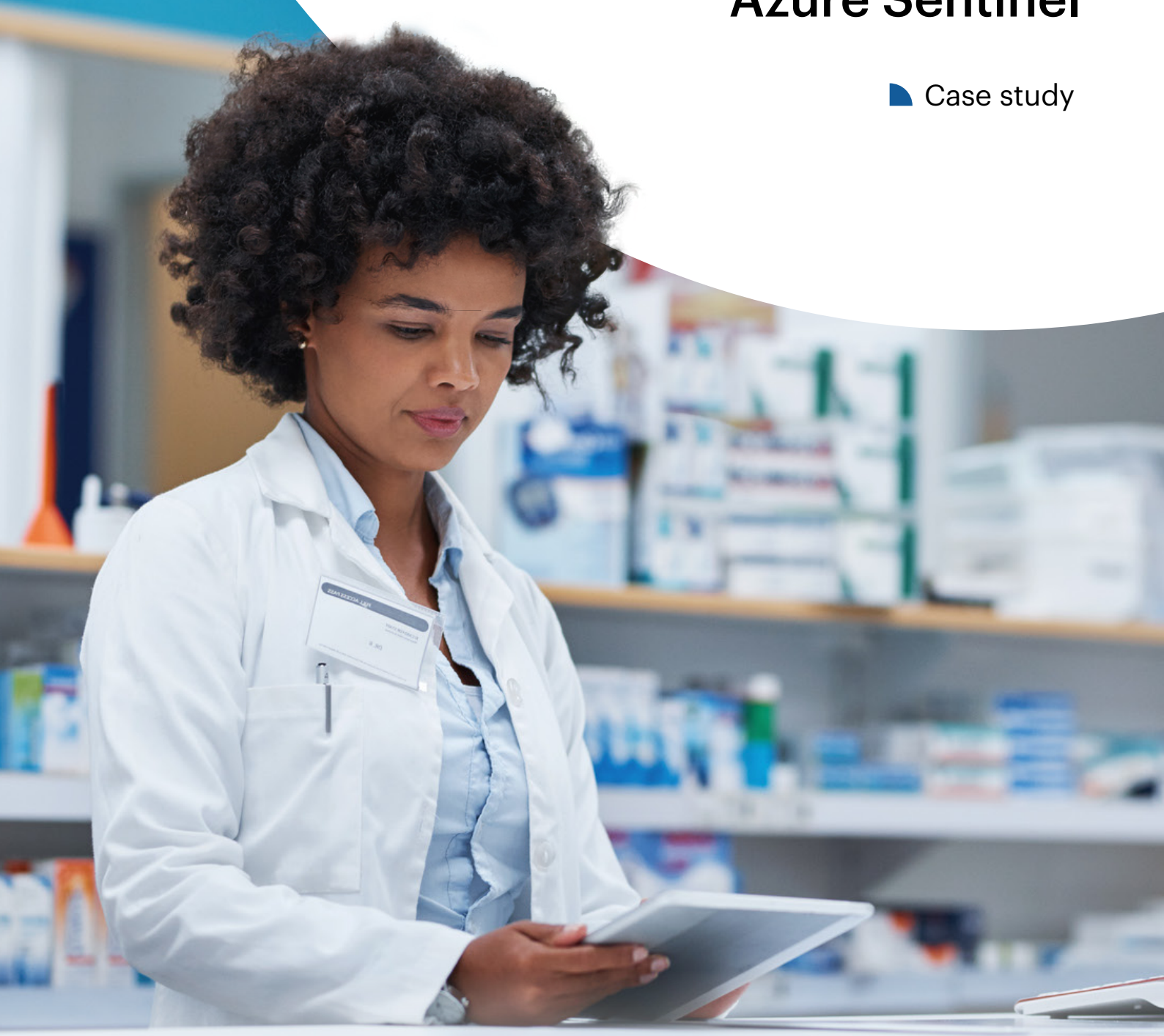
zensar

Transforming Security Monitoring for a US Pharma Company With Azure Sentinel

Case study



An RPG Company

Overview

Enabling robust global security monitoring to facilitate remote working

The client, a leading US-based pharmaceutical company with operations across Europe, Canada, and Japan, was expanding across geographies through strategic mergers and acquisitions. It needed to create an efficient security monitoring program for an organization to address the dynamic needs of remote working situations. It was imperative for the client to monitor the legacy, on-prem, and cloud servers, applications, and platforms to keep a check on advanced threats.

Zensar helped effectively onboard the client to the Azure Sentinel-based threat detection and response platform. We also integrated the platform with customer ITSM solutions to provide a single source of truth for organizational incidents. Security monitoring service was delivered from our cyber defense centers and covered a 24x7x365 service window.

Challenges

The client needed to create an efficient and cost-optimized security monitoring program for an organization to cater to the changing need for remote working situations. With a small security team, the client found it challenging to monitor its tech infrastructure effectively, minimize false-positive alerts, and automate repetitive monitoring tasks.

Solution

We conducted a two-week complementary assessment to understand the current monitoring practices and their gaps. As part of the deliverable, Zensar provided a comprehensive report on the existing security monitoring coverage, identified the scope for improvement (including additional integrations, use cases, runbooks, etc.), and enabled multifold saving opportunities to build the business case for migrating to the Azure Sentinel-based platform.

The client was onboarded to the ZenAIR platform within 12 weeks of contract sign-off. As part of onboarding, we undertook critical activities that included:

- Setting up of client subscription and Azure Sentinel, if not provisioned
- Configuring PIM roles and setting up lighthouse connectivity
- Integrating and configuring log sources, alerts, reports, threat-hunting queries, and playbooks
- Building the SOC workflows and ITSM integration
- Monitoring L1, L2, and L3 security incidents 24*7

Impact

Partnering with Zensar for comprehensive security services enabled the client to ensure the following:

- 90 percent reduction in false positive reporting and better coverage of security threats
- 70 percent increase in overall MTTR
- 60 percent improvement in resource productivity due to automation
- Single platform with ServiceNow integration to capture all organizational security incidents
- 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 145 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 11,500+ associates work across 30+ locations, including Milpitas, Seattle, Princeton, Cape Town, London, Singapore, and Mexico City.

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