CASE STUDY

KUDELSKI SECURITY

Elevating cyber resilience with next-gen threat detection and rapid incident response

Kudelski Security's 24/7 MDR ONE Resolute service empowered a global tech company to enhance security monitoring and incident response while advancing its digital transformation.

CHALLENGE

A global tech company with over 2,000 employees faced significant challenges in maintaining a comprehensive level of threat detection, investigation, and response.

The diverse threat landscapes across several business units required a nuanced, advanced approach to protecting its intellectual property, brand, and bottom line.

The group CISO wanted to replace a legacy Managed Detection and Response (MDR) service with a modern and effective solution that would avoid the need to build an internal Security Operations Center (SOC).

The goal was clear: to enhance the company's overall security posture in a cost-effective manner compared to an in-house approach, support the company's digital transformation efforts, and achieve improved visibility and detection capabilities for cloud resources and identities.

SOLUTION

To strengthen its security, the company partnered with Kudelski Security. They implemented MDR ONE Resolute, a next-gen MDR solution which includes the following:

- Configured to ingest security data from multiple sources: emails, networks, cloud platforms (e.g., AWS and Azure), identities, endpoints, vulnerabilities and applications from across the globally distributed workforce.
- Integration of a high-performant data lake and a SOC platform into Kudelski Security's FusionDetect™ XDR platform to enable seamless ingestion, storage, enrichment and cross-correlation, creating context-rich attack stories for analysts.

GROUP CISO

> "Kudelski Security's MDR ONE Resolute service has transformed our approach to threat management. The enhanced threat detection and investigation capabilities, coupled with IR expertise have been instrumental in improving our security posture."
>
> *Group CISO, B2B technology company*

COMPANY PROFILE

Industry: B2B Tech

Sector: Technology Solutions

Location: Global

Footprint: 2,000+ employees worldwide

MAIN CHALLENGE

- The company required a flexible and robust cybersecurity solution to manage its diverse threat landscape with efficient, 24/7 threat detection and investigation without compromising security objectives vs growing data storage costs.

- 24/7 Risk-based threat detection, hunting, investigation, and response should a breach occur.
- The solution enables a smooth transition to a cloud-based model. Threat detection, investigation, and response are enhanced thanks to advanced analytics and AI-based detection support.

OUTCOMES

Within days of implementing MDR ONE Resolute, the client observed significant improvements:

- **Enhanced visibility** and contextual understanding of threats improved investigations and identification of system configuration issues.
- **Proactive detection** of inappropriate end user behavior, such as accessing resources from non-compliant devices, was enabled by correlating identity, cloud, and EDR data.
- **Budget predictability** was achieved, thanks to the coupling of costs with the number of endpoints rather than data volume.
- **Improved collaboration and efficiency.** Streamlined access to the platform for direct insights, custom investigations and self-integrations.
- **Improved retroactive threat hunting** and supported compliance efforts through ongoing monitoring and the default 12-month hot data retention.

Threat detection accuracy improved significantly, thanks to greater visibility into the enterprise IT environment.

MDR ONE Resolute has helped the company achieve its digital transformation goals. The client now has greater confidence, enhanced security and streamlined operational costs.

RESULTS

Strengthened overall security and risk management processes.

Achieved four times more true positive detections compared to the previous siloed approach.

Elevated confidence in protecting partner, client, and employee data.

Delivered cost predictability with billing based on asset count rather than data volume.

Provided detailed reports enabling the in-house security team to effectively remediate issues, while the C-suite gained valuable insights for monitoring and performance tracking.

Seamless integration with existing systems.

Kudelski Security, a division of the Kudelski Group (SIX: KUD.S), is an innovative, independent provider of tailored cybersecurity solutions to enterprises and public sector institutions. Kudelski Security is headquartered in Cheseaux-sur-Lausanne, Switzerland, and Phoenix, Arizona, with operations in countries around the world.

KUDELSKI SECURITY

info@kudelskisecurity.com | www.kudelskisecurity.com