simple notification controls.

Integration with Security Tools: Easily integrates with existing SIEMs and other security tools, enhancing incident response workflows.

Core Benefits for MSSPs

NodeZero Tripwires provide MSSPs with key advantages that elevate their threat detection and response capabilities as follows:

Proactive Threat Detection

Quickly identify lateral movement, privilege escalation, and data exfiltration attempts by placing decoys in sensitive areas. Real-time alerts provide actionable insights, helping MSSPs address threats before they escalate.

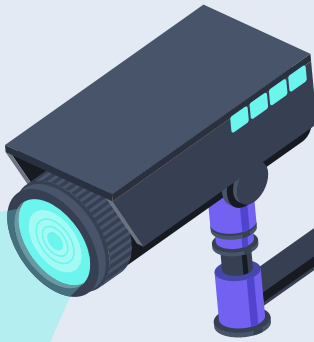
Continuous Monitoring

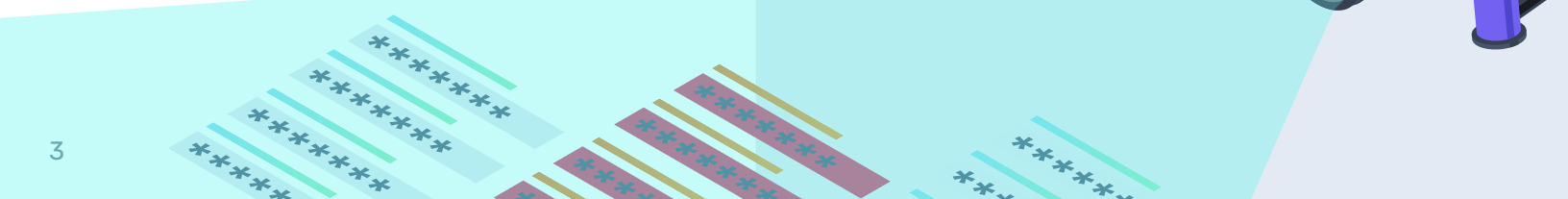
Once deployed, Tripwires ensure persistent visibility into client environments, detecting new threats as they emerge and maintaining protection long after initial pentests.

Seamless Integration

Easily integrate Tripwire alerts into SOC workflows, incident response playbooks, and client dashboards. This streamlines operations, enhances transparency, and solidifies MSSPs as trusted cybersecurity partners.

These benefits allow MSSPs to deliver proactive, ongoing protection while building stronger client relationships and differentiating their services.





Building the Overwatch Service

An Overwatch Service powered by NodeZero Tripwires can be offered in a tiered structure, accommodating diverse client needs and budgets while maximizing revenue potential. Here is an example of a tiered service model. (Note: The monetization models that follow serve as example pricing only.)

Tiered Service Model

Tier 1: Basic Monitoring and Alerting

Service Description:

- MSSPs monitor alerts for clients and provide basic notifications of suspicious activity.
- Alerts include contextual details (e.g., time of access, source IP) to inform client teams.

Monetization Model:

- Charge a flat monthly fee per tripwire or per environment.
- Example Pricing: $500/month for up to 10 tripwires.

Key Benefits for Clients:

- Affordable early detection.
- Basic visibility into potential threats.

Tier 2: Enhanced Monitoring with Incident Response Playbooks

Service Description:

- Includes everything in Tier 1.
- MSSPs initiate pre-defined incident response playbooks based on tripwire alert types.
- Playbooks can include actions like isolating affected systems, escalating to client teams, or deploying containment measures.

Monetization Model:

- Subscription fee plus per-incident fees for response actions.
- Example Pricing: $1,500/month for monitoring, plus $1,000 per incident response engagement.

Key Benefits for Clients:

- Rapid containment and response.
- Reduced mean time to detect and respond (MTTD/MTTR).

Tier 3: Advanced Overwatch with Continuous Improvement

Service Description:

- Includes everything in Tier 2.
- MSSPs offer continuous environment optimization by deploying additional tripwires in response to detected threats.
- Includes bi-weekly or monthly reviews of alert patterns and recommendations for improving security posture.

