zensar

# U.S. based life science equipment manufacturer secures its digital transformation journey

Case Study

# Overview
## A geographical expansion

The client is a life science equipment manufacturer headquartered in the U.S. with operations in Europe, Canada, and Japan. It was expanding across geographies via strategic mergers and acquisitions. There was a need to create an efficient security monitoring program for remote working situations brought about by the COVID-19 pandemic. The client wanted to monitor advanced threats on the legacy, on-premise, and cloud servers, applications, and platforms.

# Challenges
## Security at stake

The client had a small security team and wanted to reduce false-positive alerts and automate repetitive monitoring tasks. It was undergoing a digital transformation journey to create a cost-effective and efficient security monitoring program that handled the concerns and challenges of remote working conditions.

# Solution
## 24x7 monitoring of security incidents

We conducted a two-week free assessment to understand the client's current monitoring practices. We also provided a report on the recent security monitoring coverage, possible improvements (additional integrations, use cases, runbooks, etc.), and multi-fold cost-saving opportunities to make a business case for migration to Microsoft Azure Sentinel-based platform.

Within 12 weeks of contract sign-off, the client was onboarded to the Microsoft Azure Sentinel-powered managed detection and response (MDR) platform. As part of the onboarding process, the following key activities were carried out:

- Customer subscription and Azure Sentinel set up
- Privileged identity management (PIM) roles configuration and lighthouse connectivity set up
- Log sources, alerts, reports, threat-hunting queries, and playbooks integration and configuration
- Security operation center (SOC) workflow creation and information technology service management (ITSM) integration
- 24x7 security incidents monitoring

# Impact

## Secured environment and improved productivity

- Better use case coverage to security threats and improved overall mean time to respond (MTTR)
- Enhanced resource productivity due to automation
- Integration with ServiceNow to capture all organizational security incidents in one common platform
- Fixed charge based on the capacity reservation

zensar

An RPG Company

We conceptualize, build, and manage digital products through experience design, data engineering, and advanced analytics for over 130 leading companies. Our solutions leverage industry-leading platforms to help our clients be competitive, agile, and disruptive while moving with velocity through change and opportunity.

With headquarters in Pune, India, our 10,000+ associates work across 33 locations, including San Jose, Seattle, Princeton, Cape Town, London, Singapore, and Mexico City.

For more information please contact: **velocity@zensar.com | www.zensar.com**