Incident Story

From €500K Loss to Zero Impact: The Power of Microsoft MXDR

Chorus Cyber | www.choruscyber.com

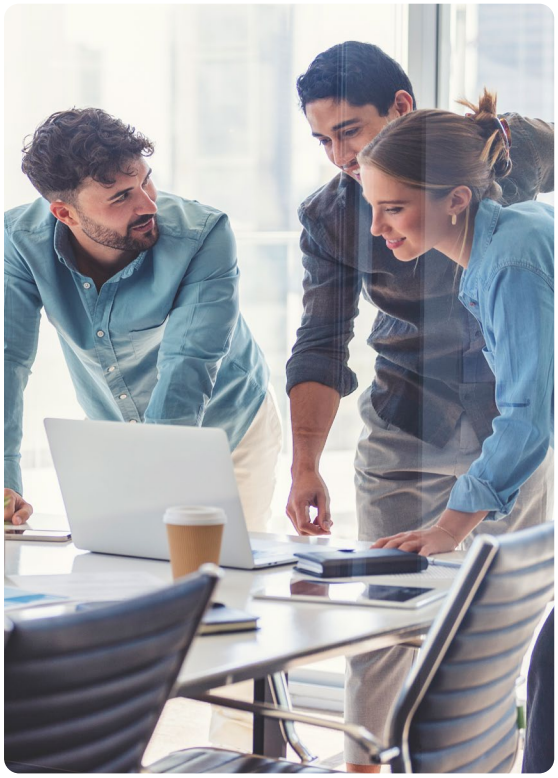
How Microsoft MXDR helped a European Manufacturer from disaster

Executive Summary

For SMBs in 2025, downtime has big impact on reputation, risk and customer confidence. How you respond and how quickly you respond is everything.

For one European manufacturer, a lack of real-time visibility and response capabilities turned a single vulnerability into €500,000 of operational and reputational loss. Just months later, when faced with an almost identical threat, the same company experienced less than one hour of email disruption; with no data loss and no lateral movement—thanks to a modern, Microsoft-powered Managed Extended Detection and Response (MXDR) service delivered by Chorus Cyber's 24/7 Cyber Security Operations Centre (CSOC).

This white paper contrasts two nearly identical attacks with vastly different outcomes. It explores the Microsoft security stack, explains the role of a proactive MXDR service, and outlines how partners can unlock new revenue opportunities through Chorus Cyber's partner programme.



> **"What took months to detect and recover from was neutralised in hours - with zero impact to operations."**
>
> Mark Jones, Head of Cyber Security at Chorus Cyber

The Background

A large manufacturing business, serving critical industries across Europe, had long been operating with a basic security setup. Despite its size and reach, the company lacked a dedicated security operations centre, real-time threat monitoring, or automated incident response capabilities. Responsibility for IT security fell largely on internal teams and a managed service provider (MSP) focused on infrastructure rather than cyber defence.

The First Incident

In 2024, a well-known critical vulnerability, ProxyLogon, was exploited in the company's on-premises Microsoft Exchange environment. The breach enabled attackers to deploy malware, exfiltrate data, and disrupt operations. With no active monitoring in place, the compromise went undetected for days.

The Result?

Three months of disrupted operations

More than €500,000 in financial damage

Significant risk of regulatory penalties

The Turning Point

In the wake of the breach, the company made a strategic shift. Microsoft 365 Business Premium licensing was fully adopted, and the business was onboarded into Chorus Cyber's MDR service, later upgraded to MXDR. Delivered in partnership with their existing MSP, the MXDR solution provided comprehensive threat detection and response across endpoints, identity, cloud, and email - underpinned by 24/7 monitoring from Chorus Cyber's CSOC.

