



MSSP Cyber Fusion Success Story

Threat Intelligence, Incident
Management, and Security
Orchestration in Action



Executive Summary

To stay resilient amidst the ever-evolving cyber landscape, organizations are increasingly relying on Managed Security Services Providers (MSSPs) to strengthen their security posture. Catering to each enterprise client's diverse operational requirements, types of infrastructure, and unique threats presents tremendous challenges for MSSP teams. They require automated and threat intelligence-driven security solutions to serve this growing scale of managed security operations. This case study describes how one of the leading global MSSPs deployed Cyware's Cyber Fusion suite of solutions including Respond, Orchestrate, and Intel Exchange to achieve measurable performance gains and cost savings, while enhancing capabilities for their diverse client base.

Cyber Fusion MSSP Outcomes

50%

Improvement in MTTR

30%

Reduction in Service Cost

25%

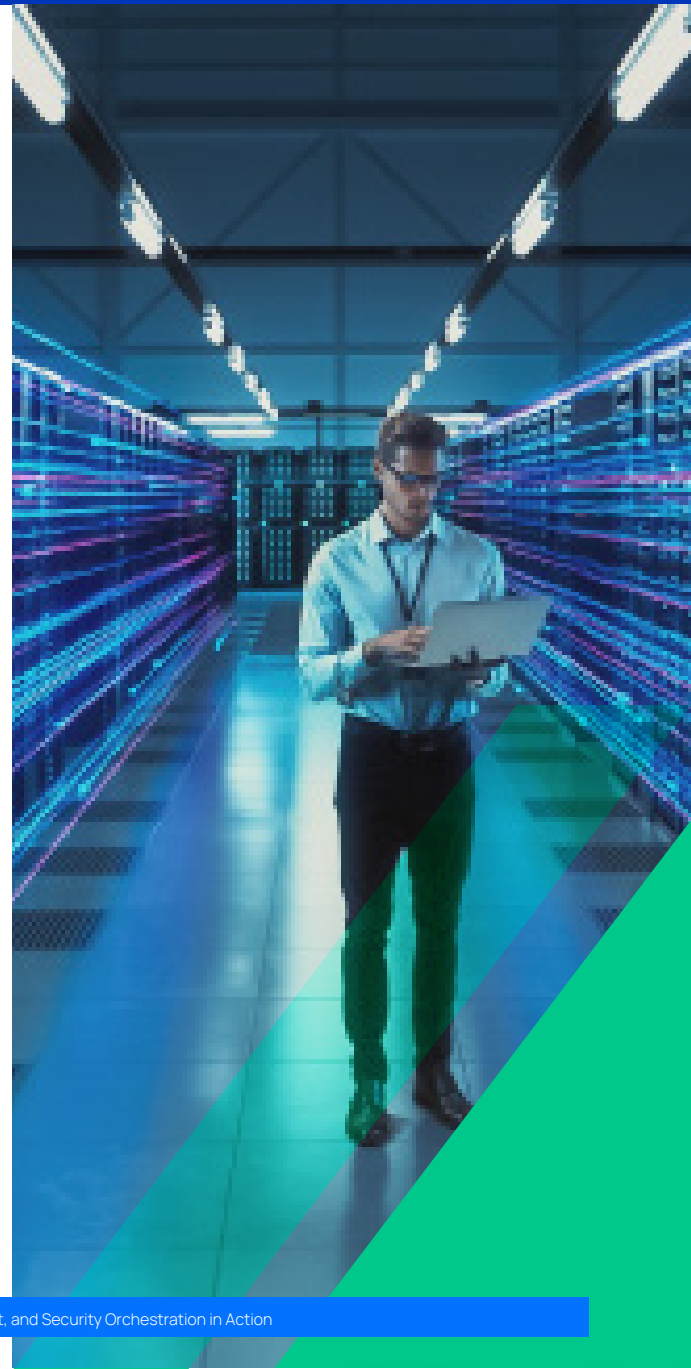
Increased Service Margins

Guardians at the Gate Face Growing Challenges

As a leader in the managed services field, Cyware's MSSP client encountered several key challenges reflective of the sector's growing pains.

