STACKTITAN

PLAY OFFENSIVE. STAY DEFENSIVE.

CASE STUDY: MSP / MSSP

SHIP FAST, WITH CONFIDENCE

Case Study: MSP / MSSP

OVERVIEW

A billion dollar managed service provider (“MSP”) with a large customer base wants to extend its service portfolio to include security assessments and penetration tests. However, it cannot perform these services directly due to potential conflict of interest that arises from self-assessing.

INDUSTRY

Managed Services

CHALLENGES

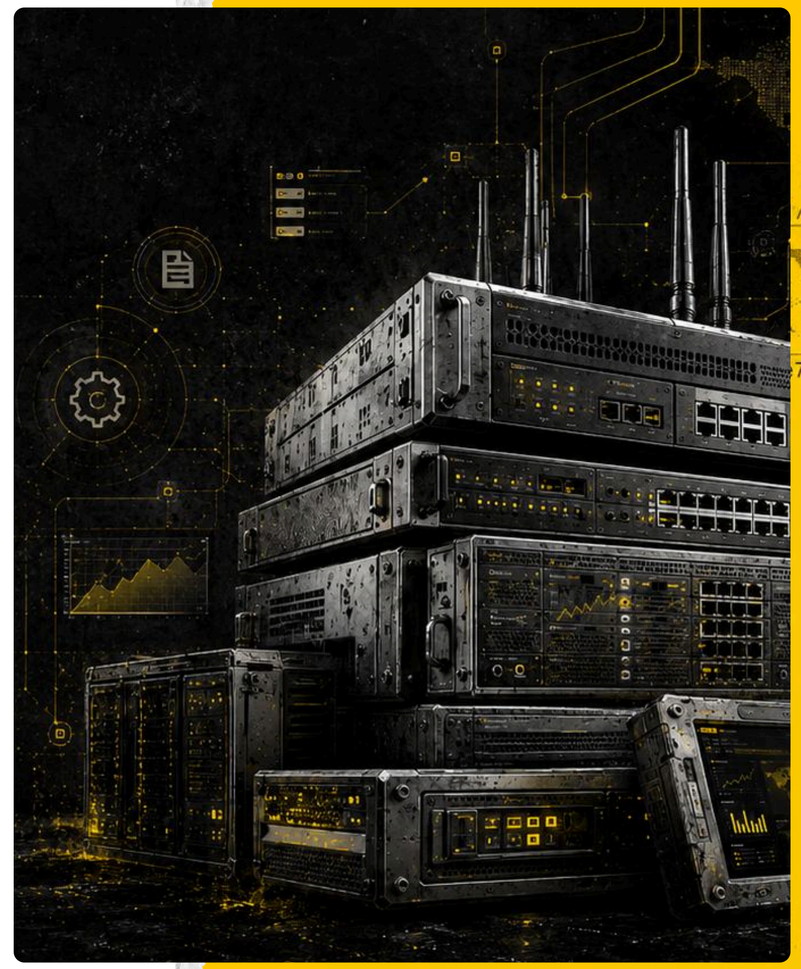
Providing managed security services to the MSP’s customer base while avoiding a conflict of interest.

HOW STACKTITAN HELPED

STACKTITAN established a named partnership with the MSP, offering its full suite of security services as an extension of the MSPs extensive portfolio, which included:

- **Web and mobile application penetration testing**
- **Source code analysis / reverse-engineering**
- **Network Penetration Testing**
- **Cloud security assessments**
- **Social engineering**
- **Wireless penetration testing**

Furthermore, STACKTITAN performed penetration testing services directly for the MSP, to evaluate the security of its supporting architecture and remote management utilities.



Case Study: MSP / MSSP

30
Penetration assessments

>3
Years of partnership

100%
Complete impartiality

$$$
Increased revenue

SOLUTION

Establish a named partnership through which the MSP refers its customers for unbiased, 3rd party security services.

RESULTS

STACKTITAN's service portfolio was included in the catalog of the MSP's capabilities, allowing its customers to perform recurring or ad-hoc assessments and penetration tests of their managed environments while avoiding a conflict of interest.

NEXT STEPS

Recurring assessments can be used to track trends, to meet regulatory & cyber insurance requirements, and proactively identify risk in a landscape of evolving threats.

PLAY OFFENSIVE.
STAY DEFENSIVE.

STACKTITAN

3606 North 156th St, Suite 101 - 294
Omaha, NE, 68116

sales@stacktitan.com | stacktitan.com

STACKTITAN delivers expert-led cybersecurity assessment and advisory programs for organizations that need to understand how their defenses perform under real-world pressure. We expose risk, test controls, guide remediation, and strengthen security posture over time.

Our work shifts security teams and their attack surfaces towards greater scrutiny and resilience. With red team thinking, purple team collaboration, and platform-assisted delivery, we bring adversarial insight and practical guidance together to help organizations harden and deepen their defenses.