HCLTech | Supercharging Progress™

# Providing intelligent security to a medical OEM

Through proven cybersecurity framework using Microsoft SIEM and SOAR solution

## Customer profile

The  client is an America-based company that specializes in the manufacturing of medical equipment and sales of medical devices, instrument systems and reagents.

## Customer business challenges

- The client was significantly reliant on a cloud-native business model for business and operational concerns which were prime targets for cyber-attacks and lacking advanced security measures.
- There was a lack of robust monitoring tools to detect and respond to security threats as a defense against business disruptions.
- The client was struggling to connect its disparate tools and leverage its data assets at scale for proactive defense and business solutioning.
- The client's endpoint detection and response (EDR) and lacking any advanced threat protection (ATP) solutions were outdated.

# HCLTech's solution approach

The client chose HCLTech Cybersecurity & GRC as its trusted technology partner to help supercharge progress of their enterprise security posture with a proven security framework and transformation delivery. HCLTech stepped in to evaluate the client's existing digital ecosystem and assessed that the company needed advanced next-gen security upgrades to secure its system and assets from outside threats. This also included the deployment of an effective security monitoring and data security framework across the enterprise environment and leveraging information insights to handle its current and future use case scenarios.

To address these goals, HCLTech deployed a security information and event management (SIEM) and a security orchestration, automation, and response (SOAR) platform for their IT landscape. Additionally, we also upgraded and replaced the client's legacy EDR and ATP systems with an advanced solution stack with four key components:

### Microsoft Sentinel:

- We carried out a complete Microsoft Sentinel proof of concept (POC) exercise in the client's development environment for current and future use cases and formulated a strategic vision for SIEM and SOAR implementation.
- Next, we planned, analyzed, designed, built, tested, and run activities for Sentinel tools and built use cases and workbooks for SOAR.

### Azure Microsoft Defender:

- Following that, we completed the Microsoft Defender ATP POC and deployed the solution in the client's environment through the design, build, test, and run stages.
- HCLTech implemented an active data loss prevention (DLP) solution using the Defender ATP/DLP to support the client's ability to identify and label sensitive or classified information.

### MDCA (Microsoft Defender for Cloud Apps):

- We conducted app discoveries with the Cloud App Discovery tool.
- Additionally, the solution stack secured SaaS applications end-to-end, using the MDCA tool.
- Our team of experts also implemented the MIP (Microsoft Information Protection) setup and MDCA for data protection.

### Azure Security Center:

- HCLTech designed and deployed the Azure Security Center and its supporting capabilities (Log Analytics, etc.) to monitor and manage the security of cloud computing resources.
- At the end, we connected the client's existing centralized management system to the security center, via application programming interfaces (APIs).

## Value delivered

**20%** reduction in cost on license & agent management cost

**65000** endpoints managed through automated detection & remediation through MS Defender

Completed Microsoft Defender ATP POC with **3 months** & deployed the solution in client's environment within **12 months**

**~ 10%** increase in efficiency of threat detection and still qualifying

CI-112AllAll734745796581-EN00GL