- **Manual Incident and Alert Management:** With the rising number and complexity of cyber threats, the MSSP's processes for incident triage and response, which involved manual and time-consuming tasks, became increasingly untenable – especially when managing multiple client environments.
- **Lack of Centralized Orchestration and Automation:** The MSSP's use of disparate tools for different security functions, without a unified integration framework, led to inefficiencies and a disjointed response to security incidents.
- **Lack of Threat Intelligence Operationalization:** Without a centralized system for collecting, analyzing, and operationalizing threat intelligence, the MSSP struggled to keep pace with the rapidly evolving threat landscape, a necessity for effective and proactive cybersecurity measures.
- **Limited SecOps Visibility:** Lastly, the lack of centralized metrics hindered their ability to effectively monitor and manage operations on a large scale, making it difficult to assess, adjust, and optimize their cybersecurity strategies.

These challenges reinforced the need for the MSSP to adopt a more integrated, automated, and intelligent approach that would enhance its operations and strengthen its standing as an industry leader.



SecOps Reimagined

MSSP's Strategic Move to Cyware

In addressing the challenges faced by the MSSP, the implementation of advanced cybersecurity solutions brought about transformative benefits by adding scale and gaining technology-enabled efficiency. These improvements not only streamlined operations but also elevated the overall effectiveness of their clients' security postures through the delivery of advanced and customized services.

- 1 Automated Incident Management:** The MSSP achieved a more efficient incident handling process. This was accomplished by automatically retrieving incident details from ITSM systems, conducting automated analyses, enriching Indicators of Compromise (IOCs), and executing response actions through sophisticated orchestration playbooks. This streamlined approach reduced the average response times (MTTR) by 50% and increased accuracy in handling incidents.
- 2 Enhanced SLA Performance:** The MSSP enhanced its performance oversight and saw noticeable improvements in adhering to Service Level Agreements (SLAs). Cyware implemented customized SLA-related notifications and comprehensive dashboards, enabling the MSSP to take more proactive measures to avoid SLA breaches and maintain high service standards.
- 3 Efficient Roster Management:** The MSSP gained comprehensive operational visibility and implemented role-based access control for incident management. This led to smoother SOC management and a 30% reduction in service cost through efficient and effective resource allocation for each incident.
- 4 Centralized Security Orchestration:** The integration of their security infrastructure was significantly enhanced through Cyware's centralized orchestration technology. By using pre-built connectors and low-code playbooks, the MSSP was able to leverage previously siloed threat data and construct cross-functional orchestration workflows. This unified approach facilitated more cohesive and effective security operations.
- 5 Threat Intelligence Operationalization:** The MSSP implemented a system for aggregating, enriching, and prioritizing threat intelligence. This centralized approach enabled more proactive detection and response measures, ensuring that the MSSP's teams were ready to handle any emerging threats.
- 6 Automated Threat Prioritization and Enrichment:** Cyware automated the MSSP's process of scoring and enriching IOCs. By integrating different feeds and third-party sources, the MSSP could now prioritize threats more effectively, leading to more informed decision-making and an efficient incident management process.

These advancements collectively enabled the firm to not only overcome their initial challenges but also set a new benchmark in managed security services by increasing their service margins by 25%, showcasing the power of integrating cutting-edge collaborative technologies in cybersecurity operations.

Empowering Next-Gen Managed Security Services

Driven by the increasing frequency and sophistication of cyberattacks and the expanding digital footprint of businesses globally, the demand for specialized cybersecurity expertise is set to grow rapidly in the coming years. Cyware's solutions are helping facilitate various existing MSSP business models as well as unlocking new opportunities to achieve increased gross margin and deliver innovative solutions, such as threat intelligence-as-a-service.

This case study exemplifies the transformative power of embracing technology-driven solutions in the face of rapidly evolving cyber threats. By overcoming complex challenges with innovative approaches to SecOps, the MSSP has not only resolved its immediate operational inefficiencies but has also set a new standard in proactive cybersecurity management.



Cyware Labs Inc
111 Town Square Place
Suite 1203, #4
Jersey City, NJ 07310

www.cyware.com

sales@cyware.com

