# CASE STUDY

## From Crisis to Control: Adarma's Incident Response in Action

Written by Laura Ingram,
Managing Consultant at Adarma

## Introduction

Given the ever-changing nature of cyber threats, businesses need to implement swift and effective incident response (IR) strategies to mitigate damage and restore operations.

A global FTSE 100 engineering firm with operations across EMEA, APAC, and the USA, faced repeated ransomware incidents that disrupted its operations and left its security team exhausted.

Seeking to enhance its cyber resilience and centralise security operations, the organisation turned to Adarma for expert IR and long-term security transformation.

## Adarma's Rapid Deployment and Immediate Actions

Upon being contacted by the customer's CISO and technical director, Adarma responded within 12 hours, deploying a dedicated team onsite. The immediate focus was to assess the severity of the breach, implement containment strategies, and restore critical operations.

Recognising that the customer's Security Operations Centre (SOC) was under-resourced and fatigued, Adarma provided 24x7 monitoring and hands-on support to stabilise the situation.

## Adarma's Key Initial Actions Included:

- Conducting rapid triage, containment, and remediation to reduce the impact of the ransomware.
- Providing 24x7 on-site monitoring to alleviate stress on the customer's security team.
- Leveraging available threat intelligence and customer-specific data to identify high-priority threats.
- Establishing an interim security monitoring system using a temporary Security Information and Event Management (SIEM) solution to regain visibility.

These swift interventions helped the customer regain control of its security posture while ensuring continuous threat detection and mitigation.

# Adarma Acts as the Primary SOC

## Restoring Security and Preventing Reinfection

Due to the severity of the attack and the strain on the internal security team, Adarma assumed the role of the customer's primary SOC during the live incident. Adarma's experts followed the 'Get Them Out, Keep Them Out' (GTO-KTO) strategy.

This methodology prioritises two fundamental security principles:

- GTO: Quickly identify, isolate, and eradicate attackers from the environment.
- KTO: Reinforce defences to prevent adversaries from re-entering the network.

By adhering to this structured approach, Adarma ensured a well-documented response, enabling seamless collaboration with the customer's internal teams and external stakeholders.

## Enhancing Detection Capabilities with Temporary SIEM

This ransomware attack severely disrupted the customer's existing SIEM infrastructure, leaving security teams without crucial visibility into ongoing threats. To restore detection capabilities, Adarma took the following actions:

- Deployed a temporary SIEM solution, leveraging the customer's Splunk instance to quickly re-establish centralised security monitoring.
- Re-established log collection processes, prioritising critical data sources that had been compromised by the ransomware.
- Integrated multiple security technologies, including Microsoft Defender and Tanium, ensuring end-to-end threat detection across both cloud and on-premises environments.

This strategic move enabled real-time security monitoring, allowing Adarma to detect and neutralise emerging threats efficiently during the recovery process.

## Adapting to a Heightened Threat Landscape

During the ransomware attack, an international geopolitical event introduced additional risks, requiring heightened vigilance. Adarma took a proactive stance to mitigate these threats by:

- Conducting industry-specific threat hunts to identify new vulnerabilities.
- Onboarding critical detections into Adarma's 24x7 SOC for continuous monitoring.
- Providing real-time intelligence briefings to the customer's executive leadership for informed decision-making.

This proactive approach ensured that the customer was equipped to manage both immediate and emerging cyber threats with confidence.

## Structured Onboarding and Strengthening Cyber Resilience

While managing the live incident, Adarma laid the foundation for long-term security improvements. The onboarding process included:

- Developing and implementing custom Splunk use case detections to safeguard the customer's most valuable assets.
- Conducting comprehensive security assessments and risk evaluations to refine the customer's security posture.
- Offering hands-on training and guidance to the customer's internal team, enabling them to adopt advanced security measures confidently.
- Modifying standard on-call monitoring processes to provide strengthened interim support.

Through these efforts, the customer transitioned from reactive crisis management to a more structured and resilient security framework.

## Delivering Long-Term Value and a Strategic Partnership

Adarma's support extended well beyond the initial ransomware recovery, delivering lasting security improvements that have transformed the customer's cybersecurity operations. Key benefits included:

- Minimised Operational Downtime: Swift containment and remediation allowed business operations to resume quickly.
- Enhanced Cybersecurity Maturity: Strengthened security operations positioned the organisation to better withstand future cyber threats.
- Reduced Security Team Burnout: Adarma's 24x7 coverage alleviated pressure on internal staff, allowing them to focus on strategic initiatives.
- Trusted Long-Term Partnership: Initially an industry connection, the organisation became a long-term Adarma customer, adopting Adarma's XDR Managed Service for ongoing security support.

# Key Lessons Learned

**Based on the customer's experience and feedback, here are some key takeaways for other organisations aiming to improve their cyber resilience:**

- **Rapid IR Matters:** A well-coordinated, expert-led response can significantly reduce the impact of cyber incidents.
- **Investment in Security Operations is Crucial:** A well-resourced SOC with expert threat intelligence enhances overall security posture.
- **Trusted Cybersecurity Partnerships Provide Strength:** Engaging a dedicated cybersecurity partner ensures the right expertise, tools, and support are available when needed most.
- **Continuous Learning and Improvement is Key:** Regular security assessments, training, and strategic planning enhance long-term preparedness.

ADARMA
TOGETHER WE'VE GOT THIS

# Conclusion

**This ransomware attack could have resulted in severe financial and reputational damage, but with Adarma's rapid intervention, its security posture was restored and strengthened.**

**By leveraging advanced threat detection, real-time monitoring, and expert guidance, Adarma mitigated the immediate impact and helped the customer to build a resilient security framework for the future.**

**For organisations seeking expert-led cybersecurity solutions, Adarma's IR services offer a proven approach to minimising risks and ensuring operational continuity.**

**More information can be found on our website: adarma.com**
**To speak to an expert, email us at: hello@adarma.com**