Monetization Model:

- Premium subscription plus consulting fees.
- Example Pricing: $3,000/month, inclusive of quarterly environment reviews.

Key Benefits for Clients:

- Ongoing security posture improvement.
- Proactive adjustments to threat trends.

Tier 4: Fully Managed Detection and Response (MDR)

Service Description:

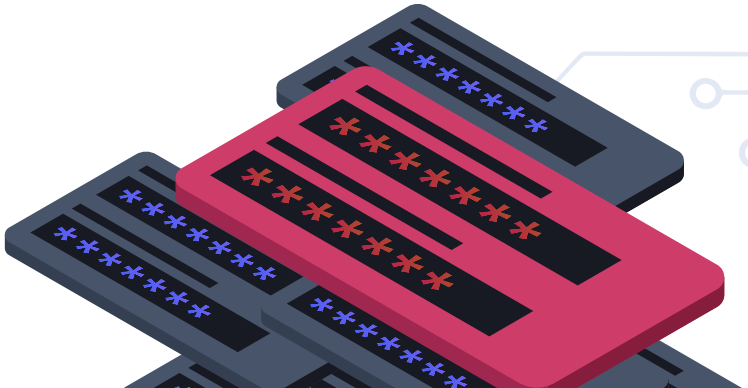
- Combines tripwire alerts with full MDR capabilities.
- MSSPs provide 24/7 SOC monitoring, correlating tripwire data with other telemetry (e.g., SIEM, EDR logs).
- Provides end-to-end incident management, from detection to remediation.

Monetization Model:

- High-margin annual contracts.
- Example Pricing: $5,000–$10,000/month, depending on environment size and complexity.

Key Benefits for Clients:

- Comprehensive threat visibility.
- Seamless integration of tripwire alerts into broader threat detection workflows.



HORIZON3.ai
~~TRUST BUT~~ VERIFY

Driving Demand for Overwatch Services

NodeZero Tripwires presents MSSPs with unique opportunities to promote and monetize their Incident Response (IR) Services:

Educational Campaigns: MSSPs can educate clients about the risks of lateral movement and insider threats, emphasizing how Tripwires serve as an early warning system.

Pentest Follow-Ups: After completing NodeZero pentests, MSSPs can recommend Tripwires to monitor vulnerabilities and at-risk systems identified during testing. This follow-up creates a natural entry point for Overwatch Services.

Demo Alerts: Deploy demo tripwires in client environments to simulate the types of alerts they might receive. This tangible demonstration helps clients understand the value of proactive monitoring.

Bundling with IR Retainers: Include a limited number of tripwires as part of an incident response retainer package, creating upsell opportunities for higher-tier monitoring services.

Operationalizing the Overwatch Service

Staffing Requirements

Example staffing needed:

- **SOC Analysts:** Monitor alerts and provide Tier 1 and Tier 2 support.
- **Incident Responders:** Execute playbooks and manage escalations.
- **Account Managers:** Conduct client reviews and identify upsell opportunities.

Technology Integration

Integrate NodeZero Tripwires with:

- **SIEM Platforms:** Correlate tripwire data with other telemetry.
- **SOAR Tools:** Automate responses to tripwire alerts.
- **Ticketing Systems:** Streamline alert tracking and client communication.

Playbook Development

Create standardized incident response playbooks for scenarios like:

- Unauthorized file access.
- Credential harvesting.
- Suspected lateral movement.

Reporting and Insights

Deliver detailed reports with:

- Tripwire activity summaries.
- Recommendations for tripwire placement.
- Trends and patterns across alerts.

Monetizing Additional Services

MSSPs can enhance revenue by offering add-ons and complementary services tied to tripwire monitoring: *(Note: The monetization models that follow serve as example pricing only.)*

Custom Tripwire Deployment: Deploy Tripwires in unique or high-risk client environments for an additional fee.

- Example Pricing: $200 per custom tripwire.

Incident Response Drills: Conduct tabletop exercises or simulations triggered by tripwire alerts.

- Example Pricing: $5,000 per drill.

Forensic Analysis: Provide post-incident forensic investigation for tripwire-triggered events.

- Example Pricing: $3,000 per incident.

Integration Consulting: Help clients integrate tripwire alerts with their existing tools and workflows.