The Second Incident

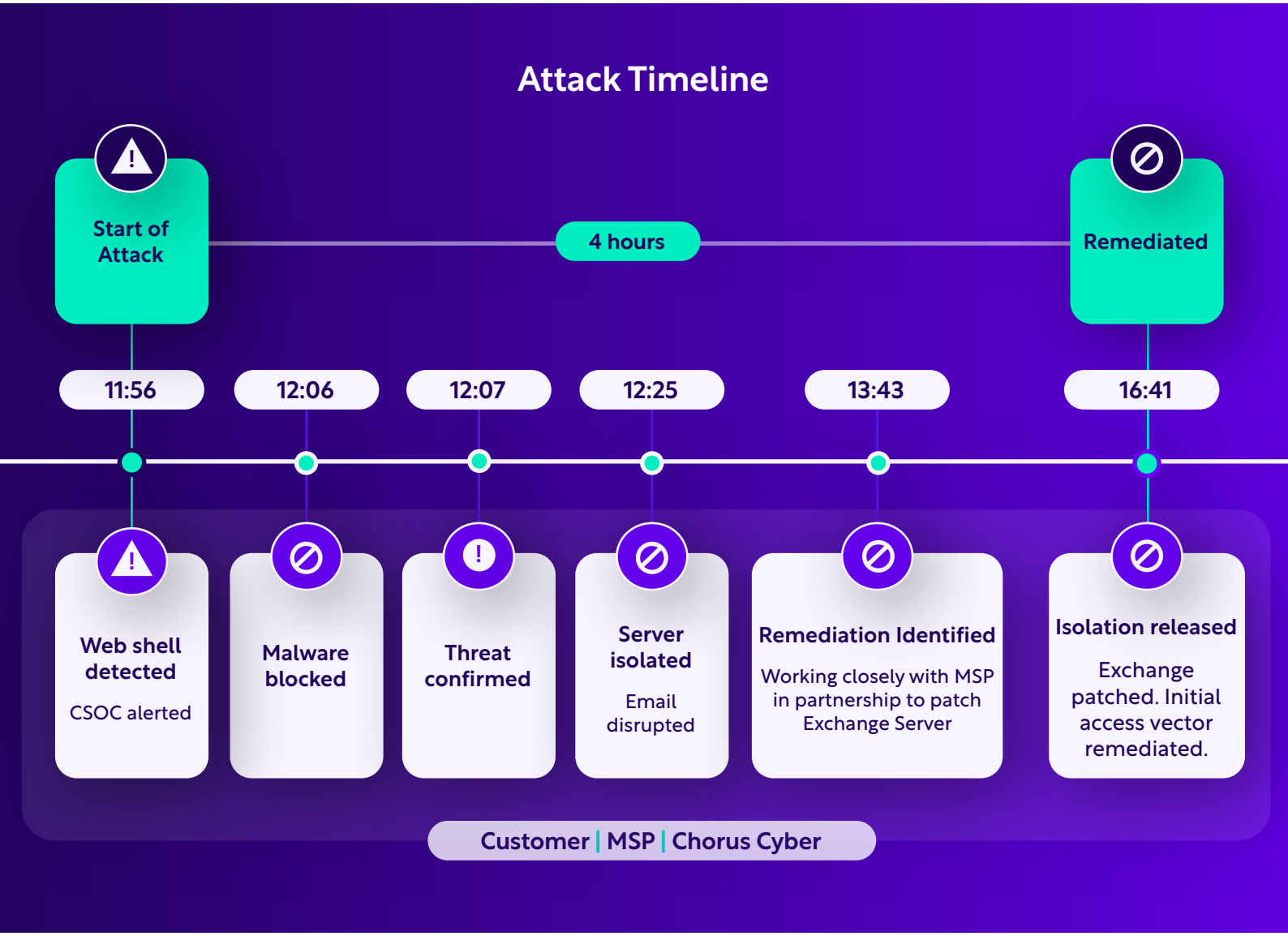
Weeks after onboarding, a new variant of the original exploit emerged. Within hours of disclosure, the same company was once again targeted, this time with more refined tactics.

But this time, the outcome was very different.

At 11:56 AM, the Chorus CSOC detected a webshell on the Exchange server. The threat was escalated immediately:

- The affected server was isolated within minutes
- Malware artefacts were identified, contained, and removed
- Recovery was coordinated directly with the MSP
- Full email functionality was restored by 4:41 PM

Total operational impact: One hour of email disruption. Four hours for threat to be totally eliminated.



The Role of MXDR and Microsoft

What is MXDR?

Managed Extended Detection and Response (MXDR) is a next-generation approach to cybersecurity that combines 24/7 threat monitoring with AI-driven threat intelligence, incident response, and ongoing security improvement. Chorus Cyber's MXDR service builds on Microsoft's leading security technologies, including:

- **Microsoft Defender XDR:** Unifies signals across identity, email, endpoints, and apps
- **Microsoft Sentinel:** Cloud-native SIEM and SOAR for proactive threat hunting
- **Microsoft Purview:** Ensures compliance, governance, and insider risk management

With MXDR, organisations gain a proactive posture, enabling them to detect and respond to threats faster than attackers can act.

Why Microsoft Security?

Microsoft is now a clear leader in enterprise cybersecurity. Its integrated stack allows organisations to consolidate tooling while improving their ability to detect, analyse, and respond to advanced threats.

Key benefits include:

- 73 trillion global threat signals ingested daily
- Built-in Zero Trust architecture
- Native integration with Microsoft 365 workloads
- AI-powered response and analytics
- Available in existing licensing (e.g., Microsoft 365 Business Premium, Microsoft Defender Suite)

> **"We already had Microsoft 365 and MXDR turned it into a security powerhouse."**
>
> IT Manager, Manufacturing Client

Whitepaper

Why Partner with Chorus Cyber?

Expand your services, not your overhead

Chorus Cyber offers a Microsoft-centric partner programme that enables MSPs, resellers, and systems integrators to deliver enterprise-grade cybersecurity services to their own customers without building an in-house SOC.

As members of the Microsoft Intelligent Security Association (MISA), our services meet Microsoft's stringent technical requirements to deliver a best-in-class service.

Member of
Microsoft Intelligent Security Association
Microsoft Security
Microsoft Verified Managed XDR Solution

<5 mins
Mean Time to Acknowledge

<20 mins
Mean Time to Respond

98%
Client Satisfaction Feedback

Key benefits to partners

- Easily deliver sought-after managed security services
- Open opportunities with new and existing clients
- Best-in-class service with industry leading response times
- Benefit from sales & marketing support as a partner
- Reduce your customers' cyber risk and increase loyalty
- Maximise value from clients' Microsoft licensing

What next?

If you have any questions or wish to find out more about our services, please contact us.

partners@choruscyber.com | www.choruscyber.com

chorus cyber