- Example Pricing: $2,000 per engagement.

Strategic Benefits for MSSPs

Building an Overwatch service around NodeZero Tripwires offers MSSPs several advantages:

Recurring Revenue: Subscription-based pricing ensures predictable cash flow.

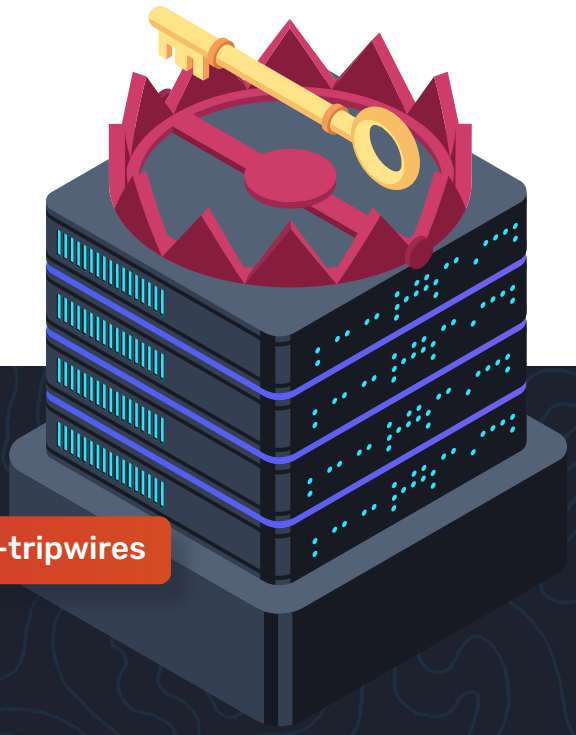
Client Stickiness: Proactive monitoring and regular engagement build trust and long-term relationships.

Upsell Opportunities: Higher-tier monitoring and complementary services generate incremental revenue.

Market Differentiation: Few MSSPs offer tripwire-based services, positioning you as an innovator in cybersecurity.

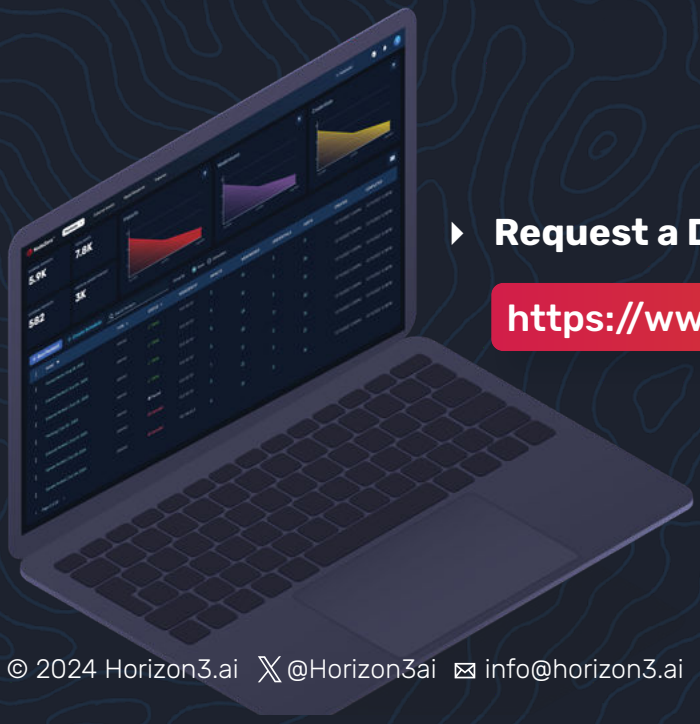
Conclusion

NodeZero Tripwires is a game-changer for MSSPs looking to enhance their offerings and grow their business. By building an Overwatch Service, MSSPs can provide proactive monitoring, drive demand for incident response, and monetize higher-tier services. This approach not only strengthens client security but also positions MSSPs as strategic partners in the fight against modern cyber threats.



Learn More About NodeZero Tripwires

https://www.horizon3.ai/nodezero/nodezero-tripwires



Request a Demo of NodeZero Tripwires

https://www.horizon3.ai/demo